Cryptographic security of individual instances for conference key distribution

SONGSONG DAI, SIZHAO LI, YANGBING WU and DONGHUI GUO*
Department of Electronic Engineering
Xiamen University
Xiamen, 361005, Fujian
CHINA
{ssdai,sizhao.li,ybwu}@stu.xmu.edu.cn;dhguo@xmu.edu.cn

Abstract: A conference key distribution is a scheme that allows the designated subset of users to compute a shared key for secure communication. In this paper we analyze secure instances of conference key distribution based on the ideas of Kolmogorov complexity. First, Kolmogorov complexity is used as a measure of the individual security in conference key distribution, we present a model for conference key distribution in terms of Kolmogorov complexity. Then, Kolmogorov complexity is used as a measure of the amount of randomness needed by secure instances of conference key distribution. Thus we give the lower bounds holding in the model for each user needed to store. Moreover, we give lower bounds on the amount of information in conference key distribution for various types of combinatorial structures.

Key–Words: Cryptography, Conference key distribution, Combinatorial design, Cryptographic security, Kolmogorov complexity.

1 Introduction

Key distribution is an important part in both theoretical and practical cryptography. In a conference key distribution system, a group of users obtains a shared private key that is only known to the group members. The key can be used for securing group communications. In conference key distribution systems, the conference key can be computed by the conference members without any interaction.

In many theoretical and application researches, information measures play an important role in conference key distribution. In conference key distribution schemes, the entropy based security property can be formalized in information-theoretic security framework. The entropy measures, includes Shannon, min and Renyi entropies, are frequently used in conference key distribution schemes. Shannon entropy is the most widely used information measure in conference key distribution schemes (see [5, 6, 7, 8, 9, 16]). Recently, min and Renyi entropies have been used in key distribution schemes [1, 13, 17, 33]. Kolmogorov complexity [23], known as algorithmic information theory, measures the quantities of information in a single string x, by the size of the smallest program that generates it. Kolmogorov complexity and entropy measure are two different measures. Relations between Kolmogorov complexity and entropy measures (including Shannon, min, Yao and Renyi entropies) have been proposed in [22, 28, 37]. Kolmogorov complexity has been used in various areas of cryptography. Kolmogorov complexity is applied to analysis the existence of pseudorandom generators in [2] and one-way function in [4, 24, 25]. Tadaki and Doi [36] investigated the secure instantiation of the random oracle using concepts and methods of algorithmic randomness.

Traditionally, information-theoretic security is a notion of average-case analysis for cryptographic systems. This notion based on Shannon entropy $H(X)$ which a measure of the average uncertainty in the random variable X. Perfect secrecy [34] is a strong security notion. We know that plaintexts M and ciphertexts C are statistically independent does not mean every plaintext $m \in M$ and ciphertext $c \in C$ are (algorithmic) independent. This means even in unconditionally secure cryptosystems, there are particular instances are insecure in terms of Kolmogorov complexity. In practice, a plaintext is encrypted into a ciphertext, we should consider the algorithmic mutual information $I(m;c)$ between the plaintext m and the ciphertext c, not the mutual information $I(M;C)$ between plaintexts M and ciphertexts C. Also notice that perfect secrecy implies the lower bound on secret keys $H(S) \geq H(M)$. However, there are par-

*Corresponding author

ticular instances with $K(s) < K(m)$ in the case of $H(S) \geq H(M)$. In the set of binary strings $\{0,1\}^{\mathrm{n}}$, many $\mathrm{x} \in \{0,1\}^{\mathrm{n}}$ have low Kolmogorov complexity even if the adversary does not know the ciphertext. For example, the Kolmogorov complexity of $111\cdots11 \in \{0,1\}^{\mathrm{n}}$ is almost vanishing, which can not be used as a key in our daily life. So entropy based security is a notion of average case security, which cannot replace individual instance security. Antunes et al. [3] proposed cryptographic security of individual instances based on Kolmogorov complexity and characterized the relation between instance security and information theoretic security. Recently, security of individual instances in the frame work of Kolmogorov complexity for secret sharing schemes have been studied in [3, 12, 18]. Here, we consider the Kolmogorov complexity based security of conference key distribution and the lower bounds holding for each user needed to store in conference key distribution.

By varying the designs of conferences, we can generate various schemes. There have been numerous proposals for key distribution schemes based on various types of combinatorial structures. Blom [6] proposed a key predistribution scheme for conferences. Matsumoto and Imai [26] extended this work to conferences of size larger than two. Blundo et al. [8] proposed a key distribution scheme for communication graphs and asymmetric communication models. Fiat and Naor [15] used a combinatorial approach to construct key distribution schemes. Camtepe and Yener [11] introduced the use of combinatorial designs in key predistribution schemes. Many researchers continued to further develop this combinatorial approach. Lee and Stinson [19, 20, 21] gave a construction based on transversal designs, Dong et al. [14] used 3-designs, Ruj and Roy [29] used partially balanced designs, and Bose et al. [10] and Ruj et al. [30, 31, 32] used balanced incomplete block designs in key predistribution schemes. Paterson and Stinson [27] provided a general framework for these combinatorial key predistribution schemes.

In this paper, we study conference key distribution schemes by using Kolmogorov complexity. In Section 2, we recall related works of individual security for cryptographic systems. In Section 3, we give some preliminaries on Kolmogorov complexity. In Section 4, we present a model for conference key distribution in terms of Kolmogorov complexity. In Section 5, we present the lower bounds holding in the model of conference key distribution. In Section 6, we use combinatorial designs for conference key distribution and present lower bounds on the amount of information (in Kolmogorov complexity) that each user has to store for various types of combinatorial structures. The conclusion and future work are presented in Section 7.

2 Related works

There are several researches related to security of individual instances in the frame work of Kolmogorov complexity for cryptographic systems. We list some researches on the individual security of cryptographic systems, cipher systems and secret sharing schemes.

2.1 Individual Secrecy of Cipher Systems

A private key cipher system is a five tuple (M, C, S, e, d), where M is the plaintext space, C is the ciphertext space, S is the key space, $e : S\times M\rightarrow C$ is the encryption algorithm, $d : S\times C\rightarrow M$ is the decryption algorithm and $d(k, e(k, m)) = m$.

Antunes et al. [3] introduced the following concept.

Definition 1. *Let (M, C, S, e, d) be a private key cipher system, f be a distribution over $M \times S$. An instance (m, s) of the system is ε-secure if $I(m : e(s, m)|f)\leq\varepsilon$.*

Theorem 1. *Let (M, C, S, e, d) be a private key cipher system, f be a distribution over $M \times S$. If the probability that an instance is ε-secure is at least $(1 - \delta)$, then the system has $(\varepsilon + \delta \log |M|)$-secure,i.e.,$I(M; C)\leq\varepsilon + \delta \log |M|$.*

2.2 Individual Secrecy of Threshold Secret Sharing Schemes

A (t, n)-threshold secret sharing scheme is a four tuple $(S, V, f_{share}, f_{comb})$, where S is the set of secret information, V is the set of shares for all users, $|V| = n$, f_{share} is an algorithm for generating shares for all users, f_{comb} is an algorithm for recovering a secret.

There are several researches related to individual security of secret sharing schemes [3, 12, 18]. For simplicity, we only recall the individual security of threshold scheme in [3].

Definition 2. *Let $(S, V, f_{share}, f_{comb})$ be a (t, n)-threshold secret sharing scheme. An instance $(s, v_1, v_2, ..., v_n)$ is ε-secure if*

$$I(m : (v_{i_1}, ...v_{i_{t-1}}))\leq\varepsilon,$$

for any $(v_{i_1}, ...v_{i_{t-1}}) \subseteq (v_1, v_2, ..., v_n)$.

Theorem 2. *Let $(S, V, f_{share}, f_{comb})$ be a (t, n)-threshold secret sharing scheme, f be a distribution over $S \times V_{[n]}$. If the probability that an instance is ε-secure is at least $(1-\delta)$, then the scheme has $(\varepsilon + \delta \log |S|)$ secrecy.*

3 Preliminaries

String means a finite binary string. The set of all finite binary strings is denoted by $\Sigma^* := \{0,1\}^*$. Function log represents the function $\log_2$. $|x|$ represents the length of a string x. For the cardinality of a set A we write |A|. We first briefly recall some basic notions of Kolmogorov complexity [23].

Definition 3. *The conditional Kolmogorov complexity $K(y|x)$ of with y condition x, with respect to a universal Turing machine U, is defined by*

$$K_U(y|x) = min\{|p| : U(p,x) = y\}. \quad (1)$$

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

$$K_U(y|x) \leq K_F(y|x) + c_F. \quad (2)$$

for all x, y, where c_F depends on F but not on x, y. So we fix such a universal machine U, write $K(y|x) := K_U(y|x)$, and call $K(y|x)$ the conditional Kolmogorov complexity of y with respect to x. The (unconditional) Kolmogorov complexity $K_U(y|\Lambda)$ of y is defined as where Λ is the empty string.

Let $\overset{+}{\leq}$ be an inequality to within an additive constant, and $\overset{+}{=}$ be the situation when both $\overset{+}{\leq}$ and $\overset{+}{\geq}$ hold.

The *algorithmic entropy* of y with respect to x is

$$H(y|x) := -log \sum_{p:U(p,x)=y} 2^{-l(p)}, \quad (3)$$

and we have

$$H(y|x) \overset{+}{=} K(y|x). \quad (4)$$

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

$$I(x:y) = K(x) - K(x|y). \quad (5)$$

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

In algorithmic information theory, symmetry of information phenomenon for strings was known that if x has a constant amount information about y, then y has $O(\log n)$ information about x.

Similar to $\overset{+}{\leq}$ and $\overset{+}{=}$, $\overset{\log}{\leq}$ is used to denote an inequality to within an additive logarithmic term, and $\overset{\log}{=}$ to denote the situation when both $\overset{\log}{\leq}$ and $\overset{\log}{\geq}$ hold.

Theorem 3 (Symmetry of Algorithmic Information)**.** *(See [4, 24, 25].) For all strings x and y in $\{0,1\}^n$*

$$K(x,y) \overset{\log}{=} K(x) + K(y|x). \quad (6)$$

Within logarithmic error, $I(x:y)$ represents both the information in about x and y that in about y and x, i.e.,

$$I(x:y) \overset{\log}{=} I(y:x). \quad (7)$$

Up to an additive logarithmic term, $K(x,y)$ is the length of the shortest program such that U computes both x and y and away to tell them apart (See [23],p.109), i.e.,

$$K(x,y) \overset{\log}{\leq} K(x) + K(y) \quad (8)$$

for all x, y.

4 The Model

In this section we formally describe the key distribution problem and model.

Let $[n] := \{1,2,...,n\}$ be a finite set of IDs of n users. For every $i \in [n]$, let u_i be information of the user i. Similarly, for any subset $X := \{i_1, i_2, ..., i_u\} \subset [n]$, $u_X := \{u_{i_1}, u_{i_2}, ..., u_{i_u}\}$. We denote by S_Y the common key for the group $Y \subset [n]$. An instance of t-conference key distribution is denoted by $(s_X, u_{[n]})$ where $s_X \in S_X, u_{[n]} \in U_{[n]}$.

Definition 4. *Let t and w be nonnegative integers with $w + t \leq n$. An instance $(s_X, u_{[n]})$of t-conference key distribution is w-secure for n users if:*

1. Each t user can compute the common key. Formally, for all $X \subset [n]$ with $|X| = t$, for each user i, $i \in X$, it holds that

$$K(s_X|u_i) \overset{+}{=} 0. \quad (9)$$

2. Any group of w users have no algorithmic information on any key they should not know. Formally, for all $Y, X \subseteq [1,2,...,n]$, with $|Y| = w, |X| = t$, and $X \cap Y = \emptyset$, it holds that

$$K(s_X) \overset{+}{=} K(s_X|u_Y). \quad (10)$$

Notice that $K(s_X) = K(s_X|u_Y)$ is equivalent to saying that $s_X$and u_Y are algorithmic independent. Thus, the values u_Y reveal no algorithmic information on the common key s_X.

This security notion is also based on algorithmic entropy because of Eq.(4).

Moreover, property 2 can be equivalently written as;

2'. For all $Y, X \subset [n]$, with $|Y| = w$,$|X| = t$, and $X \bigcap Y = \emptyset$, it holds that

$$I(s_X; u_Y) \overset{+}{=} 0 \quad (11)$$

We use Kolmogorov complexity to define what it means for an individual instance of a conference key distribution system to be secure. We now prove that if almost all individual instances of a conference key distribution system are secure with $K(s_X) \stackrel{+}{=} K(s_X|u_Y)$, then the system is almost perfect secure.

Theorem 4. *For any conference key distribution system, if the probability that an instance $(s_X, u_{[n]})$is secure with $K(s_X) \stackrel{+}{=} K(s_X|u_Y)$ is at least $1-\frac{1}{|s_X+u_Y|^c}$ for some constant c, then the system is secure with $\mathrm{I(S_X; U_Y)} \leq \frac{1}{|s_X+u_Y|^{c-1}}$*

Proof. We have that up to an additive constant, $\mathrm{I(S_X; U_Y)} \leq \sum_{s_X,u_Y} f(s_X, u_Y)I(s_X; u_Y)$, where f is the distribution over $S_{[n]} \times U_{[n]}$. Let $\mathrm{Q} = \{(s_X, u_Y)|K(s_X) \stackrel{+}{=} K(s_X|u_Y)\}$ for a fixed constant c, then we have

$$\begin{aligned} I(S_X; U_Y) &\leq \sum_{(s_X,u_Y)\in Q} f(s_X, u_Y)I(s_X; u_Y) \\ &\quad + \sum_{(s_X,u_Y)\notin Q} f(s_X, u_Y)I(s_X; u_Y) \\ &\stackrel{+}{\leq} K \sum_{(s_X,u_Y)\notin Q} f(s_X, u_Y)I(s_X; u_Y) \\ &\stackrel{+}{\leq} \frac{1}{|s_X + u_Y|^c}(K(s_X) - K(s_X|u_Y)) \\ &\stackrel{+}{\leq} \frac{1}{|s_X + u_Y|^c}K(s_X) \\ &\stackrel{+}{\leq} \frac{1}{|s_X + u_Y|^{c-1}}. \end{aligned}$$

Thus, up to an additive constant, $\mathrm{I(S_X; U_Y)} \leq \frac{1}{|s_X+u_Y|^{c-1}}$. □

This result shows that Kolmogorov complexity based security is a sharper notion than entropy based security for conference key distribution.

5 Lower bound

In this section, we prove lower bound on the amount of information (in Kolmogorov complexity) of the user in a w-secure t-conference key distribution scheme.

Up to an additive logarithmic term, the knowledge of $w$keys does not convey more information on any other key in a w-secure t-conference key distribution scheme. This is formalized by the next lemma.

Lemma 1. *Let r, w, and t be integers with $w+t \leq n$. Let $X, Y_1, ..., Y_r, Z \subseteq [n]$ such that $|Z| = w, Z \cap X = \emptyset, Z \cap Y_i \neq \emptyset$ and $|X| = |Y_i| = t$, for $i = 1, ..., r$. If an instance $(s_X, u_{[n]})$of t-conference key distribution is w-secure for n users. Then,*

$$K(s_X|s_{Y_1}, \cdots, s_{Y_r}) \stackrel{\log}{\geq} K(s_X). \tag{12}$$

Proof. First, by property 1, we have

$$\begin{aligned} & I(s_{Y_1}, \cdots, s_{Y_r}; s_X|u_Z) \\ = \; & K(s_{Y_1}, \cdots, s_{Y_r}|u_Z) \\ & -K(s_{Y_1}, \cdots, s_{Y_r}|u_Z, S_X) \\ \leq \; & K(s_{Y_1}, \cdots, s_{Y_r}|u_Z) \\ \stackrel{\log}{\leq} \; & K(s_{Y_1}|u_Z) + \cdots + K(s_{Y_r}|u_Z) \\ \stackrel{\log}{\leq} \; & 0. \end{aligned}$$

Then by the symmetry of algorithmic information,

$$I(s_{Y_1}, \cdots, s_{Y_r}; s_X|u_Z) \stackrel{\log}{=} I(s_X; s_{Y_1}, \cdots, s_{Y_r}|u_Z).$$

This means

$$K(s_X|u_Z) - K(s_X|u_Z, s_{Y_1}, \cdots, s_{Y_r}) \stackrel{\log}{\leq} 0,$$

i.e.,

$$K(s_X|u_Z) \stackrel{\log}{\leq} K(s_X|u_Z, s_{Y_1}, \cdots, s_{Y_r}).$$

Then we have

$$\begin{aligned} K(s_X) &\stackrel{+}{=} K(s_X|u_Z) \\ &\stackrel{\log}{\leq} K(s_X|u_Z, s_{Y_1}, \cdots, s_{Y_r}) \\ &\leq K(s_X|s_{Y_1}, \cdots, s_{Y_r}) + O(1). \end{aligned}$$

Therefore, $K(s_X) \stackrel{\log}{\leq} K(s_X|s_{Y_1}, \cdots, s_{Y_r})$. □

Then we obtain a lower bound on the amount of information (in Kolmogorov complexity) of the each user.

Theorem 5. *Let k and t be integers with $k + t \leq n$. Let $(s_X, u_{[n]})$an instance of w-secure t-conference key distribution for n users, if $K(s_X) \stackrel{\log}{=} \mu$ for all $X \subset [n]$ with $|X| = t$, then the Kolmogorov complexity $K(u_i)$ satisfies*

$$K(U_i) \stackrel{\log}{\geq} \binom{k+t-1}{t-1}\mu. \tag{13}$$

Proof. Consider the set of indices $I = [j_1, ..., j_{k+t-1}]$ and an index i such that $i \notin I$. Define set C as $C = [j_1, ..., j_k]$ and set A as $A = [i, jk+1, ..., jk+t-1]$. Let $m = \binom{k+t-1}{t-1}$. B_l, for $l = 1, 2, ..., m$, is constructed taking the element i along with any $(t-1)$ elements from the set I, with the exception of $[j_{k+1}, ..., j_{k+t-1}]$, i.e.,

$$\begin{aligned} B_l \in \{\{i, x_1, ..., x_{t-1}\} | x_1, ..., x_{t-1} \in I, \\ \{x_1, ..., x_{t-1}\} \neq \{[j_{k+1}, ..., j_{k+t-1}\}\}. \end{aligned}$$

From symmetry of algorithmic information and property 2, we have

$$\begin{aligned} & K(u_i) - K(u_i | s_{B_1}, \cdots, s_{B_m}, s_A) \\ \stackrel{\log}{=} & K(s_{B_1}, \cdots, s_{B_m}, s_A) \\ & -K(s_{B_1}, \cdots, s_{B_m}, s_A | u_i) \\ \stackrel{\log}{\geq} & K(s_{B_1}, \cdots, s_{B_m}, s_A) \\ & -\sum_{l=1}^{m} K(s_{B_l} | u_i) - K(s_A | u_i) \\ \stackrel{\log}{\geq} & K(s_{B_1}, \cdots, s_{B_m}, s_A). \end{aligned}$$

Moreover, by symmetry of algorithmic information

$$\begin{aligned} K(u_i) \stackrel{\log}{\geq} & K(s_{B_1}, \cdots, s_{B_m}, s_A) \\ = & K(s_{B_1}) + K(s_{B_2} | s_{B_1}) + , \cdots , \\ & + K(s_A | s_{B_1}, \cdots, s_{B_m}) \end{aligned}$$

Let $X = A, Z = C$, and $Y_i = B_i$ for $i = 1, ..., m$, by lemma 1

$$K(s_A | s_{B_1}, \cdots, s_{B_m}) \stackrel{\log}{\geq} K(s_X)$$

Moreover, for each $h, 1 \leq h \leq m$, let $X = B_h, Z = I/B_h$, and $Y_i = B_i$, for $i = 1, ..., h-1$. Then,

$$K(s_{B_h} | s_{B_1}, \cdots, s_{B_{h-1}}) \stackrel{\log}{\geq} K(s_{B_h})$$

Therefore,

$$\begin{aligned} K(u_i) \stackrel{\log}{\geq} & K(s_{B_1}, \cdots, s_{B_m}, s_A) \\ \stackrel{\log}{\geq} & K(s_{B_1}) + K(s_{B_2} | s_{B_1}) + , \cdots , \\ & + K(s_A | s_{B_1}, \cdots, s_{B_m}) \\ \stackrel{\log}{\geq} & K(s_{B_1}) + K(s_{B_2}) + , \cdots , + K(s_A) \\ \stackrel{\log}{\geq} & (m+1)\mu \\ = & \binom{k+t-1}{t-1} \mu. \end{aligned}$$

□

6 Instance Security of conference key distribution for combinatorial framework

By varying the designs of conferences, we can generate various schemes and this makes the model quite flexible. In this section, we use combinatorial designs for conference key distribution. First we formally define the combinatorial framework we use in this paper. This framework is employed in several recent papers [27, 29, 30, 31, 32]. Then Conference key distribution schemes for various types of combinatorial structures are discussed.

We begin with the definition of a design [27]. A combinatorial design (or, a design) is a pair (U, Γ), where Γ is a finite set of subsets of U called blocks. The number of blocks containing a point $x \in U$ is called the degree of x . If all points have the same degree r, then (U, Γ) is called to be regular (of degree r) . The rank of (U, Γ) is the size of the largest block. If all blocks have the same size k, then (U, Γ) is said to be uniform (of rank k).

Example 1. *Let*

$$U = \{1, 2, 3, 4, 5, 6, 7, 8\},$$

and

$$\mathcal{A} = \{1234, 4568, 1256, 3478, 1278, 3456\}.$$

Then $(U, \mathcal{A})$ is a design in which there are eight points and six blocks. This design is regular of degree 3 and uniform of rank 4.

A design (U, Γ) is used as the key ring space. In a w-conference key distribution scheme for n users each block of users is able to compute a common key. It can be the case that some t-tuples of users will never need to compute a common key.

Definition 4 can be extended to a key distribution scheme for any combinatorial design $(U, \mathcal{A})$, as follows.

Definition 5. *Let $(U, \mathcal{A})$ is a design, $U = \{U_i : 1 \leq i \leq n\}$ and $\mathcal{A} = \{A_j : 1 \leq j \leq b\}$. A non-interactive key distribution scheme for $(U, \mathcal{A})$ is secure if*

1". Each block of users can non-interactively compute the common key. For all $U_i \in A_j$,

$$K(S_{A_j} | U_i) \stackrel{+}{=} 0. \tag{14}$$

2". Any group of w users have no information on a key they should not know. Formally, for all $X \subseteq U$, with $|X| = w$ and $X \cap Y = \emptyset$, it holds that

$$K(S_{A_j}) \stackrel{+}{=} K(S_{A_j}|U_X). \tag{15}$$

for any A_j, $1 \leq j \leq b$, with $X \cap A_j = \emptyset$.

Then we obtain a lower bound on the amount of information (in Kolmogorov complexity) of the each user for the above security model of conference key distribution.

Theorem 6. *Let (U, Γ) be a design with $U := [n]$ and $\Gamma := \{A_j : 1 \leq j \leq b\}$, Suppose that all keys have the same Kolmogorov complexity within an additive logarithmic term, i.e. , $K(s_{A_j}) \stackrel{\log}{=} \mu$, for all $A_j \in \Gamma$, $1 \leq j \leq b$. If a key distribution instance $(s_A, u_{[n]})$ is w-secure for (U, Γ), then the Kolmogorov complexity $K(u_i)$ of each user satisfies*

$$K(u_i) \stackrel{\log}{\geq} \lambda \cdot \mu \tag{16}$$

where $\lambda = \min\{w + 1, \deg(i)\}$.

Proof. Let $A_1, ..., A_\gamma$ be blocks containing i of the design described by (U, Γ). Then

$$\begin{aligned} & K(u_i) - K(u_i|s_{A_1}, \cdots, s_{A_\gamma}) \\ \stackrel{\log}{=} & K(s_{A_1}, \cdots, s_{A_\gamma}) - K(s_{A_1}, \cdots, s_{A_\gamma}|u_i). \end{aligned}$$

Then from property 1", we have

$$\begin{aligned} K(u_i) & \stackrel{\log}{\geq} K(s_{A_1}, \cdots, s_{A_\gamma}) - K(s_{A_1}, \cdots, s_{A_\gamma}|u_i) \\ & \stackrel{\log}{\geq} K(s_{A_1}|s_{A_2}) + K(s_{A_2}|s_{A_1}) +, \cdots, \\ & \quad + K(s_{A_\gamma}|s_{A_2}, ..., s_{A_\gamma}) - \sum_{l=1}^{\gamma} K(s_{A_l}|u_i) \\ & \stackrel{\log}{\geq} K(s_{A_1}) + K(s_{A_2}) +, \cdots, + K(s_{A_\gamma}) - 0 \\ & \stackrel{\log}{\geq} \gamma \cdot \mu \end{aligned}$$

□

We have discussed the non-interactive conference key distribution for combinatorial designs based on Kolmogorov complexity. There are several combinatorial structures widely used in key distribution. Next we discuss conference key distribution schemes for various types of combinatorial structures, such as partially balanced t-designs, transversal designs, communication graph and asymmetric communication models.

6.1 Partially balanced t-design

Let v, k, t be positive integers and let λ_i be a positive integer, for $0 \leq i \leq t-1$. A $t-(v, k, \lambda_0, ..., \lambda_{t-1})$-partially balanced t-design [27] is a pair (U, Γ) that satisfies the following properties:

1. (U, Γ) is uniform of rank k, i.e., Γ is a set of k-subsets of U.
2. $|\Gamma| = \lambda_0$.
3. For $1 \leq i \leq t-1$, every i-subset of points occurs in either 0 or λ_i blocks.
4. For $t \leq i \leq k$, every i-subset of points occurs in either 0 or 1 blocks.

A partially balanced t-design is a design of degree $r = \gamma_1$, i.e., every point occurs in exactly γ_1 blocks [27]. Then from theorem 6, we have next corollary that the lower bound on the size of user's information in a w-secure key distribution scheme for a partially balanced t-design.

Corollary 1. *Let (U, Γ) be a $t-(v, k, \gamma_0, ..., \gamma_{t-1})$-partially balanced t-design with $U := [n]$. suppose that $K(s_{A_j}) \stackrel{\log}{=} \mu$ for all $A_j \in \Gamma$, $1 \leq j \leq b$. If a key distribution instance $(s_A, u_{[n]})$ is w-secure for (U, Γ), then the Kolmogorov complexity $K(u_i)$ of each user satisfies*

$$K(u_i) \stackrel{\log}{\geq} \lambda \cdot \mu \tag{17}$$

where $\lambda = \min\{w + 1, \gamma_1\}$.

6.2 Transversal design

A transversal design $TD(t, k, n)$ [27, 31, 35], with $k$groups of size n and indexγ, is a triple (U, H, Γ) where:

1, $|U| = kn$.
2, $\mathcal{H}$ is a partition of U into k parts of size n.
3, (U, Γ) is uniform of rank k, i.e., Γ is a set of k-subsets of U.
4, $|H \cap A| = 1$ for every $H \in \mathcal{H}$ and $A \in \mathcal{A}$
5, Every t-subsets of U from t different parts occurs in exactly one block in Γ.

The following result follows from simple counting in [27] .

Lemma 2. *Suppose $(U, \mathcal{H}, \mathcal{A})$ is a transversal design $TD(t, k, n)$. Then $(U, \mathcal{A})$ is a $t-(v, k, \lambda_0, ..., \lambda_{t-1})$-partially balanced t-design where $v = kn$ and $\lambda_i = n^{t-i}$ for $0 \leq i \leq t-1$.*

Then by lemma 2 and corollary 1, we have next corollary that the lower bound on the size of user's

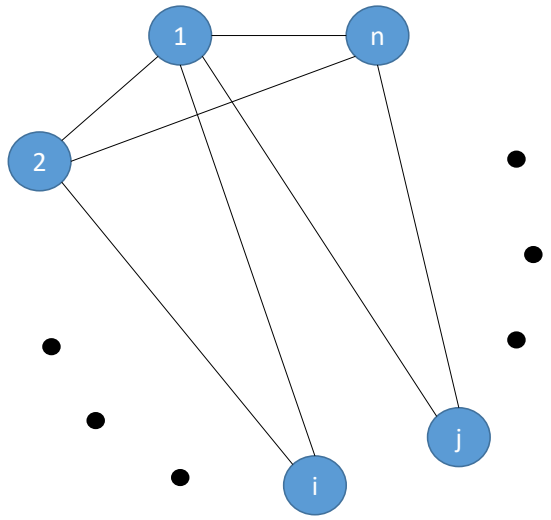

Figure 1: Communication graph

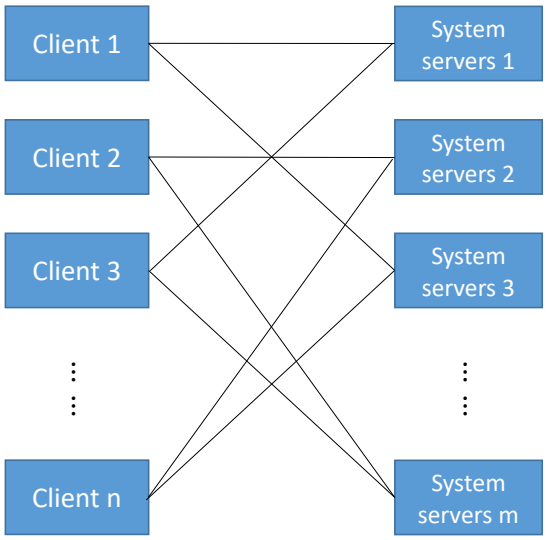

Figure 2: The asymmetric model

information in a noninteractive w-secure key distribution scheme for a transversal design $TD(t,k,n)$.

Corollary 2. *Let (U,H,Γ) be a transversal design $TD(t,k,n)$. Let w be a known integer with $w+k \leq kn$, suppose that $K(s_{A_j}) \overset{\log}{=} \mu$ for all $A_j \in \Gamma$, $1 \leq j \leq b$. If a key distribution instance $(s_A, u_{[n]})$ is w-secure for (U,H,Γ), then the Kolmogorov complexity $K(u_i)$ of each user satisfies*

$$K(u_i) \overset{\log}{\geq} \lambda \cdot \mu \tag{18}$$

where $\lambda = \min\{w+1, n^{t-1}\}$.

6.3 Communication graph

Communication graph [8] is a communication structure, which contains all possible pairs (conferences). Communication graph C is a subset of $U \times U$, as shown in Fig. 1. The communication structure C is a uniform design of rank 2.

The next corollary gives a lower bound on the size of user's information in a w-secure key distribution scheme for a communication graph. Its proof is very similar to the proof of Theorem 3, so it is omitted.

Corollary 3. *Let U be a set of n users, C be a communication graph on U. Let w be a known integer with $w+2 \leq n$, suppose that $K(s_{A_j}) \overset{\log}{=} \mu$ for all $A_j \in C$. If a key distribution instance $(s_A, u_{[n]})$ is w-secure for C, the Kolmogorov complexity $K(u_i)$ of each user satisfies*

$$K(u_i) \overset{\log}{\geq} \lambda \cdot \mu \tag{19}$$

where $\lambda = \min\{w+1, \deg(i)\}$.

6.4 The asymmetric model

An asymmetric key distribution [8] distributes some information among a clients set A and a system-servers set B. Each pair consisting of a system-server and a client is able to compute a common key. A client is not able to claim to be a system-server nor is a system-server able to claim to be a client. This is called the asymmetric key distribution for clients set A and system-servers set B. It is w-secure if any w entities (clients, system-servers, or both) have no information on any common key they should not know. Formally, the asymmetric model is a combinatorial design $(U,(A,B),C)$ where:

1, $|U| = m+n$.
2, (A,B) is a partition of U into 2 parts with $|A| = n, |B| = m$.
3, (U,C) is uniform of rank k, i.e., C is a set of 2-subsets of U.
4, For each C, $|C \bigcap A| = 1$and $|C \bigcap B| = 1$.
5, Every 2-subsets of U from 2 different parts occurs in exactly one block in C.

The asymmetric model $(U,(A,B),C)$ is a combinatorial design of degree $\max\{m,n\}$ in which there are $m+n$ points and 2 blocks, as shown in Fig. 2.

Corollary 4. *Let $(U,(A,B),C)$ be a asymmetric model and let $w$be an integer with $w+2 \leq n+m$. Suppose that $K(s_{A_j}) \overset{\log}{=} \mu_1$ for all $A_j \in A$, $K(s_{B_j}) \overset{\log}{=} \mu_2$ for all $B_j \in B$. If an asymmetric key distribution instance is w-secure for the asymmetric model*

$(U,(A,B),C)$, then for $i \in A$, $K(u_i)$ satisfies

$$K(u_i) \overset{\log}{\geq} \lambda \cdot \mu_1 \tag{20}$$

where $\lambda = \min\{w+1, m\}$, while for $i \in B$, $K(u_i)$ satisfies

$$K(u_i) \overset{\log}{\geq} \lambda \cdot \mu_2 \tag{21}$$

where $\lambda = \min\{w+1, n\}$.

7 Conclusions

In this paper we studied conference key distribution based on Kolmogorov complexity. We considered definitions of security for conference key distribution. We derived a lower bound for the Kolmogorov complexity of user key, $K(u_i)$, for conference key distribution. Then, we considered conference key distribution for a general class of combinatorial designs and we gave the bounds on the amount of information of user. Finally, we discussed conference key distribution for partially balanced t-designs, transversal designs, communication graph and asymmetric communication models.

An interesting area for further research is to analyse interactive conference key distribution based on Kolmogorov Complexity. For example, the amount of the user's information (in Kolmogorov Complexity) for a one-round key distribution scheme.

Acknowledgements: The research was supported by the NSF Project (No. 61274133) of China.

References:

[1] Alimomeni, M., Safavi-Naini, R.: Guessing secrecy. In: Proc. of the 6th International Conference on Information Theoretic Security (ICITS 2012), LNCS7412, Springer-Verlag, pp.1–13 (2012).

[2] Allender, E.: Some consequences of the existence of pseudorandom generators. J. Comput. System Sci.,Vol. 39, pp.101-124 (1989).

[3] Antunes, L., Laplante, S., Pinto, A., et al.,: Cryptographic security of individual instances. In Proc. 3th Int. Conf. on Information Theoretical Security (ICITS 2007), Madrid, Spain, May 25-29, LNCS 4883, Springer, Berlin Heidelberg, pp. 195-210 (2009).

[4] Antunes, L., Matos, A., Pinto, A., Souto, A., Teixeira, A.: One-Way Functions Using Algorithmic and Classical Information Theories. Theory Comput Syst. **52**(1), 162–178 (2013).

[5] Blom R.: An optimal class of symmetric key generation systems. In: EUROCRYPT, 1984. Lecture Notes in Computer Science, vol. 209, pp. 335–338 (1985).

[6] Blundo C., D'Arco P.: An Information Theoretic Model for Distributed Key Distribution, In: Proceedings of the 2000 IEEE International Symposium on Information Theory, p. 270, (2000).

[7] Blundo C., D'Arco P.: Analysis and Design of Distributed Key Distribution Centers, J. Cryptology **18** 391414 (2005).

[8] Blundo C., De Santis A., Herzberg A., Kutten S., Vaccaro U., Yung M.: Perfectly Secure Key Distribution for Dynamic Conferences, Inf. Comput. **146**(1) : 1–23(1998).

[9] Blundo C., De Santis A., Vaccaro, U.: Randomness in Distribution Protocols, Inf. Comput. **131**: 111–139(1996).

[10] Bose M., Dey A., Mukerjee R.: Key predistribution schemes for distributed sensor networks via block designs. Des. Codes Cryptogr. **67**, 111-136.(2013)

[11] Çamtepe S., Yener B .: Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans. Netw. **15**, 346-358 (2007).

[12] Dai, S., Guo, D.: Comparing security notions of secret sharing schemes. Entropy, **17**, 1135-1145 (2015).

[13] Dodis, Y.: Shannon Impossibility, Revisited, In: Proc. 6th Int.Conf. on Information Theoretical Security (ICITS 12), Montreal, QC, August 15-17, Springer, Berlin. 2012, pp.100–110.

[14] Dong J., Pei D., Wang X.: A key predistribution scheme based on 3-designs. In: INSCRYPT 2007. Lecture Notes in Computer Science, vol. 4990, pp. 81-92, Springer, Berlin (2008).

[15] Fiat A., Naor M.: broad cast encryption , Advances in Cryptology-CRYPTO 1993, D. Stinson(Ed.), LNCS 773, Springer-Verlag, pp. 480-491, 1994.

[16] Fuller, B., O'Neill, A., Reyzin, L.: A unified approach to deterministic encryption: New constructions and a connection to computational entropy. J. Cryptol. 2013, DOI: 10.1007/s00145-013-9174-5.

[17] Iwamoto, M., Shikata, J.: Information theoretic security for encryption based on conditional Rényi entropies, Information Theoretic Security. Springer International Publishing, 2014, pp.103–121

[18] Kaced, T.: Almost-perfect secret sharing, Information Theory Proceedings (ISIT), 2011, IEEE International Symposium on. IEEE, pp. 1603-1607 (2011).

[19] Lee J., Stinson D.R.: A combinatorial approach to key predistribution for distributed sensor networks. In: IEEE Wireless Communications and Networking Conference (WCNC 2005), vol. 2 , pp. 1200-1205.

[20] Lee J., Stinson D.R.: Common intersection designs. J. Comb. Des. **14**, 251269 (2006).

[21] Lee J., Stinson D.R.: On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. ACM Trans. Inf. Syst. Secur. **11**(2), article No. 1 (2008).

[22] Leung-Yan-Cheong, S.K., Cover, T.M.: Some equivalences between Shannon entropy and Kolmogorov complexity. IEEE Trans. Inf. Theory. **24**,331–339 (1978).

[23] Li M., Vitányi P.M.B.: An Introduction to Kolmogorov Complexity and Its Applications, third ed., Springer-Verlag, New York, (2008).

[24] Longpré, L., Mocas, S.: Symmetry of information and one-way functions. Inf. Process. Lett. **46**(2), 95–100 (1993).

[25] Longpré, L.,Watanabe, O.: On symmetry of information and polynomial time invertibility. Inf. Comput. **121**(1), 14–22 (1995).

[26] Matsumoto, T., Imai, H.: On the Key Predistribution System: A Practical Solution to the Key Distribution Problem, Advances in Cryptology-CRYPTO'87, LNCS 239, Springer-Verlag, pp. 185-193, 1987.

[27] Paterson M.B., Stinson D.R.: A unified approach to combinatorial key predistribution schemes for sensor networks. Des. Codes Cryptogr. **71**, 433-457.(2014)

[28] Pinto, A.: Comparing notions of computational entropy. Theory Comput Syst. **45**,944–962 (2009).

[29] Ruj S., Roy B.: Key predistribution using partially balanced designs in wireless sensor networks. In: Proceedings of ISPA 2007. Lecture Notes in Computer Science, vol. 4742, pp. 431-445 (2007).

[30] Ruj S., Roy B.: Revisiting key predistribution using transversal designs for a grid-based deployment scheme. Int. J. Distrib. Sens. Netw. **5**, 660-674 (2008).

[31] Ruj S., Roy B.: Key predistribution using combinatorial designs for a grid-group deployment scheme in wireless sensor networks. ACM Trans. Sens. Netw. **6**(1), article No. 4 (2009).

[32] Ruj S., Seberry J., Roy B.: Key predistribution schemes using block designs in wireless sensor networks. In: 2009 international conference on computational science and engineering, pp. 873-878 (2009).

[33] Safavi-Naini R., Jiang S.: Unconditionally Secure Conference Key Distribution: Security Notions, Bounds and Constructions. Int. J. Found. Comput. Sci. **22**(6), 1369-1393 (2011)

[34] Shannon, C.E.: Communication theory of secrecy systems. Bell Tech. J. **28**, 656–715 (1949).

[35] Stinson D.R.: Combinatorial Designs, Constructions and Analysis. Springer, New York (2004).

[36] Tadaki, K., Doi, N.: Cryptography and Algorithmic Randomness. Theory Comput Syst, **56**, 544-580(2015).

[37] Teixeira A., Matos A., Souto A., Antunes L.: Entropy measures vs. kolmogorov complexity. Entropy, **13** (3) 595-611(2011).