entropy

MDPI

Article

# Normalized Unconditional $\epsilon$-Security of Private-Key Encryption

**Lvqing Bi [1], Songsong Dai [2,*] and Bo Hu [3]**

[1] School of Electronics and Communication Engineering, Yulin Normal University, Yulin 537000, China; bilvqing108@163.com
[2] School of Information Science and Engineering, Xiamen University, Xiamen 361005, China
[3] School of Mechanical and Electrical Engineering, Guizhou Normal University, Guiyang 550025, China; hb.gznu@gmail.com
* Correspondence: ssdai@stu.xmu.edu.cn; Tel.: +86-592-258-0135

Academic Editors: Rafael F. Schaefer, Eduard A. Jorswieck and Stefano Tomasin
Received: 12 January 2017; Accepted: 1 March 2017; Published: 7 March 2017

**Abstract:** In this paper we introduce two normalized versions of non-perfect security for private-key encryption: one version in the framework of Shannon entropy, another version in the framework of Kolmogorov complexity. We prove the lower bound on either key entropy or key size for these models and study the relations between these normalized security notions.

**Keywords:** unconditional security; entropy; kolmogorov complexity; private-key encryption

## 1. Introduction

Shannon entropy $\mathrm{H}(X)$ [1]—known as information theory—is a measure of the average uncertainty in the random variable $X$. Perfect secrecy [2] is a strong security notion which means that the ciphertext leaks no information about the plaintext. Shannon first formally studied this notion using information theory, and defined perfect secrecy as the mutual information between the plaintext $X$ and ciphertext $Y$ being zero; i.e., $\mathrm{I}(X;Y) = 0$. The mutual information $\mathrm{I}(X;Y)$ is a measure of the dependence between the two random variables. In this view, perfect secrecy requires the independence between the plaintext $X$ and ciphertext $Y$. Perfect secrecy can be achieved by one-time pad (Vernam) cipher [3], but it requires that the key space must be at least as large as the message space; i.e., $\mathrm{H}(X) \geq \mathrm{H}(Y)$. A number of authors have considered alternative definitions of secrecy to achieve more practical cryptosystems. A number of papers [4–6] considered the notion of non-perfect security—$\epsilon$-secrecy—which allows a small amount of information leakage about the plaintext after viewing the ciphertext; i.e., $\mathrm{I}(X;Y) \leq \epsilon$. Dodis [7] considered the $\epsilon$-security with a completeness error, which allows the decryption to have some small error. Several other notions of secrecy [5,6,8] have been proposed by using other entropy measures, such as min-entropy, conditional min-entropy, Rényi entropy, and conditional Rényi entropy instead of Shannon entropy. However, the security parameter $\epsilon$ in [7] is not proper to measure the security level of private-key encryption scheme. As we know, 10 leaked bits is a large amount of information leakage for a 100-bit message, but is small for a 10,000-bit message. However, using the security notion of [7], they have the same level of security. The problem is that the security notion of [7] deals with the absolute amount of information leakage rather than with the relative amount of information leakage. So, in this paper, we propose a notion of normalized $\epsilon$-Shannon security, which is a normalized version of Shannon entropy-based security for a private-key encryption scheme. The new security parameter $\epsilon$ is the information leak ratio; i.e., $\mathrm{I}(X;Y)$ divided by $\mathrm{H}(X)$. This is also a relative amount of information leakage for messages.

Kolmogorov complexity $\mathrm{K}(x)$ [9–11]—known as algorithmic information theory [12,13]—measures the quantity of information in a single string $x$ by the size of the smallest program that generates it.

Antunes et al. [14] considered a notion of individual security for cryptographic systems by using Kolmogorov complexity instead of Shannon entropy. Kaced [15] and Dai et al. [16] considered the Kolmogorov complexity-based security for secret sharing schemes. In this paper, we also propose the notion of a normalized version of Kolmogorov complexity-based security for private-key encryption scheme. Kolmogorov complexity and entropy are different information measures, and therefore a private-key encryption is secure based on one information measure but not secure based on another information measure [5]. Finally, we show the relationship between entropy-based security and Kolmogorov complexity-based security.

This paper is organized as follows: in Section 2, we review some definitions of entropy measures, Kolmogorov complexity, and private-key encryption. In Section 3, we propose several normalized versions of security notions based on Shannon entropy, and derive some lower bounds on the key size for private-key encryption under these security models. In Section 4, several Kolmogorov complexity-based security notions of private-key encryption are given and are compared to Shannon entropy-based security in Section 5. Conclusions are presented in Section 6.

## 2. Preliminaries

### 2.1. Entropy

Let $\mathcal{X}$ be a finite set. Let $X$ be a random variable over $\mathcal{X}$. We denote the probability of random variable $X$ being equal to $x$ by $p_X(x)$, and when no confusion on the random variable used may arise, we simplify it to $p(x)$.

Let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ be three finite sets. Let $X, Y, Z$ be random variables over $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, respectively. Some basic concepts of information theory are defined as follows.

The Shannon entropy [1] of a random variable $X$, defined by

$$\mathrm{H}(X) = -\sum_{x \in X} p(x) \log p(x). \tag{1}$$

The conditional Shannon entropy with respect to $X$ given $Y$ is defined as

$$\mathrm{H}(X|Y) = -\sum_{y \in Y} p(y)\mathrm{H}(X|Y = y). \tag{2}$$

The joint Shannon entropy of $X$ and $Y$ is

$$\mathrm{H}(X, Y) = \mathrm{H}(X) + \mathrm{H}(Y|X) = \mathrm{H}(Y) + \mathrm{H}(X|Y). \tag{3}$$

The Mutual information between $X$ and $Y$ is

$$\mathrm{I}(X; Y) = \mathrm{H}(X) - \mathrm{H}(X|Y). \tag{4}$$

The conditional mutual information between $X$ and $Y$ given $Z$ is defined as

$$\mathrm{I}(X; Y|Z) = \mathrm{H}(X|Z) - \mathrm{H}(X|(Y, Z)). \tag{5}$$

We recall a few properties of Shannon entropy.

**Lemma 1.** *References [7,12]. Let $X, Y, Z$ be random variables over $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, respectively.*
*(i)* $\mathrm{H}(X) \geq 0$, *with equality if and only if there exists $x_0 \in \mathcal{X}$ such that $p(x_0) = 1$;*
*(ii)* $\mathrm{H}(X) \leq \log |\mathcal{X}|$, *with equality if and only if $p(x) = 1/|\mathcal{X}|$ for all $x \in \mathcal{X}$;*
*(iii)* $\mathrm{H}(X) \geq \mathrm{H}(X|Y)$;
*(iv)* $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$;
*(v)* $\mathrm{I}(X; Y) = \mathrm{I}(Y; X)$;

*(vi)* $\mathrm{H}(X,Y,Z) = \mathrm{H}(X) + \mathrm{H}(Y|X) + \mathrm{H}(Z|(X,Y))$;
*(vii)* $\mathrm{H}(Y) \geq \mathrm{H}(X) - \mathrm{H}(X|(Y,Z)) - \mathrm{I}(X;Z)$.
*(viii) (Fano inequality)* $\mathrm{H}(X|Y) \leq \mathrm{H}(X|X') \leq \mathrm{H}(p_e) + p_e \log |\mathcal{X}|$, *where* $X' = f(Y)$ *is a function of* $Y$ *and* $p_e = p(X \neq X')$ *is the probability of error.*

### 2.2. Kolmogorov Complexity

Some definitions and basic properties of Kolmogorov complexity are recalled below. For more details, see [12,13].

Here, we use the prefix-free definition of Kolmogorov complexity. A set of strings $A$ is prefix-free if there are not two strings $x$ and $y$ in $A$ such that $x$ is a proper prefix of $y$.

The conditional Kolmogorov complexity $\mathrm{K}(y|x)$ of $y$ given $x$, with respect to a universal prefix-free Turing machine $U$, is defined by

$$\mathrm{K}_U(y|x) = \min\{|p| : U(p,x) = y\}, \tag{6}$$

where $U(p,x)$ is the output of the program $p$ with auxiliary input $x$ when it is run in the machine $U$.

Let $U$ be a universal prefix-free Turing machine, then for any other Turing machine $F$:

$$\mathrm{K}_U(y|x) \leq \mathrm{K}_F(y|x) + c_F \tag{7}$$

for all $x, y$, where the constant $c_F$ depends on $F$ but not on $x, y$.

The (unconditional) Kolmogorov complexity $\mathrm{K}_U(y)$ of $y$ is defined as $\mathrm{K}_U(y|\varepsilon)$, where $\varepsilon$ is the empty string. We fix a universal prefix-free Turing machine once and for all and for convenience, $\mathrm{K}_U(y|x)$ and $\mathrm{K}_U(y)$ are denoted, respectively, by $\mathrm{K}(y|x)$ and $\mathrm{K}(y)$.

The algorithmic mutual information between $x$ and $y$ is the quantity

$$\mathrm{I}(x:y) = \mathrm{K}(x) - \mathrm{K}(x|y). \tag{8}$$

We consider $x$ and $y$ to be algorithmically independent whenever $\mathrm{I}(x:y)$ is approximately zero.

**Lemma 2.** *References [12,13]. For any finite strings* $x, y$, *we have*
*(i)* $\mathrm{K}(x) \leq |x| + O(1)$;
*(ii)* $\mathrm{K}(x|y) \leq \mathrm{K}(x) + O(1)$;
*(iii)* $\mathrm{K}(x,y) \leq \mathrm{K}(x) + \mathrm{K}(y|x) + O(1)$,
*where* $O(1)$ *is a constant term.*

Shannon entropy and Kolmogorov complexity are different information measures, as the former is based on probability distributions and the latter on the length of programs. However, for any computable probability distributions, up to a constant term, the expected value of the (conditional) Kolmogorov complexity equals the (conditional) Shannon entropy [17,18]. Shannon mutual information and algorithmic mutual information are also related.

**Lemma 3.** *References [17,18]. Let* $X, Y$ *be two random variables over* $\mathcal{X}$, $\mathcal{Y}$, *respectively. For any computable probability distribution* $u(x,y)$ *over* $\mathcal{X} \times \mathcal{Y}$,
*(i)* $0 \leq (\sum_{x,y} u(x,y)\mathrm{K}(x|y) - \mathrm{H}(X|Y)) \leq \mathrm{K}(u) + O(1)$.
*(ii)* $\mathrm{I}(X;Y) - \mathrm{K}(u) \leq \sum_{x,y} u(x,y)\mathrm{I}(x{:}y) \leq \mathrm{I}(X;Y) + 2\mathrm{K}(u)$. *When* $u$ *is given, then* $\mathrm{I}(X;Y) = \sum_{x,y} u(x,y)\mathrm{I}(x{:}y|u) + O(1)$.

### 2.3. Private-Key Encryption

A private-key encryption $\prod$ consists of a message space $\mathcal{X}$, a ciphertext space $\mathcal{Y}$, a key space $\mathcal{K}$, and a pair of an encryption function $Enc : \mathcal{X} \times \mathcal{K} \to \mathcal{Y}$ and a decryption function $Dec : \mathcal{Y} \times \mathcal{K} \to \mathcal{X}$; i.e., $\prod =_{def} (\mathcal{X}, \mathcal{Y}, \mathcal{K}, Enc, Dec)$.

A private-key encryption $\prod$ is said to have perfect correctness if

$$Dec_k(Enc_k(x)) = x \tag{9}$$

for any key $k \in \mathcal{K}$ and plaintext $x \in \mathcal{X}$.

Dodis [7] relaxed the correctness guarantee to allow for some small decryption error $\gamma$. A private-key encryption $\prod$ is said $(1-\gamma)$-correct on $\mathcal{X}$ if

$$\Pr_{X,K}(Dec_K(Enc_K(X)) = X) > 1 - \gamma. \tag{10}$$

Dodis [7] also gave the following natural definition of imperfect correctness based on Shannon entropy. A private-key encryption $\prod$ is said $(1-\gamma)$-Shannon correct on $\mathcal{X}$ if

$$\mathrm{H}(X|Dec_K(Y)) \leq \gamma. \tag{11}$$

## 3. Normalized $\epsilon$-Shannon Security

Now we are ready to propose a new relaxation of non-perfect security for private-key encryption. In the rest of this paper, $X, Y, K$ are always used to denote the random variable for plaintext space $\mathcal{X}$, ciphertext space $\mathcal{Y}$, and key space $\mathcal{K}$, respectively.

**Definition 1.** *Let $\prod$ be a private-key encryption. We say $\prod$ is normalized $\epsilon$-Shannon secure if*

$$\mathrm{I}(X;Y) \leq \epsilon \mathrm{H}(X); \text{ i.e., } \mathrm{I}(X;Y)/\mathrm{H}(X) \leq \epsilon. \tag{12}$$

In the above notion, we use the information leak ratio instead of the absolute amount of information leak to measure the security degree of private-key encryption. It can simply be understood as a normalized version of $\epsilon$-Shannon security.

The new security parameter $\epsilon$ takes values in the range $[0,1]$. When $\epsilon = 0$, $\prod$ is perfect secrecy. When $\epsilon = 1$, $\prod$ is maximally insecure.

In [7], a private-key encryption $\prod$ is called $\epsilon$-Shannon secure if $\mathrm{I}(X,Y) \leq \epsilon$. It is easy to know that if a private-key encryption $\prod$ is normalized $\epsilon$-Shannon secure (which means the information leak ratio is at most $\epsilon$), then the absolute amount of information leak is at most $\epsilon \mathrm{H}(X)$, and $\prod$ is $\epsilon \mathrm{H}(X)$-Shannon secure. Moreover, by Lemma 1(ii), $\mathrm{H}(X) \leq \log|\mathcal{X}|$, $\prod$ is $\epsilon \log|\mathcal{X}|$-Shannon secure.

Our notion can be used to compare the security of private-key encryption schemes that have different message sizes. For example, a 2-Shannon secure encryption $\prod_1$ with $|\mathcal{X}_1| = |\mathcal{Y}_1| = |\mathcal{K}_1| = 2^{100}$ and a 1-Shannon secure encryption $\prod_2$ with $|\mathcal{X}_2| = |\mathcal{Y}_2| = |\mathcal{K}_2| = 2^{10}$. We cannot say that $\prod_2$ is more secure than $\prod_1$ (by $1 < 2$) because of the different size of the message. By using our notion, however, $\prod_1$ is normalized $2^{-99}$-Shannon secure and $\prod_2$ is normalized $2^{-10}$-Shannon secure, where we assume that $X_1$ and $X_2$ are uniformly random, then we can say that $\prod_1$ is more secure than $\prod_2$. Thus, our investigation of the above definition of security has its literature reason.

*Lower Bounds*

In this subsection, we derive some lower bounds on the key size for private-key encryption under various correctness and security models.

**Theorem 1.** *Let $\prod$ be a private-key encryption. If $\prod$ has normalized $\epsilon$-Shannon security and perfect correctness, then*

$$\mathrm{H}(K) \geq (1-\epsilon)\mathrm{H}(X). \tag{13}$$

**Proof.** From Lemma 1(vii), we have

$$\mathrm{H}(K) \geq \mathrm{H}(X) - \mathrm{H}(X|(K,Y)) - \mathrm{I}(X;Y). \tag{14}$$

From the definition of normalized $\epsilon$-Shannon security, we have

$$\mathrm{I}(X;Y) \leq \epsilon \mathrm{H}(X). \tag{15}$$

Let $X' = Dec_K(Y)$. Since $\prod$ has perfect correctness, then from Lemma 1(i) we have $p(X \neq X') = 0$. So, by Lemma 1(viii) Fano inequality, $0 \leq \mathrm{H}(X|(K,Y)) \leq \mathrm{H}(X|X') = 0$, then we have

$$\mathrm{H}(X|(K,Y)) = 0. \tag{16}$$

Then, by Equations (14)–(16), we have

$$\begin{aligned} \mathrm{H}(K) &\geq \mathrm{H}(X) - \mathrm{I}(X;Y) - \mathrm{H}(X|(K,Y)) \\ &\geq \mathrm{H}(X) - \epsilon \mathrm{H}(X) \\ &= (1-\epsilon)\mathrm{H}(X). \end{aligned}$$

□

From the above result, we know that normalized $\epsilon$-Shannon security and perfect correctness requires $\mathrm{H}(K) \geq (1-\epsilon)\mathrm{H}(X)$; this is different from $\epsilon$-Shannon security and perfect correctness, which requires $\mathrm{H}(K) \geq \mathrm{H}(X) - \epsilon$.

Next, we consider the normalized $\epsilon$-Shannon security with a completeness error $\gamma$.

**Theorem 2.** *Let $\prod$ be a private-key encryption. If $\prod$ is normalized $\epsilon$-Shannon secure and $(1-\gamma)$-Shannon correct, then*

$$\mathrm{H}(K) \geq (1-\epsilon)\mathrm{H}(X) - \gamma. \tag{17}$$

**Proof.** From Lemma 1(vii), we have

$$\mathrm{H}(K) \geq \mathrm{H}(X) - \mathrm{I}(X;Y) - \mathrm{H}(X|(K,Y)). \tag{18}$$

From the definition of normalized $\epsilon$-Shannon security, we have

$$\mathrm{I}(X;Y) \leq \epsilon \mathrm{H}(X). \tag{19}$$

From the definition of $(1-\gamma)$-Shannon correctness and Lemma 1(viii) Fano inequality, we have

$$\mathrm{H}(X|(K,Y)) \leq \mathrm{H}(X|Dec_K(Y)) \leq \gamma. \tag{20}$$

Then, by using Equations (18)–(20), we have

$$\begin{aligned} \mathrm{H}(K) &\geq \mathrm{H}(X) - \mathrm{H}(X|(K,Y)) - \mathrm{I}(X;Y) \\ &\geq \mathrm{H}(X) - \gamma - \epsilon \mathrm{H}(X) \\ &= (1-\epsilon)\mathrm{H}(X) - \gamma. \end{aligned}$$

□

From Lemma 1(ii) and Theorem 2, we conclude the following.

**Corollary 3.** *Let $X$ be the uniform distribution over $\mathcal{X}$, $\prod$ be a private-key encryption. If $\prod$ is normalized $\epsilon$-Shannon secure and $(1-\gamma)$-Shannon correct, then*

$$\mathrm{H}(K) \geq (1-\epsilon)\log|\mathcal{X}| - \gamma. \tag{21}$$

*Consequently,*

$$|\mathcal{K}| \geq 2^{-\gamma}|\mathcal{X}|^{1-\epsilon}. \tag{22}$$

## 4. Normalized $\epsilon$-Kolmogorov Security

We give a security notion for private-key encryption based on Kolmogorov complexity. This idea is that now a private-key encryption is not a distribution on binary strings, but an individual tuple of binary strings with corresponding properties of secrecy (see [14]). We use Kolmogorov complexity instead of Shannon entropy to measure the security degree for an individual tuple of strings of private-key encryption. Let $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $k \in \mathcal{K}$ be a plaintext, a ciphertext, and a key, respectively. A pair of strings $(x,y)$ is used to denote an instance of a private-key encryption which satisfies $Enc_k(x) = y$ and $Dec_k(y) = x$ for a key $k \in \mathcal{K}$.

**Definition 2.** *Let $\prod$ be a private-key encryption, $(x,y)$ be an instance of $\prod$. An instance $(x,y)$ is normalized $\epsilon$-Kolmogorov secure if*

$$\mathrm{I}(x;y) \leq \epsilon\mathrm{K}(x); \text{ i.e., } \mathrm{I}(x;y)/\mathrm{K}(x) \leq \epsilon. \tag{23}$$

The security parameter $\epsilon$ can be seen as the information leak ratio in the sense of Kolmogorov complexity. For Kolmogorov complexity, there is no natural way to define an "absolutely" perfect version of a private-key encryption scheme. We consider a private-key encryption to be approximately-perfect secure in the sense of Kolmogorov complexity whenever $\epsilon$ is approximately zero, which means that the plaintext $x$ and the ciphertext $y$ are algorithmically independent.

The notion of normalized $\epsilon$-Kolmogorov security can be simply understood as a normalized version of individual security [14], which is a formal definition of what it means for an individual instance to be secure.

Now, we show a lower bound of key sizes for an instance of private-key encryption.

**Theorem 4.** *Let $\prod$ be a private-key encryption, and $(x,y)$ be an instance of $\prod$. Suppose the decryption function Dec is given, and the length of Dec is not dependent on the length of the key k. If an instance $(x,y)$ is normalized $\epsilon$-Kolmogorov secure, then*

$$|k| \geq (1-\epsilon)\mathrm{K}(x) - O(1) \tag{24}$$

*for any key k with $Dec_k(y) = x$.*

**Proof.** Let $p$ be a shortest binary program that computes $x$ from $y$. Since $Dec_k(y) = x$, the length of $p$ is no more than the length of the decryption function $Dec$ and the key $k$, $|p| \leq |Dec| + |k|$. Because the decryption function $Dec$ is given and the length of $Dec$ is not dependent on the length of key $k$, we have $\mathrm{K}(x|y) \leq |k| + O(1)$.

If $\prod$ is normalized $\epsilon$-Kolmogorov secure, $\mathrm{I}(x;y) \leq \epsilon\mathrm{K}(x)$; i.e., $\mathrm{K}(x) - \mathrm{K}(x|y) \leq \epsilon\mathrm{K}(x)$, then we have $(1-\epsilon)\mathrm{K}(x) \leq \mathrm{K}(x|y)$. Then,

$$\mathrm{K}(x) - \epsilon\mathrm{K}(x) \leq \mathrm{K}(x|y) \leq |k| + O(1). \tag{25}$$

Thus, $|k| \geq (1-\epsilon)\mathrm{K}(x) - O(1)$. □

From the above theorem, we know that a message with high Kolmogorov complexity—or a nearly Kolmogorov random string—cannot be encrypted by a small key size with high security parameter.

## 5. Normalized $\epsilon$-Kolmogorov Security versus Normalized $\epsilon$-Shannon Security

In this section, we establish some relations between Shannon entropy-based security and Kolmogorov complexity-based security for private-key encryption.

First, from the notion of normalized $\epsilon$-Kolmogorov security for a private-key encryption, $\epsilon$ is a security parameter defined for one instance, not all instances. Many $x$'s have a small Kolmogorov complexity even if the adversary does not know the ciphertext $y$. For example, the Kolmogorov complexity of $x = 111...11 \in \{0,1\}^n$ is almost vanishing. So, we give the following definition for all instances in a private-key encryption.

**Definition 3.** *Let $\prod$ be a private-key encryption, $u$ a computable distribution over $\mathcal{X} \times \mathcal{Y}$. $\prod$ is normalized $(\epsilon, \delta)$-Kolmogorov secure if*

$$\Pr_{k \in \mathcal{K}, y \in \times \mathcal{Y}}[\mathrm{I}(x; y|u) \leq \epsilon \mathrm{K}(x)] \geq \delta. \tag{26}$$

The above security notion means that the probability that an instance is normalized $\epsilon$-Kolmogorov secure at least $\delta$ for a computable distribution.

For a private-key encryption, when the probability of an instance with low security parameter is high, this means that most of instances are secure.

Here we give following relations between normalized $(\epsilon, \delta)$-Kolmogorov security and normalized $\epsilon$-Shannon security.

**Theorem 5.** *Let $\prod$ be a private-key encryption. If for any independent variables $X, Y$ over $\mathcal{X}, \mathcal{Y}$ with a computable joint distribution $u$, $\prod$ is normalized $(\epsilon, \delta)$-Kolmogorov secure, then $\prod$ is normalized $(1 + \epsilon - \delta)$-Shannon secure.*

**Proof.** Since $\prod$ is normalized $(\epsilon, \delta)$-Kolmogorov secure, then the probability that an instance is normalized $\epsilon$-Kolmogorov secure is at least $\delta$; i.e.,

$$\Pr_{x \in \mathcal{X}, y \in \times \mathcal{Y}}[\mathrm{I}(x; y|u) \leq \epsilon \mathrm{K}(x)] \geq \delta. \tag{27}$$

Let $Q$ be the set of normalized $\epsilon$-Kolmogorov secure instances of private-key encryption $\prod$; i.e., $Q = \{(x, y); \mathrm{I}(x; y|u) \leq \epsilon \mathrm{K}(x)\}$. Then, we have

$$\Pr_{x \in \mathcal{X}, y \in \times \mathcal{Y}}[(x, y) \notin Q] \leq 1 - \delta. \tag{28}$$

By using Lemmas 2 and 3 and Equations (27) and (28), up to a constant, we have

$$\begin{aligned} \mathrm{I}(X; Y) &\leq \sum_{(x,y) \in Q} u(x, y) \mathrm{I}(x : y|u) + \sum_{(x,y) \notin Q} u(x, y) \mathrm{I}(x : y|u) \\ &\leq \epsilon \sum_{(x,y) \in Q} u(x, y) \mathrm{K}(x|u) + \sum_{(x,y) \notin Q} u(x, y)[\mathrm{K}(x|u) - \mathrm{K}(x|y, u)] \\ &\leq \epsilon \mathrm{H}(X) + (1 - \delta) \mathrm{H}(X) \\ &\leq (1 + \epsilon - \delta) \mathrm{H}(X). \end{aligned}$$

□

By using the above result and Lemma 1(ii), $\mathrm{H}(X) \leq \log(|\mathcal{X}|)$, we have $(1 + \epsilon - \delta) \log(|\mathcal{X}|)$-Shannon security from normalized $(\epsilon, \delta)$-Kolmogorov security.

The result of Theorem 5 is different from Reference [14], which we have $\epsilon + (1-\delta)\log(|\mathcal{X}|)$-Shannon security from non-normalized $(\epsilon, \delta)$-Kolmogorov security.

The result of Theorem 5 shows that if the probability of approximately-perfect secure instances ($\epsilon$ is approximately zero) is approximately 1, then the private-key encryption is approximately-perfect secure in the Shannon entropy sense.

## 6. Conclusions

In this paper, we presented two notions of normalized $\epsilon$-Shannon security and $\epsilon$-Kolmogorov security for private-key encryption. The new security parameters can make the evaluation of the security of private-key encryption more normalized and rationalized. Then, we established the relation of two normalized security notions for private-key encryption.

As future work, we can consider a special case of $\epsilon$ that is a negligible function of the message length. In this case, the amount of information leak can be ignored because negligible functions tend to zero very fast as their input (the message length) grows.

Obviously, we only considered the normalized security of private-key encryption schemes based on Shannon entropy and Kolmogorov complexity. Normalized security of other schemes based on other information measures are possible topics for future consideration.

**Acknowledgments:** Project supported by the Guangxi University Science and Technology Research Project (Grant No. 2013YB193) and the Science and Technology Foundation of Guizhou Province, China (LKS [2013] 35).

**Author Contributions:** Conceptualization, formal analysis, investigation and writing the original draft is done by Songsong Dai. Validation, review and editing is done by Lvqing Bi and Bo Hu. Project administration and Resources are provided by Lvqing Bi and Bo Hu. All authors have read and approved the final manuscript.

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

## References

1. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423, 623–656.
2. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
3. Vernam, G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.* **1926**, *45*, 109–115.
4. Iwamoto, M.; Ohta, K. Security Notions for Information Theoretically Secure Encryptions. In Proceedings of the 2011 IEEE Symposium on Information Theory, Saint Petersburg, Russia, 31 July–5 August 2011; pp. 1777–1781.
5. Jiang, S. On Unconditional $\epsilon$-Security of Private Key Encryption. *Comput. J.* **2013**, 57, 1570–1579.
6. Alimomeni, M.; Safavi-Naini, R. Guessing Secrecy. In Proceedings of the 6th International Conference on Information Theoretical Security (ICITS 12), Montreal, QC, Canada, 15–17 August 2012; pp. 1–13.
7. Dodis, Y. Shannon Impossibility, Revisited. In Proceedings of the 6th International Conference on Information Theoretical Security (ICITS 12), Montreal, QC, Canada, 15–17 August 2012; pp. 100–110.
8. Iwamoto, M.; Shikata, J. Information theoretic security for encryption based on conditional Rényi entropies. In *Proceedings of the International Conference on Information Theoretic Security (ICITS)*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 103–121.
9. Chaitin, G. On the length of programs for computing finite binary sequences. *J. ACM* **1966**, *13*, 547–569.
10. Kolmogorov, A. Three approaches to the quantitative definition of information. *Probl. Inf. Transm.* **1965**, *1*, 1–7.
11. Solomonoff, R. A formal theory of inductive inference, part I. *Inf. Control* **1964**, *7*, 1–22.
12. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley: Hoboken, NJ, USA, 2006.
13. Li, M.; Vitányi, P.M.B. *An Introduction to Kolmogorov Complexity and Its Applications*, 3rd ed.; Springer: New York, NY, USA, 2008.
14. Antunes, L.; Laplante, S.; Pinto, A.; Salvador, L. Cryptographic security of individual instances. In *Information Theoretic Security*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 195–210.
15. Kaced, T. Almost-perfect secret sharing. In Proceedings of the 2011 IEEE International Symposium on Information Theory Proceedings (ISIT), Saint Petersburg, Russia, 31 July–5 August 2011; pp. 1603–1607.
16. Dai, S.; Guo, D. Comparing security notions of secret sharing schemes. *Entropy* **2015**, *17*, 1135–1145.

17. Grünwald, P.; Vitányi, P. Shannon Information and Kolmogorov Complexity. *arXiv* **2008**, arXiv:cs/0410002.
18. Teixeira, A.; Matos, A.; Souto, A.; Antunes, L. Entropy measures vs. kolmogorov complexity. *Entropy* **2011**, *13*, 595–611.