Information Sciences 357 (2016) 6–22

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A joint Shannon cipher and privacy amplification approach to attaining exponentially decaying information leakage☆

Yahya S. Khiabani, Shuangqing Wei*

School of Electrical Engineering and Computer Science, Louisiana State University (LSU), Baton Rouge, LA 70803, United States

ARTICLE INFO

Article history:
Received 2 November 2014
Revised 28 October 2015
Accepted 30 March 2016
Available online 6 April 2016

Keywords:
Universal$_2$ hash functions
L_1 norm distance
Randomness extractor
Rényi entropy
Secrecy exponent
Equivocation

ABSTRACT

In this paper, we propose a novel layering approach to achieve end-to-end exponential security without resorting to presumed physical layer conditions. The only requirement for such an exponentially secure system is existence of a common key source between legitimate users that is partially known by Eve. The novel framework includes a random cipher and key stream generating scheme constituting the first layer and universal hash forming the second layer. The key generating scheme is based on a novel definition of a randomness extractor that derives a key stream with the required entropy from the common source, to be used for cipher. All metrics involved in characterizing the quality of secrecy of two-layer components are related to Rényi entropy and conditional Rényi entropy, which are all ultimately captured in the adopted information leakage metrics: mutual information and Eve's distinguishability based on L_1 norm distance from uniformity. Such relationships are exploited to optimize the resulting bounds for secrecy exponents by selecting appropriate operating parameters including required key rate and source entropies, as well as the required guessing error rate by Eve to attack the first layer.

1. Introduction

The basic secrecy system includes a sender Alice who attempts to transmit as many messages as possible to Bob, which are secured against an eavesdropper called Eve who attempts to attain the source information from Alice based on its prior knowledge and observation. The main problem is to design and optimize this system with a secrecy that is evaluated in terms of the amount of information leaked to Eve. In other words, this system can only guarantee a secure transmission between two parties if information leakage to the third party is minimized based on strict secrecy requirements.

1.1. Motivation and related works

In this work our main goal is to achieve end-to-end exponential security without resorting to presumed physical layer conditions, and to further quantify the level of secrecy based on associated exponents as defined by [1,2] for two information leakage metrics: mutual information and Eve's distinguishability based on L_1 norm distance from uniformity, respectively. These two metrics have been considered extensively by information theory community and cryptographic community lately.

☆ This work was supported in part by the Board of Regents of Louisiana under contract LEQSF(2009–11)-RDB-03 and National Science Foundation (NSF) under contract CNS-1018273.

* Corresponding author. Tel.: +1 225 578 5536; fax: +1 225 578 5200.
E-mail addresses: yahya.netopt@gmail.com (Y.S. Khiabani), swei@lsu.edu (S. Wei).

http://dx.doi.org/10.1016/j.ins.2016.03.049
0020-0255/

In information theory community, information leakage based on mutual information as secrecy criterion has been considered [3–5]. These works only consider a security metric based on mutual information which is required to be negligible for uniformly distributed random message sources. However, in reality, we cannot expect any finitely long messages to be uniformly random since no universally source independent compression exists for such finite sources [6]. Rather, we use a stronger notion of end-to-end security, previously used in [1], that requires mutual information to be negligible for any given message distribution. In particular, Hayashi in [1] showed that when input has equivocation in terms of Rényi entropy of order α, after application of universal$_2$ hash function, Eve's information about the generated random variable decreases at an exponential rate that can be lower bounded. This bound is more generalized and in some cases even tighter than the bound obtained by Bennett in [7].

In cryptography community, security of ciphers has been mainly evaluated in terms of computation based metrics against resource constrained attackers. However, recently some researchers have used statistical measures, like variational distance, as secrecy criterion against adversary with unbounded computational power [8–11]. Variational distance is closely related to practical notions of secrecy like Eve's distinguishability and can be used to provide a universally composable notion of secrecy that allows to express secrecy requirement for any protocol environment. As in [2,11], Eve's distinguishability is defined as half of the L_1 norm distance that is closely related to universal composable security, which is the second metric we adopt to evaluate information leakage from cryptographic point of view. As in [2], Hayashi also provided a lower bound of the L_1 distance between the output of universal hashing and the uniform random number, as well as its corresponding exponent analysis.

It should be noted that our goals of achieving end-to-end security with quantifiable secrecy exponents under metrics of mutual information and L_1 distance, respectively, are partially inspired by the works from [1,2]. However, it should also be remarked that the authors of [1,2] assume a common randomness to begin with and a physical layer channel from Alice to Eve degraded than that to Bob and propose using invertible hash for secure message transmission and secret key generation. In this work, we also assume that there exists shared common randomness, yet instead of having a degraded channel, as a contrast, we exclusively rely on Eve's uncertainty on this shared randomnesses as the privilege provided for legitimate users over adversary that allows us to utilize invertible universal hash function for secrecy enhancement. The assumption on existence of such a common random source was also used in some key extracting techniques [9,12]. As a result of the lack of degraded Eve's channel to exploit, a substantial amount of new results has been obtained to achieve our goals, which are highlighted in detail in the next subsection.

1.2. Summary of our novel results

Given the existing advantage in terms of Eve's uncertainty about the common randomness shared between Alice and Bob, and without resorting to further a degraded physical channel to the eavesdropper, we propose a novel two-layer secrecy system that can be considered as a practical construction of the methods proposed in [1,2]. In this new framework, a random cipher and key stream generating scheme constitutes the first layer and universal hash the second layer.

This new layering protocol prompts us to study many different problems than [1,2] including a key generation approach based on a novel definition of randomness extractor with results provided in Theorem 1, a novel characterization of equivocation of the message encrypted by a Shannon cipher with results provided in Theorem 2, as well as a novel joint optimization problem to maximize the attained security exponents over two layers. It should be noted that we need to put all individual metrics in our proposed scheme that comprises (a) generation of key stream and its security evaluation using Rényi entropy; (b) Shannon type cipher measured by both maximum a posteriori probability (MAP), and conditional Rényi entropy; (c) i nvertible hash at transmitter and hash at receiver; as well as (d) the end-to-end security evaluation using either mutual information or L_1 distances, in a coherent framework and then conduct optimization accordingly.

In the first layer of design, the required keys for encryption are derived using key extracting approach that consists of a statistical sampler which provides sampled data frames from a common key source between legitimate users and an extractor that derives keys with the required Rényi entropy for encryption from these partially secure data frames. Randomness extractors are well suited to address the need for key derivation functionality which maps input distributions with sufficient entropy into outputs with distributions statistically close to uniform [13]. It should be further noted that, to the best of our knowledge, so far all existing definitions of extractors measure randomness of the extracted output in terms of statistical distance from uniformity. In secrecy enhancement of the designed scheme that comprises second layer, privacy amplification is based on uncertainty measured using Rényi entropy, and hence a new notion of extractor is developed that extracts the required randomness on the basis of Rényi entropy, rather than Shannon entropy.

The main functionality of the second layer of the design is to leverage the existing equivocation provided by the first layer to establish a transmission mechanism with information leakage that decays exponentially fast. For this purpose, we utilize universal$_2$ hash function as the main secrecy enhancement approach on top of the first layer. In particular, we suggest a more generalized version of the invertible universal$_2$ hash function used in [10] based on the multiplication in finite field [14]. It should be noted that Hayashi in [15] constructs a finite field whose multiplication has small computational complexity, so that our proposed invertible hashing can be implemented with much less amount of calculation than physical layer secrecy approaches whose construction resort to some sophisticated error correction codings [16].

We design a dual mode transmission mechanism, under this two-layer framework, that switches between two modes of operation, one using only first layer based on encryption and the other one operating jointly on encryption and privacy

amplification layers, to provide various secrecy levels based on the demanded security for different types of message. In this framework, for the purpose of end-to-end security analysis, for a particular case where source messages consist of independently and identically distributed (i.i.d) symbols, we seek to optimize bounds for exponents of information leakage. These optimized bounds reflect unique characteristics of both universal hash function and general Shannon cipher in a cohesive manner as shown in the major results in Sections 4–8. In dual mode transmission mechanism, we jointly optimize key generation rate that guarantees achievable secrecy based on both optimized bounds of secrecy exponent as well as the required guessing error probability for Eve. We show that due to the demand of a higher level of secrecy in operational mode that uses both layers, its required secret key rate is much higher than the mode operating only on the first layer.

We have presented parts of the results of this paper in [17,18]. Compared to [17], in this work we have revised abstract and introduction in order to more clearly address our motivation for this work as well as the novelties of the proposed security scheme. In particular, we have clarified the difference between our work and some other relevant works in this version. We also have used a new metric for conditional Rényi entropy that has changed the whole secrecy analysis and characteristics of the first layer of the proposed scheme and has lead us to the new Theorem 2 in Section 5. This critical revision allows us to remain consistent with the definition of secrecy metrics throughout the paper. As compared with [18], in addition to the items listed above, in this paper we have presented a new analysis based on Eve's guessing error probability for the first layer of scheme. We also have proposed a new dual mode transmission mechanism and jointly optimized the required key generation rate to achieve the required security in both operational modes. It should also be noted that more complete proofs are provided in this paper.

In Section 2, we provide the required background in cryptography and information theory. Section 3 presents the whole scheme of design and illustrates denotations that are used throughout the paper. Key extractor and cipher are described and analyzed in Sections 4 and 5, respectively. Privacy amplification and exponent analysis based on mutual information and variational distance metrics are detailed in Section 6. The description of dual mode transmission mechanism and its optimization are presented in Section 7, and its related numerical analysis is provided in Section 8. Finally, we conclude in Section 9, and the proofs of some theorems are given in Appendix A.

2. Relevant background

In this section, we provide a brief review about several important notions in information theory and cryptography. Let random variable X have probability distribution of P_X defined on the alphabet set of Ω, and let U_X be a uniform distribution on the same alphabet set of X which is Ω. L_1 distance of P_X from uniform distribution is

$$d_1(P_X, U_X) \triangleq \sum_x |P_X(x) - U_X(x)|. \tag{1}$$

When the distribution P_Y of the random variable Y and the joint distribution of $P_{X,Y}$ are given, we get

$$\begin{aligned} d_1(P_{X,Y}, U_X \times P_Y) &= \sum_{x,y} |P_{X,Y}(x,y) - U_X(x)P_Y(y)| \\ &= \sum_y P_Y(y) \sum_x |P_{X|Y}(x|y) - U_X(x)| = \sum_y P_Y(y) d_1(P_{X|Y=y}, U_X). \end{aligned} \tag{2}$$

Rényi entropy of order α for $1 < \alpha \leq 2$ is defined as [19,20]:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha. \tag{3}$$

We also have joint Rényi entropy defined as

$$H_\alpha(X,Y) = \frac{1}{1-\alpha} \log \sum_{x,y} P_{X,Y}^\alpha(x,y). \tag{4}$$

Then, we shall define the conditional Rényi entropy

$$H_\alpha(X|Y) = \frac{1}{1-\alpha} \log \sum_{x,y} P_Y(y) P_{X|Y}(x|y)^\alpha. \tag{5}$$

As another measure of difference between two distributions, we can obtain distance of P_X from uniform distribution in terms of Rényi divergence of order α, for $1 < \alpha \leq 2$ [19]

$$D_\alpha(P_X||U_X) = \frac{1}{\alpha - 1} \log \sum_x P_X(x)^\alpha U_X(x)^{1-\alpha}. \tag{6}$$

For $\alpha = 1$, KL-divergence is defined as

$$D(P_X||U_X) = \sum_x P_X(x) \log \frac{P_X(x)}{U_X(x)}. \tag{7}$$

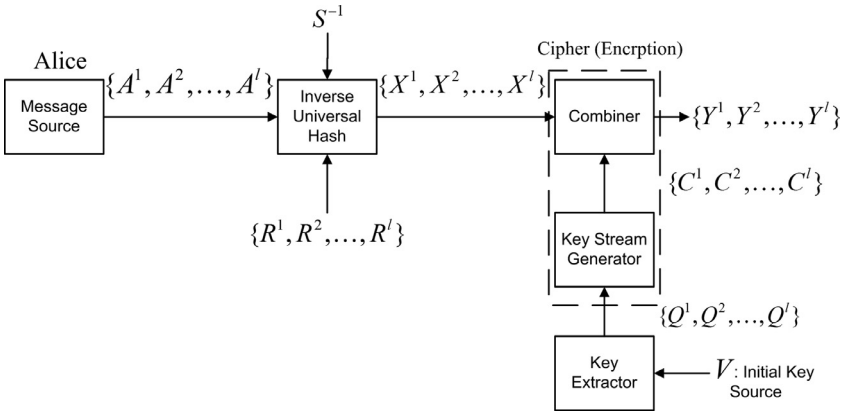

Fig. 1. Transmitter side in the proposed secrecy scheme.

The following inequality in [21] characterizes the relationship between KL-divergence and L_1 distance

$$-\log d_1(P_X, U_X) \geq -\frac{1}{2}\log D(P_X||U_X). \tag{8}$$

We adopt universal hashing for privacy amplification and key extraction. An ensemble of the functions h_s that maps set Ω to $\{1, \ldots, M\}$, where S determines statistical behavior of the function h, is called universal$_2$ when it satisfies the following conditions [22]:

Condition 1: $\forall x^1 \neq x^2 \in \Omega$, the probability that $h_s(x^1) = h_s(x^2)$ is at most $\frac{1}{M}$.

Condition 2: For any S, the cardinality of $h_s^{-1}\{i\}$ is independent of the input i.

To make this concrete we give an example of a universal$_2$ hash function with an efficiently computable inverter that can be used for key derivation and privacy amplification in our scheme. The construction was used in [10] as randomness extractor. Here, we use a more general symbol-wise format of this construction. If we interpret n-symbol strings as elements of the finite field GF(q^n), we shall define a multiplication operator $\odot$ on them. Let set Ω be $\{0, \ldots, q-1\}$ and consider seed S that is drawn uniformly from the set $\mathcal{SD} = \Omega^n \setminus 0^n$. We define the universal hash function $h{:}\mathcal{SD} \times \Omega^n \to \Omega^b$ that operates on inputs $X \in \Omega^n$ and $S \in \mathcal{SD}$ to output the first truncated b-symbols of $X \odot S$ as $A = h(X, S) = \text{trunc}_b(X \odot S)$ (this construction was also used in [14]).

Let S^{-1} be the inverse of S with respect to multiplication in GF(q^n). Then, we can efficiently invert this universal hashing by the function $h^{-1}{:}\mathcal{SD} \times \Omega^{n-b} \times \Omega^b \to \Omega^n$ defined as $h^{-1}(S, R, A) = (A||R) \odot S^{-1}$, for R uniform over Ω^{n-b}. In Appendix A we show that both conditions 1 and 2 hold for this function, meaning that in addition to uniformity of the output hash value, every point in the range has the same number of preimages.

3. Proposed model for secrecy scheme

The transmitter and the receiver side of our proposed secrecy scheme are shown in Figs. 1 and 2, respectively. We assume that there exists a source of information denoted by V about which Eve has a lower bounded uncertainty measured in terms of Rényi entropy. Key extracting module shown in Fig. 3 is used to derive nearly uniform secret key from this weakly random source of data. By independently sampling a segment of this source at time i we obtain a data frame Λ^i that will have the required randomness given Eve's knowledge in terms of Rényi entropy. We show that a key Q^i can be extracted out of Λ^i, by using extractor based on universal hashing, with Rényi entropy that is asymptotically close to the maximum value. This generated key can be used as a symmetric key for encryption in a general cipher.

Consider a uniformly distributed and randomly chosen function from a universal class of hash functions that is applied upon a source of data with a sufficient equivocation (conditional Rényi entropy given Eve's knowledge). It is proven in [1,2] that the generated output hash value will have exponentially decreasing information leakage measured in terms of mutual information or L_1 norm distance from uniform distribution.

As shown in Fig. 1, the secure transmission mechanism is applied over a sequence of l blocks with the size of b-symbols. As convention a message block at time i is shown as A^i, with symbols of $\{A_1^i, A_2^i, \ldots, A_b^i\}$. A sequence of l concatenated blocks is denoted as $A^{(l)} = \{A^1, A^2, \ldots, A^l\}$. Inverse universal hash maps this sequence into a sequence of plaintext blocks $\{X^1, X^2, \ldots, X^l\}$ using the same random seed S that is publicly known and a sequence of random vectors $\{R^1, R^2, \ldots, R^l\}$ that are uniformly generated. In our scheme we consider an invertible universal hash function based on modulo n multiplication in $GF(q^n)$. Inverse universal hash maps its input into its pre-image that increases its length by adding some randomness through binning. It has a similar functionality as the homophonic encoder in approach proposed in [23] or the random binning based encoding proposed by Wyner and Ciszar in [3,4] and can be considered as a particular encoder that tailors to Eve's uncertainty over the key source.

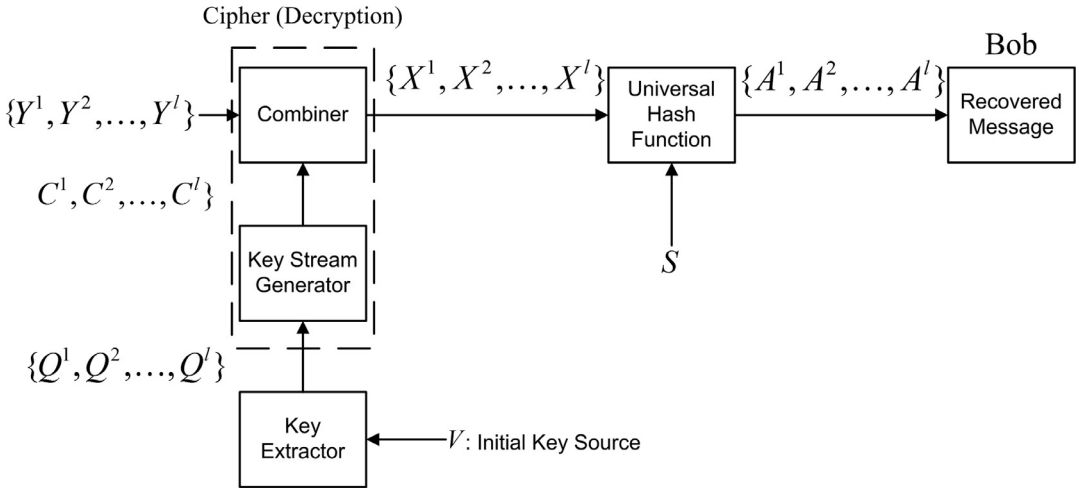

Fig. 2. Receiver side in the proposed secrecy scheme.

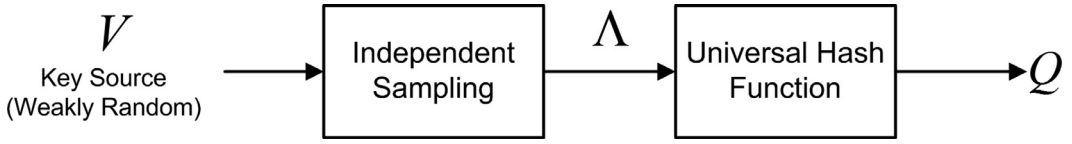

Fig. 3. Key extractor from a weakly random source.

Each of the generated n-symbol plaintext blocks at the output of inverse universal hash function will be encrypted independently using a general cipher. The cipher is comprised of a key stream generator to derive key stream C^i from this key Q^i using a bijective mapping as well as a combiner that combines this key stream with the plaintext block X^i. For $i = 1, \ldots, l$, this encryption results in a sequence of ciphertexts $Y^{(l)} = \{Y^1, Y^2, \ldots, Y^l\}$, that will be transmitted to Bob and eavesdropped by Eve.

Key extractor and the cipher constitute the first layer of secrecy that ensures sufficient equivocation of plaintext blocks provided that the extracted key has the required Rényi entropy. Upon receiving these ciphertexts, Bob has the same initial key source V and uses inverse mappings to recover the plaintext sequence $X^{(l)} = \{X^1, X^2, \ldots, X^l\}$ with a sufficient equivocation. As will be stated in Theorems 4 and 5, after applying the universal hash over this sequence, Eve's information about the restored message sequence $A^{(l)}$ approaches zero exponentially fast, whose exponent can be bounded properly.

4. Key extractor

With the existence of an initial key source that contains some good amount of randomness but is non-uniformly distributed or partially known by Eve, we need to design a key extracting function based on essential cryptographic components that derives required keys from this imperfect source with a randomness close to uniform. The assumption on existence of such a random source was also used in some key extracting techniques like [9,12,24]. This random data can be produced through different means such as hardware devices based on thermal noise, statistical sampling of user's keyboard strokes or timing data obtained from the hard disk or packet transmission in a network [9]. Here we describe characteristics of the proposed key extractor with the structure illustrated in Fig. 3, that consists of an independent sampler which provides data frames with the required Rényi entropy given Eve's knowledge, and a randomness extractor that uses universal hashing to extract keys from these data frames with Rényi entropy asymptotically close to maximum.

Consider random vector V common between Alice and Bob, consisting of ν random variables as $V = (V_1, V_2, \ldots, V_\nu)$ that is used as initial keying source. This keying source V gathered by users has to contain enough uncertainty at Eve's side in terms of Rényi entropy of order 2 denoted by $H_2(V)$. As shown in Fig. 3 the first step in key extractor is a sampling module that each time independently samples a λ-tuple from this source such that each symbol can only be sampled once. For any λ-tuple $\underline{i} = (i_1, i_2, \ldots, i_\lambda)$ with $1 \le i_1 < i_2 < \ldots < i_\lambda \le \nu$ let $V_{\underline{i}}$ be the sampled string $(V_{i_1}, V_{i_2}, \ldots, V_{i_\lambda})$. Then, it is shown in [25] that

$$H_2(V_{\underline{i}}) \ge H_2(V) - (\nu - \lambda). \tag{9}$$

For $H_2(V) - (\nu - \lambda) = \delta$ if we denote the randomly sampled λ-tuple string at time i as Λ^i, it will have collision entropy of at least δ. Rényi entropy is a decreasing function with respect to its order [20], so $H_\alpha(\Lambda^i) \ge H_2(\Lambda^i) \ge \delta$ for $1 < \alpha \le 2$, and Eve's uncertainty about the sampled output in terms of Rényi entropy of order α will be at least δ.

Each time that λ number of samples are taken for key generation out of the source V, it is assumed that these samples are excluded from upcoming samplings for future key generation. Moreover, we assume that for each key generation, the keying source keeps its minimum required collision entropy of $H_2(V)$ by replenishing its missing samples. This is to make sure that acquiring any information about previous keys will not assist Eve to reduce her uncertainty about future keys.

The second step is to use a randomness extractors that derives keys from these independently sampled data frames by mapping inputs with sufficient Rényi entropy into outputs that are statistically close to uniform. Since in our scheme privacy amplification is characterized based on Rényi entropy, we need to develop a new notion of extractor that extracts randomness in terms of Rényi entropy, unlike existing definitions of extractors that measure extracted randomness based on statistical distance. The following theorem, proven in Appendix B, explains how universal hash functions can be used to extract randomness in terms of Rényi entropy. It can be considered as a generalization of Theorem 1 in [1], from Shannon entropy to Rényi entropy of order $\alpha > 1$.

Theorem 1. *Consider a universal class of hash functions $h_s: \mathcal{X} \to \mathcal{K}$; where S is uniform over $\mathcal{SD}$. If we apply h_s over input $X \in \mathcal{X}$ with Rényi entropy of $H_\alpha(X) \geq \delta$, for $1 < \alpha \leq 2$, the generated hash value $Q = h_s(X)$ with $Q \in \mathcal{K}$ attains Rényi entropy with the following lower bound*

$$H_\alpha(Q) \geq \log|\mathcal{K}| - \frac{1}{\alpha-1} e^{-(\alpha-1)[\delta - \log|\mathcal{K}|]}. \tag{10}$$

Now, we can define the new notion of Rényi extractor:

Definition 1. *RenExt: $\mathcal{X} \times \mathcal{SD} \to \mathcal{K}$ is a (δ, ζ) Rényi extractor if for every seed S uniformly chosen on $\mathcal{SD}$ and every source $X \in \mathcal{X}$ of Rényi entropy $H_2(X) \geq \delta$, it holds that RenExt(X, S) has Rényi entropy of at least $\log|\mathcal{K}| - \zeta$.*

Rényi extractor based on universal hashing results in entropy loss ζ which is exponentially decreasing. By applying this Rényi extractor over sampled data frame Λ^i which has Rényi entropy of at least δ, provided that $\delta > \log|\mathcal{K}|$, we obtain a key $Q^i \in \mathcal{K}$ with Rény entrpy

$$H_\alpha(Q^i) \geq \log|\mathcal{K}| - \frac{1}{\alpha-1} e^{-(\alpha-1)[\delta - \log|\mathcal{K}|]} = \log|\mathcal{K}| - \zeta.$$

If we adopt universal hashing technique based on $\odot$ multiplication in GF(q^n) for key extraction, we need to use independent seeds for each key derivation. It ensures that then due to independent sampling and mapping used in key extractor, the generated keys will be independent of each other.

5. Cipher

In this section we characterize the first layer of secrecy in the proposed scheme that is based on a cipher and then use equivocation of order α as the measure to evaluate its secrecy. It then leads us to determine the definition of a good cipher and also the required key generation rate that guarantees the minimum required secrecy level for this layer. Consider a deterministic cipher that consists of a key stream generator and a combiner. Let the plaintext block at time i be $X^i = (X_1^i, X_2^i, \ldots, X_n^i)$ where $X_j^i \in \Omega$. The key extractor output is Q^i that takes values in the set $\mathcal{K}$ with total of e^{nR_s} elements. At time i key stream generator maps the input key Q^i to the key stream of length n, $C^i = (C_1^i, C_2^i, \ldots, C_n^i)$ with components from the set Ω using the mapping $\Phi: \mathcal{K} \to \Omega^n$. We define the cipher as the set $C^* = \{C^1, C^2, \ldots, C^{e^{nR_s}}\}$ of key streams with length n and key rate of $R_s = \frac{\log|\mathcal{K}|}{n}$.

For $i = 1, \ldots, l$ the cipher produces the ciphertext block Y^i from the ith plaintext block X^i and the ith key stream C^i using the combiner $f(.,.)$ that maps $\Omega^n \times \Omega^n \to \Omega^n$.

$$Y^i = f(X^i, C^i) \quad i = 1, 2, \cdots. \tag{11}$$

Bob is aware of the key Q^i used at time i and can generate the same key stream C^i using key stream generator. He applies inverse mapping $g(.,.)$ to the received ciphertext block C^i in order to recover the plaintext block X^i, with g: $\Omega^n \times \Omega^n \to \Omega^n$ and $X^i = g(Y^i, C^i)$. Depending on the mapping f, the cipher could be block, stream cipher, or additive-like cipher.

Now the question is how much Eve knows about the plaintext. She has knowledge about the system and all the mappings and can receive ciphertexts. However, she has some lack of knowledge about the key source that results in uncertainty about the cipher key. We evaluate this uncertainty in terms of equivocation of order α as defined in Eq. (5) that can be characterized using Theorem 2. The proof for this theorem is provided in Appendix C.

Theorem 2. *Let $X = (X_1, X_2, \ldots, X_n)$, $Y = (Y_1, Y_2, \ldots, Y_n)$ and $C = (C_1, C_2, \ldots, C_n)$ be random vectors representing plaintext block, ciphertext block and the key stream, respectively, where $X_i \in \mathcal{X}$, $Y_i \in \mathcal{Y}$ and $C_i \in \mathcal{C}$ such that $|\mathcal{X}| = |\mathcal{Y}|$. Let Q denote the random vector representing the key. Let us define two measures*

$$p^*(y) \triangleq \frac{P_Y(y)^{1-\alpha}}{\gamma_{\alpha,Y}}$$
$$q^*(y) \triangleq \frac{\sum_x P_{XY}^\alpha(x,y)}{\Gamma_{\alpha,XY}}, \tag{12}$$

where

$$\gamma_{\alpha,Y} \triangleq \sum_{y} P_Y(y)^{1-\alpha}$$
$$\Gamma_{\alpha,XY} \triangleq \sum_{x}\sum_{y} P_{XY}^{\alpha}(x,y) \tag{13}$$

Then, there exists $\beta > 1$ such that for $\alpha > 1$, equivocation of the plaintext satisfies:

$$H_\alpha(X|Y) \geq H_\alpha(Q) - D_\alpha(P_X||U_X) - D_\alpha(P_Y||U_Y) - \tfrac{\beta-1}{\alpha-1} D_\beta[\rho_Y^*||U_Y]. \tag{14}$$

where ρ_Y^* is defined as

$$\rho_Y^* \triangleq \begin{cases} p_Y^* & \text{if} \quad D_\beta[p_Y^*||U_Y] \geq D_\beta[q_Y^*||U_Y] \\ q_Y^* & \text{if} \quad D_\beta[q_Y^*||U_Y] \geq D_\beta[p_Y^*||U_Y] \end{cases} \tag{15}$$

We define output redundancy function as

$$\Theta_0(P_{XY}, \alpha, \beta) = D_\alpha(P_Y||U_Y) + \frac{\beta-1}{\alpha-1} D_\beta[\rho_Y^*||U_Y]. \tag{16}$$

A good cipher can be defined as a cipher that, regardless of what distribution its input has, generates ciphertext that is sufficiently close to uniform distribution. This closeness can be measured in terms of Rényi divergence defined in Eq. (6) by requiring it to be negligible. However, for our design we demand a cipher that for a given input–output distribution results in a negligible output redundancy defined in Eq. (16), implying that in addition to Rényi divergence of the ciphertext, the second term in Eq. (16) is required to be close to zero. Namely,

$$\Theta_0(P_{XY}, \alpha, \beta) \leq \varepsilon, \tag{17}$$

where ε has a sufficiently small positive value. Accordingly, for such a cipher equivocation of the plaintext satisfies

$$H_\alpha(X|Y) \geq H_\alpha(Q) - D_\alpha(P_X||U_X) - \varepsilon. \tag{18}$$

The key generation rate R_s has to be specified in order to guarantee the required secrecy for the first layer of the scheme including the cipher and key extractor. It aims at a minimum required equivocation for Eve about the message that can be characterized in terms of the average error probability in Eve's estimation of the plaintext block. Let X^* be an estimate of adversary from the plaintext block X based on the maximum a posteriori probability (MAP) given the received ciphertext Y as $X^* = \arg\max_{X\in\Omega^n} Pr[X|Y]$. MAP decision rule minimizes the average probability of error per plaintext block defined as

$$P_{e,adv} = E_Y[1 - \max_{X\in\Omega^n} Pr(X|Y)] = 1 - E_Y[\max_{X\in\Omega^n} Pr(X|Y)]. \tag{19}$$

According to the following theorem that is presented and proven as Theorem 6 in [26], Rényi entropy can be used to bound error probability of MAP decision rule based on an analogue of Fano's lemma.

Theorem 3. *Let P be the set of a posteriori probabilities as $P = \{P_1, P_2, \ldots, P_m\}$, and let $h_\alpha(P)$ be defined as*

$$h_\alpha(P) = \frac{1}{1-\alpha} \log\left(\sum_{i=1}^{m} p_i^\alpha\right), \tag{20}$$

If we consider estimation error probability defined as $P_e = 1 - \max P_i$, for $\alpha \neq 1$ the maximum upper bound for $h_\alpha(P)$ is attained as

$$\bar{h}_\alpha(P_e) = \frac{1}{1-\alpha} \log\left[(1-P_e)^\alpha + \left(\frac{1}{m-1}\right)^{\alpha-1} P_e^\alpha\right]. \tag{21}$$

Consider plaintext estimation by adversary, with the set of a posteriori probabilities as $P = \{Pr(X = x|Y = y)|\forall x \in \Omega^n\}$ and average estimation error probability for adversary as $P_{e,adv}$ defined in Eq. (19). According to the above-mentioned Theorem 6 we can obtain the maximum upper bound for $h_\alpha(P)$ based on the definition in Eq. (20) for $\alpha > 1$ as

$$\bar{h}_\alpha(P_{e,adv}) = \frac{1}{1-\alpha} \log\left[(1-P_{e,adv})^\alpha + \left(\frac{1}{|\Omega|^n - 1}\right)^{\alpha-1} P_{e,adv}^\alpha\right].$$

As a result, its average over the values of the random variable Y defined as

$$h_\alpha^{ave}(P) = \frac{1}{1-\alpha} \sum_{y\in\Omega^n} P_Y(y) \log \sum_{x\in\Omega^n} Pr(X = x|Y = y)^\alpha$$

will also follow this upper bound. $h_\alpha^{ave}(P)$ can be considered as one of the definitions of the conditional Rényi entropy as discussed in [27] that due to Jensen's inequality is always greater than or equal to the definition of the conditional Rényi entropy in Eq. (5) used in this work. Therefore, we can obtain the upper bound for conditional Rényi entropy of order α

$$H_\alpha(X|Y) \leq \bar{h}_\alpha(P_{e,adv}), \quad \text{for} \quad 1 < \alpha \leq 2. \tag{22}$$

In this work error probability of attacker in estimation of the plaintext block using MAP is adopted as the secrecy metric for the first layer of the scheme. Such metric was also used in previous works [28,29] as secrecy criterion. Let us determine a threshold as P_e^{th} and design the system with a key stream generation rate that ensures that Eve's block error probability always exceeds it. It is easy to see that for $1 < \alpha \leq 2$, $\bar{h}_\alpha(P_{e,adv})$ is a monotonic increasing function of $P_{e,adv}$. In other words, if we ensure that $\bar{h}_\alpha(P_e^{th}) \leq H_\alpha(X|Y)$ due to inequality (22) and monotonic behavior of $\bar{h}_\alpha(P_{e,adv})$ we will have $P_{e,adv} \geq P_e^{th}$. Let $\tau_\alpha \triangleq \bar{h}_\alpha(P_e^{th})$, so we need to make sure that equivocation in Eq. (18) never drops below τ_α

$$H_\alpha(Q) - D_\alpha(P_X||U_X) - \varepsilon \geq \tau_\alpha.$$

We define $\eta \triangleq \varepsilon + \tau_\alpha$ so that

$$H_\alpha(Q) - D_\alpha(P_X||U_X) \geq \eta.$$

If we use our proposed key extracting technique, $H_\alpha(Q)$ can be lower bounded according to Eq. (10). Then, for the above inequality to hold, we need to satisfy the following sufficient condition,

$$\log|\mathcal{K}| \geq D_\alpha(P_X||U_X) + \frac{1}{\alpha-1}e^{-(\alpha-1)[\delta-\log|\mathcal{K}|]} + \eta. \tag{23}$$

Since in our proposed scheme δ and $\log|\mathcal{K}|$ depend on each other, we can assume that they are chosen in a way that both satisfy $\delta - \log|\mathcal{K}| \geq \gamma$. Hence, we can infer that

$$R_s \geq \frac{D_\alpha(P_X||U_X) + \eta + \frac{1}{\alpha-1}e^{-(\alpha-1)\gamma}}{n}. \tag{24}$$

It characterizes the minimum required key stream generation rate for the first layer of secrecy.

6. Privacy amplification

In this section we discuss how universal hashing can be used to create a higher layer of secrecy on top of the cipher, as the first layer, in order to transmit messages with a security evaluated in terms of secrecy exponent that measures how fast information leakage decays with respect to the number of transmitted blocks. This exponent is defined for information leakage measured in terms of mutual information as well as L_1 distance, and is characterized based on lower bounds presented in Theorems 4 and 5 for the proposed two layer secrecy scheme.

6.1. Secrecy exponent analysis based on mutual information

The main objective of using universal hashing in our scheme is bringing secrecy up to the second layer by privacy amplification. Let h_s be an ensemble of universal$_2$ hash functions that maps set Ω^n to $\{1,\ldots,M\}$ and satisfies both conditions 1 and 2. As proven in [1], information leakage in terms of mutual information, averaged over possible seeds S, satisfies

$$E_s[I(h_s(X);Y)] \leq \min_{1<\alpha\leq 2} \frac{e^{-(\alpha-1)(H_\alpha(X|Y)-\log M)}}{\alpha-1}. \tag{25}$$

So we can find a function h_s from Ω^n to $\{1,\ldots,M\}$ that

$$I(h_s(X);Y) \leq \min_{1<\alpha\leq 2} \frac{e^{-(\alpha-1)(H_\alpha(X|Y)-\log M)}}{\alpha-1}, \tag{26}$$

where Y denotes the obtained knowledge by Eve. Eq. (26) implies that when legitimate users have a common randomness denoted by X with equivocation of at least $H_\alpha(X|Y)$, we can make sure that the upper bound for Eve's knowledge about the output of $h_s(X)$ decreases with the exponent of $(\alpha-1)(H_\alpha(X|Y)-\log M)$. It should be noted that the parameter α is introduced to the upper bound on mutual information in Eqs. (25) and (26), due to the adoption of Rényi entropy as a measure in quantifying the information leakage. By considering that both $H_\alpha(X|Y)$ and $\log(M)$ are the functions of the block length n, if we put a normalized exponent in the power of the exponential function, i.e. $1/(\alpha-1)\exp(-n(\alpha-1)(H_\alpha(X|Y)-\log(M))/n)$, we can see that as the block length grows large asymptotically, for any given $\alpha \in (1, 2]$, the mutual information is driven to zero exponentially fast with respect to the block length n. The additional optimization with respect to α that will be discussed in Section 7 is to further sharpen such exponential rate. In a word, when we present an information theoretically secure scheme, we mean the proposed metric (either mutual information or L_1 distance) about information leakage is driven asymptotically to zero at an exponential rate.

In our scheme Alice and Bob exchange random vector X through encryption that enables them to have a shared body of random data with equivocation of $H_\alpha(X|Y)$. As the next step if we apply the universal hash function based on $\odot$ multiplication in GF(q^n), that maps Ω^n to Ω^b, it can be assured that output $A = h_s(X)$ will have information leakage with the decreasing exponent of at least $(\alpha-1)(H_\alpha(X|Y)-\log M)$, for $M = |\Omega^b|$. Now if we reverse this process and obtain X from input A using inverse universal hash that maps Ω^b to Ω^n, we will get the same results since condition 2 guarantees that the cardinality $|h_s^{-1}(A)|$ does not depend on A. Let Alice generate uniformly random string R over Ω^{n-b} and apply inverse

function h_s^{-1} over the input A, R and S^{-1} to obtain plaintext $X = (A||R) \odot S^{-1}$. Then, decreasing exponent of information leakage about A will be at least $(\alpha - 1)(H_\alpha(X|Y) - \log M)$.

Consider l-fold scenario of the above-mentioned mechanism where input message is framed into a sequence of l blocks denoted by $A^{(l)} = \{A^1, A^2, \ldots, A^l\}$ for $A^i \in \Omega^b$. Alice generates the sequence of l uniformly random $(n-b)$-symbol strings $R^{(l)} = \{R^1, R^2, \ldots, R^l\}$, and then by using inverse universal hash, outputs $X^i = (A^i||R^i) \odot S^{-1}$, to map $A^{(l)}$ to the sequence of plaintexts $X^{(l)} = \{X^1, X^2, \ldots, X^l\}$. Then, $X^{(l)}$ will be mapped to the sequence of ciphertexts $Y^{(l)} = \{Y^1, Y^2, \ldots, Y^l\}$ as $Y^i = f(X^i, C^i)$ through encryption by the sequence of l key streams $C^{(l)} = \{C^1, C^2, \ldots, C^l\}$ that are generated using the cipher keys $\{Q^1, Q^2, \ldots, Q^l\}$. Let $A^{(l)} \in \mathcal{I}$. We can obtain the random number generation rate in this l-fold transmission mechanism as

$$\rho \triangleq \lim_{l\to\infty} \frac{\log|\mathcal{I}|}{l} = \lim_{l\to\infty} \frac{\log|\Omega^b|^l}{l} = \log|\Omega^b| = \log M. \tag{27}$$

At the receiver end after deciphering and recovering of $X^{(l)}$ that consists of l plaintext blocks, universal hashing will be applied over them to restore message blocks as $A^i = \mathrm{trunc}_b(X^i \odot S)$. Note that the same seed S, uniformly chosen over Ω^n, is used for hashing of all l blocks that has to be publicly known before their transmission. We define mutual information based secrecy exponent for l-fold scenario as

$$e_l^{(l)} \triangleq \lim_{l\to\infty} \frac{-\log I(h^{(l)}(X^{(l)}); Y^{(l)})}{l}, \tag{28}$$

whose lower bound is given in the following theorem.

Theorem 4. *Let random variable A represent the message block of size b with components in the set Ω where $M = |\Omega^b|$ and Q represent the cipher key. Then, for the described l-fold transmission mechanism in two layer secrecy scheme, mutual information based secrecy exponent satisfies:*

$$e_l^{(l)} \geq \max_{0<\alpha\leq 1} (\alpha - 1)(H_\alpha(Q) + H_\alpha(A) - 2\log M - \varepsilon). \tag{29}$$

Proof. Since R^i and A^i are independent of R^j and A^j for $i \neq j$, for a given S, X^i and X^j will be independent of each other. Namely, revealing any information about any of the plaintexts does not assist Eve to reduce her uncertainty about other ones. Consequently, we shall write

$$H_\alpha(X^{(l)}|Y^{(l)}) = lH_\alpha(X^i|Y^i) = lH_\alpha(X|Y). \tag{30}$$

We use Cartesian product construction of universal class of hash functions in order to enlarge the domain of hash family. In this construction hashed outputs, that are generated using hash function with the same seed, are concatenated, where $h_s^{(l)}(X^{(l)})$ is defined as $h_s(X^1)||h_s(X^2)||\ldots||h_s(X^l)$. Stinson showed in [30] that Cartesian product based universal hashing denoted by $h_s^{(l)}$ results in the same collision probability as h_s. Namely, using only one seed for l transformations does not compromise security.

At receiver l-fold universal hash function $h_s^{(l)}$ maps $X^{(l)}$ to $A^{(l)}$. Joint distribution of $X^{(l)}$ and $Y^{(l)}$ denoted by $P_{X^{(l)},Y^{(l)}}$ can be obtained by l-fold identical and independent distribution of $P_{X,Y}$ as $(P_{X,Y})^l$, so that we can infer from Eq. (30)

$$\begin{aligned} I(h_s^{(l)}(X^{(l)}); Y^{(l)}) &\leq \min_{1<\alpha\leq 2} \frac{e^{-(\alpha-1)(H_\alpha(X^{(l)}|Y^{(l)}) - \log|\mathcal{A}^b|^l)}}{\alpha - 1} \\ &= \min_{1<\alpha\leq 2} \frac{e^{-l(\alpha-1)(H_\alpha(X|Y) - \log|\mathcal{A}^b|)}}{\alpha - 1}. \end{aligned}$$

Hence, based on the definition of the secrecy exponent in Eq. (28), $e_l^{(l)}$ can be obtained

$$e_l^{(l)} \geq \max_{1<\alpha\leq 2} (\alpha - 1)(H_\alpha(X|Y) - \log M). \tag{31}$$

Based on the secrecy analysis for the first layer of the scheme which is constituted of the cipher and the key extractor, we obtained equivocation of each plaintext block in Eq. (18). On the other hand, redundancy of the plaintext can be quantified in terms of entropy of the message block from which it is derived using inverse universal hashing. Random vector R is of size $n - b$ with components in the set Ω meaning that R is uniformly generated over Ω^{n-b}. For a given seed S, distribution of random vector X that is produced as $X = (A||R) \odot S^{-1}$ is determined based on the distribution of R and input A that are independent of each other. As a result,

$$P_X(X|S) = P_A(A).P_R(R) = \frac{P_A(a)}{|\Omega|^{n-b}}. \tag{32}$$

It is easy to show that output of inverse universal hashing represented by the random vector X has the same redundancy measured in terms of Rényi divergence of order α as the input to this inverse operator represented by random vector A, i.e.

$$D_\alpha(P_A||U_A) = D_\alpha(P_X||U_X). \tag{33}$$

Consequently, in the proposed scheme with cipher and generated key Q, based on Eq. (18), equivocation of the plaintext X with respect to the input message redundancy will be

$$H_\alpha(X|Y) \geq H_\alpha(Q) - D_\alpha(P_A||U_A) - \varepsilon. \tag{34}$$

Noting that random vector A has alphabet size of $M = |\Omega|^b$, it will have Rényi entropy of

$$H_\alpha(A) = \log M - D_\alpha(P_A||U_A).$$

After replacing it in Eq. (34), we see that equivocation satisfies

$$H_\alpha(X|Y) \geq H_\alpha(Q) + H_\alpha(A) - \log M - \varepsilon. \tag{35}$$

Then, substituting it in Eq. (31) gives us the desired lower bound of the secrecy exponent in Eq. (29). □

Eq. (29) indicates that the decreasing exponent of information leakage depends only on the entropy of the generated key, $H_\alpha(Q)$, uncertainty about the source message, $H_\alpha(A)$, random number generation rate, $\log M$, as well as the upper bound for output redundancy, ε. To have positive secrecy exponent for a source with the entropy of $H_\alpha(A)$, extracted key entropy for single block encryption has to be at least

$$H_\alpha(Q) \geq 2\log M + \varepsilon - H_\alpha(A). \tag{36}$$

By replacing the entropy for extracted key given in Eq. (10), and considering that $\delta - \log|\mathcal{K}| \geq \gamma$, we get the following requirement for the key size:

$$\log|\mathcal{K}| \geq 2\log M + \frac{1}{\alpha-1}e^{-(\alpha-1)\gamma} - H_\alpha(A) + \varepsilon. \tag{37}$$

This condition guarantees exponential security for highly confidential message transmission.

6.2. Secrecy exponent analysis based on L_1 distance

We adopt Eve's distinguishability that was previously used in [2] as another metric to characterize leaked information to adversary. Namely, we obtain a lower bound of the L_1 distance between the output of universal hashing function and uniform distribution for the two layer secrecy scheme, and define secrecy exponent as an indicator of how exponentially fast this distance decreases in terms of the number of transmitted blocks. Consider an ensemble of functions h_s that maps the random number $X \in \Omega^n$ to $\{1, 2, \ldots, M\}$ satisfying both universality conditions. Alice and Bob apply the same function to the common random variable X to obtain $h_s(X)$. Let $Y \in \Omega^n$ be the random variable representing Eve's knowledge where $P_{h_s(X),Y}$ denotes the joint distribution of $h_s(X)$ and Y. Let $U_{h_s(X)}$ be the uniform distribution on $\{1, 2, \ldots, M\}$. Eve's distinguishability is defined in [2] as

$$d_1(P_{h_s(X),Y}|Y) = d_1(P_{h_s(X),Y}, U_{h_s(X)} \times P_Y). \tag{38}$$

According to Eq. (2) it can be rewritten as

$$d_1(P_{h_s(X),Y}|Y) = \sum_y P_Y(y) d_1(P_{h_s(X)|Y=y}, U_{h_s(X)}). \tag{39}$$

It measures randomness of the output value of a particular hash function h_s from Eve's perspective in terms of L_1 distance from the uniform distribution, averaged over Eve's possible knowledge Y. If we average this distance over all possible seeds $S \in \mathcal{SD}$, when the resulted value is sufficiently small, we can be certain that $h_s(X)$ is independent of random variables S and Y. Thus, the generated random variable will be suitable even when we randomly choose the hash function.

In [2] it is shown that for $1 < \alpha \leq 2$

$$E_s[d_1(P_{h_s(X),Y}|Y)] \leq \min_{1<\alpha\leq 2} 3M^{\frac{\alpha-1}{\alpha}} e^{-\frac{\alpha-1}{\alpha}H_\alpha(X|Y)},$$

where E_s denotes expectation in terms of the random variable S. As a result, there exists a function h_s such that

$$d_1(P_{h_s(X),Y}|Y) \leq \min_{1<\alpha\leq 2} 3e^{-\frac{\alpha-1}{\alpha}(H_\alpha(X|Y)-\log M)}. \tag{40}$$

This equation implies that when equivocation of X is larger than the random number generation rate, $\log M$, distribution of the generated random variable $h_s(X)$ asymptotically approaches to uniformity. Consider our two layer secrecy scheme in which inverse of l-fold universal hash function $h_s^{(l)}$, using the same publicly known seed, maps a sequence of message blocks $A^{(l)}$ to a sequence of plaintext blocks $X^{(l)}$. We define decreasing exponent of L_1 distance of generated secret messages from uniform random numbers as

$$e_1^{(l)} \triangleq \lim_{l\to\infty} \frac{-\log d_1(P_{h_s^{(l)}(X^{(l)}),Y^{(l)}}|Y^{(l)})}{l}, \tag{41}$$

whose lower bound can be characterized using Theorem 5.

Theorem 5. *Let random variable A represent the message block of size b with components in the set Ω where $M = |\Omega^b|$, and Q represent the cipher key. Then, for the proposed secrecy scheme with l-fold transmission mechanism, the secrecy exponent based on L_1 distance satisfies:*

$$e_1^{(l)} \geq \max_{1<\alpha\leq 2} \frac{(\alpha-1)(H_\alpha(Q)+H_\alpha(A)-2\log M-\varepsilon)}{\alpha}. \tag{42}$$

Proof. At receiver l-fold universal hash function $h_s^{(l)}$ generates the message sequence $A^{(l)}$ that belongs to the set $\mathcal{I}$ where $|\mathcal{I}| = |\Omega^b|^l$. By using Eqs. (30) and (40) we write

$$\begin{aligned} d_1(P_{h_s^{(l)}(X^{(l)}),Y^{(l)}}|Y^{(l)}) &\leq \min_{1<\alpha\leq 2} 3e^{-\frac{\alpha-1}{\alpha}(H_\alpha(X^{(l)}|Y^{(l)})-\log|\Omega^b|^l)} \\ &= \min_{1<\alpha\leq 2} 3e^{-\frac{(\alpha-1)l}{\alpha}(H_\alpha(X|Y)-\log|\Omega^b|)}. \end{aligned}$$

For the random number generation rate of $\rho = \log M$ where $M = |\Omega^b|$, we can obtain decreasing exponent of L_1 norm based on its definition in Eq. (41) as

$$e_1^{(l)} \geq \max_{1<\alpha\leq 2} \frac{(\alpha-1)(H_\alpha(X|Y)-\log M)}{\alpha}. \tag{43}$$

Random variable X represents the plaintext blocks that are generated by the inverse universal hash operation and then encrypted using the cipher, giving them equivocation obtained in Eq. (35). Substituting it in Eq. (43) completes the proof. □

As a result, if we use the proposed key extractor to derive cipher keys, the same condition in Eq. (37) needs to hold to have information leakage in terms of variational distance or Eve's distinguishability decay exponentially to zero.

6.3. Comparison between bounds and metrics

First of all, we compare two bounds presented for the exponent of information leakage, one based on mutual information in Eq. (31) and the other one based on L_1 distance in Eq. (43). We can rewrite mutual information between X and Y in terms of KL divergence

$$I(X;Y) = D(P_{X,Y}||U_X \times P_Y). \tag{44}$$

Hence, according to the definition of secrecy exponent $e_I^{(l)}$ in Eq. (28) we shall rewrite Eq. (31)

$$\lim_{l\to\infty} -\frac{1}{l}\log D(P_{h_s^{(l)}(X^{(l)}),Y^{(l)}}||U_{h_s^{(l)}(X^{(l)})} \times P_{Y^{(l)}}) \geq \max_{1<\alpha\leq 2}(\alpha-1)(H_\alpha(X|Y)-\log M), \tag{45}$$

so by using the property in Eq. (8), the exponent for L_1 distance can be lower bounded

$$\lim_{l\to\infty} -\frac{1}{l}\log d_1(P_{h_s^{(l)}(X^{(l)}),Y^{(l)}}|Y^{(l)}) \geq \max_{1<\alpha\leq 2} \frac{(\alpha-1)(H_\alpha(X|Y)-\log M)}{2}. \tag{46}$$

However, this bound is smaller than the lower bound we used to characterize exponent of information leakage in terms of variational distance, implying that the bound in Eq. (43) is tighter than the one for mutual information in Eq. (31).

On the other hand, If we compare these two metrics, based on the equivalence of mutual information and KL-distance and inequality (8), we infer that

$$\frac{1}{2}\log I(h_s^{(l)}(X^{(l)});Y^{(l)}) \geq \log d_1(P_{h_s^{(l)}(X^{(l)}),Y^{(l)}}|Y^{(l)}). \tag{47}$$

This inequality indicates that whenever system is secure from mutual information point of view, and the left hand side is smaller than a sufficiently small number, the right hand side will also be upper bounded making information leakage in terms of variational distance negligible. Not to mention that mutual information is a stronger metric compared to L_1 distance. Nevertheless, the main reason that makes variational distance a more suitable secrecy metric from cryptographic perspective is that it simplifies formulation for practical analysis of any protocol environment and can be augmented with practical notions of secrecy like Eve's distinuishability.

7. Dual mode transmission mechanism

As discussed in previous sections the proposed secrecy scheme provides exponential secrecy if privacy amplification is applied on top of the cipher with the stipulation on the key length that is formulated in Eq. (37). It implies that there exists a trade-off such that exponential secrecy that guarantees a higher level of secrecy requires a relatively high key rate. On the other hand, only highly confidential part of the message requires exponential secrecy and a higher key rate, whereas normally it is not demanded in regular transmission. As a result, we design a dual mode transmission mechanism depicted in Fig. 4 that, depending on the demanded level of secrecy for transmission, switches to either encryption mode operating only on first layer or privacy amplification (PA) mode that jointly utilizes both secrecy layers. In other words, PA

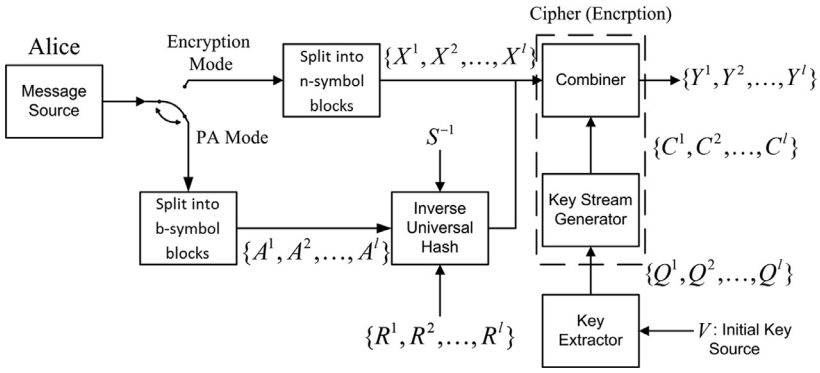

Fig. 4. Dual mode transmission with two layers of secrecy.

mode operates jointly on both encryption and privacy amplification layers to provide a higher level of secrecy based on exponential secrecy compared to lower level of secrecy based on guessing error probability that is provided by encryption mode. In this section we jointly optimize the minimum required key rate that guarantees achievable secrecy based on both optimized bounds of secrecy exponent for PA mode and the required guessing error probability for encryption mode.

For analysis, we consider a special case with binary i.i.d. message source such that $\Omega = \{0, 1\}$ where transmission unit is bit rather than symbol. For regular and efficient transmission that does not require additional security, transmission mechanism switches to encryption mode where input message is framed into n-bit blocks and then encrypted by a cipher. For this layer of secrecy, we adopt Eve's probability of failure in estimating the correct plaintext block as the secrecy criterion. Such error probability was also considered as a metric to measure security in [28,29]. As discussed in Section 5 average block error probability of Eve denoted by $P_{e,adv}$ always exceeds the required threshold P_e^{th} if the required condition for the length of the extracted key in Eq. (23) is satisfied.

In encryption mode each plaintext block is equivalent to n-bit message block. Let us represent a plaintext block with random vector $X \in \{0, 1\}^n$ whose components X_i, for $i = 1, \ldots, n$, are independently and identically generated Bernoulli random variables with $Pr(X_i = 1) = p$. It is easy to see that X has Rényi entropy of

$$H_\alpha(X) = -\frac{n}{\alpha - 1} \log[p^\alpha + (1-p)^\alpha]. \tag{48}$$

As a result, its Rényi divergence can be written as

$$D_\alpha(P_X || U_X) = n \log|\Omega| + \frac{n}{\alpha - 1} \log[p^\alpha + (1-p)^\alpha]. \tag{49}$$

Therefore, the minimum required key length for encryption mode given in Eq. (23) will be a function of p, n, P_e^{th}, α, ε and γ that we denote as $\Gamma_e(p, n, P_e^{th}, \alpha, \gamma, \varepsilon)$.

As shown in Fig. 4 when a part of message requires a higher level of secrecy, transmission mechanism switches to PA mode where the message source is encapsulated into b-bit blocks, and then a sequence of l concatenated message blocks will be mapped to a sequence of plaintext blocks using inverse universal hashing. In Section 6 we obtained the lower bound for decreasing exponent of information leakage in Eq. (29) that has to be maximized in terms of the order of Rényi entropy to have the highest possible decreasing rate for information leakage. Considering i.i.d. message source whose components are Bernoulli random variables with probability p, and extracted cipher key whose entropy is given in Eq. (10), we can obtain the lower bound for the decreasing exponent as

$$G_l(\alpha, k, p, \gamma, \varepsilon) = (\alpha - 1)(\log|\mathcal{K}| - 2\log M) - e^{-(\alpha-1)\gamma} - b\log[p^\alpha + (1-p)^\alpha] - \varepsilon, \tag{50}$$

where $\delta - \log|\mathcal{K}| \geq \gamma$. We need to maximize $G_l(\alpha, k, p, \gamma, \varepsilon)$ with respect to α where $1 < \alpha \leq 2$. As a result, the optimization problem can be formulated as

$$\max_{1<\alpha\leq 2} G_l(\alpha, k, p, \gamma, \varepsilon), \text{ for } \gamma > 0 \text{ and } G_l(\alpha, k, p, \gamma, \varepsilon) > 0. \tag{51}$$

We use numerical optimization over $1 < \alpha^* \leq 2$ and denote the optimized order as α^* and the maximized lower bound as G_l^{max}. As the secrecy requirement for PA mode, we determine a threshold for secrecy exponent as G_l^{th} and find the minimum required cipher key length for which $G_l^{max} \geq G_l^{th}$ as

$$\log|\mathcal{K}| \geq \frac{G_l^{th} + e^{-(\alpha^*-1)\gamma} + \log[p^{\alpha^*} + (1-p)^{\alpha^*}]^b + 2\log M + \varepsilon}{\alpha^* - 1} \tag{52}$$

We denote this required lower bound for the key length in PA mode as $\Gamma_{pa}(p, b, G_l^{th}, \alpha^*, \gamma, \varepsilon)$.

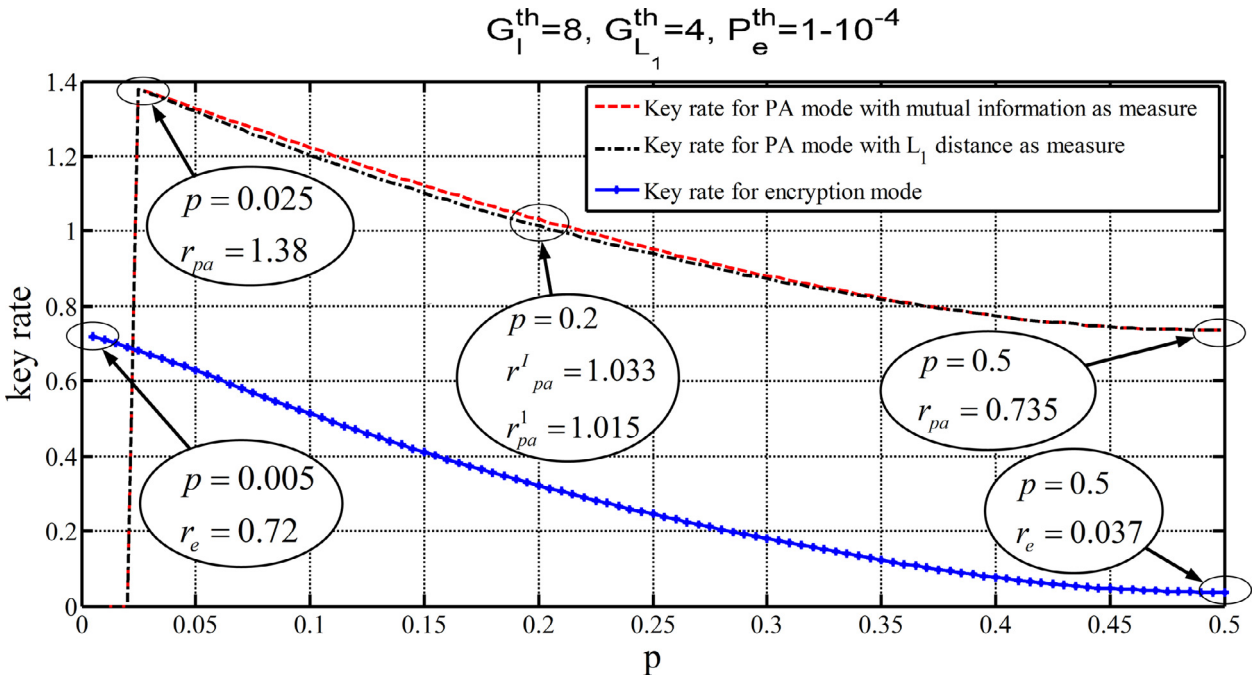

Fig. 5. Security rate in different modes with different metrics.

Considering L_1 norm distance as secrecy metric, according to Eq. (42), function G_{L_1} representing the lower bound for the decreasing exponent of information leakage turns out to be

$$G_{L_1}(\alpha, k, p, \gamma, \varepsilon) = \frac{(\alpha-1)(\log|\mathcal{K}| - 2\log M) - e^{-(\alpha-1)\gamma} - \log[p^\alpha + (1-p)^\alpha]^b - \varepsilon}{\alpha} \tag{53}$$

Similarly G_{L_1} can be maximized for $1 < \alpha \leq 2$ and $G_{L_1} > 0$. Then, for optimized α^*, if we determine the required threshold for $G_{L_1}^{max}$ as $G_{L_1}^{th}$, we can obtain the requirement for the key length to have $G_{L_1}^{max} \geq G_{L_1}^{th}$ as:

$$\log|\mathcal{K}| \geq \frac{\alpha^* G_1^{th} + e^{-(\alpha^*-1)\gamma} + \log[p^{\alpha^*} + (1-p)^{\alpha^*}]^b + \varepsilon}{\alpha^* - 1} + 2\log M. \tag{54}$$

When both modes of operations are utilized in this transmission mechanism, it is necessary to simultaneously satisfy their demanded secrecy. That allows us to use the same key stream generation rate R_s defined as $\frac{\log|\mathcal{K}|}{n}$ in both operational modes that needs to satisfy

$$R_s \geq \max\left[\Gamma_{pa}(p, b, G_I^{th}, \alpha^*, \gamma), \Gamma_e(p, n, P_e^{th}, \alpha^*, \gamma)\right]/n. \tag{55}$$

8. Optimization of dual mode mechanism based on numerical results

In this section based on the optimized bounds for the key lengths in dual mode transmission, we numerically optimize the required key generation rate for two operational modes subject to different secrecy levels that are demanded in each one. Let security rate be the minimum required key length for transmission of each message symbol or bit with the required security. In encryption mode cipher keys are generated per message block of length n-bit, hence security rate that meets the secrecy requirement is $\Gamma_e(p, n, P_e^{th}, \alpha^*, \gamma)/n$. In PA mode each generated key is applied per message block of length b-bit, therefore security rate will be $\Gamma_{pa}(b, \alpha^*, p, \gamma, G_I^{th})/b$. To compare security rate for two operational modes, we numerically optimize α by exhaustive search over $1 < \alpha \leq 2$ with step size of 10^{-4}, to obtain the maximum lower bound for secrecy exponent, and then determine the required key length and secrecy rate for each mode based on the secrecy requirement. We choose $\gamma = 5$ and use the universal hashing rate of $r_h = \frac{b}{n}$ to be 0.4. For the varying key length of $b < \log|\mathcal{K}| < 2b$, and Bernoulli parameter of $0 < p \leq 0.5$, we find α^* for which G_I and G_{L_1} are maximized. As secrecy requirement we select G_I^{th} to be 8, and $G_{L_1}^{th}$ to be half of it due to the inequality (47), meanwhile P_e^{th} is set to be $1 - 10^{-4}$. Next, for each given p, we can find the smallest $\log|\mathcal{K}|$ for which the maximized lower bound for secrecy exponent never goes below the thresholds, i.e. $G_I \geq G_I^{th}$, $G_{L_1} \geq G_{L_1}^{th}$.

Fig. 5 depicts the achievable security rate in terms of varying Bernoulli parameter $0 < p < 0.5$ for input with i.i.d. binary distribution. It shows the security rates that in PA mode satisfy the required lower bound for secrecy exponent based on

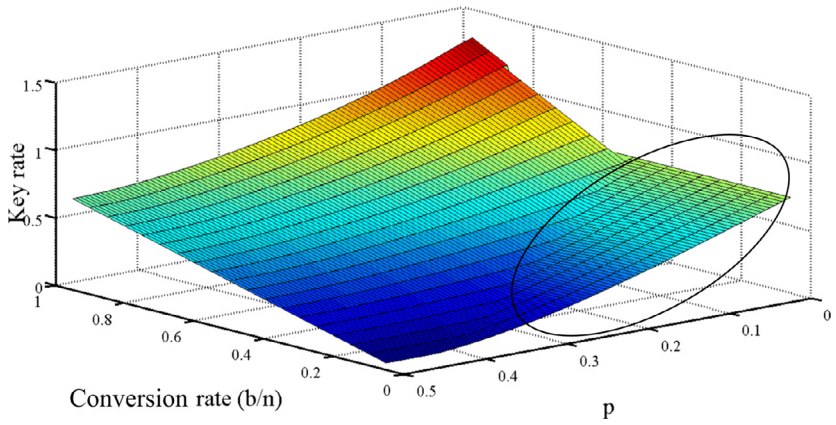

Fig. 6. Required key stream generation rate in dual mode transmission.

mutual information (denoted by r^I_{pa}) or variational distance (denoted by r^1_{pa}). It should be noted that even though here we use a new secrecy analysis for the first layer of the proposed scheme that is different than our work in [17], this figure turns out to be the same for both works. That is because the effect of the new analysis based on the new metric appears as ε in Eqs. (52) and (54) as though due to the main assumption in Eq. (17) that cipher is chosen in a way that ε has a small positive value, this effect on Γ_{pa}/b and Γ_e/n as opposed to the previous results will be ε/b and ε/n that is negligible and very close to zero. That is the main reason it does not show any change on the figure compared to our previous work.

Fig. 5 also illustrates security rate in encryption mode denoted by r_e that meets the demanded block error rate for cryptanalyst. As expected, the closer p is to 0.5 and uniformity, the smaller key length and consequently the lower secrecy rate will be needed. For instance, for uniformly distributed input with $p = 0.5$, the secrecy rate for PA mode is $r_{pa} = 0.735$ that is almost half of the required secrecy rate for $p = 0.025$. Moreover, the required security rate for PA mode is much higher than encryption mode due to its stronger secrecy requirement. As can be seen, in PA mode for $p = 0.05$ the required security rate is relatively high about 1.35 while for encryption mode it is 0.72. Note that the results obtained for both metrics in PA mode are almost the same with slight differences for $0.05 < p < 0.3$. That is because mutual information is a stronger metric compared to L_1 distance, and has a looser lower bound that will require a slightly higher security rate to meet the secrecy requirement.

Considering the scenario when both operational modes are utilized, Fig. 6, based on Eq. (55), shows how required key stream rate varies with respect to the parameter p of input binary distribution and universal hashing rate $\frac{b}{n}$. Note that low hashing rate indicates that more redundancy is added through inverse hashing. Exponential secrecy in PA mode is much stronger than the error probability metric in encryption mode, so in most areas key length is determined by the secrecy criterion in PA mode. However, in circled area the necessary key stream rate is determined based on the secrecy requirement of encryption mode. That is because for low universal hashing rate (b is much smaller than n) and low source entropy (low p) the required key length for strong secrecy of b-bit message in PA mode might not be sufficient even for weak secrecy of n-bit message in encryption mode.

9. Conclusion

In this paper, we adopted a new layering approach in design of a secure transmission mechanism with information leakage that decays at exponential rate. In our proposed two layer security scheme, a key extractor and a Shannon cipher constitute the first layer, over which a universal hashing mechanism forms the second layer for the purpose of privacy amplification. The main assumption is existence of a partially secure common source between legitimate users from which a key extracting approach that is based on a novel definition of randomness extractor derives the required key stream for the cipher. We characterized and optimized the lower bound for decreasing exponent of information leakage called secrecy exponent in terms of two metrics of mutual information and Eve's distinguishability. Under this two layer framework, a dual mode transmission mechanism is designed, with a key generation rate that is jointly optimized to provide different levels of secrecy over different operational modes, based on the required lower bound for secrecy exponent and the minimum required failure probability of attack.

Appendix A. Universality of $\odot$ multiplication in GF(q^n)

Proof. We first prove Condition 1 of universality for the function h_s defined as $h(S, X) = \text{trunc}_b[S \odot X]$. For the collision probability of this function we can write

$$Pr[S \in \mathcal{SD} : h(S, X) = h(S, X')] = Pr[S \in \mathcal{SD}, \exists R \in \Omega^{n-b} \backslash 0^{n-b} : S \odot (X \oplus X') = (0^b, R)]$$

$$\leq (q^{n-b}-1)\frac{1}{q^n-1} \leq \frac{1}{q^b}.$$

Since $X \oplus X' \neq 0$, we can find at most one $S \in \Omega^n \backslash 0^n$ for which $S \odot (X \oplus X') = (0^b, R)$ with $R \neq 0$. The last inequality holds since for $a \leq b$ we have $\frac{a-1}{b-1} \leq \frac{a}{b}$.

For the second condition consider a randomly chosen S. We can see that $h^{-1}(R,S,A) = S^{-1} \odot (A||R)$ is uniformly distributed over the preimage set $\mathcal{X}_A = \{X \in \Omega^n, h(X,S) = A\}$ which has cardinality of q^{n-b}, implying that $|h_s^{-1}(A)| = q^{n-b}$. That is because a uniformly chosen R over the set Ω^{n-b} determines which $X \in \mathcal{X}_A$ generates $(A||R)$ after multiplication by S. There exists q^b such preimage sets that are disjoint and have cardinality that does not depend on A. Contrarily, if there exists an element in both $\mathcal{X}_A$ and $\mathcal{X}_{A'}$ with $A \neq A'$, it means that $S^{-1} \odot (A||R) = S^{-1} \odot (A'||R')$. For $R \neq R'$ it is impossible to hold, but for $R = R'$ it requires that $A = A'$ which is contradictory. Therefore, $|h_s^{-1}(A)| = |\mathcal{X}_A| = q^{n-b}$ which does not depend on A. □

Appendix B. Proof of Theorem 1

Proof. It is sufficient to prove that the statement holds for $E_s H_\alpha(Q)$, where E_s denotes the expectation over S. Then, we can find a function h_s for which the inequality (10) holds. Due to convexity of the function $\frac{1}{1-\alpha}\log(.)$ for $\alpha > 1$, we can write

$$E_s H_\alpha(h_s(X)) = E_s \frac{1}{1-\alpha}\log \sum_{h_s(x)} Pr[h_s(x)]^\alpha \geq \frac{1}{1-\alpha}\log E_s \sum_{h_s(x)} Pr[h_s(x)]^\alpha, \tag{B.1}$$

where x is a realization of random variable X. We can rewrite the right hand side as

$$\sum_{h_s(x)} Pr[h_s(x)]^\alpha = \sum_{\zeta} Pr[h_s(x)=\zeta]Pr[h_s(x')=h_s(x)=\zeta]^{\alpha-1}$$

where ζ is a realization of random variable Q. If condition 2 of universality holds for the ensemble of functions h_s, it implies that preimages of different ζ's (i.e. $h_s^{-1}(\zeta)$) are distinct. Therefore, taking expectation over random variable Q is equivalent to averaging over X. For the second term in this equation the probability of occurrence of a particular ζ is equivalent to finding probability of its preimage, so we have

$$\sum_{h_s(x)} Pr[h_s(x)]^\alpha = \sum_x Pr(X=x)Pr[h_s^{-1}(\zeta)]^{\alpha-1} = \sum_x P_X(x)\left[\sum_{x':h_s(x')=h_s(x)} P_X(x')\right]^{\alpha-1}.$$

According to this equation we shall state that

$$\begin{aligned} E_s \sum_{h_s(x)} Pr[h_s(x)]^\alpha &= \sum_x P_X(x) E_s\left[\sum_{x':h_s(x')=h_s(x)} P_X(x')\right]^{\alpha-1} \\ &\leq \sum_x P_X(x)\left[E_s \sum_{x':h_s(x')=h_s(x)} P_X(x')\right]^{\alpha-1}. \end{aligned} \tag{B.2}$$

The last inequality is due to concavity of $f(x) = x^{\alpha-1}$ for $1 < \alpha \leq 2$.

$$\begin{aligned} E_s \sum_{x':h_s(x')=h_s(x)} P_X(x') &\overset{1}{=} \sum_S Pr(S=S')[Pr(x'=x) + Pr(h_s(x')=h_s(x)|x' \neq x)] \\ &\overset{2}{\leq} \sum_S P_s(S)[P_X(x) + \frac{1}{|\mathcal{K}|}] \overset{3}{=} P_X(x) + \frac{1}{|\mathcal{K}|}. \end{aligned} \tag{B.3}$$

Inequality (2) is resulted from the universality property of the family of hash functions h_s that maps $\mathcal{X}$ to the set of size $|\mathcal{K}|$. The equality 3 holds since the random variable S is uniform randomly distributed. We know that for $0 < t \leq 1$ we have $(x+y)^t \leq x^t + y^t$. Therefore

$$\left[P_X(x) + \frac{1}{|\mathcal{K}|}\right]^{\alpha-1} \leq P_X(x)^{\alpha-1} + \frac{1}{|\mathcal{K}|^{\alpha-1}}. \tag{B.4}$$

substituting Eqs. (B.2)–(B.4) into Eq. (B.1) results in

$$\begin{aligned} E_s H_\alpha(h_s(X)) &\geq \frac{1}{1-\alpha}\log \sum_x P_X(x)\left[P_X(x)^{\alpha-1} + \frac{1}{|\mathcal{K}|^{\alpha-1}}\right] \\ &= \frac{1}{1-\alpha}\log\left[\sum_x P_X(x)^\alpha + \frac{1}{|\mathcal{K}|^{\alpha-1}}\right] \\ &= \frac{1}{1-\alpha}\log\left[e^{-(\alpha-1)H_\alpha(X)} + \frac{1}{|\mathcal{K}|^{\alpha-1}}\right] \end{aligned}$$

$$= \frac{1}{\alpha-1}\log|\mathcal{K}|^{\alpha-1} - \frac{1}{\alpha-1}\log\left[1+e^{(\alpha-1)(\log|\mathcal{K}|-H_\alpha(X))}\right].$$

Finally, using the inequality $\log(1+x)\le x$ and the facts that $h_s(X)=Q$ and $H_\alpha(X)\ge\delta$ proves the statement for $E_sH_\alpha(Q)$ and hence for Eq. (10). □

Appendix C. Proof of Theorem 2

Proof. Based on the definition of two measures p_Y^* and q_Y^* we can write

$$\sum_y P_Y(y)\sum_x P_{X|Y}^{\alpha}(x|y) = \sum_y P_Y(y)^{1-\alpha}\sum_x P_{X,Y}^{\alpha}(x,y) = \gamma_{\alpha,Y}\Gamma_{\alpha,XY}\sum_y p^*(y)q^*(y).$$

So that based on the definition of the conditional Rényi entropy we get the following inequality

$$H_\alpha(X|Y) \ge \tfrac{-1}{\alpha-1}\log\Gamma_{\alpha,XY} - \tfrac{1}{\alpha-1}\log\gamma_{\alpha,XY} - \tfrac{1}{\alpha-1}\log\textstyle\sum_y p^*(y)q^*(y).$$

Based on the definition of the joint Rényi entropy in Eq. (4), we shall write

$$H_\alpha(X|Y) \ge H_\alpha(X,Y) - \tfrac{1}{\alpha-1}\log\gamma_{\alpha,Y} - \tfrac{1}{\alpha-1}\log\textstyle\sum_y p^*(y)q^*(y). \tag{C.1}$$

We first rewrite the second term in Eq. (C.1) in terms of the Rényi divergence of the ciphertext:

$$\begin{aligned}\frac{1}{\alpha-1}\log\gamma_{\alpha,Y} &= \frac{1}{\alpha-1}\log\sum_y \frac{1}{|\mathcal{Y}|^\alpha}|\mathcal{Y}|^\alpha P_Y(y)^{1-\alpha}\\ &= \frac{1}{\alpha-1}\left\{\log|\mathcal{Y}|^\alpha + \log\sum_y U_Y(y)^\alpha P_Y(y)^{1-\alpha}\right\}\\ &= \frac{\alpha}{\alpha-1}\log|\mathcal{Y}| + D_\alpha[P_Y||U_Y].\end{aligned} \tag{C.2}$$

If we use Hölder's inequality, we can get

$$\sum_y p^*(y)q^*(y) \le ||p^*(y)||_{\beta_1}||q^*(y)||_{\beta_2}, \quad \text{where} \quad \frac{1}{\beta_1}+\frac{1}{\beta_2}=1, \quad \beta_1>\beta_2>1.$$

After taking log operation from both sides, on the right hand side the first term can be written in terms of Rényi divergence

$$\begin{aligned}\log||p^*(y)||_{\beta_1} &= \log\left(\sum_y p^*(y)^{\beta_1}\right)^{\frac{1}{\beta_1}}\\ &= \frac{1}{\beta_1}\log\sum_y |\mathcal{Y}|^{1-\beta_1}\frac{1}{|\mathcal{Y}|^{1-\beta_1}}p^*(y)^{\beta_1}\\ &= \frac{1}{\beta_1}[(1-\beta_1)\log|\mathcal{Y}| + \frac{\beta_1-1}{\beta_1-1}\log\sum_y U_Y(y)^{1-\beta_1}p^*(y)^{\beta_1}]\\ &= \frac{\beta_1-1}{\beta_1}[D_{\beta_1}(p_Y^*||U_Y) - \log|\mathcal{Y}|].\end{aligned}$$

Thus, for the third term in Eq. (C.1) we shall write

$$\begin{aligned}\frac{1}{\alpha-1}\log\sum_y p^*(y)q^*(y) &\overset{1}{\le} \frac{(\beta_1-1)[D_{\beta_1}(p_Y^*||U_Y)-\log|\mathcal{Y}|]}{\beta_1(\alpha-1)} + \frac{(\beta_2-1)[D_{\beta_2}(q_Y^*||U_Y)-\log|\mathcal{Y}|]}{\beta_2(\alpha-1)}\\ &\overset{2}{\le} \frac{-1}{\alpha-1}\log|\mathcal{Y}| + \frac{\beta_1-1}{\alpha-1}\left(\frac{1}{\beta_1}D_{\beta_1}[p_Y^*||U_Y] + \frac{1}{\beta_2}D_{\beta_1}[q_Y^*||U_Y]\right).\end{aligned}$$

Inequality (2) is due to the fact that Rényi divergence is non-decreasing in order [31], and hence we have $D_{\beta_1}[q_Y^*||U_Y] \ge D_{\beta_2}[q_Y^*||U_Y]$ for $\beta_1>\beta_2$. Let us choose one of the measures p_Y^* or q_Y^* that has a larger Rényi divergence from uniformity and denote it by ρ_Y^*. As a result, the third term will satisfy the following inequality

$$\frac{1}{\alpha-1}\sum_y p^*(y)q^*(y) \le \frac{-1}{\alpha-1}\log|\mathcal{Y}| + \frac{\beta_1-1}{\alpha-1}D_{\beta_1}[\rho_Y^*||U_Y]. \tag{C.3}$$

We replace Eqs. (C.2) and (C.3) into Eq. (C.1) and define $\beta\triangleq\beta_1$, in order to obtain the equivocation for plaintext

$$H_\alpha(X|Y) \ge H_\alpha(X,Y) - \log|\mathcal{Y}| - D_\alpha[P_Y||U_Y] - \tfrac{\beta-1}{\alpha-1}D_\beta[\rho_Y^*||U_Y], \tag{C.4}$$

where ρ_Y^* is defined in Eq. (15). The goal is to see how equivocation of the plaintext depends on the entropy of the key as well as input–output distribution. Since $f(.,.)$ is a one-to-one mapping, it is easy to see that $H_\alpha(X,Y) = H_\alpha(X,C)$. But we know that the key stream C is independent of the input plaintext X implying that $H_\alpha(X,C) = H_\alpha(X) + H_\alpha(C)$. Moreover, key stream generator uses mapping rule Φ that is a bijective function and derives every key stream C from exactly one key Q and therefore does not increase entropy. Consequently, Eve's lack of knowledge about the key Q will be transformed to her uncertainty about the key stream C, i.e. $H_\alpha(C) = H_\alpha(Q)$. As a result, $H_\alpha(X,Y) = H_\alpha(X) + H_\alpha(Q)$. We can also write entropy of X in terms of Rényi divergence as $H_\alpha(X) = \log|\mathcal{X}| - D_\alpha(P_X||U_X)$. Finally, considering that $|\mathcal{X}| = |\mathcal{Y}|$, Eq. (14) can be derived from Eq. (C.4). □

References

[1] M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, IEEE Trans. Inf. Theory 57 (6) (2011) 3989–4001, doi:10.1109/TIT.2011.2110950.
[2] M. Hayashi, Tight exponential analysis of universally composable privacy amplification and its applications, IEEE Trans. Inf. Theory 59 (11) (2013) 7728–7746.
[3] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[4] I. Csiszár, J. Körner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory 24 (3) (1978) 339–348.
[5] R. Ahlswede, I. Csiszár, Common randomness in information theory and cryptography. I. Secret sharing, IEEE Trans. Inf. Theory 39 (4) (1993) 1121–1132, doi:10.1109/18.243431.
[6] A. Orlitsky, N.P. Santhanam, J. Zhang, Universal compression of memoryless sources over unknown alphabets, IEEE Trans. Inf. Theory 50 (7) (2004) 1469–1481.
[7] C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, Generalized privacy amplification, IEEE Trans. Inf. Theory 41 (6) (1995) 1915–1923.
[8] R. Renner, S. Wolf, Simple and tight bounds for information reconciliation and privacy amplification, in: Proceedings of ASIACRYPT, 2005, pp. 199–216.
[9] B. Barak, R. Shaltiel, E. Tromer, True random number generators secure in a changing environment, in: C.D. Walter, Ç.K. Koç, C. Paar (Eds.), Proceedings of 5th International Workshop, Cologne, Germany, September 8–10, 2003 on Cryptographic Hardware and Embedded Systems - CHES 2003, Springer Berlin Heidelberg, 2003, pp. 166–180, doi:10.1007/978-3-540-45238-6_14.
[10] M. Bellare, S. Tessaro, A. Vardy, Semantic security for the wiretap channel, in: Proceedings of CRYPTO, 2012, pp. 294–311.
[11] R. Canetti, Universally composable security: a new paradigm for cryptographic protocols, in: Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, 2001„ 2001, pp. 136–145, doi:10.1109/SFCS.2001.959888.
[12] H. Krawczyk, Cryptographic extraction and key derivation: the HKDF scheme, in: Proceedings of CRYPTO, 2010, pp. pp.631–648.
[13] N. Nisan, A. Ta-Shma, Extracting randomness: a survey and new constructions, J. Comput. Syst. Sci. 58 (1) (1999) 148–173.
[14] Stinson, Universal hash families and the leftover hash lemma, and applications to cryptography and computing., J. Comb. Math. Comb. Comput. 42 (2002) 3–31.
[15] M. Hayashi, T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory 62 (4) (2016) 2213–2232, doi:10.1109/TIT.2016.2526018.
[16] A. Thangaraj, S. Dihidar, A.R. Calderbank, S. McLaughlin, J. Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory 53 (8) (2007) 2933–2945.
[17] Y.S. Khiabani, S. Wei, Exponential secrecy against unbounded adversary using joint encryption and privacy amplification, in: IEEE Conference on Communications and Network Security (CNS), 2013, pp. pp.198–206.
[18] Y.S. Khiabani, S. Wei, An end-to-end exponentially secure secrecy scheme against an unbounded adversary, in: Proceedings of the 47th Annual Conference on Information Sciences and Systems (CISS), 2013, pp. pp.1–6.
[19] A. Rényi, On measures of entropy and information, in: Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability, vol. 1, 1960, pp. pp.547–561.
[20] J. Aczél, Z. Daróczy, On Measures of Information and Their Characterizations, Volume 115 of Mathematics in Science and Engineering, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1975.
[21] I. Csiszár, J. Körner, Information Theory: Coding Theorem for Discrete Memoryless Systems, Academic Press, New York, 1981.
[22] L. Carter, M.N. Wegman, Universal classes of hash functions, J. Comput. Syst. Sci. 18 (2) (1979) 143–154.
[23] M.J. Mihaljevic, H. Imai, An approach for stream ciphers design based on joint computing over random and secret data, Computing 85 (2009) 153–168.
[24] U.M. Maurer, S. Wolf, Information-theoretic key agreement: from weak to strong secrecy for free, in: Proceedings of EUROCRYPT, 2000, pp. 351–368.
[25] U. Maurer, S. Wolf, Secret-key agreement over unauthenticated public channels – part III: privacy amplification, IEEE Trans. Inf. Theory 49 (4) (2003) 839–851, doi:10.1109/TIT.2003.809559.
[26] M. Ben-Bassat, J. Raviv, Renyi's entropy and the probability of error, IEEE Trans. Inf. Theory 24 (3) (1978) 324–331, doi:10.1109/TIT.1978.1055890.
[27] A. Teixeira, A. Matos, L. Antunes, Conditional Rényi entropies, IEEE Trans. Inf. Theory 58 (7) (2012) 4273–4277, doi:10.1109/TIT.2012.2192713.
[28] R. Ahlswede, G. Dueck, Bad codes are good ciphers, Problems Control Inf. Theory 11 (5) (1982) 337–351.
[29] S.-C. Lu, Random ciphering bounds on a class of secrecy systems and discrete message sources, IEEE Trans. Inf. Theory 25 (4) (1979) 405–414.
[30] D.R. Stinson, Universal hashing and authentication codes, Des. Codes Cryptogr. 4 (4) (1994) 369–380.
[31] T. van Erven, P. Harremos, Rényi divergence and Kullback–Leibler divergence, IEEE Trans. Inf. Theory 60 (7) (2014) 3797–3820, doi:10.1109/TIT.2014.2320500.