entropy

MDPI

Article

Robust Biometric Authentication from an Information Theoretic Perspective †

Andrea Grigorescu [1,*], Holger Boche [1] and Rafael F. Schaefer [2]

[1] Chair of Theoretical Information Technology, Technical University of Munich, 80290 Munich, Germany; boche@tum.de

[2] Information Theory and Applications Chair, Technische Universität Berlin, 10587 Berlin, Germany; rafael.schaefer@tu-berlin.de

* Correspondence: andrea.grigorescu@tum.de; Tel.: +49-89-289-23248

† This paper is an extended version of our paper published in the 7th IEEE International Workshop on Information Forensics and Security, Rome, Italy, 16–19 November 2015.

Received: 22 June 2017; Accepted: 7 September 2017; Published: 9 September 2017

Abstract: Robust biometric authentication is studied from an information theoretic perspective. Compound sources are used to account for uncertainty in the knowledge of the source statistics and are further used to model certain attack classes. It is shown that authentication is robust against source uncertainty and a special class of attacks under the strong secrecy condition. A single-letter characterization of the privacy secrecy capacity region is derived for the generated and chosen secret key model. Furthermore, the question is studied whether small variations of the compound source lead to large losses of the privacy secrecy capacity region. It is shown that biometric authentication is robust in the sense that its privacy secrecy capacity region depends continuously on the compound source.

Keywords: biometric authentication; compound source; strong secrecy; privacy leakage; robustness

1. Introduction

Biometric identifiers, such as fingerprints, iris and retina scans, are becoming increasingly attractive for the use in security systems because of their uniqueness and time invariant characteristics—for example, in authentication and identification systems. Conventional personal authentication systems usually use secret passwords or physical tokens to guarantee the legitimacy of a person. On the other hand, biometric authentication systems use the physical characteristics of a person to guarantee the legitimacy of the person to be authenticated.

Biometric authentication systems are decomposed into two phases: the enrollment and the authentication phase. A simple authentication approach is to gather biometric measurements in the enrollment phase, apply a one-way function and then store the results in a public database. In the authentication phase, new biometric measurements are gathered. The same one-way is applied and the outcome is then compared to the one stored in the database. Unfortunately, biometric measurements might be affected by noise. To deal with noisy data, error correction is needed. Therefore, helper data is generated during the enrollment phase as well based on the biometric measurements and then stored directly in the public database that will be then used in the authentication phase, which will then be used in the authentication phase to correct the noisy imperfections of the measurements.

Since the database containing the helper data is public, an eavesdropper can have access to the data if desired. How can we prevent an eavesdropper from gaining information about the biometric data from the publicly stored helper data? One is interested in encoding the biometric data into a helper data and a secret key such that the helper data does not reveal any information about the secret key. Cryptographic techniques are one approach to keeping the key secret. However, security

on higher layers is usually based on the assumption of insufficient computational capabilities of eavesdroppers. Information theoretic security, on the contrary, uses the physical properties of the source to guarantee security independent from the computational capabilities of the adversary. This line of research was initiated by Shannon in [1] and has attracted considerable interest recently—cf., for example, recent textbooks [2–4] and references therein. In particular, Ahlswede and Csiszár in [5] and Maurer in [6] introduced a secret key sharing model. It consists of two terminals that observe the correlated sequences of a joint source. Both terminals generate a common key based on their observation and using public communication. The message transmitted over the public channel should not leak any amount of information about the common key.

Both works mentioned above use the weak secrecy condition as a measure of secrecy. Given a code of a certain blocklength, the weak secrecy condition is fulfilled if the mutual information between the key and the available information at the eavesdropper normalized by the code blocklength is arbitrarily small for large blocklengths. On the other hand, the strong secrecy condition is fulfilled if the un-normalized mutual information between the key and the available information at the eavesdropper is arbitrarily small for large blocklengths, i.e., the total amount of information leaked to the eavesdropper is negligible. The secret key sharing model satisfying the strong secrecy condition has been studied in [7].

One could model the biometric authentication similar to this secret key generation source model; however, this model does not take into account the amount of information that the public data (the helper data in the biometric scenario) leaks about the biometric measurement. The goal of biometric authentication is to perform a secret and successful authentication procedure without compromising the information about the user (privacy leakage). Compromised biometric information is unique and cannot be replaced, so once it is compromised, it is compromised forever, which might lead to an identity theft (see [8–10] for more information on privacy concerns). Since the helper data we use to deal with noisy data is a function of the biometric measurements, it contains information about the biometric measurement. Thus, if an attacker breaks into the data base, he could be able to extract information about the biometric measurement from where the helper data is stored. Hence, we aim to control the privacy leakage as well. An information theoretic approach of secure biometric authentication controlling the privacy leakage was studied in [11,12] under ideal conditions, i.e., with perfect source state information (SSI) and without the presence of active attackers.

In both references [11,12], the capacity results under the weak secrecy condition were derived. In [13], the capacity result for the sequential key-distillation with rate limited one-way public communication using the strong secrecy condition was shown.

For reliable authentication, SSI is needed; however, in practical systems, it is never perfectly available. Compound sources model a simple and realistic SSI scenario in which the legitimate users are not aware of the actual source realisation. Nevertheless, they know that it belongs to a known uncertainty set of sources and that it remains constant during the entire observation. This model was first introduced and studied in [14,15] in a channel coding context. Compound sources can also model the presence of an active attacker, who is able to control the state of the source. We are interested in performing an authentication process that is robust against such uncertainties and attacks. The secret key generation for source uncertainty was studied in [16–19]. In [16], the secret key generation using compound joint sources was studied and the key-capacity was established.

In [20], the achievability result of the privacy secrecy capacity region for generated secret keys for compound sources has been derived under the weak secrecy condition. In this work, we study robust biometric authentication in detail and extend this result in several directions. First, we consider a model where the legitimate users suffer from source uncertainty and/or attacks and derive achievability results under the strong secrecy conditions for both the generated and chosen secret key authentication. We then provide matching converses to obtain single-letter characterizations of the corresponding privacy secrecy capacity regions.

We further address the following question: can small changes of the compound source cause large changes in the privacy secrecy capacity region? Such a question has been first studied in [21] for arbitrarily varying quantum channels (AVQCs) showing that deterministic capacity has discontinuity points, while the randomness-assisted capacity is a continuous function of the AVQCs. This line of research is continued in [22,23], in which the classical compound wiretap channel, the arbitrarily varying wiretap channel (AVWC), and the compound broadcast channel with confidential messages (BCC) are studied. We study this for the biometric authentication problem at hand and show that the corresponding privacy secrecy capacity regions are continuous functions of the underlying uncertainty sets. Thus, small changes in the compound set lead to small changes in the capacity region only.

The rest of this paper is organized as follows. In Section 2, we introduce the biometric authentication model for perfect SSI and present the corresponding capacity results. In Section 3, we introduce the biometric authentication model for compound sources and show that secure, under the strong secrecy condition, and reliable authentication, under source uncertainty with positive rates, is possible deriving a single-letter characterization of the privacy secrecy capacity region for the chosen and generated secret key model. In Section 4, we show that the privacy secrecy capacity region for compound sources is a continuous function of the uncertainty set. Finally, the paper ends with a conclusion in Section 5.

Notation: Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters. $\mathcal{P}(\mathcal{X})$ denotes the set of all probability distributions on $\mathcal{X}$; $\mathbb{E}(\cdot)$ denotes the expectation of a random variable; $\Pr\{\cdot\}$, $H(\cdot)$ and $I(\cdot;\cdot)$ indicate the probability, the entropy of a random variable, and mutual information between two random variables; $D(\cdot\|\cdot)$ is the information divergence; $\|p-q\|_{TV}$ is the total variation distance between p and q on $\mathcal{X}$ defined as $\|p-q\|_{TV} \coloneqq \sum_{x\in\mathcal{X}} |p(x)-q(x)|$. The set $\mathcal{T}^n_{p,\delta}$ denotes the set of $\delta-$typical sequences of length n with respect to the distribution p; the set $\mathcal{T}^n_{W,\delta}(x^n)$ denotes the set of $\delta-$conditional typical sequences with respect to the conditional distribution $W\colon \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ and sequence $x^n \in \mathcal{X}^n$; p_{x^n} denotes the empirical distribution of the sequence x^n.

2. Information Theoretic Model for Biometric Authentication

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite alphabets. Let $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ be a pair of biometric sequences of length $n \in \mathbb{N}$; then, the discrete memoryless joint-source is given by the joint probability distribution $Q^n(x^n, y^n) \coloneqq \prod_{i=1}^n Q(x_i, y_i)$. This models perfect SSI, i.e., all possible measurements are generated by the discrete memoryless joint-source source Q, which is perfectly known at both the enrollment and the authentication terminal.

2.1. Generated Secret Key Model

The information theoretic authentication model consists of a discrete memoryless joint-source Q, which represents the biometric measurement source, and two terminals: the enrollment terminal and the authentication terminal as shown in Figure 1. At the enrollment terminal, the enrollment sequence X^n is observed and the secret key K and helper data M' are generated. At the authentication terminal, the authentication sequence Y^n is observed. An estimate of the secret key $\hat{K}$ is made based on the authentication sequence Y^n and the helper data M'. Since the helper data is stored in a public database, this should not reveal anything about the secret key K and also as little as possible about the enrollment measurement X^n. The distribution of the key must be close to uniform.

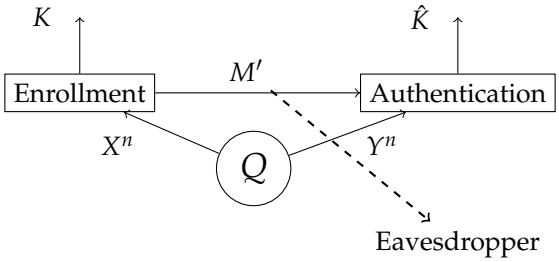

Figure 1. The biometric measurements X^n and Y^n are observed in the enrollment and authentication terminal, respectively. In the enrollment terminal, the key K and the helper data M' are generated. The helper data is public, hence the eavesdropper also has access to it. In the authentication terminal, an estimation of a key $\hat{K}$ is made based on the observed biometric measurements Y^n and the helper data M'.

We consider a block-processing of arbitrary but fixed length n. Let $\mathcal{M}' := \{1, \ldots, M'_n\}$ be the helper data set and $\mathcal{K} := \{1, \ldots, K_n\}$ the secret key set.

Definition 1. *An (n, M'_n, K_n)-code for generated secret key authentication for joint-source $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ consists of an encoder f at the enrollment terminal with*

$$f \colon \mathcal{X}^n \to \mathcal{K} \times \mathcal{M}'$$

and a decoder φ at the authentication terminal

$$\varphi \colon \mathcal{Y}^n \times \mathcal{M}' \to \mathcal{K}.$$

Remark 1. *Note that the function f means that every x^n is mapped into a $(k, m') \in \mathcal{K} \times \mathcal{M}'$, which implies that $|f(\cdot)| = K_n M'_n \leq |\mathcal{X}^n|$.*

Definition 2. *A privacy secrecy rate pair $(R_{PL}, R_K) \in \mathbb{R}^2_+$ is called achievable for the generated secret key authentication for a joint-source Q, if, for any $\delta > 0$, there exist an $n(\delta) \in \mathbb{N}$ and a sequence of (n, M'_n, K_n)-codes such that, for all $n \geq n(\delta)$, we have*

$$\Pr\{\hat{K} \neq K\} \leq \delta, \tag{1a}$$

$$\frac{1}{n} H(K) + \delta \geq \frac{1}{n} \log K_n \geq R_K - \delta, \tag{1b}$$

$$\frac{1}{n} I(K; M') \leq \delta, \tag{1c}$$

$$\frac{1}{n} I(X^n; M') \leq R_{PL} + \delta. \tag{1d}$$

Remark 2. *Condition (1b) requires the key distribution p_K to be close to the uniform distribution $p_{\tilde{K}}$, where $\tilde{K}$ is a random variable uniformly distributed over the key set $\mathcal{K}$. By (1b), we have $\frac{1}{n} \log K_n - \frac{1}{n} H(K) = D(K \| \tilde{K}) \leq \delta$; combined with Pinsker's inequality, we have $\| p_K - p_{\tilde{K}} \| \leq \sqrt{2 \ln 2 \delta}$. For small δ, we have that both distributions are close to each other.*

Remark 3. *Condition (1a) stands for reliable authentication, the information about the key leaked by the helper data is negligible by (1c) and the information about the biometric measurements leaked by the helper data $\frac{1}{n} I(X^n; M')$ is close to R_{PL} by (1d).*

Definition 3. *The set of all achievable privacy secrecy rate pairs for generated key authentication is called privacy secrecy capacity region and is denoted by $\mathfrak{C}_G(Q)$.*

We next present the privacy secrecy capacity region for the generated key authentication for the joint-source Q, which was first established in [11,12].

To do so, for some U with alphabet $|\mathcal{U}| \leq |\mathcal{X}| + 1$ and $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, we define the region $\mathcal{R}(Q, V)$ as the set of all $(R_{PL}, R_K) \in \mathbb{R}_+^2$ satisfying

$$\begin{aligned} R_K &\leq I(U;Y), \\ R_{PL} &\geq I(U;X) - I(U;Y), \end{aligned}$$

with $P_{UXY}(u, x, y) = V(u|x)Q(x, y)$.

Theorem 1 ([11,12])**.** *The privacy secrecy capacity region for generated key authentication is given by*

$$\mathfrak{C}_G(Q) = \bigcup_{V\colon \mathcal{X}\to\mathcal{P}(\mathcal{U})} \mathcal{R}(Q, V).$$

2.2. Chosen Secret Key Model

In this section, we study the authentication model for systems for which the secret key is chosen beforehand. At the enrollment terminal, a secret key K is chosen uniformly and independent of the biometric measurements. The secret key K is bound to the biometric measurements X^n, and, based on this, the helper data M' is generated as shown in Figure 2. At the authentication terminal, the authentication measurement Y^n is observed. An estimate of the secret key $\hat{K}$ is made based on the authentication sequence Y^n and the helper data M'. Since the helper data is stored in a public database, this should not reveal anything about the secret key and minimize the information leakage about the enrollment sequence X^n. However, we should be able to reconstruct K. To achieve this, a masking layer based on the one-time pad principles is used.

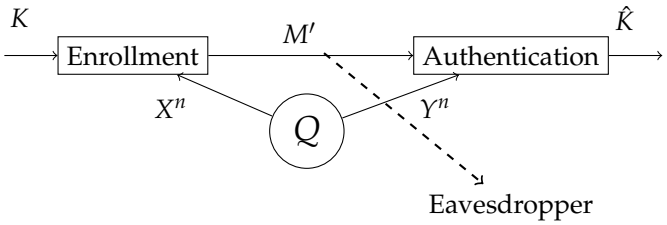

Figure 2. The biometric sequences X^n and Y^n are observed at the enrollment and authentication terminal, respectively. In the enrollment terminal, the helper data M' is generated for a given secret key K. The helper data is public, hence the eavesdropper also has access to it. In the authentication terminal, an estimation of a key $\hat{K}$ is made based on the observed biometric authentication sequence Y^n and the helper data M'.

The masking layer, which is another uniformly distributed chosen secret key K, is added to the top of the generated secret key authentication. At the enrollment terminal, a secret key K_g and a helper data M are generated. The generated secret key is added modulo-$|\mathcal{K}|$ to the masking layer K and sent together with the helper data as additional helper data, i.e., $M' = (M, K \oplus K_g)$. At the authentication terminal, an estimation of the generated secret key $\hat{K}_g$ is made based on Y^n and M and the estimation of masking layer is made $\hat{K} = K \oplus K_g \ominus \hat{K}_g$.

We consider a block-processing of arbitrary but fixed length n. Let $\mathcal{M}' := \{1, \ldots, M_n'\}$ be the helper data set and $\mathcal{K} := \{1, \ldots, K_n\}$ the secret key set.

Definition 4. *An* (n, M'_n, K_n)-code *for chosen secret key authentication for joint-source* $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ *consists of an encoder* f *at the enrollment terminal with*

$$f\colon \mathcal{K} \times \mathcal{X}^n \to \mathcal{M}'$$

and a decoder φ *at the authentication terminal*

$$\varphi\colon \mathcal{Y}^n \times \mathcal{M}' \to \mathcal{K}.$$

Definition 5. *A privacy secrecy rate pair* $(R_{PL}, R_K) \in \mathbb{R}_+^2$ *for chosen secret key authentication is called achievable for a joint-source* Q*, if, for any* $\delta > 0$*, there exist an* $n(\delta) \in \mathbb{N}$ *and a sequence of* (n, M'_n, K_n)*-codes, such that, for all* $n \geq n(\delta)$*, we have*

$$\Pr\{\hat{K} \neq K\} \leq \delta, \tag{2a}$$

$$\frac{1}{n} \log K_n \geq R_K - \delta, \tag{2b}$$

$$\frac{1}{n} I(K; M') \leq \delta, \tag{2c}$$

$$\frac{1}{n} I(X^n; M') \leq R_{PL} + \delta. \tag{2d}$$

Remark 4. *The difference between Definition 5 and 2 is that, in here, the uniformity of the key is already guaranteed.*

Definition 6. *The privacy secrecy capacity region for chosen secret key authentication for the joint-source* $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ *is called* privacy secrecy capacity region *and is denoted as* $\mathfrak{C}_C(Q)$*.*

We next present the privacy secrecy capacity region for chosen secret key authentication for the joint-source Q as showed in [11].

Theorem 2 ([11])**.** *The privacy secrecy capacity region for the chosen secret key authentication is given by*

$$\mathfrak{C}_C(Q) = \bigcup_{V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})} \mathcal{R}(Q, V).$$

3. Authentication for Compound Sources

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite sets and $\mathcal{S}$ a finite state set. Let $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ be a sequence pair of length $n \in \mathbb{N}$. For every $s \in \mathcal{S}$, the discrete memoryless joint-source is given by the joint probability distribution $Q_s^n(x^n, y^n) := \prod_{i=1}^n Q_s(x_i, y_i) = \prod_{i=1}^n p_s(x_i) W_s(y_i|x_i)$, with $p_s \in \mathcal{P}(\mathcal{X})$ a marginal distribution on $\mathcal{X}$ and $W_s\colon \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ a stochastic matrix.

Definition 7. *The discrete memoryless compound joint-source* $\mathfrak{Q}_{\mathcal{XY}}$ *is given by the family of joint probabilities distributions on* $\mathcal{X} \times \mathcal{Y}$ *as*

$$\mathfrak{Q}_{\mathcal{XY}} := \{Q_s \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})\colon s \in \mathcal{S}\}.$$

We define the finite set of marginal distributions $\mathfrak{Q}_{\mathcal{X}}$ over the alphabet $\mathcal{X}$ from the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$ as

$$\mathfrak{Q}_{\mathcal{X}} := \left\{p_s \in \mathcal{P}(\mathcal{X})\colon s \in \mathcal{S},\ \ p_s(x) = \sum_{y \in \mathcal{Y}} Q_s(x, y) \ \text{ for every } x \in \mathcal{X} \text{ and } Q_s \in \mathfrak{Q}_{\mathcal{XY}}\right\}.$$

We define $\mathcal{L}$ as the index set of $\mathfrak{Q}_{\mathcal{X}}$. Note that $|\mathcal{L}| = |\mathfrak{Q}_{\mathcal{X}}| \leq |\mathfrak{Q}_{\mathcal{XY}}|$.

For every $\ell \in \mathcal{L}$, we define the subset of the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$ with the same marginal distribution p_ℓ as

$$\mathfrak{Q}_{\mathcal{XY},\ell} \coloneqq \{Q_s \in \mathfrak{Q}_{\mathcal{XY}} : Q_s(x,y) = p_\ell(x)W_s(y|x) \text{ for every } (x,y) \in \mathcal{X} \times \mathcal{Y}\}.$$

For every $\ell \in \mathcal{L}$, we define the index set $\mathcal{S}_\ell$ of $\mathfrak{Q}_{\mathcal{XY},\ell}$ as

$$\mathcal{S}_\ell \coloneqq \{s \in \mathcal{S} \colon Q_s \in \mathfrak{Q}_{\mathcal{XY},\ell}\}.$$

Remark 5. *Note that, for every $\ell, \ell' \in \mathcal{L}$ with $\ell \neq \ell'$, it holds that $\mathfrak{Q}_{\mathcal{XY},\ell} \cap \mathfrak{Q}_{\mathcal{XY},\ell'} = \emptyset$, $\mathcal{S}_\ell \cap \mathcal{S}_{\ell'} = \emptyset$, $\mathcal{S} = \bigcup_{\ell \in \mathcal{L}} \mathcal{S}_\ell$ and $\mathfrak{Q}_{\mathcal{XY}} = \bigcup_{\ell \in \mathcal{L}} \mathfrak{Q}_{\mathcal{XY},\ell}$.*

3.1. Compound Generated Secret Key Model

In this section, we study the generated secret key authentication for finite compound joint-sources, which is a special class of sources that model a limited SSI, as shown in Figure 3.

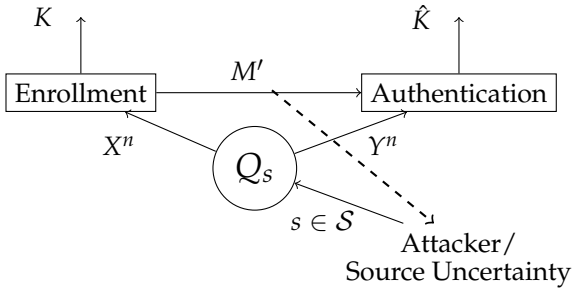

Figure 3. The attacker controls the state of the source $s \in \mathcal{S}$. The biometric sequences X^n and Y^n are observed at the enrollment and authentication, terminal respectively. In the enrollment terminal, the key K and the helper data M' are generated. The helper data is public, hence the attacker also has access to it. In the authentication terminal, an estimation of a key $\hat{K}$ is made based on the observed authentication sequence Y^n and the helper data M'.

We consider a block-processing of arbitrary but fixed length n. Let $\mathcal{M}' \coloneqq \{1, \ldots, M'_n\}$ be the helper data set and $\mathcal{K} \coloneqq \{1, \ldots, K_n\}$ the secret key set.

Definition 8. *An (n, M'_n, K_n)-*code *for generated secret key authentication for the compound joint-source $\mathfrak{Q}_{\mathcal{XY}} \subset \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ consists of an encoder f at the enrollment terminal with*

$$f \colon \mathcal{X}^n \to \mathcal{K} \times \mathcal{M}'$$

and a decoder φ at the authentication terminal

$$\varphi \colon \mathcal{Y}^n \times \mathcal{M}' \to \mathcal{K}.$$

Definition 9. *A privacy secrecy rate pair $(R_{PL}, R_K) \in \mathbb{R}_+^2$ is called achievable for generated secret key authentication for the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$, if, for any $\delta > 0$, there exist an $n(\delta) \in \mathbb{N}$ and a sequence of (n, M_n', K_n)-codes, such that for all $n \geq n(\delta)$ and for every $s \in \mathcal{S}$, we have*

$$\begin{aligned} \Pr\{\hat{K} \neq K\} &\leq \delta, \\ H(K) + \delta \geq \frac{1}{n} \log K_n &\geq R_K - \delta, \\ I(K; M') &\leq \delta, \\ \frac{1}{n} I(X_s^n; M') &\leq R_{PL} + \delta. \end{aligned}$$

Consider the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$. For a fixed $\ell \in \mathcal{L}$, $V \colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$ and for every $s \in \mathcal{S}_\ell$, we define the region $\mathcal{R}(V, \ell, s)$ as the set of all $(R_{PL}, R_K) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_K &\leq I(U_\ell; Y_s), \\ R_{PL} &\geq I(U_\ell; X_\ell) - I(U_\ell; Y_s), \end{aligned}$$

with $P_{UXY,s}(u, x, y) = V(u|x) Q_s(x, y)$.

Theorem 3. *The privacy secrecy capacity region for generated secret key authentication for the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$ is given by*

$$\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}}) = \bigcap_{\ell \in \mathcal{L}} \bigcup_{\substack{V: \mathcal{X} \to \mathcal{P}(\mathcal{U}) \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_\ell|}} \bigcap_{s \in \mathcal{S}_\ell} \mathcal{R}(V, \ell, s).$$

Proof. The proof of Theorem 3 consists of two parts: achievability and converse. The achievability scheme uses the following protocol:

- Estimate the marginal distribution $p_{\hat{\ell}} \in \mathfrak{Q}_{\mathcal{X}}$ from the observed sequence X^n at the enrollment terminal via hypothesis testing.
- Compute the key K and a helper data M based on X^n, a common shared sequence $T = U^n$ by the enrollment and authentication terminal and using an extractor function $g \colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^k$ with $N, d, k \in \mathbb{N}$ whose input are the shared sequence T and a sequence of d uniformly distributed bits U_d. The helper data M is equivalent to the helper data for the case with perfect SSI. The extended helper data in this case contains also the state of the marginal distribution and the uniformly distributed bits sequence, i.e., $M' = (M, \hat{L}, U_d)$.
- Store the extended helper data M' in the public database.
- Estimate the key $\hat{K}$ at the authentication terminal, based on the observations M' and Y^n, which can be seen as the outcome of one of the channels in $\mathfrak{W}_{\hat{\ell}} := \{W_s \colon \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \colon s \in \mathcal{S}_{\hat{\ell}}\}$.

A detailed proof can be found in Appendix A. □

Remark 6. *Note that the authentication for compound source model is a generalization of the models studied by [11,12], i.e., $|\mathcal{S}| = 1$. Furthermore, one can see that, for $|\mathcal{S}| = 1$, the capacity region under the strong secrecy condition equals the capacity region under the weak secrecy condition showed by [11,12].*

Remark 7. *As we already mentioned, we aim for strong secrecy, i.e., in contrast to the weak secrecy constraint in (1c), we now require the un-normalized mutual information between the key and the helper data to be negligibly small. It would be Ideal to show perfect secrecy and a perfectly uniformed key, i.e., $I(K; M') = 0$ and $H(K) = \frac{1}{n} \log K_n$. It would be interesting to see how this constraint affects the achievable rate region. We suspect that the achievable rate region under perfect secrecy and perfectly uniformed key remains the same as in Theorem 3.*

Remark 8. *From the protocol, note that once we have estimated the marginal distribution $p_{\hat{\ell}} \in \mathfrak{Q}_{\mathcal{X}}$, we deal with a compound channel model without channel state information (CSI) at the transmitter (see [24]).*

Remark 9. *The order of the set operations of the capacity region displays the fact that the marginal distribution is first estimated. This can be seen as partial state information, where the marginal distribution over $\mathcal{X}$ is known.*

3.2. Compound Chosen Secret Key Model

In this section, we study chosen secret key authentication for finite compound joint-sources (see Figure 4).

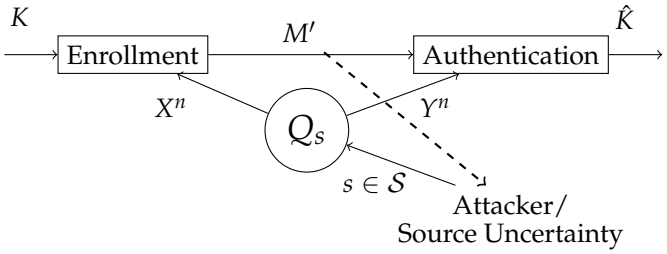

Figure 4. The attacker controls the state of the source $s \in \mathcal{S}$. The biometric sequences X^n and Y^n are observed in the enrollment and authentication terminal, respectively. In the enrollment terminal, the key K is predefined and the helper data M' is generated. The helper data is public, hence the attacker also has access to it. In the authentication terminal, an estimation of a key $\hat{K}$ is made based on the observed authentication sequences Y^n and the helper data M'.

We consider a (n, M'_n, K_n)-code of arbitrary but fixed length n.

Definition 10. *A privacy secrecy rate pair $(R_{PL}, R_K) \in \mathbb{R}_+^2$ is called achievable for chosen secret key authentication for the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$, if for any $\delta > 0$ there exist an $n(\delta) \in \mathbb{N}$ and a sequence of (n, M'_n, K_n)-codes, such that, for all $n \geq n(\delta)$ and for every $s \in \mathcal{S}$, we have*

$$\Pr\{\hat{K} \neq K\} \leq \delta, \tag{3a}$$

$$\frac{1}{n} \log K_n \geq R_K - \delta, \tag{3b}$$

$$I(K; M') \leq \delta, \tag{3c}$$

$$\frac{1}{n} I(X_s^n; M') \leq R_{PL} + \delta. \tag{3d}$$

Consider the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$. For a fixed $\ell \in \mathcal{L}$, $V \colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$ and for every $s \in \mathcal{S}_\ell$, we define the region $\mathcal{R}(V, \ell, s)$ as the set of all $(R_{PL}, R_K) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_K &\leq I(U_\ell; Y_s), \\ R_{PL} &\geq I(U_\ell; X_\ell) - I(U_\ell; Y_s), \end{aligned}$$

with $P_{UXY,s}(u, x, y) = V(u|x) Q_s(x, y)$.

Theorem 4. *The privacy secrecy capacity region for chosen secret key authentication for the compound joint-source $\mathfrak{Q}_{\mathcal{XY}}$ is given by*

$$\mathfrak{C}_C(\mathfrak{Q}_{\mathcal{XY}}) = \bigcap_{\ell \in \mathcal{L}} \bigcup_{\substack{V: \mathcal{X} \to \mathcal{P}(\mathcal{U}) \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_\ell|}} \bigcap_{s \in \mathcal{S}_\ell} \mathcal{R}(V, \ell, s).$$

Proof. The proof can be found in Appendix B. □

Remark 10. *Note that, as for generated secret key authentication for compound sources, chosen secret key authentication for compound sources is a generalization of the models studied by [11]. Furthermore, for perfect SSI, one can see that the capacity region under the strong secrecy condition equals the capacity region under the weak secrecy condition showed by [11].*

Remark 11. *Note that the privacy secrecy capacity region for the generated key model equals the privacy secrecy capacity region for chosen secret key authentication, i.e.,* $\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}}) = \mathfrak{C}_C(\mathfrak{Q}_{\mathcal{XY}})$.

4. Continuity of the Privacy Secrecy Capacity Region for Compound Sources

We are interested in studying how small variations in the compound source affect the privacy secrecy capacity region. The question of whether the capacity or capacity region is a continuous function of a source or channel is not always clear, especially if the source or channel are complicated. In [22], one can find an example of AVWCs, whose uncertainty set consists of only two channels, which already shows discontinuity points in its unassisted secrecy capacity. For a detailed discussion, see [25]. In this section, we study the continuity of the privacy secrecy capacity region for compound sources. For this purpose, we introduce the distance between two compound sources and capacity regions, respectively.

4.1. Distance between Compound Sources

Definition 11. *Let* $\mathfrak{Q}_{\mathcal{XY},1}$ *and* $\mathfrak{Q}_{\mathcal{XY},2}$ *be two compound sources. We define*

$$d_1(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2}) = \max_{s_2 \in \mathcal{S}_2} \min_{s_1 \in \mathcal{S}_1} \|Q_{s_1} - Q_{s_2}\|_{TV},$$
$$d_2(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2}) = \max_{s_1 \in \mathcal{S}_1} \min_{s_2 \in \mathcal{S}_2} \|Q_{s_1} - Q_{s_2}\|_{TV}.$$

The Hausdorff distance $D_H(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2})$ *between* $\mathfrak{Q}_{\mathcal{XY},1}$ *and* $\mathfrak{Q}_{\mathcal{XY},2}$ *is defined as*

$$D_H(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2}) = \max\Big\{d_1(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2}), d_2(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2})\Big\}.$$

Definition 12. *Let* $\mathcal{R}_1$, *and* $\mathcal{R}_2$ *be two non-empty subsets of the metric space* $(\mathbb{R}^2, d)$ *with* $d(x,y) = \sqrt{\sum_{i=1}^2 |x_i - y_i|^2}$ *for all* $x, y \in \mathbb{R}^2$. *We define the distance between two sets as*

$$D_R(\mathcal{R}_1, \mathcal{R}_2) = \max\{\max_{r_1 \in \mathcal{R}_1} \min_{r_2 \in \mathcal{R}_2} d(r_1, r_2), \max_{r_2 \in \mathcal{R}_2} \min_{r_1 \in \mathcal{R}_2} d(r_1, r_2)\}.$$

4.2. Continuity of the Privacy Secrecy Capacity Region

Theorem 5. *Let* $\epsilon \in (0,1)$ *and* $n \in \mathbb{N}$. *Let* $\mathfrak{Q}_{\mathcal{XY},1}$ *and* $\mathfrak{Q}_{\mathcal{XY},2}$ *be two compound sources. If*

$$D_H(\mathfrak{Q}_{\mathcal{XY},1}, \mathfrak{Q}_{\mathcal{XY},2}) \leq \epsilon,$$

then it holds

$$D_R(\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY},1}), \mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY},2})) \leq \delta(\epsilon, |\mathcal{X}|, |\mathcal{Y}|) \tag{4}$$

with $\delta(\epsilon) = \sqrt{\delta_1(\epsilon)^2 + \delta_2(\epsilon)^2}$, *where* $\delta_1(\epsilon) = 2\epsilon \log |\mathcal{Y}| + 2H_2(\epsilon) - \epsilon \log \frac{\epsilon}{|\mathcal{U}|}$ *and* $\delta_2(\epsilon) = 2\epsilon \log |\mathcal{Y}||\mathcal{X}| + 4H_2(\epsilon) - 2\epsilon \log \frac{\epsilon}{|\mathcal{U}|}$.

Remark 12. *Note that since the privacy secrecy capacity region for the chosen secret key equals the privacy secrecy capacity region for the chosen secret key, the continuity behaviour holds also for the chosen secret key privacy capacity region.*

Remark 13. *This theorem shows that the privacy secrecy capacity region is a continuous function of the uncertainty set. In other words, small variations of the uncertainty set lead to small variations in the capacity region.*

Proof. A detailed proof can be found in Appendix C. □

Remark 14. *A complete characterisation of the discontinuity behaviour of the AVC capacity under list decoding can be found in [26]. Note that this behaviour, based on Theorem 5, can not occur.*

5. Conclusions

In this paper, we considered a biometric authentication model in the presence of source uncertainty. In particular, we studied a model where the actual source realization is not known, however it belongs to a known source set: this is the finite compound source model. We have shown that biometric authentication is robust against source uncertainty and certain classes of attacks. In other words, reliable and secure authentication is possible at positive key rates. We further characterize the minimum privacy leakage rate under source uncertainty. For future work, perfect secrecy for the biometric authentication model and a compound source with infinite sources is of great interest.

Acknowledgments: The authors would like to thank their Sebastian Baur for insightful discussions. This work was supported by the Gottfried Wilhelm Leibniz Programme of the German Research Foundation (DFG) under Grant BO 1734/20-1, Grant BO 1734/24-1 and Grant BO 1734/25-1.

Author Contributions: Andrea Grigorescu, Holger Boche and Rafael Schaefer conceived this study and derived the results. Andrea Grigorescu and wrote the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Theorem 3

Appendix A.1. Achievability of Theorem 3

Appendix A.1.1. State Estimation

We first show that we can estimate the marginal distribution $p_{\hat{\ell}} \in \mathfrak{Q}_{\mathcal{X}}$ correctly with probability approaching one. Then, for every $\ell = \hat{\ell} \in \mathcal{L}$, we use the random coding argument to show that all rate pairs $(R_{PL}, R_K) \in \mathcal{R}(V, \ell, s)$ are achievable.

To estimate the actual source realization, we perform hypothesis testing. The set of hypotheses is the set of finite marginal distributions $\mathfrak{Q}_{\mathcal{X}}$. For every $\ell \in \mathcal{L}$, we define

$$\delta_\ell = \frac{1}{2} \min_{\substack{\ell' \neq \ell \\ \ell' \in \mathcal{L}}} \|p_\ell - p_{\ell'}\|_{TV}.$$

We choose $0 < \delta < \min_{\ell \in \mathcal{L}} \delta_\ell$ and consider the test set (typical sequences set) $\mathcal{T}^n_{p_\ell, \delta} := \{x^n \in \mathcal{X}^n \colon \|p_{x^n} - p_\ell\| \leq \delta\}$. Note that, for every $\ell, \ell' \in \mathcal{L}$ with $\ell' \neq \ell$, we have that $\mathcal{T}^n_{p_{\ell'}, \delta} \cap \mathcal{T}^n_{p_\ell, \delta} = \emptyset$. We show this by arbitrarily choosing a sequence $x^n \in \mathcal{T}^n_{p_\ell, \delta}$ of type p_{x^n} and show that $\|p_{\ell'} - p_{x^n}\|_{TV} > \delta$ for $\ell' \neq \ell$. By the triangle inequality, we have

$$\begin{aligned} \|p_\ell - p_{\ell'}\|_{TV} &= \|p_\ell - p_{\ell'} + p_{x^n} - p_{x^n}\|_{TV} \\ &\leq \|p_\ell - p_{x^n}\|_{TV} + \|p_{x^n} - p_{\ell'}\|_{TV}. \end{aligned}$$

Hence,

$$\begin{aligned} \|p_{x^n} - p_{\ell'}\|_{TV} &\geq \|p_\ell - p_{\ell'}\|_{TV} - \|p_\ell - p_{x^n}\|_{TV} \\ &\geq 2\delta_{\ell'} - \delta > \delta, \end{aligned}$$

proving the disjointness of the sets.

The test function is the indicator function $\mathbb{1}[x^n \in \mathcal{T}^n_{p_{\ell},\delta}]$, i.e., after observing x^n the test looks for the hypothesis $p_{\hat{\ell}} = p_{\ell}$ for which $\mathbb{1}[x^n \in \mathcal{T}^n_{p_{\ell},\delta}] = 1$.

An error occurs, if the sequence x^n was generated by the source p_{ℓ} for any $\ell \in \mathcal{L}$; however, $x^n \notin \mathcal{T}^n_{p_{\ell},\delta}$. This implies that either $x^n \notin \bigcup_{\ell \in \mathcal{L}} \mathcal{T}^n_{p_{\ell},\delta}$ or $x^n \in \mathcal{T}^n_{p_{\ell'},\delta}$ with $\ell' \neq \ell$. Using Lemma 2.12 in [27], we upper bound the probability of this error event by

$$p_{\ell}({\mathcal{T}^n_{p_{\ell},\delta}}^c) \leq \epsilon_{\delta}(n, |\mathcal{X}|), \tag{A1}$$

where $\epsilon_{\delta}(n, |\mathcal{X}|) = (n+1)^{|\mathcal{X}|} 2^{-nc\delta^2}$. Letting $n \to \infty$, the right-hand side of (A1) tends to zero.

Appendix A.1.2. Code Construction

For each $\ell \in \mathcal{L}$, we consider the auxiliary random variable U and the channel V and construct a code for which we analyze the decoding error, secrecy and privacy condition.

Generate $2^{n(R_K+R_M)}$ codewords $U^n_{k,m}$ with $k \in \mathcal{K} := \{1, \ldots, 2^{nR_K}\}$ and $m \in \mathcal{M} := \{1, \ldots, 2^{nR_M}\}$ by choosing each symbol $U_{i_{k,m}}$ in the codebook independently at random according to $p_u \in \mathcal{P}(\mathcal{U})$, computed from $p_{\ell}(x)V(u|x)$ for every $(x,u) \in \mathcal{X} \times \mathcal{U}$. We denote the codebook as $\tilde{U} = \{U^n_{k,m}\}_{(k,m) \in \mathcal{K} \times \mathcal{M}}$.

For every $\ell \in \mathcal{L}$ and every $s \in \mathcal{S}_{\ell}$, we define the following channels $\Sigma_{\mathcal{X}_{\ell}} : \mathcal{U} \to \mathcal{P}(\mathcal{X})$, $\Sigma_{\mathcal{Y}_s} : \mathcal{U} \to \mathcal{P}(\mathcal{Y})$ and $\Sigma_{\mathcal{X}\mathcal{Y}_s} : \mathcal{U} \to \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ that satisfy:

$$\begin{aligned}
\Sigma_{\mathcal{X}_{\ell}}(x|u) &= \frac{p_{\ell}(x)V(u|x)}{\sum_{x \in \mathcal{X}} p_{\ell}(x)V(u|x)}, \\
\Sigma_{\mathcal{Y}_s}(y|u) &= \frac{\sum_{x \in \mathcal{X}} V(u|x)Q_s(x,y)}{\sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} V(u|x)Q_s(x,y)}, \\
\Sigma_{\mathcal{X}\mathcal{Y}_s}(x,y|u) &= \frac{V(u|x)Q_s(x,y)}{\sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} V(u|x)Q_s(x,y)},
\end{aligned}$$

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

Appendix A.1.3. Encoding Sets

For every $(k,m,\ell) \in \mathcal{K} \times \mathcal{M} \times \mathcal{L}$, we define the encoding sets $\mathcal{E}_{k,m,\ell}(\tilde{U}) \subset \mathcal{X}^n$ as follows:

$$\mathcal{E}_{k,m,\ell}(\tilde{U}) = \mathcal{T}^n_{\Sigma_{\mathcal{X}_{\ell}},\delta'}(U^n_{k,m}),$$

with $\delta' > \frac{\delta}{|\mathcal{U}|}$.

Remark 15. *Note that, by the definition of δ' and Lemma 2.10 in [27], if $U^n_{k,m} \in \mathcal{T}^n_{p_u,\delta'''}$ with $\delta''' = \frac{\delta}{|\mathcal{U}|} - \delta'$ and $x^n \in \mathcal{T}^n_{\Sigma_{\mathcal{X}_{\ell}},\delta'}(U^n_{k,m})$, then $x^n \in \mathcal{T}^n_{p_{\ell},\delta}$.*

Appendix A.1.4. Decoding Sets

For every $(k,m,\ell) \in \mathcal{K} \times \mathcal{M} \times \mathcal{L}$, we define the decoding sets $\mathcal{D}_k(m(\tilde{U}),\ell) \subset \mathcal{Y}^n$ as follows:

$$\begin{aligned}
\mathcal{D}'_k(m(\tilde{U}),\ell) &:= \bigcup_{s \in \mathcal{S}_{\ell}} \mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k,m}), \\
\mathcal{D}_k(m(\tilde{U}),\ell) &:= \mathcal{D}'_k(m(\tilde{U}),\ell) \cap \Big(\bigcup_{\substack{k' \neq k \\ k' \in \mathcal{K}}} \mathcal{D}'_{k'}(m(\tilde{U}),\ell) \Big)^c,
\end{aligned}$$

with $\delta'' > \frac{\delta}{|\mathcal{U}|}$.

Remark 16. *One could consider sending some bits of the sequences X^n through the public channel, such that the user at the authentication terminal can be able to estimate the actual source realization and so avoid the complicated decoding strategy. However, this approach would violate the strong secrecy condition.*

Appendix A.1.5. Encoder–Decoder Pair Sets

For every $(k,m) \in \mathcal{K} \times \mathcal{M}$, we define the encoder–decoder pair set $\mathcal{C}_{k,m,\ell}(\tilde{U}) \in \mathcal{X}^n \times \mathcal{Y}^n$ as follows:

$$\mathcal{C}_{k,m,\ell}(\tilde{U}) = (\mathcal{E}_{k,m,\ell}(\tilde{U}) \times \mathcal{D}_k(m(\tilde{U}),\ell)) \cap \big(\bigcup_{s \in \mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})\big),$$

with $\tilde{\delta} > 0$.

Appendix A.1.6. Error Analysis

For every $\ell \in \mathcal{L}$, assume that the marginal distribution was estimated correctly, i.e., $\hat{\ell} = \ell$. We analyze the probability of each error event separately. We denote the error at the enrollment terminal given the codebook $\tilde{U}$ as $\epsilon_{E,n}(\tilde{U})$. An error occurs at the enrollment terminal if, for every $(k,m,\ell) \in \mathcal{K} \times \mathcal{M} \times \mathcal{L}$, the observed sequence x^n does not belong to $\mathcal{E}_{k,m,\ell}(\tilde{U})$, i.e.,

$$\begin{aligned}
\epsilon_{E,n}(\tilde{U}) &= p^n_\ell \big(\big(\bigcup_{(k,m)\in\mathcal{K}\times\mathcal{M}} \mathcal{E}_{k,m,\ell}(\tilde{U})\big)^c\big) \\
&= p^n_\ell \big(\bigcap_{(k,m)\in\mathcal{K}\in\mathcal{M}} \mathcal{E}_{k,m,\ell}(\tilde{U})^c\big) \\
&= \prod_{(k,m)\in\mathcal{K}\in\mathcal{M}} \big[1 - p^n_\ell(\mathcal{E}_{k,m,\ell}(\tilde{U}))\big].
\end{aligned}$$

Averaging over all codebooks, from the independence of the random variables involved and from Lemma 2.13 in [27], we have

$$\begin{aligned}
\mathbb{E}_{\tilde{U}}(\epsilon_{E,n}(\tilde{U})) &= \prod_{(k,m)\in\mathcal{K}\in\mathcal{M}} \mathbb{E}_{U^n_{k,m}}\big[1 - p^n_\ell(\mathcal{T}^n_{\Sigma_{\mathcal{X}_\ell},\delta'}(U^n_{k,m}))\big] \\
&\leq \big[1 - (n+1)^{-|\mathcal{U}||\mathcal{X}|}(2^{-n(I(U_\ell;X_\ell)}2^{\psi(\delta',|\mathcal{U}||\mathcal{X}|)})\big]^{2^{n(R_K+R_M)}} \\
&\leq \exp\big(-(n+1)^{-|\mathcal{U}||\mathcal{X}|}\big) \exp\big(2^{n(R_K+R_M-I(U_\ell;X_\ell)-\psi(\delta',|\mathcal{U}||\mathcal{X}|))}\big). \qquad \text{(A2)}
\end{aligned}$$

The inequality (A2) follows from $(1-x)^r \leq \exp(-rx)$, which holds for every $x, r > 0$.
Letting $n \to \infty$ and choosing

$$R_K + R_M > I(U_\ell; X_\ell) + \psi(\delta', |\mathcal{U}||\mathcal{X}|), \qquad \text{(A3)}$$

the right-hand side of (A2) goes doubly exponentially fast to zero. An error at the authentication terminal occurs, when (k,m) was encoded at the enrollment terminal, but $k' \neq k$ was decoded at the authentication terminal. The set of joint observations describing this event is given by

$$\begin{aligned}
\mathcal{C}_{\mathcal{E}_{k,m,\ell}}(\tilde{U})^c &= \mathcal{C}_{k,m,\ell}(\tilde{U})^c \cap \big(\mathcal{E}_{k,m,\ell}(\tilde{U}) \times \mathcal{D}_k(m(\tilde{U}),\ell)^c\big) \\
&= \big(\mathcal{E}_{k,m,\ell}(\tilde{U}) \times \mathcal{D}_k(m(\tilde{U}),\ell)^c\big) \cup \big(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c\big).
\end{aligned}$$

We denote the error probability of this event given the codebook $\tilde{U}$ for each correlated source Q_t with $t \in \mathcal{S}_\ell$ as $\epsilon^t_{n,k}(\tilde{U})$.

$$\begin{aligned}
\epsilon^t_{n,k}(\tilde{U}) &= \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\mathcal{C}_{\mathcal{E}_{k,m,\ell}}(\tilde{U})^c|U^n_{k,m}) \\
&= \Sigma^n_{\mathcal{X}\mathcal{Y}_t}((\mathcal{E}_{k,m,\ell}(\tilde{U}) \times \mathcal{D}_k(m(\tilde{U}),\ell)^c) \cup (\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c)|U^n_{k,m}) \\
&\leq \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\mathcal{E}_{k,m,\ell}(\tilde{U}) \times \mathcal{D}_k(m(\tilde{U}),\ell)^c|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}) \\
&\leq \Sigma^n_{\mathcal{Y}_t}(\mathcal{D}_k(m(\tilde{U}),\ell)^c|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}) \\
&= \Sigma^n_{\mathcal{Y}_t}(\mathcal{D}'_k(m)^c \cup (\bigcup_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \mathcal{D}'_{k'}(m(\tilde{U}),\ell))|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}) \\
&\leq \Sigma^n_{\mathcal{Y}_t}(\mathcal{D}'_k(m)^c|U^n_{k,m}) + \Sigma^n_{\mathcal{Y}_t}(\bigcup_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \mathcal{D}'_{k'}(m(\tilde{U}),\ell)|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}) \\
&= \Sigma^n_{\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k,m})^c|U^n_{k,m}) + \Sigma^n_{\mathcal{Y}_t}(\bigcup_{s\in\mathcal{S}_\ell}\bigcup_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m})|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\bigcap_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}) \\
&\leq \Sigma^n_{\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_t},\delta}(U^n_{k,m})^c|U^n_{k,m}) + \sum_{s\in\mathcal{S}_\ell}\sum_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \Sigma^n_{\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m})|U^n_{k,m}) + \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_t},\tilde{\delta}}(U^n_{k,m})^c|U^n_{k,m}).
\end{aligned}$$

Averaging over all codebooks and applying Lemma 2.12 in [27], we have

$$\mathbb{E}_{\tilde{U}}(\epsilon^t_{n,k}(\tilde{U})) \leq \epsilon_{\delta''}(n,|\mathcal{U}||\mathcal{Y}|) + \epsilon_{\tilde{\delta}}(n,|\mathcal{U}||\mathcal{X}||\mathcal{Y}|) + \sum_{s\in\mathcal{S}_\ell}\sum_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \mathbb{E}_{U^n_{k',m}}\mathbb{E}_{U^n_{k,m}}\Sigma^n_{\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m})|U^n_{k,m}),$$

with $\epsilon_{\delta''}(n,|\mathcal{U}||\mathcal{Y}|) = (n+1)^{|\mathcal{U}||\mathcal{Y}|}2^{-nc\delta''^2}$ and $\epsilon_{\tilde{\delta}}(n,|\mathcal{U}||\mathcal{X}||\mathcal{Y}|) = (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}|}2^{-nc\tilde{\delta}^2}$.

For $k' \neq k$ and applying from Lemma 3.3 in [28], we can bound the second term of the last inequality by

$$\mathbb{E}_{U^n_{k,m}}\Sigma^n_{\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m})|U^n_{k,m}) \leq \frac{p^n_{Y,t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m}))}{p^n_u(\mathcal{T}^n_{p_u,\delta'''})},$$

with $\delta''' = \delta' - \frac{\delta}{|\mathcal{U}|}$, since $U^n_{k',m} \in \mathcal{T}^n_{p_u,\delta}$ with probability one. For any $t,s \in \mathcal{S}_\ell$, we have

$$\mathbb{E}_{U^n_{k,m}}\Sigma^n_{\mathcal{Y}_t}(\mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k',m})|U^n_{k,m}) \leq \frac{(n+1)^{|\mathcal{U}||\mathcal{Y}|}}{1-\epsilon_{\delta'''}(n,|\mathcal{U}|)}2^{-n(I(U_\ell;Y_s)-\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|))}.$$

For every $t,s \in \mathcal{S}_\ell$ and every $k \in \mathcal{K}$, we have

$$\begin{aligned}
\mathbb{E}_{\tilde{U}}(\epsilon^t_{n,k}(\tilde{U})|U^n_{k,m}) &\leq \epsilon_{\delta''}(n,|\mathcal{U}||\mathcal{Y}|) + \sum_{s\in\mathcal{S}_\ell}\sum_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \frac{(n+1)^{|\mathcal{U}||\mathcal{Y}|}}{1-\epsilon_{\delta'''}(n,|\mathcal{U}|)}2^{-n(I(U_\ell;Y_s)-\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|))} \\
&\quad + \epsilon_{\tilde{\delta}}(n,|\mathcal{U}||\mathcal{X}||\mathcal{Y}|) \\
&\leq \epsilon_{\delta''}(n,|\mathcal{U}||\mathcal{Y}|) + \frac{(n+1)^{|\mathcal{U}||\mathcal{Y}|}}{1-\epsilon_{\delta'''}(n,|\mathcal{U}|)}|\mathcal{S}_\ell|2^{-n(\min_{s\in\mathcal{S}_\ell} I(U_\ell;Y_s)-R_K-\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|))} \\
&\quad + \epsilon_{\tilde{\delta}}(n,|\mathcal{U}||\mathcal{X}||\mathcal{Y}|).
\end{aligned}$$

There is an $n(\delta'',\delta''',\tilde{\delta},|\mathcal{U}|,|\mathcal{X}|,|\mathcal{Y}|)$ such that for all $n > n(\delta,\delta''',\tilde{\delta},|\mathcal{U}|,|\mathcal{X}|,|\mathcal{Y}|)$ for which we have

$$\mathbb{E}_{\tilde{U}}(\epsilon^t_{n,k}(\tilde{U})|U^n_{k,m}) \leq |\mathcal{S}_\ell|2^{-n(\min_{s\in\mathcal{S}_\ell} I(U_\ell;Y_s)-R_K-\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|))} \tag{A4}$$

for all $k \in \mathcal{K}$. By choosing

$$R_K < I(U_\ell; Y_s) - \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) \tag{A5}$$

and letting $n \to \infty$, the right-hand side of (A4) tends to zero. Considering (A5) and (A3), the helper data rate is lower bounded by

$$R_M > I(U_\ell; X_\ell) - I(U_\ell; Y_s) + \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) + \psi(\delta', |\mathcal{U}|, |\mathcal{X}|). \tag{A6}$$

Appendix A.1.7. Key Distribution

Besides reliability, a privacy secrecy rate pair has to fulfill three other conditions. One of them is that the secret key distribution must be close to the uniform distribution. Here, we show that this is indeed satisfied using the proof of [13]. For completeness, we introduce a sketch of the proof shown in [13] for a sequential key distillation, which consists of two phases: reconciliation and privacy amplification. The reconciliation step is equivalent to the reliability proved above. The privacy amplification step consists on the construction of the key K from a common shared sequence $T = U^n$ using an extractor function $g\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^k$ with $d, k, N \in \mathbb{N}$ whose inputs are the shared sequence T and a sequence of d uniformly distributed bits U_d and gives as output a k nearly uniformly distributed sequence.

Lemma 1 ([7]). *Let $T \in \{0,1\}^n$ be the random variable that represents the common sequence shared by both terminals and let E be the random variable that represents the total knowledge about T available to the eavesdropper. Let e be a particular realization of E. If both terminals know the conditional min-entropy $H_\infty(T|E = e) \geq \gamma n$ for some $\gamma \in (0,1)$, then there exists an extractor*

$$g\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^k$$

with

$$d \leq n\delta(n) \quad \text{and} \quad k \geq n(\gamma - \delta(n)),$$

with $\lim_{n\to\infty} \delta(n) = 0$ and if U_d is a random variable with uniform distribution on $\{0,1\}^d$ and both terminals choose $K = g(T, U_d)$ as their secret key, then

$$H(K|U_d, E = e) \geq k - \delta(n).$$

Sequential key distillation protocol: For every source realization $s \in \mathcal{S}$, we have an $\ell = \ell(s) \in \mathcal{L}$ such that $Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}$. For every $\ell \in \mathcal{L}$, we perform the following protocol:

- Repeat $i \in \mathbb{N}$ times the reconciliation protocol creating i shared sequences $T_1, T_2, \ldots, T_i$ of length n.
- Perform the privacy amplification phase based on an extractor with output size k, i.e., $K = g(T_1, T_2, \ldots, T_i, U_d) = g(U_1^n, U_2^n, \ldots, U_i^n, U_d) = g(U^N, U_d)$ with $N = in$. U_d has to be transmitted through the public channel together with the public message M^i.
- The total information available to the eavesdropper is $E = (M^i, U_d, \Theta)$, with Θ being a binary random variable introduced for calculation purposes informing if $T^i \in \mathcal{T}^n_{p_T,\delta}$.

In [13], it was shown that

$$\begin{aligned} H_\infty(T^i|M^i_\ell = m^i, \hat{L} = \ell, \Theta = 1, U_d) \geq & NI(U_\ell; Y_s) - N\phi(\delta,'' |\mathcal{U}|, |\mathcal{Y}|)H(X_\ell|U_\ell) - 2i \\ & - i\phi(\delta,'' |\mathcal{U}|, |\mathcal{Y}|) - \delta_\epsilon(i) - N\delta(N) - \sqrt{(N)}, \end{aligned} \tag{A7}$$

with $\lim_{n\to\infty} \delta_\epsilon(n) = 0$ (see Lemma 1 in [13]). Using Lemma 1, we have

$$H(K_\ell|M^i_\ell = m^i, \hat{L} = \ell, \Theta = 1, U_d) \geq k - \delta(N),$$

which implies that

$$H(K_\ell|\hat{L}=\ell) \geq H(K_\ell|M_\ell^i,\Theta,U_d,\hat{L}=\ell) \geq k-\delta(N). \tag{A8}$$

Since this holds for every $\ell \in \mathcal{L}$, we have that

$$\begin{aligned}\log|\mathcal{K}| &\geq k\\ &\geq H(K_\ell)\\ &\geq H(K_\ell|\hat{L}).\end{aligned} \tag{A9}$$

Furthermore, we have

$$\begin{aligned}H(K_\ell|\hat{L}) &= \sum_{\tilde{\ell}\in\mathcal{L}} \Pr\{\hat{L}=\tilde{\ell}\}H(K_\ell|\hat{L}=\tilde{\ell})\\ &= \Pr\{\hat{L}=\ell\}H(K_\ell|L=\ell) + \sum_{\substack{\tilde{\ell}\neq\ell\\ \tilde{\ell}\in\mathcal{L}}} \Pr\{\hat{L}=\tilde{\ell}\}H(K_\ell|\hat{L}=\tilde{\ell})\\ &= \Pr\{\hat{L}=\ell\}H(K_\ell|\hat{L}=\ell) + \Pr\{\hat{L}\neq\ell\}H(K_\ell|\hat{L}\neq\ell)\\ &\leq \Pr\{\hat{L}=\ell\}H(K_\ell|\hat{L}=\ell) + \Pr\{\hat{L}\neq\ell\}\max_{\ell\in\mathcal{L}} H(K_\ell|\hat{L}\neq\ell)\\ &\leq \Pr\{\hat{L}=\ell\}H(K_\ell|\hat{L}=\ell) + \epsilon_\delta(n,|\mathcal{X}|)^i N\log|\mathcal{X}| \qquad \text{(A10)}\\ &\leq H(K_\ell|\hat{L}=\ell) + (n+1)^{|\mathcal{X}|i} N\log|\mathcal{X}|2^{-Nc\delta^2}\\ &= H(K_\ell|\hat{L}=\ell) + \epsilon_\delta(n,i,|\mathcal{X}|), \qquad \text{(A11)}\end{aligned}$$

where $\lim_{i,n\to\infty}\epsilon_\delta(n,i,|\mathcal{X}|)=0$ and (A10) follows from (A1). We then have that

$$\left|H(K_\ell|\hat{L}) - H(K_\ell|\hat{L}=\ell)\right| \leq \epsilon_\delta(n,i,|\mathcal{X}|), \tag{A12}$$

showing that $H(K_\ell|\hat{L})$ approaches $H(K_\ell|\hat{L}=\ell)$ for increasing n or i or both at the same time.

Combining (A8), (A9) and (A12), we get

$$\begin{aligned}\log|\mathcal{K}| &\geq H(K_\ell|\hat{L}=\ell) - \epsilon_\delta(n,i,|\mathcal{X}|)\\ &\geq k-\delta(N)-\epsilon_\delta(n,i,|\mathcal{X}|)\\ &= \log|\mathcal{K}| - \delta(N) - \epsilon_\delta(n,i,|\mathcal{X}|).\end{aligned} \tag{A13}$$

Appendix A.1.8. Privacy Leakage

Another condition that has to be fulfilled by an achievable privacy secrecy rate pair is that the information rate provided by the helper data about the sequence X^n is bounded. We show here that this condition is fulfilled.

For every source realization $s \in \mathcal{S}$, we have an $\ell = \ell(s) \in \mathcal{L}$ such that $Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}$. For every $\ell \in \mathcal{L}$, we have

$$\begin{aligned}\frac{1}{N}I(X_\ell^N; M_\ell^i,\Theta,U_d,\hat{L}) &= \frac{1}{N}I(X_\ell^N;\hat{L}) + \frac{1}{N}I(X_\ell^N; M_\ell^i,\Theta,U_d|\hat{L})\\ &\leq \frac{\log|\mathcal{L}|}{N} + \frac{1}{N}I(X_\ell^N; M_\ell^i,\Theta,U_d|\hat{L}).\end{aligned} \tag{A14}$$

We analyze the second term of the right-hand side of (A14):

$$\frac{1}{N}I(X_\ell^N; M_\ell^i,\Theta,U_d|\hat{L}) \leq \Pr\{\hat{L}=\ell\}\frac{1}{N}I(X_\ell^N; M_\ell^i,\Theta,U_d|\hat{L}=\ell) + \Pr\{\hat{L}\neq\ell\}\log|\mathcal{X}|.$$

Similar to (A11), we have

$$\frac{1}{N} I(X_\ell^N; M_\ell^i, \Theta, U_d | \hat{L}) \leq \frac{1}{N} I(X_\ell^N; M_\ell^i, \Theta, U_d | \hat{L} = \ell) + \epsilon_\delta(n, |\mathcal{X}|)^i \log |\mathcal{X}|. \tag{A15}$$

For every $\ell \in \mathcal{L}$ and from (A6), it holds

$$\begin{aligned} \frac{1}{N} I(X_\ell^N; M_\ell^i, \Theta, U_d | \hat{L} = \ell) &\leq \frac{i \log |\mathcal{M}|}{N} + \frac{d+1}{N} \\ &\leq I(U_\ell; X_\ell | \hat{L} = \ell) - I(U_\ell; Y_s) + \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) + \psi(\delta', |\mathcal{U}|, |\mathcal{X}|) \quad \text{(A16)} \\ &\quad + \frac{d+1}{N}, \quad \text{(A17)} \end{aligned}$$

with $\phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) > 0$ and $\psi(\delta', |\mathcal{U}|, |\mathcal{X}|) > 0$. Combining (A14), (A15) and (A17), it follows that

$$\begin{aligned} \frac{1}{N} I(X_\ell^N; M_\ell^i, \Theta, U_d, \hat{L}) \leq I(U_\ell; X_\ell | \hat{L} = \ell) - I(U_\ell; Y_s) + \frac{\log |\mathcal{L}|}{N} + \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) \\ + \psi(\delta', |\mathcal{U}|, |\mathcal{X}|) + \epsilon_\delta(n, |\mathcal{X}|)^i \log |\mathcal{X}|, \end{aligned}$$

where the last three terms of the right-hand side of the inequality goes to zero for large enough n and i.

Appendix A.1.9. Secrecy Leakage

The last condition that has to be fulfilled by an achievable privacy secrecy rate pair is that the information rate provided by the helper data about the secret key is negligibly small. For every source realization $s \in \mathcal{S}$, we have an $\ell = \ell(s) \in \mathcal{L}$ such that $Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}$. For every $\ell \in \mathcal{L}$, we have

$$I(K_\ell; M_\ell^i, \Theta, U_d, \hat{L}) = I(K_\ell; \hat{L}) + I(K_\ell; M_\ell^i, \Theta, U_d, | \hat{L}). \tag{A18}$$

We first consider the first term of (A18). Using (A8) and (A12), we get that

$$I(K_\ell; \hat{L}) = H(K_\ell) - H(K_\ell | \hat{L}) \leq \delta(N) + \epsilon_\delta(n, i, |\mathcal{X}|).$$

We consider the second term of (A18). Using (A13), we get

$$\begin{aligned} I(K_\ell; M_\ell^i, \Theta, U_d | \hat{L}) &\leq \Pr\{\hat{L} = \ell\} I(K_\ell; M_\ell^i, \Theta, U_d | \hat{L} = \ell) + \Pr\{\hat{L} \neq \ell\} N \log |\mathcal{X}| \\ &\leq H(K_\ell | \hat{L} = \ell) - H(K_\ell | M_\ell^i, \Theta, U_d, \hat{L} = \ell) + \epsilon(n, |\mathcal{X}|)^i N \log |\mathcal{X}| 2^{-Nc\delta^2} \\ &\leq \log |\mathcal{K}| - \log |\mathcal{K}| + \delta(N) + \epsilon_\delta(n, i, |\mathcal{X}|) \\ &= \delta(N) + \epsilon_\delta(n, i, |\mathcal{X}|). \end{aligned} \tag{A19}$$

Hence,

$$I(K_\ell; M_\ell^i, \Theta, U_d, \hat{L}) \leq 2\delta(N) + 2\epsilon_\delta(n, i, |\mathcal{X}|). \tag{A20}$$

Note that the right-hand side of the inequality goes to zero for large enough N, showing that for every source realization $s \in \mathcal{S}$, the secret key information rate leaked by the helper is negligibly small.

Note that we showed that the rate pair can be achieved for large $N = in$, i.e., not for all $N \in \mathbb{N}$. To show the achievability for all blocklengths $N \in \mathbb{N}$, we define the sequence N_i with $i \in \mathbb{N}$ with $N_i = i^2$. We showed that for the sequence N_i of blocklengths with $i \in \mathbb{N}$, there exists a blocklength N_{i_0} such that for all blocklengths $N_i > N_{i_0}$, we can find a code sequence that fulfills the achievability conditions. For every $N_i < N < N_{i+1}$, one can rewrite $N = N_i + r_i$ with $r_i < N_{i+1} - N_i$. We use only the first N_i symbols to generate the key and discard the rest r_i. One can easily see that there is a $\epsilon(N)$ such that, for $\delta = \epsilon(N)$, all conditions are fulfilled. This completes the proof of achievability.

Appendix A.2. Converse of Theorem 3

For the converse, we consider a genie-aided enrollment and authentication terminal, i.e., the user at the enrollment and authentication terminal has partial knowledge of the source, i.e., he knows the actual state of the marginal distribution $\ell \in \mathcal{L}$ but not the complete source state. The converse follows from the corresponding result for a joint-source with perfect SSI shown in [11]. For a fixed $\ell \in \mathcal{L}$, $s \in \mathcal{S}_\ell$ and $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, we define the region $\mathcal{R}(V, \ell, s)$ as the set of all $(R_{PL}, R_K) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_K &\leq I(U_\ell; Y_s), \\ R_{PL} &\geq I(U_\ell; X_\ell | L = \ell) - I(U_\ell; Y_s). \end{aligned}$$

We start analyzing the secret key rate. For a fixed $\ell \in \mathcal{L}$ and $s \in \mathcal{S}_\ell$, we have

$$\begin{aligned} H(K_\ell) &= H(K_\ell | L = \ell) \\ &= I(K_\ell; M_\ell Y_s^n | L = \ell) + H(K_\ell | M_\ell Y_s^n \hat{K}, L = \ell), \end{aligned}$$

where $\hat{K}$ is a deterministic function of M, Y^n and $L = \ell$, i.e., $\hat{K} = f(M, Y^n, L = \ell)$,

$$\begin{aligned} H(K_\ell) &\leq I(K_\ell; M_\ell Y_s^n | L = \ell) + H(K_\ell | \hat{K}) \\ &\leq I(K_\ell; M_\ell Y_s^n | L = \ell) + \epsilon_n \qquad \text{(A21)} \\ &= I(K_\ell; M_\ell | L = \ell) + I(K_\ell M_\ell; Y_s^n | L = \ell) + \epsilon_n \\ &= I(K_\ell; M_\ell | L = \ell) + \sum_{i=1}^n I(K_\ell M_\ell; Y_{s,i} | Y_s^{i-1} L = \ell) + \epsilon_n \\ &= I(K_\ell; M_\ell | L = \ell) + \sum_{i=1}^n I(K_\ell M_\ell Y_s^{i-1}; Y_{s,i} | L = \ell) + \epsilon_n \\ &\leq I(K_\ell; M_\ell | L = \ell) + \sum_{i=1}^n I(K_\ell M_\ell X_\ell^{i-1}; Y_{s,i} | L = \ell) + \epsilon_n \qquad \text{(A22)} \\ &= I(K_\ell; M_\ell | L = \ell) + n I(U_\ell; Y_s | L = \ell) + \epsilon_n, \qquad \text{(A23)} \end{aligned}$$

where (A21) holds for $\epsilon_n = 1 + \Pr\{\hat{K} \neq K\} \log K_n$ and follows from Fano's Inequality and (A22) from $Y^{i-1} - KMX^{i-1} - Y_i$ forming a Markov chain. This comes from

$$\begin{aligned} P_{KMY^{i-1}X^{i-1}Y_i}(k, m, y^{i-1}, x^{i-1}, y_i) &= \sum_{x_{i+1}^n} \sum_{x_i} p_\ell(x^{i-1}) p_\ell(x_i) p_\ell(x_{i-1}^n) P_{KM}(k, m | x^n) W_s(y_i, x_i) W_s(y^{i-1} | x^{i-1}) \\ &= P_{X^{i-1}KMY_i}(x^{i-1}, k, m, y_i) W_s(y^{i-1} | x^{i-1}) \\ &= p_\ell(x^{i-1}) \Pr(k, m, y_i | x^{i-1}) W_s(y^{i-1} | x^{i-1}). \end{aligned}$$

We define $U_{\ell,i} = (K_\ell M_\ell X_\ell^{i-1})$. The Equality (A23) is obtained using a time-sharing variable T uniformly distributed over $\{1, \ldots, n\}$ and independent of all other variables. Setting $U = (U_{\ell,i})$, $X = X_{\ell,i}$ and $Y = Y_{\ell,i}$ for $T = i$, we obtain

$$\begin{aligned} \sum_{i=1}^n I(K_\ell M_\ell X_\ell^{i-1}; Y_{s,i} | L = \ell) &= \sum_{i=1}^n I(U_{\ell,i}; Y_{s,i} | L = \ell) \\ &= n I(U_{\ell,T}; Y_{s,T} | T, L = \ell) \\ &= n I((U_{\ell,T}, T); Y_{s,T} | L = \ell) \\ &= n I(U_\ell; Y_s | L = \ell). \end{aligned}$$

Dividing by n, we get

$$\begin{aligned}\frac{1}{n}H(K_\ell) &\leq \frac{1}{n}I(K_\ell;M_\ell|L=\ell)+I(U_\ell;Y_s,L=\ell)+\frac{1}{n}\epsilon\\ &\leq I(U_\ell;Y_s,L=\ell)+\lambda_{n,\ell}+\frac{1}{n}+\frac{1+\epsilon}{n},\end{aligned}$$

where the last inequality holds with $\lambda_{n,\ell}\to 0$ for $n\to\infty$ (see [11]).

Assuming the rate pair (R_{PL},R_K) is achievable, we have that $\epsilon\leq 1+\delta\log K_n$ and obtain

$$R_K-\delta\leq I(U_\ell;Y_s,L=\ell)+\lambda_{n,\ell}+\frac{1}{n}+\frac{1+\delta\log K_n}{n}. \tag{A24}$$

We continue with the privacy leakage. For a fixed $s\in\mathcal{S}_\ell$ we have

$$\begin{aligned}I(X_\ell^n;M_\ell) &= I(X_\ell^n;M_\ell|L=\ell)\\ &= H(M_\ell|L=\ell)-H(M_\ell|X_\ell^n,L=\ell)\\ &\geq H(M_\ell|Y_s^n,L=\ell)-H(K_\ell M_\ell|X_\ell^n,L=\ell)\\ &= H(K_\ell M_\ell|Y_s^n,L=\ell)-H(K|MY^n\hat{K})-H(K_\ell M_\ell|X_\ell^n,L=\ell)\\ &\geq H(K_\ell M_\ell|Y_s^n,L=\ell)-H(K|\hat{K})-H(K_\ell M_\ell|X_\ell^n,L=\ell)\\ &\geq H(K_\ell M_\ell|Y_s^n,L=\ell)-\epsilon_n-H(K_\ell M_\ell|X_\ell^n,L=\ell)\\ &= I(K_\ell M_\ell;X_\ell^n|L=\ell)-I(K_\ell M_\ell;Y_s^n|L=\ell)-\epsilon)_n\\ &= \sum_{i=1}^n I(K_\ell M_\ell;X_{\ell,i}|X_\ell^{i-1},L=\ell)-\sum_{i=1}^n I(K_\ell M_\ell;Y_{s,i}|Y_\ell^{i-1},L=\ell)-\epsilon_n\\ &= \sum_{i=1}^n I(K_\ell M_\ell X_\ell^{i-1};X_{\ell,i},L=\ell)-\sum_{i=1}^n I(K_\ell M_\ell Y_s^{i-1};Y_{s,i},L=\ell)-\epsilon_n\\ &\geq \sum_{i=1}^n I(K_\ell M_\ell X_\ell^{i-1};X_{\ell,i},L=\ell)-\sum_{i=1}^n I(K_\ell M_\ell X_\ell^{i-1};Y_{s,i},L=\ell)-\epsilon_n\\ &= nI(U_\ell;X_\ell|L=\ell)-nI(U_\ell;Y_s|L=\ell)-\epsilon_n.\end{aligned}$$

Dividing by n, we get

$$\frac{1}{n}I(X_\ell^n;M_\ell)\geq I(U_\ell;X_\ell|L=\ell)-I(U_\ell;Y_s|L=\ell)+\frac{1}{n}\epsilon_n.$$

Assuming (R_{PL},R_K) is achievable, we have that $\epsilon\leq 1+\delta\log K_n$ and obtain

$$R_{PL}+\delta\geq I(U_\ell;X_\ell|L=\ell)-I(U_\ell;Y_s|L=\ell)+\frac{1+\delta\log K_n}{n}. \tag{A25}$$

We have shown that $\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}})\subseteq\bigcap_{\ell\in\mathcal{L}}\mathcal{C}_\ell$. This means that if $(R_{PL},R_K)\in\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}})$ holds, then we have that $(R_{PL},R_K)\in\bigcap_{\ell\in\mathcal{L}}\mathcal{C}_\ell$. Equivalently, if $(R_{PL},R_K)\notin\bigcap_{\ell\in\mathcal{L}}\mathcal{C}_\ell$, then $(R_{PL},R_K)\notin\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}})$. Assume $(R_{PL}^*,R_K^*)\notin\bigcap_{\ell\in\mathcal{L}}\mathcal{C}_\ell$. This implies that there exists a $\ell\in\mathcal{L}$ such that, for all auxiliary channels V, we have that $(R_{PL}^*,R_K^*)\notin\mathcal{R}(V,\ell)$, which implies that $(R_{PL}^*,R_K^*)\notin\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{XY}})$. This completes the converse and therewith proves the desired result.

It remains to derive the bound on the cardinality of the auxiliary random variables U. Let $\ell\in\mathcal{L}$ be arbitrarily but fixed and U be a random variable fulfilling $P_{UXY,s}(u,x,y)=V(u|x)Q_s(x,y)$ for all $s\in\mathcal{S}(\ell)$. We show that there is a random variable $\bar{U}$ with range $|\bar{\mathcal{U}}|=|\mathcal{X}|+|\mathcal{S}_\ell|$

$$\begin{aligned}I(\bar{U};Y)&=I(U;Y),\\ I(\bar{U};X)-I(\bar{U};Y)&=I(U;X)-I(U;Y),\end{aligned} \tag{A26}$$

for all $s \in \mathcal{S}_\ell$. We consider the following $|\mathcal{X}| + |\mathcal{S}_\ell|$ real valued continuous functions on $\mathcal{P}(\mathcal{X})$

$$\begin{aligned} f_x(p) &= p(x), \quad \text{for all } x \in \mathcal{X} \text{ but one,} \\ g_s(P) &= H(pW_s), \\ h(P) &= H(p), \end{aligned}$$

for all $s \in \mathcal{S}_\ell$. We have that $\Sigma_{\mathcal{X}_\ell}(\cdot|u) \in \mathcal{P}(\mathcal{X})$ having μ-measure p_u. Then, it holds that

$$\begin{aligned} \sum_u p_u(u) f_x(\Sigma_{\mathcal{X}_\ell}(\cdot|u)) &= p(x), \\ \sum_u p_u(u) g_s(\Sigma_{\mathcal{X}_\ell}(\cdot|u)) &= H(Y|U), \\ \sum_u p_u(u) h(\Sigma_{\mathcal{X}_\ell}(\cdot|u)) &= H(X|U), \end{aligned}$$

for all $s \in \mathcal{S}_\ell$. According to (Lemma 15.4, [27]), there exists a random variable $\bar{U}$ fulfilling the Markov condition with values in $\bar{\mathcal{U}} = \{1, \cdots, |\mathcal{X}| + |\mathcal{S}_\ell|\}$ and (A26) holds (see also Lemma 15.5 in [27]). □

Appendix B. Proof of Theorem 4

Appendix B.1. Achievability of Theorem 4

The achievability proof of Theorem 4 is very similar to the achievability proof of Theorem 3, where first the index of marginal distribution ℓ over $\mathcal{X}$ is estimated. The difference is that, in this model, we use a generated secret key $K_{\ell,g}$ in a one-pad system to conceal the uniformly distributed chosen key K over the set $\mathcal{K}$; as in [11], it is additionally sent together with the generated helper message $M_{\ell,g}$ and the index of the estimated marginal distribution $\hat{L}$ over the public message, i.e., the helper data is $M' = (M_{\ell,g}, K \oplus K_{\ell,g}, \hat{L})$. The error analysis is similar to the error analysis for Theorem 3 and the key is already uniformly distributed; however, we should take a deeper look into the privacy leakage and the secrecy leakage. We perform the privacy amplification step as in Appendix A to show that the strong secrecy is fulfilled.

Appendix B.1.1. Privacy Leakage

Another condition that has to be fulfilled by an achievable privacy secrecy rate pair is that the information rate provided by the helper data about the sequence X^n is bounded. We show here that this condition is fulfilled.

For every source realization $s \in \mathcal{S}$, we have an $\ell = \ell(s)$ such that $Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}$. We have

$$\frac{1}{N} I(X^N; M^i_{\ell,g}, K \oplus K_{\ell,g}, \Theta, U_d, \hat{L}) \leq \frac{\log|\mathcal{L}|}{N} + \frac{1}{N} I(X^N; M^i_{\ell,g}, K \oplus K_{\ell,g}, \Theta, U_d|\hat{L}). \tag{A27}$$

We analyze the second term of the right-hand side of (A27)

$$\begin{aligned} &\frac{1}{N} I(X^N; M^i_{\ell,g}, K \oplus K_{\ell,g}, \Theta, U_d|\hat{L}) \\ &\quad \leq \Pr\{\hat{L} = \ell\} \frac{1}{N} I(X^N; M^i_{\ell,g}, K \oplus K_{\ell,g}, \Theta, U_d|\hat{L} = \ell) + \Pr\{\hat{L} \neq \ell\} \frac{N \log|\mathcal{X}|}{N} \\ &\quad \leq \Pr\{\hat{L} = \ell\} \times \frac{1}{N} I(X^N; M^i_{\ell,g}, K \oplus K_{\ell,g}, \Theta, U_d|\hat{L} = \ell) + \epsilon_\delta(n, i, |\mathcal{X}|) \log|\mathcal{X}|. \end{aligned}$$

Similar to (A11), we have

$$\begin{aligned}&\frac{1}{N}I(X^N;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L})\\&\leq\frac{1}{N}I(X^N;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}=\ell)+\epsilon_\delta(n,i,|\mathcal{X}|)\log|\mathcal{X}|.\end{aligned}\tag{A28}$$

In [11], the authors show that, for every $\ell\in\mathcal{L}$, it holds

$$\begin{aligned}&\frac{1}{N}I(X^N;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}=\ell)\\&\leq\frac{1}{N}I(X^N;M^i_{\ell,g},\Theta,U_d|\hat{L}=\ell\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})+\frac{1}{N}H(K\oplus K_{\ell,g}|\hat{L}=\ell\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})\\&\quad-\frac{1}{N}H(K\oplus K_{\ell,g}|X^n,M^i_{\ell,g},\Theta,U_d,K_{\ell,g},\hat{L}=\ell)\\&\leq\frac{1}{N}I(X^N;M^i_{\ell,g},\Theta,U_d|\hat{L}=\ell\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})+\frac{1}{N}\log K_N-\frac{1}{N}\log K_N\\&\leq\frac{1}{N}I(X^n;M^i_{\ell,g},\Theta,U_d|\hat{L}=\ell\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})\\&\leq I(U;X|\hat{L}=\ell\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})-I(U;Y\|Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})+\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|)+\psi(\delta',|\mathcal{U}|,|\mathcal{X}|)\\&\quad+\frac{d+1}{N},\end{aligned}\tag{A29}$$

which proves the bound on the privacy leakage.

Appendix B.1.2. Secrecy Leakage

For every source realization $s\in\mathcal{S}$, we have an $\ell=\ell(s)$ such that $Q_s\in\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}$. Following similar steps as for the privacy leakage, it can be shown that the secrecy leakage is upper-bounded by

$$I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d,\hat{L})=I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}).\tag{A30}$$

We analyze the right-hand side of (A30):

$$\begin{aligned}&I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L})=\sum_{\tilde{\ell}\in\mathcal{L}}\Pr\{\hat{L}=\tilde{\ell}\}I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}=\tilde{\ell})\\&=\Pr\{\hat{L}=\ell\}I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}=\ell)+\Pr\{\hat{L}\neq\ell\}I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}\neq\ell).\end{aligned}$$

For every $\ell\in\mathcal{L}$, it holds

$$\begin{aligned}I(K;M^i_{\ell,g},K\oplus K_{\ell,g},\Theta,U_d|\hat{L}=\ell)&\leq\log|\mathcal{K}|-H(K_{\ell,g}|\hat{L}=\ell)+I(K_{\ell,g};M^i_{\ell,g},\Theta,U_d|\hat{L}=\ell)\\&\leq\log|\mathcal{K}|-\log|\mathcal{K}|+I(K_{\ell,g};M^i_{\ell,g},\Theta,U_d|\hat{L}=\ell).\end{aligned}\tag{A31}$$

The last inequality follows from (A13). Substituting $K_{\ell,g}$ with K, combining (A31) with (A19) and letting $i,n\to\infty$, we obtain the desired result.

Appendix B.2. Converse of Theorem 4

The converse of Theorem 4 can be shown using the same lines of arguments as for the converse of Theorem 3. □

Appendix C. Proof Lemma 1

For every channel $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, for every $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$, we have the following effective sources:

$$\begin{aligned} P_{UXY,s_1}(u,x,y) &= V(u|x)Q_{s_1}(x,y), \\ P_{UXY,s_2}(u,x,y) &= V(u|x)Q_{s_2}(x,y). \end{aligned}$$

Let $d_H(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}_1}, \mathfrak{Q}_{\mathcal{X}\mathcal{Y}_2}) \leq \epsilon$ then there exists a $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$ such that $(\bar{V}, \bar{s_1}, \bar{s_2}) = \text{argmax}\, d_H(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}_1}, \mathfrak{Q}_{\mathcal{X}\mathcal{Y}_2})$. Then, we have that

$$\begin{aligned} \|P_{UXY,\bar{s_1}} - P_{UXY,\bar{s_2}}\|_{TV} &= \sum_{u\in\mathcal{U}} \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} |P_{UXY,\bar{s_1}}(u,x,y) - P_{UXY,\bar{s_2}}(u,x,y)| \\ &= \sum_{u\in\mathcal{U}} \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} |V(u|x)Q_{\bar{s_1}}(x,y) - V(u|x)Q_{\bar{s_2}}(x,y)| \\ &= \sum_{u\in\mathcal{U}} \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} |V(u|x)(Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y))| \\ &= \sum_{u\in\mathcal{U}} \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} V(u|x)|Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y)| \\ &= \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} \big(|Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y)| \sum_{u\in\mathcal{U}} V(u|x)\big) \\ &= \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} |Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y)| \\ &\leq \epsilon, \end{aligned} \tag{A32}$$

and

$$\begin{aligned} \|P_{U,\bar{s_1}} - P_{U,\bar{s_2}}\|_{TV} &= \sum_{u\in\mathcal{U}} |\sum_{x,y\in\mathcal{X}\times\mathcal{Y}} P_{UXY,\bar{s_1}}(u,x,y) - P_{UXY,\bar{s_2}}(u,x,y)| \\ &= \sum_{u\in\mathcal{U}} |\sum_{x,y\in\mathcal{X}\times\mathcal{Y}} V(u|x)(Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y))| \\ &\leq \sum_{u\in\mathcal{U}} \sum_{x,y\in\mathcal{X}\times\mathcal{Y}} V(u|x)|(Q_{\bar{s_1}}(x,y) - Q_{\bar{s_2}}(x,y))| \\ &\leq \epsilon. \end{aligned} \tag{A33}$$

For every channel $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, for every $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$, there is an $\ell_1 = \ell_1(s_1)$ and $\ell_2 = \ell_2(s_2)$ the region $\mathcal{R}(V, \ell_i, s_i)$ with $i = \{1, 2\}$ is rectangular. Therefore, to calculate the Hausdorff distance between regions, we are only interested in the corner points:

$$\begin{aligned} R_{K,s_i} &= I(U_{\ell_i}; Y_{s_i}), \\ R_{PL,s_i} &= I(U_{\ell_i}; X_{\ell_i}) - I(U_{\ell_i}; Y_{s_i}). \end{aligned}$$

Let V be arbitrary but fixed. Then, for every $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$, we have

$$\begin{aligned} |I(U_{\ell_1}; Y_{s_1} - I(U_{\ell_2}; Y_{s_2})| &= |H(U_{\ell_1}) - H(U_{\ell_2}) + H(Y_{s_2}|U_{\ell_2}) - H(Y_{s_2}|U_{\ell_1})| \\ &\leq |H(U_{\ell_1}) - H(U_{\ell_2})| + |H(Y_{s_2}|U_{\ell_2}) - H(Y_{s_2}|U_{\ell_1})|. \end{aligned}$$

For $\bar{V}$, $\bar{s_1}$ and $\bar{s_2}$, there is a $\bar{\ell_1} = \bar{\ell_1}(\bar{s_1})$ and $\bar{\ell_2} = \bar{\ell_2}(\bar{s_2})$. Using [27] Lemma 2.12 and Using Lemma 1 in [22], we get

$$|I(U_{\bar{\ell_1}}; Y_{\bar{s_1}} - I(U_{\bar{\ell_2}}; Y_{\bar{s_2}})| \leq 2\epsilon \log |\mathcal{Y}| + 2H_2(\epsilon) - \epsilon \log \frac{\epsilon}{|\mathcal{U}|}. \tag{A34}$$

Following the same line of arguments as for (A34), we get

$$|I(U_{\bar{\ell_1}}; X_{\bar{\ell_1}} - I(U_{\bar{\ell_2}}; X_{\bar{\ell_2}})| \leq 2\epsilon \log |\mathcal{X}| + 2H_2(\epsilon) - \epsilon \log \frac{\epsilon}{|\mathcal{U}|}. \tag{A35}$$

Hence, for every channel $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, $\bar{s_1}$ and $\bar{s_2}$, we have

$$D_H(\mathcal{R}(V, \bar{\ell_1}, \bar{s_1}), \mathcal{R}(V, \bar{\ell_2}, \bar{s_2})) \leq \delta(\epsilon), \tag{A36}$$

with $\delta(\epsilon) = \sqrt{\delta_1(\epsilon)^2 + \delta_2(\epsilon)^2}$, where $\delta_1(\epsilon) = 2\epsilon \log |\mathcal{Y}| + 2H_2(\epsilon) - \epsilon \log \frac{\epsilon}{|\mathcal{U}|}$ and $\delta_2(\epsilon) = 2\epsilon \log |\mathcal{Y}||\mathcal{X}| + 4H_2(\epsilon) - 2\epsilon \log \frac{\epsilon}{|\mathcal{U}|}$.

For fixed ℓ_1 and ℓ_2, we denote

$$\begin{aligned}
\mathcal{R}(V, \ell_1) &= \bigcap_{s_i \in \mathcal{S}_1} \mathcal{R}(V, \ell_1, s_1), \\
\mathcal{R}(V, \ell_2) &= \bigcap_{s_i \in \mathcal{S}_2} \mathcal{R}(V, \ell_2, s_2), \\
\mathcal{R}(\ell_1) &= \bigcup_{\substack{V:\mathcal{X}\to\mathcal{P}(\mathcal{U}) \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_{\ell_1}}} \mathcal{R}(V, \ell_1), \\
\mathcal{R}(\ell_2) &= \bigcup_{\substack{V:\mathcal{X}\to\mathcal{P}(\mathcal{U}), \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_{\ell_2}}} \mathcal{R}(V, \ell_2).
\end{aligned}$$

We have

$$\begin{aligned}
D_H(\mathcal{R}(V, \ell_1), \mathcal{R}(V, \ell_2)) &= D_H\Big(\bigcap_{s_1 \in \mathcal{S}_1} \mathcal{R}(V, \ell_1, s_1), \bigcap_{s_2 \in \mathcal{S}_2} \mathcal{R}(V, \ell_2, s_2)\Big) \\
&= D_H\Big(\bigcup_{s_1 \in \mathcal{S}_1} \mathcal{R}(V, \ell_1, s_1)^c, \bigcup_{s_2 \in \mathcal{S}_2} \mathcal{R}(V, \ell_2, s_2)^c\Big) \qquad \text{(A37)} \\
&\leq D_H(\mathcal{R}(\bar{V}, \bar{\ell_1}, \bar{s_1})^c, \mathcal{R}(\bar{V}, \bar{\ell_2}, \bar{s_2})^c) \qquad \text{(A38)} \\
&\leq \delta(\epsilon).
\end{aligned}$$

Equation (A37) holds since the Hausdorff distance between two sets equals the Hausdorf distance between the complements of each set. Inequation (A38) holds since $\bar{V}, \bar{s_1}, \bar{s_2}$ is the index of the sets that maximises the Hausdorf distance. It also holds that

$$\begin{aligned}
D_H(\mathcal{R}(\ell_1), \mathcal{R}(\ell_2)) &= D_H\Big(\bigcup_{\substack{V:\mathcal{X}\to\mathcal{P}(\mathcal{U}) \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_{\ell_1}}} \mathcal{R}(V, \ell_1), \bigcup_{\substack{V:\mathcal{X}\to\mathcal{P}(\mathcal{U}) \\ |\mathcal{U}| \leq |\mathcal{X}| + |\mathcal{S}_{\ell_2}}} \mathcal{R}(V, \ell_2)\Big) \\
&\leq D_H(\mathcal{R}(\bar{V}, \bar{\ell_1}, \bar{s_1})^c, \mathcal{R}(\bar{V}, \bar{\ell_2}, \bar{s_2})^c) \\
&\leq \delta(\epsilon),
\end{aligned}$$

and

$$\begin{aligned} D_H(\mathfrak{C}_G(\mathfrak{Q}_{\mathcal{X}\mathcal{Y},1}), \mathfrak{C}_G(\mathfrak{Q}_{\mathcal{X}\mathcal{Y},2})) &= D_H\Big(\bigcap_{\ell_1\in\mathcal{L}_1} \mathcal{R}(\ell_1), \bigcap_{\ell_2\in\mathcal{L}_2} \mathcal{R}(\ell_2)\Big) \\ &= D_H\Big(\bigcup_{\ell_1\in\mathcal{L}_1} \mathcal{R}(\ell_1)^c, \bigcup_{\ell_2\in\mathcal{L}_2} \mathcal{R}(\ell_2)^c\Big) \\ &\leq D_H\big(\mathcal{R}(\bar{V}, \bar{\ell_1}, \bar{s_1})^c, \mathcal{R}(\bar{V}, \bar{\ell_2}, \bar{s_2})^c\big) \\ &\leq \delta(\epsilon). \end{aligned}$$

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
2. Liang, Y.; Poor, H.V.; Shamai, S. Information theoretic security. *Found. Trends Commun. Inf. Theor.* **2009**, *5*, 355–580.
3. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011.
4. Schaefer, R.F.; Boche, H.; Khisti, A.; Poor, H.V. *Information Theoretic Security and Privacy of Information Systems*; Cambridge University Press: Cambridge, UK, 2017.
5. Ahlswede, R.; Csiszàr, I. Common randomness in information theory and cryptography—Part I: Secret sharing. *IEEE Trans. Inf. Theor.* **1993**, *39*, 1121–1132.
6. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theor.* **1993**, *39*, 733–742.
7. Maurer, U.; Wolf, S. Information-theoretic key agreement: From weak to strong secrecy for free. *Adv. Crypt. EUROCRYPT* **2000**, *1807*, 351–368.
8. Schneier, B. Inside risks: The uses and abuses of biometrics. *Commun. ACM* **1999**, *42*, 136.
9. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634.
10. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42.
11. Ignatenko, T.; Willems, F.M. Biometric systems: Privacy and secrecy aspects. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 956–973.
12. Lai, L.; Ho, S.W.; Poor, H.V. Privacy–security trade-offs in biometric security systems—Part I: Single use case. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 122–139.
13. Chou, R.A.; Bloch, M.R. One-way rate-limited sequential key-distillation. In Proceedings of the IEEE International Symposium Information Theory, Cambridge, MA, USA, 1–6 July 2012; pp. 1777–1781.
14. Wolfowitz, J. Simultaneous channels. *Arch. Ration. Mech. Anal.* **1959**, *4*, 371–386.
15. Blackwell, D.; Breiman, L.; Thomasian, A. The capacity of a class of channels. *Ann. Math. Stat.* **1959**, *30*, 1229–1241.
16. Boche, H.; Wyrembelski, R.F. Secret key generation using compound sources-optimal key-rates and communication costs. In Proceedings of the 9th International ITG Conference on Systems, Communication and Coding, München, Germany, 21–24 January 2013; pp. 1–6.
17. Bloch, M. Channel intrinsic randomness. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 2607–2611.
18. Chou, R.; Bloch, M.R. Secret-key generation with arbitrarily varying eavesdropper's channel. In Proceedings of the IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, 3–5 December 2013; pp. 277–280.
19. Tavangaran, N.; Boche, H.; Schaefer, R.F. Secret-key generation using compound sources and one-way public communication. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 227–241.
20. Grigorescu, A.; Boche, H.; Schaefer, R.F. Robust PUF based authentication. In Proceedings of the IEEE International Workshop on Information Forensics and Security, Rome, Italy, 16–19 November 2015; pp. 1–6.
21. Boche, H.; Nötzel, J. Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels. *J. Math. Phys.* **2014**, *55*, 122201.

22. Boche, H.; Schaefer, R.F.; Poor, H.V. On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2531–2546.
23. Grigorescu, A.; Boche, H.; Schaefer, R.F.; Poor, H.V. Capacity region continuity of the compound broadcast channel with confidential messages. In Proceedings of the IEEE Information Theory Workshop, Jerusalem, Israel, 24 April–1 May 2015; pp. 1–6.
24. Wolfowitz, J. *Coding Theorems of Information Theory*; Springer: New York, NY, USA, 1978.
25. Schaefer, R.F.; Boche, H.; Poor, H.V. Super-activation as a unique feature of secure communication in malicious environments. *Information* **2016**, *7*, 24.
26. Boche, H.; Schaefer, R.F.; Poor, H.V. Characterization of Super-Additivity and Discontinuity Behavior of the Capacity of Arbitrarily Varying Channels Under List Decoding. Available online: http://ieeexplore.ieee.org/abstract/document/8007044/ (accessed on 7 September 2017).
27. Csiszàr, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*; Cambridge University Press: Cambridge, UK, 2011.
28. Bjelaković, I.; Boche, H.; Sommerfeld, J. Secrecy results for compound wiretap channels. *Probl. Inf. Transm.* **2013**, *49*, 73–98.