Technische Universität München

Fakultät für Elektrotechnik und Informationstechnik

Secret Key Generation with Perfect Secrecy; Source Uncertainty and Jamming Attacks

Sebastian Johannes Baur

Vollständiger Abdruck der von der Fakultät für Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender:		Prof. Dr.-Ing. Georg Sigl
Prüfer der Dissertation:	1.	Prof. Dr.-Ing. Dr.rer.nat. Holger Boche
	2.	Prof. H. Vincent Poor, Ph.D.

Die Dissertation wurde am 25.09.2019 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 10.11.2021 angenommen.

Secret Key Generation with Perfect Secrecy; Source Uncertainty and Jamming Attacks

Sebastian Johannes Baur

Acknowledgement

This dissertation was written during my time as a research assistant at the Technische Universität München. I would like to thank all the people who supported me while working on this dissertation. First and foremost I thank my advisor Prof. Holger Boche, for giving me the opportunity to work with him and for all his advice and motivation. Particular thanks go to Prof. H. Vincent Poor for acting as the second referee of this dissertation and to Prof. Georg Sigl for serving as the chairman of the dissertation committee. I want to thank all my colleagues for the pleasant social atmosphere and helpful discussions. I am very grateful for the constant support and encouragement of my family. Finally my special thanks go to Steffie for her support.

Zusammenfassung

Es wird die Erzeugung eines geheimen Schlüssels an zwei Datenendgeräten betrachtet. Jedes Datenendgerät beobachtet dabei jeweils einen Ausgang einer Quelle mit zwei korrelierten Komponenten. Zusätzlich kann eine Hilfsnachricht vom ersten Datenendgerät zum zweiten Datenendgerät über einen rauschfreien, öffentlichen Kanal gesendet werden. Es wird angenommen, dass die Hilfsnachricht bzw. die privacy leakage ratenbeschränkt ist. Es wird die maximale geheime Schlüsselrate bestimmt, die erreicht werden kann, so dass der Schlüssel gleichverteilt und perfekt sicher ist. Damit ist der Schlüssel unabhängig von der Hilfsnachricht. Entsprechende Resultate werden für verschiedene Quellenmodelle bewiesen. Dazu zählen ein Compoundmodell und verschiedene Szenarien mit Störsendern, bei denen die Quelle von einem aktiven Angreifer manipuliert wird.

Abstract

Secret key generation at two terminals is considered. Each terminal observes one of the outputs of a source with two correlated components. Additionally one terminal can send a helper message to the second terminal via a noiseless public channel. It is assumed that this message or the privacy leakage respectively is rate constrained. The maximum secret key rate, that can be achieved such that the key is uniformly distributed and meets the perfect secrecy requirement, is determined. So the key is independent of the helper message. Corresponding results are established for different source models, comprising a compound model and various jamming scenarios, where the source is manipulated by an active attacker.

Contents

Notation

We use standard notation, comparable to the notation introduced in [26] or [47]. For the convenience of the reader we repeat some of these conventions used in this work. For $n \in \mathbb{N}$ we define $[n] = \{1, \cdots, n\}$. The convex hull of a set $\mathcal{A}$ is denoted by $conv(\mathcal{A})$. For $x \in \mathbb{R}$ we define $|x|^+ := \max\{x, 0\}$ whereas $\lfloor x \rfloor$ and $\lceil x \rceil$ denote the largest integer k with $k \leqslant x$ and the smallest integer l with $l \geqslant x$ respectively. We write log for the logarithm to base 2 and $\exp(x)$ for 2^x. The natural logarithm to base e is denoted by ln. For a set $\mathcal{X}$ and a subset $\mathcal{A} \subset \mathcal{X}$ we write $\mathcal{A}^c$ for $\mathcal{X} \backslash \mathcal{A}$ and we denote the indicator function of $\mathcal{A}$ by $\mathbb{1}_{\mathcal{A}} \colon \mathcal{X} \to \{1, 0\}$. So for $x \in \mathcal{X}$ we have $\mathbb{1}_{\mathcal{A}}(x) = 1$ if and only if $x \in \mathcal{A}$. We denote the set of all distributions on $\mathcal{X}$ by $\mathcal{P}(\mathcal{X})$ and define the set of all channels from $\mathcal{X}$ to $\mathcal{Y}$ (i.e. stochastic matrices)

$$\mathcal{P}(\mathcal{Y}|\mathcal{X}) = \{(W(\cdot|x))_{x \in \mathcal{X}} \colon W(\cdot|x) \in \mathcal{P}(\mathcal{Y}) \quad \forall x \in \mathcal{X}\}.$$

Let $P, Q \in \mathcal{P}(\mathcal{X})$. We define the total variation distance between P and Q such that

$$\|P - Q\|_1 = \sum_{x \in \mathcal{X}} |P(x) - Q(x)|.$$

For $P \in \mathcal{P}(\mathcal{X})$ and $Q \in \mathcal{P}(\mathcal{Y})$ we define $P \otimes Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ by

$$(P \otimes Q)(x, y) = P(x)Q(y)$$

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$. For $n \in \mathbb{N}$ we define $P^{\otimes n} \in \mathcal{P}(\mathcal{X}^n)$ by

$$P^{\otimes n}(x^n) = \prod_{i=1}^{n} P(x_i)$$

for all $x^n \in \mathcal{X}^n$. For $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ and $V \in \mathcal{P}(\bar{\mathcal{Y}}|\bar{\mathcal{X}})$ we define $W \otimes V \in \mathcal{P}(\mathcal{Y} \times \bar{\mathcal{Y}}|\mathcal{X} \times \bar{\mathcal{X}})$ by

$$(W \otimes V)(y, \bar{y}|x, \bar{x}) = W(y|x)V(\bar{y}|\bar{x})$$

for all $(x, \bar{x}, y, \bar{y}) \in \mathcal{X} \times \bar{\mathcal{X}} \times \mathcal{Y} \times \bar{\mathcal{Y}}$. Consider random variables X, Y and Z. We denote the entropy of X by $H(X)$, the conditional entropy of X given Y by $H(X|Y)$ and the mutual information of X and Y by $I(X \wedge Y)$. $X - Y - Z$ means that these random variables form a Markov chain in this order.

1 Introduction

1.1 Motivation

Lately, considerable effort has been devoted to deriving information theoretic results that can be applied in communication scenarios where low delay is an essential requirement [40]. For many of these applications, the communication task should be performed securely due to the presence of eavesdroppers. Examples for such applications in the context of the Tactile Internet are discussed in [27]. These applications range from vehicle to vehicle communications to automation in industry. The authors of [27] also discuss the infrastructure requirements to realize these applications. The Tactile Internet is considered a promising forthcoming innovation and motivated considerable fundamental research. Currently the Tactile Internet is in the process of standardization and the corresponding results can contribute fundamentally to the fifth generation mobile network 5G and systems beyond, especially 6G [1]. As discussed in [27], information theoretic security can contribute significantly to realize communication systems that combine low latency and security. Encryption algorithms that exploit the limited computing power of an eavesdropper to achieve secure communication are implemented at higher protocol layers. So the low delay constraints imposed by the applications that we want to realize can not be met using such encryption algorithms. In contrast, security should be implemented together with error correction on the physical layer. By not separating encryption from error correction information theoretic security allows for secure communication with low delay.

A well known model in information theoretic security is the source model for secret key (SK) generation with one way public communication where we study the problem of establishing a SK at two terminals. We consider SK generation based on the correlated outputs of a source with two components where one of the outputs is available at each terminal. Additionally information can be transmitted from one terminal to the other via a noiseless public channel. So in this work we consider SK generation from a two component source with one way forward communication which is a special case of the general problem of SK generation from a source. We are interested in the largest possible SK that can be generated from the source output.

The problem of SK generation was introduced by Maurer in [36] and by Ahlswede & Csiszár in [5]. There it is allowed that the message sent over the noiseless public channel is arbitrarily large. In [25] various extensions of the model are studied. In particular the authors consider the setting where the public message is rate constrained. In [46] the source is replaced by a compound source, thus taking uncertainty on the source statistics into account, while also assuming that the public message is rate constrained. (For an introduction to SK generation see the standard reference for physical layer security [20].)

In a different line of research Ignatenko & Willems study SK generation from a biometric source in [32]. They analyse the source model described in [5] but they regard the privacy leakage of the SK generation process. The privacy leakage is the information on the source output observed at the first terminal contained in the public message. In [32] the privacy leakage is rate constrained. In [29] the corresponding compound setting is studied.

In the literature different secrecy requirements and different requirements on the key distribution are considered. In [5] Ahlswede & Csiszár prove their results for perfect secrecy and uniform key distribution. In [25], [29], [32] and [46] the authors allow for weaker secrecy conditions and weaker requirements on the key distributions.

The SK generated from the source can for example be used for secure storage. For this purpose the SK is used as a one time pad. The model for SK generation further serves as the basis for an information theoretic treatment of authentication when an additional privacy leakage rate constraint on the source observations is imposed [32].

1.2 Contributions

In this work we consider generalizations of the source model for SK generation. In contrast to a lot of the literature on source models for SK generation we describe protocols for this model that achieve perfect secrecy and uniform distribution of the SK. As discussed, in large parts of the literature protocols for SK generation meet weaker requirements such as weak secrecy or strong secrecy and near uniform distribution of the SK. Determining the largest possible SK that can be generated from the source output under the strongest requirements, that is perfect secrecy and uniform key distribution, has only been achieved for the unconstrained public communication case.

We generalize the source model by taking source uncertainty into account. In particular we study the compound source model and a jammed source that is modeled by means of an arbitrarily varying channel (AVC). For the latter model we distinguish between the case where the jammer knows the public message and the case where the public message is only known to the eavesdropper but not to the jammer. For all of these settings we consider SK generation with a privacy leakage rate constraint. The corresponding capacity results are derived in Chapter 3 (and auxiliary results needed for the proofs in Chapter 2). Parts of the results are published in [7], [8], [9] and [10].

We also consider the case where the public message is rate constrained. Again we study a compound model and an AVC based model. Various jamming constellations are taken into account. That is a jammer that has access to the public message and a jammer without access to the public message. In the context of AVCs common randomness (CR) is known to be an important resource. Thus we also consider jamming scenarios where CR is available to the legitimate users. Capacity results for these scenarios are proved in Chapter 4. These results are published in [12] and [13].

Further Results

During my time as a research assistant at the Technische Universität München we obtained further interesting results not included in this thesis:

- Ahlswede & Dueck introduced identification via channels as a new paradigm in information theory. They showed that the number of messages that can reliably be identified over a noisy channel grows doubly exponentially with the block length. In [14] we also consider identification, but we assume that messages are stored on a database such that they can be identified. Additionally the legitimate users have access to the output of a source. This source allows us to store messages securely. It is also used to increase the number of messages that can be stored securely on the database and identified reliably. We define a protocol for secure storage for identification such that the number of stored messages that can be identified grows doubly exponentially with the number of symbols read from the source and the number of storage cells available respectively. We also consider the privacy leakage of the protocols used for identification. So it makes sense to consider two sources. We assume one source is public whereas the other source only is available to the legitimate users. The public source is used to increase the number of messages that can be identified while the second source is used to guarantee secrecy. Using the public source does not increase the privacy leakage. So we can possibly achieve a higher number of messages that can be identified while the privacy leakage does not increase using two sources. As a by-product we also get new results on common randomness generation.

- In [11] a scenario related to the source model for SK generation is considered where instead of SK generation, the goal is to securely store data in a public database. The database allows for error-free storing of the data, but is constrained in its size which imposes a rate constraint on the storing. The corresponding capacity for secure storage is known and it has been shown that the capacity-achieving strategy satisfies the strong secrecy criterion. Then the case when the storage in the public database is subject to errors is considered and the corresponding capacity is characterized. Additionally, the continuity properties of the two capacity functions are analyzed. These capacity functions are continuous as opposed to the discontinuous secret key capacity with rate constraint. It is shown that for secure storage the phenomenon of super activation can occur. Finally, it is discussed how the results differ from previous results on super activation.

A complete list of publications is given at the end of the thesis.

Copyright Information

ding journal or conference proceedings. The publications [7, 9, 11, 14] are

2 Preliminaries

In this chapter we briefly review the source model for SK generation. We present various definitions of achievability for this model and motivate our interest in protocols for SK generation that achieve perfect secrecy. We also explain how the source model for SK generation can be interpreted as a model for secure storage of cryptographic keys using physical unclonable functions (PUFs). As mentioned above this allows the source model for SK generation to provide a basis for an information theoretic study of authentication.

In the second part of this chapter we summarize fundamental results of information theory that will prove to be useful in later parts of this work.

2.1 Source model for SK generation and perfect secrecy

In [25] several scenarios for SK generation from a source are considered. One of these is the basis for the settings that we consider in this work. It is depicted in Figure 2.1. As described before, a SK K should be generated at two terminals. SK generation is based on the correlated source outputs X^n and Y^n, where at each terminal one of these source outputs is available. Additionally a helper message M can be transmitted from one terminal to the other via a noiseless public channel.

Consider the RVs X and Y. The source puts out RVs $X^n = (X_1, \cdots, X_n)$ observed at one terminal and $Y^n = (Y_1, \cdots, Y_n)$ observed at the other terminal, both of block lengths $n \in \mathbb{N}$. We assume $P_{X^nY^n} = P_{XY}^{\otimes n}$, i.e., the source is a discrete memoryless multiple source (DMMS) with two components. As in [25] we represent the terminals by the symbol of the corresponding alphabet. Terminal $\mathcal{X}$ represents the terminal that sends the helper message, whereas terminal $\mathcal{Y}$ represents the terminal that receives the helper message. So the RV M that represents the helper message and the RV K that

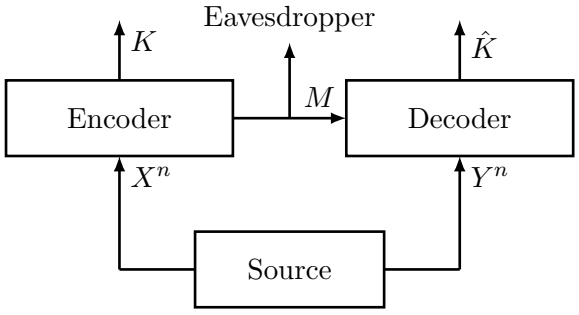

Figure 2.1: SK generation with one way public communication as in [25].

represents the SK are generated at terminal $\mathcal{X}$ (making use of X^n). The RV $\hat{K}$ that represents the reconstruction of the SK is generated at terminal $\mathcal{Y}$ (making use of M and Y^n).

In [25] it is assumed that $(K, M) = f(X^n)$ and $\hat{K} = g(M, Y^n)$ are generated from the data available at $\mathcal{X}$ and $\mathcal{Y}$ respectively using deterministic functions (i.e., no randomization is used to generate these RVs) and that K and $\hat{K}$ take values in the same alphabet $\mathcal{K}$. We call the pair (f, g) with $f\colon \mathcal{X}^n \to \mathcal{K} \times \mathcal{M}$ and $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$ a SK generation protocol.

The considerations above establish the joint distribution of K, M and $\hat{K}$ as follows. For all $(k, m, \hat{k}) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K}$ we have

$$P_{KM\hat{K}}(k, m, \hat{k}) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} P_{XY}^{\otimes n}(x^n, y^n) \mathbb{1}_{f^{-1}((k,m))}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}((y^n, m)).$$

A SK generation protocol should have certain properties, specified in the following definition, to be considered a good SK generation protocol. (This definition is equivalent to the corresponding definition in [25], cf. [25, Definition 1.2].)

Definition 2.1. *Let $L \geqslant 0$. We call $R \geqslant 0$ an* achievable secret key rate with rate constraint L *if for any $\epsilon > 0$ and sufficiently large n there is a SK generation protocol such that*

$$Pr(K \neq \hat{K}) \leqslant \epsilon \tag{2.1}$$
$$\tfrac{1}{n} I(K \wedge M) \leqslant \epsilon \tag{2.2}$$
$$\tfrac{1}{n} H(K) \geqslant \tfrac{1}{n} \log |\mathcal{K}| - \epsilon \tag{2.3}$$
$$\tfrac{1}{n} \log |\mathcal{K}| \geqslant R - \epsilon \tag{2.4}$$
$$\tfrac{1}{n} \log |\mathcal{M}| \leqslant L + \epsilon. \tag{2.5}$$

The SK capacity with rate constraint L *is the largest achievable secret key rate with rate constraint L and is denoted by $C_{SK}(L)$.*

According to this definition the RVs K and $\hat{K}$ represent a SK for the terminals $\mathcal{X}$ and $\mathcal{Y}$ if it holds that the SK can be reconstructed at terminal $\mathcal{Y}$ with high probability which follows from (2.1), the weak secrecy requirement (2.2) is met and K is nearly uniformly distributed which follows from (2.3). Moreover the rate of the SK is $\frac{1}{n} \log |\mathcal{K}|$ (cf. (2.4)) and the noiseless public channel from terminal $\mathcal{X}$ to terminal $\mathcal{Y}$ is rate constrained (cf. (2.5)).

$C_{SK}(L)$ (which corresponds to $C_{SK}(0, L)$ in [25]) is characterized in [25, Theorem 2.4].

Theorem 2.1 ([25]). *It holds that*

$$C_{SK}(L) = \max_U I(U \wedge Y)$$

where the maximization is over all RVs U such that $U - X - Y$ and

$$I(U \wedge X) - I(U \wedge Y) \leqslant L.$$

In fact it is shown in [25] that replacing each ϵ in Definition 2.1 by $\exp(-n\alpha)$ with some $\alpha > 0$ small enough but independent of n (which means replacing (2.1) - (2.5) by stronger constraints for n sufficiently large) does not reduce $C_{SK}(L)$. As mentioned in [25] the fact that stronger constraints often do not reduce capacity has been demonstrated for various models in information theoretic security. In [37] it has been pointed out that it is desirable to strengthen the (secrecy) conditions under which a given performance is achievable. This is one of the motivations of this work.

In [5] Ahlswede & Csiszár consider a simplified version of the setting studied in [25] described above in the sense that the public channel is not rate constrained. They characterize the corresponding capacity. Interestingly the authors of [5] show that replacing ϵ in (2.2) and (2.3) by 0 does not reduce the capacity for the unconstrained public communication setting. (It is pointed out in [5] that this can not be expected for a model where the eavesdropper has access to a third correlated output of the source. Thus we do not assume that the eavesdropper has such side information in our work.) This naturally motivates the problem of characterizing $C_{SK}(L)$ when ϵ is replaced by zero in (2.2) and (2.3).

$I(K \wedge M) = 0$, i.e., K and M are independent, is known as the perfect secrecy requirement and $\log |\mathcal{K}| = H(K)$ means the SK is uniformly distributed. (The combination of both requirements is equivalent to the requirement $H(K|M) = \log |\mathcal{K}|$.) Our interest in characterizing $C_{SK}(L)$ when these requirements are met has an additional motivation. Perfect secrecy in SK generation and uniform distribution of the SK are optimal in the sense described in [26, Proposition 17.1] and [20, Lemma 3.1]. There the generated SK is used as a one time pad to encrypt a message. The encrypted message then is transmitted via a public channel together with the helper message corresponding to SK generation. Then it is shown that perfect secrecy and uniform distribution of the SK allow for the best possible properties of this protocol in terms of secrecy. In order to achieve perfect secrecy and uniform distribution of the SK we allow for randomization at terminal $\mathcal{X}$ in contrast to the protocols used in [25].

2.2 Secure storage of cryptographic keys using PUFs

As described in [43, Chapter 13] variations in the manufacturing process of physical circuits lead to unpredictable variations of certain properties of the circuits (e.g. different run times). These variations can be exploited to construct PUFs. This means these PUFs are constructed from standard circuit components. Thus they can easily be integrated in the manufacturing process. The PUFs can be used to bind a SK to a physical device without storing the SK in secured non-volatile memory [43, Chapter 13]. So PUFs offer

a low cost alternative to storing a SK in secured non-volatile memory which is not always available.

We now describe how SK storage with PUFs can be realized according to [43, Chapter 13]. The PUF puts out a PUF response (by using a certain challenge as input to the PUF). This is a sequence of symbols from a finite alphabet after quantization (e.g. a sequence of bits). The PUF response can be generated whenever needed but it is influenced by noise. So the PUF response is not used as a SK directly. Instead error correction is used to generate a reliable SK. For this purpose after manufacturing the PUF a helper message, that is generated from a PUF response, is stored in non-secured non-volatile memory. This helper message is used for error correction. So all following PUF responses generated from the PUF can be mapped on the same SK making use of the helper message. As the helper message is stored in non-secured memory it should not reveal information about the SK as we have to assume that an attacker interested in the SK has access to the helper message. Additionally the helper message should be small such that the size of the non-volatile memory needed to store the helper message is small. This is important as the non-volatile memory is an expensive resource compared to the PUF construction.

We can interpret the source model for SK generation as a model for SK storage with PUFs. The PUF response used to generate the helper message is modeled by X^n. It is a RV as the manufacturing process is subject to unpredictable variations. The helper message corresponds to M and the corresponding SK is modeled by K. The noisy PUF response is modeled by Y^n and $\hat{K}$ models the reconstruction of the SK from Y^n and M.

In [32] the same model is used for a treatment of SK generation from a biometric source. In this model the source represents a biometric source, thus X^n models biometric data. Here the authors consider an additional quantity that is the privacy leakage. The privacy leakage represents the information about X^n contained in M. Motivated by the information theoretic interpretation of mutual information it is defined as $I(X^n \wedge M)$. The privacy leakage should be as small as possible because an eavesdropper should not learn a lot about the biometric data. In the context of SK storage with PUFs we can also try to minimize the privacy leakage (or more precisely the privacy leakage rate). As stated in [28] the privacy leakage should be minimized so that an eavesdropper cannot obtain information about a second SK stored using a second helper message but using the same PUF response.

In the remainder of this work we call the source in the source model for SK generation a PUF source or biometric source when we want to consider SK generation protocols that meet requirements (2.1)-(2.4) but where (2.5) is replaced by the privacy leakage rate constraint $\frac{1}{n} I(X^n \wedge M) \leqslant L + \delta$. Denote the corresponding SK capacity with privacy leakage rate constraint L by $C_{SK}^{PL}(L)$. From $I(X^n \wedge M) \leqslant \log |\mathcal{M}|$ it is clear that a constraint on the rate of the helper message at the same time is a constraint on the privacy leakage rate. So $C_{SK}^{PL}(L) \geqslant C_{SK}(L)$ for all $L \geqslant 0$. In [32, Theorem 3.1] it is shown that $C_{SK}^{PL}(L) = C_{SK}(L)$ for all $L \geqslant 0$.

2.3 Fundamentals, types and typical sequences

In this work we make use of some fundamental results in information theory which can for the most part be found in the corresponding textbooks like [26]. For the convenience of the reader we state some of these results. We also present proofs for some of the results for reasons of completeness.

Lemma 2.2 (Pinsker inequality [26]). *Let $P, Q \in \mathcal{P}(\mathcal{X})$. It holds that*

$$D(P\|Q) \geqslant \tfrac{1}{2\ln 2}\|P - Q\|_1^2.$$

Lemma 2.3 (Continuity of entropy [26]). *Let $P, Q \in \mathcal{P}(\mathcal{X})$ and $\|P - Q\|_1 = \delta \leqslant \frac{1}{2}$. It holds that*

$$|H(P) - H(Q)| \leqslant -\delta \log \tfrac{\delta}{|\mathcal{X}|}.$$

Definition 2.2 ([26]). *Let $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, $n \in \mathbb{N}$. We define*

$$N(a|x^n) = |\{i \in [n] \colon x_i = a\}|$$

and

$$N(a, b|x^n, y^n) = |\{i \in [n] \colon x_i = a \wedge y_i = b\}|$$

where $(a, b) \in \mathcal{X} \times \mathcal{Y}$.

Definition 2.3 (Type and joint type [26]). *The type of a sequence $x^n \in \mathcal{X}^n$ is the empirical probability P_{x^n} where $P_{x^n}(a) = \frac{1}{n}N(a|x^n)$ for all $a \in \mathcal{X}$. We denote the set of all sequences of type P by $\mathcal{T}_P^n$. We denote the set of all types of sequences in $\mathcal{X}^n$ by $\mathcal{P}(n, \mathcal{X})$.*

Correspondingly the joint type of a tuple of sequences $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ is the empirical probability P_{x^n,y^n} where $P_{x^n,y^n}(a, b) = \frac{1}{n}N(a, b|x^n, y^n)$ for all $(a, b) \in \mathcal{X} \times \mathcal{Y}$. We denote the set of all tuples of sequences of joint type P by $\mathcal{T}_P^n$. We denote the set of all joint types of tuples of sequences in $\mathcal{X}^n \times \mathcal{Y}^n$ by $\mathcal{P}(n, \mathcal{X} \times \mathcal{Y})$.

Lemma 2.4 ([26]). *It holds that $|\mathcal{P}(n, \mathcal{X})| \leqslant (n+1)^{|\mathcal{X}|}$ and correspondingly $|\mathcal{P}(n, \mathcal{X} \times \mathcal{Y})| \leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|}$.*

Lemma 2.5 ([4]). *Let $P \in \mathcal{P}(n, \mathcal{X})$. It holds that*

$$\tfrac{1}{(n+1)^{|\mathcal{X}|}} \exp(nH(P)) \leqslant |\mathcal{T}_P^n| \leqslant \exp(nH(P)).$$

Lemma 2.6 ([26]). *Let $P \in \mathcal{P}(n, \mathcal{X})$ and $Q \in \mathcal{P}(\mathcal{X})$. It holds that*

$$Q^{\otimes n}(x^n) = \exp(-n(H(P) + D(P\|Q)))$$

for all $x^n \in \mathcal{T}_P^n$ and

$$\tfrac{1}{(n+1)^{|\mathcal{X}|}} \exp(-nD(P\|Q)) \leqslant Q^{\otimes n}(\mathcal{T}_P^n) \leqslant \exp(-nD(P\|Q)).$$

Definition 2.4 ([26]). *Let $P \in \mathcal{P}(\mathcal{X})$, $n \in \mathbb{N}$ and $\delta > 0$. We define*

$$\mathcal{T}_{P,\delta}^n = \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ |Q(a)-P(a)| \leqslant \delta \forall a \in \mathcal{X} \\ \wedge Q(a) > 0 \Rightarrow P(a) > 0}} \mathcal{T}_Q^n.$$

If $x^n \in \mathcal{T}_{P,\delta}^n$ we say x^n is P-typical with constant δ.

Lemma 2.7 ([45, 50]). *Let $\delta > 0$, $n \in \mathbb{N}$ and $P \in \mathcal{P}(\mathcal{X})$. It holds that*

$$P^{\otimes n}(\mathcal{T}_{P,\delta}^n) \geqslant 1 - (n+1)^{|\mathcal{X}|} \exp(-n \tfrac{1}{2 \ln 2} \delta^2).$$

Proof. Consider

$$\begin{aligned}(\mathcal{T}_{P,\delta}^n)^c &= \{x^n \in \mathcal{X}^n \colon \exists a \in \mathcal{X} \colon |P_{x^n}(a) - P(a)| > \delta\} \\ &\qquad \cup \{x^n \in \mathcal{X}^n \colon \exists a \in \mathcal{X} \colon P_{x^n}(a) > 0 \wedge P(a) = 0\} \\ &\subseteq \{x^n \in \mathcal{X}^n \colon \|P_{x^n} - P\|_1 > \delta\} \cup \{x^n \in \mathcal{X}^n \colon \exists a \in \mathcal{X} \colon P_{x^n}(a) > 0 \wedge P(a) = 0\}.\end{aligned}$$

We define

$$\begin{aligned}\mathcal{A} &= \{x^n \in \mathcal{X}^n \colon \|P_{x^n} - P\|_1 > \delta\} \\ \mathcal{B} &= \{x^n \in \mathcal{X}^n \colon \exists a \in \mathcal{X} \colon P_{x^n}(a) > 0 \wedge P(a) = 0\}.\end{aligned}$$

It holds that

$$P^{\otimes n}(\mathcal{B}) = \sum_{x^n \in \mathcal{B}} \prod_{i \in [n]} P(x_i) = \sum_{x^n \in \mathcal{B}} \prod_{a \in \mathcal{X}} P(a)^{N(a|x^n)} = 0.$$

Moreover we have

$$\mathcal{A} = \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 > \delta}} \mathcal{T}_Q^n.$$

So

$$P^{\otimes n}(\mathcal{A}) = P^{\otimes n}(\bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1>\delta}} \mathcal{T}_Q^n) = \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1>\delta}} P^{\otimes n}(\mathcal{T}_Q^n) \leqslant \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1>\delta}} \exp(-nD(Q\|P))$$

where we use Lemma 2.6 for the last step. With the Pinsker inequality we can upper bound this expression by

$$\begin{aligned}\sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1>\delta}} \exp(-n\tfrac{1}{2\ln 2}\|P-Q\|_1^2) &\leqslant \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1>\delta}} \exp(-n\tfrac{1}{2\ln 2}\delta^2)\\ &\leqslant (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2).\end{aligned}$$

So we have

$$\begin{aligned}P^{\otimes n}(\mathcal{T}_{P,\delta}^n) = 1 - P^{\otimes n}((\mathcal{T}_{P,\delta}^n)^c) &\geqslant 1 - P^{\otimes n}(\mathcal{A}) - P^{\otimes n}(\mathcal{B})\\ &\geqslant 1 - (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2).\end{aligned}$$

■

Lemma 2.8 ([26]). *Let $\delta > 0$ with $\delta < \frac{1}{2|\mathcal{X}|}$ and $P \in \mathcal{P}(\mathcal{X})$. It holds for all $n \in \mathbb{N}$ large enough that*

$$\tfrac{\exp(n(H(P)-(-\delta|\mathcal{X}|\log\delta)))}{(n+1)^{|\mathcal{X}|}} \leqslant |\mathcal{T}_{P,\delta}^n| \leqslant (n+1)^{|\mathcal{X}|}\exp(n(H(P)+(-\delta|\mathcal{X}|\log\delta))).$$

Proof. We have

$$\mathcal{T}_{P,\delta}^n = \bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ |Q(a)-P(a)|\leqslant\delta\forall a\in\mathcal{X}\\ \wedge Q(a)>0\Rightarrow P(a)>0}} \mathcal{T}_Q^n \subseteq \bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1\leqslant\delta|\mathcal{X}|}} \mathcal{T}_Q^n$$

and thus

$$|\mathcal{T}_{P,\delta}^n| \leqslant \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1\leqslant\delta|\mathcal{X}|}} |\mathcal{T}_Q^n| \leqslant \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1\leqslant\delta|\mathcal{X}|}} \exp(nH(Q))$$

where the last step follows from Lemma 2.5. From the continuity of entropy it follows from $\|P-Q\|_1 \leqslant \delta|\mathcal{X}|$ that $H(Q) \leqslant H(P) + (-\delta|\mathcal{X}|\log\delta)$. So we can upper bound the expression above by

$$\sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1\leqslant\delta|\mathcal{X}|}} \exp(n(H(P)+(-\delta|\mathcal{X}|\log\delta))) \leqslant (n+1)^{|\mathcal{X}|}\exp(n(H(P)+(-\delta|\mathcal{X}|\log\delta))).$$

Let $\mathcal{T}^n_{P,\delta} \neq \varnothing$ (for n large enough this follows from Lemma 2.7). So there is a $Q \in \mathcal{P}(n, \mathcal{X})$ such that $\|P - Q\|_1 \leqslant \delta|\mathcal{X}|$ and $\mathcal{T}^n_Q \subseteq \mathcal{T}^n_{P,\delta}$, i.e.,

$$|\mathcal{T}^n_{P,\delta}| \geqslant |\mathcal{T}^n_Q| \geqslant \tfrac{1}{(n+1)^{|\mathcal{X}|}} \exp(nH(Q))$$

where the last step follows from Lemma 2.5. From the continuity of entropy we can lower bound this expression by

$$\tfrac{1}{(n+1)^{|\mathcal{X}|}} \exp(n(H(P) - (-\delta|\mathcal{X}| \log \delta))).$$

■

Remark 2.9 ([26]). *We can write joint types as*

$$P_{x^n,y^n}(x, y) = P_{x^n}(x)V(y|x)$$

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ where $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. $V(y|x)$ is not uniquely determined given $P_{x^n,y^n}(x, y)$ for the $x \in \mathcal{X}$ that do not occur in x^n.

Definition 2.5 (Conditional type and V-shell [26]). *The sequence $y^n \in \mathcal{Y}^n$ has conditional type $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ given $x^n \in \mathcal{X}^n$ if*

$$N(x, y|x^n, y^n) = N(x|x^n)V(y|x) \tag{2.6}$$

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$. For $x^n \in \mathcal{X}^n$ and stochastic matrix $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ we call the set of all sequences $y^n \in \mathcal{Y}^n$ with conditional type V given x^n the V-shell of x^n and denote it by $\mathcal{T}_V(x^n)$ (or $\mathcal{T}^n_V(x^n)$).

Remark 2.10 ([26]). *The conditional type of y^n given x^n is not determined uniquely if there is a $x \in \mathcal{X}$ that does not occur in x^n, but the set $\mathcal{T}_V(x^n)$ that contains y^n is determined uniquely. (This set is the same for all choices of $V(y|x)$ for the $x \in \mathcal{X}$ that do not occur in x^n, because (2.6) is independent of these $V(y|x)$.)*

Lemma 2.11 ([26]). *For $x^n \in \mathcal{X}^n$ and $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\mathcal{T}_V(x^n) \neq \varnothing$ it holds that*

$$(n + 1)^{-|\mathcal{X}||\mathcal{Y}|} \exp(nH(V|P_{x^n})) \leqslant |\mathcal{T}_V(x^n)| \leqslant \exp(nH(V|P_{x^n})).$$

Lemma 2.12 ([26]). *Let $n \in \mathbb{N}$, $x^n \in \mathcal{X}^n$ and $V, W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\mathcal{T}_V(x^n) \neq \varnothing$. It holds that*

$$W^{\otimes n}(y^n|x^n) = \exp(-n(D(V\|W|P_{x^n}) + H(V|P_{x^n})))$$

for $y^n \in \mathcal{T}_V(x^n)$ and

$$\tfrac{1}{(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \exp(-n(D(V\|W|P_{x^n}))) \leqslant W^{\otimes n}(\mathcal{T}_V(x^n)|x^n) \leqslant \exp(-nD(V\|W|P_{x^n})).$$

Definition 2.6 ([26]). *Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, $n \in \mathbb{N}$, $x^n \in \mathcal{X}^n$ and $\delta > 0$. We define*

$$\mathcal{T}_{W,\delta}(x^n) = \bigcup_{\substack{Q \in \mathcal{P}(n, \mathcal{X}\times\mathcal{Y}): \\ \sum_{b\in\mathcal{Y}} Q(a,b) = P_{x^n}(a) \forall a \in \mathcal{X} \\ \wedge |P_{x^n}(a)W(b|a) - Q(a,b)| \leqslant \delta \forall (a,b) \in \mathcal{X}\times\mathcal{Y} \\ \wedge W(b|a)=0 \Rightarrow Q(a,b)=0}} \mathcal{T}_{V(Q)}(x^n),$$

where $V(Q) \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with

$$V(Q)(b|a) = \begin{cases} \frac{Q(a,b)}{\sum_{b\in\mathcal{Y}} Q(a,b)} & \sum_{b\in\mathcal{Y}} Q(a,b) > 0 \\ \frac{1}{|\mathcal{Y}|} & \text{otherwise} \end{cases}.$$

Lemma 2.13 ([45, 50]). *Let $\delta > 0$, $n \in \mathbb{N}$, $x^n \in \mathcal{X}^n$ and $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. It holds that*

$$W^{\otimes n}(\mathcal{T}_{W,\delta}(x^n)|x^n) \geqslant 1 - (n+1)^{|\mathcal{X}||\mathcal{Y}|} \exp(-n\tfrac{1}{2\ln 2}\delta^2).$$

Proof. We show

$$W^{\otimes n}((\mathcal{T}_{W,\delta}(x^n))^c|x^n) \leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|} \exp(-n\tfrac{1}{2\ln 2}\delta^2).$$

We know

$$\begin{aligned}(\mathcal{T}_{W,\delta}(x^n))^c &= \{y^n \in \mathcal{Y}^n \colon \exists (a,b) \in \mathcal{X}\times\mathcal{Y} \colon |P_{x^n,y^n}(a,b) - P_{x^n}(a)W(b|a)| > \delta\} \\ &\quad \cup \{x^n \in \mathcal{X}^n \colon \exists (a,b) \in \mathcal{X}\times\mathcal{Y} \colon P_{x^n,y^n}(a,b) > 0 \wedge W(b|a) = 0\} \\ &\subseteq \{y^n \in \mathcal{Y}^n \colon \sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} |P_{x^n,y^n}(a,b) - P_{x^n}(a)W(b|a)| > \delta\} \\ &\quad \cup \{y^n \in \mathcal{Y}^n \colon \exists (a,b) \in \mathcal{X}\times\mathcal{Y} \colon P_{x^n,y^n}(a,b) > 0 \wedge W(b|a) = 0\}.\end{aligned}$$

We define

$$\begin{aligned}\mathcal{A} &= \{y^n \in \mathcal{Y}^n \colon \sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} |P_{x^n,y^n}(a,b) - P_{x^n}(a)W(b|a)| > \delta\} \\ \mathcal{B} &= \{y^n \in \mathcal{Y}^n \colon \exists (a,b) \in \mathcal{X}\times\mathcal{Y} \colon P_{x^n,y^n}(a,b) > 0 \wedge W(b|a) = 0\}.\end{aligned}$$

It holds that

$$W^{\otimes n}(\mathcal{B}|x^n) = \sum_{y^n\in\mathcal{B}} \prod_{i\in[n]} W(y_i|x_i) = \sum_{y^n\in\mathcal{B}} \prod_{(a,b)\in\mathcal{X}\times\mathcal{Y}} W(b|a)^{N(a,b|x^n,y^n)} = 0.$$

Moreover we have

$$\mathcal{A} = \bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} |P_{x^n}(a)W(b|a)-Q(a,b)|>\delta}} \mathcal{T}_{V(Q)}(x^n)$$

Thus

$$\begin{aligned} W^{\otimes n}(\mathcal{A}|x^n) &= W^{\otimes n}\Big(\bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} |P_{x^n}(a)W(b|a)-Q(a,b)|>\delta}} \mathcal{T}_{V(Q)}(x^n)|x^n\Big)\\ &= \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)|W(b|a)-V(Q)(b|a)|>\delta}} W^{\otimes n}(\mathcal{T}_{V(Q)}(x^n)|x^n)\\ &\leqslant \sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)|W(b|a)-V(Q)(b|a)|>\delta}} \exp(-nD(V(Q)\|W|P_{x^n})) \end{aligned}$$

where we use Lemma 2.12 for the last step. As

$$D(V(Q)\|W|P_{x^n}) = \sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)V(Q)(b|a)\log\tfrac{V(Q)(b|a)P_{x^n}(a)}{W(b|a)P_{x^n}(a)}$$

we can use the Pinsker inequality to upper bound this expression by

$$\begin{aligned} &\sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)|W(b|a)-V(Q)(b|a)|>\delta}} \exp(-n\tfrac{1}{2\ln 2}\sum_{a\in\mathcal{X}} P_{x^n}(a)\|W(\cdot|a)-V(Q)(\cdot|a)\|_1^2)\\ \leqslant &\sum_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}} Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)|W(b|a)-V(Q)(b|a)|>\delta}} \exp(-n\tfrac{1}{2\ln 2}\delta^2) \leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2). \end{aligned}$$

So we have

$$\begin{aligned} W^{\otimes n}(\mathcal{T}_{W,\delta}(x^n)|x^n) &= 1 - W^{\otimes n}((\mathcal{T}_{W,\delta}(x^n))^c|x^n)\\ &\geqslant 1 - W^{\otimes n}(\mathcal{A}|x^n) - W^{\otimes n}(\mathcal{B}|x^n)\\ &\geqslant 1 - (n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2). \end{aligned}$$

■

Lemma 2.14 ([26]). *Let $\delta > 0$ with $\delta < \frac{1}{2|\mathcal{X}||\mathcal{Y}|}$ and $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, $x^n \in \mathcal{X}^n$. It holds*

for all $n \in \mathbb{N}$ *large enough that*

$$(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P_{x^n})-\epsilon)) \leqslant |\mathcal{T}^n_{W,\delta}(x^n)| \leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P_{x^n})+\epsilon)),$$

where $\epsilon = \epsilon(\delta, |\mathcal{X}|, |\mathcal{Y}|) = -\delta|\mathcal{X}||\mathcal{Y}|\log\delta$. *For* $x^n \in \mathcal{T}_{P,\delta}$, $P \in \mathcal{P}(\mathcal{X})$, *it holds that*

$$(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P)-\bar{\epsilon})) \leqslant |\mathcal{T}^n_{W,\delta}(x^n)| \leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P)+\bar{\epsilon})),$$

where $\bar{\epsilon} = \epsilon + \delta|\mathcal{X}|\log|\mathcal{Y}|$.

Proof. We have

$$\mathcal{T}_{W,\delta}(x^n) = \bigcup_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}}Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge|P_{x^n}(a)W(b|a)-Q(a,b)|\leqslant\delta\forall(a,b)\in\mathcal{X}\times\mathcal{Y}\\ \wedge W(b|a)=0\Rightarrow Q(a,b)=0}} \mathcal{T}_{V(Q)}(x^n).$$

Thus it holds that

$$\begin{aligned}|\mathcal{T}_{W,\delta}(x^n)| &\leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|} \max_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}}Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge|P_{x^n}(a)W(b|a)-Q(a,b)|\leqslant\delta\forall(a,b)\in\mathcal{X}\times\mathcal{Y}\\ \wedge W(b|a)=0\Rightarrow Q(a,b)=0}} |\mathcal{T}_{V(Q)}(x^n)|\\ &\leqslant (n+1)^{|\mathcal{X}||\mathcal{Y}|} \max_{\substack{Q\in\mathcal{P}(n,\mathcal{X}\times\mathcal{Y}):\\ \sum_{b\in\mathcal{Y}}Q(a,b)=P_{x^n}(a)\forall a\in\mathcal{X}\\ \wedge|P_{x^n}(a)W(b|a)-Q(a,b)|\leqslant\delta\forall(a,b)\in\mathcal{X}\times\mathcal{Y}\\ \wedge W(b|a)=0\Rightarrow Q(a,b)=0}} \exp(nH(V(Q)|P_{x^n})).\end{aligned}$$

It holds that

$$H(V(Q)|P_{x^n}) = -\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} P_{x^n}(a)V(Q)(b|a)\log(P_{x^n}(a)V(Q)(b|a)) - H(P_{x^n})$$

and form the continuity of entropy it follows from

$$\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} |P_{x^n}(a)V(Q)(b|a) - P_{x^n}W(b|a)| \leqslant \delta|\mathcal{X}||\mathcal{Y}|$$

that

$$H(V(Q)|P_{x^n}) \leqslant H(W|P_{x^n}) + (-\delta|\mathcal{X}||\mathcal{Y}|\log\delta), \tag{2.7}$$

so we can upper bound $|\mathcal{T}_{W,\delta}(x^n)|$ by

$$(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P_{x^n}) + (-\delta|\mathcal{X}||\mathcal{Y}|\log\delta))).$$

Moreover, we have for n large enough that $\mathcal{T}_{W,\delta}(x^n) \neq \varnothing$ and thus for a $V(Q) \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$

(with corresponding Q)

$$\begin{aligned}|\mathcal{T}_{W,\delta}(x^n)| &\geqslant |\mathcal{T}_{V(Q)}(x^n)| \geqslant (n+1)^{-|\mathcal{X}||\mathcal{Y}|}\exp(nH(V(Q)|P_{x^n})) \\ &\geqslant (n+1)^{-|\mathcal{X}||\mathcal{Y}|}\exp(n(H(W|P_{x^n}) - (-\delta|\mathcal{X}||\mathcal{Y}|\log\delta))),\end{aligned}$$

where the last step follows from the continuity of entropy. For the case $x^n \in \mathcal{T}^n_{P,\delta}$ the result follows from

$$\begin{aligned}|H(W|P_{x^n}) - H(W|P)| &= |\sum_{a\in\mathcal{X}} H(W(\cdot|a))(P_{x^n}(a) - P(a))| \\ &\leqslant \sum_{a\in\mathcal{X}} H(W(\cdot|a))|P_{x^n}(a) - P(a)| \\ &\leqslant \log|\mathcal{Y}| \sum_{a\in\mathcal{X}} |P_{x^n}(a) - P(a)| \leqslant \delta|\mathcal{X}|\log|\mathcal{Y}|.\end{aligned}$$

■

Lemma 2.15 ([26]). *Consider $\delta_1, \delta_2 > 0$, $n \in \mathbb{N}$, $P \in \mathcal{P}(\mathcal{X})$ and $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. Let $x^n \in \mathcal{T}^n_{P,\delta_1}$ and $y^n \in \mathcal{T}_{W,\delta_2}(x^n)$. It holds that $(x^n, y^n) \in \mathcal{T}^n_{Q,\delta_1+\delta_2}$ with $Q \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, $Q(x,y) = P(x)W(y|x)$ for all $(x,y) \in \mathcal{X}\times\mathcal{Y}$ and $y^n \in \mathcal{T}_{PW,(\delta_1+\delta_2)|\mathcal{X}|}$ with $PW \in \mathcal{P}(\mathcal{Y})$, $PW(y) = \sum_{x\in\mathcal{X}} P(x)W(y|x)$ for all $y \in \mathcal{Y}$.*

Lemma 2.16. *Let $n \in \mathbb{N}$, $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$,$P \in \mathcal{P}(\mathcal{X})$ and $\delta_1, \delta_2 > 0$. Let $x^n \in \mathcal{T}^n_{P,\delta_1}$ and $y^n \in \mathcal{T}^n_{W,\delta_2}(x^n)$. It holds that $PW^{\otimes n}(y^n) \leqslant \exp(-n(H(PW) - \theta\log\frac{|\mathcal{X}|}{\theta}))$ where $\theta = (\delta_1+\delta_2)|\mathcal{X}||\mathcal{Y}|$.*

Proof. With Lemma 2.15, $x^n \in \mathcal{T}^n_{P,\delta_1}$ and $y^n \in \mathcal{T}^n_{W,\delta_2}(x^n)$ we have $y^n \in \mathcal{T}^n_{PW,(\delta_1+\delta_2)|\mathcal{X}|}$. Thus

$$\|P_{y^n} - PW\|_1 \leqslant (\delta_1+\delta_2)|\mathcal{X}||\mathcal{Y}|. \tag{2.8}$$

It holds that

$$PW^{\otimes n}(y^n) = \exp(-n(D(P_{y^n}\|PW) + H(P_{y^n}))) \leqslant \exp(-nH(P_{y^n})).$$

With (2.8) and Lemma 2.3 it holds that

$$H(P_{y^n}) \geqslant H(PW) - \theta\log\tfrac{|\mathcal{Y}|}{\theta}.$$

■

Lemma 2.17. *Let $n \in \mathbb{N}$, $\delta > 0$, $0 < \eta < \frac{1}{2\ln 2}\delta^2$ and $P \in \mathcal{P}(\mathcal{X})$. Let $\mathcal{A} \subseteq \mathcal{X}^n$ such that $P^{\otimes n}(\mathcal{A}) \geqslant \exp(-n\eta)$. It holds for all n large enough that*

$$\tfrac{1}{n}\log|\mathcal{A}| \geqslant H(P) - \delta|\mathcal{X}|\log\delta - \eta - \tfrac{1}{n} - \tfrac{|\mathcal{X}|}{n}\log(n+1).$$

Proof. We have with Lemma 2.7

$$\begin{aligned} P^{\otimes n}(\mathcal{A} \cap \mathcal{T}^n_{P,\delta}) &\geqslant P^{\otimes n}(\mathcal{A}) + P^{\otimes n}(\mathcal{T}^n_{P,\delta}) - 1 \\ &\geqslant \exp(-n\eta) - (n+1)^{|\mathcal{X}|} \exp(-n\tfrac{1}{2\ln 2}\delta^2) \geqslant \exp(-n\eta)/2 \end{aligned}$$

for n large enough. It holds that

$$\mathcal{A} \cap \mathcal{T}^n_{P,\delta} = \mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ |Q(a)-P(a)| \leqslant \delta \forall a \in \mathcal{X} \\ \wedge\, Q(a)>0 \Rightarrow P(a)>0}} \mathcal{T}^n_Q \subseteq \mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \mathcal{T}^n_Q$$

Thus

$$\begin{aligned} \exp(-n\eta)/2 \leqslant P^{\otimes n}(\mathcal{A} \cap \mathcal{T}^n_{P,\delta}) &\leqslant P^{\otimes n}(\mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \mathcal{T}^n_Q) \\ &= \sum_{x^n \in \mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \mathcal{T}^n_Q} P^{\otimes n}(x^n). \end{aligned}$$

For all $x^n \in \mathcal{T}^n_Q$ we know that $P^{\otimes n}(x^n)$ is constant, so we have for

$$x^n \in \mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \mathcal{T}^n_Q$$

that

$$P^{\otimes n}(x^n) \leqslant \max_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \tfrac{1}{|\mathcal{T}^n_Q|}.$$

With Lemma 2.3 and Lemma 2.5 it follows for $x^n \in \mathcal{A} \cap \bigcup_{\substack{Q \in \mathcal{P}(n,\mathcal{X}):\\ \|P-Q\|_1 \leqslant \delta |\mathcal{X}|}} \mathcal{T}^n_Q$ that

$$P^{\otimes n}(x^n) \leqslant (n+1)^{|\mathcal{X}|} \exp(-n(H(P) - \delta |\mathcal{X}| \log \delta)).$$

Thus we have

$$\exp(-n\eta)/2 \leqslant |\mathcal{A}|(n+1)^{|\mathcal{X}|} \exp(-n(H(P) - \delta |\mathcal{X}| \log \delta))$$

and consequently

$$\tfrac{1}{n} \log |\mathcal{A}| \geqslant H(P) - \delta |\mathcal{X}| \log \delta - \eta - \tfrac{1}{n} - \tfrac{|\mathcal{X}|}{n} \log(n+1).$$

■

Theorem 2.18 (Fano's inequality [26]). *For RVs X and Y on the alphabet $\mathcal{X}$ it*

holds that

$$H(X|Y) \leqslant Pr(X \neq Y) \log(|\mathcal{X}| - 1) + h(Pr(X \neq Y)).$$

Theorem 2.19. *Let A,B,C and D be jointly distributed RVs. It holds that*

$$A - B - C \Leftrightarrow C - B - A \tag{2.9}$$
$$AB - C - D \Rightarrow B - C - D \tag{2.10}$$
$$AB - C - D \Rightarrow A - BC - D \tag{2.11}$$
$$P_{ABC}(a,b,c) = P_{AB}(a,b)P_C(c) \quad \forall (a,b,c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$$
$$\wedge\ A - BC - D \Rightarrow A - B - CD. \tag{2.12}$$

Proof. We give a proof for each of the statements.

- We have

$$\begin{aligned} P_{ABC}(a,b,c) &\overset{a)}{=} P_{A|B}(a|b)P_{BC}(b,c) \\ &= P_{A|B}(a|b)P_{C|B}(c|b)P_B(b) = P_{AB}(a,b)P_{C|B}(c|b) \end{aligned}$$

  for all $(a,b,c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$. Here $a)$ follows from $A - B - C$. So we see that (2.9) is true.

- We have $P_{ABCD}(a,b,c,d) = P_{AB|C}(a,b|c)P_{CD}(c,d)$ for all $(a,b,c,d) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} \times \mathcal{D}$ from $AB - C - D$. Summing both sides over all $b \in \mathcal{B}$ we get (2.10).

- We have

$$\begin{aligned} P_{ABCD}(a,b,c,d) &\overset{a)}{=} P_{AB|C}(a,b|c)P_{CD}(c,d) \\ &= P_{B|C}(b,c)P_{A|BC}(a|b,c)P_{CD}(c,d) \\ &\overset{b)}{=} P_{A|BC}(a|b,c)P_{B|CD}(b|c,d)P_{CD}(c,d) \\ &= P_{A|BC}(a|b,c)P_{BCD}(b,c,d) \end{aligned}$$

  for all $(a,b,c,d) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} \times \mathcal{D}$, where $a)$ follows from $AB - C - D$ and $b)$ from (2.10). This means (2.11) is true.

- We have

$$\begin{aligned} P_{ABCD}(a,b,c,d) &\overset{a)}{=} P_{A|BC}(a|b,c)P_{BCD}(b,c,d) \\ &= P_{A|BC}(a|b,c)P_{D|BC}(d|b,c)P_{BC}(b,c) \\ &\overset{b)}{=} P_{AB}(a,b)P_C(c)P_{D|BC}(d|b,c) \\ &= P_{A|B}(a|b)P_B(b)P_C(c)P_{D|BC}(d|b,c) \\ &\overset{c)}{=} P_{A|B}(a|b)P_{BC}(b,c)P_{D|BC}(d|b,c) \\ &= P_{A|B}(a|b)P_{BCD}(b,c,d) \end{aligned}$$

Figure 2.2: Message transmission over point-to-point channel.

for all $(a, b, c, d) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} \times \mathcal{D}$, where a) follows from $A - BC - D$ and b) and c) follow as C is independent of AB. So we have (2.12).

■

2.4 Channel coding

A discussion on the noisy channel coding problem for the discrete memoryless channel (DMC) can be found in the standard textbooks on information theory, e.g. [26]. In Figure 2.2 we see a block diagram of the setting. Here a message from a set $\mathcal{M}$ should be transmitted over a channel where we assume this channel is the DMC $W^{\otimes n}$ with $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. For this purpose we use an encoder $f\colon \mathcal{M} \to \mathcal{X}^n$ to map the message to a codeword that serves as the input of the DMC. After transmission we use a decoder $g\colon \mathcal{Y}^n \to \mathcal{M}$ to reconstruct the message. We call (f, g) a channel code.

Consequently, for this scenario of message transmission the probability that message $m \in \mathcal{M}$ is reconstructed correctly is $W^{\otimes n}(g^{-1}(m)|f(m))$. The set of possible messages $\mathcal{M}$ and the probability to correctly reconstruct the message should be as large as possible. This suggests the following definition.

Definition 2.7. *We call $R \geqslant 0$ an* achievable rate *if for all $\delta > 0$ there is an $N \in \mathbb{N}$ and a $c > 0$ such that for all $n > N$ there is a channel code (f, g) with*

$$\min_{m \in \mathcal{M}} W^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc)$$
$$\tfrac{1}{n} \log |\mathcal{M}| \geqslant R - \delta.$$

We call the supremum of all achievable rates the channel capacity $C(W)$.

According to this definition the error probability decays exponentially with the block length n for n large enough. The error probability that we consider is the maximum probability of error. We can prove the following achievability result.

Theorem 2.20. *It holds that $C(W) \geqslant \max_{P \in \mathcal{P}(\mathcal{X})} I(P, W)$.*

This result is well known and one can find various proofs in the literature. Nevertheless we present a proof below. After presenting this proof we add an additional requirement to the achievability requirements in Definition 2.7. Then we can use the same proof technique to prove a corresponding achievability result. The following proof is based on the proof of [26, Lemma 6.3].

Proof. Let $\delta_1, \delta_2, c > 0$ small enough and $P \in \mathcal{P}(\mathcal{X})$. We construct the code for all n large enough using an iterative procedure. (Assume w.l.o.g. that $\mathcal{M} = [k]$, $k \in \mathbb{N}$.) In the first step choose $f(1) \in \mathcal{T}^n_{P,\delta_1}$ and $g^{-1}(1) \subset \mathcal{T}^n_{W,\delta_2}(f(1))$ such that

$$W^{\otimes n}(g^{-1}(1)|f(1)) \geqslant 1 - \exp(-nc)$$

holds true. We know from Lemma 2.13 that this is possible with $0 < c < \frac{1}{2\ln 2}\delta_2^2$ for n large enough. We choose $c = \delta_2^2/2$ and n large enough. In the m-th step choose $f(m) \in \mathcal{T}^n_{P,\delta_1} \backslash f([m-1])$ and $g^{-1}(m) \subset \mathcal{T}^n_{W,\delta_2}(f(m)) \backslash \bigcup_{\bar{m}\in[m-1]} g^{-1}(\bar{m})$ such that

$$W^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc)$$

holds true. After the k-th step we can not find an additional code word with an appropriate decoding set. (As the sets that we choose the code words and the decoding sets from are finite, the procedure will terminate.) For the remaining $y^n \in \mathcal{Y}^n \backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)$ we choose for $g(y^n)$ an arbitrary $m \in \mathcal{M}$. Assume the procedure terminates because we can not find an additional decoding set. Then for all $x^n \in \mathcal{T}^n_{P,\delta_1} \backslash f(\mathcal{M})$ it holds that

$$W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n) \backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) < 1 - \exp(-nc) \tag{2.13}$$

as otherwise the procedure would not have terminated yet. For $f(m)$, $m \in \mathcal{M}$, it holds that

$$\begin{aligned} W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(f(m)) \backslash \bigcup_{\bar{m}\in\mathcal{M}} g^{-1}(\bar{m})|f(m)) &\leqslant W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(f(m)) \backslash g^{-1}(m)|f(m)) \\ &\leqslant W^{\otimes n}((g^{-1}(m))^c|f(m)) \leqslant \exp(-nc), \end{aligned}$$

so (2.13) holds true for all $x^n \in \mathcal{T}^n_{P,\delta_1}$ for n large enough. For the left hand side of (2.13) we can write

$$W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n) \cap (\bigcup_{m\in\mathcal{M}} g^{-1}(m))^c|x^n)$$

which equals

$$\begin{aligned} &W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n)|x^n) + 1 - W^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) \\ &\qquad\qquad - W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n) \cup (\bigcup_{m\in\mathcal{M}} g^{-1}(m))^c|x^n) \\ \geqslant &W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n)|x^n) - W^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n). \end{aligned}$$

With Lemma 2.13 we get

$$\begin{aligned} W^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) &\geqslant 1-(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta_2^2) \\ &\quad - W^{\otimes n}(\mathcal{T}^n_{W,\delta_2}(x^n)\cap(\bigcup_{m\in\mathcal{M}} g^{-1}(m))^c|x^n) \\ &\geqslant \exp(-n\delta_2^2/2)-(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta_2^2)\geqslant \exp(-n\delta_2^2), \end{aligned}$$

where for the second to last inequality we use (2.13). The last step holds for all n large enough. Furthermore with Lemma 2.7 it holds that

$$\begin{aligned} PW^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)) &= \sum_{y^n\in\bigcup_{m\in\mathcal{M}} g^{-1}(m)}\prod_{i=1}^n\sum_{x\in\mathcal{X}} P(x)W(y_i|x) \\ &\overset{a)}{=} \sum_{x^n\in\mathcal{X}^n} P^{\otimes n}(x^n)W^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) \\ &\geqslant \sum_{x^n\in\mathcal{T}^n_{P,\delta_1}} P^{\otimes n}(x^n)W^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) \qquad (2.14) \\ &\geqslant (1-(n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta_1^2))\exp(-n\delta_2^2). \qquad (2.15) \end{aligned}$$

Here we can prove $a)$ for all $n\in\mathbb{N}$ by induction. Now consider

$$\begin{aligned} PW^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)) &= \sum_{y^n\in\bigcup_{m\in\mathcal{M}} g^{-1}(m)} PW^{\otimes n}(y^n) \\ &= \sum_{y^n\in\bigcup_{m\in\mathcal{M}}(g^{-1}(m)\cap\mathcal{T}^n_{W,\delta_2}(f(m)))} PW^{\otimes n}(y^n) \\ &\leqslant \sum_{y^n\in\bigcup_{m\in\mathcal{M}}(g^{-1}(m)\cap\mathcal{T}^n_{W,\delta_2}(f(m)))} \exp(-n(H(PW)-\theta\log\tfrac{|\mathcal{X}|}{\theta})) \\ &= \sum_{y^n\in\bigcup_{m\in\mathcal{M}} g^{-1}(m)} \exp(-n(H(PW)-\theta\log\tfrac{|\mathcal{X}|}{\theta})) \\ &= |\bigcup_{m\in\mathcal{M}} g^{-1}(m)|\exp(-n(H(PW)-\theta\log\tfrac{|\mathcal{X}|}{\theta})) \end{aligned}$$

where we use Lemma 2.16 for the third step and define θ accordingly. Note that here we also use that $f(m)\in\mathcal{T}^n_{P,\delta_1}$ for all $m\in\mathcal{M}$. So we get

$$|\bigcup_{m\in\mathcal{M}} g^{-1}(m)|\geqslant(1-(n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta_1^2))\exp(-n\delta_2^2)\exp(n(H(PW)-\theta\log\tfrac{|\mathcal{X}|}{\theta})).$$

With Lemma 2.14 it holds that

$$\begin{aligned}|\bigcup_{m\in\mathcal{M}} g^{-1}(m)| &\leqslant |\bigcup_{m\in\mathcal{M}} \mathcal{T}^n_{W,\delta_2}(f_n(m))| \leqslant \sum_{m\in\mathcal{M}} |\mathcal{T}^n_{W,\delta_2}(f_n(m))| \\ &\leqslant |\mathcal{M}| \exp(n(H(W|P) + |\mathcal{X}||\mathcal{Y}|\delta_2 \log(1/\delta_2) + \delta_1|\mathcal{X}|\log|\mathcal{Y}|))(n+1)^{|\mathcal{X}||\mathcal{Y}|}.\end{aligned}$$

Thus overall we obtain

$$\begin{aligned}|\mathcal{M}| \geqslant &\frac{1-(n+1)^{|\mathcal{X}|}\exp(-n\frac{1}{2\ln 2}\delta_1^2)}{(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \\ &\cdot \exp(n(I(P,W) - \delta_2^2 - \theta \log\tfrac{|\mathcal{X}|}{\theta} - |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) - \delta_1|\mathcal{X}|\log|\mathcal{Y}|)).\end{aligned}$$

If the procedure terminates because we can not choose an additional code word from the set of possible code words we have with Lemma 2.8

$$|\mathcal{M}| \geqslant \tfrac{1}{(n+1)^{|\mathcal{X}|}} \exp(n(H(P) - \epsilon))$$

for $\epsilon > 0$ and n large enough.

■

As mentioned above we want to add a requirement to the achievability requirements in Definition 2.7. We want to consider channel codes such that the code words are elements of a set $\mathcal{A}$ with a certain property (which guarantees that $\mathcal{A}$ is large enough).

Definition 2.8. *Let $P \in \mathcal{P}(\mathcal{X})$. We call $R \geqslant 0$ an* achievable rate given P *if for all $\delta > 0$ there is an $N \in \mathbb{N}$, a $c > 0$ and $\eta > 0$ such that for all $n > N$, given $\mathcal{A} \subset \mathcal{X}^n$ with $P^{\otimes n}(\mathcal{A}) > \exp(-n\eta)$, there is a channel code (f, g) with*

$$\begin{aligned}&\min_{m\in\mathcal{M}} W^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc) \\ &\tfrac{1}{n}\log|\mathcal{M}| \geqslant R - \delta\end{aligned}$$

and $f(\mathcal{M}) \subset \mathcal{A}$.

We prove the following theorem (which is very similar to [26, Theorem 6.10]).

Theorem 2.21. *Let $P \in \mathcal{P}(\mathcal{X})$. The rate $I(P,W)$ is achievable given P.*

Proof. To prove this result we change the iterative procedure for the code construction such that in the m-th step $f(m)$ is not chosen from $\mathcal{T}^n_{P,\delta_1}\backslash f([m-1])$ anymore but from $(\mathcal{A} \cap \mathcal{T}^n_{P,\delta_1})\backslash f([m-1])$. At first we consider the case where the procedure terminates because we can not find an appropriate decoding set. So after the procedure terminates we have (2.13) for all $x^n \in \mathcal{A} \cap \mathcal{T}^n_{P,\delta_1}$ for all n large enough. Moreover with Lemma 2.7 we have

$$P^{\otimes n}(\mathcal{A} \cap \mathcal{T}^n_{P,\delta_1}) \geqslant 1 - (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta_1^2) + \exp(-n\eta) - 1 \geqslant \exp(-n\eta)/2$$

for all n large enough. In (2.14), instead of summing over $\mathcal{T}^n_{P,\delta_1}$ we take the sum over $\mathcal{A} \cap \mathcal{T}^n_{P,\delta_1}$ and get instead of (2.15) that

$$PW^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)) \geqslant \exp(-n\eta)\exp(-n\delta_2^2)/2$$

and thus overall

$$|\mathcal{M}| \geqslant \frac{1/2}{(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \cdot \exp(n(I(P;W) - \delta_2^2 - \eta - \theta\log\tfrac{|\mathcal{X}|}{\theta} - |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) - \delta_1|\mathcal{X}|\log|\mathcal{Y}|)).$$

Lemma 2.17 implies that if the procedure terminates because we can not choose a code word anymore we have

$$|\mathcal{M}| \geqslant \exp(n(H(P) - \epsilon))$$

for $\epsilon > 0$ and all n large enough if we choose η small enough.

■

Note that the encoders constructed in the proofs above are injective.

2.5 Compound channels

The compound channel is introduced in [17]. It is used to incorporate channel uncertainty in the model for message transmission over a point-to-point channel. The compound channel is also discussed for example in [26].

In the block diagram depicted in Figure 2.2 the channel is now assumed to not be known perfectly. A message from a set $\mathcal{M}$ should be transmitted over the channel which is one of the DMCs of the set $\{W_s^{\otimes n}\}_{s\in\mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$. Again an encoder $f\colon \mathcal{M} \to \mathcal{X}^n$ and a decoder $g\colon \mathcal{Y}^n \to \mathcal{M}$ are used to map the message on a codeword and to reconstruct the message from the channel output respectively. We call (f, g) a compound channel code.

A compound channel code should allow for reliable reconstruction of the message sent for all possible DMCs i.e. the compound channel codes should be robust against channel uncertainty. This suggests the following definition.

Definition 2.9. *We call $R \geqslant 0$ an* achievable rate *if for all $\delta > 0$ there is an $N \in \mathbb{N}$ and a $c > 0$ such that for all $n > N$ there is a compound channel (f, g) code with*

$$\inf_{s\in\mathcal{S}} \min_{m\in\mathcal{M}} W_s^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc)$$
$$\tfrac{1}{n}\log|\mathcal{M}| \geqslant R - \delta.$$

We call the supremum of all achievable rates the compond channel capacity $C(\{W_s\}_{s\in\mathcal{S}})$.

So the error probability decays exponentially with the block length n for n large enough for all DMCs in the compound set and again we consider the maximum probability of error.

We now assume that $|\mathcal{S}| < \infty$. We can prove the following achievability result.

Theorem 2.22. *It holds that* $C(\{W_s\}_{s\in\mathcal{S}}) \geqslant \max_{P\in\mathcal{P}(\mathcal{X})} \min_{s\in\mathcal{S}} I(P, W_s)$.

This result is well known, see for example [26, Corollary 10.10]. We prove a result that implies Theorem 2.22. Similarly to the channel coding problem we add the requirement that the code words of the compound channel codes are elements of a set $\mathcal{A}$ with a certain property. (For the following definition we do not assume $|\mathcal{S}| < \infty$.)

Definition 2.10. *Let $P \in \mathcal{P}(\mathcal{X})$. We call $R \geqslant 0$ an* achievable rate given P *if for all $\delta > 0$ there is an $N \in \mathbb{N}$, a $c > 0$ and $\eta > 0$ such that for all $n > N$, given $\mathcal{A} \subset \mathcal{X}^n$ with $P^{\otimes n}(\mathcal{A}) > \exp(-n\eta)$, there is a compound channel code (f, g) with*

$$\begin{aligned} &\inf_{s\in\mathcal{S}} \min_{m\in\mathcal{M}} W^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc) \\ &\tfrac{1}{n}\log|\mathcal{M}| \geqslant R - \delta \end{aligned}$$

and $f(\mathcal{M}) \subset \mathcal{A}$.

We prove the following theorem.

Theorem 2.23. *Let $P \in \mathcal{P}(\mathcal{X})$. The rate $\min_{s\in\mathcal{S}} I(P, W_s)$ is achievable given P.*

The proof again is based on the proof of [26, Lemma 6.3].

Proof. Let $\delta_1, \delta_2, c > 0$ small enough and $P \in \mathcal{P}(\mathcal{X})$. We construct the code for all n large enough using an iterative procedure. (We assume w.l.o.g. that $\mathcal{M} = [k]$, $k \in \mathbb{N}$.)

In the first step choose $f(1) \in \mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}$ and $g^{-1}(1) \subset \bigcup_{s\in\mathcal{S}} \mathcal{T}^n_{W_s,\delta_2}(f(1))$ such that for all $s \in \mathcal{S}$

$$W_s^{\otimes n}(g^{-1}(1)|f(1)) \geqslant 1 - \exp(-nc)$$

holds true. We know from Lemma 2.13 that this is possible with $0 < c < \frac{1}{2\ln 2}\delta_2^2$ for n large enough. We choose $c = \delta_2^2/2$ and n large enough. In the m-th step choose $f(m) \in (\mathcal{T}^n_{P,\delta_1} \cap \mathcal{A})\backslash f([m-1])$ and $g^{-1}(m) \subset \bigcup_{s\in\mathcal{S}} \mathcal{T}^n_{W_s,\delta_2}(f(m))\backslash \bigcup_{\bar{m}\in[m-1]} g^{-1}(\bar{m})$ such that for all $s \in \mathcal{S}$

$$W_s^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc)$$

holds true. After the k-th step we can not choose an additional code word with appropriate decoding set. (As the set the code words and decoding sets are chosen form are finite the procedure terminates.) For the remaining $y^n \in \mathcal{Y}^n\backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)$ we choose for $g(y^n)$ an arbitrary $m \in \mathcal{M}$. Assume the procedure terminates because we can not

find an additional appropriate decoding set. Then for all $x^n \in (\mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}) \backslash f(\mathcal{M})$ there is an $s \in \mathcal{S}$ such that

$$W_s^{\otimes n}(\bigcup_{\bar{s}\in\mathcal{S}} \mathcal{T}^n_{W_{\bar{s}},\delta_2}(x^n) \backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) < 1 - \exp(-nc) \tag{2.16}$$

as otherwise the procedure would not have terminated yet. For $f(m)$, $m \in \mathcal{M}$, we have for all $s \in \mathcal{S}$

$$\begin{aligned} W_s^{\otimes n}(\bigcup_{\bar{s}\in\mathcal{S}} \mathcal{T}^n_{W_{\bar{s}},\delta_2}(f(m)) \backslash \bigcup_{\bar{m}\in\mathcal{M}} g^{-1}(\bar{m})|f(m)) &\leqslant W_s^{\otimes n}(\bigcup_{\bar{s}\in\mathcal{S}} \mathcal{T}^n_{W_{\bar{s}},\delta_2}(f(m)) \backslash g^{-1}(m)|f(m)) \\ &\leqslant W_s^{\otimes n}((g^{-1}(m))^c|f(m)) \leqslant \exp(-nc), \end{aligned}$$

so (2.16) holds true for all $x^n \in \mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}$ for all n large enough for at least one $s \in \mathcal{S}$. Moreover with Lemma 2.7 it holds that

$$P^{\otimes n}(\mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}) \geqslant P^{\otimes n}(\mathcal{A}) + P^{\otimes n}(\mathcal{T}^n_{P,\delta_1}) - 1 \geqslant \exp(-n\eta)/2$$

for all n large enough. (Similarly to the proof without channel uncertainty.) Now consider for all $s \in \mathcal{S}$ the set

$$\mathcal{A}_{W_s} := \{x^n \in \mathcal{T}^n_{P,\delta_1} \cap \mathcal{A} \colon W_s^{\otimes n}(\bigcup_{\bar{s}\in\mathcal{S}} \mathcal{T}^n_{W_{\bar{s}},\delta_2}(x^n) \backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) < 1 - \exp(-nc)\}.$$

It is clear that $\bigcup_{s\in\mathcal{S}} \mathcal{A}_{W_s} = \mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}$ as for all $x^n \in \mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}$ there is at least one $s \in \mathcal{S}$ such that (2.16) holds true. Thus we have

$$\exp(-n\eta)/2 \leqslant P^{\otimes n}(\mathcal{T}^n_{P,\delta_1} \cap \mathcal{A}) = P^{\otimes n}(\bigcup_{s\in\mathcal{S}} \mathcal{A}_{W_s}) \leqslant \sum_{s\in\mathcal{S}} P^{\otimes n}(\mathcal{A}_{W_s}) \leqslant |\mathcal{S}| \max_{s\in\mathcal{S}} P^{\otimes n}(\mathcal{A}_{W_s}).$$

So there is an $\tilde{s} \in \mathcal{S}$ such that for all $x^n \in \mathcal{A}_{W_{\tilde{s}}}$ it holds that

$$W_{\tilde{s}}^{\otimes n}(\bigcup_{s\in\mathcal{S}} \mathcal{T}^n_{W_s,\delta_2}(x^n) \backslash \bigcup_{m\in\mathcal{M}} g^{-1}(m)|x^n) < 1 - \exp(-nc) \tag{2.17}$$

and

$$P^{\otimes n}(\mathcal{A}_{W_{\tilde{s}}}) \geqslant \exp(-n\eta)/(2|\mathcal{S}|). \tag{2.18}$$

Moreover for the left hand side of (2.17) we have

$$\begin{aligned}
&W_{\tilde{s}}^{\otimes n}(\bigcup_{s\in\mathcal{S}}\mathcal{T}^n_{W_s,\delta_2}(x^n)\cap(\bigcup_{m\in\mathcal{M}}g^{-1}(m))^c|x^n)\\
=&W_{\tilde{s}}^{\otimes n}(\bigcup_{s\in\mathcal{S}}\mathcal{T}^n_{W_s,\delta_2}(x^n)|x^n)+1-W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)|x^n)\\
&\qquad\qquad-W_{\tilde{s}}^{\otimes n}(\bigcup_{s\in\mathcal{S}}\mathcal{T}^n_{W_s,\delta_2}(x^n)\cup(\bigcup_{m\in\mathcal{M}}g^{-1}(m))^c|x^n)\\
\geqslant&W_{\tilde{s}}^{\otimes n}(\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(x^n)|x^n)-W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)|x^n).
\end{aligned}$$

With Lemma 2.13 we get

$$\begin{aligned}
W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)|x^n)\geqslant&1-(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta_2^2)\\
&\qquad-W_{\tilde{s}}^{\otimes n}(\bigcup_{s\in\mathcal{S}}\mathcal{T}^n_{W_s,\delta_2}(x^n)\cap(\bigcup_{m\in\mathcal{M}}g^{-1}(m))^c|x^n)\\
\geqslant&\exp(-n\delta_2^2/2)-(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta_2^2),
\end{aligned}$$

where for the last inequality we use (2.17). So we have

$$\begin{aligned}
&W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|x^n)\\
&\geqslant W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)|x^n)+W_{\tilde{s}}^{\otimes n}(\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|x^n)-1\\
&\geqslant\exp(-n\delta_2^2/2)-2(n+1)^{|\mathcal{X}||\mathcal{Y}|}\exp(-n\tfrac{1}{2\ln 2}\delta_2^2)\geqslant\exp(-n\delta_2^2)
\end{aligned}$$

where for the second to last inequality we use Lemma 2.13. The last step holds true for all n large enough. Moreover, with (2.18) it holds that

$$\begin{aligned}
&PW_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n))\\
&=\sum_{y^n\in\bigcup_{m\in\mathcal{M}}g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)}\prod_{i=1}^n\sum_{x\in\mathcal{X}}P(x)W_{\tilde{s}}(y_i|x)\\
&=\sum_{x^n\in\mathcal{X}^n}P^{\otimes n}(x^n)W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|x^n)\\
&\geqslant\sum_{x^n\in\mathcal{A}_{W_{\tilde{s}}}}P^{\otimes n}(x^n)W_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}}g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|x^n)\\
&\geqslant\exp(-n\eta)/(2|\mathcal{S}|)\exp(-n\delta_2^2).
\end{aligned}$$

Now consider

$$\begin{aligned}
&PW_{\tilde{s}}^{\otimes n}(\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n))\\
&=\sum_{y^n\in\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)} PW_{\tilde{s}}^{\otimes n}(y^n)\\
&\leqslant\sum_{y^n\in\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)} \exp(-n(H(PW_{\tilde{s}})-\theta\log\tfrac{|\mathcal{X}|}{\theta}))\\
&=|\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|\exp(-n(H(PW_{\tilde{s}})-\theta\log\tfrac{|\mathcal{X}|}{\theta}))
\end{aligned}$$

where we use Lemma 2.16 for the third step and define θ correspondingly. So we get

$$\begin{aligned}
&|\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|\\
&\qquad\geqslant\exp(-n\eta)/(2|\mathcal{S}|)\exp(-n\delta_2^2)\exp(n(H(PW_{\tilde{s}})-\theta\log\tfrac{|\mathcal{X}|}{\theta})).
\end{aligned}$$

Furthermore we have

$$\begin{aligned}
|\bigcup_{m\in\mathcal{M}} g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)| &= |\bigcup_{m\in\mathcal{M}}(g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n))|\\
&\leqslant\sum_{m\in\mathcal{M}}|g^{-1}(m)\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|\\
&\leqslant\sum_{m\in\mathcal{M}}|\bigcup_{s\in\mathcal{S}}\mathcal{T}^n_{W_s,\delta_2}(f(m))\cap\bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)|.
\end{aligned}$$

We define for all $m\in\mathcal{M}$

$$\mathcal{S}^*_m=\{s\in\mathcal{S}\colon\mathcal{T}^n_{W_s,\delta_2}(f(m))\cap\bigcup_{x^n\in\mathcal{T}^n_{P,\delta_1}}\mathcal{T}^n_{W_{\tilde{s}},\delta_2}(x^n)\neq\varnothing\}.$$

So we have

$$
\begin{aligned}
&|\bigcup_{m\in\mathcal{M}} g^{-1}(m) \cap \bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}} \mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)| \\
&\leqslant \sum_{m\in\mathcal{M}} \sum_{s\in\mathcal{S}^*_m} |\mathcal{T}^n_{W_s,\delta_2}(f(m)) \cap \bigcup_{\bar{x}^n\in\mathcal{T}^n_{P,\delta_1}} \mathcal{T}^n_{W_{\tilde{s}},\delta_2}(\bar{x}^n)| \\
&\leqslant \sum_{m\in\mathcal{M}} \max_{s\in\mathcal{S}^*_m} |\mathcal{T}^n_{W_s,\delta_2}(f(m))||\mathcal{S}| \\
&\leqslant |\mathcal{S}| \sum_{m\in\mathcal{M}} \max_{s\in\mathcal{S}^*_m} \exp(n(H(W_s|P) + |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) + \delta_1|\mathcal{X}|\log|\mathcal{Y}|))(n+1)^{|\mathcal{X}||\mathcal{Y}|} \\
&\leqslant |\mathcal{S}||\mathcal{M}| \max_{m\in\mathcal{M}} \max_{s\in\mathcal{S}^*_m} \exp(n(H(W_s|P) + |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) + \delta_1|\mathcal{X}|\log|\mathcal{Y}|))(n+1)^{|\mathcal{X}||\mathcal{Y}|}.
\end{aligned}
$$

For all $m \in \mathcal{M}$ it holds that for all $s \in \mathcal{S}^*_m$ there is a $y^n \in \mathcal{Y}^n$ such that $y^n \in \mathcal{T}^n_{W_s,\delta_2}(f(m))$ and $y^n \in \mathcal{T}^n_{W_{\tilde{s}},\delta_2}(x^n)$ for a $x^n \in \mathcal{T}^n_{P,\delta_1}$. With Lemma 2.15 it follows that $y^n \in \mathcal{T}^n_{PW_s,(\delta_1+\delta_2)|\mathcal{X}|}$ and $y^n \in \mathcal{T}^n_{PW_{\tilde{s}},(\delta_1+\delta_2)|\mathcal{X}|}$. So we have

$$
\begin{aligned}
&\|PW_s - PW_{\tilde{s}}\|_1 = \sum_{y\in\mathcal{Y}} |PW_s(y) - PW_{\tilde{s}}(y)| \\
&= \sum_{y\in\mathcal{Y}} |PW_s(y) - N(y|y^n)/n + N(y|y^n)/n - PW_{\tilde{s}}(y)| \\
&\leqslant \sum_{y\in\mathcal{Y}} |PW_s(y) - N(y|y^n)/n| + |N(y|y^n)/n - PW_{\tilde{s}}(y)| \leqslant 2|\mathcal{Y}|(\delta_1+\delta_2)|\mathcal{X}|.
\end{aligned}
$$

With Lemma 2.3 it follows that

$$
|H(PW_s) - H(PW_{\tilde{s}})| \leqslant 2|\mathcal{Y}|(\delta_1+\delta_2)|\mathcal{X}|\log\tfrac{1}{2(\delta_1+\delta_2)|\mathcal{X}|}
$$

for all $m \in \mathcal{M}$ and all $s \in \mathcal{S}^*_m$. (We assume δ_1 and δ_2 are small enough.) So altogether we have

$$
\begin{aligned}
|\mathcal{M}| &\geqslant \exp(n(H(PW_{\tilde{s}}) - \theta\log\tfrac{|\mathcal{X}|}{\theta} - \eta - |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) - \delta_1|\mathcal{X}|\log|\mathcal{Y}|)) \\
&\qquad \cdot \tfrac{1}{2|\mathcal{S}|^2(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \exp(-n\delta_2^2) \exp(-n(\min_{m\in\mathcal{M}} \min_{s\in\mathcal{S}^*_m} H(W_s|P))) \\
&= \exp(n(H(PW_{\tilde{s}}) - H(W_{s^*}|P) - \theta\log\tfrac{|\mathcal{X}|}{\theta} - \eta - |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2) - \delta_1|\mathcal{X}|\log|\mathcal{Y}|)) \\
&\qquad \cdot \tfrac{1}{2|\mathcal{S}|^2(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \exp(-n\delta_2^2),
\end{aligned}
$$

for a $s^* \in \bigcup_{m\in\mathcal{M}} S^*_m$. So we have

$$
\begin{aligned}
|\mathcal{M}| \geqslant \exp(n(&-2|\mathcal{Y}|(\delta_1+\delta_2)|\mathcal{X}|\log\tfrac{1}{2(\delta_1+\delta_2)|\mathcal{X}|} - \theta\log\tfrac{|\mathcal{X}|}{\theta} - \eta - |\mathcal{X}||\mathcal{Y}|\delta_2\log(1/\delta_2))) \\
&\cdot \tfrac{1}{2|\mathcal{S}|^2(n+1)^{|\mathcal{X}||\mathcal{Y}|}} \exp(-n\delta_2^2 - n\delta_1|\mathcal{X}|\log|\mathcal{Y}|) \exp(nI(P,W_{s^*})).
\end{aligned}
$$

The result follows as $I(P,W_{s^*}) \geqslant \min_{s\in\mathcal{S}} I(P,W_s)$. (If the procedure terminates because

we can not choose an additional code word we get the same bound as in the case without channel uncertainty.)

■

Now we consider the case of an arbitrary compound channel, i.e. $|\mathcal{S}| < \infty$ does not necessarily hold true. We use the following theorem which essentially is [17, Lemma 4]. (We omit one statement of [17, Lemma 4] in the theorem presented here.) The proof can also be found in [17].

Theorem 2.24 ([17]). *Let $M \in \mathbb{N}$, $M \geqslant 2|\mathcal{Y}|^2$ and $\{W_s\}_{s\in\mathcal{S}}$ with $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$. We can construct $\{V_t\}_{t\in\mathcal{T}}$ with $V_t \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $t \in \mathcal{T}$ such that $|\mathcal{T}| \leqslant (M+1)^{|\mathcal{X}||\mathcal{Y}|}$ and for all $s \in \mathcal{S}$ there is a $t \in \mathcal{T}$ with*

$$\begin{aligned} |W_s(y|x) - V_t(y|x)| &\leqslant \tfrac{|\mathcal{Y}|}{M} \\ W_s(y|x) &\leqslant e^{2|\mathcal{Y}|^2/M} V_t(y|x) \end{aligned}$$

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$.

Similarly to the approach in [17] we use Theorem 2.24 to prove the following achievability result for arbitrary compound channels.

Theorem 2.25. *Let $P \in \mathcal{P}(\mathcal{X})$. The rate $\inf_{s\in\mathcal{S}} I(P, W_s)$ is achievable given P.*

Proof. Consider the smallest possible set $\{V_t\}_{t\in\mathcal{T}}$ as described in Theorem 2.24 (where M is determined below and chosen large enough). For all $s \in \mathcal{S}$ we denote the $t \in \mathcal{T}$ corresponding to s by $t(s)$. From Theorem 2.23 we know that given $\delta > 0$, for all n large enough there is a compound channel code (f, g), such that

$$\begin{aligned} &\tfrac{1}{n} \log |\mathcal{M}| \geqslant \min_{t\in\mathcal{T}} I(P, V_t) - \delta \\ &\min_{t\in\mathcal{T}} \min_{m\in\mathcal{M}} V_t^{\otimes n}(g^{-1}(m)|f(m)) \geqslant 1 - \exp(-nc) \end{aligned}$$

for a $c > 0$. Let $t^* = \arg\min_{t\in\mathcal{T}} I(P, V_t)$ and s^* such that

$$\|W_{s^*}(\cdot|x) - V_{t^*}(\cdot|x)\|_1 \leqslant \tfrac{|\mathcal{Y}|^2}{M}$$

for all $x \in \mathcal{X}$. (The existence of such an s^* follows as we consider the smallest possible set $\{V_t\}_{t\in\mathcal{T}}$.) Thus it holds that

$$\begin{aligned} |I(P, W_{s^*}) - I(P, V_{t^*})| &= |H(W_{s^*}|P) - H(V_{t^*}|P)| \\ &= |\sum_{x\in\mathcal{X}} P(x)(H(W_{s^*}(\cdot|x)) - H(V_{t^*}(\cdot|x)))| \\ &\leqslant \sum_{x\in\mathcal{X}} P(x)|H(W_{s^*}(\cdot|x)) - H(V_{t^*}(\cdot|x))| \leqslant \tfrac{|\mathcal{Y}|^2}{M} \log \tfrac{M}{|\mathcal{Y}|}. \end{aligned}$$

Moreover we have

$$\inf_{s\in\mathcal{S}} I(P,W_s) \leqslant I(P,W_{s^*}) \leqslant I(P,V_{t^*}) + \tfrac{|\mathcal{Y}|^2}{M}\log\tfrac{M}{|\mathcal{Y}|} = \min_{t\in\mathcal{T}} I(P,V_t) + \tfrac{|\mathcal{Y}|^2}{M}\log\tfrac{M}{|\mathcal{Y}|}.$$

For all $s \in \mathcal{S}$ and $m \in \mathcal{M}$ Theorem 2.24 implies

$$\begin{aligned} W_s^{\otimes n}((g^{-1}(m))^c|f(m)) &= \sum_{y^n\in(g^{-1}(m))^c} W_s^{\otimes n}(y^n|f(m)) \\ &\leqslant \sum_{y^n\in(g^{-1}(m))^c} e^{2|\mathcal{Y}|^2 n/M} V_{t(s)}^{\otimes n}(y^n|f(m)) \\ &= e^{2|\mathcal{Y}|^2 n/M} V_{t(s)}^{\otimes n}((g^{-1}(m))^c|f(m)) \leqslant e^{2|\mathcal{Y}|^2 n/M}\exp(-nc). \end{aligned}$$

Now we choose $M = n^2$. Thus the desired result follows.

∎

Note that the encoders constructed in the proofs above are injective.

2.6 Arbitrarily varying channels

The AVC is presented for the first time in [18]. It is another model that allows to include channel uncertainty in the scenario of message transmission over a point-to-point channel. A discussion on AVCs can for example be found in [26].

Compared to the compound channel the AVC is a more pessimistic model in the following sense. As described in [26, Chapter 12], for the compound channel the unknown parameter is constant during the transmission of a codeword, whereas for the AVC the parameter can vary from symbol to symbol.

So again consider Figure 2.2 where this time the channel is an AVC. A code word is generated from a message that should be transmitted over the channel using an encoder $f\colon \mathcal{M} \to \mathcal{X}^n$. This code word serves as the channel input. For each of the n symbols of the code word the channel is represented by one of the stochastic matrices in the set $\{W_s\}_{s\in\mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$. So the channel for the whole transmission is one of the stochastic matrices in the set $\{W_{s^n}\}_{s^n\in\mathcal{S}^n}$ where we define $W_{s^n} = \bigotimes_{i=1}^n W_{s_i}$ for $s^n \in \mathcal{S}^n$. Then we use a decoder $g\colon \mathcal{Y}^n \to \mathcal{M}$ to reconstruct the message from the channel output. We assume that $\mathcal{S}$ is finite and we call the tuple (f,g) an AVC code.

For the DMC and the compound channel achievability is defined with respect to the maximum probability of error. For the AVC we consider the average probability of error. (For a discussion on these two possibilities to measure the performance of AVC codes see for example [26, Chapter 12].) Consequently we arrive at the following definition.

Definition 2.11. *We call $R \geqslant 0$ an* achievable rate *if for all $\delta > 0$ there is an $N \in \mathbb{N}$*

such that for all $n > N$ there is an AVC code (f, g) with

$$\max_{s^n \in \mathcal{S}^n} \tfrac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} W_{s^n}((g^{-1}(m))^c | f(m)) \leqslant \delta$$
$$\tfrac{1}{n} \log |\mathcal{M}| \geqslant R - \delta.$$

We call the supremum of all achievable rates the AVC capacity $C(\{W_s\}_{s \in \mathcal{S}})$.

It is well known that the best possible transmission rate for reliable communication over an AVC (evaluated in terms of average error probability) strongly depends on whether the AVC is symmetrizable. An AVC corresponding to $\{W_s\}_{s \in \mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, is symmetrizable if there is a $U \in \mathcal{P}(\mathcal{S}|\mathcal{X})$ such that

$$\sum_{s \in \mathcal{S}} W_s(y|x) U(s|x') = \sum_{s \in \mathcal{S}} W_s(y|x') U(s|x)$$

for all $x, x', y \in \mathcal{X}^2 \times \mathcal{Y}$ [24, Definition 2].

In order to illustrate the concept of symmetrizability of AVCs we present an example of a symmetrizable AVC. (This example is also discussed in [18] and [2, Example 1], cf. [21].) Assume $|\mathcal{X}| = |\mathcal{S}| = 2$ and $|\mathcal{Y}| = 3$. We define

$$W_1(\cdot|1) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad W_2(\cdot|1) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$
$$W_1(\cdot|2) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad W_2(\cdot|2) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

We can easily check that for all $y \in \mathcal{Y}$

$$\begin{aligned} &W_1(y|1)q_1 + W_2(y|1)(1 - q_1) \\ &\quad = W_1(y|2)q_2 + W_2(y|2)(1 - q_2) \end{aligned}$$

holds true for $q_1 = 1$ and $q_2 = 0$. So the corresponding AVC is symmetrizable which is illustrated in Figure 2.3.

Now we can state an achievability result for AVCs which is proved in [24].

Theorem 2.26. *If the AVC corresponding to $\{W_s\}_{s \in \mathcal{S}}$ is not symmetrizable then*

$$C(\{W_s\}_{s \in \mathcal{S}}) \geqslant \max_{P \in \mathcal{P}(\mathcal{X})} \min_{\bar{W} \in \bar{\mathcal{W}}} I(P, \bar{W})$$

where we define $\bar{\mathcal{W}} = conv(\{W_s\}_{s \in \mathcal{S}})$.

Similarly to the previous models we now want to add the requirement that the code words corresponding to the AVC code are elements of a set $\mathcal{A}$ with a specific property.

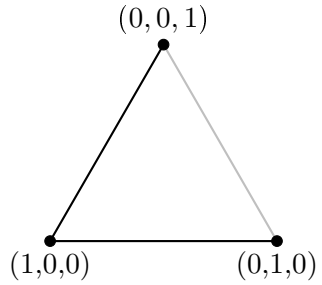

Figure 2.3: The simplex is the set of all distributions on $\mathcal{Y}$. $W_1(\cdot|1)$, $W_1(\cdot|2)$, $W_2(\cdot|1)$ and $W_2(\cdot|2)$ correspond to extreme points. It can be seen that the two sets of convex combinations (represented by the black lines) intersect at $(1, 0, 0)$.

To prove this achievability result we use the following lemma, which basically is [24, Lemma A1]. We give the complete proof from [24] for the reader's convenience.

Lemma 2.27 ([24]). *Let $Z_1 \cdots Z_N$ be arbitrary (discrete) RVs (on a finite alphabet) and let $f_i(Z_1 \cdots Z_i)$ be arbitrary with $0 \leqslant f_i \leqslant 1$, $i = 1, \cdots N$. Then*

$$\sum_{z_i \in \mathcal{Z}_i} P_{Z_i|Z_1 \cdots Z_{i-1}}(z_i|z_1 \cdots z_{i-1}) f_i(z_1 \cdots z_i) \leqslant a \tag{2.19}$$

for all $z_1 \cdots z_{i-1} \in \mathcal{Z}_1 \times \cdots \times \mathcal{Z}_{i-1}$ and all $i \in \{1 \cdots N\}$ implies

$$Pr(\tfrac{1}{N} \sum_{i=1}^{N} f_i(Z_1 \cdots Z_i) > t) \leqslant \exp(-N(t - a \log e)).$$

Proof. We have

$$\begin{aligned} \Pr(\tfrac{1}{N} \sum_{i=1}^{N} f_i(Z_1 \cdots Z_i) > t) &= \Pr(\exp \sum_{i=1}^{N} f_i(Z_1 \cdots Z_i) > \exp(Nt)) \\ &\leqslant \exp(-Nt) E(\exp \sum_{i=1}^{N} f_i(Z_1 \cdots Z_i)) \end{aligned}$$

where for the last inequality we use Markov's inequality. The expectation in the last line equals

$$\begin{aligned} &\sum_{\substack{z_1 \cdots z_{N-1} \\ \in \mathcal{Z}_1 \times \cdots \times \mathcal{Z}_{N-1}}} P_{Z_1 \cdots Z_{N-1}}(z_1 \cdots z_{N-1}) \exp(\sum_{i=1}^{N-1} f_i(z_1 \cdots z_i)) \\ &\cdot \sum_{z_N \in \mathcal{Z}_N} P_{Z_N|Z_1 \cdots Z_{N-1}}(z_N|z_1 \cdots z_{N-1}) \exp(f_N(z_1 \cdots z_N)). \end{aligned}$$

As $0 \leqslant f \leqslant 1$ implies $\exp f \leqslant 1 + f$ we use (2.19) to bound the second factor by $1 + a \leqslant e^a = \exp(a \log e)$. Repeating this procedure $N - 1$ times we get the desired result.

∎

Using Lemma 2.27 we prove the next lemma that is similar to [24, Lemma 3] (see also [23, Lemma V.1]). Compared to [24, Lemma 3], the code words are contained in a more restricted set. We also show how to choose the code words such that they are distinct.

Lemma 2.28 ([24]). *Let $1 > \eta > 0$, $\delta > 0$ and $P \in \mathcal{P}(n, \mathcal{X})$. Choose real numbers R, ϵ that satisfy $0 < \epsilon \leqslant R \leqslant H(P)$. There is a $n_0(\epsilon, \eta, |\mathcal{X}|, |\mathcal{S}|) \in \mathbb{N}$ such that for all $n \geqslant n_0$ it holds that given $\mathcal{A} \subset \mathcal{T}_P^n$ with $P^{\otimes n}(\mathcal{A}) > \frac{\eta}{(n+1)^{|\mathcal{X}|}}$ and $N = \exp(\lceil nR \rceil)$ there exist (not necessarily distinct) codewords $x_1^n \cdots x_N^n \in \mathcal{A}$ such that for every $x^n \in \mathcal{X}^n$, $s^n \in \mathcal{S}^n$ and $P_{X\bar{X}S} \in \mathcal{P}(n, \mathcal{X} \times \mathcal{X} \times \mathcal{S})$ we have*

$$|\{j \colon (x^n, x_j^n, s^n) \in \mathcal{T}^n_{P_{X\bar{X}S}}\}| \leqslant \exp(n(|R - I(\bar{X} \wedge XS)|^+ + \epsilon)) \tag{2.20}$$

$$\tfrac{1}{N}|\{i \colon (x_i^n, s^n) \in \mathcal{T}^n_{P_{\bar{X}S}}\}| \leqslant \exp(-n\epsilon/2) \text{ if } I(\bar{X} \wedge S) > \epsilon \tag{2.21}$$

$$\tfrac{1}{N}|\{i \colon (x_i^n, x_j^n, s^n) \in \mathcal{T}^n_{P_{X\bar{X}S}} \text{ for some } j \neq i\}| \leqslant \exp(-n\epsilon/2) \text{ if } I(X \wedge \bar{X}S) - |R - I(\bar{X} \wedge S)|^+ > \epsilon. \tag{2.22}$$

Assume $R > \epsilon$. Then we can choose a set of at least $\lfloor N \exp(-n(\epsilon + \delta)) \rfloor$ sequences from $x_1^n \cdots x_N^n$ which are all distinct.

The proof relies on the probabilistic method. It basically differs from the proof of [24, Lemma 3] in the set the codewords are randomly chosen from. We also add a requirement such that most of the code words can be chosen distinct.

In short, for the proof we randomly choose the codewords from $\mathcal{A}$. For an arbitrary x^n, s^n and $P_{X|XS}$ we use Chernoff bounds to show that (2.20), (2.21) and (2.22) hold with probabilities going to 1 doubly exponentially with respect to n. (An additional property used to have distinct codewords is proved similarly.) As $\mathcal{S}^n$, $\mathcal{X}^n$ and $\mathcal{P}(n, \mathcal{X} \times \mathcal{X} \times \mathcal{S})$ depend at most exponentially on n the union bound gives the desired result for the probabilistic method.

Proof. As in [24, Proof of Lemma 3] let $Z_1 \cdots Z_N$ be independent RVs each uniformly distributed on $\mathcal{A}$. For $P_{XS} \neq P_{x^n, s^n}$ or $P_{\bar{X}} \neq P$ (2.20) holds trivially. Now we consider $P_{XS} = P_{x^n, s^n}$ and $P_{\bar{X}} = P$. As done in [24, Proof of Lemma 3] define for all $i \in \{1 \cdots N\}$

$$f_i(Z_1 \cdots Z_i) = \begin{cases} 1 & \text{if } Z_i \in \mathcal{T}^n_{P_{\bar{X}|XS}}(x^n, s^n) \\ 0 & \text{otherwise} \end{cases}. \tag{2.23}$$

It holds that

$$\eta(n+1)^{-|\mathcal{X}|} \leqslant P^{\otimes n}(\mathcal{A}) = |\mathcal{A}| P^{\otimes n}(x^n) = |\mathcal{A}| \exp(-nH(P)).$$

We see that (2.19) is fulfilled with

$$\begin{aligned} a = \Pr(Z_j \in \mathcal{T}^n_{P_{\bar{X}|XS}}(x^n, s^n)) &= \frac{|\mathcal{T}^n_{P_{\bar{X}|XS}}(x^n, s^n) \cap \mathcal{A}|}{|\mathcal{A}|} \\ \leqslant \frac{\exp(nH(\bar{X}|XS))}{(n+1)^{-|\mathcal{X}|}\eta \exp(nH(P))} &= \frac{(n+1)^{|\mathcal{X}|}}{\eta} \exp(-nI(\bar{X} \wedge XS)) \end{aligned}$$

where the last step follows from $H(P) = H(\bar{X})$. Now we continue as in [24, Proof of Lemma 3], i.e., we choose

$$t = \tfrac{1}{N} \exp(n(|R - I(\bar{X} \wedge XS)|^+ + \epsilon)).$$

Thus $N(t - a \log e) \geqslant \exp(n\epsilon)/2$ if $n \geqslant n_1(\epsilon, \eta, |\mathcal{X}|)$, where

$$n_1(\epsilon, \eta, |\mathcal{X}|) = \min(n \colon \tfrac{(n+1)^{|\mathcal{X}|}}{\eta} \log e < \tfrac{1}{2} \exp(n\epsilon)).$$

Lemma 2.27 implies

$$\Pr(|\{j \colon Z_j \in \mathcal{T}^n_{P_{\bar{X}|XS}}(x^n, s^n)\}| > \exp(n(|R - I(\bar{X} \wedge XS)|^+ + \epsilon))) < \exp(-\tfrac{1}{2} \exp(n\epsilon)).$$

By the same argumentation, replacing $\mathcal{T}^n_{P_{\bar{X}|XS}}(x^n, s^n)$ by $\mathcal{T}^n_{P_{\bar{X}|X}}(x^n)$ in (2.23), we get

$$\Pr(|\{j \colon Z_j \in \mathcal{T}^n_{P_{\bar{X}|X}}(x^n)\}| > \exp(n(|R - I(\bar{X} \wedge X)|^+ + \epsilon))) < \exp(-\tfrac{1}{2} \exp(n\epsilon)) \quad (2.24)$$

for $P_{\bar{X}} = P$.

Now it is clear that using the same argumentation as in [24, Proof of Lemma 3] we also get

$$\Pr(\tfrac{1}{N}|\{j \colon Z_j \in \mathcal{T}^n_{P_{\bar{X}|S}}(s^n)\}| > \exp(-n\epsilon/2)) < \exp(-\tfrac{1}{2} \exp(n\epsilon/2)).$$

if $I(\bar{X} \wedge S) > \epsilon$ and

$$\Pr(\tfrac{1}{N}|\{i \colon Z_i \in \mathcal{T}_{P_{X|\bar{X}S}}(Z_j, s^n) \text{ for some } j \neq i\}| > \exp(-\tfrac{n\epsilon}{2})) < 4 \exp(-\tfrac{1}{2} \exp(\tfrac{n\epsilon}{4}))$$

if $I(X \wedge \bar{X}S) > |R - I(\bar{X} \wedge S)|^+ + \epsilon$ and $n \geqslant n_1(\epsilon/4, \eta, |\mathcal{X}|)$.

Now we use the same argumentation as in [24, Proof of Lemma 3]. The number of all possible combinations of $x^n \in \mathcal{X}^n$, $s^n \in \mathcal{S}^n$ and $P_{X\bar{X}S} \in \mathcal{P}(n, \mathcal{X} \times \mathcal{X} \times \mathcal{S})$ grows exponentially in n. Thus the doubly exponential probability bounds ensure that with probability close to 1 the above inequalities hold simultaneously if n is sufficiently large. So there are codewords $x_1^n, \cdots, x_N^n$ with the desired properties.

As done in the proof of [22, Lemma 2] we can now select a set of at least $\lfloor N \exp(-n(\epsilon + \delta)) \rfloor$ sequences from $x_1^n \cdots x_N^n$ which are all distinct (if we assume $R > \epsilon$). This works as follows. We know from (2.24) that for all $x^n \in \mathcal{X}^n$ and all $P_{X\bar{X}} \in \mathcal{P}(n, \mathcal{X} \times \mathcal{X})$

$$|\{j\colon x_j^n \in \mathcal{T}^n_{P_{\bar{X}|X}}(x^n)\}| \leqslant \exp(n(|R - I(\bar{X} \wedge X)|^+ + \epsilon)). \tag{2.25}$$

Assume $I(x_i^n \wedge x_j^n) < R$ for $i \neq j$. Now assume $x_i^n = x_j^n$. This implies $H(P) < R$ which contradicts our assumption $R \leqslant H(P)$. So if we keep only the codewords with $I(x_i^n \wedge x_j^n) < R$ we know that they are all distinct. Now (2.25) implies that

$$|\{j\colon x_j^n \in \mathcal{T}^n_{P_{\bar{X}|X}}(x^n)\}| \leqslant \exp(n\epsilon)$$

if $I(P, P_{\bar{X}|X}) \geqslant R$. As $|\mathcal{P}(n, \mathcal{X} \times \mathcal{X})| \leqslant (n+1)^{|\mathcal{X}|^2}$ this implies for all $i \leqslant N$

$$|\{j\colon I(x_j^n \wedge x_i^n) \geqslant R\}| \leqslant \exp(n\epsilon)(n+1)^{|\mathcal{X}|^2}. \tag{2.26}$$

Now successively choose sequences from $x_1^n \cdots x_N^n$ such that for these sequences it holds that $I(x_i^n \wedge x_j^n) < R$ for $i \neq j$. Assume we have q such sequences and can not find an additional one. Then from (2.26) we know

$$q \exp(n\epsilon)(n+1)^{|\mathcal{X}|^2} > N.$$

This means $q > N \frac{\exp(-n\epsilon)}{(n+1)^{|\mathcal{X}|^2}} \geqslant \lfloor N \exp(-n(\epsilon + \delta)) \rfloor$ for n large enough.

∎

Now we can prove the result on channel codes for arbitrarily varying channels. This is a slight variation of [24, Theorem 1]. The main difference again is that the codewords are taken from a more restricted set. Additionally we consider injective encoders.

Lemma 2.29 ([24]). *Let $1 > \eta > 0$, $\epsilon > 0$, $\frac{1}{2|\mathcal{Y}|} > \delta > 0$, $\tau > 0$, $P_X \in \mathcal{P}(\mathcal{X})$ with*

$$\min_{x \in \mathcal{X}} P_X(x) > \delta$$

and $\mathcal{D}$ a finite set. Consider the AVC corresponding to $\{W_s\}_{s \in \mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$ and assume it is not symmetrizable. There is an $n_0(\epsilon, \eta, \tau, |\mathcal{X}|, |\mathcal{S}|, |\mathcal{Y}|) \in \mathbb{N}$ such that for all $n \geqslant n_0$ for all $\mathcal{A} \subset \mathcal{T}^n_{P_{\bar{X}}}$, $P_{\bar{X}} \in \mathcal{P}(n, \mathcal{X})$ with $\|P_{\bar{X}} - P_X\|_1 \leqslant \delta$ (thus $\min_{x \in \mathcal{X}} P_{\bar{X}}(x) > \beta > 0$) and

$$P_X^{\otimes n}(\mathcal{A}) > \tfrac{\eta}{(n+1)^{|\mathcal{X}|}} \exp(-nD(P_{\bar{X}} \| P_X))$$

there is a pair of mappings (f_n, ϕ_n), $f_n\colon \mathcal{D} \to \mathcal{X}^n$, $\phi_n\colon \mathcal{Y}^n \to \mathcal{D}$, $f_n(\mathcal{D}) \subset \mathcal{A}$, such that

$$\tfrac{1}{n} \log |\mathcal{D}| \geqslant \min_{\bar{W} \in \bar{\mathcal{W}}} I(P_X, \bar{W}) - \tau - \rho(\delta)$$

where $\rho\colon \mathbb{R}_+ \to \mathbb{R}$, $\rho(\delta) = -|\mathcal{Y}|\delta \log \frac{\delta|\mathcal{Y}|}{|\mathcal{X}|} + \log|\mathcal{Y}|\delta$, $\bar{\mathcal{W}} = conv(\{W_s\}_{s\in\mathcal{S}})$ *and*

$$\max_{s^n\in\mathcal{S}^n} \tfrac{1}{|\mathcal{D}|} \sum_{d\in\mathcal{D}} W_{s^n}((\phi_n^{-1}(d))^c | f_n(d)) \leqslant \epsilon. \tag{2.27}$$

We call such tuples (f_n, ϕ_n) *constant composition* (n,ϵ)*-codes for the AVC corresponding to* $\{W_s\}_{s\in\mathcal{S}}$*. Additionally* f_n *is injective.*

For the proof we use Lemma 2.28 and [24, Lemma 4]. The proof then follows the same argumentation as the proof of [24, Lemma 5]. Additionally we use [26, Lemma 2.7]. So the result above follows from Lemma 2.28 exactly as in [24]. We only need an additional continuity argument.

Proof. From $P_{\bar{X}}^{\otimes n}(\mathcal{A}) > \frac{\eta \exp(-nD(P_{\bar{X}}\|P_X))}{(n+1)^{|\mathcal{X}|}}$ we have

$$|\mathcal{A}| > \tfrac{\eta \exp(nH(P_{\bar{X}}))}{(n+1)^{|\mathcal{X}|}}.$$

So we have

$$P_{\bar{X}}^{\otimes n}(\mathcal{A}) = |\mathcal{A}| \exp(-nH(P_{\bar{X}})) > \tfrac{\eta}{(n+1)^{|\mathcal{X}|}}.$$

So from Lemma 2.28 and [24, Lemma 4] we can show in the same way as in the proof of [24, Lemma 5] that (f_n, ϕ_n) with

$$\tfrac{1}{n}\log|\mathcal{D}| \geqslant \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_{\bar{X}}, \bar{W}) - \tau$$

and (2.27) exist for all n large enough. The corresponding decoder is the decoder described in [24, Definition 3], which can be chosen such that the decoding rule is unambiguous as shown in [24, Lemma 4]. (f_n is injective as the codewords can be chosen distinct as described in Lemma 2.28.) Now consider

$$\begin{aligned} |I(P_X, \bar{W}) - I(P_{\bar{X}}, \bar{W})| &= |I(X \wedge Y) - I(\bar{X} \wedge \bar{Y})| \\ &\leqslant |H(Y) - H(\bar{Y})| + |H(Y|X) - H(\bar{Y}|\bar{X})| \end{aligned}$$

where $P_{XY}(x,y) = P_X(x)\bar{W}(y|x)$ and $P_{\bar{X}\bar{Y}}(x,y) = P_{\bar{X}}(x)\bar{W}(y|x)$ for all $(x,y) \in \mathcal{X}\times\mathcal{Y}$. We have

$$\begin{aligned} \|P_Y - P_{\bar{Y}}\|_1 &= \sum_{y\in\mathcal{Y}} |\sum_{x\in\mathcal{X}} (P_X(x) - P_{\bar{X}}(x))\bar{W}(y|x)| \\ &\leqslant \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} \bar{W}(y|x)|P_X(x) - P_{\bar{X}}(x)| \leqslant |\mathcal{Y}|\delta. \end{aligned}$$

So [26, Lemma 2.7] implies

$$|H(Y) - H(\bar{Y})| \leqslant -|\mathcal{Y}|\delta \log \tfrac{\delta|\mathcal{Y}|}{|\mathcal{X}|}$$

for $\delta < \frac{1}{2|\mathcal{Y}|}$. We also have

$$H(Y|X=x) = H(\bar{W}(\cdot|x)) = H(\bar{Y}|\bar{X}=x)$$

for all $x \in \mathcal{X}$. So

$$\begin{aligned}
|H(Y|X) - H(\bar{Y}|\bar{X})| &= |\sum_{x\in\mathcal{X}} P_X(x)H(Y|X=x) - P_{\bar{X}}(x)H(\bar{Y}|\bar{X}=x)| \\
&\leqslant \sum_{x\in\mathcal{X}} |P_X(x)H(Y|X=x) - P_{\bar{X}}(x)H(\bar{Y}|\bar{X}=x)| \\
&= \sum_{x\in\mathcal{X}} H(Y|X=x)|P_X(x) - P_{\bar{X}}(x)| \leqslant \log|\mathcal{Y}|\delta.
\end{aligned}$$

Now let $\min_{\bar{W}\in\bar{\mathcal{W}}} I(P_{\bar{X}}, \bar{W}) = I(P_{\bar{X}}, \bar{W})$. We have

$$I(P_{\bar{X}}, \bar{W}) - \tau \geqslant I(P_X, \bar{W}) - \tau - \rho(\delta) \geqslant \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_X, \bar{W}) - \tau - \rho(\delta).$$

■

3 SK Generation with Constrained Privacy Leakage Rate

In this chapter we consider SK generation from a PUF source, i.e. the source model for SK generation with a rate constraint on the privacy leakage cf. Section 2.2. As described in Section 2.2 we can study secure storage of a key using a PUF with this model. Motivated by the discussion in Section 2.1 we consider generation of a uniformly distributed SK such that perfect secrecy is achieved. In the course of this chapter we vary the model inasmuch as we weaken the assumptions on our knowledge of the PUF source statistics. For all three settings that we consider we derive corresponding capacity results.

3.1 SK generation from a PUF source

The scenario for SK generation from a PUF source is depicted in Figure 3.1. As discussed in Section 2.1 and Section 2.2 a SK (represented by the RV K) is generated at one terminal and reconstructed at a second terminal (where the reconstruction is represented by the RV $\hat{K}$). A message (represented by the RV M) can be sent from one terminal to the other via a noiseless public channel. The PUF source, represented by a DMMS with generic RVs X and Y, puts out RVs X^n and Y^n. X^n is observed at the first terminal whereas Y^n is observed at the second terminal.

As mentioned in Section 2.1 we consider a randomized encoder F. So (K, M) are generated from X^n using a randomized encoder F and $\hat{K} = g(M, Y^n)$ where we call the tuple (F, g) with $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n)$ and $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$ a SK generation protocol.

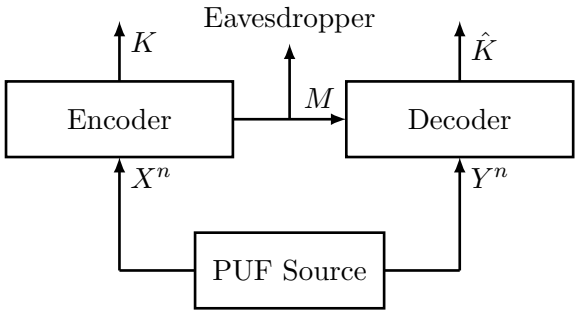

Figure 3.1: SK generation from a PUF source (or equivalently from a biomatric source as considered in [32], cf. Section 2.2).

This model establishes the joint distribution of K, M and $\hat{K}$. For all $(k, m, \hat{k}) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K}$ we have

$$P_{KM\hat{K}}(k, m, \hat{k}) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} P_{XY}^{\otimes n}(x^n, y^n) F(k, m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}((y^n, m)).$$

A SK generation protocol should have certain properties to be considered a good SK generation protocol which are specified in the following definition.

Definition 3.1. *A tuple (R, L), $R, L \geqslant 0$, is an achievable SK generation/privacy leakage rate pair if for all $\delta > 0$ there is an $n_0 \in \mathbb{N}$ and a $c > 0$ such that for all $n \geqslant n_0$ there is a SK generation protocol (F, g) such that*

$$\begin{aligned} &Pr(K \neq \hat{K}) \leqslant \exp(-nc) \\ &I(K \wedge M) = 0 \\ &H(K) = \log |\mathcal{K}| \\ &\tfrac{1}{n} \log |\mathcal{K}| \geqslant R - \delta \\ &\tfrac{1}{n} I(M \wedge X^n) \leqslant L + \delta. \end{aligned}$$

We call the set of all such achievable rate pairs the capacity region $\mathcal{R}_{SK}^{PL}$.

In particular we want to control the privacy leakage rate of the protocols as we consider a PUF source, cf. Section 2.2, and we want that the protocols meet the perfect secrecy requirement and that the SK is uniformly distributed, cf. Section 2.1.

We now want to characterize $\mathcal{R}_{SK}^{PL}$.

Theorem 3.1. *It holds that*

$$\mathcal{R}_{SK}^{PL} \supseteq \bigcup_U \{(R, L) \colon 0 \leqslant R \leqslant I(U \wedge Y), L \geqslant I(U \wedge X) - I(U \wedge Y)\}$$

where the union is taken over all RVs U with $U - X - Y$.

The proof technique is based on [5, Proof of Proposition 1a)].

Proof. Let $\delta > 0$. Choose $\eta > 0$ and $c > 0$ small enough. Choose the RV U such that $U - X - Y$. For all n large enough construct the set $\mathcal{J} = \{u_{k,m}\}_{(k,m) \in \mathcal{K} \times \mathcal{M}}$ where $u_{k,m} \in \mathcal{U}^n$ and

$$|\mathcal{K}| = \exp(n(I(U \wedge Y) - \delta - \xi)) \tag{3.1}$$

where $0 \leqslant \xi \leqslant \frac{1}{n}$ such that $n(I(U \wedge Y) - \delta - \xi)$ is an integer. Moreover $\mathcal{J}$ is chosen such that it holds that

$$P_U^{\otimes n}(\mathcal{J}) > 1 - \exp(-n\eta)(n+1)^{|\mathcal{U}|}$$

and for all $m \in \mathcal{M}$ there is a $g_m \colon \mathcal{Y}^n \to \mathcal{K}$ such that

$$P_{Y|U}^{\otimes n}(g_m^{-1}(k)|u_{k,m}) \geqslant 1 - \exp(-nc) \tag{3.2}$$

for all $k \in \mathcal{K}$ and for all $m \in \mathcal{M}$ there is a $P \in \mathcal{P}(n,\mathcal{U})$ such that for all $k \in \mathcal{K}$ it holds that $u_{k,m} \in \mathcal{T}_P^n$.

We can construct $\mathcal{J}$ as follows. First choose a $P \in \mathcal{P}(n,\mathcal{U})$. Then choose an arbitrary set $\mathcal{A}_1 \subset \mathcal{T}_P^n$ with $P_U^{\otimes n}(\mathcal{A}_1) \geqslant \exp(-n\eta)$. For η small enough and all n large enough we can choose a channel code for the DMC $P_{Y|U}^{\otimes n}$ corresponding to $(u_{k,1}, g_1^{-1}(k))_{k\in\mathcal{K}}$ such that (3.2) and (3.1) hold true and $\{u_{k,1}\}_{k\in\mathcal{K}} \subset \mathcal{A}_1$. This follows from Theorem 2.21. In the i-th step choose $\mathcal{A}_i \subset \mathcal{T}_P^n \backslash \bigcup_{j\in[i-1]} \{u_{k,j}\}_{k\in\mathcal{K}}$ with $P_U^{\otimes n}(\mathcal{A}_i) \geqslant \exp(-n\eta)$. If this is not possible anymore (that is this choice of $\mathcal{A}_i$) do the same procedure for all $P \in \mathcal{P}(n,\mathcal{U})$. Thus after this procedure terminates it holds that $P_U^{\otimes n}(\mathcal{J}) > 1 - \exp(-n\eta)(n+1)^{|\mathcal{U}|}$.

Now define (F, g) as follows.

$$\begin{aligned} F(k,m|x^n) &= P_{U|X}^{\otimes n}(u_{k,m}|x^n) + P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} \\ g(y^n, m) &= g_m(y^n) \end{aligned}$$

It holds that

$$\begin{aligned} \Pr(K \neq \hat{K}) &= \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K} \\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n) F(k,m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\ &= \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K} \\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n) P_{U|X}^{\otimes n}(u_{k,m}|x^n) \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n) \\ &\quad + \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K} \\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n) P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n). \end{aligned}$$

For the second summand we have

$$\begin{aligned} &\sum_{m\in\mathcal{M}} \sum_{k\in\mathcal{K}} \sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n) P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} \sum_{\substack{\hat{k}\in\mathcal{K}: \\ \hat{k}\neq k}} \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n) \\ \leqslant &\sum_{m\in\mathcal{M}} \sum_{k\in\mathcal{K}} \sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n) P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} \end{aligned}$$

as $\sum_{\substack{\hat{k}\in\mathcal{K}: \\ \hat{k}\neq k}} \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n) \leqslant 1$ for all $k \in \mathcal{K}$. This expression equals

$$\sum_{m\in\mathcal{M}} \sum_{k\in\mathcal{K}} P_U^{\otimes n}(\mathcal{J}^c)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} \leqslant \exp(-n\eta)(n+1)^{|\mathcal{U}|}.$$

For the first summand we have

$$\begin{aligned}
&\sum_{m\in\mathcal{M}}\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}}\sum_{y^n} P_{Y|U}^{\otimes n}(y^n|u_{k,m})P_U^{\otimes n}(u_{k,m})\mathbb{1}_{g_m^{-1}(\hat{k})}(y^n)\\
&= \sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}} P_U^{\otimes n}(u_{k,m})\sum_{y^n}\sum_{\substack{\hat{k}\in\mathcal{K}:\\ \hat{k}\neq k}} \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n)P_{Y|U}^{\otimes n}(y^n|u_{k,m})\\
&= \sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}} P_U^{\otimes n}(u_{k,m})P_{Y|U}^{\otimes n}((g_m^{-1}(k))^c|u_{k,m})\\
&\leqslant \sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}} P_U^{\otimes n}(u_{k,m})\exp(-nc) \leqslant \exp(-nc).
\end{aligned}$$

Now consider

$$\begin{aligned}
\Pr(K=k,M=m) &= \sum_{\hat{k}}\sum_{x^n,y^n} P_{XY}^{\otimes n}(x^n,y^n)F(k,m|x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)\\
&= \sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n) + \sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}|}\tfrac{1}{|\mathcal{M}|}
\end{aligned}$$

and

$$\Pr(M=m) = \sum_{k\in\mathcal{K}}\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n) + \sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{M}|}.$$

Consider a permutation π on $[n]$ (and we also denote by π the corresponding permutation on e.g. $\mathcal{X}^n$). So we have $\pi^{-1}(\mathcal{X}^n)=\mathcal{X}^n$. It holds that

$$\begin{aligned}
&\sum_{x^n\in\mathcal{X}^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(\pi(u_{k,m})|x^n) = \sum_{\bar{x}^n\in\pi^{-1}(\mathcal{X}^n)} P_X^{\otimes n}(\pi(\bar{x}^n))P_{U|X}^{\otimes n}(\pi(u_{k,m})|\pi(\bar{x}^n))\\
&= \sum_{\bar{x}^n\in\pi^{-1}(\mathcal{X}^n)} P_X^{\otimes n}(\bar{x}^n)P_{U|X}^{\otimes n}(u_{k,m}|\bar{x}^n) = \sum_{\bar{x}^n\in\mathcal{X}^n} P_X^{\otimes n}(\bar{x}^n)P_{U|X}^{\otimes n}(u_{k,m}|\bar{x}^n).
\end{aligned}$$

For the second step we use the product structure of the distribution. As according to our construction there is a $P\in\mathcal{P}(n,\mathcal{U})$ such that $u_{k,m}\in\mathcal{T}_P^n$ for all $k\in\mathcal{K}$ we have

$$\sum_{k\in\mathcal{K}}\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n) = |\mathcal{K}|\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n)$$

for an arbitrary $k\in\mathcal{K}$. Thus we get

$$\begin{aligned}
\Pr(K=k|M=m) &= \tfrac{\Pr(K=k,M=m)}{\Pr(M=m)}\\
&= \frac{\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n)+\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{M}|}}{|\mathcal{K}|\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(u_{k,m}|x^n)+\sum_{x^n} P_X^{\otimes n}(x^n)P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\frac{1}{|\mathcal{M}|}} = \tfrac{1}{|\mathcal{K}|}
\end{aligned}$$

which means $H(K|M)=\log|\mathcal{K}|$.

Moreover, using Fano's inequality, we get $H(K|MY^n) \leqslant F$ for a $F > 0$ arbitrarily small for all n large enough. So it holds that

$$\begin{aligned} I(M \wedge X^n) &\leqslant I(M \wedge X^n) - H(K|MY^n) + F \\ &= I(MK \wedge X^n) - H(K|MY^n) + F - I(K \wedge X^n|M). \end{aligned}$$

With $I(K \wedge X^n|M) = H(K|M) - H(K|MX^n)$ and $H(K|M) = \log|\mathcal{K}|$ it follows that

$$I(M \wedge X^n) \leqslant I(MK \wedge X^n) - \log|\mathcal{K}| - H(K|MY^n) + H(K|MX^n) + F.$$

It is obvious that $KM - X^n - Y^n$. This implies $K - MX^n - Y^n$. So it holds that

$$H(K|MX^n) = H(K|MX^nY^n) \leqslant H(K|MY^n)$$

and as $\log|\mathcal{K}| = n(I(U \wedge Y) - \delta - \xi)$ we have

$$I(M \wedge X^n) \leqslant I(MK \wedge X^n) - n(I(U \wedge Y) - \delta - \xi) + F.$$

Now consider the mapping $q\colon \mathcal{K} \times \mathcal{M} \to \mathcal{U}^n$, $q(k,m) = u_{k,m}$. This mapping is injective. So it holds that $I(KM \wedge X^n) = I(q(K,M) \wedge X^n)$. Furthermore we have

$$P_{q(K,M)|X^n}(u^n|x^n) = \sum_{(k,m)\in\mathcal{K}\times\mathcal{M}} F(k,m|x^n)\mathbb{1}_{\{u_{k,m}\}}(u^n).$$

Now consider

$$\begin{aligned} \|P_{q(K,M)X^n} - P_{UX}^{\otimes n}\|_1 &= \sum_{x^n\in\mathcal{X}^n} P_X^{\otimes n}(x^n) \sum_{(k,m)\in\mathcal{K}\times\mathcal{M}} P_{U|X}^{\otimes n}(\mathcal{J}^c|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|} + P_U^{\otimes n}(\mathcal{J}^c) \\ &= 2P_U^{\otimes n}(\mathcal{J}^c) \leqslant 2\exp(-n\eta)(n+1)^{|\mathcal{U}|}. \end{aligned}$$

From the continuity of entropy it follows that

$$I(q(K,M) \wedge X^n) \leqslant I(U^n \wedge X^n) + \delta$$

for all n large enough and the RV U^n such that $P_{U^nX^n} = P_{UX}^{\otimes n}$. Altogether we thus have

$$\tfrac{1}{n}I(M \wedge X^n) \leqslant I(U \wedge X) - I(U \wedge Y) + F/n + \delta + \xi + \delta/n.$$

■

Now we prove the converse result.

Theorem 3.2. *It holds that*

$$\mathcal{R}_{SK}^{PL} \subseteq \bigcup_U \{(R,L)\colon 0 \leqslant R \leqslant I(U \wedge Y), L \geqslant I(U \wedge X) - I(U \wedge Y)\}$$

where the union is taken over all RVs U with $U - X - Y$.

Proof. It holds that

$$\log|\mathcal{K}| = H(K) = I(K \wedge \hat{K}) + H(K|\hat{K}) \leqslant I(K \wedge MY^n) + F$$

where we use Fano's inequality and thus F is arbitrarily small for all n large enough (and $K - MY^n - \hat{K}$). Additionally it holds that $I(K \wedge Y^n M) = I(K \wedge M) + I(K \wedge Y^n|M)$ and $I(K \wedge Y^n|M) \leqslant I(Y^n \wedge MK)$. We also have

$$\log|\mathcal{K}| \leqslant I(Y^n \wedge MK) + F = \sum_{i=1}^{n} I(KMY^{i-1} \wedge Y_i) + F.$$

We know that $MK - X^n - Y^n$. This implies $KM - X^{i-1}X_iY_i - Y^{i-1}$. Thus we get $KMY_i - X^{i-1} - Y^{i-1}$ and consequently $Y_i - KMX^{i-1} - Y^{i-1}$. This means

$$I(KMY^{i-1} \wedge Y_i) \leqslant I(KMY^{i-1}X^{i-1} \wedge Y_i) = I(KMX^{i-1} \wedge Y_i).$$

So

$$\log|\mathcal{K}| \leqslant \sum_{i=1}^{n} I(KMX^{i-1} \wedge Y_i) + F = \sum_{i=1}^{n} I(U_i \wedge Y_i) + F$$

where for the last step we define $U_i = KMX^{i-1}$. From $KM - X^n - Y^n$ it follows that $KM - X^{i-1}X_i - Y_i$ and thus $KMX^{i-1} - X_i - Y_i$, so $U_i - X_i - Y_i$. Moreover we have

$$\begin{aligned} &I(X^n \wedge M) = H(M) - H(M|X^n) \geqslant H(M|Y^n) - H(KM|X^n) \\ &= H(KM|Y^n) - H(K|Y^nM) - H(KM|X^n) \geqslant I(KM \wedge X^n) - I(KM \wedge Y^n) - F, \end{aligned}$$

where for the last step we again use Fano's inequality (and $K - MY^n - \hat{K}$). Following the same argumentation as above we thus have

$$I(X^n \wedge M) \geqslant \sum_{i=1}^{n} I(U_i \wedge X_i) - \sum_{i=1}^{n} I(U_i \wedge Y_i) - F.$$

Define $U = QU_Q$ and consider X_Q and Y_Q where Q is a RV uniformly distributed on $[n]$ and independent of $X^nY^nU^n$. It is clear that $P_{X_QY_Q} = P_{XY}$ as X^nY^n are i.i.d. random vectors. So we have

$$P_{UX_QY_Q}((q,u),x,y) = P_{QU_qX_qY_q}(q,u,x,y) = P_Q(q)P_{U_q|X_q}(u|x)P_{X_qY_q}(x,y)$$

where the last step follows from $U_q - X_q - Y_q$. As $P_{X_qY_q} = P_{XY}$ we have

$$P_{UX_QY_Q}((q,u),x,y) = P_Q(q)P_{U_q|X_q}(u|x)P_{XY}(x,y) = P_{U|X_Q}((q,u)|x)P_{X_QY_Q}(x,y)$$

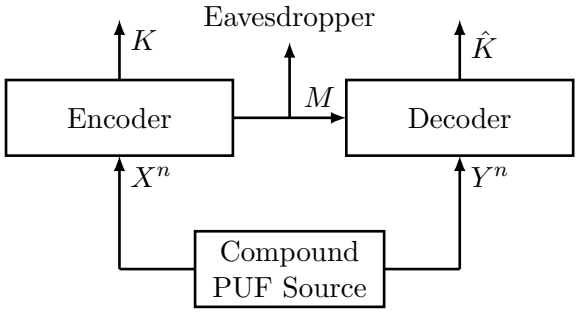

Figure 3.2: SK generation from a compound PUF source.

with $P_{U|X_Q}((q,u)|x) = P_Q(q)P_{U_q|X_q}(u|x)$ (i.e. $U - X_Q - Y_Q$). Finally consider

$$\sum_{i=1}^{n} \tfrac{1}{n} I(U_i \wedge Y_i) = \sum_{q=1}^{n} P_Q(q) I(U_Q \wedge Y_Q|Q=q) = I(U_Q \wedge Y_Q|Q)$$
$$= H(Y_Q|Q) - H(Y_Q|U_Q Q) = H(Y_Q) - H(Y_Q|U) = I(U \wedge Y_Q)$$

and

$$\sum_{i=1}^{n} I(U_i \wedge X_i) - \sum_{i=1}^{n} I(U_i \wedge Y_i) = I(U_Q \wedge X_Q|Q) - I(U_Q \wedge Y_Q|Q)$$
$$= H(X_Q|Q) - H(Y_Q|Q) - H(X_Q|U) + H(Y_Q|U)$$
$$= H(X_Q) - H(Y_Q) - H(X_Q|U) + H(Y_Q|U) = I(U \wedge X_Q) - I(U \wedge Y_Q).$$

■

3.2 SK generation from a compound PUF source

Now we consider SK generation from a PUF source where the source statistics are not known exactly. Instead we know a set of distributions the actual distribution belongs to. We call this PUF source with source uncertainty a compound PUF source. These considerations not only generalize our results, but they also make sense from a practical point of view. When a probabilistic model is used in practice, it might be hard to determine the corresponding distributions with measurements. By incorporating the possible measurement errors into our model we get SK generation protocols that are robust against these errors. Good system performance has to be guaranteed for all possible source statistics.

The scenario for SK generation from a PUF source is depicted in Figure 3.2. So for the model for SK generation from a compound PUF source we replace the PUF source by a compound PUF source. This means we consider the RVs $\{X_s Y_s\}_{s\in\mathcal{S}}$ and the random vectors $\{X_s^n Y_s^n\}_{s\in\mathcal{S}}$ with $P_{X_s^n Y_s^n} = P_{X_s Y_s}^{\otimes n}$ for all $s \in \mathcal{S}$. X_s^n and Y_s^n represent the source output observed at terminal $\mathcal{X}$ and terminal $\mathcal{Y}$ respectively when the actual

source statistics are determined by the parameter $s \in \mathcal{S}$. Correspondingly the RVs (K_s, M_s) model the SK and the helper message and $\hat{K}_s$ represents the reconstruction of the SK. Again we consider a randomized encoder $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n)$ and a decoder $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$. In the context of SK generation from a compound PUF source we call (F, g) a compound SK generation protocol. Thus we get the joint distributions of the RVs $K_s M_s \hat{K}_s$

$$P_{K_s M_s \hat{K}_s}(k, m, \hat{k}) = \sum_{x^n, y^n \in \mathcal{X}^n \times \mathcal{Y}^n} P_{X_s Y_s}^{\otimes n}(x^n, y^n) F(k, m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, m)$$

for all $(k, m, \hat{k}) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K}$ and $s \in \mathcal{S}$.

We also define the set

$$\mathcal{I}(\hat{s}) = \{s \in \mathcal{S}\colon \sum_{y \in \mathcal{Y}} P_{X_s Y_s}(x, y) = P_{X_{\hat{s}}}(x) \text{ for all } x \in \mathcal{X}\}$$

for $\hat{s} \in \mathcal{S}$. We choose an arbitrary set of representatives corresponding to the equivalence relation $\sim \subset \mathcal{S} \times \mathcal{S}$ defined by this partition of $\mathcal{S}$ and denote it by $\hat{\mathcal{S}}$. Additionally we define $f_{\hat{\mathcal{S}}}\colon \mathcal{S} \to \mathcal{S}$, $f_{\hat{\mathcal{S}}}(s) = \hat{s}$ if and only if $s \sim \hat{s}$ for all $s \in \mathcal{S}$, $\hat{s} \in \hat{\mathcal{S}}$. For the RVs $\{X_{\hat{s}}\}_{\hat{s} \in \hat{\mathcal{S}}}$ we now define $P_{Y_s|X_{f_{\hat{\mathcal{S}}}(s)}} = P_{Y_s|X_s}$ (for $s \neq f_{\hat{\mathcal{S}}}(s)$). Thus it holds that $P_{X_s Y_s} = P_{X_{f_{\hat{\mathcal{S}}}(s)} Y_s}$ for all $s \in \mathcal{S}$.

In the following we assume that $|\hat{\mathcal{S}}| < \infty$.

A compound SK generation protocol should have certain properties despite the source uncertainty. These properties are determined by the following definition.

Definition 3.2. *A tuple (R, L), $R, L \geqslant 0$, is an achievable SK generation/privacy leakage rate pair if for all $\delta > 0$ there is an $n_0 \in \mathbb{N}$ and a $c > 0$ such that for all $n \geqslant n_0$ there is a compound SK generation protocol (F, g) such that*

$$\begin{aligned}
&\sup_{s \in \mathcal{S}} Pr(K_s \neq \hat{K}_s) \leqslant \exp(-nc)\\
&\sup_{s \in \mathcal{S}} I(K_s \wedge M_s) = 0\\
&\inf_{s \in \mathcal{S}} H(K_s) = \log|\mathcal{K}|\\
&\tfrac{1}{n} \log|\mathcal{K}| \geqslant R - \delta\\
&\sup_{s \in \mathcal{S}} \tfrac{1}{n} I(M_s \wedge X_s^n) \leqslant L + \delta.
\end{aligned}$$

We call the set of all such achievable rate pairs the capacity region $\mathcal{R}_{SK}^{PL,comp}$.

So for the compound model we also want to control the privacy leakage rate of the protocols and we require perfect secrecy and uniform key distribution.

In the following we want to characterize $\mathcal{R}_{SK}^{PL,comp}$.

Theorem 3.3. *It holds that*

$$\mathcal{R}_{SK}^{PL,comp} \supseteq \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \bigcup_{U_{\hat{s}}} \{(R,L)\colon 0 \leqslant R \leqslant \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s), \\ L \geqslant I(U_{\hat{s}} \wedge X_{\hat{s}}) - \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s)\}$$

where for all $\hat{s} \in \hat{\mathcal{S}}$ the union is taken over all RVs $U_{\hat{s}}$ with $U_{\hat{s}} - X_{\hat{s}} - Y_s$ for all $s \in \mathcal{I}(\hat{s})$.

Again the proof technique is based on [5, Proof of Proposition 1a)].

Proof. Let $\delta > 0$. Choose $\eta > 0$ and $c > 0$ small enough. Choose RVs $\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}$ such that $U_{\hat{s}} - X_{\hat{s}} - Y_s$ for all $s \in \mathcal{I}(\hat{s})$. For all n large enough construct the sets $\mathcal{J}_{\hat{s}} = \{u_{k,m}\}_{(k,m)\in\mathcal{K}_{\hat{s}}\times\mathcal{M}_{\hat{s}}}$ with $u_{k,m} \in \mathcal{U}^n$ for all $\hat{s} \in \hat{\mathcal{S}}$,

$$|\mathcal{K}_{\hat{s}}| = \exp(n(\inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s) - \delta - \xi_{\hat{s}})) \tag{3.3}$$

with $0 \leqslant \xi_{\hat{s}} \leqslant \frac{1}{n}$ such that the $n(\inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s) - \delta - \xi_{\hat{s}})$ are integers and disjoint sets $\mathcal{M}_{\hat{s}}$, $\hat{s} \in \hat{\mathcal{S}}$. Moreover for $\mathcal{J}_{\hat{s}}$ it should hold that

$$P_{U_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}) > 1 - \exp(-n\eta)(n+1)^{|\mathcal{U}|}$$

and for all $m \in \mathcal{M}_{\hat{s}}$ there is a $g_m\colon \mathcal{Y}^n \to \mathcal{K}$ such that

$$\inf_{s\in\mathcal{I}(\hat{s})} P_{Y_s|U_{\hat{s}}}^{\otimes n}((g_m)^{-1}(k)|u_{k,m}) \geqslant 1 - \exp(-nc) \tag{3.4}$$

for all $k \in \mathcal{K}_{\hat{s}}$ and for all $m \in \mathcal{M}_{\hat{s}}$ there is a $P \in \mathcal{P}(n,\mathcal{U})$ such that for all $k \in \mathcal{K}_{\hat{s}}$ it holds that $u_{k,m} \in \mathcal{T}_P^n$. Additionally we define $\mathcal{M} = \bigcup_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{M}_{\hat{s}}$.

We choose for all $\hat{s} \in \hat{\mathcal{S}}$ the set $\mathcal{J}_{\hat{s}}$ as follows. At first choose a $P \in \mathcal{P}(n,\mathcal{U})$. Then choose an arbitrary set $\mathcal{A}_{(1,\hat{s})} \subset \mathcal{T}_P^n$ with $P_{U_{\hat{s}}}^{\otimes n}(\mathcal{A}_{(1,\hat{s})}) \geqslant \exp(-n\eta)$. For η small enough and all n large enough we can choose a compound channel code for the compound channel $\{P_{Y_s|U_{\hat{s}}}\}_{s\in\mathcal{I}(\hat{s})}$ corresponding to $(u_{k,(1,\hat{s})}, (g_{(1,\hat{s})})^{-1}(k))_{k\in\mathcal{K}_{\hat{s}}}$ such that (3.4) and (3.3) hold true with $\{u_{k,(1,\hat{s})}\}_{k\in\mathcal{K}_{\hat{s}}} \subset \mathcal{A}_{(1,\hat{s})}$. This follows from Theorem 2.25. In the i-th step choose $\mathcal{A}_{(i,\hat{s})} \subset \mathcal{T}_P^n \backslash \bigcup_{j\in[i-1]} \{u_{k,(j,\hat{s})}\}_{k\in\mathcal{K}_{\hat{s}}}$ with $P_{U_{\hat{s}}}^{\otimes n}(\mathcal{A}_{(i,\hat{s})}) \geqslant \exp(-n\eta)$. If this is not possible anymore (that is this choice of $\mathcal{A}_{(i,\hat{s})}$) repeat this procedure for all $P \in \mathcal{P}(n,\mathcal{U})$. So at the end of the procedure it holds that $P_{U_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}) > 1 - \exp(-n\eta)(n+1)^{|\mathcal{U}|}$.

Moreover we define $\mathcal{K} = [\min_{\hat{s}\in\hat{\mathcal{S}}} |\mathcal{K}_{\hat{s}}|]$ and for all $\hat{s} \in \hat{\mathcal{S}}$ mappings $h_{\hat{s}}\colon \mathcal{K}_{\hat{s}} \to \mathcal{K} \cup \{\tilde{k}\}$ with $\tilde{k} \notin \mathcal{K}$ such that for all $k \in \mathcal{K}$ it holds that $|h_{\hat{s}}^{-1}(k)| = \lfloor \frac{|\mathcal{K}_{\hat{s}}|}{|\mathcal{K}|} \rfloor$. Thus it holds for $|\mathcal{K}_{\hat{s}}| > |\mathcal{K}|$ that $|h_{\hat{s}}^{-1}(\tilde{k})| < |\mathcal{K}|$ and $|h_{\hat{s}}^{-1}(\tilde{k})| = 0$ for $|\mathcal{K}_{\hat{s}}| = |\mathcal{K}|$.

We have

$$\sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k\in\mathcal{K}_{\hat{s}}} P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) \leqslant 1.$$

Moreover, for all $k, \bar{k} \in \mathcal{K}_{\hat{s}}$, $k \neq \bar{k}$, there is a permutation π on $\mathcal{X}^n$ such that $u_{k,m} = \pi(u_{\bar{k},m})$. Thus we have

$$P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) = P_{U_{\hat{s}}}^{\otimes n}(\pi(u_{\bar{k},m})) = P_{U_{\hat{s}}}^{\otimes n}(u_{\bar{k},m})$$

which follows from the product structure of $P_{U_{\hat{s}}}^{\otimes n}$. So it holds that

$$\sum_{k \in \mathcal{K}_{\hat{s}}} P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) = |\mathcal{K}_{\hat{s}}| P_{U_{\hat{s}}}^{\otimes n}(u_{k,m})$$

for an arbitrary $k \in \mathcal{K}_{\hat{s}}$. Thus we have

$$\sum_{m \in \mathcal{M}_{\hat{s}}} P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) \leqslant \tfrac{1}{|\mathcal{K}_{\hat{s}}|}.$$

Now we have the bound

$$\sum_{m \in \mathcal{M}_{\hat{s}}} \sum_{k \in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) = \sum_{k \in h_{\hat{s}}^{-1}(\tilde{k})} \sum_{m \in \mathcal{M}_{\hat{s}}} P_{U_{\hat{s}}}^{\otimes n}(u_{k,m}) \leqslant \tfrac{1}{|\mathcal{K}_{\hat{s}}|} |h_{\hat{s}}^{-1}(\tilde{k})|.$$

If $|\mathcal{K}| < |\mathcal{K}_{\hat{s}}|$ we can upper bound this expression by

$$\tfrac{|\mathcal{K}|}{|\mathcal{K}_{\hat{s}}|} \leqslant \exp(-n(\inf_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s) - \xi_{\hat{s}} - \min_{\hat{s} \in \hat{\mathcal{S}}} \inf_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s))) < \exp(-n(2\epsilon - \xi_{\hat{s}}))$$

with $\epsilon > 0$ and thus for all n large enough we have the upper bound $\exp(-n\epsilon)$. If $|\mathcal{K}| = |\mathcal{K}_{\hat{s}}|$ we have 0 as an upper bound.

(Additionally define $h\colon \mathcal{K} \cup \{\tilde{k}\} \to \mathcal{K}$, $h(k) = k$ for $k \in \mathcal{K}$ and $h(\tilde{k}) = k$ for an arbitrary $k \in \mathcal{K}$ and $\hat{s}\colon \mathcal{M} \to \hat{\mathcal{S}}$, $\hat{s}(m) = \hat{s}$ for $m \in \mathcal{M}_{\hat{s}}$.)

Consider RVs $\{K'_s\}_{s \in \mathcal{S}}$, $\{M'_s\}_{s \in \mathcal{S}}$ and $\{\hat{K}'_s\}_{s \in \mathcal{S}}$ with $P_{K'_s M'_s \hat{K}'_s} \in \mathcal{P}(\mathcal{K}_{f_{\hat{\mathcal{S}}}(s)} \times \mathcal{M}_{f_{\hat{\mathcal{S}}}(s)} \times \mathcal{K}_{f_{\hat{\mathcal{S}}}(s)})$ and

$$P_{K'_s M'_s \hat{K}'_s X_s^n Y_s^n}(k, m, \hat{k}, x^n, y^n) = P_{X_s Y_s}^{\otimes n}(x^n, y^n) F_{f_{\hat{\mathcal{S}}}(s)}(k, m|x^n) \mathbb{1}_{g_{f_{\hat{\mathcal{S}}}(s)}^{-1}(\hat{k})}(y^n, m)$$

where for all $(k, m, x^n, y^n) \in \mathcal{K}_{\hat{s}} \times \mathcal{M}_{\hat{s}} \times \mathcal{X}^n \times \mathcal{Y}^n$ it holds that

$$\begin{aligned} F_{\hat{s}}(k, m|x^n) &= P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k,m}|x^n) + P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \tfrac{1}{|\mathcal{M}_{\hat{s}}||\mathcal{K}_{\hat{s}}|} \\ g_{\hat{s}}(y^n, m) &= g_m(y^n). \end{aligned}$$

Using the same argumentation as in the proof of Theorem 3.1 we can show that the following properties hold for these RVs. (In order to show this we use the properties of the sets $\mathcal{J}_{\hat{s}}$.) For all $s \in \mathcal{S}$ it holds for all n large enough that

$$\Pr(K'_s \neq \hat{K}'_s) \leqslant \exp(-nc)$$
$$H(K'_s|M'_s) = \log|\mathcal{K}_{f_{\hat{\mathcal{S}}}(s)}|$$
$$\tfrac{1}{n} I(M'_s \wedge X_s^n) \leqslant I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge X_{f_{\hat{\mathcal{S}}}(s)}) - \inf_{\bar{s}\in\mathcal{I}(f_{\hat{\mathcal{S}}}(s))} I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{\bar{s}}) + \delta.$$

Now define (F, g) as follows. (For δ small enough such that the sets $\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}$ are disjoint for all $\hat{s} \in \hat{\mathcal{S}}$.)

$$F(k,m|x^n) = \sum_{\hat{s}\in\hat{\mathcal{S}}} \Big(\sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} F_{\hat{s}}(k_{\hat{s}}, m|x^n) + \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} F_{\hat{s}}(k_{\hat{s}}, m|x^n) \tfrac{1}{|\mathcal{K}|} \Big) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)$$
$$+ \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n)$$

which is equivalent to

$$F(k,m|x^n) = \sum_{\hat{s}\in\hat{\mathcal{S}}} \Big(\sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n) + \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n) \tfrac{1}{|\mathcal{K}|}$$
$$+ P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|} \Big) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) + \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n)$$

and

$$g(y^n, m) = h(h_{\hat{s}(m)}(g_m(y^n)))$$

Now consider for $s \in \mathcal{S}$ the mapping $q_s \colon \mathcal{M}_{f_{\hat{\mathcal{S}}}(s)} \to \mathcal{M}$, $q_s(m) = m$. This mapping is injective so we have $I(M'_s \wedge X_s^n) = I(q_s(M'_s) \wedge X_s^n)$. It is clear that for all $s \in \mathcal{S}$

$$\begin{aligned}\|P_{M_s X_s^n} - P_{q_s(M'_s)X_s^n}\|_1 &\leqslant \sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \|P_{M_s|X_s^n}(\cdot|x^n) - P_{q_s(M'_s)|X_s^n}(\cdot|x^n)\|_1 \\ &\qquad + 2(n+1)^{|\mathcal{X}|} \exp(-n\tfrac{1}{2\ln 2}\delta^2) \\ &= 2(n+1)^{|\mathcal{X}|} \exp(-n\tfrac{1}{2\ln 2}\delta^2).\end{aligned}$$

So for all n large enough we have

$$\begin{aligned}&\tfrac{1}{n} I(M_s \wedge X_s^n) \leqslant \tfrac{1}{n} I(q_s(M'_s) \wedge X_s^n) + \epsilon = \tfrac{1}{n} I(M'_s \wedge X_s^n) + \epsilon \\ &\leqslant I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge X_{f_{\hat{\mathcal{S}}}(s)}) - \inf_{\bar{s}\in\mathcal{I}(f_{\hat{\mathcal{S}}}(s))} I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{\bar{s}}) + \delta + \epsilon\end{aligned}$$

for all $s \in \mathcal{S}$. This implies

$$\tfrac{1}{n} I(M_s \wedge X_s^n) \leqslant \max_{\hat{s}\in\hat{\mathcal{S}}} I(U_{\hat{s}} \wedge X_{\hat{s}}) - \inf_{\bar{s}\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_{\bar{s}}) + \delta + \epsilon.$$

Moreover note that

$$\begin{aligned}((h(h_{\hat{s}(m)}(g_m)))^{-1}(k))^c &= (g_m^{-1}(h_{\hat{s}(m)}^{-1}(h^{-1}(k))))^c \\ &= (g_m^{-1}(h_{\hat{s}(m)}^{-1}(k)))^c \subset (g_m^{-1}(k_{\hat{s}}))^c\end{aligned}$$

with $k_{\hat{s}} \in h_{\hat{s}(m)}^{-1}(k)$. We have for all $s \in \mathcal{S}$ that

$$\begin{aligned}\Pr(K_s \neq \hat{K}_s) &= \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{(x^n,y^n)\in\mathcal{X}^n\times\mathcal{Y}^n} P_{X_sY_s}^{\otimes n}(x^n,y^n) F(k,m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \\
&\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&+ \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \\
&\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \tfrac{1}{|\mathcal{K}|} \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&+ \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \\
&\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|} \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&+ \sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n\in\mathcal{X}^n\times\mathcal{Y}^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m).\end{aligned}$$

We can rewrite the first summand as

$$\begin{aligned}&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \\
&\qquad \cdot \sum_{k_{\hat{s}}\in h_{f_{\hat{\mathcal{S}}}(s)}^{-1}(k)} P_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&+ \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}^{\otimes n}(x^n,y^n) \\
&\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)\end{aligned}$$

where again we consider both summands separately. At first we have

$$
\begin{aligned}
&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
\leqslant &\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k\in\mathcal{K}} \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} \sum_{y^n\in\mathcal{Y}^n} \sum_{\substack{\hat{k}\in\mathcal{K}:\\ \hat{k}\neq k}} \sum_{x^n\in\mathcal{X}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
= &\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k\in\mathcal{K}} \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}) \\
&\qquad\qquad \cdot \sum_{y^n\in\mathcal{Y}^n} \sum_{\hat{k}\in\mathcal{K}:\ \hat{k}\neq k} P^{\otimes n}_{Y_s|U_{f_{\hat{\mathcal{S}}}(s)}}(y^n|u_{k_{\hat{s}},m})\mathbb{1}_{g_m^{-1}(h^{-1}_{\hat{s}(m)}(h^{-1}(\hat{k})))}(y^n) \\
= &\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k\in\mathcal{K}} \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}) P^{\otimes n}_{Y_s|U_{f_{\hat{\mathcal{S}}}(s)}}((g_m^{-1}(h^{-1}_{\hat{s}(m)}(h^{-1}(k))))^c|u_{k_{\hat{s}},m}) \\
\leqslant &\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k\in\mathcal{K}} \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}) P^{\otimes n}_{Y_s|U_{f_{\hat{\mathcal{S}}}(s)}}((g_m^{-1}(k_{\hat{s}})))^c|u_{k_{\hat{s}},m}) \\
\leqslant &\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k\in\mathcal{K}} \sum_{k_{\hat{s}}\in h^{-1}_{f_{\hat{\mathcal{S}}}(s)}(k)} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m})\exp(-nc) \leqslant \exp(-nc).
\end{aligned}
$$

Furthermore it holds that

$$\begin{aligned}
&\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{k\in\mathcal{K}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&\leqslant \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{k_{\hat{s}}\in\mathcal{K}_{\hat{s}}} \sum_{m\in\mathcal{M}_{\hat{s}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&\leqslant \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \leqslant (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2),
\end{aligned}$$

where the first step follows as $\sum_{\substack{\hat{k}\in\mathcal{K}:\\ \hat{k}\neq k}} \mathbb{1}_{g_m^{-1}(\hat{k})}(y^n) \leqslant 1$ for all $k\in\mathcal{K}$ and the second to last step follows because the $\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}$, $\hat{s}\in\hat{\mathcal{S}}$, are disjoint.

Now we consider the second summand, that is

$$\begin{aligned}
&\sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&= \sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&+ \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m).
\end{aligned}$$

Again we consider the summands separately. So starting with the first summand we

have

$$\begin{aligned}
&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{x^n\in\mathcal{X}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}|x^n) \\
&= \sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(u_{k_{\hat{s}},m}) \leqslant \exp(-n\epsilon),
\end{aligned}$$

where the last step follows as described above. Furthermore it holds that

$$\begin{aligned}
&\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{k\in\mathcal{K}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\tfrac{1}{|\mathcal{K}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&= \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\tilde{k})} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&\leqslant \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \leqslant (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2).
\end{aligned}$$

For the third summand we have

$$\begin{aligned}
&\sum_{m\in\mathcal{M}}\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}}\sum_{x^n,y^n\in\mathcal{X}^n\times\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\\
&\qquad\cdot\sum_{\hat{s}\in\hat{\mathcal{S}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n)\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)\\
=&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}}\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}}\sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}}\sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\\
&\qquad\cdot P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(\mathcal{J}^c_{f_{\hat{\mathcal{S}}}(s)}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}|}\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)\\
+&\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}}\sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}}\sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\\
&\qquad\cdot\sum_{\hat{s}\in\hat{\mathcal{S}}}\sum_{m\in\mathcal{M}_{\hat{s}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)
\end{aligned}$$

and again we consider both summands separately. At first we again have

$$\begin{aligned}
&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}}\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}}\sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}}\sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\\
&\qquad\cdot P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(\mathcal{J}^c_{f_{\hat{\mathcal{S}}}(s)}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}|}\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m)\\
\leqslant&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}}\sum_{k\in\mathcal{K}}\sum_{x^n\in\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}}\sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\\
&\qquad\cdot P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(\mathcal{J}^c_{f_{\hat{\mathcal{S}}}(s)}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}|}
\end{aligned}$$

which we upper bound by

$$\begin{aligned}
&\sum_{m\in\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}}\sum_{k\in\mathcal{K}}\sum_{x^n\in\mathcal{X}^n}\sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}|X_{f_{\hat{\mathcal{S}}}(s)}}(\mathcal{J}^c_{f_{\hat{\mathcal{S}}}(s)}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{f_{\hat{\mathcal{S}}}(s)}|}\\
&= P^{\otimes n}_{U_{f_{\hat{\mathcal{S}}}(s)}}(\mathcal{J}^c_{f_{\hat{\mathcal{S}}}(s)}) \leqslant (n+1)^{|\mathcal{U}|}\exp(-\eta n).
\end{aligned}$$

Additionally it holds that

$$\begin{aligned}
&\sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{k\in\mathcal{K}} \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n) \\
&\qquad\qquad \cdot \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{m\in\mathcal{M}_{\hat{s}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|}\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&= \sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \sum_{\hat{s}\in\hat{\mathcal{S}}} P^{\otimes n}_{U_{\hat{s}}|X_{\hat{s}}}(\mathcal{J}^c_{\hat{s}}|x^n)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)
\end{aligned}$$

and as the $\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}$, $\hat{s}\in\hat{\mathcal{S}}$, are disjoint we can upper bound this expression by

$$\sum_{x^n\notin\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta}} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n) \leqslant (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2).$$

For the fourth summand we have

$$\begin{aligned}
&\sum_{m\in\mathcal{M}} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{x^n,y^n\in\mathcal{X}^n\times\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|}\mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}}\mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,m) \\
&\leqslant \sum_{m\in\mathcal{M}} \sum_{k\in\mathcal{K}} \sum_{x^n,y^n\in\mathcal{X}^n\times\mathcal{Y}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}Y_s}(x^n,y^n)\tfrac{1}{|\mathcal{K}||\mathcal{M}|}\mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}}\mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n) \\
&= \sum_{x^n\in\mathcal{X}^n} P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}(x^n)\mathbb{1}_{(\bigcup_{\hat{s}\in\hat{\mathcal{S}}}\mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n) \leqslant P^{\otimes n}_{X_{f_{\hat{\mathcal{S}}}(s)}}((\mathcal{T}^n_{P_{X_{f_{\hat{\mathcal{S}}}(s)}},\delta})^c) \\
&\leqslant (n+1)^{|\mathcal{X}|}\exp(-n\tfrac{1}{2\ln 2}\delta^2).
\end{aligned}$$

So for n large enough we upper bounded all four summands by $\exp(-nd)$ for a $d>0$ and thus the sum by $\exp(-nb)$ for a $b>0$. Thus we have

$$\sup_{s\in\mathcal{S}} \Pr(K_s\neq\hat{K}_s) \leqslant \exp(-nb),$$

because $\exp(-nb)$ is an upper bound. Now consider

$$\begin{aligned}
&\Pr(K_s = k, M_s = m) = \sum_{\hat{k}} \sum_{x^n, y^n} P_{X_s Y_s}^{\otimes n}(x^n, y^n) F(k, m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, m) \\
&= \sum_{x^n} P_{X_s}^{\otimes n}(x^n) \Big(\sum_{\hat{s} \in \hat{\mathcal{S}}} \Big(\sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) + \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \tfrac{1}{|\mathcal{K}|} \\
&+ P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|} \Big) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) + \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s} \in \hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n) \Big) \\
&= \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \tfrac{1}{|\mathcal{K}|} \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|} \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s} \in \hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n).
\end{aligned}$$

and

$$\begin{aligned}
&\Pr(M_s = m) \\
&= \sum_{k \in \mathcal{K}} \sum_{x^n} P_{X_s}^{\otimes n}(x^n) \Big(\sum_{\hat{s} \in \hat{\mathcal{S}}} \Big(\sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) + \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \tfrac{1}{|\mathcal{K}|} \\
&+ P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \tfrac{1}{|\mathcal{K}||\mathcal{M}_{\hat{s}}|} \Big) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) + \tfrac{1}{|\mathcal{K}||\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s} \in \hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n) \Big) \\
&= \sum_{k \in \mathcal{K}} \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(\tilde{k})} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\mathcal{J}_{\hat{s}}^c|x^n) \tfrac{1}{|\mathcal{M}_{\hat{s}}|} \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&+ \sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \tfrac{1}{|\mathcal{M}|} \mathbb{1}_{(\bigcup_{\hat{s} \in \hat{\mathcal{S}}} \mathcal{T}^n_{P_{X_{\hat{s}}},\delta})^c}(x^n).
\end{aligned}$$

Consider permutations $\{\pi_{k_{\hat{s}}}\}_{k_{\hat{s}} \in \mathcal{K}_{\hat{s}}}$ on $[n]$ (and we denote by $\pi_{k_{\hat{s}}}$ the corresponding permutation on e.g. $\mathcal{X}^n$). As $\pi_{k_{\hat{s}}}^{-1}(\mathcal{X}^n) = \mathcal{X}^n$, it holds that

$$\begin{aligned}
&\sum_{x^n \in \mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n) \\
&= \sum_{k_{\hat{s}} \in h_{\hat{s}}^{-1}(k)} \sum_{x^n \in \pi_{k_{\hat{s}}}^{-1}(\mathcal{X}^n)} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s} \in \hat{\mathcal{S}}} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n) \mathbb{1}_{\mathcal{M}_{\hat{s}}}(m) \mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n).
\end{aligned}$$

Given the product structure of $P_{X_s}^{\otimes n}$ and $P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}$ (and as $\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)$ is invariant to permutations of x^n) this expression equals

$$\sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} \sum_{x^n\in\pi_{k_{\hat{s}}}^{-1}(\mathcal{X}^n)} P_{X_s}^{\otimes n}(\pi_{k_{\hat{s}}}(x^n)) \sum_{\hat{s}\in\hat{\mathcal{S}}} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\pi_{k_{\hat{s}}}(u_{k_{\hat{s}},m})|\pi_{k_{\hat{s}}}(x^n))\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(\pi_{k_{\hat{s}}}(x^n))$$
$$= \sum_{\bar{x}\in\mathcal{X}^n} P_{X_s}^{\otimes n}(\bar{x}^n) \sum_{\hat{s}\in\hat{\mathcal{S}}} \sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(\pi_{k_{\hat{s}}}(u_{k_{\hat{s}},m})|\bar{x}^n)\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(\bar{x}^n).$$

According to our construction there is a $P\in\mathcal{P}(n,\mathcal{U})$ such that $u_{k_{\hat{s}},m}\in\mathcal{T}_P^n$ for all $k_{\hat{s}}\in\mathcal{K}_{\hat{s}}$. So for all $\bar{k}\in\mathcal{K}$ we can choose the permutations $\{\pi_{k_{\hat{s}}}\}_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\bar{k})}$ such that $\{\pi_{k_{\hat{s}}}(u_{k_{\hat{s}},m})\}_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(\bar{k})} = \{u_{k_{\hat{s}},m}\}_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)}$ for an arbitrary $k\in\mathcal{K}$. Thus it holds that

$$\sum_{k\in\mathcal{K}}\sum_{x^n\in\mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s}\in\hat{\mathcal{S}}}\sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)$$
$$= |\mathcal{K}| \sum_{x^n\in\mathcal{X}^n} P_{X_s}^{\otimes n}(x^n) \sum_{\hat{s}\in\hat{\mathcal{S}}}\sum_{k_{\hat{s}}\in h_{\hat{s}}^{-1}(k)} P_{U_{\hat{s}}|X_{\hat{s}}}^{\otimes n}(u_{k_{\hat{s}},m}|x^n)\mathbb{1}_{\mathcal{M}_{\hat{s}}}(m)\mathbb{1}_{\mathcal{T}^n_{P_{X_{\hat{s}}},\delta}}(x^n)$$

for an arbitrary $k\in\mathcal{K}$. So we have

$$\Pr(K_s=k|M_s=m) = \tfrac{\Pr(K_s=k,M_s=m)}{\Pr(M_s=m)} = \tfrac{1}{|\mathcal{K}|}$$

which means $H(K_s|M_s)=\log|\mathcal{K}|$ for all $s\in\mathcal{S}$ and accordingly

$$\inf_{s\in\mathcal{S}} H(K_s|M_s) = \log|\mathcal{K}|.$$

So we showed that

$$\mathcal{R}_{SK}^{comp} \supseteq \bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}} \{(R,L)\colon 0\leqslant R\leqslant \min_{\hat{s}\in\hat{\mathcal{S}}}\inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}}\wedge Y_s),$$
$$L\geqslant \max_{\hat{s}\in\hat{\mathcal{S}}} I(U_{\hat{s}}\wedge X_{\hat{s}}) - \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}}\wedge Y_s)\}$$
$$= \bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}})$$

where we define

$$\mathcal{R}_{\hat{s}}(U_{\hat{s}}) = \{(R,L)\colon 0\leqslant R\leqslant \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}}\wedge Y_s), L\geqslant I(U_{\hat{s}}\wedge X_{\hat{s}}) - \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}}\wedge Y_s)\}.$$

It holds that

$$\bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}) = \bigcup_{U_{\hat{s}_1}} \bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}}} \Big(\bigcap_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}) \cap \mathcal{R}_{\hat{s}_1}(U_{\hat{s}_1})\Big).$$

Now we apply the distributive law two times, so

$$\begin{aligned}
&\bigcup_{U_{\hat{s}_1}} \bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}}} \Big(\bigcap_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}) \cap \mathcal{R}_{\hat{s}_1}(U_{\hat{s}_1})\Big) \\
&= \bigcup_{U_{\hat{s}_1}} \Big(\Big(\bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}} \mathcal{R}_{\hat{s}}(U_{\hat{s}})\Big) \cap \mathcal{R}_{\hat{s}_1}(U_{\hat{s}_1})\Big) \\
&= \Big(\bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}\setminus\{\hat{s}_1\}} \mathcal{R}_{\hat{s}}(U_{\hat{s}})\Big) \cap \Big(\bigcup_{U_{\hat{s}_1}} \mathcal{R}_{\hat{s}_1}(U_{\hat{s}_1})\Big).
\end{aligned}$$

If we repeat these steps for all $\hat{s} \in \hat{\mathcal{S}}$ we arrive at

$$\bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}) = \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \bigcup_{U_{\hat{s}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}).$$

■

Now consider the converse.

Theorem 3.4. *It holds that*

$$\begin{aligned}
\mathcal{R}_{SK}^{comp,PL} \subseteq \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \bigcup_{U_{\hat{s}}} \{(R,L)\colon 0 \leqslant R \leqslant \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s), \\
L \geqslant I(U_{\hat{s}} \wedge X_{\hat{s}}) - \inf_{s\in\mathcal{I}(\hat{s})} I(U_{\hat{s}} \wedge Y_s)\}
\end{aligned}$$

where for all $\hat{s} \in \hat{\mathcal{S}}$ the union is taken over all RVs $U_{\hat{s}}$ with $U_{\hat{s}} - X_{\hat{s}} - Y_s$ for all $s \in \mathcal{I}(\hat{s})$.

Proof. Using the same steps as in the proof of Theorem 3.2 we can show that for $\delta > 0$ and RVs $\{U_s\}_{s\in\mathcal{S}}$ with $U_s = QU_{s,Q}$, where $U_{s,i} = K_s M_s X_s^{i-1}$ and Q uniformly distributed on $[n]$ and independent of $\{X_s^n Y_s^n U_s^n\}_{s\in\mathcal{S}}$, it holds that

$$P_{U_s X_{s,Q} Y_{s,Q}}((q,u),x,y) = P_Q(q) P_{U_{s,q}|X_{s,q}}(u|x) P_{X_s Y_s}(x,y)$$

for all $s \in \mathcal{S}$,

$$\tfrac{1}{n} \log |\mathcal{K}| \leqslant I(U_s \wedge Y_{s,Q}) + \delta$$

and

$$\tfrac{1}{n} I(M_s \wedge X_s^n) \geqslant I(U_s \wedge X_{s,Q}) - I(U_s \wedge Y_{s,Q}) - \delta.$$

It holds that

$$\begin{aligned}
&P_{U_s X_{s,Q}}((q,u),x) = P_Q(q) P_{U_{s,q} X_{s,q}}(u,x) \\
&= P_{K_s M_s X_s^{q-1} X_{s,q}}(u,x) P_Q(q) = P_{K_s M_s X_s^{q-1} X_{s,q}}((k,m,x^{q-1}),x) P_Q(q) \\
&= P_Q(q) \sum_{x_{q+1}^n \in \mathcal{X}^{n-q}} P_{X_{f_{\hat{\mathcal{S}}}(s)}}^{\otimes n}((x^{q-1},x,x_{q+1}^n)) F(k,m|(x^{q-1},x,x_{q+1}^n)),
\end{aligned}$$

which only depends on s via $f_{\hat{\mathcal{S}}}(s)$. (We introduce $u = (k, m, x^{q-1})$ above to access the components of u.) Correspondingly we can consider the RVs $\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}$ and define for $s \neq f_{\hat{S}}(s)$

$$P_{Y_{s,Q}|U_{f_{\hat{\mathcal{S}}}(s)}X_{f_{\hat{\mathcal{S}}}(s),Q}} = P_{Y_{s,Q}|U_sX_{s,Q}}.$$

Then it holds that $P_{U_{f_{\hat{\mathcal{S}}}(s)}X_{f_{\hat{\mathcal{S}}}(s),Q}Y_{s,Q}} = P_{U_sX_{s,Q}Y_{s,Q}}$ for all $s \in \mathcal{S}$ and $U_{f_{\hat{\mathcal{S}}}(s)} - X_{f_{\hat{\mathcal{S}}}(s),Q} - Y_{s,Q}$. Additionally we have for all $s \in \mathcal{S}$

$$\tfrac{1}{n}\log|\mathcal{K}| \leqslant I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{s,Q}) + \delta$$

and

$$\sup_{s\in\mathcal{S}} \tfrac{1}{n} I(M_s \wedge X_s^n) \geqslant I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge X_{f_{\hat{\mathcal{S}}}(s),Q}) - I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{s,Q}) - \delta.$$

So

$$\begin{aligned}
&\tfrac{1}{n}\log|\mathcal{K}| \leqslant \inf_{s\in\mathcal{S}} I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{s,Q}) + \delta \\
&= \inf_{\substack{(s,\hat{s})\in\mathcal{S}\times\hat{\mathcal{S}}:\\ \hat{s}=f_{\hat{\mathcal{S}}}(s)}} I(U_{\hat{s}} \wedge Y_{s,Q}) + \delta = \min_{\hat{s}\in\hat{\mathcal{S}}} \inf_{s\in\mathcal{J}(\hat{s})} I(U_{\hat{s}} \wedge Y_{s,Q}) + \delta
\end{aligned}$$

and

$$\begin{aligned}
\sup_{s\in\mathcal{S}} \tfrac{1}{n} I(M_s \wedge X_s^n) &\geqslant \sup_{s\in\mathcal{S}} I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge X_{f_{\hat{\mathcal{S}}}(s),Q}) - I(U_{f_{\hat{\mathcal{S}}}(s)} \wedge Y_{s,Q}) - \delta \\
&= \max_{\hat{s}\in\hat{\mathcal{S}}} I(U_{\hat{s}} \wedge X_{\hat{s},Q}) - \inf_{s\in\mathcal{J}(\hat{s})} I(U_{\hat{s}} \wedge Y_{s,Q}) - \delta.
\end{aligned}$$

This implies

$$\mathcal{R}_{SK}^{comp} \subseteq \bigcup_{\{U_{\hat{s}}\}_{\hat{s}\in\hat{\mathcal{S}}}} \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}) = \bigcap_{\hat{s}\in\hat{\mathcal{S}}} \bigcup_{U_{\hat{s}}} \mathcal{R}_{\hat{s}}(U_{\hat{s}}).$$

■

3.3 SK generation from a jammed PUF source

In information theoretic security a very basic channel model is the wiretap channel introduced in [49]. In this scenario we assume that additionally to a legitimate receiver there is an eavesdropper. A sender wants to send a message reliably to the legitimate receiver. The eavesdropper gets the messages from the sender via a channel different from the channel to the legitimate receiver. Nevertheless the eavesdropper should not be able to decode the message correctly from his received signal. One problem of this model is that we assume perfect knowledge of the channel to the eavesdropper, which obviously is an unrealistic assumption. We can improve the model by considering channel uncertainty [44]. Accordingly in [16, 35] the authors consider the compound wiretap

channel to account for the channel uncertainty. This means we assume that the channels the model comprises are not known perfectly. Instead, for each channel we know a set of channels the actual channel belongs to. This channel is used for the whole duration of transmission which means for all channel uses. In [15, 39] the authors consider the arbitrarily varying wiretap channel. This is a different way to model channel uncertainty. Again we do not know the channels in the model but a set of channels to the legitimate receiver and the eavesdropper respectively. For each channel use the actual channels are elements of the corresponding sets. So the channels do not necessarily remain constant during the whole duration of transmission. These models also allow for modeling an active attacker who jams the communication.

The standard scenario for SK generation from a PUF source described in Section 3.1 is very restrictive as it only allows for passive attacks where an eavesdropper who is interested in K gets to know M. If we want to model more powerful attackers we have to expand the standard scenario by considering active attacks. After the first phase the active attacker could try to manipulate the statistics of the PUF source. We call such an active attacker a jammer. In general, incorporating a jammer in models for information theoretic security is natural, as active attacks fit the scenarios considered in this context. As discussed for the wiretap channel, a compound model can be used to model an active attacker. So a compound PUF source can be interpreted as a PUF source that is jammed by an active attacker. It is discussed in [43, Chapter 13] that such a scenario, where an active attacker jams the PUF source is relevant from a practical point of view. An active attacker could for example use electromagnetic waves to jam the PUF. As mentioned in [43, Chapter 13] the active attacker could also tamper with the environmental parameters like temperature to influence the PUF.

So now we look at SK generation from a PUF source where we want to incorporate an active attacker in the model. In our model we allow for very general active attacks. They are more powerful than the jamming attacks modeled by a compound PUF source as we will see later.

From a practical and especially from a cryptanalytic point of view we should assume that the jammer knows the encoder F and the decoder g, i.e. the algorithm for generating K, M and $\hat{K}$. We denote the set of all possible encoding and decoding algorithms by $\mathcal{F}$ and $\mathcal{G}$. Then all functions

$$A\colon \mathcal{F} \times \mathcal{G} \to \mathcal{S}^n$$

are possible jamming strategies, where $A \in \mathrm{Mapp}(\mathcal{F} \times \mathcal{G}, \mathcal{S}^n)$. This scenario is depicted in Figure 3.3. (There is an additional eavesdropper interested in K with access to M.)

The most powerful jamming attack results from a jammer choosing s^n while additionally knowing M. Then all functions

$$B\colon \mathcal{F} \times \mathcal{G} \times \mathcal{M} \to \mathcal{S}^n$$

are possible jamming strategies, where $B \in \mathrm{Mapp}(\mathcal{F} \times \mathcal{G} \times \mathcal{M}, \mathcal{S}^n)$. This scenario is depicted in Figure 3.4. (Again there is an additional eavesdropper interested in K with

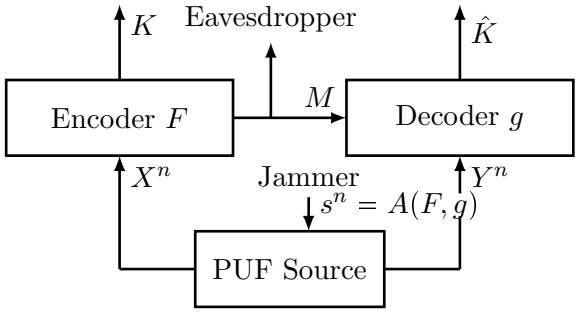

Figure 3.3: SK generation process under jamming attacks where the jammer knows F and g.

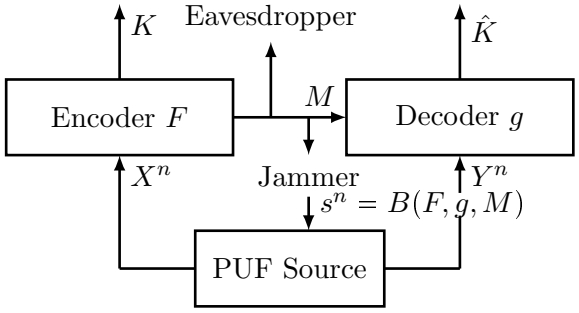

Figure 3.4: SK generation process under jamming attacks where the jammer knows M, F and g.

access to M.)

We will see that (in our model) the knowledge of the jammer has a substantial influence on his potential of preventing a successful SK generation. It turns out that when the jammer knows M in some cases no successful SK generation is possible at all. This is the case when the PUF source has a property that is strongly connected to the property of symmetrizability of AVCs.

Similarly to the model of a compound PUF source we could interpret our model of a jammed PUF source as a model for source uncertainty. This directly makes sense for the case where the jammer does not know M. For the case where the jammer knows M we can still interpret the model as a model for source uncertainty but now the publicly transmitted helper message influences the environment and simultaneously the PUF source. So our models are not restricted to the case where a jammer is present.

For the model for SK generation from a jammed PUF source we consider the RVs X and $\{Y_s\}_{s\in\mathcal{S}}$ with $P_{XY_s}(x,y) = P_X(x)W_s(y|x)$ for all $(x,y) \in \mathcal{X} \times \mathcal{Y}$, $P_X \in \mathcal{P}(\mathcal{X})$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$, i.e. $\{W_s\}_{s\in\mathcal{S}}$ corresponds to an AVC. Consider the random vectors X^n and $Y^n_{s^n}$ with

$$\Pr(X^n Y^n_{s^n}) = (x^n, y^n)) = P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n)$$

for all $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ and $s^n \in \mathcal{S}^n$, where $W_{s^n} = \bigotimes_{i=1}^n W_{s_i}$ for $s^n \in \mathcal{S}^n$. X^n and $Y_{s^n}^n$ represent the source output observed at terminal $\mathcal{X}$ and terminal $\mathcal{Y}$ respectively when the actual source statistics are determined by $s^n \in \mathcal{S}^n$. Correspondingly the RVs (K, M) model the SK and the helper message and $\hat{K}_{s^n}$ represents the reconstruction of the SK. Again we consider a randomized encoder $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n)$ and a decoder $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$. In the context of SK generation from a jammed PUF source we call (F, g) a SK generation protocol. The RVs K and M are generated from X^n using F and the RVs $\hat{K}_{s^n}$ are generated from $Y_{s^n}^n$ and M using g for all $s^n \in \mathcal{S}^n$.

Thus we get the joint distributions of the RVs $KM\hat{K}_{s^n}$

$$P_{KM\hat{K}_{s^n}}(k, m, \hat{k}) = \sum_{x^n, y^n \in \mathcal{X}^n \times \mathcal{Y}^n} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F(k, m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, m)$$

for all $(k, m, \hat{k}) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K}$ and $s^n \in \mathcal{S}^n$.

Again we want to specify properties that the SK generation protocols should have. The SK should be reconstructed correctly with high probability in spite of the possible jamming attacks. Again we want to construct protocols that achieve perfect secrecy and uniform distribution of the SK.

This motivates the following definitions of achievability for the source model.

Definition 3.3. *We call the tuple (R, L), $R, L \geqslant 0$, an achievable SK versus privacy leakage rate pair for the source model if for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geqslant n_0$ there is a SK generation protocol such that*

$$\begin{aligned} &\min_{s^n \in \mathcal{S}^n} \mathrm{P}(K = \hat{K}_{s^n}) \geqslant 1 - \delta \\ &H(K) = \log |\mathcal{K}|, \\ &I(M \wedge K) = 0 \\ &\tfrac{1}{n} \log |\mathcal{K}| \geqslant R - \delta, \\ &\tfrac{1}{n} I(M \wedge X^n) \leqslant L + \delta. \end{aligned} \tag{3.5}$$

We call the set of all rate pairs that are achievable using such SK generation protocols the capacity region $\mathcal{R}'_{AVC}$.

Definition 3.4. *We call the tuple (R, L), $R, L \geqslant 0$, an achievable SK versus privacy leakage rate pair for the source model when the jammer knows the helper message if for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geqslant n_0$ there is a SK generation*

protocol such that

$$\sum_{m\in\mathcal{M}} P_M(m) \min_{s^n\in\mathcal{S}^n} \mathrm{P}(K = \hat{K}_{s^n}|M = m) \geqslant 1-\delta \tag{3.6}$$

$$H(K) = \log|\mathcal{K}| \tag{3.7}$$

$$I(M \wedge K) = 0 \tag{3.8}$$

$$\tfrac{1}{n}\log|\mathcal{K}| \geqslant R-\delta,$$

$$\tfrac{1}{n} I(M \wedge X^n) \leqslant L+\delta.$$

We call the set of all rate pairs that are achievable using such SK generation protocols the capacity region $\mathcal{R}_{AVC}$.

We have two definitions of achievability, one for the case where the jammer does not know M, that is Definition 3.3, and one for the case where the jammer has access to M, that is Definition 3.4.

Note that in Definition 3.3 the mapping A does not appear explicitly. It is clear that the reconstructed SK depends on the jamming strategy that is used for the corresponding SK generation protocol (F, g), i.e. $\hat{K} = \hat{K}(A(F, g))$. Thus in the definition of achievability one could expect that (3.5) is replaced by

$$\min_A \Pr(K = \hat{K}(A(F, g))) \geqslant 1-\delta.$$

But this is equivalent to (3.5). Correspondingly in Definition 3.4 the mapping B does not appear explicitly. Here we have $\hat{K} = \hat{K}(B(F, g, \cdot))$ and in the definition of achievability one could expect that (3.6) is replaced by

$$\min_B \Pr(K = \hat{K}(B(F, g, \cdot))) \geqslant 1-\delta,$$

which is equivalent to (3.6).

We are interested in characterizing $\mathcal{R}_{AVC}$ and $\mathcal{R}'_{AVC}$. It is clear that

$$\mathcal{R}_{AVC} \subset \mathcal{R}'_{AVC}. \tag{3.9}$$

Given a jammed PUF source described by RVs X and $\{Y_s\}_{s\in\mathcal{S}}$ as described above we define $\mathcal{R}$ as the set

$$\bigcup_U \{(R, L)\colon R \leqslant \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U, \bar{W}) \\ L \geqslant I(P_X, P_{U|X}) - \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U, \bar{W})\},$$

where the union is over all RVs U such that

$$P_{UXY_s}(u, x, y) = W_s(y|x)P_{U|X}(u|x)P_X(x)$$

for all $(u, x, y) \in \mathcal{U} \times \mathcal{X} \times \mathcal{Y}$, $P_{U|X} \in \mathcal{P}(\mathcal{U}|\mathcal{X})$ and all $s \in \mathcal{S}$ and $\bar{\mathcal{W}} = \text{conv}(\{P_{Y_s|U}\}_{s\in\mathcal{S}})$.

In this work we will prove two central results.

Theorem 3.5. *It holds that* $\mathcal{R}'_{AVC} = \mathcal{R}$.

In the scenario corresponding to Theorem 3.5 the jammer can freely choose the state of the system $s^n \in \mathcal{S}^n$, but he has no knowledge about the helper message. As discussed the jammer knows the protocol, i.e. the encoding and decoding algorithm F and g, because they are assumed to be standardized in our application scenario of a public communication system.

When analyzing $\mathcal{R}$ we see that the presence of the jammer, who is able to suitably choose the system state, has an influence on the capacity region $\mathcal{R}'_{AVC}$.

$\mathcal{R}$ is a single letter characterization of the capacity region $\mathcal{R}'_{AVC}$ which in principle can be computed and analyzed easily. It is interesting that it is not clear if there is such a single letter characterization of the capacity of the compound wiretap channel or the arbitrarily varying wiretap channel [16, 39, 48].

Remark 3.6. *As mentioned before, in [32,33] the authors consider protocols with weaker secrecy requirements. For example in [32] they replace* (3.7) *and* (3.8) *by*

$$\log|\mathcal{K}| - H(K) \leqslant \delta, \qquad \frac{1}{n} I(M \wedge K) \leqslant \delta.$$

We will see that one might show that weakening our secrecy requirements in such a way does not increase the corresponding capacity region. So in this sense we do not pay a prize for requiring perfect secrecy and a uniform distribution of the secret key instead of the weaker requirements.

Now we consider the case where the jammer knows the helper message.

Theorem 3.7. *If the AVC corresponding to* $\{W_s\}_{s\in\mathcal{S}}$ *is symmetrizable then* $\mathcal{R}_{AVC} = \{(R, L) \colon R \leqslant 0, L \geqslant 0\}$. *If the AVC is not symmetrizable then* $\mathcal{R}_{AVC} = \mathcal{R}$.

Thus we get the following corollary.

Corollary 3.8. *It holds that* $\mathcal{R}_{AVC} = \mathcal{R}'_{AVC}$ *if and only if the AVC corresponding to* $\{W_s\}_{s\in\mathcal{S}}$ *is not symmetrizable.*

Theorem 3.5, 3.7 and Corollary 3.8 show the influence of the presence of a jammer with knowledge of the helper message compared to a jammer without this knowledge. We remember that the jammer is absolutely adversarial, i.e. he tries to make SK generation impossible. If the jammer knows the helper message, he can succeed if the channel corresponding to the PUF source is symmetrizable. This means if the corresponding channel is symmetrizable there is a denial of service attack for each possible SK generation protocol (F, g). We will explicitly prove the existence of such denial of service attacks. If the channel is not symmetrizable the jammer has no additional benefit from knowing the helper message, because in this case it holds that $\mathcal{R}_{AVC} = \mathcal{R}'_{AVC}$.

For our considerations we also need the following result which can for example be found in [41].

Lemma 3.9 ([41]). *Consider the RV X^nY^n. If $P_{X^n} = \bigotimes_{i=1}^n P_{X_i}$ then $I(X^n \wedge Y^n) \geqslant \sum_{i=1}^n I(X_i \wedge Y_i)$.*

For the construction of the SK generation protocol that we use in the achievability proof, we use the following observation which can also be found in [39].

Lemma 3.10 ([39]). *Consider the AVC corresponding to $\{W_s\}_{s\in\mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ for all $s \in \mathcal{S}$, which we suppose is not symmetrizable and the AVC corresponding to $\{V_s\}_{s\in\mathcal{S}}$, $V_s \in \mathcal{P}(\mathcal{Y}|\mathcal{U})$ for all $s \in \mathcal{S}$. Let $m \in \mathbb{N}$. The AVC corresponding to $\{V_{s^{m-1}} \otimes W_{s_m}\}_{s^m\in\mathcal{S}^m}$ is not symmetrizable as well.*

Proof. Assume $\{V_{s^{m-1}} \otimes W_{s_m}\}_{s^m\in\mathcal{S}^m}$ is symmetrizable. Then there exists a stochastic matrix $U \in \mathcal{P}(\mathcal{S}^m|\mathcal{U}^{m-1} \times \mathcal{X})$ such that for all $y^m, u^{m-1}, x_m, u^{m-1,\prime}, x'_m$

$$\begin{aligned}&\sum_{s^m} V_{s^{m-1}}(y^{m-1}|u^{m-1,\prime})W_{s_m}(y_m|x'_m)U(s^m|u^{m-1}, x_m)\\ &= \sum_{s^m} V_{s^{m-1}}(y^{m-1}|u^{m-1})W_{s_m}(y_m|x_m)U(s^m|u^{m-1,\prime}, x'_m).\end{aligned}$$

Taking the sum over all y^{m-1} on both sides we get

$$\begin{aligned}&\sum_{s_m} W_{s_m}(y_m|x'_m)\bar{U}(s_m|u^{m-1}x_m)\\ &= \sum_{s_m} W_{s_m}(y_m|x_m)\bar{U}(s_m|u^{m-1}x'_m)\end{aligned}$$

for all y_m, x_m, x'_m (and an arbitrary choice of u^{m-1}) where $\bar{U} \in \mathcal{P}(\mathcal{S}|\mathcal{U}^{m-1} \times \mathcal{X})$ such that

$$\bar{U}(s_m|u^{m-1}, x) = \sum_{s^{m-1}} U(s^{m-1}, s_m|u^{m-1}, x).$$

This contradicts the assumption that the AVC corresponding to $\{W_s\}_{s\in\mathcal{S}}$ is not symmetrizable.

■

The following theorem is one of our main achievability results. This theorem is equivalent to the achievability part of Theorem 3.7.

Theorem 3.11. *If the AVC corresponding to $\{W_s\}_{s\in\mathcal{S}}$ is non symmetrizable it holds that $\mathcal{R}_{AVC} \supset \mathcal{R}$.*

For the proof we use a technique similar to the one that is used for the direct proof of [5, Proposition 1a)]. For this proof the set, the first output of the source is distributed on, is exhausted by subsequently choosing channel codes with codewords from this set. For our achievability proof we use the first output of the source to generate a sequence from a set $\mathcal{U}^n$. We use the technique discussed above to exhaust $\mathcal{U}^n$. As we use a randomized encoder we use blocking to guarantee that the corresponding channel is non symmetrizable, cf. Lemma 3.10.

Proof. Let $\tau > 0$. (We can assume $\min_{x\in\mathcal{X}} P_X(x) \geqslant \beta > 0$. If this is not the case we construct our protocol for the support of P_X. This protocol has the desired performance as entropy only depends on the support of the corresponding distributions.) Choose the RV U (where we again can assume $\min_{u\in\mathcal{U}} P_U(u) \geqslant \beta > 0$) such that $U - X - Y_s$ for all $s \in \mathcal{S}$. Choose $l \in \mathbb{N}$ large enough such that $\epsilon_1(l)$ and $\epsilon_4(l)$ are both less than $\delta/2$ (where the functions $\epsilon_1, \epsilon_4 \colon \mathbb{N} \to \mathbb{R}$ will be determined later). For all t large enough, construct constant composition (t, ϵ)-codes $\{(f_t^{m,l}, \phi_t^{m,l})\}_{m\in\mathcal{M}}$, $f_t^{m,l} \colon \mathcal{K} \to (\mathcal{U}^{l-1} \times \mathcal{X})^t$, $\phi_t^{m,l} \colon \mathcal{Y}^{lt} \to \mathcal{K}$, for the AVC corresponding to $\{\bigotimes_{i=1}^{l-1} P_{Y_{s_i}|U} \otimes P_{Y_{s_l}|X}\}_{s^l\in\mathcal{S}^l}$ with $f_t^{m,l}(\mathcal{K}) \cap f_t^{m',l}(\mathcal{K}) = \varnothing$ for all $m, m' \in \mathcal{M}$, $m \neq m'$ and

$$|\mathcal{K}| = \lfloor \exp(t(\min_{\bar{W}^l\in\bar{\mathcal{W}}^l} I(P_U^{\otimes l-1} \otimes P_X, \bar{W}^l) - \tau)) \rfloor$$

for $\bar{\mathcal{W}}^l = \operatorname{conv}(\{\bigotimes_{i=1}^{l-1} P_{Y_{s_i}|U} \otimes P_{Y_{s_l}|X}\}_{s^l\in\mathcal{S}^l})$.

For this purpose choose these codes iteratively for each $\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X})$ with

$$\|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta,$$

$\frac{1}{2|\mathcal{Y}|} > \delta > 0$, $\delta \leqslant \beta^l$. (Note that $\min_{(u^{l-1},x_l)\in\mathcal{U}^{l-1}\times\mathcal{X}} P_U^{\otimes l-1} \otimes P_X(u^{l-1}, x_l) \geqslant \beta^l > 0$.) Start by choosing $\mathcal{A}_{m_1} \subset \mathcal{T}_{\bar{P}}^t$, $m_1 \in \mathcal{M}$, with

$$(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{A}_{m_1}) > \frac{\eta \exp(-tD(\bar{P}\|P_U^{\otimes l-1}\otimes P_X))}{(t+1)^{|\mathcal{U}^{l-1}\times\mathcal{X}|}}.$$

Now choose $(f_t^{m_1,l}, \phi_t^{m_1,l})$ such that $f_t^{m_1,l}(\mathcal{K}) \subset \mathcal{A}_{m_1}$. This is possible for δ small enough, as follows from Lemma 3.10 and Lemma 2.29. Now choose $\mathcal{A}_{m_2} \subset \mathcal{T}_{\bar{P}}^t \backslash f_t^{m_1,l}(\mathcal{K})$, $m_2 \in \mathcal{M}$, such that

$$(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{A}_{m_2}) > \frac{\eta \exp(-tD(\bar{P}\|P_U^{\otimes l-1}\otimes P_X))}{(t+1)^{|\mathcal{U}^{l-1}\times\mathcal{X}|}}$$

and choose $(f_t^{m_2,l}, \phi_t^{m_2,l})$ such that $f_t^{m_2,l}(\mathcal{K}) \subset \mathcal{A}_{m_2}$. In the m_i-th step choose $\mathcal{A}_{m_i} \subset \mathcal{T}_{\bar{P}}^t \backslash \bigcup_{j\in\{1\cdots i-1\}} f_t^{m_j,l}(\mathcal{K})$, $m_i \in \mathcal{M}$, such that

$$(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{A}_{m_i}) > \frac{\eta \exp(-tD(\bar{P}\|P_U^{\otimes l-1}\otimes P_X))}{(t+1)^{|\mathcal{U}^{l-1}\times\mathcal{X}|}}$$

and choose $(f_t^{m_i,l}, \phi_t^{m_i,l})$ such that $f_t^{m_i,l}(\mathcal{K}) \subset \mathcal{A}_{m_i}$.

When we can not find a set $\mathcal{A}_{m_{i+1}} \subset \mathcal{T}_{\bar{P}}^t \backslash \bigcup_{j\in\{1\cdots i\}} f_t^{m_j,l}(\mathcal{K})$, $m_{i+1} \in \mathcal{M}$, with

$$(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{A}_{m_{i+1}}) > \frac{\eta \exp(-tD(\bar{P}\|P_U^{\otimes l-1}\otimes P_X))}{(t+1)^{|\mathcal{U}^{l-1}\times\mathcal{X}|}}$$

anymore, we continue with the next type.

We repeat the procedure for all types $\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X})$ such that

$$\|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta.$$

We denote the set of indices $m \in \mathcal{M}$ corresponding to type $\bar{P}$ by $\mathcal{M}_{\bar{P}}$, i.e. $\mathcal{M} = \bigcup_{\bar{P}} \mathcal{M}_{\bar{P}}$, where the union is over all $\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X})$ such that $\|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta$.

So we have

$$\begin{aligned}
&(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}((\bigcup_{m \in \mathcal{M}} f_t^{m,l}(\mathcal{K}))^c) \\
&= (P_U^{\otimes l-1} \otimes P_X)^{\otimes t}((\mathcal{T}^t_{P_U^{\otimes l-1} \otimes P_X, \delta/|\mathcal{U}^{l-1} \times \mathcal{X}|})^c) \\
&+ (P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{T}^t_{P_U^{\otimes l-1} \otimes P_X, \delta/|\mathcal{U}^{l-1} \times \mathcal{X}|} \setminus \bigcup_{m \in \mathcal{M}} f_t^{m,l}(\mathcal{K}))
\end{aligned}$$

where the first summand can be upper bounded by $\xi > 0$ arbitrarily small for t large enough. We also have

$$\begin{aligned}
\mathcal{T}^t_{P_U^{\otimes l-1} \otimes P_X, \delta/|\mathcal{U}^{l-1} \times \mathcal{X}|} \setminus \bigcup_{m \in \mathcal{M}} f_t^{m,l}(\mathcal{K}) &\subset \Big(\bigcup_{\substack{\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X}): \\ \|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta}} \mathcal{T}^t_{\bar{P}} \Big) \setminus \bigcup_{m \in \mathcal{M}} f_t^{m,l}(\mathcal{K}) \\
&= \bigcup_{\substack{\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X}): \\ \|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta}} \Big(\mathcal{T}^t_{\bar{P}} \setminus \bigcup_{m \in \mathcal{M}_{\bar{P}}} f_t^{m,l}(\mathcal{K}) \Big).
\end{aligned}$$

So the second summand can be upper bounded by

$$\begin{aligned}
&\sum_{\substack{\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X}): \\ \|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta}} (P_U^{\otimes l-1} \otimes P_X)^{\otimes t}(\mathcal{T}^t_{\bar{P}} \setminus \bigcup_{m \in \mathcal{M}_{\bar{P}}} f_t^{m,l}(\mathcal{K})) \\
&\leqslant \sum_{\substack{\bar{P} \in \mathcal{P}(t, \mathcal{U}^{l-1} \times \mathcal{X}): \\ \|\bar{P} - P_U^{\otimes l-1} \otimes P_X\|_1 \leqslant \delta}} \frac{\eta \exp(-tD(\bar{P} \| P_U^{\otimes l-1} \otimes P_X))}{(t+1)^{|\mathcal{U}^{l-1} \times \mathcal{X}|}} \leqslant \eta
\end{aligned}$$

and thus altogether we have

$$(P_U^{\otimes l-1} \otimes P_X)^{\otimes t}((\bigcup_{m \in \mathcal{M}} f_t^{m,l}(\mathcal{K}))^c) \leqslant \xi + \eta. \tag{3.10}$$

Define $v_{t,l} \colon \mathcal{X}^{tl} \times \mathcal{U}^{tl} \to (\mathcal{U}^{l-1} \times \mathcal{X})^t$, $v_{t,l}(x^{tl}, u^{tl}) = u^{l-1} x_l u_{l+1}^{2l-1} x_{2l} \cdots u_{(t-1)l+1}^{tl-1} x_{tl}$. Consider the independent RV Z_1 uniformly distributed on $\mathcal{K}$ and the mappings $\bar{f}_{tl} \colon \mathcal{X}^{tl} \times \mathcal{U}^{tl} \times \mathcal{Z}_1 \to \mathcal{K} \times \mathcal{M}$ and $\bar{\phi}_{tl} \colon \mathcal{Y}^{tl} \times \mathcal{M} \to \mathcal{K}$

$$\bar{f}_{tl}(x^{tl}, u^{tl}, z_1) = \begin{cases} ((f_t^{m,l})^{-1}(v_{t,l}(x^{tl}, u^{tl})), m) & v_{t,l}(x^{tl}, u^{tl}) \in f_t^{m,l}(\mathcal{K}) \\ (z_1, \bar{m}) & \text{else} \end{cases}$$

$$\bar{\phi}_{tl}(y^{tl}, m) = \phi_k^{m,l}(y^{tl})$$

for all $m \in \mathcal{M}$ and an arbitrary $\bar{m} \in \mathcal{M}$. Note that $\bar{f}_{tl}(x^{tl}, u^{tl}, z_1)$ is well defined as the $f_t^{m,l}$ are injective. (Above we introduce the following notation. Given a sequence $x^n \in \mathcal{X}^n$ and $1 \leqslant i \leqslant j \leqslant n$ we write x_i^j for the subsequence $x_i, \cdots, x_j$.)

Consider the RV U^n with

$$\Pr(U^n X^n Y_{s^n}^n = (u^n, x^n, y^n)) = P_X^{\otimes n}(x^n) P_{U|X}^{\otimes n}(u^n|x^n) W_{s^n}(y^n|x^n)$$

for all $(u^n, x^n, y^n) \in \mathcal{U}^n \times \mathcal{X}^n \times \mathcal{Y}^n$ and all $s^n \in \mathcal{S}^n$. We define

$$\begin{aligned} F(k, m|x^n) &= \Pr(\bar{f}_{\lfloor \frac{n}{l} \rfloor l}(x^{l\lfloor \frac{n}{l} \rfloor}, U^{l\lfloor \frac{n}{l} \rfloor}, Z_1) = (k, m)) \\ g(y^n, m) &= \bar{\phi}_{\lfloor \frac{n}{l} \rfloor l}(y^{l\lfloor \frac{n}{l} \rfloor}, m) \end{aligned}$$

for all $(k, m, x^n, y^n) \in \mathcal{K} \times \mathcal{M} \times \mathcal{X}^n \times \mathcal{Y}^n$ and we have $n = \lfloor \frac{n}{l} \rfloor l + r$ with $r \in \mathbb{N}$, $0 \leqslant r < l$.

We now analyse the performance of this SK generation protocol. For notational convenience we define

$$V_{\lfloor \frac{n}{l} \rfloor, l} = v_{\lfloor \frac{n}{l} \rfloor, l}(X^{l\lfloor \frac{n}{l} \rfloor}, U^{l\lfloor \frac{n}{l} \rfloor}).$$

We have

$$\begin{aligned} &\Pr(K = k|M = m) \\ &= \Pr(K = k|M = m, V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})) \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})|M = m) \\ &+ \Pr(K = k|M = m, V_{\lfloor \frac{n}{l} \rfloor, l} \notin f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})) \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \notin f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})|M = m) = \tfrac{1}{|\mathcal{K}|}. \end{aligned}$$

For the last step consider

$$\begin{aligned} &\Pr(K = k|M = m, V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})) \\ &= \Pr(K = k|V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})) \\ &= \Pr((f_{\lfloor \frac{n}{l} \rfloor}^{m,l})^{-1}(V_{\lfloor \frac{n}{l} \rfloor, l}) = k|V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K})) \\ &= \frac{\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} = f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(k) \wedge V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K}))}{\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K}))} \\ &= \frac{\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} = f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(k))}{\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K}))} = \frac{(P_U^{\otimes l-1} \otimes P_X)^{\otimes \lfloor \frac{n}{l} \rfloor}(f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(k))}{\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f_{\lfloor \frac{n}{l} \rfloor}^{m,l}(\mathcal{K}))} = \tfrac{1}{|\mathcal{K}|}, \end{aligned} \tag{3.11}$$

where the last step follows as the type $P_{f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(k)}$ is the same for all $k \in \mathcal{K}$,

$$\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \notin f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K}) | M = m) = 0$$

for $m \neq \bar{m}$ and

$$\Pr(K = k | M = \bar{m}, V_{\lfloor \frac{n}{l} \rfloor, l} \notin f^{\bar{m},l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})) = \Pr(Z_1 = k) = \tfrac{1}{|\mathcal{K}|}.$$

We have for all $m \in \mathcal{M}$

$$\begin{aligned}
&\min_{s^n \in \mathcal{S}^n} \Pr(K = \hat{K}_{s^n} | M = m) \\
&\geqslant \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K}) | M = m) \min_{s^n \in \mathcal{S}^n} \Pr(K = \hat{K}_{s^n} | M = m, V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})).
\end{aligned}$$

This equals

$$\begin{aligned}
&\Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K}) | M = m) \\
&\cdot \min_{s^n \in \mathcal{S}^n} \sum_{k \in \mathcal{K}} \Pr(K = k | M = m, V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})) \\
&\qquad \cdot \Pr(K = \hat{K}_{s^n} | M = m, K = k, V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})) \\
&= \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K}) | M = m) \min_{s^n \in \mathcal{S}^n} \tfrac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} W_{s^{n-r}}((\phi^{m,l}_{\lfloor \frac{n}{l} \rfloor})^{-1}(k) | f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(k)), \qquad (3.12)
\end{aligned}$$

where we use (3.11) and the definition of the SK generation protocol. So

$$\begin{aligned}
&\sum_{m \in \mathcal{M}} P_M(m) \min_{s^n \in \mathcal{S}^n} \Pr(K = \hat{K}_{s^n} | M = m) \\
&\geqslant \sum_{m \in \mathcal{M}} \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K}), M = m) \min_{s^n \in \mathcal{S}^n} \tfrac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} W_{s^{n-r}}((\phi^{m,l}_{\lfloor \frac{n}{l} \rfloor})^{-1}(k) | f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(k)) \\
&= \sum_{m \in \mathcal{M}} \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})) \min_{s^n \in \mathcal{S}^n} \tfrac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} W_{s^{n-r}}((\phi^{m,l}_{\lfloor \frac{n}{l} \rfloor})^{-1}(k) | f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(k)) \\
&\geqslant (1 - \epsilon) \Pr(V_{\lfloor \frac{n}{l} \rfloor, l} \in \bigcup_{m \in \mathcal{M}} f^{m,l}_{\lfloor \frac{n}{l} \rfloor}(\mathcal{K})) \\
&\geqslant (1 - \epsilon)(1 - \xi - \eta) \geqslant 1 - \delta
\end{aligned}$$

for n large enough, where we use (3.12), (2.27) and (3.10).

We have

$$\tfrac{1}{\lfloor \frac{n}{l} \rfloor} \log |\mathcal{K}| \geqslant \min_{\bar{W}^l \in \bar{\mathcal{W}}^l} I(P_U^{\otimes l-1} \otimes P_X, \bar{W}^l) - \tau - \tfrac{1}{\lfloor \frac{n}{l} \rfloor}$$

for n large enough. Consider $\bar{W}^l \in \bar{\mathcal{W}}^l$ corresponding to $P_{S^l} \in \mathcal{P}(\mathcal{S}^l)$ with marginals $P_{S_i} \in \mathcal{P}(\mathcal{S})$, $i \in \{1 \cdots l\}$. Define $\bar{W}_i \in \mathcal{P}(\mathcal{Y}|\mathcal{U})$ such that $\bar{W}_i(y|u) = \sum_{s \in \mathcal{S}} P_{S_i}(s) P_{Y_s|U}(y|u)$,

$i \in \{1 \cdots l-1\}$, and $\bar{W}_l \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\bar{W}_l(y|x) = \sum_{s\in\mathcal{S}} P_{S_l}(s)P_{Y_s|X}(y|x)$ for all $(x,y,u) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{U}$. As according to Lemma 3.9

$$I(P_U^{\otimes l-1}\otimes P_X, \bar{W}^l) \geqslant \sum_{i=1}^{l-1} I(P_U,\bar{W}_i) + I(P_X,\bar{W}_l)$$

we have

$$\begin{aligned}\min_{\bar{W}^l\in\bar{\mathcal{W}}^l} I(P_U^{\otimes l-1}\otimes P_X,\bar{W}^l) &\geqslant \min_{\bar{W}^l\in\bar{\mathcal{W}}^l}\sum_{i=1}^{l-1} I(P_U,\bar{W}_i) + I(P_X,\bar{W}_l)\\ &= (l-1)\min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U,\bar{W}) + \min_{\bar{W}\in\bar{\mathcal{W}}_l} I(P_X,\bar{W})\end{aligned}$$

where $\bar{\mathcal{W}} = \mathrm{conv}(\{P_{Y_s|U}\}_{s\in\mathcal{S}})$ and $\bar{\mathcal{W}}_l = \mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})$. So

$$\begin{aligned}&\tfrac{1}{l}\min_{\bar{W}^l\in\bar{\mathcal{W}}^l} I(P_U^{\otimes l-1}\otimes P_X,\bar{W}^l) \geqslant \tfrac{l-1}{l}\min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U,\bar{W})\\ &\geqslant \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U,\bar{W}) - \tilde{\tau}\end{aligned}$$

for $\tilde{\tau} > 0$ (where $\tilde{\tau}$ depends on l such that $\tilde{\tau}(l)\to 0$ for $l\to\infty$). So we have

$$\begin{aligned}&\tfrac{1}{n}\log|\mathcal{K}| = \tfrac{1}{\lfloor\frac{n}{l}\rfloor l+r}\log|\mathcal{K}| = \tfrac{1}{1+\frac{r}{\lfloor\frac{n}{l}\rfloor l}}\tfrac{1}{\lfloor\frac{n}{l}\rfloor l}\log|\mathcal{K}|\\ &\geqslant \tfrac{1}{1+\frac{1}{\lfloor\frac{n}{l}\rfloor}}\big(\min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U,\bar{W}) - \tilde{\tau} - \tfrac{\tau}{l} - \tfrac{1}{n}\big) \geqslant \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U,\bar{W}) - \epsilon_1(l) - \epsilon_2(l,n)\end{aligned}$$

for $\epsilon_1(l), \epsilon_2(l,n) > 0$ and $\epsilon_1(l)\to 0$ for $l\to\infty$ and $\epsilon_2(l,n)\to 0$ for $n\to\infty$ for all $l\in\mathbb{N}$.

Note that

$$\begin{aligned}&H(U^n|M) = H(U^nX_lX_{2l}\cdots X_{\lfloor\frac{n}{l}\rfloor l}|M) - H(X_lX_{2l}\cdots X_{\lfloor\frac{n}{l}\rfloor l}|MU^n)\\ &\geqslant H(V_{\lfloor\frac{n}{l}\rfloor,l}|M) - \log|\mathcal{X}|\tfrac{n}{l}.\end{aligned}$$

Now we consider

$$\begin{aligned}&H(V_{\lfloor\frac{n}{l}\rfloor,l}|M) \geqslant H(V_{\lfloor\frac{n}{l}\rfloor,l}|M\mathbb{1}_{\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})}(V_{\lfloor\frac{n}{l}\rfloor,l}))\\ &\geqslant \sum_{m\in\mathcal{M}}\Pr(V_{\lfloor\frac{n}{l}\rfloor,l}\in\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K}))\\ &\cdot\Pr(M=m|V_{\lfloor\frac{n}{l}\rfloor,l}\in\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K}))H(V_{\lfloor\frac{n}{l}\rfloor,l}|M=m,\mathbb{1}_{\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})}(V_{\lfloor\frac{n}{l}\rfloor,l})=1)\end{aligned}$$

As $f^{m,l}_{\lfloor\frac{n}{l}\rfloor}$ is injective we have

$$\begin{aligned} H(V_{\lfloor\frac{n}{l}\rfloor,l}|M=m,\mathbb{1}_{\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})}(V_{\lfloor\frac{n}{l}\rfloor,l})=1) &= H(V_{\lfloor\frac{n}{l}\rfloor,l}|\mathbb{1}_{f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})}(V_{\lfloor\frac{n}{l}\rfloor,l})=1) \\ &= H((f^{m,l}_{\lfloor\frac{n}{l}\rfloor})^{-1}(V_{\lfloor\frac{n}{l}\rfloor,l})|\mathbb{1}_{f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})}(V_{\lfloor\frac{n}{l}\rfloor,l})=1) \\ &= \log|\mathcal{K}|. \end{aligned}$$

It follows that

$$\begin{aligned} H(U^n|M) &\geqslant \log|\mathcal{K}|\Pr(V_{\lfloor\frac{n}{l}\rfloor,l}\in\bigcup_{m\in\mathcal{M}} f^{m,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K}))-\log|\mathcal{X}|\tfrac{n}{l} \\ &\geqslant (1-\xi-\eta)\log|\mathcal{K}|-\log|\mathcal{X}|\tfrac{n}{l}. \end{aligned} \tag{3.13}$$

and (for an arbitrary $s^n\in\mathcal{S}^n$)

$$\begin{aligned} H(U^n)-H(M|X^n)-I(U^n\wedge X^n) &= H(U^n|X^n)-H(M|X^n) \\ &= H(U^nM|X^n)-H(M|X^n) \\ &= H(U^n|MX^n)=H(U^n|MX^nY^n_{s^n}) \\ &\leqslant H(V_{\lfloor\frac{n}{l}\rfloor,l}|MY^n_{s^n})+\log|\mathcal{U}|(\lfloor\tfrac{n}{l}\rfloor+r) \\ &\leqslant \log|\mathcal{U}|(\tfrac{n}{l}+l)+\epsilon_3, \end{aligned} \tag{3.14}$$

where $\epsilon_3>0$ arbitrarily small for n large enough which follows from $H(M|U^nX^n)=0$ [26, Problem 3.1], $U^nM-X^n-Y^n_{s^n}$ which implies $U^n-MX^n-Y^n_{s^n}$ and Fano's inequality [26, Lemma 3.8] in combination with

$$\Pr(V_{\lfloor\frac{n}{l}\rfloor,l}=f^{M,l}_{\lfloor\frac{n}{l}\rfloor}(g(Y^n_{s^n},M)))\geqslant\Pr(V_{\lfloor\frac{n}{l}\rfloor,l}\in\bigcup_{m\in\mathcal{M}} f^{M,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K})\wedge g(Y^n_{s^n},M)=K)$$

which can be lower bounded by

$$\Pr(V_{\lfloor\frac{n}{l}\rfloor,l}\in\bigcup_{m\in\mathcal{M}} f^{M,l}_{\lfloor\frac{n}{l}\rfloor}(\mathcal{K}))+\Pr(g(Y^n_{s^n},M)=K)-1\geqslant 1-2\xi-2\eta-\epsilon$$

for n large enough.

Thus we get

$$\begin{aligned} I(M\wedge X^n) &= I(M\wedge U^n)-H(M|X^n)+H(M|U^n) \\ &\leqslant H(U^n)-H(U^n|M)-H(M|X^n)+\log|\mathcal{X}|(\tfrac{n}{l}+l) \\ &\leqslant nI(U\wedge X)-(1-\xi-\eta)\log|\mathcal{K}|+\epsilon_3+\log|\mathcal{X}^2\times\mathcal{U}|(\tfrac{n}{l}+l), \end{aligned}$$

where we use

$$\begin{aligned}
&H(M|U^n)\\
&= H(M|U^n(X_l, X_{2l}, \cdots, X_{\lfloor \frac{n}{l} \rfloor l}))\\
&\qquad\qquad + H(X_l, X_{2l}, \cdots, X_{\lfloor \frac{n}{l} \rfloor l}|U^n) - H(X_l, X_{2l}, \cdots, X_{\lfloor \frac{n}{l} \rfloor l}|U^n M)\\
&\leqslant \log |\mathcal{X}|^{\frac{n}{l}}
\end{aligned}$$

together with [26, Problem 3.1] and (3.13) and (3.14) for the last inequality.

So

$$\tfrac{1}{n} I(M \wedge X^n) \leqslant I(P_X, P_{U|X}) - \min_{\bar{W} \in \bar{\mathcal{W}}} I(P_U, \bar{W}) + \epsilon_4(l) + \epsilon_5(l, n),$$

for $\epsilon_4(l), \epsilon_5(l,n) > 0$ and $\epsilon_4(l) \to 0$ for $l \to \infty$ and $\epsilon_5(l,n) \to 0$ for $n \to \infty$ for all $l \in \mathbb{N}$.

■

Our second achievability result is the following theorem. This theorem is equivalent to the achievability part of Theorem 3.5.

Theorem 3.12. *It holds that* $\mathcal{R}'_{AVC} \supset \mathcal{R}$.

For the proof we use the Ahlswede robustification that is for example applied in [3]. This means we can use a result for compound sources to prove our result.

Proof. Given $\delta > 0$ there is an $n_0 \in \mathbb{N}$ and a $c > 0$ such that for all $n \geqslant n_0$ and $(R, L) \in \mathcal{R}$ we can find (F_c, g_c), where $F_c \in \mathcal{P}(\mathcal{K}_c \times \mathcal{M}_c | \mathcal{X}^n)$ and $g_c \colon \mathcal{Y}^n \times \mathcal{M}_c \to \mathcal{K}_c$, such that for RVs K_c and M_c with

$$P_{K_c M_c}(k, m) = \sum_{x^n \in \mathcal{X}^n} P_X^{\otimes n}(x^n) F_c(k, m | x^n)$$

for all $(k, m) \in \mathcal{K}_c \times \mathcal{M}_c$ it holds that

$$\max_{\substack{\bar{W} \in \\ \operatorname{conv}(\{W_s\}_{s \in \mathcal{S}})}} \sum_{x^n, y^n} \sum_{\substack{k, \hat{k}: \\ k \neq \hat{k}}} \sum_{m \in \mathcal{M}_c} P_X^{\otimes n}(x^n) \bar{W}^{\otimes n}(y^n | x^n) F_c(k, m | x^n) \mathbb{1}_{g_c^{-1}(\hat{k})}(y^n, m) \leqslant \exp(-nc)$$

$$\begin{aligned}
&H(K_c) = \log |\mathcal{K}_c|\\
&I(K_c \wedge M_c) = 0\\
&\tfrac{1}{n} \log |\mathcal{K}_c| \geqslant R - \delta\\
&\tfrac{1}{n} I(M_c \wedge X^n) \leqslant L + \delta,
\end{aligned}$$

as follows from Theorem 3.3.

We now define $\{(F^\pi, g^\pi)\}_{\pi \in \Pi_n}$, $F^\pi \in \mathcal{P}(\mathcal{K}_c \times \mathcal{M}_c | \mathcal{X}^n)$ and $g^\pi \colon \mathcal{Y}^n \times \mathcal{M}_c \to \mathcal{Y}^n$ for all

$\pi \in \Pi_n$, by

$$F^\pi(k,m|x^n) = F_c(k,m|\pi x^n)$$
$$g^\pi(y^n,m) = g_c(\pi y^n, m)$$

for all $(x^n, y^n, k, m) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{K}_c \times \mathcal{M}_c$, where Π_n is the set of all permutations on $\{1 \cdots n\}$. (With a slight abuse of notation we write πx^n for $x_{\pi^{-1}(1)} \cdots x_{\pi^{-1}(n)}$ so in this sense π induces a bijection on $\mathcal{X}^n$.)

Now we define $h \colon \mathcal{S}^n \to [0,1]$

$$h(s^n) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n,m).$$

For all $P \in \mathcal{P}(\mathcal{S})$ we have

$$\begin{aligned}
&\sum_{s^n \in \mathcal{S}^n} h(s^n) P^{\otimes n}(s^n) \\
&= \sum_{s^n \in \mathcal{S}^n} P^{\otimes n}(s^n) \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n,m)
\end{aligned}$$

which equals

$$\begin{aligned}
&\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) \sum_{s^n \in \mathcal{S}^n} \prod_{i=1}^n W_{s_i}(y_i|x_i) P(s_i) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n,m) \\
&= \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) \prod_{i=1}^n \sum_{s \in \mathcal{S}} W_s(y_i|x_i) P(s) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n,m).
\end{aligned}$$

So for $\bar{W}$ such that $\bar{W}(y|x) = \sum_{s \in \mathcal{S}} W_s(y|x) P(s)$ for all $(x,y) \in \mathcal{X} \times \mathcal{Y}$ (i.e. $\bar{W} \in \mathrm{conv}(\{W_s\}_{s \in \mathcal{S}})$) we have

$$\sum_{s^n \in \mathcal{S}^n} h(s^n) P^{\otimes n}(s^n) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) \bar{W}^{\otimes n}(y^n|x^n) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n,m).$$

From our choice of (F_c, g_c) we thus know that

$$\sum_{s^n \in \mathcal{S}^n} h(s^n) P^{\otimes n}(s^n) > 1 - \exp(-nc).$$

Using [3, Theorem RT] we get

$$\tfrac{1}{n!} \sum_{\pi \in \Pi_n} h(\pi s^n) > 1 - \exp(-nc)(n+1)^{|\mathcal{S}|}. \tag{3.15}$$

Now we consider for $\pi \in \Pi_n$

$$h(\pi s^n) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) W_{\pi s^n}(y^n|x^n) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n, m).$$

This equals

$$\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} \prod_{i=1}^{n} P_X(x_{\pi(i)}) W_{s_i}(y_{\pi(i)}|x_{\pi(i)}) F_c(k,m|x^n) \mathbb{1}_{g_c^{-1}(k)}(y^n, m).$$

As π is a bijection and we take the sum over all (x^n, y^n) this equals

$$\begin{aligned} &\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} \prod_{i=1}^{n} P_X(x_i) W_{s_i}(y_i|x_i) F_c(k,m|\pi x^n) \mathbb{1}_{g_c^{-1}(k)}(\pi y^n, m) \\ &= \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k \in \mathcal{K}_c \\ m \in \mathcal{M}_c}} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F_c^{\pi}(k,m|x^n) \mathbb{1}_{(g_c^{\pi})^{-1}(k)}(y^n, m). \end{aligned}$$

So considering (3.15) we conclude that the SK generation protocol (F, g), $F \in \mathcal{P}(\mathcal{K}_c \times (\mathcal{M}_c \times \Pi_n)|\mathcal{X}^n)$ and $g\colon \mathcal{Y}^n \times (\mathcal{M}_c \times \Pi_n) \to \mathcal{K}_c$, achieves an arbitrarily small error probability for n large enough when used to generate a SK from $\{P_{XY_s}\}_{s \in \mathcal{S}}$, where for all $(x^n, y^n, k, m, \pi) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{K}_c \times \mathcal{M}_c \times \Pi_n$

$$\begin{aligned} F(k,(m,\pi)|x^n) &= \tfrac{1}{n!} F^{\pi}(k,m|x^n) \\ g(y^n,(m,\pi)) &= g^{\pi}(y^n,m). \end{aligned}$$

Correspondingly we define $\mathcal{K} = \mathcal{K}_c$ and $\mathcal{M} = \mathcal{M}_c \times \Pi_n$. It holds for $(k, m, \pi) \in \mathcal{K} \times \mathcal{M}$ that

$$\begin{aligned} P_{KM}(k,(m,\pi)) &= \sum_{x^n \in \mathcal{X}^n} P^{\otimes n}(x^n) F(k,(m,\pi)|x^n) \\ &= \sum_{x^n \in \mathcal{X}^n} \tfrac{1}{n!} P^{\otimes n}(x^n) F^{\pi}(k,m|x^n) \\ &= \tfrac{1}{n!} \sum_{x^n \in \mathcal{X}^n} P^{\otimes n}(x^n) F_c(k,m|\pi x^n) \\ &= \tfrac{1}{n!} \sum_{x^n \in \mathcal{X}^n} P^{\otimes n}(x^n) F_c(k,m|x^n) = \tfrac{1}{n!} P_{K_c M_c}(k,m). \end{aligned} \tag{3.16}$$

So we have

$$P_{K|M}(k|m,\pi) = \tfrac{P_{KM}(k,(m,\pi))}{\sum_{k \in \mathcal{K}} P_{KM}(k,(m,\pi))} = P_{K_c|M_c}(k|m) = \tfrac{1}{|\mathcal{K}|}$$

which is equivalent to $I(K \wedge M) = 0$ and $H(K) = \log|\mathcal{K}|$. Finally consider

$$\begin{aligned} P_{MX^n}((m,\pi),x^n) &= \sum_{k\in\mathcal{K}} P^{\otimes n}(x^n)F(k,(m,\pi)|x^n) \\ &= \sum_{k\in\mathcal{K}} \tfrac{1}{n!}P^{\otimes n}(x^n)F^{\pi}(k,m|x^n) \\ &= \sum_{k\in\mathcal{K}} \tfrac{1}{n!}P^{\otimes n}(x^n)F_c(k,m|\pi x^n). \end{aligned} \tag{3.17}$$

It holds that

$$I(M \wedge X^n) = \sum_{(m,\pi)\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} P_{MX^n}((m,\pi),x^n) \log \tfrac{P_{MX^n}((m,\pi),x^n)}{P_M(m,\pi)P_{X^n}(x^n)}.$$

Using (3.16) and (3.17) we see that this expression equals

$$\begin{aligned} &\sum_{(m,\pi)\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} P_{MX^n}((m,\pi),x^n) \log \tfrac{\sum_{k\in\mathcal{K}} F_c(k,m|\pi x^n)}{P_{M_c}(m)} \\ &= \sum_{(m,\pi)\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} P_{MX^n}((m,\pi),\pi^{-1}x^n) \log \tfrac{\sum_{k\in\mathcal{K}} F_c(k,m|x^n)}{P_{M_c}(m)}, \end{aligned}$$

where we make use of the summation over all $x^n \in \mathcal{X}^n$. Again using (3.17) this equals

$$\begin{aligned} &\sum_{(m,\pi)\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{k\in\mathcal{K}} \tfrac{1}{n!}P^{\otimes n}(\pi^{-1}x^n)F_c(k,m|x^n) \log \tfrac{P_{M_c|X^n}(m|x^n)}{P_{M_c}(m)} \\ &= \sum_{(m,\pi)\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{k\in\mathcal{K}} \tfrac{1}{n!}P^{\otimes n}(x^n)F_c(k,m|x^n) \log \tfrac{P_{M_c|X^n}(m|x^n)}{P_{M_c}(m)} \\ &= \sum_{m\in\mathcal{M}_c} \sum_{x^n\in\mathcal{X}^n} \sum_{k\in\mathcal{K}} P^{\otimes n}(x^n)F_c(k,m|x^n) \log \tfrac{P_{M_c|X^n}(m|x^n)}{P_{M_c}(m)} \\ &= I(M_c \wedge X^n) \leqslant n(L+\delta). \end{aligned}$$

■

Now we prove converse results, complementing our achievability results. The first converse result is equivalent to the first part of the converse part of Theorem 3.7, that is the part where the corresponding AVC is symmetrizable.

Theorem 3.13. *If the AVC corresponding to $\{W_s\}_{s\in\mathcal{S}}$ is symmetrizable, then $\mathcal{R}_{AVC} \subset \{(R,L)\colon R \leqslant 0, L \geqslant 0\}$.*

Here we proof the existence of a jamming strategy s^n for all $m \in \mathcal{M}$ such that reliable SK generation can be prevented using the probabilistic method, cf. [24].

Proof. Consider the SK generation protocol (F,g). We want to show that

$$\sum_{m\in\mathcal{M}} P_M(m) \max_{s^n\in\mathcal{S}^n} \Pr(K \neq \hat{K}_{s^n}|M=m) \geqslant \epsilon$$

for an $\epsilon > 0$. For this purpose we show

$$\max_{s^n \in \mathcal{S}^n} \Pr(K \neq \hat{K}_{s^n} | M = m) \geqslant \epsilon \tag{3.18}$$

for all $m \in \mathcal{M}$. So let $m \in \mathcal{M}$. Consider RVs $\{S_k\}_{k\in\mathcal{K}}$, such that

$$\Pr(S_k = s^n) = \sum_{x^n \in \mathcal{X}^n} P_{X^n|MK}(x^n|m,k) P_{S|X}^{\otimes n}(s^n|x^n)$$

where $P_{S|X}$ symmetrizes $\{W_s\}_{s\in\mathcal{S}}$.We have for all $\bar{k} \in \mathcal{K}$

$$\begin{aligned}
&\sum_{s^n \in \mathcal{S}^n} \Pr(S_{\bar{k}} = s^n) \Pr(\hat{K}_{s^n} \neq K | M = m) \\
&= \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} \sum_{s^n \in \mathcal{S}^n} \Pr(S_{\bar{k}} = s^n) \Pr(\hat{K}_{s^n} \neq k | M = m, K = k) \\
&= \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} \sum_{y^n \in \mathcal{Y}^n} \mathbb{1}_{(g^{-1}(k))^c}(y^n, m) \sum_{s^n \in \mathcal{S}^n} \Pr(S_{\bar{k}} = s^n) \sum_{x^n \in \mathcal{X}^n} P_{X^n|MK}(x^n|m,k) W_{s^n}(y^n|x^n).
\end{aligned}$$

We have

$$\begin{aligned}
&\sum_{s^n \in \mathcal{S}^n} \Pr(S_{\bar{k}} = s^n) \sum_{x^n \in \mathcal{X}^n} P_{X^n|MK}(x^n|m,k) W_{s^n}(y^n|x^n) \\
&= \sum_{s^n \in \mathcal{S}^n} \sum_{\substack{x_1^n \in \mathcal{X}^n \\ x_2^n \in \mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k}) P_{S|X}^{\otimes n}(s^n|x_2^n) P_{X^n|MK}(x_1^n|m,k) W_{s^n}(y^n|x_1^n)
\end{aligned}$$

which is equal to

$$\begin{aligned}
&\sum_{\substack{x_1^n \in \mathcal{X}^n \\ x_2^n \in \mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k}) P_{X^n|MK}(x_1^n|m,k) \sum_{s^n \in \mathcal{S}^n} \prod_{i=1}^n P_{S|X}(s_i|x_{2,i}) W_{s_i}(y_i|x_{1,i}) \\
&= \sum_{\substack{x_1^n \in \mathcal{X}^n \\ x_2^n \in \mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k}) P_{X^n|MK}(x_1^n|m,k) \prod_{i=1}^n \sum_{s\in\mathcal{S}} P_{S|X}(s|x_{2,i}) W_s(y_i|x_{1,i})
\end{aligned}$$

where the last step can be shown by induction. Now we use that the AVC corresponding

to $\{W_s\}_{s\in\mathcal{S}}$ is symmetrizable and get

$$\sum_{\substack{x_1^n\in\mathcal{X}^n\\ x_2^n\in\mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k})P_{X^n|MK}(x_1^n|m,k)\prod_{i=1}^n\sum_{s\in\mathcal{S}}P_{S|X}(s|x_{1,i})W_s(y_i|x_{2,i})$$

$$=\sum_{\substack{x_1^n\in\mathcal{X}^n\\ x_2^n\in\mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k})P_{X^n|MK}(x_1^n|m,k)\sum_{s^n\in\mathcal{S}^n}\prod_{i=1}^n P_{S|X}(s_i|x_{1,i})W_{s_i}(y_i|x_{2,i})$$

which equals

$$\sum_{s^n\in\mathcal{S}^n}\sum_{\substack{x_1^n\in\mathcal{X}^n\\ x_2^n\in\mathcal{X}^n}} P_{X^n|MK}(x_2^n|m,\bar{k})P_{S|X}^{\otimes n}(s^n|x_1^n)P_{X^n|MK}(x_1^n|m,k)W_{s^n}(y^n|x_2^n)$$

$$=\sum_{s^n\in\mathcal{S}^n}\Pr(S_k=s^n)\sum_{x^n\in\mathcal{X}^n}P_{X^n|MK}(x^n|m,\bar{k})W_{s^n}(y^n|x^n).$$

So it holds that

$$\sum_{y^n\in\mathcal{Y}^n}\mathbb{1}_{(g^{-1}(\bar{k}))^c}(y^n,m)\sum_{s^n\in\mathcal{S}^n}\Pr(S_k=s^n)\sum_{x^n\in\mathcal{X}^n}P_{X^n|MK}(x^n|m,\bar{k})W_{s^n}(y^n|x^n)$$
$$+\sum_{y^n\in\mathcal{Y}^n}\mathbb{1}_{(g^{-1}(k))^c}(y^n,m)\sum_{s^n\in\mathcal{S}^n}\Pr(S_{\bar{k}}=s^n)\sum_{x^n\in\mathcal{X}^n}P_{X^n|MK}(x^n|m,k)W_{s^n}(y^n|x^n)$$

can be lower bounded by

$$\sum_{y^n\in\mathcal{Y}^n}\sum_{s^n\in\mathcal{S}^n}\Pr(S_k=s^n)\sum_{x^n\in\mathcal{X}^n}P_{X^n|MK}(x^n|m,\bar{k})W_{s^n}(y^n|x^n)=1$$

for $k\neq\bar{k}$ and for all $h\colon\mathcal{K}^2\to[0,1]$ with $h(k,\bar{k})+h(\bar{k},k)\geqslant 1$ for $k\neq\bar{k}$ we have

$$\tfrac{1}{|\mathcal{K}|^2}\sum_{k,\bar{k}\in\mathcal{K}}h(k,\bar{k})\geqslant\sum_{\substack{k,\bar{k}\in\mathcal{K}\\ k\neq\bar{k}}}h(k,\bar{k})\geqslant\tfrac{1}{|\mathcal{K}|^2}\sum_{i=1}^{|\mathcal{K}|-1}(|\mathcal{K}|-i)$$
$$=|\mathcal{K}|(|\mathcal{K}|-1)-\tfrac{(|\mathcal{K}|-1)^2+(|\mathcal{K}|-1)}{2}=\tfrac{|\mathcal{K}|-1}{2|\mathcal{K}|}.$$

Thus we get

$$\tfrac{1}{|\mathcal{K}|}\sum_{\bar{k}\in\mathcal{K}}\sum_{s^n\in\mathcal{S}^n}\Pr(S_{\bar{k}}=s^n)\Pr(\hat{K}_{s^n}\neq K|M=m)\geqslant\tfrac{|\mathcal{K}|-1}{2|\mathcal{K}|}\geqslant\tfrac{1}{4}$$

for $|\mathcal{K}|\geqslant 2$. So for all $m\in\mathcal{M}$ there is at least one strategy s^n of the attacker such that

$$\Pr(K\neq\hat{K}_{s^n}|M=m)\geqslant\epsilon$$

which implies (3.18) for all $m \in \mathcal{M}$ (with $\epsilon = 1/4$).

■

Remark 3.14. *The jamming strategy the existence of which we prove above is a denial of service attack which consequently exists for all SK generation protocols if the jammer knows M and the PUF source is such that the corresponding channel is symmetrizable.*

Now we prove our second converse result. This result is equivalent to the converse part of Theorem 3.5. Together with (3.9) it implies the second converse part of Theorem 3.7, that is the part where the corresponding AVC is not symmetrizable.

Theorem 3.15. *It holds that $\mathcal{R}'_{AVC} \subset \mathcal{R}$.*

Proof. Consider a SK generation protocol (F, g) for $\{P_{XY_s}\}_{s\in\mathcal{S}}$. We have

$$\max_{s^n} \Pr(K \neq \hat{K}_{s^n}) = \max_{s^n} \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \sum_{\substack{m\in\mathcal{M}\\ k\in\mathcal{K}}} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F(k,m|x^n) \mathbb{1}_{(g^{-1}(k))^c}(y^n,m)$$

$$\geqslant \max_{\substack{P_{S_1}\cdots P_{S_n}\\ \in\mathcal{P}(\mathcal{S})}} \sum_{s^n} \prod_{i=1}^n P_{S_i}(s_i) \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \sum_{\substack{m\in\mathcal{M}\\ k\in\mathcal{K}}} P_X^{\otimes n}(x^n) W_{s^n}(y^n|x^n) F(k,m|x^n) \mathbb{1}_{(g^{-1}(k))^c}(y^n,m)$$

which equals

$$\max_{\substack{P_{S_1}\cdots P_{S_n}\\ \in\mathcal{P}(\mathcal{S})}} \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \sum_{\substack{m\in\mathcal{M}\\ k\in\mathcal{K}}} P_X^{\otimes n}(x^n) F(k,m|x^n) \mathbb{1}_{(g^{-1}(k))^c}(y^n,m) \prod_{i=1}^n \sum_{s\in\mathcal{S}} P_{S_i}(s) W_s(y_i|x_i)$$

$$\geqslant \max_{P_S\in\mathcal{P}(\mathcal{S})} \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \sum_{\substack{m\in\mathcal{M}\\ k\in\mathcal{K}}} P_X^{\otimes n}(x^n) F(k,m|x^n) \mathbb{1}_{(g^{-1}(k))^c}(y^n,m) \prod_{i=1}^n \sum_{s\in\mathcal{S}} P_S(s) W_s(y_i|x_i).$$

This implies that a rate pair (R, L) that is achievable according to Definition 3.3 is also achievable according to Definition 3.2, using the same SK generation protocol for the compound source $\{P_W\}_{W\in\mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})}$, $P_W \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, where $P_W(x,y) = P_X(x)W(y|x)$ for all $(x,y) \in \mathcal{X}\times\mathcal{Y}$. So from Theorem 3.4 we have

$$\mathcal{R}'_{AVC} \subset \bigcup_U \{(R,L)\colon R \leqslant \inf_{\substack{P_{Y|X}\in\\ \mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})}} I(U\wedge Y)$$
$$L \geqslant I(U\wedge X) - \inf_{\substack{P_{Y|X}\in\\ \mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})}} I(U\wedge Y)\}$$

for RVs U and Y with $U - X - Y$. As the mutual information is continuous, $\mathcal{P}(\mathcal{U}|\mathcal{X})$ and $\mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})$ are compact and

$$\min_{\substack{P_{Y|X}\in\\ \mathrm{conv}(\{W_s\}_{s\in\mathcal{S}})}} I(U\wedge Y) = \min_{\bar{W}\in\bar{\mathcal{W}}} I(P_U, \bar{W})$$

we get the result.

■

Remark 3.16. *In [30] the authors prove a capacity result for SK generation from a compound PUF source with weaker secrecy requirements. We can also use the converse part of this result instead of Theorem 3.4, cf. Remark 3.6.*

We have derived a single letter characterization of the capacity regions $\mathcal{R}_{AVC}$ and $\mathcal{R}'_{AVC}$. We have seen that the performance of the SK generation protocols strongly depends on whether the AVC corresponding to the source $\{P_{XY_s}\}_{s\in\mathcal{S}}$ is symmetrizable or not given the jammer knows the helper message. For the symmetrizable case we have proved the existence of a denial of service attack for all SK generation protocols. If the jammer does not know the helper message we can use a common randomness assisted protocol. Then symmetrizability does not decrease the performance.

4 SK Generation with Constrained Public Communication Rate

In this chapter we consider SK generation with a rate constraint on the helper message. As done for SK generation from a PUF source, we require perfect secrecy and uniform distribution of the SK. We study various models that differ in the assumptions on the source uncertainty and we prove corresponding capacity results.

4.1 Results for the compound source

In addition to strengthening the achievability requirements of the protocols for SK generation we consider a more general setting for SK generation in this section compared to the setting of [25] described in Section 2.1. As in Section 3.2 we assume that the source used for SK generation is not perfectly known. Thus now we consider the RVs X and $\{Y_s\}_{s\in\mathcal{S}}$ (where $\mathcal{S}$ is a possibly infinite set). The source puts out RVs $X^n = (X_1, \cdots, X_n)$ observed at terminal $\mathcal{X}$ and $Y_s^n = (Y_{s,1}, \cdots, Y_{s,n})$ observed at terminal $\mathcal{Y}$ for a $s \in \mathcal{S}$ and we assume $P_{X^nY_s^n} = P_{XY_s}^{\otimes n}$. This means we still consider a DMMS but now the distribution of the corresponding generic RVs is not known. Instead we know that this distribution is an element of the set $\{P_{XY_s}\}_{s\in\mathcal{S}}$. This is called a compound DMMS.

Taking into account that we now allow for randomized encoders the generation of the SK K and the helper message M from X^n is described by a stochastic matrix $F \in \mathcal{P}(\mathcal{K}\times\mathcal{M}|\mathcal{X}^n)$. For the reconstruction of the SK we have to consider a set of RVs $\{\hat{K}_s\}_{s\in\mathcal{S}}$ that represent the reconstruction for each possible source statistic. The decoder is assumed to be a deterministic function $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$, i.e., $\hat{K}_s = g(Y_s^n, M)$ for all $s \in \mathcal{S}$. So here the pair (F, g) is a SK generation protocol.

The joint distributions of K, M and $\{\hat{K}_s\}_{s\in\mathcal{S}}$ are as follows. For all $(k, m, \hat{k}) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K}$ and $s \in \mathcal{S}$ we have

$$P_{KM\hat{K}_s}(k, m, \hat{k}) = \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} P_{XY_s}^{\otimes n}(x^n, y^n)F(k, m|x^n)\mathbb{1}_{g^{-1}(\hat{k})}((y^n, m)).$$

We adjust Definition 2.1 accordingly.

Definition 4.1. *Let $L \geqslant 0$. We call $R \geqslant 0$ an* achievable compound secret key rate with rate constraint L *if for any $\epsilon > 0$ and sufficiently large n there is a SK generation*

protocol such that

$$\sup_{s\in\mathcal{S}} Pr(K \neq \hat{K}_s) \leqslant \epsilon \tag{4.1}$$
$$H(K|M) = \log|\mathcal{K}|$$
$$\tfrac{1}{n}\log|\mathcal{K}| \geqslant R - \epsilon$$
$$\tfrac{1}{n}\log|\mathcal{M}| \leqslant L + \epsilon. \tag{4.2}$$

The compound SK capacity with rate constraint L *is the largest achievable compound secret key rate with rate constraint* L *and is denoted by* $C_{SK}^{comp}(L)$.

As discussed in Chapter 3 models that take source uncertainty into account are important from a practical point of view and can also be interpreted as models for a jammed source.

Our first result is the following characterization of $C_{SK}^{comp}(L)$.

Theorem 4.1. *It holds that*

$$C_{SK}^{comp}(L) = \max_{U} \inf_{s\in\mathcal{S}} I(U \wedge Y_s)$$

where the maximization is over all RVs U *such that* $U - X - Y_s$ *and* $I(U \wedge X) - \inf_{s\in\mathcal{S}} I(U \wedge Y_s) \leqslant L$ *for all* $s \in \mathcal{S}$.

Proof. The converse follows from Theorem 3.4. There SK generation protocols are considered that instead of (4.2) meet the requirement

$$\tfrac{1}{n} I(X^n \wedge M) \leqslant L + \delta.$$

From $I(X^n \wedge M) \leqslant \log|\mathcal{M}|$ it is clear that the corresponding converse result implies the converse part of Theorem 4.1.

The achievability follows directly from Lemma 4.4 below.

■

For the special case where $|\{P_{XY_s}\}_{s\in\mathcal{S}}| = 1$ Theorem 4.1 shows that replacing (2.2) and (2.3) by the requirement $H(K|M) = \log|\mathcal{K}|$ does not decrease $C_{SK}(L)$ (cf. Theorem 2.1).

As explained, we can assume that the source statistics are chosen by a jammer. As the helper message is transmitted publicly we could assume that the jammer knows the helper message. So the jammer can choose the source statistics based on the helper message. (This attack scenario makes sense because the marginal distribution of the source output available at terminal $\mathcal{X}$, which is used to generate K and M, is the same for all distributions that the jammer can choose.) So we can replace (4.1) by the stronger requirement

$$\sum_{m\in\mathcal{M}} P_M(m) \sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s | M = m) \leqslant \epsilon.$$

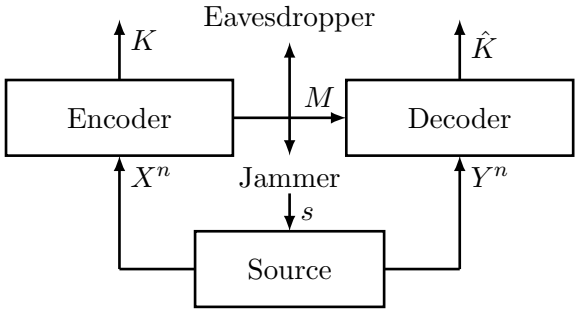

Figure 4.1: SK generation from a jammed source, where the jammer knows the helper message.

The setting that we consider is depicted in Figure 4.1. We denote the corresponding capacity by $C_{SK}^{comp,m}(L)$. Our next result is the characterization of $C_{SK}^{comp,m}(L)$.

Theorem 4.2. *It holds that*

$$C_{SK}^{comp,m}(L) = C_{SK}^{comp}(L).$$

So the SK capacity does not decrease, even if the jammer knows the helper message and chooses the source statistics based on the helper message.

Proof. The achievability part of the proof follows directly from Lemma 4.5 below. The converse part is clear from the converse part of Theorem 4.1.

■

4.2 Achievability proofs for the compound source

In order to prove Lemma 4.4 (which basically is the achievability part of Theorem 4.1) we need the following lemma.

Lemma 4.3. *Let U, X be RVs with $P_{UX} \in \mathcal{P}(\bar{n},\mathcal{U} \times \mathcal{X})$ for some $\bar{n} \in \mathbb{N}$ such that $H(U|X) > 0$. Choose a $\delta > 0$ such that $\delta < H(U|X)$. Choose real numbers ϵ, R satisfying $R, \epsilon > 0$. For any $n \in \mathbb{N}$, define integers K, L, M satisfying*

$$\begin{aligned} L = KM &= \exp(\lceil n(I(U \wedge X) + \delta)\rceil) \\ K &= \exp(\lceil nR\rceil). \end{aligned}$$

Then there exist constants $c_1, c_2 > 0$ such that for every sufficiently large multiple n of $\bar{n}$ there is a set $\mathcal{J} = \{u_{k,m}\}_{(k,m)\in[K]\times[M]} \subset \mathcal{T}_U^n$ satisfying

$$(1 - \exp(-nc_1))\frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|}L < |\mathcal{J} \cap \mathcal{T}_{U|X}^n(x^n)| < (1 + \exp(-nc_1))\frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|}L \qquad (4.3)$$

for all $x^n \in \mathcal{T}_X^n$. *Moreover, let* Y *be any additional RV with*

$$P_{UXY}(u,x,y) = P_{UX}(u,x)P_{Y|X}(y|x)$$

for all $(u,x,y) \in \mathcal{U} \times \mathcal{X} \times \mathcal{Y}$ *and* $R < I(U \wedge Y) - \epsilon$. *For* $k \in [K]$, $m \in [M]$ *we define*

$$\mathcal{D}_{k,m} := \bigcup_{\substack{q \in [K] \\ q \neq k}} \{y^n \colon I(y^n \wedge u_{k,m}) \leqslant I(y^n \wedge u_{q,m})\}.$$

Then

$$\bar{e}_m := \tfrac{1}{K} \sum_{k \in [K]} P_{Y|U}^{\otimes n}(\mathcal{D}_{k,m}|u_{k,m}) \leqslant \exp(-nc_2), \tag{4.4}$$

for all $m \in [M]$.

The proof technique is based on [23, Poof of Theorem IV.1] and [24, Proof of Lemma 3].

Proof. It is clear that $P_{UX} \in \mathcal{P}(n, \mathcal{U} \times \mathcal{X})$. We randomly choose $u_1, \cdots, u_L$ from $\mathcal{T}_U^n$ without replacement according to a uniform distribution and let $u_{k,m} = u_{K(m-1)+k}$ for all $(k,m) \in [K] \times [M]$. Denote the corresponding RVs by $U_1, \cdots, U_L$. Consider $x^n \in \mathcal{T}_X^n$ and the RV $Z_{x^n} = \sum_{l \in [L]} Z_{x^n}^l$ with $Z_{x^n}^l = \mathbb{1}_{\mathcal{T}_{U|X}^n(x^n)}(U_l)$ for $l \in [L]$. So Z_{x^n} is hypergeometrically distributed such that $Z_{x^n} \sim H(|\mathcal{T}_U^n|, |\mathcal{T}_{U|X}^n(x^n)|, L)$. From [38] we know that for $0 < \zeta < 1$

$$\Pr(|Z_{x^n} - \tfrac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L| \geqslant \zeta \tfrac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L) \leqslant 2e^{-\zeta^2 \frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L/4}.$$

This can be upper bounded by

$$\begin{aligned} &2e^{-\frac{\zeta^2}{4} \exp(-nI(U \wedge X))(n+1)^{-|\mathcal{X}||\mathcal{U}|} \exp([n(I(U \wedge X)+\delta)])} \\ &\leqslant 2e^{-\frac{\zeta^2}{2}(n+1)^{-|\mathcal{X}||\mathcal{U}|} \exp(n\delta)} \end{aligned}$$

using the definition of L and bounds on the corresponding type classes, cf. [26]. So we can choose $\zeta = \exp(-nc_1)$ for

$$0 < c_1 < \tfrac{1}{2}(\delta - \tfrac{|\mathcal{X}||\mathcal{U}|}{n} \log(n+1)),$$

e.g. $c_1 = \frac{\delta}{4}$ for n large enough such that

$$\tfrac{\delta}{2} > \tfrac{|\mathcal{X}||\mathcal{U}|}{n} \log(n+1),$$

and get

$$\Pr(|Z_{x^n} - \tfrac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L| \geqslant \zeta \tfrac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L) \leqslant 2e^{-\exp(n\delta/4)/2}.$$

Now consider $u^n \in \mathcal{T}_U^n$ and the RV $\bar{U}$ such that $P_{U\bar{U}} \in \mathcal{P}(n, \mathcal{U} \times \mathcal{U})$ and $P_{\bar{U}} = P_U$. We define

$$f_{k,m}^{(P_{U\bar{U}}, u^n)}(U_{1,m}, \cdots, U_{k,m}) = \mathbb{1}_{\mathcal{T}_{\bar{U}|U}^n(u^n)}(U_{k,m})$$

for all $k \in [K]$ and $m \in [M]$. Consider

$$\sum_{u_{k,m} \in \mathcal{T}_U^n} f_{k,m}^{(P_{U\bar{U}}, u^n)}(u_{1,m}, \cdots, u_{k,m}) \cdot P_{U_{k,m}|U_{1,m}, \cdots, U_{k-1,m}}(u_{k,m}|u_{1,m}, \cdots, u_{k-1,m}) \tag{4.5}$$

which equals

$$\sum_{u_{k,m} \in \mathcal{T}_U^n} \sum_{\substack{\mathbf{u}_{1,1}^{K,m-1} \\ \in (\mathcal{T}_U^n)^{K(m-1)}}} \mathbb{1}_{\mathcal{T}_{\bar{U}|U}^n(u^n)}(u_{k,m}) P_{U_{k,m}|U_{1,1}, \cdots, U_{k-1,m}}(u_{k,m}|u_{1,1}, \cdots, u_{k-1,m}) \cdot P_{\mathbf{U}_{1,1}^{K,m-1}|\mathbf{U}_{1,m}^{k-1,m}}(\mathbf{u}_{1,1}^{K,m-1}|\mathbf{u}_{1,m}^{k-1,m}),$$

where we introduce the notation

$$\begin{aligned} \mathbf{U}_{1,1}^{K,m-1} &= (U_{1,1}, \cdots, U_{K,m-1}) \\ \mathbf{U}_{1,m}^{k-1,m} &= (U_{1,m}, \cdots, U_{k-1,m}) \\ \mathbf{u}_{1,1}^{K,m-1} &= (u_{1,1}, \cdots, u_{K,m-1}) \\ \mathbf{u}_{1,m}^{k-1,m} &= (u_{1,m}, \cdots, u_{k-1,m}) \end{aligned} \tag{4.6}$$

We can exchange the sums and get

$$\sum_{\substack{\mathbf{u}_{1,1}^{K,m-1} \\ \in (\mathcal{T}_U^n)^{K(m-1)}}} P_{\mathbf{U}_{1,1}^{K,m-1}|\mathbf{U}_{1,m}^{k-1,m}}(\mathbf{u}_{1,1}^{K,m-1}|\mathbf{u}_{1,m}^{k-1,m}) \sum_{u_{k,m} \in \mathcal{T}_U^n} \mathbb{1}_{\mathcal{T}_{\bar{U}|U}^n(u^n)}(u_{k,m}) P_{U_{k,m}|U_{1,1}, \cdots, U_{k-1,m}}(u_{k,m}|u_{1,1}, \cdots, u_{k-1,m})$$

which equals

$$\begin{aligned} &\sum_{\substack{\mathbf{u}_{1,1}^{K,m-1} \\ \in (\mathcal{T}_U^n)^{K(m-1)}}} P_{\mathbf{U}_{1,1}^{K,m-1}|\mathbf{U}_{1,m}^{k-1,m}}(\mathbf{u}_{1,1}^{K,m-1}|\mathbf{u}_{1,m}^{k-1,m}) \frac{|\mathcal{T}_{\bar{U}|U}^n(u^n) \setminus \{u_{1,1}, \cdots, u_{k-1,m}\}|}{|\mathcal{T}_U^n| - (K(m-1)+k-1)} \\ &\leqslant \frac{|\mathcal{T}_{\bar{U}|U}^n(u^n)|}{|\mathcal{T}_U^n| - KM} \leqslant \frac{\exp(-nI(\bar{U} \wedge U))(n+1)^{|\mathcal{U}|}}{1 - 2\exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}}. \end{aligned} \tag{4.7}$$

So we can apply Lemma [24, Lemma A 1] with

$$a = \frac{\exp(-nI(\bar{U}\wedge U))(n+1)^{|\mathcal{U}|}}{1-2\exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}}.$$

We thus get for all $m \in [M]$ and

$$Z^m_{(P_{U\bar{U}},u^n)} = \sum_{k\in[K]} f^{(P_{U\bar{U}},u^n)}_{k,m}(U_{1,m},\cdots,U_{k,m})$$

that

$$\Pr(Z^m_{(P_{U\bar{U}},u^n)} > Kt) \leqslant \exp(-K(t - a\log e)).$$

Choose

$$t = \tfrac{1}{K}\exp(n(|R - I(\bar{U}\wedge U)|^+ + \epsilon)).$$

So $K(t - a\log e) \geqslant \exp(n\epsilon)/2$ if $n \geqslant n_1(\epsilon)$ where $n_1(\epsilon)$ is defined as

$$\min\{n\colon 0 < \tfrac{2(n+1)^{|\mathcal{U}|}\log e}{1-2\exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}} < \tfrac{1}{2}\exp(n\epsilon)\}.$$

As $|\mathcal{T}^n_U|$, $|\mathcal{T}^n_X|$, $|\mathcal{P}(n,\mathcal{U}\times\mathcal{U})|$ and M only increase exponentially with respect to n we can use the union bound to show that the probability that $\mathcal{J}$ has the following properties is greater than 0. This follows as we showed that the probabilities of the corresponding complementary events each go to 0 doubly exponentially with respect to n. So for all n large enough there is a $\mathcal{J}$ such that (4.3) holds for all $x^n \in \mathcal{T}^n_X$ and for all $m \in [M]$, all $u^n \in \mathcal{T}^n_U$ and all $P_{U\bar{U}} \in \mathcal{P}(n,\mathcal{U}\times\mathcal{U})$ we have

$$|\{k\colon u_{k,m} \in \mathcal{T}^n_{\bar{U}|U}(u^n)\}| \leqslant \exp(n(|R - I(\bar{U}\wedge U)|^+ + \epsilon)). \tag{4.8}$$

For each $y^n \in \mathcal{Y}^n$ there is a RV $\hat{Y}$ such that $(u_{k,m}, y^n) \in \mathcal{T}^n_{U\hat{Y}}$. So there is a set of RVs $\{\hat{Y}_1,\cdots,\hat{Y}_P\}$ with $P \leqslant |\mathcal{P}(n,\mathcal{U}\times\mathcal{Y})|$ such that $\{\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m})\}_{p\in[P]}$ forms a partition of $\mathcal{Y}^n$. So for each $m \in [M]$ we can write $\bar{e}_m$ defined in (4.4) as

$$\begin{aligned}
&\tfrac{1}{K}\sum_{k\in[K]} P^{\otimes n}_{Y|U}(\bigcup_{p\in[P]} \mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \mathcal{D}_{k,m}|u_{k,m})\\
&= \sum_{p\in[P]} \tfrac{1}{K}\sum_{k\in[K]} P^{\otimes n}_{Y|U}(\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \mathcal{D}_{k,m}|u_{k,m})\\
&= \sum_{p\in[P]} \tfrac{1}{K}\sum_{k\in[K]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U) + H(\hat{Y}_p|U))|\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \mathcal{D}_{k,m}|.
\end{aligned}$$

For each

$$y^n \in \mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \{y^n\colon I(y^n \wedge u_{k,m}) \leqslant I(y^n \wedge u_{q,m})\},$$

$q \in [K]$ and $q \neq k$, there is a RV $\bar{U}$ with $I(\hat{Y}_p \wedge U) \leqslant I(\hat{Y}_p \wedge \bar{U})$ and $P_{\bar{U}} = P_U$ such that $(y^n, u_{k,m}, u_{q,m}) \in \mathcal{T}^n_{\hat{Y}_p U \bar{U}}$. So there is a set of RVs $\{\bar{U}^p_1, \cdots, \bar{U}^p_{O_p}\}$ with

$$O_p \leqslant |\mathcal{P}(n, \mathcal{Y} \times \mathcal{U} \times \mathcal{U})|$$

such that $\{\mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m})\}_{o\in[O_p]}$ forms a partition of

$$\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \{y^n \colon I(y^n \wedge u_{k,m}) \leqslant I(y^n \wedge u_{q,m})\}$$

and $I(\hat{Y}_p \wedge U) \leqslant I(\hat{Y}_p \wedge \bar{U}^p_o)$, $P_{\bar{U}^p_o} = P_U$. We can write

$$\begin{aligned}
\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \mathcal{D}_{k,m} &= \bigcup_{\substack{q\in[K]\\ q\neq k}} (\mathcal{T}^n_{\hat{Y}_p|U}(u_{k,m}) \cap \{y^n \colon I(y^n \wedge u_{k,m}) \leqslant I(y^n \wedge u_{q,m})\}) \\
&= \bigcup_{\substack{q\in[K]\\ q\neq k}} \bigcup_{o\in[O_p]} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m}) \\
&= \bigcup_{o\in[O_p]} \bigcup_{\substack{q\in[K]\\ q\neq k}} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m}).
\end{aligned}$$

So

$$\bar{e}_m \leqslant \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \sum_{o\in[O_p]} \tfrac{1}{K} \sum_{k\in[K]} \frac{|\bigcup_{q\in[K],q\neq k} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|}{\exp(nH(\hat{Y}_p|U)))}.$$

It is clear that an upper bound for

$$\frac{|\bigcup_{q\in[K],q\neq k} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|}{\exp(nH(\hat{Y}_p|U)))}$$

is 1. So we have

$$\begin{aligned}
\bar{e}_m \leqslant & \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \\
& \cdot \sum_{o\in[O_p]} \tfrac{1}{K} \sum_{k\in[K]} \min\{\frac{|\bigcup_{q\in[K],q\neq k} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|}{\exp(nH(\hat{Y}_p|U)))}, 1\}.
\end{aligned}$$

As $\mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m}) = \varnothing$ for $(u_{k,m}, u_{q,m}) \notin \mathcal{T}^n_{U\bar{U}^p_o}$ we have

$$\bigcup_{q\in[K],q\neq k} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m}) = \bigcup_{\substack{q\in[K]\colon q\neq k\\ \wedge(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}}} \mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m}, u_{q,m})$$

and thus

$$|\bigcup_{q\in[K],q\neq k}\mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|\leqslant\sum_{\substack{q\in[K]\colon q\neq k\\ \wedge(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}}}|\mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|. \tag{4.9}$$

As

$$\frac{|\mathcal{T}^n_{\hat{Y}_p|U\bar{U}^p_o}(u_{k,m},u_{q,m})|}{\exp(nH(\hat{Y}_p|U))}\leqslant\frac{\exp(nH(\hat{Y}_p|U\bar{U}^p_o))}{\exp(nH(\hat{Y}_p|U))}=\exp(-n(I(\bar{U}^p_o\wedge U\hat{Y}_p)-I(U\wedge\bar{U}^p_o)))$$

we can upper bound (4.9) by

$$\frac{|\{q\neq k\colon(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}\}|}{\exp(n(I(\bar{U}^p_o\wedge U\hat{Y}_p)-I(U\wedge\bar{U}^p_o)))}$$

and thus

$$\begin{aligned}\bar{e}_m\leqslant&\sum_{p\in[P]}\exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U)))\\&\cdot\sum_{o\in[O_p]}\frac{1}{K}\sum_{k\in[K]}\min\{\frac{|\{q\neq k\colon(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}\}|}{\exp(n(I(\bar{U}^p_o\wedge U\hat{Y}_p)-I(U\wedge\bar{U}^p_o)))},1\}\end{aligned}$$

which can be upper bounded by

$$\begin{aligned}&\sum_{p\in[P]}\exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U)))\\&\qquad\cdot(\sum_{\substack{o\in[O_p]\colon\\ I(U\wedge\bar{U}^p_o)>R}}\frac{1}{K}\sum_{k\in[K]}\frac{|\{q\neq k\colon(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}\}|}{\exp(n(I(\bar{U}^p_o\wedge U\hat{Y}_p)-I(U\wedge\bar{U}^p_o)))}\\&+\sum_{\substack{o\in[O_p]\colon\\ I(U\wedge\bar{U}^p_o)\leqslant R}}\frac{1}{K}\sum_{k\in[K]}\min\{\frac{|\{q\neq k\colon(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}\}|}{\exp(n(I(\bar{U}^p_o\wedge U\hat{Y}_p)-I(U\wedge\bar{U}^p_o)))},1\}).\end{aligned}$$

We have with (4.8)

$$|\{q\neq k\colon(u_{k,m},u_{q,m})\in\mathcal{T}^n_{U\bar{U}^p_o}\}|\leqslant\exp(n(|R-I(U\wedge\bar{U}^p_o)|^+\epsilon)).$$

For $I(U\wedge\bar{U}^p_o)>R$ this equals $\exp(n\epsilon)$ and for $I(U\wedge\bar{U}^p_o)\leqslant R$ it equals $R-I(U\wedge\bar{U}^p_o)$,

so

$$\begin{aligned}\bar{e}_m \leqslant & \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \\ & \cdot \Big(\sum_{\substack{o\in[O_p]:\\ I(U\wedge\bar{U}_o^p)>R}} \min\{\tfrac{\exp(n\epsilon))}{\exp(n(I(\bar{U}_o^p\wedge U\hat{Y}_p)-I(U\wedge\bar{U}_o^p)))}, 1\} \\ & \quad + \sum_{\substack{o\in[O_p]:\\ I(U\wedge\bar{U}_o^p)\leqslant R}} \min\{\tfrac{\exp(n(R-I(U\wedge\bar{U}_o^p)+\epsilon))}{\exp(n(I(\bar{U}_o^p\wedge U\hat{Y}_p)-I(U\wedge\bar{U}_o^p)))}, 1\}\Big).\end{aligned}$$

For $I(U\wedge\bar{U}_o^p) > R$ we have

$$\begin{aligned}& \exp(n\epsilon)\exp(-n(I(\bar{U}_o^p\wedge U\hat{Y}_p) - I(U\wedge\bar{U}_o^p))) \\ & \leqslant \exp(-n(I(\bar{U}_o^p\wedge\hat{Y}_p) - I(U\wedge\bar{U}_o^p) - \epsilon)) \\ & < \exp(-n(I(\bar{U}_o^p\wedge\hat{Y}_p) - R - \epsilon)).\end{aligned}$$

So we have

$$\begin{aligned}\bar{e}_m \leqslant & \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \\ & \cdot \Big(\sum_{\substack{o\in[O_p]:\\ I(U\wedge\bar{U}_o^p)>R}} \min\{\exp(-n(I(\bar{U}_o^p\wedge\hat{Y}_p) - R - \epsilon)), 1\} \\ & + \sum_{\substack{o\in[O_p]:\\ I(U\wedge\bar{U}_o^p)\leqslant R}} \min\{\exp(-n(I(\hat{Y}_pU\wedge\bar{U}_o^p) - R - \epsilon)), 1\}\Big)\end{aligned}$$

which can be upper bounded by

$$\begin{aligned}& \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \sum_{o\in[O_p]} \min\{\exp(-n(I(\bar{U}_o^p\wedge\hat{Y}_p) - R - \epsilon)), 1\} \\ & \leqslant \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U))) \sum_{o\in[O_p]} \min\{\exp(-n(I(U\wedge\hat{Y}_p) - R - \epsilon)), 1\}\end{aligned}$$

which is less or equal than

$$\begin{aligned}& (n+1)^{|\mathcal{Y}||\mathcal{U}|^2} \sum_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U)))\exp(-n|I(\hat{Y}_p\wedge U) - R - \epsilon|^+) \\ & \leqslant (n+1)^{|\mathcal{Y}|^2|\mathcal{U}|^3} \max_{p\in[P]} \exp(-n(D(P_{\hat{Y}_p|U}\|P_{Y|U}|P_U)))\exp(-n|I(\hat{Y}_p\wedge U) - R - \epsilon|^+) \\ & \leqslant (n+1)^{|\mathcal{Y}|^2|\mathcal{U}|^3} \max_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{U})} \exp(-n(D(V\|P_{Y|U}|P_U)))\exp(-n|I(P_U,V) - R - \epsilon|^+)\end{aligned}$$

This implies that for all $P_{Y|U}$ such that $I(Y \wedge U) - \epsilon > R$ we have $\bar{e}_m \leqslant \exp(-nc_2)$.

■

Now we can prove Lemma 4.4.

Lemma 4.4. *Consider the RVs $\tilde{X}$ and $\{\tilde{Y}_s\}_{s\in\mathcal{S}}$ with $P_{\tilde{X}\tilde{Y}_s} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ for all $s \in \mathcal{S}$ and a RV $\tilde{U}$ such that $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$, $P_{\tilde{U}} \in \mathcal{P}(\mathcal{U})$. Let $\delta > 0$. For all n large enough there is a stochastic matrix $F \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}|\mathcal{X}^n)$ and a mapping $g\colon \mathcal{Y}^n \times \bar{\mathcal{M}} \to \mathcal{K}$ such that for the RVs K, $\bar{M}$, $\{\hat{K}_s\}_{s\in\mathcal{S}}$ and $\tilde{X}^n$ with $P_{K\bar{M}\hat{K}_s\tilde{X}^n} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n)$ for all $s \in \mathcal{S}$ defined by*

$$P_{K\bar{M}\hat{K}_s\tilde{X}^n}(k,\bar{m},\hat{k},x^n) = \sum_{y^n\in\mathcal{Y}^n} P^{\otimes n}_{\tilde{X}\tilde{Y}_s}(x^n,y^n)F(k,\bar{m}|x^n)\mathbb{1}_{g^{-1}(\hat{k})}((y^n,\bar{m}))$$

for $(k,\bar{m},\hat{k},x^n) \in \mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n$ it holds that

$$\sup_{s\in\mathcal{S}} Pr(K \neq \hat{K}_s) \leqslant \delta \tag{4.10}$$

$$H(K|\bar{M}) = \log|\mathcal{K}| \tag{4.11}$$

$$\frac{1}{n}\log|\mathcal{K}| \geqslant \inf_{s\in\mathcal{S}} I(\tilde{U}\wedge\tilde{Y}_s) - \delta$$

$$\frac{1}{n}\log|\bar{\mathcal{M}}| \leqslant I(\tilde{U}\wedge\tilde{X}) - \inf_{s\in\mathcal{S}} I(\tilde{U}\wedge\tilde{Y}_s) + \delta.$$

Proof. Assume first that $H(\tilde{U}|\tilde{X}) > 0$. The case $H(\tilde{U}|\tilde{X}) = 0$ is treated at the end of the proof. We can also assume that $\inf_{s\in\mathcal{S}} I(\tilde{U}\wedge\tilde{Y}_s) > 0$, because the result follows trivially for $\inf_{s\in\mathcal{S}} I(\tilde{U}\wedge\tilde{Y}_s) = 0$. Let $\delta_1, \delta_2 > 0$ small enough.

Consider sets of RVs $\{X_t\}_{t\in[T]}$ and $\{U_t\}_{t\in[T]}$ with $T \leqslant |\mathcal{P}(n,\mathcal{X})|$ such that $P_{U_tX_t\tilde{Y}_s} \in \mathcal{P}(\mathcal{U}\times\mathcal{X}\times\mathcal{Y})$ and $P_{U_tX_t} \in \mathcal{P}(n,\mathcal{U}\times\mathcal{X})$, $P_{U_tX_t\tilde{Y}_s}(u,x,y) = P_{\tilde{Y}_s|\tilde{X}}(y|x)P_{U_tX_t}(u,x)$ for all $(u,x,y) \in \mathcal{U}\times\mathcal{X}\times\mathcal{Y}$ for all $s \in \mathcal{S}$ and $t \in [T]$ while $\{\mathcal{T}^n_{X_t}\}_{t\in[T]}$ forms a partition of $\mathcal{T}^n_{\tilde{X},\delta_1}$ and

$$|P_{U_tX_t}(u,x) - P_{\tilde{U}\tilde{X}}(u,x)| \leqslant \delta_1 + \delta_2$$

for all $(u,x) \in \mathcal{U}\times\mathcal{X}$ for all $t \in [T]$. Such RVs exist which can be seen as follows. First choose $\{X_t\}_{t\in[T]}$. Then consider $\{x_t\}_{t\in[T]}$ with $x_t \in \mathcal{T}^n_{X_t}$ for all $t \in [T]$. For each $t \in [T]$ choose a $u_t \in \mathcal{T}^n_{\tilde{U}|\tilde{X},\delta_2}(x_t)$. Define the RVs $\{U_t\}_{t\in[T]}$ with $P_{U_tX_t} = P_{u_t,x_t} \in \mathcal{P}(n,\mathcal{U}\times\mathcal{X})$. (This choice of $P_{U_tX_t}$ is possible for n large enough, cf. [26, Chapter 2].)

From [26, Lemma 2.7] we know that for all $t \in [T]$ it holds that $H(U_t|X_t) > 0$ and $\inf_{s\in\mathcal{S}} I(U_t\wedge\tilde{Y}_s) > 0$ for δ_1, δ_2 small enough.

For each $t \in [T]$ generate the set $\mathcal{J}_t$ according to Lemma 4.3 with

$$R = \min_{t\in[T]} \inf_{s\in\mathcal{S}} I(U_t\wedge\tilde{Y}_s) - \delta/2,$$

(and the corresponding K, M_t and L_t). For all $t \in [T]$ define for all $u^n \in \mathcal{J}_t$

$$\begin{aligned}\tilde{Q}_t(u^n) &= \sum_{x^n \in \mathcal{X}^n} \frac{1}{|\mathcal{T}^n_{X_t}|} \frac{\mathbb{1}_{\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)}(u^n)}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|} \\ &= \sum_{x^n \in \mathcal{X}^n} \frac{1}{|\mathcal{T}^n_{X_t}|} \frac{\mathbb{1}_{\mathcal{T}^n_{U_t|X_t}(x^n)}(u^n)}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|} \\ &= \sum_{x^n \in \mathcal{T}^n_{X_t|U_t}(u^n)} \frac{1}{|\mathcal{T}^n_{X_t}||\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|}\end{aligned}$$

and $Q_t = \min_{u^n \in \mathcal{J}_t} \tilde{Q}_t(u^n)$. From (4.3) we know that for $t \in [T]$ and all $u^n \in \mathcal{J}_t$

$$\frac{1}{1+\exp(-nc_1)} \frac{1}{L_t} < \tilde{Q}_t(u^n) < \frac{1}{1-\exp(-nc_1)} \frac{1}{L_t}. \tag{4.12}$$

Here we also use that

$$|\mathcal{T}^n_{U_t}||\mathcal{T}^n_{X_t|U_t}(u^n)| = |\mathcal{T}^n_{X_t}||\mathcal{T}^n_{U_t|X_t}(x^n)| = |\mathcal{T}^n_{U_tX_t}|$$

for $u^n \in \mathcal{T}^n_{U_t}$ and $x^n \in \mathcal{T}^n_{X_t}$. Let $u^* \in \mathcal{U}^n \backslash \bigcup_{t\in[T]} \mathcal{J}_t$. Consider the RV U_n, $P_{U_n} \in \mathcal{P}(\mathcal{U}^n)$. We define U_n such that for all $t \in [T]$ it holds that

$$P_{U_n|\tilde{X}^n}(u^n|x^n) = \frac{Q_t}{\tilde{Q}_t(u^n)} \frac{1}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|}$$

for $x^n \in \mathcal{T}^n_{X_t}$ and $u^n \in \mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)$,

$$P_{U_n|\tilde{X}^n}(u^n|x^n) = 1 - \sum_{u \in \mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)} \frac{Q_t}{\tilde{Q}_t(u)} \frac{1}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|}$$

for $x^n \in \mathcal{T}^n_{X_t}$ and $u^n = u^*$ and

$$P_{U_n|\tilde{X}^n}(u^n|x^n) = 0$$

for $x^n \in \mathcal{T}^n_{X_t}$ and all other $u^n \in \mathcal{U}^n$. For $x^n \in \mathcal{X}^n \backslash \bigcup_{t\in[T]} \mathcal{T}^n_{X_t}$ define

$$P_{U_n|\tilde{X}^n}(u^n|x^n) = \begin{cases} 1 & u^n = u^* \\ 0 & \text{else} \end{cases}.$$

We have for $t \in [T]$ and all $u^n \in \mathcal{J}_t$

$$\begin{aligned}\Pr(U_n = u^n|\tilde{X}^n \in \mathcal{T}^n_{X_t}) &= \sum_{x^n \in \mathcal{T}^n_{X_t}} \Pr(U_n = u^n|\tilde{X}^n = x^n)\Pr(\tilde{X}^n = x^n|\tilde{X}^n \in \mathcal{T}^n_{X_t}) \\ &= \sum_{x^n \in \mathcal{T}^n_{X_t}} \Pr(U_n = u^n|\tilde{X}^n = x^n)\tfrac{1}{|\mathcal{T}^n_{X_t}|} \\ &= \sum_{x^n \in \mathcal{X}^n} \tfrac{Q_t}{\tilde{Q}_t(u^n)} \tfrac{\mathbb{1}_{\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)}(u^n)}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|} \tfrac{1}{|\mathcal{T}^n_{X_t}|} = Q_t. \end{aligned} \tag{4.13}$$

For $t \in [T]$ and all $x^n \in \mathcal{T}^n_{X_t}$ we have by (4.12)

$$\begin{aligned}\Pr(U_n \neq u^*|\tilde{X}^n = x^n) &= \sum_{u \in \mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)} \tfrac{Q_t}{\tilde{Q}_t(u)} \tfrac{1}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|} \\ &> L_t(1 - \exp(-nc_1))Q_t \\ &> \tfrac{1-\exp(-nc_1)}{1+\exp(-nc_1)} = 1 - \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)}. \end{aligned} \tag{4.14}$$

Now we consider for $t \in [T]$, $u^n \in \mathcal{J}_t$ and $(x^n, u^n) \in \mathcal{T}^n_{X_tU_t}$

$$\Pr(\tilde{X}^n = x^n|\tilde{X}^n \in \mathcal{T}^n_{X_t}, U_n = u^n) = \tfrac{\Pr(\tilde{X}^n = x^n, U_n = u^n|\tilde{X}^n \in \mathcal{T}^n_{X_t})}{\Pr(U_n = u^n|\tilde{X}^n \in \mathcal{T}^n_{X_t})}$$

which equals

$$\begin{aligned}\tfrac{\Pr(\tilde{X}^n = x^n|\tilde{X}^n \in \mathcal{T}^n_{X_t})\Pr(U_n = u^n|\tilde{X}^n = x^n)}{Q_t} &= \tfrac{Q_t}{\tilde{Q}_t(u^n)} \tfrac{1}{|\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|} \tfrac{1}{Q_t|\mathcal{T}^n_{X_t}|} \\ &= \tfrac{1}{|\mathcal{T}^n_{X_t}||\mathcal{J}_t \cap \mathcal{T}^n_{U_t|X_t}(x^n)|\tilde{Q}_t(u^n)}. \end{aligned}$$

From (4.3) and (4.12) this implies

$$\Pr(\tilde{X}^n = x^n|\tilde{X}^n \in \mathcal{T}^n_{X_t}, U_n = u^n) < \tfrac{1+\exp(-nc_1)}{1-\exp(-nc_1)} \tfrac{1}{|\mathcal{T}^n_{X_t|U_t}(u^n)|}. \tag{4.15}$$

We also know $\Pr(\tilde{X}^n = x^n|\tilde{X}^n \in \mathcal{T}^n_{X_t}, U_n = u^n) = 0$ for $x^n \in \mathcal{X}^n \backslash \mathcal{T}^n_{X_t|U_t}(u^n)$. Define $\mathcal{K} = [K]$, $\mathcal{M} = [\max_{t\in[T]} M_t]$ and $\bar{\mathcal{M}} = \mathcal{M} \times [T]$. Let $x^n \in \mathcal{T}^n_{X_t}$, $t \in [T]$. We define for $k \in \mathcal{K}$ and $m \in [M_t]$

$$F(k, (m, t)|x^n) = \Pr(U_n = u^t_{k,m}|\tilde{X}^n = x^n) + \Pr(U_n = u^*|\tilde{X}^n = x^n)\tfrac{1}{L_t},$$

where we denote the elements in $\mathcal{J}_t$ by $u^t_{k,m}$ for all $k \in [K]$ and $m \in [M_t]$. For $M_t < m \leqslant \max_{t\in[T]} M_t$ and $k \in \mathcal{K}$ we define

$$F(k, (m, t)|x^n) = 0.$$

For $\bar{t} \in [T]$, $\bar{t} \neq t$ we define for $(k, m) \in \mathcal{K} \times \mathcal{M}$

$$F(k, (m, \bar{t})|x^n) = 0.$$

Let $x^n \in \mathcal{X}^n \backslash \bigcup_{t \in [T]} \mathcal{T}^n_{X_t}$. We define

$$F(k, (m, t)|x^n) = \tfrac{1}{K \sum_{t \in [T]} M_t}$$

for all $(k, m, t) \in \mathcal{K} \times \mathcal{M} \times [T]$ with $m \leqslant M_t$. For $(k, m, t) \in \mathcal{K} \times \mathcal{M} \times [T]$ with $m > M_t$ we define

$$F(k, (m, t)|x^n) = 0.$$

We have not defined g yet, but nevertheless start analyzing the properties of F. We introduce the definition of g when needed. We start the analysis with the error probability. Let $s \in \mathcal{S}$. We have

$$\Pr(K \neq \hat{K}_s) \leqslant \sum_{t \in [T]} \Pr(K \neq \hat{K}_s | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) + \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X}, \delta_1}). \tag{4.16}$$

Thus we now consider $\Pr(K \neq \hat{K}_s | \tilde{X}^n \in \mathcal{T}^n_{X_t})$ for $t \in [T]$.

$$\begin{aligned}
\Pr(K \neq \hat{K}_s | \tilde{X}^n \in \mathcal{T}^n_{X_t}) = & \sum_{(m, \bar{t}) \in \mathcal{M} \times [T]} \sum_{\substack{k, \hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s | \tilde{X}}(y^n | x^n) \\
& \cdot F(k, (m, \bar{t})|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, (m, \bar{t})) \\
= & \sum_{m \in [M_t]} \sum_{\substack{k, \hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s | \tilde{X}}(y^n | x^n) \\
& \cdot F(k, (m, t)|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, (m, t)),
\end{aligned}$$

where we make use of the definition of $F(k, (m, t)|x^n)$. With our choice of $F(k, (m, t)|x^n)$ this equals

$$\begin{aligned}
& \sum_{m \in [M_t]} \sum_{\substack{k, \hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s | \tilde{X}}(y^n | x^n) \Pr(U_n = u^t_{k,m} | \tilde{X}^n = x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n, (m, t)) \\
+ & \sum_{m \in [M_t]} \sum_{\substack{k, \hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s | \tilde{X}}(y^n | x^n) \Pr(U_n = u^* | \tilde{X}^n = x^n) \tfrac{1}{L_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n, (m, t)).
\end{aligned}$$

Using (4.14) the second summand can be upper bounded by

$$\begin{aligned}
&\tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} \sum_{m\in[M_t]} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{L_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\
&\leqslant \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} \sum_{m\in[M_t]} \sum_{\hat{k}\in\mathcal{K}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{M_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\
&= \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} \sum_{m\in[M_t]} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{M_t} \\
&= \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)}.
\end{aligned}$$

The first summand equals

$$\begin{aligned}
&\sum_{m\in[M_t]} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \\
&\quad \cdot \Pr(U_n = u^t_{k,m}, \tilde{X}^n = x^n | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\
&= \sum_{m\in[M_t]} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \\
&\quad \cdot \Pr(\tilde{X}^n = x^n | U_n = u^t_{k,m}, \tilde{X}^n \in \mathcal{T}^n_{X_t}) \Pr(U_n = u^t_{k,m} | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).
\end{aligned}$$

Using (4.15) and (4.13) this can be upper bounded by

$$\tfrac{1+\exp(-nc_1)}{1-\exp(-nc_1)} \sum_{m\in[M_t]} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{|\mathcal{T}^n_{X_t|U_t}(u^t_{k,m})|} Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).$$

It is clear (cf. [26]) that for n large enough and $x^n \in \mathcal{T}^n_{X_t}$

$$\tfrac{1}{|\mathcal{T}^n_{X_t|U_t}(u^t_{k,m})|} \leqslant \tfrac{1}{\exp(n(H(X_t|U_t)-\xi))} = \exp(n\xi) P^{\otimes n}_{X_t|U_t}(x^n|u^t_{k,m}) \tag{4.17}$$

for $\xi > 0$. So we get the upper bound

$$\begin{aligned}
&\tfrac{1+\exp(-nc_1)}{1-\exp(-nc_1)} \exp(n\xi) \sum_{m\in[M_t]} \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \\
&\qquad \cdot P^{\otimes n}_{X_t|U_t}(x^n|u^t_{k,m}) Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).
\end{aligned} \tag{4.18}$$

We now define for $y^n \in \mathcal{Y}^n$, $t \in [T]$ and $m \in [M_t]$ the mapping g such that $g(y^n,(m,t)) = k$ (for $k \in \mathcal{K}$) satisfies

$$I(u^t_{m,k} \wedge y^n) = \max_{k\in\mathcal{K}} I(u^t_{m,k} \wedge y^n).$$

So using (4.12) we can upper bound (4.18) by

$$\tfrac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2}\exp(n\xi)\tfrac{1}{M_t}\sum_{m\in[M_t]}\tfrac{1}{K}\sum_{k\in\mathcal{K}}\sum_{x^n\in\mathcal{X}^n}P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(\mathcal{D}^t_{k,m}|x^n)P^{\otimes n}_{X_t|U_t}(x^n|u^t_{k,m}), \tag{4.19}$$

where

$$\mathcal{D}^t_{k,m}=\bigcup_{q\in\mathcal{K},q\neq k}\{y^n\colon I(y^n\wedge u^t_{k,m})\leqslant I(y^n\wedge u^t_{q,m})\}.$$

This equals

$$\tfrac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2}\exp(n\xi)\tfrac{1}{M_t}\sum_{m\in[M_t]}\tfrac{1}{K}\sum_{k\in\mathcal{K}}P^{\otimes n}_{\tilde{Y}_s|U_t}(\mathcal{D}^t_{k,m}|u^t_{k,m}) \tag{4.20}$$

From our choice of R we can upper bound this expression for all $s\in\mathcal{S}$ and $t\in[T]$ by

$$\tfrac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2}\exp(n\xi)\exp(-nc_2)=\exp(-nc_3)$$

for a $c_3>0$, n large enough and an appropriate choice of ξ. So

$$\begin{aligned}&\sum_{t\in[T]}\Pr(K\neq\hat{K}_s|\tilde{X}^n\in\mathcal{T}^n_{X_t})\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_t})\\&\leqslant\exp(-nc_3)\sum_{t\in[T]}\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_t})\leqslant\exp(-nc_3).\end{aligned}$$

Thus with (4.16) and [26, Lemma 2.12] overall the error probability goes to 0 exponentially with respect to n. Now we consider the secrecy requirement. For $k\in\mathcal{K}$ and $(m,t)\in\mathcal{M}\times[T]$ such that $m\in[M_t]$ consider

$$\begin{aligned}&\Pr(K=k,\bar{M}=(m,t))\\&=\sum_{\bar{t}\in[T]}\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n\in\mathcal{T}^n_{X_{\bar{t}}})\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_{\bar{t}}})\\&\qquad+\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n\in\mathcal{X}^n\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}^n_{X_{\bar{t}}})\Pr(\tilde{X}^n\in\mathcal{X}^n\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}^n_{X_{\bar{t}}})\\&=\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n\in\mathcal{T}^n_{X_t})\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_t})+\tfrac{1}{K\sum_{t\in[T]}M_t}\Pr(\tilde{X}^n\in\mathcal{X}^n\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}^n_{X_{\bar{t}}})\end{aligned}$$

where we use the properties of $F(k,(m,t)|x^n)$ for the last step. We have

$$\begin{aligned}
&\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n\in\mathcal{T}^n_{X_t})\\
&=\sum_{x^n\in\mathcal{T}^n_{X_t}}\tfrac{1}{|\mathcal{T}^n_{X_t}|}\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n=x^n)\\
&=\sum_{x^n\in\mathcal{T}^n_{X_t}}\tfrac{1}{|\mathcal{T}^n_{X_t}|}\Pr(U_n=u^t_{k,m}|\tilde{X}^n=x^n)+\sum_{x^n\in\mathcal{T}^n_{X_t}}\tfrac{1}{|\mathcal{T}^n_{X_t}|}\tfrac{1}{L_t}\Pr(U_n=u^*|\tilde{X}^n=x^n).
\end{aligned}$$

The first summand equals

$$\begin{aligned}
&\sum_{x^n\in\mathcal{T}^n_{X_t}}\Pr(\tilde{X}^n=x^n|\tilde{X}^n\in\mathcal{T}^n_{X_t})\Pr(U_n=u^t_{k,m}|\tilde{X}^n=x^n,\tilde{X}^n\in\mathcal{T}^n_{X_t})\\
&=\sum_{x^n\in\mathcal{T}^n_{X_t}}\Pr(\tilde{X}^n=x^n|U_n=u^t_{k,m},\tilde{X}^n\in\mathcal{T}^n_{X_t})\Pr(U_n=u^t_{k,m}|\tilde{X}^n\in\mathcal{T}^n_{X_t})=Q_t.
\end{aligned}$$

For the second summand we have

$$\tfrac{1}{L_t}\sum_{x^n\in\mathcal{T}^n_{X_t}}\Pr(U_n=u^*|\tilde{X}^n\in\mathcal{T}^n_{X_t})\Pr(\tilde{X}^n=x^n|U_n=u^*,\tilde{X}^n\in\mathcal{T}^n_{X_t}).$$

As

$$\sum_{u\in\mathcal{J}_t\cup\{u^*\}}\Pr(U_n=u|\tilde{X}^n=x^n)=1$$

we have

$$\Pr(U_n=u^*|\tilde{X}^n\in\mathcal{T}^n_{X_t})=1-L_tQ_t.$$

So we have

$$\Pr(K=k,\bar{M}=(m,t)|\tilde{X}^n\in\mathcal{T}^n_{X_t})=Q_t+\tfrac{1}{L_t}-Q_t=\tfrac{1}{L_t}. \tag{4.21}$$

Thus

$$\Pr(K=k,\bar{M}=(m,t))=\tfrac{1}{L_t}\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_t})+\tfrac{1}{K\sum_{t\in[T]}M_t}\Pr(\tilde{X}^n\in\mathcal{X}^n\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}^n_{X_{\bar{t}}})$$

and consequently

$$\Pr(\bar{M}=(m,t))=\tfrac{1}{M_t}\Pr(\tilde{X}^n\in\mathcal{T}^n_{X_t})+\tfrac{1}{\sum_{t\in[T]}M_t}\Pr(\tilde{X}^n\in\mathcal{X}^n\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}^n_{X_{\bar{t}}})$$

which implies

$$\Pr(K=k|\bar{M}=(m,t)) = \frac{\frac{1}{L_t}\Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) + \frac{1}{K\sum_{t\in[T]} M_t}\Pr(\tilde{X}^n \in \mathcal{X}^n \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}^n_{X_{\bar{t}}})}{\frac{1}{M_t}\Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) + \frac{1}{\sum_{t\in[T]} M_t}\Pr(\tilde{X}^n \in \mathcal{X}^n \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}^n_{X_{\bar{t}}})} = \frac{1}{K}.$$

So $H(K|\bar{M}) = \log|\mathcal{K}|$.

Finally we consider the cardinalities of $\mathcal{K}$ and $\bar{\mathcal{M}}$. From our choice of $P_{U_tX_t}$ we know that for all $t \in [T]$ it holds that

$$\|P_{U_tX_t} - P_{\tilde{U}\tilde{X}}\|_1 \leqslant (\delta_1+\delta_2)|\mathcal{U}||\mathcal{X}|.$$

This also implies for all $t \in [T]$ and all $s \in \mathcal{S}$ that

$$\|P_{U_t\tilde{Y}_s} - P_{\tilde{U}\tilde{Y}_s}\|_1 \leqslant (\delta_1+\delta_2)|\mathcal{U}||\mathcal{X}|.$$

Consequently [26, Lemma 2.7] implies for δ_1 and δ_2 small enough that

$$\max_{t\in[T]} I(U_t \wedge X_t) - \inf_{s\in\mathcal{S}} I(U_t \wedge \tilde{Y}_s) \leqslant I(\tilde{U} \wedge \tilde{X}) - \inf_{s\in\mathcal{S}} I(\tilde{U} \wedge \tilde{Y}_s) + \tau$$

and

$$\min_{t\in[T]} \inf_{s\in\mathcal{S}} I(U_t \wedge \tilde{Y}_s) \geqslant \inf_{s\in\mathcal{S}} I(\tilde{U} \wedge \tilde{Y}_s) - \tau$$

for a $\tau > 0$ arbitrarily small. So from our choice of R we know

$$\tfrac{1}{n}\log|\mathcal{K}| \geqslant \inf_{s\in\mathcal{S}} I(\tilde{U} \wedge \tilde{Y}_s) - \tau$$

and

$$\tfrac{1}{n}\log|\bar{\mathcal{M}}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \inf_{s\in\mathcal{S}} I(\tilde{U} \wedge \tilde{Y}_s) + \tau + \tfrac{|\mathcal{X}|}{n}\log(n+1),$$

where the last summand is an upper bound for $\frac{1}{n}\log T$.

We still have to consider the case $H(\tilde{U}|\tilde{X}) = 0$. It holds that $I(\tilde{U} \wedge \tilde{X}) = H(\tilde{U})$. For the protocol constructed in the proof of Theorem 3.3 we know

$$\tfrac{1}{n}\log|\mathcal{M}| \leqslant H(\tilde{U}) - \inf_{s\in\mathcal{S}} I(\tilde{U} \wedge \tilde{Y}_s) + \delta.$$

This proves the result for the case $H(\tilde{U}|\tilde{X}) = 0$.

■

Thus Theorem 4.1 is proved. Note that we actually have shown that the error probability decreases exponentially with n. For the achievability part of Theorem 4.2 we adjust the analysis of the error probability in the achievability proof of Theorem 4.1.

Lemma 4.5. *Lemma 4.4 holds true even when we replace* (4.10) *by*

$$\sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \sup_{s\in\mathcal{S}} Pr(K \neq \hat{K}_s|\bar{M}=\bar{m}) \leqslant \delta.$$

Proof. In order to prove this result we rewrite the analysis of the error probability starting from (4.16) and implement the necessary adjustments. We have

$$\begin{aligned}
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s|\bar{M}=(m,t)) \\
&= \sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t)(\sup_{s\in\mathcal{S}} \sum_{\tilde{t}\in[T]} \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_{\tilde{t}}}|\bar{M}=(m,t)) \\
&\qquad\qquad \cdot \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \in \mathcal{T}^n_{X_{\tilde{t}}}) \\
&\quad + \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}|\bar{M}=(m,t)))
\end{aligned}$$

which can be upper bounded by

$$\begin{aligned}
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t)(\sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \in \mathcal{T}^n_{X_t}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}|\bar{M}=(m,t)) \\
&\quad + \sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}|\bar{M}=(m,t)))
\end{aligned}$$

which is smaller or equal than

$$\begin{aligned}
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t)(\sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \in \mathcal{T}^n_{X_t}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}|\bar{M}=(m,t)) \\
&\quad + \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}|\bar{M}=(m,t))) \qquad (4.22) \\
&= \sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s|\bar{M}=(m,t), \tilde{X}^n \in \mathcal{T}^n_{X_t}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}|\bar{M}=(m,t)) \\
&\quad + \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1}). \qquad (4.23)
\end{aligned}$$

Thus we now consider $\Pr(K \neq \hat{K}_s | \bar{M} = (m,t), \tilde{X}^n \in \mathcal{T}^n_{X_t})$ for $(m,t) \in \bar{\mathcal{M}}$ and $s \in \mathcal{S}$.

$$\begin{aligned}\Pr(K \neq \hat{K}_s | \bar{M} = (m,t), \tilde{X}^n \in \mathcal{T}^n_{X_t}) &= \frac{\Pr(K \neq \hat{K}_s \wedge \bar{M} = (m,t) | \tilde{X}^n \in \mathcal{T}^n_{X_t})}{\Pr(\bar{M} = (m,t) | \tilde{X}^n \in \mathcal{T}^n_{X_t})} \\ &= M_t \Pr(K \neq \hat{K}_s \wedge \bar{M} = (m,t) | \tilde{X}^n \in \mathcal{T}^n_{X_t})\end{aligned}$$

which follows from (4.21). This expression equals

$$M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) F(k,(m,t)|x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).$$

Similar to the corresponding steps in the proof of Lemma 4.4, with our choice of $F(k,(m,t)|x^n)$ this equals

$$\begin{aligned}&M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \Pr(U_n = u^t_{k,m} | \tilde{X}^n = x^n) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\ &+ M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \Pr(U_n = u^* | \tilde{X}^n = x^n) \tfrac{1}{L_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).\end{aligned}$$

The second summand can be upper bounded by

$$\begin{aligned}&\tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{L_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\ &\leqslant \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} M_t \sum_{\hat{k} \in \mathcal{K}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{M_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\ &= \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)} M_t \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} \tfrac{1}{|\mathcal{T}^n_{X_t}|} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \tfrac{1}{M_t} \\ &= \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)}.\end{aligned}$$

The first summand equals

$$\begin{aligned}&M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \\ &\qquad \cdot \Pr(U_n = u^t_{k,m}, \tilde{X}^n = x^n | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\ &= M_t \sum_{\substack{k,\hat{k} \in \mathcal{K} \\ k \neq \hat{k}}} \sum_{y^n \in \mathcal{Y}^n} \sum_{x^n \in \mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \Pr(U_n = u^t_{k,m} | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\ &\qquad \cdot \Pr(\tilde{X}^n = x^n | U_n = u^t_{k,m}, \tilde{X}^n \in \mathcal{T}^n_{X_t})\end{aligned}$$

Using (4.15) and (4.13) this can be upper bounded by

$$\frac{1+\exp(-nc_1)}{1-\exp(-nc_1)} M_t \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \frac{1}{|\mathcal{T}^n_{X_t|U_t}(u^t_{k,m})|} Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).$$

With (4.17) we get the upper bound

$$\begin{aligned}\frac{1+\exp(-nc_1)}{1-\exp(-nc_1)} \exp(n\xi) M_t \sum_{\substack{k,\hat{k}\in\mathcal{K}\\ k\neq\hat{k}}} \sum_{y^n\in\mathcal{Y}^n} \sum_{x^n\in\mathcal{T}^n_{X_t}} & P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(y^n|x^n) \\ & \cdot P^{\otimes n}_{X_t|U_t}(x^n|u^t_{k,m}) Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)). \end{aligned} \tag{4.24}$$

We use the same definition for g as in the proof of Lemma 4.4. So together with (4.12) we can upper bound (4.24) by

$$\frac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2} \exp(n\xi) \frac{1}{M_t} M_t \frac{1}{K} \sum_{k\in\mathcal{K}} \sum_{x^n\in\mathcal{X}^n} P^{\otimes n}_{\tilde{Y}_s|\tilde{X}}(\mathcal{D}^t_{k,m}|x^n) P^{\otimes n}_{X_t|U_t}(x^n|u^t_{k,m}).$$

This equals

$$\frac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2} \exp(n\xi) \frac{1}{K} \sum_{k\in\mathcal{K}} P^{\otimes n}_{\tilde{Y}_s|U_t}(\mathcal{D}^t_{k,m}|u^t_{k,m})$$

Again, from our choice of R we can upper bound this expression for all $s \in \mathcal{S}$ and $t \in [T]$ by

$$\frac{1+\exp(-nc_1)}{(1-\exp(-nc_1))^2} \exp(n\xi) \exp(-nc_2) = \exp(-nc_3)$$

for a $c_3 > 0$, n large enough and an appropriate choice of ξ. We thus have

$$\begin{aligned}&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \sup_{s\in\mathcal{S}} \Pr(K \neq \hat{K}_s | \bar{M} = (m,t), \tilde{X}^n \in \mathcal{T}_{X_t}) \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t} | \bar{M} = (m,t)) \\ &\leqslant \exp(-nc_3) \sum_{(m,t)\in\bar{\mathcal{M}}} \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) \Pr(\bar{M} = (m,t) | \tilde{X}^n \in \mathcal{T}^n_{X_t}),\end{aligned}$$

which equals

$$\begin{aligned}&\exp(-nc_3) \sum_{t\in[T]} \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) \sum_{m\in[M_t]} \Pr(\bar{M} = (m,t) | \tilde{X}^n \in \mathcal{T}^n_{X_t}) \\ &\leqslant \exp(-nc_3) \sum_{t\in[T]} \Pr(\tilde{X}^n \in \mathcal{T}^n_{X_t}) \leqslant \exp(-nc_3).\end{aligned}$$

Thus with (4.23) and [26, Lemma 2.12] altogether the error probability goes to 0 exponentially with respect to n.

■

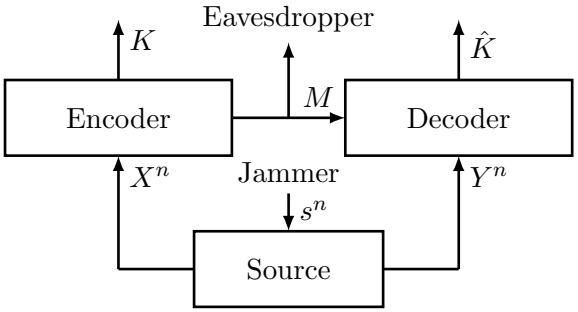

Figure 4.2: SK generation from a jammed source. The jammer does not know the helper message and can choose an attack strategy $s^n \in \mathcal{S}^n$.

4.3 Results for the jammed source

As described in Chapter 3, besides the compound DMMS, there is another possibility of modeling jammers in our setting for SK generation. We again consider RVs X and $\{Y_s\}_{s\in\mathcal{S}}$, but now we assume that $|\mathcal{S}| < \infty$. The jammer can choose a sequence $s^n \in \mathcal{S}^n$ (which we call an attack strategy) and the source puts out RVs $X^n = (X_1, \cdots, X_n)$ observed at terminal $\mathcal{X}$ and $Y_{s^n}^n = (Y_{s_1,1}, \cdots, Y_{s_n,n})$ observed at terminal $\mathcal{Y}$ and we assume $P_{X^n Y_{s^n}^n} = \bigotimes_{i=1}^n P_{XY_{s_i}}$. In contrast to the compound DMMS here the jammer can choose the source statistics for each pair of symbols read from the source. For the compound DMMS the distribution is chosen once, i.e., it is fixed for the whole block length n. Obviously a jammer who can choose the source distribution for each pair of symbols read from the source is more powerful.

We also note that the set of conditional distributions $\{P_{Y_s|X}\}_{s\in\mathcal{S}}$ determines an AVC.

Again we allow for randomized encoders, i.e., the SK K and the helper message M are generated from X^n which is described by a stochastic matrix $F \in \mathcal{P}(\mathcal{K}\times\mathcal{M}|\mathcal{X}^n)$. For the reconstruction of the SK we now have to consider a set of RVs $\{\hat{K}_{s^n}\}_{s^n\in\mathcal{S}^n}$ that represent the reconstruction for each possible attack strategy $s^n \in \mathcal{S}^n$. The decoder again is assumed to be a deterministic function $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$, i.e., $\hat{K}_{s^n} = g(Y_{s^n}^n, M)$ for all $s^n \in \mathcal{S}^n$. As before the tuple (F, g) is a SK generation protocol.

It follows that for all $s^n \in \mathcal{S}^n$ the joint distribution of K, M and $\hat{K}_{s^n}$ is

$$P_{KM\hat{K}_{s^n}}(k, m, \hat{k}) = \sum_{\substack{x^n\in\mathcal{X}^n \\ y^n\in\mathcal{Y}^n}} \prod_{i=1}^n P_{XY_{s_i}}(x_i, y_i) F(k, m|x^n) \mathbb{1}_{g^{-1}(\hat{k})}((y^n, m))$$

for all $(k, m, \hat{k}) \in \mathcal{K}\times\mathcal{M}\times\mathcal{K}$.

At first we assume that the jammer does not read the helper message from the public database. The setting is depicted in Figure 4.2.

Again we determine desirable properties for SK generation protocols in this setting.

Definition 4.2. *Let $L \geqslant 0$. We call $R \geqslant 0$ an* achievable AVC secret key rate with rate constraint *L if for any $\epsilon > 0$ and sufficiently large n there is a SK generation protocol*

such that

$$\begin{aligned}
&\max_{s^n \in \mathcal{S}^n} Pr(K \neq \hat{K}_{s^n}) \leqslant \epsilon \\
&H(K|M) = \log |\mathcal{K}| \\
&\tfrac{1}{n} \log |\mathcal{K}| \geqslant R - \epsilon \\
&\tfrac{1}{n} \log |\mathcal{M}| \leqslant L + \epsilon.
\end{aligned}$$

The AVC SK capacity with rate constraint L *is the largest achievable compound secret key rate with rate constraint* L *and is denoted by* $C_{SK}^{AVC}(L)$.

$C_{SK}^{AVC}(L)$ can be characterized as follows.

Theorem 4.6. *It holds that*

$$C_{SK}^{AVC}(L) = \max_{U} \min_{W \in conv(\{P_{Y_s|U}\}_{s\in\mathcal{S}})} I(P_U, W)$$

where the maximization is over all RVs U *such that* $U - X - Y_s$ *and*

$$I(U \wedge X) - \min_{W \in conv(\{P_{Y_s|U}\}_{s\in\mathcal{S}})} I(P_U, W) \leqslant L$$

for all $s \in \mathcal{S}$.

Proof. The converse is a consequence of Theorem 3.15. It follows in the same way as the converse part of Theorem 4.1 follows from Theorem 3.4.

Achievability follows from Lemma 4.10 below.

■

As mentioned before, $\{P_{Y_s|X}\}_{s\in\mathcal{S}}$ corresponds to an AVC. When considering this AVC we assume that, given the block length n, the probability of receiving $y^n \in \mathcal{Y}^n$ at the channel output is given by

$$\prod_{i=1}^{n} P_{Y_{s_i}|X}(y_i|x_i)$$

where $x^n \in \mathcal{X}^n$ is the channel input and $s^n \in \mathcal{S}^n$ is a state sequence. In [31] list decoding with fixed list size L is considered for communication over an AVC (see also [19]). This means the receiver does not necessarily try to decode the channel output. Instead the receiver tries to construct a list of size at most L that should contain the message sent over the channel. L is independent of n.

As described in [31] the best possible transmission rate for reliable communication (with respect to the average probability of error criterion) over an AVC with list decoding and a given list size strongly depends on the symmetrizability of the AVC.

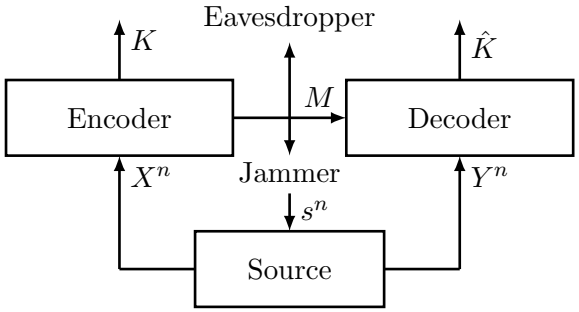

Figure 4.3: SK generation from a jammed source. The jammer chooses an attack strategy $s^n \in \mathcal{S}^n$ based on the helper message M.

Definition 4.3 ([31]). *For $\hat{m} \geqslant 1$ the AVC corresponding to $\{W_s\}_{s\in\mathcal{S}}$, $W_s \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ is $\hat{m}$- symmetrizable if there is a stochastic matrix $U \in \mathcal{P}(\mathcal{S}|\mathcal{X}^{\hat{m}})$ such that*

$$\sum_{s\in\mathcal{S}} W_s(y|x)U(s|x_1,\cdots,x_{\hat{m}})$$

is invariant over all permutations of $x, x_1, \cdots, x_{\hat{m}}$ for all $(y, x, x_1, \cdots, x_{\hat{m}}) \in \mathcal{Y} \times \mathcal{X}^{\hat{m}+1}$ [31, Definition 2]. We also say

$$\sum_{s\in\mathcal{S}} W_s(y|x)U(s|x_1,\cdots,x_{\hat{m}})$$

is symmetric in $x, x_1, \cdots, x_{\hat{m}}$.

All AVCs are said to be 0-symmetrizable. The symmetrizability of the AVC denoted by $\hat{M}$ is the largest integer $\hat{m}$ such that the AVC is $\hat{m}$-symmetrizable. If no such $\hat{m}$ exists, we take $\hat{M} = \infty$ [31, Definition 3].

In the following we make use of the notion of symmetrizability for our model of SK generation from a jammed source.

As done for the compound source we now assume that the jammer has access to the helper message from the public database and thus can choose the attack strategy s^n based on the helper message. The setting is depicted in Figure 4.3.

We also generalize the SK generation protocols as we now consider list decoding with fixed list size $\hat{L}$ at terminal $\mathcal{Y}$. Again we allow for randomized encoders $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n)$. Instead of the reconstruction of the SK we now consider a set of RVs $\{\hat{K}_{s^n}^{\hat{L}}\}_{s^n\in\mathcal{S}^n}$ distributed on the set of all subsets of $\mathcal{K}$ with cardinality at most $\hat{L}$, which we denote by $\hat{\mathcal{P}}_{\hat{L}}$. $\hat{K}_{s^n}^{\hat{L}}$ represents the list of size at most $\hat{L}$ generated at terminal $\mathcal{Y}$ for attack strategy $s^n \in \mathcal{S}^n$. The decoder is a deterministic function $g_{\hat{L}} \colon \mathcal{Y}^n \times \mathcal{M} \to \hat{\mathcal{P}}_{\hat{L}}$, i.e., $\hat{K}_{s^n}^{\hat{L}} = g_{\hat{L}}(Y_{s^n}^n, M)$ for all $s^n \in \mathcal{S}^n$. The tuple $(F, g_{\hat{L}})$ is a SK generation protocol.

So for all $s^n \in \mathcal{S}^n$ the joint distribution of K, M and $\hat{K}_{s^n}^{\hat{L}}$ is

$$P_{KM\hat{K}_{s^n}^{\hat{L}}}(k,m,\hat{k}) = \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \prod_{i=1}^{n} P_{XY_{s_i}}(x_i,y_i) F(k,m|x^n) \mathbb{1}_{g_{\hat{L}}^{-1}(\hat{k})}((y^n,m))$$

for all $(k,m,\hat{k}) \in \mathcal{K}\times\mathcal{M}\times\hat{\mathcal{P}}_{\hat{L}}$.

The following definition again determines the properties we want the SK generation protocols to have.

Definition 4.4. *Let $L \geqslant 0$ and $\hat{L} > 0$. We call $R \geqslant 0$ an* achievable AVC SK rate with rate constraint L and list decoding with list size $\hat{L}$ *if for any $\epsilon > 0$ and sufficiently large n there is a SK generation protocol such that*

$$\begin{aligned}
&\sum_{m\in\mathcal{M}} P_M(m) \max_{s^n\in\mathcal{S}^n} Pr(K \notin \hat{K}_{s^n}^{\hat{L}} | M = m) \leqslant \epsilon\\
&H(K|M) = \log|\mathcal{K}|\\
&\tfrac{1}{n}\log\tfrac{|\mathcal{K}|}{\hat{L}} \geqslant R - \epsilon\\
&\tfrac{1}{n}\log|\mathcal{M}| \leqslant L + \epsilon.
\end{aligned}$$

The AVC SK capacity with rate constraint L and list decoding with list size $\hat{L}$ *is the largest achievable AVC SK rate with rate constraint L and list decoding with list size $\hat{L}$ and is denoted by $C_{SK}^{AVC,\hat{L}}(L)$.*

Our next result is the following lower bound on $C_{SK}^{AVC,\hat{L}}(L)$.

Theorem 4.7. *Denote the symmetrizability of the AVC corresponding to $\{P_{Y_s|X}\}_{s\in\mathcal{S}}$ by $\hat{M}$ and assume $\hat{M} < \infty$. Let $\hat{L} = \hat{M} + 1$. It holds that $C_{SK}^{AVC,\hat{L}}(L) \geqslant C_{SK}^{AVC}(L)$.*

Corollary 4.8. *It holds that $C_{SK}^{AVC,1}(L) = C_{SK}^{AVC}(L)$ if the AVC corresponding to $\{P_{Y_s|X}\}_{s\in\mathcal{S}}$ is not symmetrizable (i.e., has symmetrizability 0), otherwise $C_{SK}^{AVC,1}(L) = 0$.*

Proof. Theorem 4.7 follows from Lemma 4.13 below. The achievability part of the corollary is a direct consequence of Theorem 4.7.

The converse part of the corollary follows from the converse part of Theorem 3.7 in the same way as the converse part of Theorem 4.1 follows from Theorem 3.4.

■

Finally we consider the setting depicted in Figure 4.4. Here we do not consider list decoding (or equivalently, only lists of size 1) i.e., the SK is reconstructed at terminal $\mathcal{Y}$. We still assume the jammer knows the helper message, but now there is CR available at both terminals. We assume the jammer does not know the CR while the eavesdropper knows the CR. This means both terminals have access to a RV Γ which we assume is uniformly distributed on a set $\mathcal{G}$ and independent of X^n and $Y_{s^n}^n$. Again we allow for

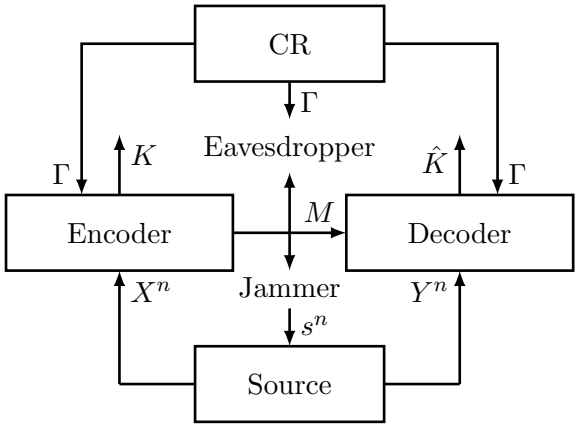

Figure 4.4: SK generation from a jammed source. The jammer chooses an attack strategy $s^n \in \mathcal{S}^n$ based on the helper message M. CR not known to the jammer is available at terminal $\mathcal{X}$ and $\mathcal{Y}$ and known to the eavesdropper.

randomized encoders, i.e., the SK K and the helper message M are generated from X^n and Γ which is described by a stochastic matrix $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n \times \mathcal{G})$. For the reconstruction of the SK we again consider a set of RVs $\{\hat{K}_{s^n}\}_{s^n \in \mathcal{S}^n}$. The decoder is assumed to be a deterministic function $g\colon \mathcal{Y}^n \times \mathcal{M} \times \mathcal{G} \to \mathcal{K}$, i.e., $\hat{K}_{s^n} = g(Y^n_{s^n}, M, \Gamma)$ for all $s^n \in \mathcal{S}^n$. The tuple (F, g) is a SK generation protocol.

It follows that for all $s^n \in \mathcal{S}^n$ the joint distribution of K, M, $\hat{K}_{s^n}$ and Γ is

$$P_{KM\hat{K}_{s^n}\Gamma}(k, m, \hat{k}, \gamma) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \prod_{i=1}^{n} P_{XY_{s_i}}(x_i, y_i) F(k, m|x^n, \gamma) \mathbb{1}_{g^{-1}(\hat{k})}((y^n, m, \gamma)) P_\Gamma(\gamma)$$

for all $(k, m, \hat{k}, \gamma) \in \mathcal{K} \times \mathcal{M} \times \mathcal{K} \times \mathcal{G}$.

We want to consider the case where the amount of CR available is small. So the SK generation protocols should have the properties specified by the following definition.

Definition 4.5. *Let $L \geqslant 0$. We call $R \geqslant 0$ an* achievable CR assisted AVC secret key rate with rate constraint *L if for any $\epsilon > 0$ and sufficiently large n there is a SK generation protocol such that*

$$\begin{aligned}
&\sum_{m \in \mathcal{M}} P_M(m) \max_{s^n \in \mathcal{S}^n} Pr(K \notin \hat{K}_{s^n} | M = m) \leqslant \epsilon \\
&H(K|M\Gamma) = \log |\mathcal{K}| \\
&\tfrac{1}{n} \log |\mathcal{K}| \geqslant R - \epsilon \\
&\tfrac{1}{n} \log |\mathcal{M}| \leqslant L + \epsilon \\
&\tfrac{1}{n} \log |\mathcal{G}| \leqslant \epsilon.
\end{aligned}$$

The CR assisted AVC SK capacity with rate constraint *L is the largest achievable CR*

assisted AVC secret key rate with rate constraint L and is denoted by $C_{SK}^{AVC,CR}(L)$.

The following theorem characterizes $C_{SK}^{AVC,CR}(L)$.

Theorem 4.9. *It holds that $C_{SK}^{AVC,CR}(L) = C_{SK}^{AVC}(L)$.*

Proof. Achievability follows from Lemma 4.15. When the helper message is not known to the jammer, the CR can be made available to both terminals by generating Γ at terminal $\mathcal{X}$ and appending it to the helper message. As $\frac{1}{n}\log|\mathcal{G}| \leqslant \epsilon$ this does not increase the rate of the helper message. This argumentation implies the converse, as $C_{SK}^{AVC}(L)$ is the capacity where the jammer does not know the helper message.

■

Note that the achievability proof provides an application for identification codes. One could expect that it is possible to prove the achievability part of Theorem 4.9 using Theorem 4.2 and Ahlswede robustification with elimination of correlation. This does not work as expected because the union bound as used e.g. to get from (4.30) to (4.31) does not work for this case. So instead, motivated by [34] and [42], we use list decoding with a constrained list size at terminal $\mathcal{Y}$ and an identification code to find out which of the keys in the list is the actual key generated at terminal $\mathcal{X}$. Additionally we encrypt the part of the helper message corresponding to the identification code with two keys. One key is unknown to the eavesdropper (this key is generated using some CR), the other key is unknown to the jammer (for this key we can directly use some CR).

Assume that the amount of CR is arbitrarily large. Theorem 3.15 implies that this does not increase the corresponding capacity compared to $C_{SK}^{AVC,CR}(L)$, i.e. the case with small amount of CR.

4.4 Achievability proofs for the jammed source

Lemma 4.10, which proves the achievability part of Theorem 4.6, is proved with the Ahlswede robustification technique.

Lemma 4.10. *Consider the RVs $\tilde{X}$ and $\{\tilde{Y}_s\}_{s\in\mathcal{S}}$, $|\mathcal{S}| < \infty$ with $P_{\tilde{X}\tilde{Y}_s} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ for all $s \in \mathcal{S}$ and a RV $\tilde{U}$ such that $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$, $P_{\tilde{U}} \in \mathcal{P}(\mathcal{U})$. Let $\delta > 0$. For all n large enough there is a stochastic matrix $F_{CR} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}|\mathcal{X}^n)$ and a mapping $g_{CR}\colon \mathcal{Y}^n \times \bar{\mathcal{M}} \to \mathcal{K}$ such that for RVs K, $\bar{M}$ and $\{\hat{K}_{s^n}\}_{s^n\in\mathcal{S}^n}$ with $P_{K\bar{M}\hat{K}_{s^n}} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K})$ for all $s^n \in \mathcal{S}^n$ defined by*

$$P_{K\bar{M}\hat{K}_{s^n}}(k,\bar{m},\hat{k}) = \sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_{CR}(k,\bar{m}|x^n)\mathbb{1}_{g_{CR}^{-1}(\hat{k})}((y^n,\bar{m}))$$

for $(k, \bar{m}, \hat{k}) \in \mathcal{K} \times \bar{\mathcal{M}} \times \mathcal{K}$ *it holds that*

$$\begin{aligned}
&\max_{s^n \in \mathcal{S}^n} Pr(K \neq \hat{K}_{s^n}) \leqslant \delta \\
&H(K|\bar{M}) = \log|\mathcal{K}| \\
&\tfrac{1}{n}\log|\mathcal{K}| \geqslant \min_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}}, W) - \delta \\
&\tfrac{1}{n}\log|\bar{\mathcal{M}}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \min_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}}, W) + \delta.
\end{aligned}$$

Proof. Given $\delta > 0$ there is a $c > 0$ such that for all n large enough we can find $F \in \mathcal{P}(\mathcal{K} \times \mathcal{M}|\mathcal{X}^n)$ and $g\colon \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$ such that for RVs K' and M' with

$$P_{K'M'}(k, m) = \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, m|x^n)$$

for all $(k, m) \in \mathcal{K} \times \mathcal{M}$ it holds that

$$\begin{aligned}
&\max_{W \in conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}})} \sum_{x^n, y^n} \sum_{k,m} P_{\tilde{X}}^{\otimes n}(x^n) W^{\otimes n}(y^n|x^n) \\
&\qquad \cdot F(k, m|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, m)) \leqslant \exp(-nc) && (4.25)\\
&H(K'|M') = \log|\mathcal{K}| && (4.26)\\
&\tfrac{1}{n}\log|\mathcal{K}| \geqslant \inf_{t\in\mathcal{T}} I(\tilde{U} \wedge Y_t) - \delta && (4.27)\\
&\tfrac{1}{n}\log|\mathcal{M}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \inf_{t\in\mathcal{T}} I(\tilde{U} \wedge Y_t) + \delta && (4.28)
\end{aligned}$$

where the RVs $\{Y_t\}_{t\in\mathcal{T}}$ are such that $\{P_{Y_t|\tilde{X}}\}_{t\in\mathcal{T}} = conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}})$ and $\tilde{U} - \tilde{X} - Y_t$ for all $t \in \mathcal{T}$. This follows from the achievability proof of Lemma 4.4.

Define $h\colon \mathcal{S}^n \to [0, 1]$ such that for all $s^n \in \mathcal{S}^n$

$$h(s^n) = \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{\substack{k,m \in \\ \mathcal{K}\times\mathcal{M}}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F(k, m|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, m)).$$

It holds for all $P \in \mathcal{P}(n, \mathcal{S})$ that

$$\begin{aligned}
&\sum_{s^n \in \mathcal{S}^n} h(s^n) P^{\otimes n}(s^n) \\
&= \sum_{s^n \in \mathcal{S}^n} P^{\otimes n}(s^n) \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{k,m \in \mathcal{K}\times\mathcal{M}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F(k, m|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, m)) \\
&= \sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{k,m \in \mathcal{K}\times\mathcal{M}} \sum_{s^n \in \mathcal{S}^n} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) P(s_i) F(k, m|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, m))
\end{aligned}$$

which equals

$$\sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}}\sum_{k,m\in\mathcal{K}\times\mathcal{M}}\prod_{i=1}^{n}\sum_{s\in\mathcal{S}}P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i)P(s)F(k,m|x^n)\mathbb{1}_{g^{-1}(k)}((y^n,m))$$
$$=\sum_{\substack{x^n\in\mathcal{X}^n\\ y^n\in\mathcal{Y}^n}}\sum_{k,m\in\mathcal{K}\times\mathcal{M}}P_{\tilde{X}}^{\otimes n}(x^n)W^{\otimes n}(y^n|x^n)F(k,m|x^n)\mathbb{1}_{g^{-1}(k)}((y^n,m))$$

with $W\in conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}})$ defined appropriately. So from our choice of F and g we know that

$$\sum_{s^n\in\mathcal{S}^n}h(s^n)P^{\otimes n}(s^n)>1-\exp(-nc),$$

cf. (4.25) According to [3, Theorem RT] this implies for all $s^n\in\mathcal{S}^n$

$$\tfrac{1}{n!}\sum_{\pi\in\Pi_n}h(\pi s^n)>1-\exp(-nc)(n+1)^{|\mathcal{S}|}$$

where Π_n is the set of all permutations on $[n]$ and we write for $\pi\in\Pi_n$ πx^n for $x_{\pi^{-1}(1)},\cdots,x_{\pi^{-1}(n)}$, i.e. π is a bijection on $\mathcal{X}^n$. Now consider (equivalently to the proof of [47, Lemma 5.11]) independent RVs $P_1,\cdots,P_N$, $N=\lceil n^{1+\eta}\rceil$, $\eta>0$, each distributed uniformly on Π_n. We want to show that there is a realization $p_1,\cdots,p_N$ such that (for n large enough)

$$\tfrac{1}{N}\sum_{i=1}^{N}h(p_is^n)\geqslant 1-3\lambda, \tag{4.29}$$

$\lambda>0$, for all $s^n\in\mathcal{S}^n$. For this purpose we show (similar to the proof of [47, Lemma 5.11])

$$\Pr(\tfrac{1}{N}\sum_{i=1}^{N}h(P_is^n)\geqslant 1-3\lambda \text{ for all } s^n\in\mathcal{S}^n)>0. \tag{4.30}$$

As $|\mathcal{S}^n|$ grows exponentially with respect to n it is sufficient to show that

$$\Pr(\tfrac{1}{N}\sum_{i=1}^{N}h(P_is^n)<1-3\lambda)$$

or equivalently

$$\Pr(\tfrac{1}{N}\sum_{i=1}^{N}(1-h(P_is^n))>3\lambda) \tag{4.31}$$

is superexponentially small for all $s^n\in\mathcal{S}^n$. According to [47, Lemma 5.12] (4.31) is

smaller than

$$\exp(-(3\lambda - eE(1-h(P_1 s^n)))N).$$

As for n large enough and $s^n \in \mathcal{S}^n$

$$E(1-h(P_1 s^n)) = 1 - \tfrac{1}{n!}\sum_{\pi\in\Pi_n} h(\pi s^n) < \lambda$$

the exponent is negative and as $N = \lceil n^{1+\eta} \rceil$ this yields the superexponential bound we need. We define for all $\pi \in \Pi_n$ and all $(k, m, x^n) \in \mathcal{K}\times\mathcal{M}\times\mathcal{X}^n$

$$\begin{aligned} F^\pi(k,m|x^n) &= F(k,m|\pi x^n) \\ g^\pi(y^n,m) &= g(\pi y^n, m). \end{aligned}$$

We can write for all $s^n \in \mathcal{S}^n$ and $\pi \in \Pi_n$

$$\begin{aligned} h(\pi s^n) &= \sum_{\substack{x^n\in\mathcal{X}^n \\ y^n\in\mathcal{Y}^n}} \sum_{k,m\in\mathcal{K}\times\mathcal{M}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_{\pi^{-1}(i)}}}(x_i,y_i) F(k,m|x^n)\mathbb{1}_{g^{-1}(k)}((y^n,m)) \\ &= \sum_{\substack{x^n\in\mathcal{X}^n \\ y^n\in\mathcal{Y}^n}} \sum_{k,m\in\mathcal{K}\times\mathcal{M}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_{\pi(i)},y_{\pi(i)}) F(k,m|x^n)\mathbb{1}_{g^{-1}(k)}((y^n,m)). \end{aligned}$$

As π is a bijection on $\mathcal{X}^n$ and $\mathcal{Y}^n$ respectively and we sum over all elements of these sets this equals

$$\begin{aligned} &\sum_{\substack{x^n\in\mathcal{X}^n \\ y^n\in\mathcal{Y}^n}} \sum_{k,m\in\mathcal{K}\times\mathcal{M}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F(k,m|\pi x^n)\mathbb{1}_{g^{-1}(k)}((\pi y^n,m)) \\ &= \sum_{\substack{x^n\in\mathcal{X}^n \\ y^n\in\mathcal{Y}^n}} \sum_{k,m\in\mathcal{K}\times\mathcal{M}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F^\pi(k,m|x^n)\mathbb{1}_{(g^\pi)^{-1}(k)}((y^n,m)). \end{aligned} \tag{4.32}$$

Define the distribution $\Gamma \in \mathcal{P}(\Pi_n)$ such that for all $\pi \in \Pi_n$

$$\Gamma(\pi) = \sum_{i=1}^N \mathbb{1}_{\{p_i\}}(\pi)/N.$$

Define $\bar{\mathcal{M}} = \mathcal{M} \times supp(\Gamma)$. We now define for all $(k, m, p) \in \mathcal{K}\times\mathcal{M}\times supp(\Gamma)$ and $x^n \in \mathcal{X}^n$

$$\begin{aligned} F_{CR}(k,(m,p)|x^n) &= F^p(k,m|x^n)\Gamma(p) \\ g_{CR}(y^n,(m,p)) &= g^p(y^n,m). \end{aligned}$$

This means the permutation p is chosen randomly according to the distribution Γ at terminal $\mathcal{X}$. Then p is made available to terminal $\mathcal{Y}$ as a part of the helper message. The encoder and decoder are chosen form a set of encoders and decoders according to p.

From (4.29) and (4.32) it follows that $\Pr(K \neq \hat{K}_{s^n}) \leqslant 3\lambda$ for all $s^n \in \mathcal{S}^n$. Now consider for $(k, m, p) \in \mathcal{K} \times \bar{\mathcal{M}}$

$$\begin{aligned} P_{K\bar{M}}(k, m, p) &= \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F^p(k, m|x^n) \Gamma(p) \\ &= \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, m|x^n) \Gamma(p) \end{aligned}$$

which follows as p is a bijection on $\mathcal{X}^n$ and we sum over all $x^n \in \mathcal{X}^n$. So we get

$$\begin{aligned} P_{K|\bar{M}}(k|m, p) &= \frac{\sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k,m|x^n) \Gamma(p)}{\sum_{k \in \mathcal{K}} \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k,m|x^n) \Gamma(p)} \\ &= \frac{\sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k,m|x^n)}{\sum_{k \in \mathcal{K}} \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k,m|x^n)} = \frac{1}{|\mathcal{K}|} \end{aligned}$$

where we use the corresponding property (4.26) of F for the last step.

Consider $t \in \mathcal{T}$. There is a $P \in \mathcal{P}(\mathcal{S})$ such that for all $(u, y) \in \mathcal{U} \times \mathcal{Y}$

$$\begin{aligned} P_{Y_t|\tilde{U}}(y|u) &= \sum_{x \in \mathcal{X}} P_{Y_t|\tilde{X}}(y|x) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{x \in \mathcal{X}} \Big(\sum_{s \in \mathcal{S}} P(s) P_{\tilde{Y}_s|\tilde{X}}(y|x) \Big) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{s \in \mathcal{S}} P(s) \sum_{x \in \mathcal{X}} P_{\tilde{Y}_s|\tilde{X}}(y|x) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{s \in \mathcal{S}} P(s) P_{\tilde{Y}_s|\tilde{U}}(y|u), \end{aligned}$$

where we use $\tilde{U} - \tilde{X} - Y_t$ for all $t \in \mathcal{T}$ and $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$. So $\{P_{Y_t|\tilde{U}}\}_{t \in \mathcal{T}} \subset conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})$. Thus it follows that

$$\inf_{t \in \mathcal{T}} I(\tilde{U} \wedge Y_t) = \inf_{t \in \mathcal{T}} I(P_{\tilde{U}}, P_{Y_t|\tilde{U}}) \geqslant \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W).$$

Accordingly we have with (4.27) and (4.28)

$$\tfrac{1}{n} \log |\mathcal{K}| \geqslant \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) - \delta$$

and

$$\tfrac{1}{n} \log |\mathcal{M}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) + \delta.$$

The bound on $\frac{1}{n}\log|\bar{\mathcal{M}}| = \frac{1}{n}\log|\mathcal{M}| + \frac{1}{n}\log|supp(\Gamma)|$ follows for n large enough as

$$\frac{1}{n}\log|supp(\Gamma)| \leqslant \frac{1}{n}\log N \leqslant \frac{1}{n}(2+\eta)\log n.$$

The infimum can be replaced by a minimum as $conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})$ is compact and $I(P_{\tilde{U}}, W)$ is continuous in W.

■

We have thus shown the achievability part of Theorem 4.6. Now we turn to the achievability proof of Theorem 4.7. For this purpose we prove Lemma 4.13 below. We need the following auxiliary results.

Lemma 4.11. *Consider RVs X, $\{Y_s\}_{s\in\mathcal{S}}$, U and U' such that*

$$\|P_{UXY_s} - P_{U'XY_s}\|_1 \leqslant \epsilon$$

for $\epsilon > 0$ and all $s \in \mathcal{S}$ and $\min_{u\in\mathcal{U}} P_U(u) > 0$, $\min_{u\in\mathcal{U}} P_{U'}(u) > 0$. It holds that

$$|\min_{W\in\mathcal{W}} I(P_U, W) - \min_{W\in\mathcal{W}'} I(P_{U'}, W)| \leqslant \delta(\epsilon)$$

with $\delta(\epsilon) \to 0$ for $\epsilon \to 0$ and $\delta(\epsilon) > 0$, where $\mathcal{W} = conv(\{P_{Y_s|U}\}_{s\in\mathcal{S}})$ and $\mathcal{W}' = conv(\{P_{Y_s|U'}\}_{s\in\mathcal{S}})$.

Proof. Let $W \in \mathcal{W}$, so there is a $P \in \mathcal{P}(\mathcal{S})$ such that for all $(y,u) \in \mathcal{Y}\times\mathcal{U}$ it holds that

$$W(y|u) = \sum_{s\in\mathcal{S}} P(s) P_{Y_s|U}(y|u).$$

We have

$$\begin{aligned} W(y|u) &= \sum_{s\in\mathcal{S}} \tfrac{P_{Y_sU}(y,u)}{P_U(u)} \leqslant \sum_{s\in\mathcal{S}} \tfrac{P_{Y_sU'}(y,u)+\epsilon|\mathcal{X}|}{P_{U'}(u)-\epsilon|\mathcal{X}||\mathcal{Y}|} \\ &= \sum_{s\in\mathcal{S}} P(s)\left(P_{Y_s|U'}(y|u)\tfrac{P_{U'}(u)}{P_{U'}(u)-\epsilon|\mathcal{X}||\mathcal{Y}|}\right) + \tfrac{\epsilon|\mathcal{X}|}{P_{U'}(u)-\epsilon|\mathcal{X}||\mathcal{Y}|} \\ &\leqslant \sum_{s\in\mathcal{S}} P(s) P_{Y_s|U'}(y|u) + \delta_1(\epsilon), \end{aligned}$$

where we define $\delta_1(\epsilon) > 0$ appropriately and it is clear that $\delta_1(\epsilon) \to 0$ for $\epsilon \to 0$. In the same way we can show

$$W(y|u) \geqslant \sum_{s\in\mathcal{S}} P(s) P_{Y_s|U'}(y|u) - \delta_1(\epsilon).$$

So for all $W \in \mathcal{W}$ there is a $W' \in \mathcal{W}'$ such that

$$|W(y|u) - W'(y|u)| \leqslant \delta_1(\epsilon)$$

for all $(y,u) \in \mathcal{Y} \times \mathcal{U}$. From [26, Lemma 2.7] we thus get

$$\min_{W \in \mathcal{W}} I(P_U, W) \geqslant I(P_U, W') - \delta_2(\epsilon) \geqslant \min_{W \in \mathcal{W}'} I(P_U, W) - \delta_2(\epsilon) \geqslant \min_{W \in \mathcal{W}'} I(P_{U'}, W) - \delta(\epsilon),$$

where we define $\delta_2(\epsilon) > 0$ appropriately and it is clear that $\delta_2(\epsilon) \to 0$ for $\epsilon \to 0$. The last step follows as $\min_{W \in \mathcal{W}'} I(P_U, W)$ is continuous in P_U, as discussed in the context of [24, Lemma 5]. Using similar steps we can show

$$\min_{W \in \mathcal{W}} I(P_U, W) \leqslant \min_{W \in \mathcal{W}'} I(P_{U'}, W) + \delta(\epsilon).$$

■

Lemma 4.12. *Let U, X be RVs with $P_{UX} \in \mathcal{P}(\bar{n}, \mathcal{U} \times \mathcal{X})$ for some $\bar{n} \in \mathbb{N}$ such that $H(U|X) > 0$ and $\min_{u \in \mathcal{U}} P_U(u) \geqslant \beta > 0$. Choose a $\delta > 0$ such that $\delta < H(U|X)$. Additionally consider RVs $\{Y_s\}_{s \in \mathcal{S}}$, $|\mathcal{S}| < \infty$, with $Y_s - X - U$ for all $s \in \mathcal{S}$. Denote the symmetrizability of $\{P_{Y_s|U}\}_{s \in \mathcal{S}}$ by $\hat{M}$ and assume $\hat{M} < \infty$. Let $\hat{L} = \hat{M} + 1$. Assume P_U is such that $\min_{W \in conv(\{P_{Y_s|U}\}_{s \in \mathcal{S}})} I(P_U, W) > 0$. Choose real numbers τ, R satisfying $\tau > 0$ and*

$$\min_{W \in conv(\{P_{Y_s|U}\}_{s \in \mathcal{S}})} I(P_U, W) - \tau < R < \min_{W \in conv(\{P_{Y_s|U}\}_{s \in \mathcal{S}})} I(P_U, W) - 2\tau/3.$$

For any $n \in \mathbb{N}$, define integers K, L, M satisfying

$$\begin{aligned} L = KM &= \exp(\lceil n(I(U \wedge X) + \delta) \rceil) \\ K &= \exp(\lceil nR \rceil) \hat{L}. \end{aligned}$$

Then there exist constants $c_1, c_2 > 0$ such that for every sufficiently large multiple n of $\bar{n}$ there is a set $\mathcal{J} = \{u_{k,m}\}_{(k,m) \in [K] \times [M]} \subset \mathcal{T}_U^n$ satisfying

$$(1 - \exp(-nc_1)) \frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L < |\mathcal{J} \cap \mathcal{T}_{U|X}^n(x^n)| < (1 + \exp(-nc_1)) \frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|} L \tag{4.33}$$

for all $x^n \in \mathcal{T}_X^n$. Additionally we can choose sets $\mathcal{L}(y^n, m) \subset [K]$ with $|\mathcal{L}(y^n, m)| \leqslant \hat{L}$ for all $y^n \in \mathcal{Y}^n$ and $m \in [M]$ such that for all $m \in [M]$ we have

$$\bar{e}_m(s^n) = \tfrac{1}{K} \sum_{k \in [K]} \sum_{y^n \colon k \notin \mathcal{L}(y^n, m)} \prod_{i=1}^{n} P_{Y_{s_i}|U}(y_i|(u_{k,m})_i) \leqslant \exp(-nc_2), \tag{4.34}$$

for all $s^n \in \mathcal{S}^n$.

The first part of the proof is based on [31, Proof of Lemma 1]. There the probabilistic method is used. Sequences are chosen randomly from a set with replacement according to a uniform distribution. In contrast we choose the sequences without replacement. We also prove additional properties compared to [31, Proof of Lemma 1]. The second part of the proof essentially is [31, Proof of Lemma 3].

Proof. We randomly choose $u_1, \cdots, u_L$ from $\mathcal{T}_U^n$ without replacement according to a uniform distribution. Denote the corresponding RVs by $U_1, \cdots, U_L$. Consider $x^n \in \mathcal{T}_X^n$ and the RV $Z_{x^n} = \sum_{l\in[L]} Z_{x^n}^l$ with $Z_{x^n}^l = \mathbb{1}_{\mathcal{T}_{U|X}^n(x^n)}(U_l)$ for $l \in [L]$. We can show as in the proof of Lemma 4.3 that for $x^n \in \mathcal{T}_X^n$ and n large enough

$$\Pr(|Z_{x^n} - \frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|}L| \geqslant \zeta\frac{|\mathcal{T}_{U|X}^n(x^n)|}{|\mathcal{T}_U^n|}L) \leqslant 2e^{-\exp(n\delta/4)/2}$$

where $\zeta = \exp(-nc_1)$ with $c_1 = \frac{\delta}{4}$.

Now consider the RVs S and $\bar{U}^{\hat{L}} = \bar{U}_1 \cdots \bar{U}_{\hat{L}}$ such that $P_{S\bar{U}^{\hat{L}}U} \in \mathcal{P}(n, \mathcal{S} \times \mathcal{U}^{\hat{L}} \times \mathcal{U})$ and $P_{\bar{U}_k} = P_U$ for all $k \in [\hat{L}]$. Let $(s^n, u^n) \in \mathcal{T}_{SU}^n$. Similarly to [31, Proof of Lemma 1], for each $m \in [M]$ we first estimate the size of the sets

$$\{k\colon (u^n, U_{k,m}^n, s^n) \in \mathcal{T}_{U\bar{U}_l S}^n\}$$

for $1 \leqslant l \leqslant \hat{L}$. As in [31, Proof of Lemma 1], define for all $1 \leqslant l \leqslant \hat{L}$ and $(k, m) \in [K] \times [M]$

$$f_{k,m}^{(P_{U\bar{U}_l S}, u^n, s^n)}(U_{1,m}, \cdots, U_{k,m}) = \mathbb{1}_{\mathcal{T}_{\bar{U}_l|US}^n(u^n,s^n)}(U_{k,m}).$$

Using the steps from (4.5) to (4.7) but replacing $\mathcal{T}_{\bar{U}|U}^n(u^n)$ by $\mathcal{T}_{\bar{U}_l|US}^n(u^n, s^n)$ we can upper bound

$$\sum_{u_{k,m}\in\mathcal{T}_U^n} f_{k,m}^{(P_{U\bar{U}_l S}, u^n, s^n)}(u_{1,m}, \cdots, u_{k,m}) P_{U_{k,m}|U_{1,m},\cdots,U_{k-1,m}}(u_{k,m}|u_{1,m}, \cdots, u_{k-1,m})$$

by

$$\frac{|\mathcal{T}_{\bar{U}_l|US}^n(u^n,s^n)|}{|\mathcal{T}_U^n| - KM} \leqslant \frac{\exp(-nI(\bar{U}_l \wedge US))(n+1)^{|\mathcal{U}|}}{1 - 2\hat{L}\exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}}.$$

So we can apply Lemma [24, Lemma A 1] with

$$a = \frac{\exp(-nI(\bar{U}_l \wedge US))(n+1)^{|\mathcal{U}|}}{1 - 2\hat{L}\exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}}.$$

We thus get for all $1 \leqslant l \leqslant \hat{L}$, $m \in [M]$ and

$$Z_{(P_{U\bar{U}_l S}, u^n, s^n)}^{m,l} = \sum_{k\in[K]} f_{k,m}^{(P_{U\bar{U}_l S}, u^n, s^n)}(U_{1,m}, \cdots, U_{k,m})$$

that

$$\Pr(Z_{(P_{U\bar{U}_l S}, u^n, s^n)}^{m,l} > Kt) \leqslant \exp(-K(t - a\log e)). \tag{4.35}$$

Choose an ϵ satisfying $0 < \epsilon < R$ and

$$t = \tfrac{1}{K} \exp(n(|R - I(\bar{U}_l \wedge US)|^+ + \epsilon)).$$

So $K(t - a \log e) \geqslant \exp(n\epsilon)/2$ if $n \geqslant n_1(\epsilon, \hat{L})$, where we define $n_1(\epsilon, \hat{L})$ as

$$\min\{n \colon 0 < \tfrac{2(n+1)^{|\mathcal{U}|} \hat{L} \log e}{1 - 2\hat{L} \exp(n(-H(U|X)+\delta))(n+1)^{|\mathcal{U}|}} < \tfrac{1}{2} \exp(n\epsilon)\}.$$

If $\mathcal{T}^n_{\bar{U}_l|US}(u^n, s^n)$ is replaced by $\mathcal{T}^n_{\bar{U}_l|S}(s^n)$ then analogously we get for

$$f^{(P_{\bar{U}_l S}, s^n)}_{k,m}(U_{1,m}, \cdots, U_{k,m}) = \mathbb{1}_{\mathcal{T}_{\bar{U}_l|S}(s^n)}(U_{k,m})$$

and $Z^{m,l}_{(P_{\bar{U}_l S}, s^n)} = \sum_{k \in [K]} f^{(P_{\bar{U}_l S}, s^n)}_{k,m}(U_{1,m}, \cdots, U_{k,m})$

$$\Pr(Z^{m,l}_{(P_{\bar{U}_l S}, s^n)} > \exp(n(|R - I(\bar{U}_l \wedge S)|^+ + \epsilon))) \leqslant \exp(-\tfrac{1}{2} \exp(n\epsilon))$$

for $n > n_1(\epsilon, \hat{L})$. Equivalently, as done in [31, Proof of Lemma 1], if $\mathcal{T}^n_{\bar{U}_l|S}(s^n)$ is replaced by $\mathcal{T}^n_{U|S}(s^n)$ and ϵ with $\frac{\epsilon}{2} + \log(\hat{L})/n$ we get for

$$f^{(P_{US}, s^n)}_{k,m}(U_{1,m}, \cdots, U_{k,m}) = \mathbb{1}_{\mathcal{T}_{U|S}(s^n)}(U_{k,m})$$

and $Z^{m}_{(P_{US}, s^n)} = \sum_{k \in [K]} f^{(P_{US}, s^n)}_{k,m}(U_{1,m}, \cdots, U_{k,m})$

$$\Pr(Z^{m}_{(P_{US}, s^n)} > \hat{L} \exp(n(|R - I(U \wedge S)|^+ + \epsilon/2))) \leqslant \exp(-\tfrac{\hat{L}}{2} \exp(n\epsilon/2))$$

for $n > n_1(\epsilon/2, 1)$. If $I(U \wedge S) \geqslant \epsilon$ then

$$|R - I(U \wedge S)|^+ = R - \min\{R, I(U \wedge S)\} \leqslant R - \epsilon$$

(as $R \geqslant \epsilon$). So

$$\Pr(\tfrac{1}{K} Z^{m}_{(P_{US}, s^n)} > \exp(-n\epsilon/2)) < \exp(-\tfrac{\hat{L}}{2} \exp(n\epsilon/2)).$$

As in [31] denote by $\mathcal{P}_{\hat{L}}$ the set of all subsets of $[K]$ with cardinality $\hat{L}$ and by $\mathcal{P}_{\hat{L},k}$, $k \in [K]$, the collection of sets in $\mathcal{P}_{\hat{L}}$ that do not contain k. Now it is clear that continuing, using the same steps as in [31, Proof of Lemma 1], we also get for all $m \in [M]$

$$\Pr(|\{J \in \mathcal{P}_{\hat{L}} \colon (u^n, U_{J,m}, s^n) \in \mathcal{T}^n_{U\bar{U}^{\hat{L}}S}\}| > \exp(n\epsilon)) < \hat{L} \exp(-\tfrac{1}{2} \exp(n\epsilon/\hat{L}))$$

for $R < \min_{l \in [\hat{L}]} I(\bar{U}_l \wedge S)$ and $n \geqslant n_1(\epsilon/\hat{L}, \hat{L})$. (Here we use the notation from [31, Proof of Lemma 1]. For $J \in \mathcal{P}_{\hat{L}}$, $J = \{j_1, \cdots, j_{\hat{L}}\}$ we denote by $U_{J,m}$ the ordered $\hat{L}$-tuple $(U_{j_1,m}, \cdots, U_{j_{\hat{L}},m})$ where the indices are ordered as $j_1 < j_2 < \cdots < j_{\hat{L}}$.) Still using the

steps from [31, Proof of Lemma 1] we additionally get

$$\begin{aligned}&\Pr(K^{-1}|\{k\colon (U_{k,m}, U_{J,m}, s^n) \in \mathcal{T}^n_{U\bar{U}^{\hat{L}}S} \text{ for some } J \in \mathcal{P}_{\hat{L},k}\}| > \exp(-n\epsilon/2))\\ &\leqslant (\hat{L}+1)\exp(n\epsilon/6 - \tfrac{1}{2}\exp(n\epsilon/4\hat{L})).\end{aligned}$$

for $I(U \wedge \bar{U}^{\hat{L}}S) \geqslant \epsilon$, $R < \min_{l\in[\hat{L}]} I(\bar{U}_l \wedge S)$ and all $m \in [M]$, $n > \max\{n_1(\epsilon/(12\hat{L}), 1), \log(2\hat{L})\}$ and n large enough such that

$$n(\hat{L}+1)^2(\log|\mathcal{U}|+1) \leqslant \exp(n\epsilon/6)$$

and finally

$$\begin{aligned}&\Pr(K^{-1}|\{k\colon (U_{k,m}, U_{i,m}, s^n) \in \mathcal{T}^n_{U\bar{U}_lS} \text{ for some } i \in \mathcal{P}_{1,k}\}| > \exp(-n\epsilon/2))\\ &\leqslant 2\exp(n\epsilon/6 - \tfrac{1}{2}\exp(n\epsilon/4)).\end{aligned}$$

for $I(U \wedge \bar{U}_l S) - |R - I(\bar{U}_l \wedge S)|^+ \geqslant \epsilon$ and all $l \in [\hat{L}]$, $m \in [M]$ and $n > n_1(\epsilon/12, 1)$ and n large enough such that

$$n4(\log|\mathcal{U}|+1) \leqslant \exp(n\epsilon/6).$$

As $|\mathcal{T}^n_U|$, $|\mathcal{T}^n_X|$, $|\mathcal{S}^n|$, $|\mathcal{P}(n, \mathcal{U}\times\mathcal{U}^{\hat{L}}\times\mathcal{S})|$ and M increase exponentially with respect to n we can use the union bound to show that the probability that $\mathcal{J}$ has the following properties is greater than 0. This follows as we showed that the probabilities of the corresponding complementary events each go to 0 doubly exponentially with respect to n. So for all n large enough there is a $\mathcal{J}$ such that (4.33) holds for all $x^n \in \mathcal{T}^n_X$ and for all $m \in [M]$, all $u^n \in \mathcal{T}^n_U$, all $s^n \in \mathcal{S}^n$ and all $P_{U\bar{U}^{\hat{L}}S} \in \mathcal{P}(n, \mathcal{U}\times\mathcal{U}^{\hat{L}}\times\mathcal{S})$ we have

$$\begin{aligned}&K^{-1}|\{k\colon u_{k,m} \in \mathcal{T}^n_{U|S}(s^n)\}| \leqslant \exp(-n\epsilon/2))\\ &\text{for } I(U \wedge S) \geqslant \epsilon\end{aligned}$$

$$\begin{aligned}&K^{-1}|\{k\colon (u_{k,m}, u_{i,m}, s^n) \in \mathcal{T}^n_{U\bar{U}_lS} \text{ for some } i \neq k\}| \leqslant \exp(-n\epsilon/2)\\ &\text{for } I(U \wedge \bar{U}_l S) \geqslant |R - I(\bar{U}_l \wedge S)|^+ + \epsilon \text{ and all } l \in [\hat{L}]\end{aligned}$$

$$\begin{aligned}&|\{k\colon (u^n, u_{k,m}, s^n) \in \mathcal{T}^n_{U\bar{U}_lS}\}| \leqslant \exp(n(|R - I(\bar{U}_l \wedge US)|^+ + \epsilon))\\ &\text{for all } l \in [\hat{L}]\end{aligned}$$

$$\begin{aligned}&|\{J \in \mathcal{P}_{\hat{L}}\colon (u^n, u_{J,m}, s^n) \in \mathcal{T}^n_{U\bar{U}^{\hat{L}}S}\}| \leqslant \exp(n\epsilon)\\ &\text{for } R < \min_{l\in[\hat{L}]} I(\bar{U}_l \wedge S)\end{aligned}$$

$$K^{-1}|\{k\colon (u_{k,m}, u_{J,m}, s^n) \in \mathcal{T}^n_{U\bar{U}^{\hat{L}}S} \text{ for some } J \in \mathcal{P}_{\hat{L},k}\}| \leqslant \exp(-n\epsilon/2)$$
$$\text{for } R < \min_{l\in[\hat{L}]} I(\bar{U}_l \wedge S) \text{ and } I(U \wedge \bar{U}^{\hat{L}}S) \geqslant \epsilon.$$

Comparing the properties above and our choice of R with [31, Proof of Lemma 3] it is clear that we can show for each $m \in [M]$ that (4.34) holds by following the steps in [31, Proof of Lemma 3]. $|\mathcal{L}(y^n, m)| \leqslant \hat{L}$ for all $y^n \in \mathcal{Y}^n$ and $m \in [M]$ follows from [31, Lemma 2].

■

Now we can prove Lemma 4.13.

Lemma 4.13. *Consider the RVs $\tilde{X}$ and $\{\tilde{Y}_s\}_{s\in\mathcal{S}}$, $|\mathcal{S}| < \infty$ with $P_{\tilde{X}\tilde{Y}_s} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ for all $s \in \mathcal{S}$ and a RV $\tilde{U}$ such that $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$, $P_{\tilde{U}} \in \mathcal{P}(\mathcal{U})$. Denote the symmetrizability of the AVC corresponding to $\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}}$ by $\hat{M}$ and assume $\hat{M} < \infty$. Let $\hat{L} = \hat{M} + 1$ and $\delta > 0$. For all n large enough there is a stochastic matrix $F \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}|\mathcal{X}^n)$ and a mapping $g\colon \mathcal{Y}^n \times \bar{\mathcal{M}} \to \hat{\mathcal{P}}_{\hat{L}}$ such that for RVs K, $\bar{M}$, $\{\hat{K}_{s^n}\}_{s^n\in\mathcal{S}^n}$ and $\tilde{X}^n$ with $P_{K\bar{M}\hat{K}_{s^n}\tilde{X}^n} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}\times\hat{\mathcal{P}}_{\hat{L}}\times\mathcal{X}^n)$ for all $s^n \in \mathcal{S}^n$ defined by*

$$P_{K\bar{M}\hat{K}_{s^n}\tilde{X}^n}(k,\bar{m},\hat{k},x^n) = \sum_{y^n\in\mathcal{Y}^n}\prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i)F(k,\bar{m}|x^n)\mathbb{1}_{g^{-1}(\hat{k})}((y^n,\bar{m}))$$

for $(k,\bar{m},\hat{k},x^n) \in \mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n$ it holds that

$$\sum_{\bar{m}\in\bar{\mathcal{M}}} Pr(\bar{M}=\bar{m}) \max_{s^n\in\mathcal{S}^n} Pr(K \notin \hat{K}_{s^n}|\bar{M}=\bar{m}) \leqslant \delta \tag{4.36}$$
$$H(K|\bar{M}) = \log|\mathcal{K}| \tag{4.37}$$
$$\tfrac{1}{n}\log\tfrac{|\mathcal{K}|}{\hat{L}} \geqslant \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) - \delta \tag{4.38}$$
$$\tfrac{1}{n}\log|\bar{\mathcal{M}}| \leqslant I(\tilde{U}\wedge\tilde{X}) - \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) + \delta. \tag{4.39}$$

Proof. Assume first that $H(\tilde{U}|\tilde{X}) > 0$. The case $H(\tilde{U}|\tilde{X}) = 0$ is treated at the end of the proof. Additionally assume that $\min_{u\in\mathcal{U}} P_{\tilde{U}}(u), \min_{x\in\mathcal{X}} P_{\tilde{X}}(x) \geqslant \bar{\beta} > 0$ for $\bar{\beta}$ small enough. (Note that (4.36) - (4.39) depend on $\mathcal{X}$ and $\mathcal{U}$ only via the support of $P_{\tilde{U}}$ and $P_{\tilde{X}}$.) We can also assume that

$$\min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) > 0,$$

because otherwise the result follows trivially. Choose $\delta_1, \delta_2 > 0$ and $q \in \mathbb{N}$ such that $\epsilon_1(q) + \epsilon_3(q) + \tau_2(q, \delta_1+\delta_2)/q < \delta/2$ where the functions $\epsilon_1, \epsilon_3\colon \mathbb{N}\to\mathbb{R}$ and $\tau_2\colon \mathbb{N}\times\mathbb{R}\to\mathbb{R}$ are determined at the end of the proof. So $n = \lfloor\frac{n}{q}\rfloor q + r$ for $0 \leqslant r < q$. Consider RVs

$\{U_t\}_{t\in[T]}$, $\{X_t\}_{t\in[T]}$ and $\{Y_{s^q}\}_{s^q\in\mathcal{S}^q}$ with $T \leqslant |\mathcal{P}(\lfloor\frac{n}{q}\rfloor, \mathcal{X}^q)|$ such that

$$P_{U_tX_tY_{s^q}} \in \mathcal{P}((\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q\times\mathcal{Y}^q)$$

and $P_{U_tX_t} \in \mathcal{P}(\lfloor\frac{n}{q}\rfloor, (\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q)$,

$$P_{U_tX_tY_{s^q}}((u^{q-1},x),x^q,y^q) = P_{U_tX_t}((u^{q-1},x),x^q)\prod_{i=1}^{q} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i)$$

for all $((u^{q-1},x),x^q,y^q) \in (\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q\times\mathcal{Y}^q$ for all $s^q\in\mathcal{S}^q$ and $t\in[T]$ while $\{\mathcal{T}_{X_t}^{\lfloor\frac{n}{q}\rfloor}\}_{t\in[T]}$ forms a partition of $\mathcal{T}_{X_q,\delta_1}^{\lfloor\frac{n}{q}\rfloor}$ and

$$|P_{U_tX_t}(u,x) - P_{U_qX_q}(u,x)| \leqslant \delta_1+\delta_2 \tag{4.40}$$

for all $(u,x)\in(\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q$, where U_qX_q are RVs such that $P_{U_qX_q}\in\mathcal{P}((\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q)$ with

$$P_{U_qX_q}((u^{q-1},x),x^q) = P_{\tilde{U}\tilde{X}}^{\otimes q-1}\otimes P_{\tilde{X}}(u^{q-1},x^{q-1},x_q)\mathbb{1}_{\{x\}}(x_q).$$

Such RVs exist which can be seen as follows. First choose $\{\mathcal{T}_{X_t}^{\lfloor\frac{n}{q}\rfloor}\}_{t\in[T]}$. Then consider $\{x_t\}_{t\in[T]}$ with $x_t\in\mathcal{T}_{X_t}^{\lfloor\frac{n}{q}\rfloor}$ for all $t\in[T]$. For each $t\in[T]$ choose a $u_t\in\mathcal{T}_{U_q|X_q,\delta_2}^{\lfloor\frac{n}{q}\rfloor}(x_t)$ (which implies that the qj-th component of u_t equals the qj-th component of x_t, for all $j\in[\lfloor\frac{n}{q}\rfloor]$). Define the RVs $\{U_t\}_{t\in[T]}$ with $P_{U_tX_t}=P_{u_t,x_t}$. (This construction of $P_{U_tX_t}$ is possible for n large enough, cf. [26, Chapter 2].)

Denote the symmetrizability of $\bar{\mathcal{W}} := \{P_{Y_{s^q}|U_t}\}_{s^q\in\mathcal{S}^q}$ by $\tilde{M}$ and assume $\tilde{M}>\hat{M}$. This means there exists a stochastic matrix $U\in\mathcal{P}(\mathcal{S}^q|(\mathcal{U}^{m-1}\times\mathcal{X})^{\tilde{M}})$ such that

$$\begin{aligned}&\sum_{s^q\in\mathcal{S}^q} P_{Y_{s^q}|U_t}(y^q|(u^{q-1},x))U(s^q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}}))\\ &= \sum_{s^q\in\mathcal{S}^q}\sum_{\bar{x}^q\in\mathcal{X}^q}\prod_{i=1}^{q} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|\bar{x}_i)P_{X_t|U_t}(\bar{x}^q|(u^{q-1},x))U(s^q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}}))\end{aligned}$$

is symmetric in $(u^{q-1},x),(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}})$. Summing over all $y^{q-1}\in\mathcal{Y}^{q-1}$ we get with $\bar{U}\in\mathcal{P}(\mathcal{S}|(\mathcal{U}^{m-1}\times\mathcal{X})^{\tilde{M}})$,

$$\bar{U}(s_q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}})) = \sum_{s^{q-1}\in\mathcal{S}^{q-1}} U(s^q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}}))$$

that

$$\sum_{s_q\in\mathcal{S}}\sum_{\bar{x}_q\in\mathcal{X}} P_{\tilde{Y}_{s_q}|\tilde{X}}(y_q|\bar{x}_q)\sum_{\bar{x}^{q-1}\in\mathcal{X}^{q-1}} P_{X_t|U_t}(\bar{x}^q|(u^{q-1},x))\bar{U}(s_q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}}))$$
$$=\sum_{s_q\in\mathcal{S}} P_{\tilde{Y}_{s_q}|\tilde{X}}(y_q|x)\sum_{\bar{x}^{q}\in\mathcal{X}^{q}} P_{X_t|U_t}(\bar{x}^q|(u^{q-1},x))\bar{U}(s_q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}}))$$

where the last step follows as

$$\sum_{\bar{x}^{q-1}\in\mathcal{X}^{q-1}} P_{X_t|U_t}(\bar{x}^q|(u^{q-1},x))=0$$

for $\bar{x}_q\neq x$. This equals

$$\sum_{s_q\in\mathcal{S}} P_{\tilde{Y}_{s_q}|\tilde{X}}(y_q|x)\bar{U}(s_q|(u_1^{q-1},x_1),\cdots,(u_{\tilde{M}}^{q-1},x_{\tilde{M}})).$$

Thus this expression is symmetric in $x,x_1,\cdots,x_{\tilde{M}}$ for an arbitrary choice of $u_1^{q-1},\cdots,u_{\tilde{M}}^{q-1}$. It follows that $\bar{\mathcal{W}}:=\{P_{Y_{s^q}|U_t}\}_{s^q\in\mathcal{S}^q}$ has symmetrizability $\tilde{M}\leqslant\hat{M}$.

From $\min_{x\in\mathcal{X}} P_{\tilde{X}}(x)\geqslant\bar{\beta}$ we have for all $t\in[T]$ that for $\delta_1+\delta_2$ small enough

$$\min_u P_{U_t}(u)\geqslant\tilde{\beta}>0.$$

It is also clear from [26, Lemma 2.7] that for $\delta_1+\delta_2$ small enough

$$H(U_t|X_t)>0$$

and

$$\min_{W\in conv(\bar{\mathcal{W}})} I(P_{U_t},W)>0.$$

This can be seen as follows. Define RVs $\{\tilde{Y}_{s^q}\}_{s^q\in\mathcal{S}^q}$ such that for all $s^q\in\mathcal{S}^q$

$$P_{\tilde{Y}_{s^q}U_qX_q}(y^q,(u^{q-1},x),x^q)=\prod_{i=1}^{q} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i)P_{U_qX_q}((u^{q-1},x),x^q)$$

for all $(y^q,(u^{q-1},x),x^q)\in\mathcal{Y}^q\times(\mathcal{U}^{q-1}\times\mathcal{X})\times\mathcal{X}^q$. From (4.40) and [26, Lemma 2.7] we have for $\zeta>0$

$$\min_{W\in conv(\bar{\mathcal{W}})} I(P_{U_t},W)>\min_{W\in conv(\{P_{\tilde{Y}_{s^q}|U_q}\}_{s^q\in\mathcal{S}^q})} I(P_{U_q},W)-\zeta, \tag{4.41}$$

which is also discussed more explicitly in Lemma 4.11. For all convex combinations $W\in conv(\{P_{\tilde{Y}_{s^q}|U_q}\}_{s^q\in\mathcal{S}^q})$ consider the corresponding $P_{S^q}\in\mathcal{P}(\mathcal{S}^q)$ with marginals $P_{S_i}\in\mathcal{P}(\mathcal{S})$, $i\in\{1,\cdots,q\}$. Define $W_i\in\mathcal{P}(\mathcal{Y}|\mathcal{U})$ such that $W_i(y|u)=\sum_{s\in\mathcal{S}} P_{S_i}(s)P_{\tilde{Y}_s|\tilde{U}}(y|u)$,

$i \in \{1, \cdots, q-1\}$, and $W_q \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $W_q(y|x) = \sum_{s\in\mathcal{S}} P_{S_q}(s) P_{\tilde{Y}_s|\tilde{X}}(y|x)$ for all $(x, y, u) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{U}$. According to Lemma 3.9 we have

$$\begin{aligned}\min_{W\in conv(\{P_{\tilde{Y}_{s^q}|U_q}\}_{s^q\in\mathcal{S}^q})} I(P_{U_q}, W) &\geqslant \min_{W\in conv(\{P_{\tilde{Y}_{s^q}|U_q}\}_{s^q\in\mathcal{S}^q})} \sum_{i=1}^{q-1} I(P_{\tilde{U}}, W_i) + I(P_{\tilde{X}}, W_q) \\ &= (q-1) \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\})_{s\in\mathcal{S}}} I(P_{\tilde{U}}, W) \\ &\quad + \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{X}}\})_{s\in\mathcal{S}}} I(P_{\tilde{X}}, W). \quad (4.42)\end{aligned}$$

For each $t \in [T]$ generate the set $\mathcal{J}_t$ accoding to Theorem 4.12 with

$$\min_{W\in conv(\bar{\mathcal{W}})} I(P_{U_t}, W) - \tau < R < \min_{W\in conv(\bar{\mathcal{W}})} I(P_{U_t}, W) - 2\tau/3,$$

with $\tau > 0$ (and the corresponding K, M_t and L_t), where the RVs corresponding to U, X and $\{Y_s\}_{s\in\mathcal{S}}$ are U_t, X_t and $\{Y_{s^q}\}_{s^q\in\mathcal{S}^q}$ and the block length (corresponding to n in Theorem 4.12) is $\lfloor \frac{n}{q} \rfloor$.

We define for all $t \in [T]$

$$\mathcal{T}_{X,t} := \mathcal{T}_{X_t}^{\lfloor \frac{n}{q} \rfloor}$$

and for $x^{n-r} \in \mathcal{X}^{n-r}$

$$\mathcal{T}_{U|X,t}(x^{n-r}) := \mathcal{T}_{U_t|X_t}^{\lfloor \frac{n}{q} \rfloor}(x^{n-r}).$$

For all $t \in [T]$ define for all $u_q \in \mathcal{J}_t$

$$\begin{aligned}\tilde{Q}_t(u_q) &= \sum_{x^{n-r}\in\mathcal{X}^{n-r}} \frac{1}{|\mathcal{T}_{X,t}|} \frac{\mathbb{1}_{\mathcal{J}_t\cap\mathcal{T}_{U|X,t}(x^{n-r})}(u_q)}{|\mathcal{J}_t\cap\mathcal{T}_{U|X,t}(x^{n-r})|} \\ &= \sum_{x^{n-r}\in\mathcal{X}^{n-r}} \frac{1}{|\mathcal{T}_{X,t}|} \frac{\mathbb{1}_{\mathcal{T}_{U|X,t}(x^{n-r})}(u_q)}{|\mathcal{J}_t\cap\mathcal{T}_{U|X,t}(x^{n-r})|} \\ &= \sum_{x^{n-r}\in\mathcal{T}_{X|U,t}(u_q)} \frac{1}{|\mathcal{T}_{X,t}||\mathcal{J}_t\cap\mathcal{T}_{U|X,t}(x^{n-r})|}\end{aligned}$$

and $Q_t = \min_{u_q\in\mathcal{J}_t} \tilde{Q}_t(u_q)$. From (4.33) we know that for $t \in [T]$ and all $u_q \in \mathcal{J}_t$

$$\frac{1}{1+\exp(-\lfloor \frac{n}{q} \rfloor c_1)} \frac{1}{L_t} < \tilde{Q}_t(u_q) < \frac{1}{1-\exp(-\lfloor \frac{n}{q} \rfloor c_1)} \frac{1}{L_t}. \quad (4.43)$$

Let $u^* \in (\mathcal{U}^{q-1} \times \mathcal{X})^{\lfloor \frac{n}{q} \rfloor} \setminus \bigcup_{t\in[T]} \mathcal{J}_t$. Consider the RV U_{n-r}, $P_{U_{n-r}} \in \mathcal{P}((\mathcal{U}^{q-1} \times \mathcal{X})^{\lfloor \frac{n}{q} \rfloor})$,

such that for $x^{n-r} \in \mathcal{T}_{X,t}$, $t \in [T]$

$$P_{U_{n-r}|\tilde{X}^{n-r}}(u_q|x^{n-r}) = \frac{Q_t}{\tilde{Q}_t(u_q)} \frac{1}{|\mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})|}$$

for $u_q \in \mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})$,

$$P_{U_{n-r}|\tilde{X}^{n-r}}(u_q|x^{n-r}) = 1 - \sum_{u \in \mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})} \frac{Q_t}{\tilde{Q}_t(u)} \frac{1}{|\mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})|}$$

for $u_q = u^*$ and

$$P_{U_{n-r}|\tilde{X}^{n-r}}(u_q|x^{n-r}) = 0$$

else and for $x^{n-r} \in \mathcal{X}^{n-r} \backslash \bigcup_{t \in [T]} \mathcal{T}_{X,t}$

$$P_{U_{n-r}|\tilde{X}^{n-r}}(u_q|x^{n-r}) = \begin{cases} 1 & u_q = u^* \\ 0 & \text{else} \end{cases}.$$

We have for $t \in [T]$ and all $u_q \in \mathcal{J}_t$

$$\begin{aligned} &\Pr(U_{n-r} = u_q | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\ &= \sum_{x^{n-r} \in \mathcal{T}_{X,t}} \Pr(U_{n-r} = u_q | \tilde{X}^{n-r} = x^{n-r}) \Pr(\tilde{X}^{n-r} = x^{n-r} | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\ &= \sum_{x^{n-r} \in \mathcal{T}_{X,t}} \Pr(U_{n-r} = u_q | \tilde{X}^{n-r} = x^{n-r}) \frac{1}{|\mathcal{T}_{X,t}|} \\ &= \sum_{x^{n-r} \in \mathcal{X}^{n-r}} \frac{Q_t}{\tilde{Q}_t(u_q)} \frac{\mathbb{1}_{\mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})}(u_q)}{|\mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})|} \frac{1}{|\mathcal{T}_{X,t}|} = Q_t. \end{aligned} \tag{4.44}$$

For $t \in [T]$ and all $x^{n-r} \in \mathcal{T}_{X,t}$ we have

$$\begin{aligned} \Pr(U_{n-r} \neq u^* | \tilde{X}^{n-r} = x^{n-r}) &= \sum_{u \in \mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})} \frac{Q_t}{\tilde{Q}_t(u)} \frac{1}{|\mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})|} \\ &> L_t(1 - \exp(-\lfloor \tfrac{n}{q} \rfloor c_1)) Q_t \\ &> \frac{1-\exp(-\lfloor \frac{n}{q} \rfloor c_1)}{1+\exp(-\lfloor \frac{n}{q} \rfloor c_1)} = 1 - \frac{2\exp(-\lfloor \frac{n}{q} \rfloor c_1)}{1+\exp(-\lfloor \frac{n}{q} \rfloor c_1)}. \end{aligned}$$

Now we consider for $t \in [T]$, $x^{n-r} \in \mathcal{T}_{X,t}$ and $u_q \in \mathcal{J}_t \cap \mathcal{T}_{U|X,t}(x^{n-r})$

$$\Pr(\tilde{X}^{n-r} = x^{n-r} | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}, U_{n-r} = u_q) = \frac{\Pr(\tilde{X}^{n-r} = x^{n-r}, U_{n-r} = u_q | \tilde{X}^{n-r} \in \mathcal{T}_{X,t})}{\Pr(U_{n-r} = u_q | \tilde{X}^{n-r} \in \mathcal{T}_{X,t})}$$

which equals

$$\begin{aligned}\frac{\Pr(\tilde{X}^{n-r}=x^{n-r}|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\Pr(U_{n-r}=u_q|\tilde{X}^{n-r}=x^{n-r})}{Q_t} &= \frac{Q_t}{\tilde{Q}_t(u_q)}\frac{1}{|\mathcal{J}_t\cap\mathcal{T}_{U|X,t}(x^{n-r})|}\frac{1}{Q_t|\mathcal{T}_{X,t}|}\\ &= \frac{1}{|\mathcal{T}_{X,t}||\mathcal{J}_t\cap\mathcal{T}^n_{U|X,t}(x^{n-r})|\tilde{Q}_t(u_q)}.\end{aligned}$$

From (4.33) and (4.43) this implies

$$\Pr(\tilde{X}^{n-r}=x^{n-r}|\tilde{X}^{n-r}\in\mathcal{T}_{X,t},U_{n-r}=u_q) < \frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1-\exp(-\lfloor\frac{n}{q}\rfloor c_1)}\frac{1}{|\mathcal{T}_{X|U,t}(u_q)|}, \tag{4.45}$$

where $\mathcal{T}_{X|U,t}(u_q) = \mathcal{T}^{\lfloor\frac{n}{q}\rfloor}_{X_t|U_t}(u_q)$. We also know $\Pr(\tilde{X}^{n-r}=x^{n-r}|\tilde{X}^{n-r}\in\mathcal{T}_{X,t},U_{n-r}=u_q)=0$ for $u_q\notin\mathcal{T}_{U|X,t}(x^{n-r})$. Define $\mathcal{K}=[K]$, $\mathcal{M}=[\max_{t\in[T]}M_t]$ and $\bar{\mathcal{M}}=\mathcal{M}\times[T]$. Let $x^{n-r}\in\mathcal{T}_{X,t}$, $t\in[T]$. We define for $k\in\mathcal{K}$ and $m\in[M_t]$

$$F(k,(m,t)|x^n) = \Pr(U_{n-r}=u^t_{k,m}|\tilde{X}^{n-r}=x^{n-r}) + \Pr(U_{n-r}=u^*|\tilde{X}^{n-r}=x^{n-r})\tfrac{1}{L_t},$$

where we denote the elements in $\mathcal{J}_t$ by $u^t_{k,m}$ for all $k\in[K]$ and $m\in[M_t]$. For

$$M_t < m \leqslant \max_{t\in[T]} M_t$$

and $k\in\mathcal{K}$ we define

$$F(k,(m,t)|x^n)=0.$$

For $\bar{t}\in[T]$, $\bar{t}\neq t$ we define for $(k,m)\in\mathcal{K}\times\mathcal{M}$

$$F(k,(m,\bar{t})|x^n)=0.$$

Let $x^{n-r}\in\mathcal{X}^{n-r}\setminus\bigcup_{t\in[T]}\mathcal{T}_{X,t}$. We define

$$F(k,(m,t)|x^n)=\tfrac{1}{K\sum_{t\in[T]}M_t}$$

for all $(k,m,t)\in\mathcal{K}\times\mathcal{M}\times[T]$ with $m\leqslant M_t$. (Here $x^n=(x^{n-r},x^r)$ with and arbitrary $x^r\in\mathcal{X}^r$.) For $(k,m,t)\in\mathcal{K}\times\mathcal{M}\times[T]$ with $m>M_t$ we define

$$F(k,(m,t)|x^n)=0.$$

For $k \in \mathcal{K}$ and $(m,t) \in \mathcal{M} \times [T]$ such that $m \in [M_t]$ consider

$$\begin{aligned}
&\Pr(K=k, \bar{M}=(m,t)) \\
&= \sum_{\bar{t}\in[T]} \Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,\bar{t}}) \Pr(K=k, \bar{M}=(m,t) | \tilde{X}^{n-r} \in \mathcal{T}_{X,\bar{t}}) \\
&\qquad + \Pr(K=k, \bar{M}=(m,t) | \tilde{X}^{n-r} \in \mathcal{X}^{n-r} \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}_{X,\bar{t}}) \\
&\qquad\qquad \cdot \Pr(\tilde{X}^{n-r} \in \mathcal{X}^{n-r} \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}_{X,\bar{t}}) \\
&= \Pr(K=k, \bar{M}=(m,t) | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\
&\qquad + \tfrac{1}{K \sum_{t\in[T]} M_t} \Pr(\tilde{X}^{n-r} \in \mathcal{X}^{n-r} \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}_{X,\bar{t}})
\end{aligned}$$

where we use the properties of $F(k,(m,t)|x^n)$ for the last step. We have

$$\begin{aligned}
&\Pr(K=k, \bar{M}=(m,t) | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\
&= \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \Pr(K=k, \bar{M}=(m,t) | \tilde{X}^{n-r} = x^{n-r}) \\
&= \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \Pr(U_{n-r} = u^t_{k,m} | \tilde{X}^{n-r} = x^{n-r}) \\
&+ \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \tfrac{1}{L_t} \Pr(U_{n-r} = u^* | \tilde{X}^{n-r} = x^{n-r}).
\end{aligned}$$

The first summand equals

$$\begin{aligned}
&\sum_{x^{n-r}\in\mathcal{T}_{X,t}} \Pr(\tilde{X}^{n-r} = x^{n-r} | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \Pr(U_{n-r} = u^t_{k,m} | \tilde{X}^{n-r} = x^{n-r}, \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\
&= \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \Pr(U_{n-r} = u^t_{k,m} | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \Pr(\tilde{X}^{n-r} = x^{n-r} | U_{n-r} = u^t_{k,m}, \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\
&= Q_t.
\end{aligned}$$

For the second summand we have

$$\tfrac{1}{L_t} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \Pr(U_{n-r} = u^* | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \Pr(\tilde{X}^{n-r} = x^{n-r} | U_{n-r} = u^*, \tilde{X}^{n-r} \in \mathcal{T}_{X,t}).$$

As

$$\sum_{u\in\mathcal{J}_t\cup\{u^*\}} \Pr(U_{n-r} = u | \tilde{X}^{n-r} = x^{n-r}) = 1$$

we have

$$\Pr(U_{n-r} = u^* | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) = 1 - L_t Q_t.$$

So we have

$$\Pr(K = k, \bar{M} = (m,t) | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) = Q_t + \tfrac{1}{L_t} - Q_t = \tfrac{1}{L_t}. \tag{4.46}$$

Thus

$$\Pr(K = k, \bar{M} = (m,t)) = \tfrac{1}{L_t}\Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,t}) + \tfrac{1}{K\sum_{t\in[T]} M_t}\Pr(\tilde{X}^{n-r} \in \mathcal{X}^{n-r} \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}_{X,\bar{t}})$$

and consequently

$$\Pr(\bar{M} = (m,t)) = \tfrac{1}{M_t}\Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,t}) + \tfrac{1}{\sum_{t\in[T]} M_t}\Pr(\tilde{X}^{n-r} \in \mathcal{X}^{n-r} \setminus \bigcup_{\bar{t}\in[T]} \mathcal{T}_{X,\bar{t}})$$

which implies

$$\Pr(K = k | \bar{M} = (m,t)) = \frac{\frac{1}{L_t}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t}) + \frac{1}{K\sum_{t\in[T]} M_t}\Pr(\tilde{X}^{n-r}\in\mathcal{X}^{n-r}\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}_{X,\bar{t}})}{\frac{1}{M_t}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t}) + \frac{1}{\sum_{t\in[T]} M_t}\Pr(\tilde{X}^{n-r}\in\mathcal{X}^{n-r}\setminus\bigcup_{\bar{t}\in[T]}\mathcal{T}_{X,\bar{t}})} = \tfrac{1}{K}.$$

So $H(K|\bar{M}) = \log|\mathcal{K}|$.

Now consider

$$\begin{aligned}
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \max_{s^n\in\mathcal{S}^n} \Pr(K \notin \hat{K}_{s^n} | \bar{M} = (m,t)) = \\
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \Big(\max_{s^n\in\mathcal{S}^n} \sum_{\bar{t}\in[T]} \Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,\bar{t}} | \bar{M} = (m,t)) \\
&\qquad \cdot \Pr(K \notin \hat{K}_{s^n} | \bar{M} = (m,t), \tilde{X}^{n-r} \in \mathcal{T}_{X,\bar{t}}) \\
&\qquad + \Pr(K \notin \hat{K}_{s^n} | \bar{M} = (m,t), \tilde{X}^{n-r} \notin \mathcal{T}^{\lfloor \frac{n}{q} \rfloor}_{\tilde{X}^q,\delta_1}) \Pr(\tilde{X}^{n-r} \notin \mathcal{T}^{\lfloor \frac{n}{q} \rfloor}_{\tilde{X}^q,\delta_1} | \bar{M} = (m,t)) \Big)
\end{aligned}$$

which can be upper bounded by

$$\begin{aligned}
&\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t) \Big(\max_{s^n\in\mathcal{S}^n} \Pr(\tilde{X}^{n-r} \in \mathcal{T}_{X,t} | \bar{M} = (m,t)) \\
&\qquad \cdot \Pr(K \notin \hat{K}_{s^n} | \bar{M} = (m,t), \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \\
&\qquad + \max_{s^n\in\mathcal{S}^n} \Pr(K \notin \hat{K}_{s^n} | \bar{M} = (m,t), \tilde{X}^{n-r} \notin \mathcal{T}^{\lfloor \frac{n}{q} \rfloor}_{\tilde{X}^q,\delta_1}) \\
&\qquad \cdot \Pr(\tilde{X}^{n-r} \notin \mathcal{T}^{\lfloor \frac{n}{q} \rfloor}_{\tilde{X}^q,\delta_1} | \bar{M} = (m,t)) \Big)
\end{aligned}$$

which is less or equal than

$$\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t)\Big(\max_{s^n\in\mathcal{S}^n}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t}|\bar{M}=(m,t)) \cdot \Pr(K\notin\hat{K}_{s^n}|\bar{M}=(m,t),\tilde{X}^{n-r}\in\mathcal{T}_{X,t}) + \Pr(\tilde{X}^{n-r}\notin\mathcal{T}^{\lfloor\frac{n}{q}\rfloor}_{\tilde{X}^q,\delta_1}|\bar{M}=(m,t))\Big).$$

This expression equals

$$\sum_{(m,t)\in\bar{\mathcal{M}}} P_{\bar{M}}(m,t)\max_{s^n\in\mathcal{S}^n}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t}|\bar{M}=(m,t)) \cdot \Pr(K\notin\hat{K}_{s^n}|\bar{M}=(m,t),\tilde{X}^{n-r}\in\mathcal{T}_{X,t}) + \Pr(\tilde{X}^{n-r}\notin\mathcal{T}^{\lfloor\frac{n}{q}\rfloor}_{\tilde{X}^q,\delta_1}). \tag{4.47}$$

Thus we now consider

$$\Pr(K\notin\hat{K}_{s^n}|\bar{M}=(m,t),\tilde{X}^{n-r}\in\mathcal{T}_{X,t})$$

for $(m,t)\in\bar{\mathcal{M}}$ and $s^n\in\mathcal{S}^n$.

$$\begin{aligned}&\Pr(K\notin\hat{K}_{s^n}|\bar{M}=(m,t),\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\\ &=\tfrac{\Pr(K\notin\hat{K}_{s^n}\wedge\bar{M}=(m,t)|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})}{\Pr(\bar{M}=(m,t)|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})}\\ &=M_t\Pr(K\notin\hat{K}_{s^n}\wedge\bar{M}=(m,t)|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\end{aligned}$$

which follows from (4.46). We will define g such that it only depends on y^{n-r}. So for all $x'\in\mathcal{X}^r$ and $y'\in\mathcal{Y}^r$ this expression equals

$$M_t\sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}}\sum_{y^{n-r}\in\mathcal{Y}^{n-r}}\sum_{x^{n-r}\in\mathcal{T}_{X,t}}\tfrac{1}{|\mathcal{T}_{X,t}|}\prod_{i=1}^{n-r}P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \cdot F(k,(m,t)|x^n)\mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)),$$

where $x^n = (x^{n-r}, x')$ and $y^n = (y^{n-r}, y')$. With our choice of $F(k,(m,t)|x^n)$ this equals

$$\begin{aligned}
&M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \\
&\quad \cdot \Pr(U_{n-r} = u^t_{k,m} | \tilde{X}^{n-r} = x^{n-r}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\
&+ M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \\
&\quad \cdot \Pr(U_{n-r} = u^* | \tilde{X}^{n-r} = x^{n-r}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).
\end{aligned}$$

The second summand can be upper bounded by

$$\begin{aligned}
&\tfrac{2\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)} M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \tfrac{1}{L_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)) \\
&\leqslant \tfrac{2\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)} M_t \sum_{\hat{k}\in\hat{P}_{\hat{L}}} \sum_{\substack{y^{n-r}\\ \in\mathcal{Y}^{n-r}}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \tfrac{1}{M_t} \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t))
\end{aligned}$$

which equals

$$\tfrac{2\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)} M_t \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \tfrac{1}{|\mathcal{T}_{X,t}|} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \tfrac{1}{M_t} = \tfrac{2\exp(-nc_1)}{1+\exp(-nc_1)}.$$

The first summand equals

$$\begin{aligned}
&M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \\
&\quad \cdot \Pr(U_{n-r} = u^t_{k,m}, \tilde{X}^{n-r} = x^{n-r} | \tilde{X}^{n-r} \in \mathcal{T}_{X,t}) \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t))
\end{aligned}$$

which equals

$$M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i)$$
$$\cdot \Pr(U_{n-r} = u^t_{k,m}|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t))$$
$$\cdot \Pr(\tilde{X}^{n-r} = x^{n-r}|U_{n-r}=u^t_{k,m}, \tilde{X}^{n-r}\in\mathcal{T}_{X,t})$$

Using (4.45) and (4.44) this can be upper bounded by

$$\frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1-\exp(-\lfloor\frac{n}{q}\rfloor c_1)} M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{\substack{y^{n-r}\\ \in\mathcal{Y}^{n-r}}} \sum_{\substack{x^{n-r}\\ \in\mathcal{T}_{X,t}}} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) \frac{1}{|\mathcal{T}_{X|U,t}(u^t_{k,m})|} Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)).$$

It is clear (cf. [26]) that for n large enough and $x^{n-r}\in\mathcal{T}_{X,t}$

$$\frac{1}{|\mathcal{T}_{X|U,t}(u^t_{k,m})|} \leqslant \frac{1}{\exp(\lfloor\frac{n}{q}\rfloor(H(X_t|U_t)-\xi))} = \exp(\lfloor\tfrac{n}{q}\rfloor\xi) P^{\otimes\lfloor\frac{n}{q}\rfloor}_{X_t|U_t}(x^{n-r}|u^t_{k,m})$$

for $\xi>0$. So we get the upper bound

$$\frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{1-\exp(-\lfloor\frac{n}{q}\rfloor c_1)} \exp(\lfloor\tfrac{n}{q}\rfloor\xi) M_t \sum_{\substack{k\in\mathcal{K}\\ \hat{k}\in\hat{P}_{\hat{L}}\\ k\notin\hat{k}}} \sum_{y^{n-r}\in\mathcal{Y}^{n-r}} \sum_{x^{n-r}\in\mathcal{T}_{X,t}} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i)$$
$$\cdot P^{\otimes\lfloor\frac{n}{q}\rfloor}_{X_t|U_t}(x^{n-r}|u^t_{k,m}) Q_t \mathbb{1}_{g^{-1}(\hat{k})}(y^n,(m,t)). \tag{4.48}$$

We now define for $y^n\in\mathcal{Y}^n$, $t\in[T]$ and $m\in[M_t]$ the mapping g such that $k\in g(y^n,(m,t))$ (for $k\in\mathcal{K}$) if and only if

$$k\in\mathcal{L}^t_{y^{n-r},m}.$$

(It is clear that $|\mathcal{L}^t_{y^{n-r},m}|\leqslant\hat{L}$.) So together with (4.43) we can upper bound (4.48) by

$$\frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{(1-\exp(-\lfloor\frac{n}{q}\rfloor c_1))^2} \exp(\lfloor\tfrac{n}{q}\rfloor\xi) \tfrac{1}{M_t} M_t \tfrac{1}{K}$$
$$\cdot \sum_{k\in\mathcal{K}} \sum_{\substack{y^{n-r}:\\ k\notin\mathcal{L}^t_{y^{n-r},m}}} \sum_{x^{n-r}\in\mathcal{X}^{n-r}} \prod_{i=1}^{n-r} P_{\tilde{Y}_{s_i}|\tilde{X}}(y_i|x_i) P^{\otimes\lfloor\frac{n}{q}\rfloor}_{X_t|U_t}(x^{n-r}|u^t_{k,m}). \tag{4.49}$$

This equals

$$\frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{(1-\exp(-\lfloor\frac{n}{q}\rfloor c_1))^2}\exp(\lfloor\tfrac{n}{q}\rfloor\xi)\tfrac{1}{K}$$
$$\cdot\sum_{k\in\mathcal{K}}\sum_{y^{n-r}:\, k\notin\mathcal{L}^t_{y^{n-r},m}}\prod_{i=1}^{\lfloor\frac{n}{q}\rfloor}P_{Y_{(s^{n-r})_i}|U_t}((y^{n-r})_i|(u^t_{k,m})_i). \tag{4.50}$$

Here we use the notation

$$(s^{n-r})_i = (s_{(i-1)q+1},\cdots,s_{iq})$$
$$(y^{n-r})_i = (y_{(i-1)q+1},\cdots,y_{iq})$$
$$(u^t_{k,m})_i = (u_{(i-1)q+1},\cdots,u_{iq}),$$

where $u^{n-r} = u^t_{k,m}$, for the corresponding projections. (Note that $u^t_{k,m}$ denotes a sequence in $\mathcal{J}_t$ and thus we introduce this notation to access the components of $u^t_{k,m}$.) From our choice of R we can upper bound this expression for all $s^n\in\mathcal{S}^n$ and $t\in[T]$ by

$$\frac{1+\exp(-\lfloor\frac{n}{q}\rfloor c_1)}{(1-\exp(-\lfloor\frac{n}{q}\rfloor c_1))^2}\exp(\lfloor\tfrac{n}{q}\rfloor\xi)\exp(-\lfloor\tfrac{n}{q}\rfloor c_2) = \exp(-\lfloor\tfrac{n}{q}\rfloor c_3)$$

for a $c_3>0$, n large enough and an appropriate choice of ξ. We thus have

$$\sum_{(m,t)\in\bar{\mathcal{M}}}P_{\bar{M}}(m,t)\max_{s^n\in\mathcal{S}^n}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t}|\bar{M}=(m,t))$$
$$\cdot\Pr(K\notin\hat{K}_{s^n}|\bar{M}=(m,t),\tilde{X}^{n-r}\in\mathcal{T}_{X,t})$$
$$\leqslant\exp(-\lfloor\tfrac{n}{q}\rfloor c_3)$$
$$\cdot\sum_{(m,t)\in\bar{\mathcal{M}}}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\Pr(\bar{M}=(m,t)|\tilde{X}^{n-r}\in\mathcal{T}_{X,t}),$$

which equals

$$\exp(-\lfloor\tfrac{n}{q}\rfloor c_3)\sum_{t\in[T]}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\sum_{m\in[M_t]}\Pr(\bar{M}=(m,t)|\tilde{X}^{n-r}\in\mathcal{T}_{X,t})$$
$$=\exp(-\lfloor\tfrac{n}{q}\rfloor c_3)\sum_{t\in[T]}\Pr(\tilde{X}^{n-r}\in\mathcal{T}_{X,t})\leqslant\exp(-\lfloor\tfrac{n}{q}\rfloor c_3).$$

So considering (4.47), altogether the error probability goes to 0 exponentially with respect to $\lfloor\frac{n}{q}\rfloor$.

From our choice of R, (4.41) and (4.42) we know that

$$\begin{aligned}\tfrac{1}{n}\log\tfrac{|\mathcal{K}|}{\hat{L}} &\geqslant \tfrac{\lfloor\frac{n}{q}\rfloor}{\lfloor\frac{n}{q}\rfloor+1}\big(\tfrac{q-1}{q}\min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W)\\ &\qquad + \tfrac{1}{q}\min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}})} I(P_{\tilde{X}},W) - (\tau+\zeta)/q\big)\\ &\geqslant \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) - \epsilon_1(q) - \epsilon_2(q,n),\end{aligned}$$

where $\epsilon_1(q),\epsilon_2(q,n)>0$, $\epsilon_1(q)\to 0$ for $q\to\infty$ and $\epsilon_2(q,n)\to 0$ for $n\to\infty$ for all $q\in\mathbb{N}$. We also have

$$T \leqslant (\lfloor\tfrac{n}{q}\rfloor+1)^{|\mathcal{X}|^{q-1}|\mathcal{U}|}$$

and (from continuity of entropy [26, Lemma 2.7] and (4.40)) for $\tau_2(q,\delta_1+\delta_2)>0$

$$\begin{aligned}&\tfrac{1}{q}I(U_t\wedge X_t) \leqslant \tfrac{1}{q}(I(U_q\wedge X_q)+\tau_2(q,\delta_1+\delta_2))\\ &= I(\tilde{U}\wedge\tilde{X}) + \epsilon_3(q) + \tau_2(q,\delta_1+\delta_2)/q.\end{aligned}$$

where $\epsilon_3(q)>0$, $\epsilon_3(q)\to 0$ for $q\to\infty$ and $\tau_2(q,\delta_1+\delta_2)\to 0$ for $\delta_1+\delta_2\to 0$ for all $q\in\mathbb{N}$. So

$$\begin{aligned}\tfrac{1}{n}\log|\bar{\mathcal{M}}| &\leqslant I(\tilde{U}\wedge\tilde{X}) - \min_{\substack{W\in\\ conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})}} I(P_{\tilde{U}},W) + \epsilon_1(q)\\ &\quad + \tau_2(q,\delta_1+\delta_2)/q + \epsilon_3(q) + \epsilon_2(q,n) + \tfrac{|\mathcal{X}|^{q-1}|\mathcal{U}|}{n}\log(n).\end{aligned}$$

For the case $H(\tilde{U}|\tilde{X})=0$ we define a RV $\tilde{U}'$ with $P_{\tilde{U}'}\in\mathcal{P}(\mathcal{U}\cup\{u'\})$ for a $u'\notin\mathcal{U}$ such that

$$\|P_{\tilde{Y}_s\tilde{X}b(\tilde{U})} - P_{\tilde{Y}_s\tilde{X}\tilde{U}'}\|_1 \leqslant \epsilon$$

for an $\epsilon>0$ arbitrarily small, where $b\colon\mathcal{U}\to\mathcal{U}\cup\{u'\}$, $b(u)=u$. We can choose $\tilde{U}'$ such that at the same time $H(\tilde{U}'|\tilde{X})>0$. For this purpose define for all $x\in\mathcal{X}$

$$P_{\tilde{U}'|\tilde{X}}(u'|x) = \epsilon/2$$

and

$$P_{\tilde{U}'|\tilde{X}}(u|x) = P_{\tilde{U}|\tilde{X}}(u|x) - \epsilon/2$$

for the unique $u\in\mathcal{U}$ with $P_{\tilde{U}|\tilde{X}}(u|x)=1$. We then construct the protocol for this new RV $\tilde{U}'$. The corresponding rates of this protocol are arbitrarily close to the desired rates which follows from [26, Lemma 2.7], cf. Lemma 4.11. ∎

For the achievability part of Theorem 4.9 we now want to prove Lemma 4.15. For the proof we use the following auxiliary result.

Lemma 4.14. *Consider the RVs $\tilde{X}$ and $\{\tilde{Y}_s\}_{s\in\mathcal{S}}$, $|\mathcal{S}| < \infty$ with $P_{\tilde{X}\tilde{Y}_s} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ for all $s \in \mathcal{S}$, the RV $\tilde{U}$ such that $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$, $P_{\tilde{U}} \in \mathcal{P}(\mathcal{U})$ and the RV Γ, $P_\Gamma \in \mathcal{P}([n!])$ with $P_\Gamma(\gamma) = \frac{1}{n!}$ for all $\gamma \in [n!]$. Let $\delta > 0$. For all n large enough there is a stochastic matrix $F_{CR} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}|\mathcal{X}^n\times[n!])$ and a mapping $g_{CR}\colon \mathcal{Y}^n\times\bar{\mathcal{M}}\times[n!]\to\mathcal{K}$ such that for RVs K, $\bar{M}$, $\{\hat{K}_{s^n}\}_{s^n\in\mathcal{S}^n}$ and $\tilde{X}^n$ with $P_{K\bar{M}\hat{K}_{s^n}\tilde{X}^n} \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n)$ for all $s^n \in \mathcal{S}^n$ defined by*

$$P_{K\bar{M}\hat{K}_{s^n}\tilde{X}^n\Gamma}(k,\bar{m},\hat{k},x^n,\gamma) = \sum_{y^n\in\mathcal{Y}^n}\prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i)F_{CR}(k,\bar{m}|x^n,\gamma) \cdot \mathbb{1}_{g_{CR}^{-1}(\hat{k})}((y^n,\bar{m},\gamma))P_\Gamma(\gamma)$$

for $(k,\bar{m},\hat{k},x^n,\gamma) \in \mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n\times[n!]$ it holds that

$$\begin{aligned}
&\sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} Pr(K \neq \hat{K}_{s^n}|\bar{M}=\bar{m}) \leqslant \delta\\
&H(K|\bar{M}\Gamma) = \log|\mathcal{K}|\\
&\tfrac{1}{n}\log|\mathcal{K}| \geqslant \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) - \delta\\
&\tfrac{1}{n}\log|\bar{\mathcal{M}}| \leqslant I(\tilde{U}\wedge\tilde{X}) - \min_{W\in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s\in\mathcal{S}})} I(P_{\tilde{U}},W) + \delta.
\end{aligned}$$

Proof. We again use Ahlswede robustification to prove this result. Given $\delta,\delta_1 > 0$ there is a $c > 0$ such that for all n large enough we can find $F \in \mathcal{P}(\mathcal{K}\times\bar{\mathcal{M}}|\mathcal{X}^n)$ and $g\colon \mathcal{Y}^n\times\bar{\mathcal{M}}\to\mathcal{K}$ such that for RVs K', $\bar{M}'$ and $\{\hat{K}'_v\}_{v\in\mathcal{V}}$ with

$$P_{K'\bar{M}'\hat{K}'_v\tilde{X}^n}(k,\bar{m},\hat{k},x^n) = \sum_{y^n\in\mathcal{Y}^n} P_{\tilde{X}Y_v}^{\otimes n}(x^n,y^n)F(k,\bar{m}|x^n)\mathbb{1}_{g^{-1}(\hat{k})}((y^n,\bar{m}))$$

for all $(k,\bar{m},\hat{k},x^n) \in \mathcal{K}\times\bar{\mathcal{M}}\times\mathcal{K}\times\mathcal{X}^n$ it holds that

$$\sup_{v\in\mathcal{V}} \Pr(K' \neq \hat{K}'_v|\bar{M}'=\bar{m},\tilde{X}^n\in\mathcal{T}^n_{\tilde{X},\delta_1}) \leqslant \exp(-nc) \tag{4.51}$$

$$H(K'|M') = \log|\mathcal{K}| \tag{4.52}$$

$$\tfrac{1}{n}\log|\mathcal{K}| \geqslant \inf_{v\in\mathcal{V}} I(\tilde{U}\wedge Y_v) - \delta \tag{4.53}$$

$$\tfrac{1}{n}\log|\mathcal{M}| \leqslant I(\tilde{U}\wedge\tilde{X}) - \inf_{v\in\mathcal{V}} I(\tilde{U}\wedge Y_v) + \delta \tag{4.54}$$

where the RVs $\{Y_v\}_{v\in\mathcal{V}}$ are such that $\{P_{Y_v|\tilde{X}}\}_{v\in\mathcal{V}} = conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s\in\mathcal{S}})$ and $\tilde{U} - \tilde{X} - Y_v$ for all $v \in \mathcal{V}$. This follows from the achievability proof of Lemma 4.5, (cf. (4.22) for (4.51)).

Define $h_{\bar{m}}\colon \mathcal{S}^n \to [0,1]$ for all $\bar{m} \in \bar{\mathcal{M}}$ such that for all $s^n \in \mathcal{S}^n$

$$h_{\bar{m}}(s^n) = \frac{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F(k,\bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n,m))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k,\bar{m}|x^n)}.$$

It holds for all $P_{\bar{m}} \in \mathcal{P}(n,\mathcal{S})$, $\bar{m} \in \bar{\mathcal{M}}$, that

$$\begin{aligned}
&\sum_{s^n \in \mathcal{S}^n} h_{\bar{m}}(s^n) P_{\bar{m}}^{\otimes n}(s^n) \\
&\quad = \sum_{s^n \in \mathcal{S}^n} P_{\bar{m}}^{\otimes n}(s^n) \frac{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F(k,\bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n,\bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k,\bar{m}|x^n)}
\end{aligned}$$

which equals

$$\frac{\sum_{x^n,y^n} \sum_k \sum_{s^n} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) P_{\bar{m}}(s_i) F(k,\bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n,\bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k,\bar{m}|x^n)}$$

This expression equals

$$\begin{aligned}
&\frac{\sum_{x^n,y^n} \sum_k \prod_{i=1}^n \sum_{s \in \mathcal{S}} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) P_{\bar{m}}(s) F(k,\bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n,\bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k,\bar{m}|x^n)} \\
&\quad = \frac{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) W_{\bar{m}}^{\otimes n}(y^n|x^n) F(k,\bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n,m))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k,\bar{m}|x^n)}
\end{aligned}$$

with $W_{\bar{m}} \in conv(\{P_{\tilde{Y}_s|\tilde{X}}\}_{s \in \mathcal{S}})$ defined appropriately. This expression equals

$$\begin{aligned}
\Pr(K' = \hat{K}'_v | \bar{M}' = \bar{m}) \geqslant \Pr(K' = \hat{K}'_v | \bar{M}' = \bar{m}, \tilde{X}^n \in \mathcal{T}^n_{\tilde{X},\delta_1}) \\
\cdot \Pr(\tilde{X}^n \in \mathcal{T}^n_{\tilde{X},\delta_1} | \bar{M}' = \bar{m})
\end{aligned}$$

for the $v \in \mathcal{V}$ corresponding to $P_{\bar{m}}$. So from our choice of F and g we know that

$$\begin{aligned}
\sum_{s^n \in \mathcal{S}^n} h_{\bar{m}}(s^n) P_{\bar{m}}^{\otimes n}(s^n) &> (1 - \exp(-nc)) \Pr(\tilde{X}^n \in \mathcal{T}^n_{\tilde{X},\delta_1} | \bar{M}' = \bar{m}) \\
&\geqslant 1 - (\exp(-nc) + \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1} | \bar{M}' = \bar{m})).
\end{aligned}$$

Now we use the Ahlswede robustification as seen before, so according to [3, Theorem RT] this implies for all $s^n \in \mathcal{S}^n$

$$\frac{1}{n!} \sum_{\pi \in \Pi_n} h_{\bar{m}}(\pi s^n) > 1 - (\exp(-nc) + \Pr(\tilde{X}^n \notin \mathcal{T}^n_{\tilde{X},\delta_1} | \bar{M}' = \bar{m}))(n+1)^{|\mathcal{S}|}$$

where Π_n is the set of all permutations on $[n]$ and again we write for $\pi \in \Pi_n$ πx^n for $x_{\pi^{-1}(1)}, \cdots, x_{\pi^{-1}(n)}$, i.e. π induces a bijection on $\mathcal{X}^n$. We define for all $\pi \in \Pi_n$ and all

$(k, \bar{m}, x^n) \in \mathcal{K} \times \bar{\mathcal{M}} \times \mathcal{X}^n$

$$F^\pi(k, \bar{m}|x^n) = F(k, \bar{m}|\pi x^n)$$
$$g^\pi(y^n, \bar{m}) = g(\pi y^n, \bar{m}).$$

We can write for all $s^n \in \mathcal{S}^n$ and $\pi \in \Pi_n$

$$h_{\bar{m}}(\pi s^n) = \frac{\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{k \in \mathcal{K}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_{\pi^{-1}(i)}}}(x_i, y_i) F(k, \bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, \bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)}$$
$$= \frac{\sum_{x^n, y^n} \sum_k \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_{\pi(i)}, y_{\pi(i)}) F(k, \bar{m}|x^n) \mathbb{1}_{g^{-1}(k)}((y^n, \bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)}.$$

As π is a bijection on $\mathcal{X}^n$ and $\mathcal{Y}^n$ respectively and we sum over all elements of these sets this equals

$$\frac{\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{k \in \mathcal{K}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F(k, \bar{m}|\pi x^n) \mathbb{1}_{g^{-1}(k)}((\pi y^n, \bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)}$$

which equals

$$\frac{\sum_{\substack{x^n \in \mathcal{X}^n \\ y^n \in \mathcal{Y}^n}} \sum_{k \in \mathcal{K}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F^\pi(k, \bar{m}|x^n) \mathbb{1}_{(g^\pi)^{-1}(k)}((y^n, \bar{m}))}{\sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)}.$$

So we get

$$\frac{1}{n!} \sum_{\pi \in \Pi_n} \sum_{\bar{m} \in \bar{\mathcal{M}}} P_{\bar{M}'}(\bar{m}) h_{\bar{m}}(\pi s_{\bar{m}}^n) > 1 - (\exp(-nc) + \Pr(\tilde{X}^n \notin \mathcal{T}_{\tilde{X}, \delta_1}^n))(n+1)^{|\mathcal{S}|} \tag{4.55}$$

for all $(s_1^n, \cdots, s_{|\bar{\mathcal{M}}|}^n) \in (\mathcal{S}^n)^{|\bar{\mathcal{M}}|}$. Note that $\Pr(\tilde{X}^n \notin \mathcal{T}_{\tilde{X}, \delta_1}^n)$ decreases exponentially with n. We now define for all $(k, \bar{m}) \in \mathcal{K} \times \bar{\mathcal{M}}$, $\{\pi_\gamma\}_{\gamma \in [n!]} = \Pi_n$, and $x^n \in \mathcal{X}^n$

$$F_{CR}(k, \bar{m}|x^n, \gamma) = F^{\pi_\gamma}(k, \bar{m}|x^n)$$
$$g_{CR}(y^n, \bar{m}, \gamma) = g^{\pi_\gamma}(y^n, \bar{m}).$$

We thus have

$$\sum_{\bar{m} \in \bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \Pr(K \neq \hat{K}_{s_{\bar{m}}^n} | \bar{M} = \bar{m})$$
$$= \frac{1}{n!} \sum_{\pi \in \Pi_n} \sum_{\bar{m} \in \bar{\mathcal{M}}} h_{\bar{m}}(\pi s_{\bar{m}}^n) \sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F^\pi(k, \bar{m}|x^n)$$
$$= \frac{1}{n!} \sum_{\pi \in \Pi_n} \sum_{\bar{m} \in \bar{\mathcal{M}}} h_{\bar{m}}(\pi s_{\bar{m}}^n) \sum_{x^n \in \mathcal{X}^n} \sum_{k \in \mathcal{K}} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)$$
$$= \frac{1}{n!} \sum_{\pi \in \Pi_n} \sum_{\bar{m} \in \bar{\mathcal{M}}} P_{\bar{M}'}(\bar{m}) h_{\bar{m}}(\pi s_{\bar{m}}^n),$$

and with (4.55) this expression is arbitrarily small for all n large enough for all $(s_1^n, \cdots, s_{|\bar{\mathcal{M}}|}^n) \in (\mathcal{S}^n)^{|\bar{\mathcal{M}}|}$. Now consider for $(k, \bar{m}, \gamma) \in \mathcal{K} \times \bar{\mathcal{M}} \times [n!]$

$$\begin{aligned} P_{K\bar{M}\Gamma}(k, \bar{m}, \gamma) &= \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F^{\pi_\gamma}(k, \bar{m}|x^n) P_\Gamma(\gamma) \\ &= \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n) P_\Gamma(\gamma) \end{aligned}$$

which follows as π_γ is a bijection on $\mathcal{X}^n$, $P_{\tilde{X}}^{\otimes n}(x^n) = P_{\tilde{X}}^{\otimes n}(\pi_\gamma x^n)$ and we sum over all $x^n \in \mathcal{X}^n$. So we get

$$\begin{aligned} P_{K|\bar{M}\Gamma}(k|\bar{m}, \gamma) &= \frac{\sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n) P_\Gamma(\gamma)}{\sum_{k \in \mathcal{K}} \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n) P_\Gamma(\gamma)} \\ &= \frac{\sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)}{\sum_{k \in \mathcal{K}} \sum_{x^n \in \mathcal{X}^n} P_{\tilde{X}}^{\otimes n}(x^n) F(k, \bar{m}|x^n)} = \frac{1}{|\mathcal{K}|} \end{aligned}$$

where we use the corresponding property (4.52) of F for the last step.

Consider $v \in \mathcal{V}$. There is a $P \in \mathcal{P}(\mathcal{S})$ such that for all $(u, y) \in \mathcal{U} \times \mathcal{Y}$

$$\begin{aligned} P_{Y_v|\tilde{U}}(y|u) &= \sum_{x \in \mathcal{X}} P_{Y_v|\tilde{X}}(y|x) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{x \in \mathcal{X}} \Big(\sum_{s \in \mathcal{S}} P(s) P_{\tilde{Y}_s|\tilde{X}}(y|x) \Big) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{s \in \mathcal{S}} P(s) \sum_{x \in \mathcal{X}} P_{\tilde{Y}_s|\tilde{X}}(y|x) P_{\tilde{X}|\tilde{U}}(x|u) \\ &= \sum_{s \in \mathcal{S}} P(s) P_{\tilde{Y}_s|\tilde{U}}(y|u) \end{aligned}$$

where we use $\tilde{U} - \tilde{X} - Y_v$ for all $v \in \mathcal{V}$ and $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$. So $\{P_{Y_v|\tilde{U}}\}_{v \in \mathcal{V}} \subset conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})$. Thus it follows that

$$\inf_{v \in \mathcal{V}} I(\tilde{U} \wedge Y_v) = \inf_{v \in \mathcal{V}} I(P_{\tilde{U}}, P_{Y_v|\tilde{U}}) \geqslant \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W).$$

Accordingly we have with (4.53) and (4.54)

$$\tfrac{1}{n} \log |\mathcal{K}| \geqslant \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) - \delta.$$

and

$$\tfrac{1}{n} \log |\bar{\mathcal{M}}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \inf_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) + \delta.$$

■

Now we can prove Lemma 4.15.

Lemma 4.15. *Consider the RVs $\tilde{X}$ and $\{\tilde{Y}_s\}_{s \in \mathcal{S}}$, $|\mathcal{S}| < \infty$ with $P_{\tilde{X}\tilde{Y}_s} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ for all*

$s \in \mathcal{S}$, the RV $\tilde{U}$ such that $\tilde{U} - \tilde{X} - \tilde{Y}_s$ for all $s \in \mathcal{S}$, $P_{\tilde{U}} \in \mathcal{P}(\mathcal{U})$ and the RV Γ, $P_\Gamma \in \mathcal{P}(\mathcal{G})$ with $P_\Gamma(\gamma) = \frac{1}{|\mathcal{G}|}$ for all $\gamma \in \mathcal{G}$. Let $\delta > 0$. For all n large enough there is a stochastic matrix $F_{CR} \in \mathcal{P}(\mathcal{K} \times \bar{\mathcal{M}}|\mathcal{X}^n \times \mathcal{G})$ and a mapping $g_{CR} \colon \mathcal{Y}^n \times \bar{\mathcal{M}} \times \mathcal{G} \to \mathcal{K}$ such that for RVs K, $\bar{M}$ and $\{\hat{K}_{s^n}\}_{s^n \in \mathcal{S}^n}$ with $P_{K\bar{M}\hat{K}_{s^n}} \in \mathcal{P}(\mathcal{K} \times \bar{\mathcal{M}} \times \mathcal{K})$ for all $s^n \in \mathcal{S}^n$ defined by

$$P_{K\bar{M}\hat{K}_{s^n}\Gamma}(k, \bar{m}, \hat{k}, \gamma) = \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F_{CR}(k, \bar{m}|x^n, \gamma) \cdot \mathbb{1}_{g_{CR}^{-1}(\hat{k})}((y^n, \bar{m}, \gamma)) P_\Gamma(\gamma)$$

for $(k, \bar{m}, \hat{k}, \gamma) \in \mathcal{K} \times \bar{\mathcal{M}} \times \mathcal{K} \times \mathcal{G}$ it holds that

$$\begin{aligned}
&\sum_{\bar{m} \in \bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n \in \mathcal{S}^n} Pr(K \neq \hat{K}_{s^n} | \bar{M} = \bar{m}) \leqslant \delta \\
&H(K|\bar{M}\Gamma) = \log |\mathcal{K}| \\
&\tfrac{1}{n} \log |\mathcal{K}| \geqslant \min_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) - \delta \\
&\tfrac{1}{n} \log |\bar{\mathcal{M}}| \leqslant I(\tilde{U} \wedge \tilde{X}) - \min_{W \in conv(\{P_{\tilde{Y}_s|\tilde{U}}\}_{s \in \mathcal{S}})} I(P_{\tilde{U}}, W) + \delta \\
&\tfrac{1}{n} \log |\mathcal{G}| \leqslant \delta.
\end{aligned}$$

Proof. Let $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3)$ where Γ_1, Γ_2, Γ_3 are independent RVs uniformly distributed on $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_3$ respectively. Let $\mathcal{G}_1 = [\exp(\lceil c_1 \log n \rceil - l)]$ where $c_1 > 1$ and $l \in \mathbb{N}$ (independent of n).

Given a DMC $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ in [6] an identification (ID) code $(n', N, \lambda_1, \lambda_2)$ is defined as a family $\{(Q(\cdot|i), \mathcal{D}_i)\}_{i \in [N]}$ with $Q(\cdot|i) \in \mathcal{P}(\mathcal{X}^{n'})$, $\mathcal{D}_i \subset \mathcal{Y}^{n'}$ for all $i \in [N]$. The ID code also satisfies bounds on the probabilities of an error of the first kind and an error of the second kind respectively such that

$$\begin{aligned}
\sum_{x^n \in \mathcal{X}^n} Q(x^{n'}|i) V^{\otimes n'}(\mathcal{D}_i^c | x^{n'}) &\leqslant \lambda_1 \\
\sum_{x^n \in \mathcal{X}^n} Q(x^{n'}|j) V^{\otimes n'}(\mathcal{D}_i | x^{n'}) &\leqslant \lambda_2
\end{aligned}$$

for all $i, j \in [N]$, $i \neq j$.

We are interested in ID codes for the noiseless binary channel. In the proof of [6, Theorem 1 a)] the authors construct an ID code for the binary noiseless channel. They consider a family $\mathcal{A}_1, \cdots, \mathcal{A}_N$ of subsets of $\{0,1\}^{n'}$ with

$$N = \exp(-n') \exp(\exp(n' - l)) - 1.$$

Each subset has cardinality $\exp(n' - l)$. l is chosen large enough such that

$$\lambda \log(\exp(l) - 1) > 2 \qquad \exp(l) > 6$$

for a $\lambda \in (0, 1)$. Additionally it holds that

$$|\mathcal{A}_i \cap \mathcal{A}_j| \leqslant \lambda \exp(n' - l)$$

for $i \neq j$. Such a family exists according to [6, Proposition 1]. The $(n', N, 0, \lambda)$ ID code for the noiseless binary channel is defined such that

$$Q(x^{n'}|i) = \tfrac{1}{\exp(n'-l)} \mathbb{1}_{\mathcal{A}_i}(x^{n'})$$

for all $x^{n'} \in \mathcal{X}^{n'}$ and $\mathcal{D}_i = \mathcal{A}_i$ for $i \in [N]$.

Accordingly we know that there is a $(\lceil c_1 \log n \rceil, |\mathcal{K}|, 0, \lambda)$ ID code for the noiseless binary channel with

$$|\mathcal{K}| = \exp(-\lceil c_1 \log n \rceil) \exp(\exp(\lceil c_1 \log n \rceil - l)) - 1.$$

So there is a mapping $T \colon \mathcal{K} \times \mathcal{G}_1 \to [\exp(\lceil c_1 \log n \rceil)]$ such that

$$\tfrac{1}{|\mathcal{G}_1|} \sum_{\gamma_1 \in \mathcal{G}_1} \mathbb{1}_{\{T(k,\gamma_1)\}}(T(\bar{k}, \gamma_1)) \leqslant \lambda$$

for all $k, \bar{k} \in \mathcal{K}$ with $k \neq \bar{k}$. More explicitly we can define

$$T(k, \gamma_1) = d(c_{\mathcal{A}_k}^{-1}(\gamma_1))$$

for all $k \in \mathcal{K}$ (and for convenience we assume w.l.o.g. that $\mathcal{K} = [|\mathcal{K}|]$) where $c_{\mathcal{A}_k} \colon \mathcal{A}_k \to \mathcal{G}_1$ is an arbitrary bijection for all $\mathcal{A}_k$ and $d \colon \{0,1\}^{\lceil c_1 \log n \rceil} \to [\exp(\lceil c_1 \log n \rceil)]$ is a bijection too. For n large enough we have

$$\tfrac{1}{n} \log |\mathcal{K}| \geqslant n^{c_1 - 1} 2^{-l} - \tfrac{\lceil c_1 \log n \rceil}{n} \geqslant \alpha$$

for an arbitrary choice of $\alpha > 0$. (We could also use different constructions for identification protocols in this step.)

Consider $(F_!, g_!)$ as described in Lemma 4.14 with block length $n_1 = \lceil c_2 \log n \rceil$, $c_2 > 0$, for all n large enough and we choose the corresponding $\tilde{U}_! = \tilde{X}$. For the corresponding set $\mathcal{K}_!$ we have

$$|\mathcal{K}_!| \geqslant \exp(\lceil c_2 \log n \rceil \epsilon)$$

for an $\epsilon > 0$. (If such a lower bound does not hold the theorem we want to prove is trivially true.) So for an appropriate choice of c_2 we have

$$\exp(\lceil (c_1 + \epsilon) \log n \rceil) \geqslant |\mathcal{K}_!| \geqslant \exp(\lceil c_1 \log n \rceil).$$

We also have for an appropriate choice of $c_3 > 0$

$$\bar{\mathcal{M}}_! \leqslant \exp(\lceil c_2 \log n \rceil c_3)$$

and $n_1! \leqslant (\lceil c_2 \log n \rceil)^{\lceil c_2 \log n \rceil}$. So for an appropriate choice of $c_4 > 0$ we have

$$\tfrac{1}{n} \log(n_1!) \leqslant \tfrac{c_4 (\log(n))^2}{n}.$$

We choose $\mathcal{G}_2 = [n_1!]$ and $\mathcal{G}_3 = \mathcal{K}_!$.

Finally choose (F_L, g_L) as described in Lemma 4.13 with block length $n - n_1$ and choose the corresponding $\tilde{U}_L = \tilde{U}$. We can assume that the symmetrizability of $\{P_{\tilde{Y}_s|\tilde{X}}\}_{s \in \mathcal{S}}$ is $\hat{M} < \infty$. Otherwise the lemma we want to prove holds trivially [31, Theorem 1]. So we have the corresponding list size $\hat{L} < \infty$.

Choose $\mathcal{K} = \mathcal{K}_L$. Define (for an arbitrary injective mapping $b\colon [\exp(\lceil c_1 \log n \rceil)] \to \mathcal{K}_!$) for all $(k, \tilde{k}, \bar{m}_L, \bar{m}_!) \in \mathcal{K} \times \mathcal{K}_! \times \bar{\mathcal{M}}_L \times \bar{\mathcal{M}}_!$, $(\gamma_1, \gamma_2, \gamma_3) \in \mathcal{G}_1 \times \mathcal{G}_2 \times \mathcal{G}_3$ and $(x^{n_1}, x^{n-n_1}) \in \mathcal{X}^n$

$$\begin{aligned} &F_{CR}(k, (\tilde{k}, \bar{m}_L, \bar{m}_!)|(x^{n_1}, x^{n-n_1}), (\gamma_1, \gamma_2, \gamma_3)) \\ &= F_!((b(T(k, \gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1}, \gamma_2) F_L(k, \bar{m}_L|x^{n-n_1}), \end{aligned}$$

where $*$ is a commutative group operation on $\mathcal{K}_!$ and for $k_! \in \mathcal{K}_!$ we denote the corresponding inverse element by $k_!^{-1}$. (This definition makes sense as $f\colon \mathcal{K}_! \to \mathcal{K}_!$, $f(\tilde{k}) = (b(T(k, \gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}$ is a bijection for all $k \in \mathcal{K}$, $\gamma_1 \in \mathcal{G}_1$ and $\gamma_3 \in \mathcal{G}_3$.) So we have $\bar{\mathcal{M}} = \mathcal{K}_! \times \bar{\mathcal{M}}_L \times \bar{\mathcal{M}}_!$.

We also define for all $(k, \tilde{k}, \bar{m}_L, \bar{m}_!) \in \mathcal{K} \times \mathcal{K}_! \times \bar{\mathcal{M}}_L \times \bar{\mathcal{M}}_!$, $(\gamma_1, \gamma_2, \gamma_3) \in \mathcal{G}_1 \times \mathcal{G}_2 \times \mathcal{G}_3$ and $(y^{n_1}, y^{n-n_1}) \in \mathcal{Y}^n$

$$\begin{aligned} &g_{CR}((y^{n_1}, y^{n-n_1}), (\tilde{k}, \bar{m}_L, \bar{m}_!), (\gamma_1, \gamma_2, \gamma_3)) \in \\ &\{q \in g_L(y^{n-n_1}, \bar{m}_L)\colon b^{-1}(\tilde{k} * \gamma_3^{-1} * (g_!(y^{n_1}, \bar{m}_!, \gamma_2))^{-1}) = T(q, \gamma_1)\} \end{aligned}$$

if the set on the right hand side has cardinality 1. So for this case the decoder is specified. If this cardinality is not 1, an arbitrary element from $\mathcal{K}$ is chosen. Here we define $b^{-1}(k_!) = 1$ for all $k_! \notin b([\exp(\lceil c_1 \log n \rceil)])$.

It holds that

$$P_{K|\bar{M}\Gamma}(k|\bar{m}_L, \bar{m}_!, \tilde{k}, \gamma_1, \gamma_2, \gamma_3) = \frac{\sum_{x^n} F_{CR}(k, (\tilde{k}, \bar{m}_L, \bar{m}_!)|x^n, (\gamma_1, \gamma_2, \gamma_3)) P_{\tilde{X}}^{\otimes n}(x^n)}{\sum_{x^n} \sum_k F_{CR}(k, (\tilde{k}, \bar{m}_L, \bar{m}_!)|x^n, (\gamma_1, \gamma_2, \gamma_3)) P_{\tilde{X}}^{\otimes n}(x^n)}.$$

In the following we use the notation $x^n = (x^{n_1}, x^{n-n_1})$. The numerator of the fraction above equals

$$\begin{aligned} &\sum_{x^{n_1}} F_!((b(T(k, \gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1}, \gamma_2) P_{\tilde{X}}^{\otimes n_1}(x^{n_1}) \\ &\sum_{x^{n-n_1}} F_L(k, \bar{m}_L|x^{n-n_1}) P_{\tilde{X}}^{\otimes n-n_1}(x^{n-n_1}), \end{aligned}$$

for the denominator we have

$$\sum_k \sum_{x^{n_1}} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1}, \gamma_2)$$
$$P_{\tilde{X}}^{\otimes n_1}(x^{n_1}) \sum_{x^{n-n_1}} F_L(k, \bar{m}_L|x^{n-n_1}) P_{\tilde{X}}^{\otimes n-n_1}(x^{n-n_1}).$$

Now we use the properties of $(F_!, g_!)$ and get

$$\sum_{x^{n_1}} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1}, \gamma_2) P_{\tilde{X}}^{\otimes n_1}(x^{n_1})$$
$$= \tfrac{1}{|\mathcal{K}_!|} \sum_{k_! \in \mathcal{K}_!} \sum_{x^{n_1}} F_!(k_!, \bar{m}_!|x^{n_1}, \gamma_2) P_{\tilde{X}}^{\otimes n_1}(x^{n_1})$$

which is independent of k. So the complete fraction equals

$$\frac{\sum_{x^{n-n_1}} F_L(k,\bar{m}_L|x^{n-n_1}) P_{\tilde{X}}^{\otimes n-n_1}(x^{n-n_1})}{\sum_{x^{n-n_1}} \sum_k F_L(k,\bar{m}_L|x^{n-n_1}) P_{\tilde{X}}^{\otimes n-n_1}(x^{n-n_1})} = \tfrac{1}{|\mathcal{K}|}$$

where the last step follows from the properties of (F_L, g_L).

Now we consider

$$\sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} \Pr(K \neq \hat{K}_{s^n}|\bar{M} = \bar{m})$$
$$= \sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} \sum_{k\in\mathcal{K}} \Pr(k \neq \hat{K}_{s^n}|\bar{M} = \bar{m}, K = k)$$
$$\cdot \sum_{\gamma\in\mathcal{G}} P_{K|\bar{M}\Gamma}(k|\bar{m},\gamma) P_{\Gamma|\bar{M}}(\gamma|\bar{m})$$
$$= \sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} \Pr(k \neq \hat{K}_{s^n}|\bar{M} = \bar{m}, K = k)$$

The term $\Pr(k \neq \hat{K}_{s^n}|\bar{M} = \bar{m}, K = k)$ for $(k, \bar{m}) \in \mathcal{K} \times \bar{\mathcal{M}}$ and $s^n \in \mathcal{S}^n$ can be written as the fraction with numerator

$$\sum_{\substack{\hat{k}\in\mathcal{K}:\\ \hat{k}\neq k}} \sum_{\substack{x^n,y^n\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^n P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F_L(k, \bar{m}_L|x^{n-n_1})$$
$$\cdot \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1}, \gamma_2) \mathbb{1}_{g_{CR}^{-1}(\hat{k})}(y^n, (\tilde{k}, \bar{m}_L, \bar{m}_!), (\gamma_1, \gamma_2, \gamma_3)) \quad (4.56)$$

and denominator

$$\sum_{\substack{x^n,y^n\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1}) \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2). \tag{4.57}$$

For all $k \in \mathcal{K}$ and $(y^n, (\tilde{k}, \bar{m}_L, \bar{m}_!), (\gamma_1,\gamma_2,\gamma_3)) \in \mathcal{Y}^n \times \bar{\mathcal{M}} \times \mathcal{G}$ it holds that

$$\begin{aligned}
&\sum_{\substack{\hat{k}\in\mathcal{K}:\\ \hat{k}\neq k}} \mathbb{1}_{g_{CR}^{-1}(\hat{k})}(y^n,(\tilde{k},\bar{m}_L,\bar{m}_!),(\gamma_1,\gamma_2,\gamma_3))\\
&\leqslant \mathbb{1}_{(g_!^{-1}((b(T(k,\gamma_1)))^{-1}*\tilde{k}*\gamma_3^{-1}))^c}(y^{n_1},\bar{m}_!,\gamma_2)\\
&+ \mathbb{1}_{(g_L^{-1}(k))^c}(y^{n-n_1},\bar{m}_L)\\
&+ \mathbb{1}_{\substack{\{(y^{n-n_1},\bar{m}_L,k,\gamma_1):\\ \exists q\in g_L(y^{n-n_1},\bar{m}_L):\\ q\neq k\wedge T(q,\gamma_1)=T(k,\gamma_1)\}}}(y^{n-n_1},\bar{m}_L,k,\gamma_1),
\end{aligned}$$

where we use $y^n = (y^{n_1}, y^{n-n_1})$.

Thus we can upper bound the fraction with numerator (4.56) and denominator (4.57) by the sum of the three fractions with the same denominator and the numerators

$$\begin{aligned}
&\sum_{\substack{x^n,y^n\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1})\\
&\cdot \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2)\\
&\cdot \mathbb{1}_{(g_!^{-1}((b(T(k,\gamma_1)))^{-1}*\tilde{k}*\gamma_3^{-1}))^c}(y^{n_1},\bar{m}_!,\gamma_2),
\end{aligned} \tag{4.58}$$

$$\begin{aligned}
&\sum_{\substack{x^n,y^n\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1})\\
&\cdot \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2)\\
&\cdot \mathbb{1}_{(g_L^{-1}(k))^c}(y^{n-n_1},\bar{m}_L)
\end{aligned} \tag{4.59}$$

and

$$\sum_{\substack{x^n,y^n\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1}) \cdot \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2) \cdot \mathbb{1}_{\substack{\{(y^{n-n_1},\bar{m}_L,k,\gamma_1):\\ \exists q\in g_L(y^{n-n_1},\bar{m}_L):\\ q\neq k \wedge T(q,\gamma_1)=T(k,\gamma_1)\}}} (y^{n-n_1},\bar{m}_L,k,\gamma_1). \tag{4.60}$$

At first consider the fraction with numerator (4.58). This numerator can be rewritten as

$$\sum_{\substack{x^{n_1},y^{n_1}\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n_1} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2) \cdot \mathbb{1}_{(g_!^{-1}((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}))^c}(y^{n_1},\bar{m}_!,\gamma_2) \cdot \sum_{x^{n-n_1},y^{n-n_1}} \prod_{i=n_1+1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1})$$

while the denominator can be rewritten as

$$\sum_{\substack{x^{n_1},y^{n_1}\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n_1} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2) \cdot \sum_{x^{n-n_1},y^{n-n_1}} \prod_{i=n_1+1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1}).$$

We can again rewrite this fraction and get

$$\frac{\sum_{\substack{x^{n_1},y^{n_1}\\ \gamma_2,\gamma_3}} \prod_{i=1}^{n_1} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_!(\gamma_3,\bar{m}_!|x^{n_1},\gamma_2) \mathbb{1}_{(g_!^{-1}(\gamma_3))^c}(y^{n_1},\bar{m}_!,\gamma_2)}{\sum_{x^{n_1},y^{n_1},\gamma_2} \sum_{\gamma_3} \prod_{i=1}^{n_1} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_!(\gamma_3,\bar{m}_!|x^{n_1},\gamma_2)}.$$

This is possible because $f\colon \mathcal{G}_3 \to \mathcal{G}_3$, $f(\gamma_3) = (b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}$ is a bijection. (Note that this expression does not depend on $\tilde{k}$, k and $\bar{m}_L$.) Now we consider the fraction with numerator (4.59). This numerator can be rewritten as

$$\sum_{\substack{x^{n_1},y^{n_1}\\ \gamma_1,\gamma_2,\gamma_3}} \prod_{i=1}^{n_1} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) \tfrac{1}{|\mathcal{G}|} F_!((b(T(k,\gamma_1)))^{-1} * \tilde{k} * \gamma_3^{-1}, \bar{m}_!|x^{n_1},\gamma_2) \cdot \sum_{x^{n-n_1},y^{n-n_1}} \prod_{i=n_1+1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i,y_i) F_L(k,\bar{m}_L|x^{n-n_1}) \mathbb{1}_{(g_L^{-1}(k))^c}(y^{n-n_1},\bar{m}_L)$$

while the denominator can be rewritten as before. We can again rewrite this fraction and get the fraction with numerator

$$\sum_{\substack{x^{n-n_1}\\ y^{n-n_1}}} \prod_{i=n_1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F_L(k, \bar{m}_L | x^{n-n_1}) \cdot \mathbb{1}_{(g_L^{-1}(k))^c}(y^{n-n_1}, \bar{m}_L)$$

and denominator

$$\sum_{\substack{x^{n-n_1}\\ y^{n-n_1}}} \prod_{i=n_1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F_L(k, \bar{m}_L | x^{n-n_1}). \tag{4.61}$$

(This expression does not depend on $\bar{m}_!$ and $\tilde{k}$.) Now we consider the the fraction with numerator (4.60). Using the same steps as for the second fraction this fraction can be rewritten as the fraction with numerator

$$\sum_{\substack{x^{n-n_1}\\ y^{n-n_1}}} \prod_{i=n_1}^{n} P_{\tilde{X}\tilde{Y}_{s_i}}(x_i, y_i) F_L(k, \bar{m}_L | x^{n-n_1}) \cdot \frac{1}{|\mathcal{G}_1|} \sum_{\gamma_1} \mathbb{1}_{\substack{\{(y^{n-n_1}, \bar{m}_L, k, \gamma_1):\\ \exists q \in g_L(y^{n-n_1}, \bar{m}_L):\\ q \neq k \wedge T(q,\gamma_1) = T(k,\gamma_1)\}}} (y^{n-n_1}, \bar{m}_L, k, \gamma_1)$$

and denominator (4.61). We have

$$\begin{aligned}
&\frac{1}{|\mathcal{G}_1|} \sum_{\gamma_1} \mathbb{1}_{\substack{\{(y^{n-n_1}, \bar{m}_L, k, \gamma_1):\\ \exists q \in g_L(y^{n-n_1}, \bar{m}_L):\\ q \neq k \wedge T(q,\gamma_1) = T(k,\gamma_1)\}}} (y^{n-n_1}, \bar{m}_L, k, \gamma_1) \\
&\leqslant \frac{1}{|\mathcal{G}_1|} \sum_{\gamma_1} \sum_{\substack{q \in g_L(y^{n-n_1}, \bar{m}_L):\\ q \neq k}} \mathbb{1}_{\{T(k,\gamma_1)\}}(T(q, \gamma_1)) \\
&= \sum_{\substack{q \in g_L(y^{n-n_1}, \bar{m}_L):\\ q \neq k}} \frac{1}{|\mathcal{G}_1|} \sum_{\gamma_1} \mathbb{1}_{\{T(k,\gamma_1)\}}(T(q, \gamma_1)) \\
&\leqslant (\hat{L} - 1)\lambda.
\end{aligned}$$

So the third fraction can be upper bounded by $(\hat{L} - 1)\lambda$. Now we write $F_1(\bar{m}_!, s^{n_1})$ for the first fraction and $F_2(k, \bar{m}_L, s^{n-n_1})$ for the second fraction (and we use the notation

$s^n = (s^{n_1}, s^{n-n_1})$). Consequently we have

$$\begin{aligned}
&\sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} \Pr(K \neq \hat{K}_{s^n} | \bar{M} = \bar{m}) \\
&\leqslant \sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^{n_1}\in\mathcal{S}^{n_1}} \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} F_1(\bar{m}_!, s^{n_1}) \\
&+ \sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^{n-n_1}\in\mathcal{S}^{n-n_1}} \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} F_2(k, \bar{m}_L, s^{n-n_1}) \\
&+ \sum_{\bar{m}\in\bar{\mathcal{M}}} P_{\bar{M}}(\bar{m}) \max_{s^n\in\mathcal{S}^n} \tfrac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} (\hat{L} - 1)\lambda.
\end{aligned}$$

The first and second summand are arbitrarily small for n large enough, which follows from our choice of $(F_!, g_!)$ and (F_L, g_L) respectively. Thus the error probability of the whole protocol is arbitrarily small for n large enough.

Finally consider

$$\tfrac{1}{n}\log|\mathcal{K}| = (1 - \tfrac{\lceil c_2 \log n\rceil}{n})(\tfrac{1}{n-n_1}\log|\mathcal{K}_L|)$$

and

$$\begin{aligned}
&\tfrac{1}{n}\log|\bar{\mathcal{M}}| = \tfrac{1}{n}(\log|\bar{\mathcal{M}}_!| + \log|\bar{\mathcal{M}}_L| + \log|\bar{\mathcal{K}}_!|) \\
&\leqslant \tfrac{1}{n-n_1}\log|\bar{\mathcal{M}}_L| + \tfrac{1}{n}(\lceil c_2 \log n\rceil c_3 + \lceil (c_1+\epsilon)\log n\rceil)
\end{aligned}$$

and thus the desired results for $\frac{1}{n}\log|\mathcal{K}|$ and $\frac{1}{n}\log|\bar{\mathcal{M}}|$ follow from the properties of (F_L, g_L). We also have

$$\begin{aligned}
&\tfrac{1}{n}\log|\mathcal{G}| = \tfrac{1}{n}(\log|\mathcal{G}_1| + \log|\mathcal{G}_2| + \log|\mathcal{G}_3|) \\
&\leqslant \tfrac{1}{n}(\lceil c_1 \log n\rceil - l + c_4(\log(n))^2 + \lceil (c_1+\epsilon)\log n\rceil).
\end{aligned}$$

■

Publication List

- S. Baur, N. Cai, M. Wiese, H. Boche: "Secret Key Generation from a Two Component Source with Rate Constrained One Way Communication: Perfect Secrecy". submitted

- S. Baur, H. Boche, N. Cai: "Secret Key Generation from a PUF Source under Jamming Attacks". submitted

- S. Baur, N. Cai, M. Wiese, H. Boche: "Secret Key Generation from a Two Component Compound Source with Rate Constrained One Way Communication: Perfect Secrecy". IEEE International Workshop on Information Forensics and Security (WIFS) 2019, accepted for publication

- H. Boche, R.F. Schaefer, S. Baur, H.V. Poor: "On the Algorithmic Computability of the Secret Key and Authentication Capacity under Channel, Storage, and Privacy Leakage Constraints". IEEE Transactions on Signal Processing 67 (17), 2019, 4636-4648

- S. Baur, C. Deppe and H. Boche: "Secure Storage for Identification; Random Resources and Privacy Leakage". IEEE Transactions on Information Forensics and Security 14 (8), 2019, 2013 - 2027

- S. Baur, H. Boche, N. Cai: "Secret Key Generation from a Biometric Source with an Eavesdropping Jammer". IEEE Conference on Computer Communcations (INFOCOM) Workshops, 2019

- S. Baur, H. Boche, R.F. Schaefer, H.V. Poor: "Secure Storage Capacity under Rate Constraints — Continuity and Super Activation". IEEE Transactions on Information Forensics and Security (Early Access), 2019

- S. Baur, C. Deppe, H. Boche: "Secure Storage for Identification". IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2018

- S. Baur, H. Boche: "Robust Secure Authentication and Data Storage with Perfect Secrecy". MDPI Cryptography 2 (2), 2018

- S. Baur, H. Boche: "Robust secure storage of data sources with perfect secrecy". IEEE Workshop on Information Forensics and Security (WIFS), 2017

- S. Baur, H. Boche: "Storage of general data sources on a public database with security and privacy constraints". IEEE Conference on Communications and Network Security (CNS), 2017
- M. Khavari, S. Baur, H. Boche: "Optimal capacity region for PUF-based authentication with a constraint on the number of challenge-response pairs". IEEE Conference on Communications and Network Security (CNS), 2017
- S. Baur, H. Boche: "Robust Authentication and Data Storage with Perfect Secrecy". IEEE International Conference on Computer Communications (INFOCOM) Workshops, 2017

Bibliography

[1] IEEE Communications Society Tactile Internet Emerging Technical Subcommittee. `http://ti.committees.comsoc.org/standardisation/`. Accessed 15 Oct. 2018.

[2] Rudolf Ahlswede. Elimination of correlation in random codes for arbitrarily varying channels. *Probability Theory and Related Fields*, 44(2):159–175, 1978.

[3] Rudolf Ahlswede. Arbitrarily varying channels with states sequence known to the sender. *IEEE Transactions on Information Theory*, 32(5):621–629, 1986.

[4] Rudolf Ahlswede. *Storing and Transmitting Data: Rudolf Ahlswede's Lectures on Information Theory 1.* Springer International Publishing, 2014.

[5] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography–part I: Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[6] Rudolf Ahlswede and Gunter Dueck. Identification via channels. *IEEE Transactions on Information Theory*, 35(1):15–29, 1989.

[7] Sebastian Baur and Holger Boche. Robust authentication and data storage with perfect secrecy. In *Proc. IEEE Conference on Computer Communications Workshops*, pages 553–558, 2017.

[8] Sebastian Baur and Holger Boche. Robust secure authentication and data storage with perfect secrecy. *Cryptography*, 2(2):8, 2018.

[9] Sebastian Baur, Holger Boche, and Ning Cai. Secret key generation from a biometric source with an eavesdropping jammer. In *Proc. IEEE Conference on Computer Communications Workshops*, 2019. to appear.

[10] Sebastian Baur, Holger Boche, and Ning Cai. Secret key generation from a PUF source under jamming attacks. submitted.

[11] Sebastian Baur, Holger Boche, Rafael F Schaefer, and H Vincent Poor. Secure storage capacity under rate constraints—continuity and super activation. *IEEE Transactions on Information Forensics and Security (Early Access)*, 2019.

[12] Sebastian Baur, Ning Cai, Moritz Wiese, and Holger Boche. Secret key generation from a two component source with rate constrained one way communication: Perfect secrecy. submitted.

[13] Sebastian Baur, Ning Cai, Moritz Wiese, and Holger Boche. Secret key generation from a two component compound source with rate constrained one way communication: Perfect secrecy. In *Proc. IEEE International Workshop on Information Forensics and Security*, 2019. accepted for publication.

[14] Sebastian Baur, Christian Deppe, and Holger Boche. Secure storage for identification; random resources and privacy leakage. *IEEE Transactions on Information Forensics and Security*, 14(8):2013–2027, 2019.

[15] Igor Bjelaković, Holger Boche, and Jochen Sommerfeld. Capacity results for arbitrarily varying wiretap channels. In *Information Theory, Combinatorics, and Search Theory*, pages 123–144. Springer, Berlin, Heidelberg, 2013.

[16] Igor Bjelaković, Holger Boche, and Jochen Sommerfeld. Secrecy results for compound wiretap channels. *Problems of Information Transmission*, 49(1):73–98, 2013.

[17] David Blackwell, Leo Breiman, and AJ Thomasian. The capacity of a class of channels. *The Annals of Mathematical Statistics*, 30(4):1229–1241, 1959.

[18] David Blackwell, Leo Breiman, and AJ Thomasian. The capacities of certain channel classes under random coding. *The Annals of Mathematical Statistics*, 31(3):558–567, 1960.

[19] VM Blinovsky, P Narayan, and MS Pinsker. Capacity of the arbitrarily varying channel under list decoding. *Problems of Information Transmission*, 31(2):99–113, 1995.

[20] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[21] Holger Boche, Rafael F Schaefer, and H Vincent Poor. Denial-of-service attacks on communication systems: Detectability and jammer knowledge. submitted.

[22] I Csiszár and J Körner. On the Capacity of the Arbitrarily Varying Channel for Maximum Probability of Error. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 57(1):87–101, Mar. 1981.

[23] Imre Csiszár. The method of types [information theory]. *IEEE Transactions on Information Theory*, 44(6):2505–2523, 1998.

[24] Imre Csiszar and Prakash Narayan. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Transactions on Information Theory*, 34(2):181–193, 1988.

[25] Imre Csiszar and Prakash Narayan. Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46:344–366, 2000.

[26] Imre Csiszár and János Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[27] Gerhard Fettweis et al. The Tactile Internet. *ITU-T Technology Watch Report*, 2014.

[28] Onur Günlü. *Key Agreement with Physical Unclonable Functions and Biometric Identifiers*. Dissertation, Technische Universität München, 2019.

[29] Andrea Grigorescu, Holger Boche, and Rafael Schaefer. Robust biometric authentication from an information theoretic perspective. *Entropy*, 19(9):480, 2017.

[30] Andrea Grigorescu, Holger Boche, and Rafael F Schaefer. Robust PUF based authentication. In *Proc. IEEE Workshop on Information Forensics and Security*, pages 1–6, 2015.

[31] Brian L Hughes. The smallest list for the arbitrarily varying channel. *IEEE Transactions on Information Theory*, 43(3):803–815, 1997.

[32] Tanya Ignatenko and Frans M. J. Willems. Biometric security from an information-theoretical perspective. In *Foundations and Trends in Communications and Information Theory*, volume 7, pages 135–316. Now Publishers, Inc., 2012.

[33] Lifeng Lai, Siu-Wai Ho, and H Vincent Poor. Privacy-security tradeoffs in biometric security systems. In *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, pages 268–273. IEEE, 2008.

[34] Michael Langberg. Private codes or succinct random codes that are (almost) perfect. In *Proc. 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 325–334, 2004.

[35] Yingbin Liang, Gerhard Kramer, H Vincent Poor, and Shlomo Shamai. Compound wiretap channels. *EURASIP Journal on Wireless Communications and Networking*, 2009.

[36] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[37] Ueli M Maurer. The strong secret key rate of discrete random triples. In *Communications and Cryptography*, pages 271–285. Springer, 1994.

[38] Wolfgang Mulzer. Five proofs of chernoff's bound with applications. *arXiv preprint arXiv:1801.03365*, 2018.

[39] Janis Nötzel, Moritz Wiese, and Holger Boche. The arbitrarily varying wiretap channel—secret randomness, stability, and super-activation. *IEEE Transactions on Information Theory*, 62(6):3504–3531, 2016.

[40] Yury Polyanskiy, H Vincent Poor, and Sergio Verdú. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, 56(5):2307–2359, 2010.

[41] Yury Polyanskiy and Yihong Wu. Lecture notes on information theory. *Lecture Notes for ECE563 (UIUC)*, 2014.

[42] Anand Dilip Sarwate. *Robust and adaptive communication under uncertain interference*. PhD thesis, University of California, Berkeley, 2008.

[43] Rafael F Schaefer, Holger Boche, Ashish Khisti, and H Vincent Poor. *Information Theoretic Security and Privacy of Information Systems*. Cambridge University Press, 2017.

[44] Rafael F Schaefer, Holger Boche, and H Vincent Poor. Secure communication under channel uncertainty and adversarial attacks. *Proceedings of the IEEE*, 103(10):1796–1813, 2015.

[45] Paul C Shields. *The ergodic theory of discrete sample paths*. American Mathematical Society, 1996.

[46] Nima Tavangaran. *Robust Secret-Key Generation under Source Uncertainty and Communication Rate Constraint*. Dissertation, Technische Universität München, 2018.

[47] Moritz Wiese. *Multiple access channels with cooperating encoders*. Dissertation, Technische Universität München, 2013.

[48] Moritz Wiese, Janis Nötzel, and Holger Boche. A channel under simultaneous jamming and eavesdropping attack—correlated random coding capacities under strong secrecy criteria. *IEEE Transactions on Information Theory*, 62(7):3844–3862, 2016.

[49] Aaron D Wyner. The wire-tap channel. *Bell Labs Technical Journal*, 54(8):1355–1387, 1975.

[50] Rafael Felix Wyrembelski. *Robust Coding Strategies and Physical Layer Service Integration for Bidirectional Relaying*. Dissertation, Technische Universität München, 2012.