Entropy **2015**, *17*, 1135-1145; doi:10.3390/e17031135

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Comparing Security Notions of Secret Sharing Schemes

Songsong Dai and Donghui Guo *

Department of Electronic Engineering, Xiamen University, Xiamen 361005, China;
E-Mail: ssdai@stu.xmu.edu.cn

* Author to whom correspondence should be addressed; E-Mail: dhguo@xmu.edu.cn;
Tel.:+86-592-2580070.

Academic Editors: James Park and Wanlei Zhou

Received: 15 January 2015 / Accepted: 3 March 2015 / Published: 10 March 2015

Abstract: Different security notions of secret sharing schemes have been proposed by different information measures. Entropies, such as Shannon entropy and min entropy, are frequently used in the setting security notions for secret sharing schemes. Different to the entropies, Kolmogorov complexity was also defined and used in study the security of individual instances for secret sharing schemes. This paper is concerned with these security notions for secret sharing schemes defined by the variational measures, including Shannon entropy, guessing probability, min entropy and Kolmogorov complexity.

Keywords: cryptography; secret sharing scheme; information theoretic security; entropy; Kolmogorov complexity

1. Introduction

A secret sharing scheme [1,2] is a protocol to share a secret among participants such that only specified subsets of participants can recover the secret. In considering the security notions of secret sharing schemes, some authors have introduced concepts of security for secret sharing schemes based on different information measures [3–7]. These information measures include four very important information measures: Shannon entropy, min entropy, Rényi entropy and Kolmogorov complexity. Shannon entropy is the most widely used information measure, which is used to prove bounds on the share size and on the information rate in secret sharing schemes [3–5]. Recently, min and Rényi entropies are also used in study of the security of secret sharing schemes [6,7].

Kolmogorov complexity $K(x)$ [8–10], known as algorithmic information theory [11,12], measures the quantity of information in a single string x, by the size of the smallest program that generates it. It is well known that Kolmogorov complexity and entropy measure are different but related measures [13–15]. Measuring the security by Kolmogorov complexity offers us some new security criteria. Antunes *et al.* [16] gave a notion of individual security for cryptographic systems by using Kolmogorov complexity. Kaced [17] defined a normalized version of individual security for secret sharing schemes.

However these information measures are different. This means a scheme is secure based on one information measure but not secure based on another information measure [18]. Recently, several relations of security notions of cryptography have been studied. Iwamoto *et al.* [6] and Jiang [18] studied relations between security notions for the symmetric-key cryptography. In this paper, we are interested in relationships of security notions for secret sharing schemes. Antunes *et al.* [16] and Kaced [17] also studied relations between security notions for secret sharing schemes. However, their studies are between security notions based on Shannon entropy and Kolmogorov complexity. We study relationships of different security notions for secret sharing schemes under various information measures including Shannon entropy, guessing probability, min entropy and Kolmogorov complexity.

This paper is organized as follows: In Section 2, we review some definitions of entropy measures, Kolmogorov complexity and secret sharing schemes. In Section 3, we propose several security notions in entropies, and their relations. In Section 4, by using Kolmogorov complexity, security notions of secret sharing schemes are given, then are compared to entropy-based security in Section 5. Conclusions are presented in Section 6.

2. Preliminaries

In this paper, string means a finite binary string $\Sigma^* := \{0,1\}^*$. $|x|$ represents the length of a string x. For the cardinality of a set A we write $|A|$. Function $\log$ means the function $\log_2$. $\ln(\cdot)$ denotes the logarithm function with natural base $e = 2.71828....$

Let $[n] := \{1, 2, ..., n\}$ be a finite set of IDs of n users. For every $i \in [n]$, let V_i be a finite set of shares of the user i. Similarly, let S be a finite set of secret information. In the following, for any subset $U := \{i_1, i_2, ..., i_u\} \subset [n]$, we use the notation $v_U := \{v_{i_1}, v_{i_2}, ..., v_{i_u}\}$ and $V_U := \{V_{i_1}, V_{i_2}, ..., V_{i_u}\}$.

2.1. Entropy

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite sets. Let X and Y be two random variables over $\mathcal{X}$ and $\mathcal{Y}$, respectively. The probability that X takes on the value x from a finite or countably infinite set X is denoted by $p_X(x)$; the mutual probability, the probability that both x and y occur, by $p_{XY}(x, y)$ and the conditional probability, the probability that x occurs knowing that y has occurred by $p_{XY}(x|y)$. For convenience, $p_X(x)$, $p_{XY}(x, y)$ and $p_{XY}(x|y)$ are denoted by $p(x)$, $p(x, y)$ and $p(x|y)$, respectively. Two random variables X and Y are independent if and only if $p(x, y) = p(x) \times p(y)$ for all $x \in X$ and $y \in Y$.

The Shannon entropy [19] of a random variable X, defined by $H(X) = -\sum_{x \in X} p(x) \log p(x)$, is a measure of its average uncertainty. The conditional Shannon entropy with respect to X given Y is defined as

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

The Mutual information between X and Y is

$$I(X; Y) = H(X) - H(X|Y).$$

Guessing probability [20] of X, occurred by $G(X) = \max_{x \in X} p(x)$, is the success probability of correctly guessing the value of a realization of variable when using the best guessing strategy (guessing the most probable value of the range as the guess). Conditional guessing probability with respect to X given Y is defined as

$$G(X|Y) = \sum_{y \in Y} p(y) \max_{x \in X} p(x|y).$$

Min-entropy [6,18,20] is a measure of success chance of guessing X, *i.e.*,

$$H_\infty(X) = -\log G(X) = -\log \max_{x \in X} p(x).$$

It can also be viewed as the worst case entropy compared to Shannon entropy which is an average entropy. The conditional min entropy with respect to X given Y is defined as

$$H_\infty(X|Y) = -\log G(X|Y) = -\log(\sum_{y \in Y} p(y) \max_{x \in X} p(x|y)).$$

2.2. Kolmogorov Complexity

In this subsection, some definitions and basic properties of Kolmogorov complexity are recalled below. We will 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. For more details and attributions we refer to [11,12].

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

$$K_U(y|x) = min\{|p| : U(p, x) = y\}.$$

Let U be a universal prefix-free computer, then for any other computer F:

$$K_U(y|x) \leq K_F(y|x) + c_F.$$

for all x, y, where c_F depends on F but not on x, y. The (unconditional) Kolmogorov complexity$K_U(y)$ of y is defined as $K_U(y|\Lambda)$ where Λ is the empty string. For convenience, $K_U(y|x)$ and $K_U(y)$ are denoted, respectively by $K(y|x)$ and $K(y)$.

The mutual algorithmic information between x and y is the quantity

$$I(x : y) = K(x) - K(x|y).$$

We consider x and y to be algorithmic independent whenever $I(x : y)$ is zero.

2.3. Secret Sharing Schemes

Then, secret sharing schemes for general access structures are recalled below. For more details refer to [1,3,7,21,22].

Each set of shares is classified into either a qualified set or a forbidden set. A qualified set is the set of shares that can recover the secret. Let $\mathcal{Q} \subset 2^{[n]}$ and $\mathcal{F} \subset 2^{[n]}$ be families of qualified and forbidden sets, respectively. Then $\Gamma := (\mathcal{Q}, \mathcal{F})$ an access structure. An access structure is monotone if for all $Q \in \mathcal{Q}$, every $Q \subset Q'$ satisfies $Q' \in \mathcal{Q}$ and; for all $F \in \mathcal{F}$, every $F \subset F'$ satisfies $F' \in \mathcal{F}$.

In particular, the access structure is called (t, n)-threshold access structure if it satisfies that $\mathcal{Q} := \{Q : |Q| \geq t\}$ and $\mathcal{F} := \{F : |F| \leq t - 1\}$. In this paper, the access structure is a partition of $2^{[n]}$, namely, $\mathcal{Q} \cup \mathcal{F} = 2^{[n]}$ and $\mathcal{Q} \cap \mathcal{F} = \emptyset$.

Let $\prod = (S, V_{[n]}, \prod_{share}, \prod_{comb})$ be a secret sharing scheme for an access structure Γ , as defined below:

(i) S is set of secret information;

(ii) $V_{[n]}$ is set of shares for all users;

(iii) $\prod_{share}$ is an algorithm for generating shares for all users. It takes a secret $s \in S$ on input and outputs $(v_1, v_2, ..., v_n) \in V_{[n]}$;

(iv) $\prod_{comb}$ is an algorithm for recovering a secret. It takes a set of shares v_Q , $Q \in \mathcal{Q}$, on input and outputs a secret $s \in S$.

In this paper, we assume that $\prod$ meets perfect correctness: for any secret $s \in S$, and for all shares $\prod_{share}(s) = (v_1, v_2, ..., v_n)$, it holds that $\prod_{comb}(v_Q) = s$ for any subset $Q \in \mathcal{Q}$.

3. Information Theoretic Security of Secret Sharing Schemes

In this section, we first give the security notions of information theoretic security for secret sharing schemes based on Shannon entropy, guessing probability and min entropy, respectively, and then we discuss the relations between these security notions.

Definition 1. *Let $\prod$ be a secret sharing scheme for an access structure Γ . We say $\prod$ is*
(i) *ε-Shannon security, if $I(S; V_F) \leq \varepsilon$;*
(ii) *ε-guess security, if $G(S|V_F) - G(S) \leq \varepsilon$;*
(iii) *ε-min security, if $H_\infty(S) - H_\infty(S|V_F) \leq \varepsilon$*
for any forbidden set $F \in \mathcal{F}$.

Now, we discuss the relations between above three security notions for secret sharing schemes.

The following relations are important for the present paper.

Lemma 1. [11,18,20] *Let X and Y be two random variables over $\mathcal{X}$ and $\mathcal{Y}$, respectively . Then*
(i) $G(X|Y) \geq G(X)$.
(ii) $H(X|Y) \leq H(X)$.
(iii) $H_\infty(X|Y) \leq H_\infty(X)$.

(iv) $I(X;Y) \geq (2/\ln 2)[G(X|Y) - G(X)]^2$.
(v) $|H_\infty(X) - H_\infty(X|Y)| \geq (1/\ln 2)|G(X) - G(X|Y)|$.
(vi) $H_\infty(X) - H_\infty(X|Y) \geq I(X;Y)$, *where X is uniformly random over $\mathcal{X}$.*

From above lemma, several relations of security notions for the symmetric-key cryptography in [18]. Similarly, from above lemma, we obtain the following.

Theorem 1. *Let $\prod$ be a secret sharing scheme for an access structure Γ.*
(i) *If $\prod$ is ε-Shannon security, then it is $\sqrt{\frac{1}{2}\varepsilon \ln 2}$ -guess security.*
(ii) *If $\prod$ is ε-min security, then it is $\varepsilon \ln 2$ -guess security*
(iii) *If $\prod$ is ε-min security and S is uniformly random over $\mathcal{S}$, then $\prod$ is ε-Shannon security.*

From this result, we can see that, for a secret sharing scheme, ε-Shannon and ε-min security both are stronger than ε-guess security. If we assume S is uniformly random, then, for a secret sharing scheme, ε-min security is stronger than ε-Shannon security.

In the following, using a modified example of threshold secret sharing scheme, we showed that a secret sharing scheme is ε-guess security does not imply it is ε-Shannon security.

Example 1. *Let s, and $v_1, v_2, \cdots, v_n$ be binary strings with same length k. Assume that s and $v_1, v_2, \cdots, v_{n-1}$ are independent. We generate v_n by $v_n = s \oplus v_1 \oplus v_2 \oplus \cdots \oplus v_{n-1}$ where $\oplus$ denotes the exclusive OR operation. This scheme is $(n,n)-$threshold secret sharing scheme, called Karnin–Greene–Hellman scheme* [5].

Let $\mathcal{S} = \{0,1\}^k$, $\mathcal{V}_1 = \{0,1\}^{k-1}$, $\mathcal{V}_2 = \{0,1\}^k$ and $\mathcal{V}_3 = \{0,1\}^{k-1}$. S is uniformly random over $\mathcal{S}$ and $V_1 \times V_2$ is uniformly random over $\{0,1\}^{k-1} \times \{0,1\}^k$. To share $s = s'|s''$ for $s' \in \{0,1\}^{k-1}$ and $s'' \in \{0,1\}$. Let $v_2 = v_2'|v_2''$ where $v' \in \{0,1\}^{k-1}$ and $v'' \in \{0,1\}$. And s' and v_1, v_2' are independent. Let $v_2'' = s''$ and $v_3 = s' \oplus v_1 \oplus v_2'$. Algorithm for recovering the secret is $s = s'|s''$ where $s' = v_3 \oplus v_1' \oplus v_2$ and $s'' = v_2''$. This scheme is $(3,3)-$threshold secret sharing scheme. It is easy to see that $G(S|V_2,V_3) = G(S|V_1,V_3) = G(S|V_1,V_2) = 2^{-(k-1)}$ and hence $|G(S|V_i,V_j) - G(S)| = 2^{-k}$ for $1 \leq i < j \leq 3$. However, $I(S;(V_2,V_3)) = H(S) - H(S|V_2,V_3) = k - (k-1) = 1$.

Next, we discuss the relationship between these security notions when $\varepsilon = 0$.

Theorem 2. *If a secret sharing scheme is 0-Shannon security, then it is 0-min security. Moreover, if S is uniformly random over $\mathcal{S}$, then, for a secret sharing scheme, 0-min security, 0-guess security and 0-Shannon security are all equivalent.*

However, a secret sharing scheme is 0-min security does not imply it is 0-Shannon security.

Example 2. [18]. *Let $\mathcal{S} = \mathcal{V}_1 = \mathcal{V}_2 = \{0,...,k-1\}$ for $k \geq 4$. $p_{V_1}(1) = ... = p_{V_1}(k-1) = 1/(k+1)$ and $p_{V_1}(0) = 2/(k+1)$. Let $p_S(1) = ... = p_S(k-1) = 1/(2k-2)$ and $p_S(0) = 1/2$. s and v_1 are independent. We generate v_2 by $v_2 = v_1 + s(\mod k)$. This scheme is $(2,2)-$threshold secret sharing scheme. By $\max_{s\in S} P_S(s) = 1/2$ and hence $H_\infty(S) = 1$. By $p_{S|V_2}(s|v_2) = p_S(s)p_{V_2|S}(v_2|s)/p_{V_2}(v_2)$ then $p_{0|V_2} \geq 1/(2k+2)p_{V_2}$ while $p_{S|V_2}(s|v_2) \leq 1/(k^2-1)p_{V_2}(v_2)$ for $s \neq 0$. As $k \geq 4$, for any v_2, we* *have that $p_{S|V_2}(0|v_2) > p_{S|V_2}(s|v_2)$ for $s \neq 0$. So $H_\infty(S|V_2) = 1$. $H_\infty(S|V_1) = H_\infty(S) = 1$ by s and v_1 are independent. So this scheme is 0-min security. But this scheme is not 0-Shannon security.*

Some implications do not hold in general, but holds when S is uniformly random distribution. From above results, if S is uniformly random over $\mathcal{S}$, then for a secret sharing scheme, ε-min security is stronger than ε-Shannon security, ε-Shannon security is stronger than ε-guess security, and these three security notions are the same when $\varepsilon = 0$.

4. Individual Security of Secret Sharing Schemes

In this section, we first give the security notions of individual security for secret sharing schemes based on Kolmogorov complexity, and then we consider the size of the shares based on the new concept of security in secret sharing schemes.

Definition 2. *Let $\prod$ be a secret sharing scheme for an access structure Γ. An instance $(s, v_1, v_2, ..., v_n)$ is* (i) *Kolmogorov ε-security, if for any forbidden set $F \in \mathcal{F}$ it satisfies*

$$I(s; v_F) \leq \varepsilon, \quad \textit{i.e.,} \quad K(s) - K(s|v_F) \leq \varepsilon \tag{1}$$

(ii) *normalized Kolmogorov ε-security, if for any forbidden set $F \in \mathcal{F}$ it satisfies*

$$I(s; v_F) \leq \varepsilon K(s), \quad \textit{i.e.,} \quad K(s) - K(s|v_F) \leq \varepsilon K(s). \tag{2}$$

We know that, in the notion of Kolmogorov ε-security, the security parameter ε of an instance is amount of information leakage, the maximal value of $I(s; v_F)$ for any forbidden set F. However, for example, 50 leaked bits is big for a 100-bit secret, but is small for a 1000-bit secret. So, we give the notion of normalized Kolmogorov ε-security. The parameter ε in latter notion is information leak ratio, the maximal value of $I(s; v_F)$ for any forbidden set F, divided by $K(s)$.

The notion of normalized Kolmogorov ε-security can simply be understood as a normalized version of individual security.

In fact, for the same instance $(s, v_1, v_2, ..., v_n)$, the security parameter ε is small in a forbidden set F but $I(s; v_{F'}$ is a big variance in another forbidden set F'. It is worth noting that in Definition 2, for Kolmogorov ε-security, ε is a maximum value of $\{I(s; v_F); F \in \mathcal{F}\}$, more precisely, $\varepsilon = \sup_{F \in \mathcal{F}} I(s; v_F)$. And for normalized Kolmogorov ε-security, ε is a maximum value of $\{I(s; v_F)/K(s); F \in \mathcal{F}\}$.

Now we discuss some results for Kolmogorov ε-security,

By $I(s; v_F) \leq I(s; v_{F'}) + O(1)$, if $F \subseteq F'$ (by $K(x|y) \leq K(x|y, z) + O(1)$). We know that, up to a constant, the mutual algorithmic information between s and v_i is smaller than ε, because, for any $i \in F$, we have

$$I(s; v_i) = K(s) - K(s|v_i) \leq K(s) - K(s|v_F) + O(1) \leq \varepsilon(k) + O(1).$$

Moreover, if access structure Γ is a $(t; n)$-threshold access structure, then in Definition 2(i), up to a constant, ε is a maximum value of $\{I(s; v_F); |F| = t - 1\}$, or equivalently, $\varepsilon = \sup_{|F|=t-1} I(s; v_F)$.

We show some lower bounds of share sizes of secret sharing schemes.

Theorem 3. *Let* $\prod$ *be a secret sharing scheme for an access structure* Γ.
(i) *If an instance* $(s, v_1, v_2, ..., v_n)$ *is Kolmogorov* ε*-security, then*

$$|v_i| \geq K(s) - \varepsilon - O(1)$$

for every $i \in [n]$.
(ii) *If an instance* $(s, v_1, v_2, ..., v_n)$ *is normalized Kolmogorov* ε*-security, then*

$$|v_i| \geq (1-\varepsilon)K(s) - O(1)$$

for every $i \in [n]$.

Proof. For any $i \in [n]$, there exists a forbidden set $F \in \mathcal{F}$ such that $i \notin F$ and $F \cup \{i\} \in \mathcal{Q}$. Let p a shortest binary program that computes s from v_F. By $\prod_{comb}(v_F, v_i) = s$, we have $p \leq |\prod_{comb}| + |v_i|$.
(i) If $\prod$ is Kolmogorov $\varepsilon-$security, $K(s) - K(s|v_F) \leq \varepsilon$, then we have

$$K(s) - \varepsilon \leq K(s|v_F) \leq |\Pi_{comb}| + |v_i|.$$

Thus $|v_i| \geq K(s) - \varepsilon - O(1)$.
(ii) If $\prod$ is normalized Kolmogorov ε-security, $K(s) - K(s|v_F) \leq \varepsilon K(s)$, then

$$K(s) - \varepsilon K(s) \leq K(s|v_F) \leq |\Pi_{comb}| + |v_i|.$$

Thus $|v_i| \geq (1-\varepsilon)K(s) - O(1)$. □

From above theorem, we know that a string with high Kolmogorov complexity, or a nearly Kolmogorov random string, cannot be split among participants with small share sizes and high security parameter.

5. Information Theoretic Security Versus Individual Security

In this section, we establish some relations between information theoretic security and individual security for secret sharing schemes.

First, we know that, in a secret sharing scheme, the security parameter ε is small for some instances but is a big value for other instances. This means in a secret sharing scheme, it is difficult for every instance is (normalized) Kolmogorov ε-security and ε is a small value. So we consider the case of a secret sharing scheme that the probability of an instance with low security parameter is high, *i.e.*, most of instances are (normalized) Kolmogorov ε-security and ε is a small value.

Definition 3. *Let* $\prod$ *be a secret sharing scheme for an access structure* Γ. $\prod$ *is*
(i) *Kolmogorov* (ε, δ)*-security, if for any forbidden set* F*, it satisfies*

$$\Pr_{s\in\mathcal{S}, v_F \in \times\mathcal{V}_F}[I(s; v_F|u) \leq \varepsilon] \geq \delta.$$

(ii) *normalized Kolmogorov* (ε, δ)*-security, if for any forbidden set* F*, it satisfies*

$$\Pr_{s\in\mathcal{S}, v_F \in \times\mathcal{V}_F}[I(s; v_F|u) \leq \varepsilon K(s)] \geq \delta.$$

where u *a distribution over* $\mathcal{S} \times \mathcal{V}_F$.

The following relations between Kolmogorov complexity, entropy and mutual information are important for the present paper.

Lemma 2. [11,16] *Let X, Y be random variables over $\mathcal{X}$, $\mathcal{Y}$. For any computable probability distribution $u(x,y)$ over $X \times Y$,*
(i) $0 \leq (\sum_{x,y} u(x,y)K(x|y) - H(X|Y)) \leq K(u) + O(1)$.
(ii) $I(X;Y) - K(u) \leq \sum_{x,y} u(x,y)I(x:y) \leq I(X;Y) + 2K(u)$. *When u is given, then* $I(X;Y) = \sum_{x,y} u(x,y)I(x:y|u) + O(1)$.

Here we give following relations between information theoretic security and individual security of Definition 3(i).

Theorem 4. *For any (t,n)-threshold scheme $\prod$ where S is the set of secrets and $V_{[n]}$ the set of all shares for all users, for any independent variables $S, V_{[n]}$ over $\mathcal{S}$, $\mathcal{V}_{[n]}$ with distribution u. If $\prod$ is Kolmogorov (ε,δ)-security, then , up to a constant, it is $\varepsilon + (1-\delta)\log(|S|)$-Shannon security and $\sqrt{\frac{1}{2}[\varepsilon + (1-\delta)\log(|S|)]\ln 2}$-guess security.*

Proof. For any forbidden set F, let Q be the set of Kolmogorov ε-security instances, *i.e.*, $Q = \{(s, v_{[n]}); I(s; v_F|u) \leq \varepsilon, \forall F \in \mathcal{F}\}$. Then by Lemma 2, up to a constant,

$$\begin{aligned} I(S;V_F) &\leq \sum_{(s,v_{[n]})\in Q} u(s,v)I(s:v_F|u) + \sum_{(s,v_{[n]})\notin Q} u(s,v_F)I(x:y|u) \\ &\leq \varepsilon \sum_{(s,v_{[n]})\in Q} u(s,v) + \sum_{(s,v_{[n]})\notin Q} u(s,v_F)[K(s|u) - K(s|v_F,u)] \\ &\leq \varepsilon + (1-\delta)\log(|S|). \end{aligned}$$

Then by Theorem 1, up to a constant, we have $|G(S) - G(S|V_F)| \leq \sqrt{\frac{1}{2}[\varepsilon + (1-\delta)\log(|S|)]\ln 2}$.
□

Then we establish some relations between information theoretic security and normalized individual security of Definition 3(ii).

Theorem 5. *For any (t,n)-threshold scheme $\prod$ where S is the set of secrets and $V_{[n]}$ the set of all shares for all users, for any independent variables $S, V_{[n]}$ over $\mathcal{S}$, $\mathcal{V}_{[n]}$ with distribution u. If $\prod$ is normalized Kolmogorov (ε,δ)-security, then, up to a constant, it is $(1+\varepsilon-\delta)\log(|S|)$-Shannon security and $\sqrt{\frac{1}{2}(1+\varepsilon-\delta)\log(|S|)\ln 2}$-guess security.*

Proof. $\prod$ is normalized Kolmogorov (ε,δ)-security, then the probability that an instance is normalized Kolmogorov ε-security is at least δ, *i.e.*, for any forbidden set F,

$$\Pr_{s\in\mathcal{S}, v_F \in \times \mathcal{V}_F} [I(s; v_F|u) \leq \varepsilon K(s)] \geq \delta.$$

For any forbidden set F, let Q be the set of normalized Kolmogorov ε-security instances, *i.e.*, $Q = \{(s, v_{[n]}); I(s; v_F|u) \leq \varepsilon K(s), \forall F \in \mathcal{F}\}$. Then by Lemma 2, up to a constant,

$$\begin{aligned}
I(S;V_F) &\leq \sum_{(s,v_{[n]})\in Q} u(s,v)I(s:v_F|u) + \sum_{(s,v_{[n]})\notin Q} u(s,v_F)I(x:y|u) \\
&\leq \varepsilon \sum_{(s,v_{[n]})\in Q} u(s,v)K(s|u) + \sum_{(s,v_{[n]})\notin Q} u(s,v_F)[K(s|u) - K(s|v_F,u)] \\
&\leq \varepsilon \log(|S|) + (1-\delta)\log(|S|) \\
&\leq (1+\varepsilon-\delta)\log(|S|).
\end{aligned}$$

Then by Theorem 1, up to a constant, we have $|G(S) - G(S|V_F)| \leq \sqrt{\frac{1}{2}(1+\varepsilon-\delta)\log(|S|)\ln 2}$.
□

Comparing the Theorem 4 with Theorem 5, we have different relations between entropy-based security notions and two versions of individual security for secret sharing schemes.

6. Conclusions

Kolmogorov complexity and entropy measures are fundamentally different measures. They both are used in measuring the security for secret sharing schemes. In this paper, we study relations of several security notions for secret sharing schemes. First we consider three security notions of information theoretic security of secret sharing schemes, ε-Shannon and ε-min security both are stronger than ε-guess security, and ε-min security is stronger than ε-Shannon security when S is uniformly random. However, for a secret sharing scheme, 0-min security, 0-guess security and 0-Shannon security are the same when S is uniformly random. Then after giving the security notions of individual security for secret sharing schemes in the frame work of Kolmogorov complexity, we establish some relations between information theoretic security and two versions of individual security for secret sharing schemes, respectively.

In this paper, we only considered relations of several security notions for secret sharing schemes. Naturally, a more detailed discussion of connections with other security notions in other fields of cryptography, such as the security notions based on conditional Rényi entropies in [6,7], will be both necessary and interesting.

Acknowledgments

The authors are grateful for the financial support partly from the NSF Project (No. 61274133) of China.

Author Contributions

Both authors have contributed to the study and preparation of the article. Both authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the 1979 AFIPS National Computer Conference, New York, NY, USA, 4–7 June 1979; Volume 48, pp. 313–317.
2. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613.
3. Blundo, C.; De Santis, A.; Vaccaro, U. On secret sharing schemes. *Inf. Process. Lett.* **1998**, *65*, 25–32.
4. Karnin, E.D.; Greene, J.W.; Hellman, M.E. On secret sharing systems. *IEEE Trans. Inf. Theory* **1983**, *29*, 35–41.
5. Iwamoto, M.; Ohta, K. Security notions for information theoretically secure encryptions. In Proceedings of 2011 IEEE International Symposium on Information Theory (ISIT), St. Petersburg, Russia, 31 July–5 August; pp. 1777–1781.
6. Iwamoto, M.; Shikata, J. Information theoretic security for encryption based on conditional Rényi entropies. In Proceedings of the 7th International Conference on Information Theoretic Security (ICITS 2013), Singapore, Singapore, 28–30 November 2013; pp. 103–121.
7. Iwamoto, M.; Shikata, J. Secret sharing schemes based on min-entropies. **2014**, arXiv:1401.5896.
8. Chaitin, G. On the length of programs for computing finite binary sequences. *J. ACM* **1966**, *13*, 547–569.
9. Kolmogorov, A. Three approaches to the quantitative definition of information. *Probl. Inf. Transm.* **1965**, *1*, 1–7.
10. Solomonoff, R. A formal theory of inductive inference, part I. *Inf. Control* **1964**, *7*, 1–22.
11. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley: Hoboken, NJ, USA, 2006.
12. Li, M.; Vitányi, P.M.B. *An Introduction to Kolmogorov Complexity and Its Applications*, 3rd ed.; Springer: New York, NY, USA, 2008.
13. Grünwald, P.; Vitányi, P. Shannon information and Kolmogorov complexity. **2008**, arXiv:cs/0410002v1.
14. Pinto, A. Comparing notions of computational entropy. *Theory Comput. Syst.* **2009**, *45*, 944–962.
15. Teixeira, A.; Matos, A.; Souto, A.; Antunes, L. Entropy measures *vs.* Kolmogorov complexity. *Entropy* **2011**, *13*, 595–611.
16. 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.
17. Kaced, T. Almost-perfect secret sharing. In Proceedings of 2011 IEEE International Symposium on Information Theory (ISIT), St. Petersburg, Russia, 31 July–5 August 2011, 1603–1607.
18. Jiang, S. On Unconditional ϵ-Security of Private Key Encryption. *Comput. J.* **2013**, doi:10.1093/comjnl/bxt097.
19. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948** , *27*, 379–423, 623–656.
20. Alimomeni, M.; Safavi-Naini, R. Guessing secrecy. In Proceedings of 6th International Conference on Information Theoretic Security (ICITS 2012), Montreal, QC, Canada, 15–17 August 2012; pp. 1–13.

21. Capocelli, R. M.; De Santis, A.; Gargano, L.; Vaccaro, U. On the size of shares for secret sharing schemes. *J. Cryptol.* **1993**, *6*, 157–167.
22. Stinson, D.R. Decomposition constructions for secret sharing Schemes. *IEEE Trans. Inf. Theory* **1994**, *40*, 118–125.