Mathematical Problems of Computer Science 42, 17–27, 2014.

# Information Theoretical Analysis of Biometric Generated Secret Key Sharing Model

Mariam E. Haroutunian[1] and Narek S. Pahlevanyan[2]

[1]Institute for Informatics and Automation Problems of NAS RA
[2]Gyumri State Pedagogical Institute
e-mail: armar@ipia.sci.am, narek@ravcap.com

**Abstract**

We investigate the biometric generated secret key sharing system. We consider the generalization of the secret key rate, studied by Ignatenko and Willems [1]: the notion of $E$-achievable secret key rate is introduced. The lower and upper bounds for the largest $E$-achievable secret key rate are obtained. When $E$ tends to zero, the limits of our bounds coincide and are equal to the largest achievable secret key rate stated in [1].

**Keywords:** Biometric systems, Generated secret key, $E$-achievable rate, Achievable secret rate.

## 1. Introduction

In recent years the biometric secrecy systems are being widely used, ranging from border control at airports to access control in various systems such as computer log-in, ID cards, e-passports. The purpose of using biometric secrecy systems is to avoid a lot of related problems with the usage of traditional passwords. For instance, simple passwords can be easily guessed or broken by brute-force attacks, while more complex passwords are difficult to remember. Furthermore, when a single password is compromised, it may open many other "gates", because most people use the same password for authentication in different locations. Finally, a password can be shared with another person and there will be no way to know who the actual user is.

The above mentioned limitations can be solved, if the biometric secrecy systems would be used to authenticate an individual. Besides, the authentication biometric secrecy systems can be used in identification, examinations, payment processings and in other various applications. Such systems are more secure than the traditional password-based authentication systems, because the biometric properties cannot be lost or forgotten, they are difficult to falsify or duplicate, share, and distribute. In many applications, such as, examinations, the person is required to be present at the time and point of authentication. Moreover, there are access scenarios, which require a participation of multiple previously registered users for a successful authentication or to get an access grant for a certain entity. For instance, there are cryptographic constructions known as secret sharing schemes, where a secret key is split into shares and distributed amongst the users in such a way that it can be reconstructed only when the necessary number of secret key holders comes together. The revealed secret can then be used for encryption or authentication. One of such applications could be sharing of a bank account by family members.

However, the usage of biometric secrecy systems has its own disadvantages. As the biometric data are gathered from individuals under environmental conditions and the channels are exposed to noise the biometric secrecy system may accept an impostor or reject an authorized individual. Basically, it's not possible to build an ideal biometric secrecy system, it can be information-theoretical secure up to a certain level.
Ignatenko and Willems [1] have mentioned that a perfect system for a secure biometric authentication has to satisfy three requirements. Firstly, biometric data have to be private, that means the reference information stored in database should not reveal the actual biometric data. Secondly, reference data that are communicated from a database to the place where an access can be granted or denied have to be fault-tolerant to eavesdropping. And finally reference data stored in database have to be resilient to brute-force attacks.
Nonetheless, as practice shows people do not feel comfortable in providing their biometric information to a large amount of outwardly secure databases, because one cannot fully trust the security implementations of third parties, another reason is that the database might be compromised from inside, which will allow an owner of a database to misuse biometric information. And finally people have limited biometric resources, so "identity theft" has much more serious impacts than a "simple" theft of a credit card.

In this paper we revisit the problem of generating secret keys from biometric data provided in [1]. We introduce the notion of $E$-achievable secret key rate and obtain the lower and upper bounds for the largest $E$-achievable secret key rate. When $E$ tends to zero, the limits of our results coincide with the largest achievable secret key rate defined in [1].

## 2. Related Work

Security concerns related to the use of biometric data in different secrecy systems were raised a long time ago. From the information-theoretical perspective the biometric secrecy systems were studied by O'Sullivan and Schmid [2] and Willems et al [3]. Willems [3] investigated the fundamental properties of the biometric identification system. It has been shown that it is impossible to reliably identify more persons than capacity which is an inherent characteristic of any identification system. By analogy with notion of $E$-capacity or rate-reliability function introduced for discrete memoryless channels by E. Haroutunian [4] in [5] the new concept of identification $E$-capacity for biometrical identification system was introduced. The authors derived the upper and lower bounds of biometric identification system. Later in [6] the authors investigated the rate-reliability function for biometric identification protocol with a random parameter.

The problem of generating secret keys from biometric data is closely related to the concept of secret sharing, which was introduced by Maurer [7] and by Ahlswede and Csiszar [8]. This problem in biometric setting was considered by Ignatenko and Willems [1]. Unlike in traditional secret key sharing, where the secret key is being generated and shared between terminals, in biometric secrecy systems a secret key is generated during an enrollment procedure in which the biometric data are observed for the first time. The secret key is to be reconstructed after these biometric data are observed again, during an attempt to get an access. Reliable biometric secrecy systems extract helper data from the biometric information at the time of enrollment, as biometric measurements are typically noisy. These helper data contribute to reliable reconstruction of the secret key. The detailed description of this model is given in the next section. More detailed review on information-theoretic approaches of biometric secrecy systems can be found in [9].

## 3. Biometric Generated Secret Key Sharing Model

Before we start introducing the model let's define some conventions that are applied within this paper. Capital letters are used for random variables (RV) $X, Y$ taking values in the finite alphabets $\mathcal{X}, \mathcal{Y}$, correspondingly. The cardinality of the alphabet $\mathcal{X}$ is denoted by $|\mathcal{X}|$. Biometric generated secret key sharing is one of the available models of biometric secret key sharing system. The model is represented in Figure1.

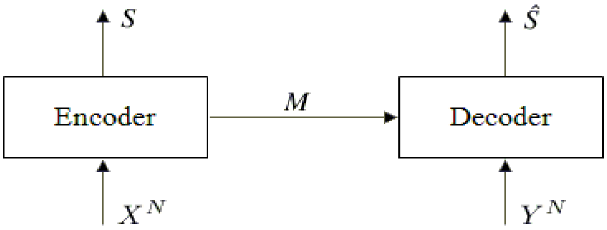

Fig. 1. Biometric generated secret key sharing model.

The model is based on a biometric source with distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. This source produces $\mathbf{x} \equiv x^N = (x_1, x_2, ..., x_N)$ of $N$ symbols from the finite alphabet $\mathcal{X}$ and a second sequence $\mathbf{y} \equiv y^N = (y_1, y_2, ..., y_N)$ of $N$ symbols from the finite alphabet $\mathcal{Y}$. The first sequence is called an enrollment sequence, and the second sequence an authentication sequence. Furthermore, the second sequence $Y^N$ is a noisy version of the first sequence $X^N$. Let us denote

$$Q(x,y) = Q_1(x)Q_2(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}.$$

We assume that

$$Q^N(\mathbf{x},\mathbf{y}) = \prod_{n=1}^{N} Q(x_n, y_n).$$

Then consider an encoder that explores the enrolment sequence $X^N$. From this sequence in biometric generated secret key sharing model the encoder generates a secret $S \in \{1, 2, ..., |S|\}$ and then a public helper-message (helper data) $M \in \{1, 2, ..., |M|\}$. That means that

$$f(X^N) = (S, M),$$

where by $f(\cdot)$ we denote the encoder function. The helper-message is sent to the decoder.

The decoder explores the authentication sequence $Y^N$ and produces an estimate $\hat{S}$ of the secret $S$ using the received helper data $M$, hence

$$g(Y^N, M) = \hat{S},$$

where by $g(\cdot,\cdot)$ we denote the decoder function. The channel between the encoder and the decoder is expected to be public. We assume that an attacker has an access to that channel, so he can see all the public information but cannot modify. The information outflow is described in terms of mutual information, and the size of the secret key– in terms of entropy. Fingerprints and irises can be modeled as such biometric sources.

The important parameters of a biometric secrecy system include the size of secret key and the information that the helper data leak on the biometric observation. That leak of biometric information is called a privacy leakage. The privacy leakage should be small, to avoid the biometric data of an individual to become compromised. Moreover, the secret key length should be large to minimize the probability that the secret key is guessed. It is the goal of both sides (encoder and decoder) to produce a secret key as large as possible, that satisifies this condition $\Pr\{S \neq \hat{S}\} \approx 0$ , this means that probability that the estimated secret $\hat{S}$ is not equal to the generated secret $S$ is close to zero. The biometric generated secret key sharing model must satisfy the following requirements [1]

$$\begin{aligned}\Pr\{S \neq \hat{S}\} \approx 0 \quad & \text{(reliability)},\\ \frac{1}{N}H(S) \approx \frac{1}{N}\log_2|S| \quad & \text{(secret uniformity)},\\ \frac{1}{N}H(S) \text{ is as large as possible} \quad & \text{(secret key rate)},\\ \frac{1}{N}I(S \wedge M) \approx 0 \quad & \text{(secrecy leakage)},\\ \frac{1}{N}I(X^N \wedge M) \text{ is as small as possible} \quad & \text{(privacy leakage)}.\end{aligned}$$

Here is a definition for the achievable secret key rate stated in [1]. A secret key rate $R$, for $R \geq 0$, is called achievable if for all $\delta > 0$ and all $N$ large enough, there exist encoders and decoders such that

$$\Pr\{S \neq \hat{S}\} \leq \delta,$$

$$\frac{1}{N}H(S) + \delta \geq \frac{1}{N}\log_2|S| \geq R - \delta,$$

$$\frac{1}{N}I(S \wedge M) \leq \delta.$$

Ahlswede and Csiszár [8] proposed and proved a theorem, which stated that for a source type model the largest achievable secret key rate $R$ is equal to mutual information $I(X \wedge Y)$. Unlike the original proof, which is based on strong typicality, another proof of the same theorem, but for biometric generated secret model, using weak typicality is given in [1]. In the next section we will introduce new concept of $E$-achievable secret key rate, which differs from traditional secret key rate by having a more solid requirement and exponentially decreases the error probability in practice.

## 4. $E$-achievable Secret Key Rate

**Definition:** *A secret key rate $R(E)$, for $R(E) \geq 0$, is called $E$-achievable if for all $\delta > 0$ , $E > 0$ and $N$ large enough, there exists a code such that*

$$\Pr\{S \neq \hat{S}\} \leq 2^{-N(E-\delta)},$$

$$\frac{1}{N}H(S) + \delta \geq \frac{1}{N}\log_2|S| \geq R(E) - \delta,$$

$$\frac{1}{N}I(S \wedge M) \leq \delta.$$

We shall use the following PD in the formulation of result:

$$Q_1 = \{Q_1(x), x \in \mathcal{X}\}, Q_2 = \{Q_2(y|x), y \in \mathcal{Y}, x \in \mathcal{X}\},$$

$$P_1 = \{P_1(x), x \in \mathcal{X}\}, P_2 = \{P_2(y|x), y \in \mathcal{Y}, x \in \mathcal{X}\},$$

$$Q = \{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\},$$

$$P = \{P(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}.$$

We refer to [4] , [10] , [11] and [12] for notions of divergence $D(P||Q)$ , mutual information $I_P(X \wedge Y)$ , information-theoretic quantities. The proofs are based on the method of types. We denote by $\mathcal{T}^N_{P_1}(X)$ the set of vectors $\mathbf{x}$ of type $P_1$, by $\mathcal{T}^N_P(X,Y)$ the set of vectors $(\mathbf{x},\mathbf{y})$ of type $P$. We use some known properties [4], [10], [11], [12].

For $(\mathbf{x},\mathbf{y}) \in \mathcal{T}^N_P(X,Y)$

$$Q^N(\mathbf{x},\mathbf{y}) = \exp\{-N(H_P(X,Y) + D(P||Q))\}, \tag{1}$$

$$|\mathcal{T}^N_P(X,Y)| \leq \exp\{NH_P(X,Y)\}, \tag{2}$$

$$Q^N(\mathcal{T}^N_P(X,Y)) \leq \exp\{-ND(P||Q)\}, \tag{3}$$

$$D(P||Q) = D(P_1||Q_1) + D(P_2||Q_2|P_1). \tag{4}$$

Our main result is stated in the following theorem.

**Theorem:** *For biometric generated-secret model the largest $E$-achievable secret key rate $R(E)$ is lower bounded by*

$$R_r(E) = \min_{P:D(P||Q)\leq E} |I_P(X \wedge Y) + D(P||Q) - E|^+ \tag{5}$$

and upper bounded by

$$R_{sp}(E) = \min_{P:D(P||Q)\leq E} I_P(X \wedge Y). \tag{6}$$

Here the notation $|a|^+$ is used for max$(a, 0)$.

**Corollary:** *When $E \to 0$, the limits of our bounds coincide and are equal to the largest achievable secret key rate defined in [1]:*

$$\lim_{E\to 0} R_r(E) = \lim_{E\to 0} R_{sp}(E) = I_Q(X \wedge Y).$$

## 5. Proof of Theorem

**Proof of Upper Bound.**

Let $E > 0$ and the error probability satisfy the condition $\Pr\{S \neq \hat{S}\} \leq \exp\{-N(E-\delta)\}$. It means that

$$\sum_{\mathbf{x}\in X^N} Q_1^N(\mathbf{x}) \frac{1}{|S|} \sum_{s\in S} Q_2^N \left\{ Y^N - g_m^{-1}(s) \middle| \mathbf{x}_m(s) \right\} \leq \exp\{-N(E-\delta)\},$$

where

$$g_m^{-1}(s) = \{\mathbf{y} : g_m(\mathbf{y}) = s\}.$$

For any $P$ we can write

$$\sum_{s\in S} \sum_{\mathbf{x}_m(s)\in\mathcal{T}_{P_1}^N(X)} Q_1^N(\mathbf{x}_m(s)) \times Q_2^N\Big\{\mathcal{T}_P^N(Y|\mathbf{x}_m(s)) - g_m^{-1}(s)\Big|\mathbf{x}_m(s)\Big\} \leq$$

$$|S|\exp\{-N(E-\delta)\}.$$

$Q_1^N(\mathbf{x}_m(s))$ and $Q_2^N(\mathbf{y}|\mathbf{x}_m(s))$ are constant for various $\mathbf{x}$ and $\mathbf{y}$ of fixed type $P$, hence, we can write

$$\sum_{s\in S} \sum_{\mathbf{x}_m(s)\in\mathcal{T}_{P_1}^N(X)} \Big\{\Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\Big| - \Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\bigcap g_m^{-1}(s)\Big|\Big\}\times$$

$$Q_1^N(\mathbf{x}_m(s)) \times Q_2^N(\mathbf{y}|\mathbf{x}_m(s)) \leq |S|\exp\{-N(E-\delta)\}.$$

According to (3)

$$\sum_{s\in S} \sum_{\mathbf{x}_m(s)\in\mathcal{T}_{P_1}^N(X)} \Big\{\Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\Big| - \Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\bigcap g_m^{-1}(s)\Big|\Big\}\times$$

$$\exp\{-N(D(P||Q) + H_{P_2}(Y|X))\} \leq |S|\exp\{-N(E-\delta)\}. \tag{7}$$

It follows from the definition of decoding function $g$ that for the given $m$ the sets $g_m^{-1}(s)$ are disjoint, therefore

$$\sum_{s\in S} \Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\bigcap g_m^{-1}(s)\Big| \leq |\mathcal{T}_P^N(Y)|.$$

Then from (7) we have

$$\sum_{s\in S} \Big|\mathcal{T}_P^N(Y|\mathbf{x}_m(s))\Big| - \frac{|S|\exp\{-N(E-\delta)\}}{\exp\{-N(D(P||Q) + H_P(Y|X))\}} \leq |\mathcal{T}_P^N(Y)|.$$

Hence,

$$|S| \leq \frac{\exp\{NI_P(X\wedge Y)\}}{(N+1)^{-|X||Y|} - \exp\{N(D(P||Q) - E - \delta)\}}.$$

The right-hand side of this inequality can be minimized by the choice of $P$ keeping the denominator positive, which takes place for large $N$, when $D(P||Q) \leq E - \delta$.

**Achievability part of theorem.**

**Code Construction.** We consider those types $P$ that $D(P||Q) \leq E$, from (4) it follows that

$$D(P_1||Q_1) \leq E \text{ and } D(P_2||Q_2|P_1) \leq E.$$

Let us denote

$$\mathcal{T}_{Q_1}^N(E) = \bigcup_{P_1:D(P_1||Q_1)\leq E} \mathcal{T}_{P_1}^N(X),$$

$$\mathcal{T}_Q^N(E) = \bigcup_{P:D(P||Q)\leq E} \mathcal{T}_P^N(X,Y).$$

We define a random partition of $\mathcal{T}_{Q_1}^N(E)$ into $|\mathcal{M}|$ bins. The encoder independently assigns a helper label (index of the bin) $m \in \{1, 2, ...|\mathcal{M}|\}$ to each sequence $\mathbf{x}$ with the probability

$$\Pr\{M(\mathbf{x}) = m\} = 1/|\mathcal{M}|.$$

Then we define a second random partition over $\mathcal{T}_{Q_1}^N(E)$ with $|\mathcal{S}|$ bins, and the encoder assigns a random label (bin-index of this second partition) $s \in \{1, 2, ...|\mathcal{S}|\}$ to each sequence $\mathbf{x}$ with the probability

$$\Pr\{S(\mathbf{x}) = s\} = 1/|\mathcal{S}|.$$

The encoder explores the sequence $\mathbf{x}$ and determines the secret label $s$ and helper label $m$. The encoder sends the helper label $m$ to the decoder.
The decoder after having observed $\mathbf{y}$ sequence looks for a unique sequence $\mathbf{x}$ with the helper label $m$ such that $(\mathbf{x}, \mathbf{y}) \in \mathcal{T}_P(X, Y)$ and $D(P||Q)$ is minimal.

**Error probability.** From (3) we obtain that for any $P$ such that $D(P||Q) > E$ the probability of the event is small enough

$$Q^N(\mathcal{T}_P^N(X, Y)) \leq \exp\{-NE\}. \tag{8}$$

The decoder can make an error if for the given $m$ the secret $s$ was determined, but there exists $\hat{s} \neq s$, such that for some $\hat{P}$

$$(\mathbf{x}_m(s), \mathbf{y}_m) \in \mathcal{T}_P(X, Y), (\hat{\mathbf{x}}_m(\hat{s}), \mathbf{y}_m) \in \mathcal{T}_{\hat{P}}(X, Y)$$

and

$$D(\hat{P}||Q) \leq D(P||Q).$$

The mathematical expectation of this event can be upper bounded by the following expression:

$$\sum_{P,\hat{P}: D(\hat{P}||Q) \leq D(P||Q)} \sum_{\hat{s} \neq s} \sum_{\mathbf{x} \in \mathcal{X}^N} \sum_{\mathbf{y} \in \mathcal{Y}^N} Q^{\mathrm{N}}(\mathbf{x}, \mathbf{y}) \times$$

$$\Pr\{(\mathbf{x}_m(s), \mathbf{y}_m) \in \mathcal{T}_P^N(X, Y)\} \times \Pr\{(\hat{\mathbf{x}}_m(\hat{s}), \mathbf{y}_m) \in \mathcal{T}_{\hat{P}}^N(X, Y)\}.$$

The first probability is different from zero only if $\mathbf{x} \in \mathcal{T}_{P_1}^N(X)$ and $\mathbf{y} \in \mathcal{T}_P^N(Y)$. Hence, the expression will have the following form:

$$\sum_{P,\hat{P}: D(\hat{P}||Q) \leq D(P||Q)} \sum_{\hat{s} \neq s} \sum_{\mathbf{x} \in \mathcal{T}_{P_1}^N(X)} \sum_{\mathbf{y} \in \mathcal{T}_P^N(Y)} Q^{\mathrm{N}}(\mathbf{x}, \mathbf{y}) \times$$

$$\Pr\{(\mathbf{x}_m(s), \mathbf{y}_m) \in \mathcal{T}_P^N(X, Y)\} \times \Pr\{(\hat{\mathbf{x}}_m(\hat{s}), \mathbf{y}_m) \in \mathcal{T}_{\hat{P}}^N(X, Y)\}.$$

Taking into account that for any $\hat{P}$

$$|S| - 1 \leq \exp\{N(I_{\hat{P}}(X \wedge Y) + D(\hat{P}||Q) - E - \delta_1)\}$$

and (1), (2) the last expression will not be greater than

$$\sum_{P,\hat{P}: D(\hat{P}||Q) \leq D(P||Q)} \exp\{N(I_{\hat{P}}(X \wedge Y) + D(\hat{P}||Q) - E - \delta_1)\} \times$$

$$\exp\{-N(H_P(X, Y) + D(P||Q))\} \times \exp\{N(H_P(X) + H_P(Y))\} \times$$

$$\exp\{-N(I_P(X \wedge Y) - \delta_2)\} \times \exp\{-N(I_{\hat{P}}(X \wedge Y) - \delta_3)\} = \sum_{P,\hat{P}:D(\hat{P}||Q)\leq D(P||Q)} \exp\{N(D(\hat{P}||Q) - E - (\delta_1 + \delta_2 + \delta_3))\}\times \exp\{-ND(P||Q)\} \leq \exp\{-N(E - \delta')\}. \tag{9}$$

Then from (8) and (9) we state that for $N$ large enough there exists a code with labelings $M$ and $S$ such that

$$\Pr\{S \neq \hat{S}\} \leq \exp\{-N(E - \delta')\} + \exp\{-NE)\} \leq \exp\{-N(E - \delta)\}.$$

For the rest of the proof we state that since $\Pr\{S \neq \hat{S}\} \leq \exp\{-N(E - \delta)\}$ for $N$ large enough, there exists at least one pair of labelings $M, S$, such that

$$H(M) \leq \log|M| = N \max_{P:D(P||Q)\leq E}(H_P(X|Y) - D(P||Q) + E + \epsilon_1). \tag{10}$$

$$H(S) \leq \log|S| = N \min_{P:D(P||Q)\leq E}(I_P(X \wedge Y) + D(P||Q) - E - \epsilon_2). \tag{11}$$

**Uniformity.** Let $\hat{X}^N$ be the estimate of $X^N$ based on $S$ and $M$, then we find that

$$H(X^N) = H(X^N, S, M) = H(S) + H(M|S)+ H(X^N|S, M) \leq H(S) + H(M) + H(X^N|S, M, \hat{X}^N) \leq H(S) + H(M) + NP_e \log|\mathcal{X}| + 1,$$

the last step follows from Fano's inequality. Hence, from (10) and (11) we have

$$H(S) \geq H(X^N) - H(M) - NP_e \log|\mathcal{X}| - 1 \geq NH(X) - N \max_{P:D(P||Q)\leq E}(H_P(X|Y) - D(P||Q) + E + \epsilon)- N\exp\{-N(E - \delta)\}\log|\mathcal{X}| - 1 \geq \log|\mathcal{S}| - N(\epsilon_1 - \epsilon_2) - N\exp\{-N(E - \delta)\}\log|\mathcal{X}| - 1.$$

**Secrecy.** Now we study the secrecy.

$$I(S \wedge M) = H(S) + H(M) + H(S, M) = H(S) + H(M) - H(S, M, X^N) + H(X^N|S, M) = H(S) + H(M) - H(X^N) + H(X^N|S, M, \hat{X}^N) \leq H(S) + H(M) - NH(X) + NP_1 \log|\mathcal{X}| + 1.$$

From (10) and (11) we obtain

$$H(S) + H(M) - NH(X) + NP_1 \log|\mathcal{X}| + 1 \leq N(\min_{P:D(P||Q)\leq E} I_P(X \wedge Y) + \max_{P:D(P||Q)\leq E} H_P(X|Y) - H(X))+ N(\epsilon_1 - \epsilon_2) + N\exp\{-N(E - \delta)\}\log|\mathcal{X}| + 1.$$

Finally, we see that the secrecy leakage is small for $N$ large enough

$$\frac{1}{N}I(S \wedge M) \leq \exp\{-N(E - \delta)\}\log|\mathcal{X}| + (\epsilon_1 - \epsilon_2) + \frac{1}{N}.$$

The theorem is proved.

## 6. Privacy Leakage

The following proposition gives the privacy leakage corresponding to the maximum $E$-achievable secret key rate in the biometric generated secret key sharing model.

**Proposition:** *In a biometric generated secret key sharing model for $E$-achievable secret key rate the privacy leakage is*

$$\frac{1}{N} I_{Q_1}(M \wedge X^N) = \max_{P: D(P||Q) \leq E} (H_P(X|Y) + D(P||Q) - E). \tag{12}$$

**Proof:** As $M$ is a function of $X^N$ we have from (11)

$$\begin{gathered} I(X^N \wedge M) = H(M) \geq H(X^N) - H(S) - NP_e \log|\mathcal{X}| - 1 \geq \\ NH_{Q_1}(X) - N \min_{P: D(P||Q) \leq E} (I_P(X \wedge Y) + D(P||Q) - E - \epsilon_2) - \\ N2^{-N(E-\delta)} \log|\mathcal{X}| - 1 \geq \\ N \max_{P: D(P||Q) \leq E} (H_P(X|Y) + D(P||Q) - E - \epsilon_2) - \\ N2^{-N(E-\delta)} \log|\mathcal{X}| - 1. \end{gathered}$$

On the other hand from (10)

$$H(M) \leq N \max_{P: D(P||Q) \leq E} (H_P(X|Y) - D(P||Q) + E + \epsilon_1).$$

Dividing both sides by N, and for $N \to \infty$ we obtain (12).

**Remark:** *The above proposition gives the privacy leakage if we apply the coding scheme outlined in the achievability proof. However, it may be possible to achieve a smaller privacy leakage depending on the secret-key rate. This problem will be considered in the future work.*

## 7. Conclusion

We studied the biometric generated-secret model for discrete i.i.d biometric sources. The new concept of $E$-achievable secret key rate is introduced and the expressions for the lower and upper bounds of largest rate are obtained. This notion is the generalization of the achievable secret key rate as it tends to the last when $E$ tends to zero. The proofs are based on the strong typicality. Also an expression for privacy leakage, which corresponds to the largest $E$-achievable secret key rate is obtained.

## References

[1] T. Ignatenko and F. M. Willems, “Biometric security from an information-theoretical perspective,” *Foundations and Trends in Communications and Information Theory*, vol. 7, no. 2-3, pp. 135–316, 2012.

[2] J. A. O’Sullivan and N. A. Schmid, “Large deviations performance analysis for biometrics recognition”, *Proc. 40th Annual Allerton Conf. on Communication, Control, and Computing*, pp. 1–10, Oct. 2002.

[3] F. Willems, T. Kalker, J. Goseling and J.-P. Linnartz, "On the capacity of a biometrical identification system," in *Information Theory, 2003. Proceedings. IEEE International Symposium on Information Theory*, Yokohama, Japan, 2003, p. 82.

[4] E. Haroutunian, "On bounds for $E$-capacity of DMC," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4210–4220, 2007.

[5] M. Haroutunian , A. Muradyan and L. Ter-Vardanyan, "Upper and lower bounds of biometric identification $E$-capacity, " *Transactions of IIAP of NAS of RA, Mathematical Problems of Computer Science*, vol. 36, pp. 1–10, 2012.

[6] M. Haroutunian and L. Ter-Vardanyan, "Investigation of $E$-capacity for biometric identification protocol with random parameter," *Transactions of IIAP of NAS of RA, Mathematical Problems of Computer Science*, vol. 39, pp. 88–93, 2013.

[7] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[9] Y. Chen and A. H. Vinck, "From password to biometrics: How far can we go," *Proceidings 7th Asia-Europe Workshop on Concepts in Information theory*, Boppard, Germany, pp. 1–8, 2011.

[10] E. A. Haroutunian, M. E. Haroutunian and A. N. Harutyunyan, "Reliability criteria in information theory and in statistical hypothesis testing," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 2-3, pp. 97–263, 2008.

[11] I. Csiszar, "The method of types," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505–2523, 1998.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory, 2nd Edition*, New York, Wiley-Interscience, 2006.

**Submitted 15.08.2014, accepted 22.11.2014.**

## Գեներացված գաղտնի բանալի փոխանակող կենսաչափական մոդելի ինֆորմացիոն-տեսական հետազոտություն

Մ. Հարությունյան և Ն. Փահլևանյան

### Ամփոփում

Հետազոտվում է գեներացված գաղտնի բանալի փոխանակող կենսաչափական համակարգը: Ներմուծվել է գաղտնիքի $E$ հասանելի արագություն նոր հասկացությունը, որն ընդհանրացնում է Իգնատենկոյի և Վիլեմսի [1] ուսումնասիրած գաղտնիքի հասանելի արագության գաղափարը: Կառուցվել են գաղտնիքի $E$ հասանելի առավելագույն արագության վերին և ստորին գնահատականները: Երբ $E \to 0$, ստացված գնահատականների սահմանները համընկնում են և հավասար են [1]-ում ստացած գաղտնի բանալուհասանելի արագության մեծագույն արժեքին:

# Информационно-теоретический анализ биометрической модели распределения сгенерированного секретного ключа

М. Арутюнян и Н. Пайлеванян

## Аннотация

Рассматривается биометрическая система распределения сгенерированного секретного ключа. Вводится новое понятие $E$-достижимой скорости секрета, которое является обобщением достижимой скорости секрета, изученной Игнатенко и Вилемсом в [1]. Построены верхняя и нижняяграницынаибольшей $E$-достижимой скорости секрета. Когда $E \to 0$, пределыполученных границ совпадают с наибольшей достижимой скоростью секретного ключа, полученной в [1].