社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－AL－97　(2)
2004／10／14

鍵共有グラフのt-安全性について

浅野泰仁[†]　水木敬明[††]　西関隆夫[†]

† 東北大学大学院情報科学研究科　〒980-8579 宮城県仙台市青葉区荒巻字青葉 6-6-05
†† 東北大学情報シナジーセンター
〒980-8578 宮城県仙台市青葉区荒巻字青葉 6-3
E-mail: †asano@nishizeki.ecei.tohoku.ac.jp, ††mizuki@isc.tohoku.ac.jp, †††nishi@ecei.tohoku.ac.jp

あらまし　複数の人間 (参加者と呼ぶ) がいて，初期秘密鍵と呼ばれる秘密鍵を共有している参加者のペアが何組かあるものとする．さらに，これらの参加者とは別の盗聴者がいるものとする．鍵共有グラフと呼ばれる無向グラフ G は，このペアを表すものである．G の各点は参加者に対応し，各辺は初期秘密鍵を共有するペアに対応している．各参加者は，公衆通信網を用いてすべての参加者にメッセージを同報できる．このメッセージは，その参加者の知っている初期秘密鍵と，これまでに同報されたメッセージから作成される．すべてのメッセージは公衆通信網を用いて同報されるので，盗聴者とすべての参加者は同報されたすべてのメッセージを聞くことができる．盗聴者はさらにある整数 $t \geq 0$ 個の初期秘密鍵をあらかじめ盗んでいるものとする．この条件の下で，すべての参加者がひとつの共通秘密鍵を共有したいものとする．本論文では，すべての参加者がひとつの共通秘密鍵を安全に共有できるための必要十分条件は、鍵共有グラフ G が $(t+1)$ 個の辺素な全域木をもつことであるということを証明する．

キーワード　プロトコル，秘密鍵

On the t-Safety of a Key-sharing Graph

Yasuhito ASANO[†], Takaaki MIZUKI[††], and Takao NISHIZEKI[†]

† Graduate School of Information Sciences, Tohoku University, Aza-Aoba 6-6-05, Aramaki, Aoba-ku, Sendai, Miyagi Pref., Japan 980-8579.
†† Information Synergy Center, Tohoku University, Aza-Aoba 6-3, Aramaki, Aoba-ku, Sendai, Miyagi Pref., Japan 980-8578.
E-mail: †asano@nishizeki.ecei.tohoku.ac.jp, ††mizuki@isc.tohoku.ac.jp, †††nishi@ecei.tohoku.ac.jp

Abstract　Assume that there are several persons and some pairs of them share secret keys, called prior secret keys, and that there is an eavesdropper. An undirected graph G, called a key-sharing graph, represents the pairs; each vertex of G corresponds to a person, and each edge corresponds to a pair sharing a prior secret key. Each person can broadcast a message to all the persons through a public communication network; the person creates the message from his prior secret keys and all the messages that have already been broadcasted through the network. We thus assume that all the persons and the eavesdropper can hear all the messages broadcasted, and that the eavesdropper can tap at most t of the prior secret keys for an integer $t \geq 0$. Under such a situation all the persons wish to share a single common secret key. In this paper we prove that the persons can securely share a common secret key if and only if the key-sharing graph G has $(t+1)$ edge-disjoint spanning trees.

Key words　Protocol, secret key.

1. Introduction

Assume that there are several persons and some pairs of them share secret keys, called *prior secret keys*, and that there is an eavesdropper, named Eve, with unlimited computational power. We use an undirected graph G, called *a key-sharing graph*, to represent the pairs; each vertex of G corresponds to a person, and each edge corresponds to a pair sharing a prior secret key. We also assume that each person knows only prior secret keys of the pairs containing him, that

is, each person does not know any prior keys corresponding to the edges not adjacent to the vertex corresponding to the person. Each person can broadcast a message to all the persons through a public communication network; the person creates the message from the prior secret keys known to him and all the messages that have already been broadcasted through the network. We thus assume that all the persons and Eve can hear all the messages broadcasted. We also assume that Eve has tapped at most t-bit of the prior secret keys for an integer $t \geq 0$. Under such a situation all the persons wish to share a single *common secret key*. Once all the persons securely shared the common secret key, they can securely communicate information to each other by using it.

In this paper we prove that the persons can securely share a common secret key if and only if the key-sharing graph G has $(t+1)$ edge-disjoint spanning trees. We observe that the sufficient condition can be obtained by relatively simple analyses. That is, if G has $(t+1)$ edge-disjoint spanning trees, then we can actually construct a protocol such that all the persons securely share a common secret key by using it. However, it is relatively difficult to obtain the necessity condition. We first consider the simplest case where Eve has tapped no prior secret key, i.e. $t = 0$. In order to obtain the sufficient condition for this case, we analyze a communication between persons by using a new class of protocols, named *one-round one-bit multi-party protocol*, for communications under the situation described above. We then prove that if G has no edge-disjoint spanning tree, i.e. G is not connected, then all the persons can securely share no information, and consequently they cannot securely share a common secret key. Once a necessary and sufficient condition is obtained for a case where $t = 0$, we discuss a case where $t > 0$, i.e. Eve has tapped arbitrary t-bit of the prior secret keys. By extending the analyses for the case $t = 0$, we then prove that if all the persons can securely share a common secret key, then G has at least $t+1$ edge-disjoint trees.

The rest of this paper is organized as follows. In Section 2, we describe our problem and a motivation to consider this problem. We also give the definition of a key-sharing graph. In Section 3, we propose a one-round one-bit multi-party protocol and t-safety of a key sharing graph; a key-sharing graph is called t-safe if there is a protocol, classified as the one-round one-bit multi-party protocol, such that all the persons can securely share a common secret key. In Section 4, we consider the simplest situation in which Eve has tapped no prior secret key. Then, we prove the necessary and sufficient condition for 0-safety of a given key-sharing graph. In Section 5, we prove the necessary and sufficient condition for t-safety by extending the result obtained in Section 3 to general situations. In Section 6, we present our concluding remarks.

2. Preliminaries and Motivations

Secure communications in several kinds of situations have been widely studied in recent years. We assume that the eavesdropper Eve has unlimited computational power, as described above. When there are several persons wishing secure communications under the assumption, one of important problems is how all the persons securely share a single common secret key. Once all the persons securely shared a common secret key, they can securely communicate information to each other by using it. This problem is called a *multiparty secret key exchange* problem, and it has been studied in several situations [1], [2]. Throughout this paper, we consider how all the persons securely share a one-bit common secret key; if they can securely share a one-bit common secret key by doing some communications, then it is easy to see that they can securely share x-bit common secret key for arbitrary integer x by iterating communications similar to those used for sharing the one-bit common secret key.

For the multiparty secret key exchange problem, we consider a new communication model, named *a public broadcast key-sharing model*, in which the following conditions (1)-(4) hold.

(1) Some pairs of persons share secret keys, called *prior secret keys*, in advance; each person knows only his prior secret keys, i.e. the prior secret keys of the pairs containing him; each person knows which pair of persons shares a prior secret key.

(2) Each person can broadcast a message to all the persons through a public communication network; the message is created from his prior secret keys and all the messages already broadcasted.

(3) All the persons and the eavesdropper can hear all the messages broadcasted.

(4) The eavesdropper Eve has tapped at most t of the prior secret keys, for an integer $t \geq 0$, in advance.

The pairs described in condition (1) can be represented by a *key-sharing graph*, defined as follows.

[Definition 1] Assume that there are $n \geq 3$ persons indexed $1, 2, ..., n$, and that a pair of persons (i, j), $1 \leq i, j \leq n$, shares a $b_{i,j}$-bit prior key. If a pair of persons (i, j) shares no prior key, let $b_{i,j} = 0$ for convenience. Let $key(i, j, k)$, for $1 \leq k \leq b_{i,j}$, be k-th bit of the prior key of a pair (i, j), and let $|key(i, j, k)|$ be the value of it. We call $key(i, j, k)$ for $1 \leq i, j \leq n$ and $1 \leq k \leq b_{i,j}$ *a one-bit prior key*. The

key-sharing graph $G = (V, E)$ is an undirected multigraph; the vertex set V of G is $\{1, 2, ..., n\}$ and each vertex i corresponds to a person i; each edge corresponds to a one-bit prior key. For each pair of vertices (i, j) with $b_{i,j} > 0$, the edge set E of G contains $b_{i,j}$ edges corresponding to $key(i, j, 1)$, $key(i, j, 2), ..., key(i, j, b_{i,j})$. If $b_{i,j} = 0$ for a pair (i, j), then there is no edge between a vertex i and a vertex j.

From the condition (1), each person i, $1 \leqq i \leqq n$, knows the shape of a key-sharing graph G, but does not know the value of any prior secret keys corresponding to edges not adjacent to a vertex i.

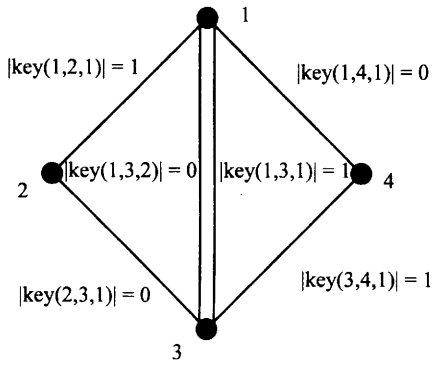

図 1 鍵共有グラフ
Fig. 1 A key-sharing graph.

Fig. 1 depicts a key-sharing graph corresponding to four persons $\{1, 2, 3, 4\}$ and five pairs. Each pair of $(1, 2)$, $(1, 4)$, $(2, 3)$, and $(3, 4)$ shares a one-bit prior secret key with a one-bit variable, while a pair $(1, 3)$ shares a prior secret key with a two-bit variable. For example, the value of the variable of the prior secret key of a pair $(1, 2)$ is equal to $|key(1, 2, 1)| = 1$. The value of the variable of the prior secret key of a pair $(1, 3)$ is equal to 01; the first bit, i.e. the rightmost bit, corresponds to $|key(1, 3, 1)| = 1$, and the second bit corresponds to $|key(1, 3, 2)| = 0$.

In the next section, we will define a new class of protocols, named a *one-round one-bit multi-party protocol*, for communications based on the public broadcast key-sharing model, where the conditions above (1)-(4) hold. The one-round one-bit multi-party protocol is an application of the multi-party protocol, proposed by Fischer and Wright [1], to communications based on the public broadcast key-sharing model. We will also define *t-safety* of a key-sharing graph; a key-sharing graph is called t-safe if there is a protocol, classified as the one-round one-bit multi-party protocol, such that all the persons can securely share a common secret key by doing some communications obedient to the protocol. The main result of this paper to prove that a key-sharing graph G is t-safe if and only if G has at least $(t + 1)$ edge-disjoint spanning trees.

Several researchers have implicitly used the key-sharing graph to represent pairs of persons on a private communication network model [1] [2], [3], and [4]. On the private communication network model, a person in a pair can securely communicate messages to the other person in the pair, that is, other persons and the eavesdropper cannot tap the messages. On the other hand, few works have used a key-sharing graph for communications using broadcasts through a public communication network. A reference [6] is one of such works, although it deals with a much limited communication model compared with the public broadcast key-sharing model used in this paper. In general, communications using broadcasts through a public communication network can be realized much easily than communications on a private communication network model, and hence our result is useful in practice.

3. One-Round One-Bit Multi-Party Protocol and t-Safety of a Key-Sharing Graph

In this section, we propose a new class of protocols, named a *one-round one-bit multi-party protocol*, for communications based on the public broadcast key-sharing model. The definition of the one-round one-bit multi-party protocol is as follows.

[Definition 2] *A one-round one-bit multi-party protocol* is a class of protocols for communications based on the public broadcast key-sharing model. A protocol, classified as the one-round one-bit multi-party protocol, determines H rounds of communications for an integer $H \geqq 0$. At h-th round, $1 \leqq h \leqq H$, each person i sets a one-bit variable, denoted by $I_{i,h}$, as follows. The value of the variable $I_{i,h}$ is denoted by $|I_{i,h}| \in \{0, 1\}$.

- *Sender.* A person, denoted by $s(h)$, becomes a "sender" of information at h-th round. That is, $s(h)$ determines the value of $I_{s(h),h}$ by using $I_{s(h),1}, I_{s(h),2}, ..., I_{s(h),h-1}, R_h, K_h$, where R_h is a random bit with a value 0 or 1 and K_h is a set of his one-bit prior keys $\{key(s(h), q, b) \mid (s(h), q, b) \in E\}$. Then, $s(h)$ determines the value of a one-bit message M_h using the one-bit variable $I_{s(h),h}$ and a one-bit prior key k_h, where $k_h \in K_h$. The value of M_h and k_h are denoted by $|M_h|$ and $|k_h|$, respectively. Then, $s(h)$ broadcasts the message M_h to all the persons through a public communication network.
- *Receiver.* A person, denoted by $r(h)$, becomes a "receiver" of information at h-th round. That is, $r(h)$ deter-

mines the value of $I_{r(h),h}$ by using the broadcasted message M_h and his one-bit prior key.

- *Others.* Each person i, except $s(h)$ and $r(h)$, set $I_{x,h}$ as $|I_{i,h}| = |M_h|$.

After H rounds communications are finished, each person i determines the value of a one-bit variable f_i by using his variables $I_{i,1}, ..., I_{i,H}$, and his one-bit prior keys $\{key(i,j,b) \mid (i,j,b) \in E\}$. The one-bit variable f_i is called a *final key.*

Prior to the communications the protocol determines methods how the players determine the values of the messages, the variables, and the final keys, and hence the methods are known to all the persons and Eve. Consequently, if Eve possesses the same information as that possessed by any person, then Eve can compute correctly the value of the final key determined by the person.

If all the final keys have the same value and Eve cannot guess correctly the value with probability more than 1/2, then the persons will be able to use the value as the value of a one-bit common secret key for secure communication. We thus define t-safety of a key-sharing graph as follows.

[Definition 3] A given key-sharing graph G is called t-safe, if there is a protocol, classified as the one-round one-bit multi-party protocol, satisfying the following conditions for any assignment $E \to \{0,1\}$ of values to the one-bit prior keys.

(1) Every person generates a final key with the same value, after the communications determined by the protocol and the assignment of the values to the one-bit prior keys.

(2) Eve does not possess information about the final keys; we say "Eve does not possess" information about a one-bit variable if Eve can guess correctly the value of the variable with probability 1/2.

A protocol, classified as the one-round one-bit multi-party protocol, can be determined by using information about the shape of the key-sharing graph G prior to the communications, but it is determined independent of particular assignment of values to the one-bit prior keys. Hence, a protocol used for the t-safety has to satisfy the conditions above for any assignment of values to the one-bit prior keys.

4. Necessary and Sufficient Condition for 0-Safety

In this section, we first analyze each round of communications based on the one-round one-bit multi-party protocol. Note that it is difficult to analyze each round of communications based on the original multi-party protocol. We then consider the simplest situation in which Eve has tapped no prior secret keys.

Let us consider how a person securely provides a piece of possessed information to another person by a communication at h-th round, for $1 \leqq h \leqq H$.

[Lemma 1] At h-th round, the sender $s(h)$ can provide information $I_{s(h),h}$ to the receiver $r(h)$ such that Eve cannot possess information about $I_{s(h),h}$ if and only if the following conditions are satisfied.

(1) $|M_h| = |I_{s(h),h}| \oplus |k_h|$ or $|M_h| = \neg(|I_{s(h),h}| \oplus |k_h|)$, where $k_h \in \{key(s(h), r(h), c) \mid (s(h), r(h), c) \in E\}$.

(2) Eve has not tapped k_h.

Proof. If the both conditions are satisfied, then the receiver can compute correctly the value of $I_{s(h),h}$ and Eve cannot guess correctly it with probability more than 1/2, and hence these conditions are sufficient. We thus prove the necessity below.

If the value of the message $|M_h|$ is determined by a randomized method or depends on a random variable, that is, if M_h may have two different values for fixed $|I_{s(h),h}|$ and $|k_h|$, no person can compute correctly $|M_h|$ from $I_{s(h),h}$ and k_h. We thus have to use a deterministic method to determine $|M_h|$ from $I_{s(h),h}$ and k_h. We then claim that if $|M_h|$ is equal to neither $|I_{s(h),h}| \oplus |k_h|$ nor $\neg(|I_{s(h),h}| \oplus |k_h|)$ for some $k_h \in \{key(s(h), r(h), c) \mid (s(h), r(h), c) \in E\}$, then either no person can compute correctly $|M_h|$ or Eve can guess correctly the value with probability more than 1/2.

Let N_0 (N_1) be the number of possible combinations of $|I_{s(h),h}|$ and $|k_h|$ such that $|M_h| = 0$ (or 1, respectively). If $N_0 > N_1$ or $N_0 < N_1$, then no person can compute correctly the value of $I_{s(h),h}$ from M_h and any k_h. Therefore, the number of possible patterns of $|M_h|$, for all the combinations of $|I_{s(h),h}|$ and $|k_h|$, is $C_{4,2} = 6$. Table 1 describes all the six patterns. The patterns are named

表 1 $|M_h|$ の取りうる 6 つのパターン
Table 1 The six possible patterns of $|M_h|$

$I_{s(h),h}$	k_h	A	B	C	D	E	F
0	0	0	0	1	0	1	1
0	1	0	1	0	1	0	1
1	0	1	0	0	1	1	0
1	1	1	1	1	0	0	0

A, B, C, D, E, and F. Pattern A (or F) corresponds to $|M_h| = |I_{s(h),h}|$ (or $|M_h| = \neg|I_{s(h),h}|$, respectively), and hence Eve can compute correctly $|I_{s(h),h}|$ from M_h. Pattern B (or E) corresponds $|M_h| = |k_h|$ (or $|M_h| = \neg|k_h|$, respectively), and hence Eve can compute correctly $|k_h|$ from M_h. Note that in this case no person can compute correctly

$|I_{s(h),h}|$ since M_h is independent of $I_{s(h),h}$. The remaining patterns are D and C, corresponding to $|M_h| = |I_{s(h),h}| \oplus |k_h|$ or $|M_h| = \neg(|I_{s(h),h}| \oplus |k_h|)$. This implies the necessity of the first condition.

If the communication at h-th round satisfies the first condition and Eve have tapped k_h, then Eve can compute correctly $I_{s(h),h}$ from M_h. Hence, the second condition is also necessary. □

We say a communication at a round is a *one-round communication* if it satisfies the condition (1), and call a one-round communication satisfying the condition (2) a *one-round secure communication.*

We now consider how securely generate a common secret key by iterating one-round communications. To begin with, we assume the simplest situation where Eve has tapped no one-bit prior key in G in advance. Under this situation, any one-round communication becomes a one-round secure communication. Recall that a person cannot provide securely information without using a one-round communication, even in this situation. In the rest of this section, we prove the following theorem hold in this situation.

[Theorem 1] A given key-sharing graph G is 0-safe if and only if G is connected.

Proof. To prove the sufficiency, we actually describe a protocol, classified as the one-round one-bit multi-party protocol, for communications to share a one-bit common secret key. Since G is connected, G has a spanning tree T. Without loss of generality, we can assume that edges of T is indexed in BFS order of T, $e_1, e_2, ..., e_{n-1}$, and that $e_1 = (1, 2, 1)$. In the following one-round one-bit multi-party protocol, the persons provide information by using the one-bit prior key corresponding to e_h at h-th round.

A Protocol for Communications to Share a One-Bit Common Secret Key

(1) The communication at the first round consists of the following four procedures (a)-(d).

(a) Person 1 sets a one-bit variable $I_{1,1}$ at random; $|I_{1,1}| = 0$ with probability 1/2, and $|I_{1,1}| = 1$ with probability 1/2.

(b) Person 1 broadcasts a message M_1, where $|M_1| = |I_{1,1}| \oplus |key(1, 2, 1)|$. Person 1 is called the sender at the first round.

(c) Person 2 receives and decodes the message, and set a one-bit variable $I_{2,1}$ as $|I_{2,1}| = |I_{1,1}| = |M_1| \oplus |key(1, 2, 1)|$. Person 2 is called the receiver at the first round.

(d) Each person x, $3 \leqq x \leqq n$, receives the message and sets $|I_{x,1}| = |M_1|$.

(2) Let $e_h = (u, v, 1)$. Let the sender at h-th round $s(h) = u$, and the receiver at this round $r(h) = v$. The communication at h-th round, $2 \leqq h \leqq n-1$, consists of the following four procedures (a)-(d).

(a) If $s(h) \neq 1$, person $s(h)$ sets $|I_{s(h),h}| = |I_{s(h),s(h)-1}|$. Otherwise, person $s(h)$ sets $|I_{s(h),h}| = |I_{1,1}|$.

(b) Person $s(h)$ broadcasts a message M_h, where $|M_h| = |I_{s(h),h}| \oplus |key(s(h), r(h), 1)|$.

(c) Person $r(h)$ receives and decodes the message, and sets a one-bit variable $I_{r(h),h}$ such that $|I_{r(h),h}| = |I_{s(h),h}| = |M_h| \oplus |key(s(h), r(h), 1)$.

(d) Every person x, except $s(h)$ and $r(h)$, receives the message and sets $|I_{x,h}| = |M_h|$.

After these communications, all the players do the following procedures.

(1) Person i determines the value of a final key f_1 such that $|f_1| = |I_{1,1}|$.

(2) For $1 \leqq h \leqq n-1$, person $r(h)$, the receiver at h-th round, determines the value of a final key $f_{r(h)}$ such that $|f_{r(h)}| = |I_{r(h),h}|$.

We prove that the persons securely generate the final keys such that $|f_1| = |f_2| = \cdots = |f_n|$. Without loss of generality, we can assume that $r(h) = h + 1$ for $2 \leqq h \leqq n-1$, i.e. $r(2) = 3$, $r(3) = 4$, ..., $r(n-1) = n$. The communication at h-th round, $1 \leqq h \leqq n-1$, is a one-round secure communication, and hence Eve cannot possess information about f_{h+1} with the value $|f_{h+1}| = |I_{h+1,h}| = |I_{s(h),h}|$. It is easy to see $|I_{1,1}| = |I_{2,1}| = \cdots = |I_{s(h),h+1}| = |I_{h+1,h}|$. This completes the proof for the sufficiency.

To prove the necessity, we introduce two lemmas.

[Lemma 2] Let us consider a point of time when h-th round just finished. Then, let KNOW$(h, I_{h'})$ be a set of persons who know the value of $I_{h'}$, where $I_{h'} = I_{s(h'),h'}$ for an integer $h' \leqq h$; we say "a person i knows the value of $I_{h'}$," when he can compute correctly the value from his information $I_{i,h}, I_{i,h-1}, ..., I_{i,1}$ and his prior secret keys $\{key(i, j, c) \mid (i, j, c) \in E\}$. We define KNOW$(0, I_{h'}) = \emptyset$ for any $1 \leqq h' \leqq H$, for convenience. Assume that Eve does not possess information about $I_{h'}$ at this point of time. Thus, KNOW$(h, I_{h'}) \subset$ KNOW$(h+1, I_{h'})$ implies a fact that another person knows the value of $I_{h'}$ when $(h+1)$-th round just finished.

We claim that KNOW$(h, I_{h'}) \subset$ KNOW$(h+1, I_{h'})$ holds and Eve does not possess information about $I_{h'}$ when $(h+1)$-th round just finished if and only if the protocol, classified as the one-round one-bit multi-party protocol, used for the communication at $(h+1)$-th round satisfies the following conditions (1)-(3).

(1) The sender at $(h+1)$-th round, denoted by $s(h+1)$,

is contained in KNOW$(h, I_{h'})$.

(2) The receiver at $(h+1)$-th round, denoted by $r(h+1)$, is contained in $V \setminus$ KNOW$(h, I_{h'})$.

(3) The communication at $(h+1)$-th round is a one-round secure communication. Thus the key, k_{h+1}, used in this communication is contained in $\{key(s(h+1), r(h+1), c) \mid key(s(h+1), r(h+1), c) \in E\}$. The sender creates a message M_{h+1} from k_{h+1} and $I_{s(h+1),h+1}$, where $|I_{s(h+1),h+1}| = |I_{h'}|$. The receiver $r(h+1)$ then computes correctly $|I_{s(h+1),h+1}|$ from M_{h+1} and k_{h+1}, and sets $|I_{r(h+1),h+1}| = |I_{s(h+1),h+1}| = |I_{h'}|$.

Proof. If all the conditions (1)-(3) hold, then $r(h+1) \notin$ KNOW$(h, I_{h'})$ knows the value of $I_{h'}$ after the communication, and hence these conditions are sufficient.

We prove the necessity below. From Lemma 1, the condition (3) is necessary. If the sender $s(h+1) \notin$ KNOW$(h, I_{h'})$, then this person cannot compute correctly the value of $I_{h'}$. Therefore, no person in $V \setminus$ KNOW$(h, I_{h'})$ compute correctly this value from M_{h+1}, the message created by $s(h+1)$. This implies the necessity of the condition (1). If the receiver $r(h+1) \in$ KNOW$(h, I_{h'})$, then no person in $V \setminus$ KNOW$(h, I_{h'})$ knows the value of the one-bit prior key k_{h+1} used in this round. Consequently, no person can compute correctly the value of $I_{s(h+1),h+1}$ from M_{h+1}, the message created from $I_{s(h+1),h+1}$ and k_{h+1} as described in Lemma 1. Thus, even if $|I_{s(h+1),h+1}| = |I_{h'}|$, no person contained in $V \setminus$ KNOW$(h, I_{h'})$ knows the value of $I_{h'}$ immediately after $(h+1)$-th round, and hence KNOW$(h, I_{h'}) =$ KNOW$(h+1, I_{h'})$. This implies that the condition (2) is also necessary. □

[Corollary 1] If KNOW$(h, I_{h'}) = V$, where $I_{h'} = I_{s(h'),h'}$ for two integers h and h' such that $1 \leqq h' \leqq h \leqq H$, and Eve does not possess information about $I_{h'}$ when h-th round just finished, then the key-sharing graph G has a spanning tree, i.e. G is connected.

Proof. From Lemma 2, if KNOW$(h, I_{h'}) = V$ and Eve does not possess information about $I_{h'}$ when h-th round just finished, then the players has done at least $n-1$ times one-round secure communications when h-th round just finished, and consequently the edge set, corresponding to the set of one-bit prior keys used in the communications, forms a spanning tree of G. □

[Lemma 3] After H rounds communications based on a one-round one-bit multi-party protocol, if every person i for $1 \leqq i \leqq n$ can generate the final key f_i such that $|f_1| = |f_2| = \cdots = |f_n|$ and Eve cannot guess correctly the value of f_i with probability more than $1/2$, then $\exists I_{h'} = I_{s(h'),h'}$, $1 \leqq h' \leqq H$, such that KNOW$(H, I_{h'}) = V$ and Eve does not possess information about $I_{h'}$ when H-th round finished.

Proof. Let F_i be the set of one-bit variables used to determine the value of the final key f_i of a person i. Thus, f_i depends on every one-bit variable contained in F_i. If there is no one-bit variable $z_i \in F_i$ for each $1 \leqq i \leqq n$ such that either $|z_i| = |z_1|$ or $|z_i| = \neg|z_1|$ holds for arbitrary assignment of values to the one-bit prior keys, where $|z_i|$ denotes the value of z_i, then the persons cannot generate the final keys with the same value from $F_1, F_2, ..., F_n$. Thus, without loss of generality, we can assume that there is a one-bit variable $z_i \in F_i$ for each $1 \leqq i \leqq n$ such that $|z_1| = |z_2| = \cdots = |z_n|$. From the definition of the one-bit one-round multi-party protocol, F_i is a subset of $\{I_{i,1}, I_{i,2}, ..., I_{i,H}\} \cup \{key(i,j,b) \mid (i,j,b) \in E\}\}$. However, z_i cannot be contained in $\{key(i,j,b) \mid (i,j,b) \in E\}$, because the values of the one-bit prior keys depend on the used assignment of values to the one-bit prior keys; since the number of persons $n \geqq 3$, all the persons share no set of one-bit prior keys. Hence, $z_i \in \{I_{i,1}, ..., I_{i,H}\}$ for each $1 \leqq i \leqq n$, and thus there is a one-bit variable $I_{h'} = z_i$, $1 \leqq h' \leqq H$, such that KNOW$(H, I_{h'}) = V$. This also implies that if Eve possess information about $I_{h'}$, then Eve can guess correctly the value of the final keys. □

Now Corollary 1 and Lemma 3 complete the proof for the necessity in Theorem 1. □

5. Necessary and Sufficient Condition for t-Safety

In this section, we give the necessary and sufficient condition for t-safety of a key-sharing graph. Assume that for an integer $t > 0$ Eve has tapped t one-bit prior keys in the key-sharing graph G in advance. Recall Lemma 1, i.e. a person cannot provide a part of his information safely without the one-round secure communication.

[Corollary 2] Let $A_1, A_2, ..., A_Y$ be one-bit variables satisfying the following conditions.

(1) A_i is contained in $\{I_{s(h),h} \mid 1 \leqq h \leqq H\}$ for $1 \leqq y \leqq Y$.

(2) $A_1, A_2, ..., A_Y$ are independent of each other. That is, $|A_i| = |A_j|$ for any $1 \leqq i \neq j \leqq Y$ with probability $1/2$ for any assignment of values to the one-bit prior keys.

(3) KNOW(H, A_1) = KNOW(H, A_2) = $\cdots$ = KNOW$(H, A_Y) = V$.

After H rounds communications, if each person i, $1 \leqq i \leqq n$, can generate the final key f_i such that $|f_1| = |f_2| = \cdots = |f_n|$

and Eve cannot guess correctly the value of f_i with probability more than 1/2, then Eve does not possess information about at least one A_y for $1 \leqq y \leqq Y$.

Proof. From Lemma 3, there is at least one-bit variable A_y, $1 \leqq y \leqq Y$, such that $\mathrm{KNOW}(H, A_y) = V$ and Eve does not possess information about A_y for generating the final keys with the same value. □

[Lemma 4] Assume that there is a one-bit variable $I_{h'}$ such that $\mathrm{KNOW}(h, I_{h'}) = V$ for two integers $h \geqq h' \geqq 1$. Let T'_h be a subgraph of G consists of the edges corresponding to the set D of the one-bit prior keys used by $(n-1)$ persons to provide information about $I_{h'}$ to another person in one-round communications. That is,

$$D = \{k_d \mid 1 \leqq d \leqq H,\ \mathrm{KNOW}(d-1, I_{h'}) \subset \mathrm{KNOW}(d, I_{h'})\},$$

the set of the one-bit prior keys used at d-th round where $\mathrm{KNOW}(d, I_{h'})$ contains a person not contained in $\mathrm{KNOW}(d, I_{h'})\}$.

If Eve has tapped a one-bit prior key k_a corresponding to some edge in T'_h, then Eve can guess correctly the value of $I_{h'}$ and the values of all the one-bit prior keys corresponding to the edges of T'_h.

Proof. Assume that Eve has tapped a one-bit prior key k_a corresponding to some edge in T'_h. The communication at a-th round is a one-round communication, because $\mathrm{KNOW}(a-1, I_{h'}) \subset \mathrm{KNOW}(a, I_{h'})$. See Lemma 2. Hence, $|I_{s(a),a}| = |I_{h'}|$, and either $|M_a| = |I_{s(a),a}| \oplus |k_a|$ or $|M_h| = \neg(|I_{s(a),a}| \oplus |k_a|)$. Consequently, Eve can compute correctly the value of $I_{s(a),a} = I_{h'}$, from M_h and k_a; this one-round communication is not a one-round secure communication.

The communication at d-th round, where $\mathrm{KNOW}(d-1, I_{h'}) \subset \mathrm{KNOW}(d, I_{h'})$, is a one-round communication to provide information about $I_{s(d),d}$, where $|I_{s(d),d}| = |I_{h'}|$, and hence from M_d and $I_{h'}$ Eve can compute correctly the value of any one-bit prior key $k_d \in D$ corresponding to an edge in T'_h. □

[Corollary 3] Let $A_1, A_2, ..., A_Y$ be one-bit variables satisfying the following conditions.

(1) A_i is contained in $\{I_{s(h),h} \mid 1 \leqq h \leqq H\}$ for $1 \leqq y \leqq Y$.

(2) $A_1, A_2, ..., A_Y$ are independent of each other. That is, $|A_i| = |A_j|$ for any $1 \leqq i \neq j \leqq Y$ with probability 1/2 for any assignment of values to the one-bit prior keys.

(3) $\mathrm{KNOW}(H, A_1) = \mathrm{KNOW}(H, A_2) = \cdots = \mathrm{KNOW}(H, A_Y) = V$.

Let $T_1, T_2, ..., T_Y$ be subgraphs of G, such that the edges of T_y $(1 \leqq y \leqq Y)$ are corresponding to a set D_y of the one-bit prior keys, where

$$D_y = \{k_d \mid 1 \leqq d \leqq H,\ \mathrm{KNOW}(d-1, A_y) \subset \mathrm{KNOW}(d, A_y)\}.$$

If there are two subgraphs T_a and T_b for $1 \leqq a \neq b \leqq Y$ such that T_a and T_b are not edge-disjoint, and Eve has tapped the one-bit prior key corresponding to an edge $e \in T_a \cup T_b$, then Eve can compute correctly the values of A_a and A_b and the value of the one-bit prior key corresponding to any edge $e' \in T_a \cup T_b$.

Proof. From Lemma 4, Eve can compute correctly the value of A_a because Eve has tapped the one-bit prior key corresponding to $e \in T_a$ and can also compute correctly the value of the one-bit prior key corresponding to any edge $e' \in T_a$. In the same way, Eve can compute correctly the value of A_b and the value of the one-bit prior key corresponding to any edge $e' \in T_b$. □

[Theorem 2] A given key-sharing graph G is t-safe if and only if G has $(t+1)$ edge-disjoint spanning trees.

Proof. First, we prove the sufficiency.

Let $T_1, T_2, ..., T_{t+1}$ be $(t+1)$ edge-disjoint spanning trees of G. All the persons can share $(t+1)$ one-bit independent variables $A_1, A_2, ..., A_{t+1}$ by iterating the communications obedient to "the protocol for communications to share a one-bit common secret key" described in Section 4.. Assume that for $1 \leqq j \leqq t+1$ all the persons use the one-bit prior keys corresponding to all the edges of T_j to share each A_j. In the communications for sharing A_j, the first sender determines the value of a one-bit variable at random and regard the variable as A_j. Eve has tapped at most t one-bit prior keys, and hence there is at least one edge-disjoint spanning tree T_j, $1 \leqq j \leqq t+1$, such that Eve has not tapped the one-bit prior key corresponding to any edge in T_j. $T_1, ..., T_{t+1}$ are edge-disjoint each other, and the communications obedient to "the protocol for communications to share a one-bit common secret key" use only the one-bit prior keys corresponding to the edges in T_j for sharing each A_j, and hence each set of the one-bit prior keys used in the communications for sharing each of A_j is disjoint each other. Consequently, Eve can possess information at most t one-bit variables in $A_1, A_2, ..., A_{t+1}$, after the communications. Although the persons cannot know whether or not Eve possesses information about a particular one-bit variable or one-bit prior key, the persons can generate the final key with the same value by setting $|f_1| = |f_2| = \cdots = |f_n| = |A_1| \oplus |A_2| \oplus \cdots \oplus |A_{t+1}|$. Eve does not possess information about at least one variables in $A_1, A_2, ..., A_{t+1}$, and hence it is easy to observe that Eve can guess correctly the value of the final keys with probability at most 1/2.

Next, we prove the necessity.

Let $A_1, A_2, ..., A_Y$ be one-bit variables satisfying the following conditions.

(1) A_i is contained in $\{I_{s(h),h} \mid 1 \leqq h \leqq H\}$ for $1 \leqq y \leqq Y$.

(2) $A_1, A_2, ..., A_Y$ are independent of each other. That is, $|A_i| = |A_j|$ for any $1 \leqq i \neq j \leqq Y$ with probability 1/2 for any assignment of values to the one-bit prior keys.

(3) $\mathrm{KNOW}(H, A_1) = \mathrm{KNOW}(H, A_2) = \cdots = \mathrm{KNOW}(H, A_Y) = V$.

Let $T_1, T_2, ..., T_Y$ be subgraphs of G, such that the edges of T_y $(1 \leqq y \leqq Y)$ are corresponding to a set D_y of the one-bit prior keys, where

$$D_y = \{k_d \mid 1 \leqq d \leqq H,\ \mathrm{KNOW}(d-1, A_y) \subset \mathrm{KNOW}(d, A_y)\}.$$

From Lemma 1, each T_y for $1 \leqq y \leqq Y$ contains a spanning tree of G, denoted by T'_y. From Corollary 2, Eve should not possess information about at least one one-bit variable A_y in $A_1, A_2, ..., A_Y$. If $Y \leqq t$, then we can assume that Eve has tapped at least one one-bit prior secret key in T'_j for each $1 \leqq j \leqq Y$, and hence Eve can compute correctly the values of $A_1, A_2, ..., A_Y$, and consequently Eve can compute correctly the value of the final keys. Hence, we can assume that G has at most t edge-disjoint spanning trees. Without loss of generality, we can also assume that for an integer $t' \leqq t$ $T'_1, T'_2, ..., T'_{t'}$ are edge-disjoint spanning trees and each of $T'_{t'+1}, T'_{t'+2}, ..., T'_y$ shares at least one edge with one of $T'_1, T'_2, ..., T'_{t'}$. Since $t' \leqq t$, we can assume that Eve has tapped at least one prior secret key in each of $T'_1, T'_2, ..., T'_{t'}$, and consequently Eve can compute correctly $A_1, A_2, ..., A_Y$. See Corollary 3. This implies that G must have at least $(t+1)$ edge-disjoint spanning trees. □

6. Concluding Remarks

We have assumed that there are persons wishing secure communications, and there is an eavesdropper. We have considered how the persons securely share a common secret key under the following situation. Some pairs of persons share prior secret keys in advance; each person can broadcast a message to all the persons through a public communication network; the message is created from his prior secret keys and all the messages already broadcasted; all the persons and the eavesdropper can hear all the messages broadcasted; the eavesdropper Eve has tapped at most t of the prior secret keys, for an integer $t \geqq 0$, in advance. We have used a key-sharing graph G to represent the pairs sharing prior secret keys; each vertex of G corresponds to a person, and each edge corresponds to a pair sharing a prior secret key.

In this paper we have proved that the persons can securely share a common secret key under the situation above if and only if the key-sharing graph G has $(t+1)$ edge-disjoint spanning trees. We have first considered the simplest case where Eve has tapped no prior secret key, i.e. $t = 0$, and have analyzed a communication between persons by using a new class of protocols, named *one-round one-bit multi-party protocol*, for communications under the situation above. Once a necessary and sufficient condition has been obtained for a case where $t = 0$, by extending the lemmas and the corollaries proved for the case $t = 0$ to a case $t > 0$ we have given a necessary and sufficient condition where Eve has tapped arbitrary t-bit of the prior secret keys; the persons can securely share a common secret key if and only if the key-sharing graph G has $(t + 1)$ edge-disjoint spanning trees.

It is known that an undirected graph has $(t + 1)$ edge-disjoint spanning trees if and only if for every partition of V into r sets, at least $(t + 1)(r - 1)$ edges of G have endpoints in different sets of the partition [5].

One of the future works is to compare the one-round one-bit multi-party protocol with the multi-party protocol. For this purpose, we are considering an extension of the one-round one-bit multi-party protocol; it allows a person to use multiple bits of prior secret keys for a communication at one round, while in the one-round one-bit multi-party protocol a person can use only one bit of a prior secret key at one round. It is easy to prove that the extended protocol is equivalent to the multi-party protocol, and hence the remaining problem is to compare the extended protocol with the one-round one-bit multi-party protocol.

Another interesting future work is to consider a situation in which more than two persons share the same prior secret key, while this paper deals with a situation in which just two persons share the same prior secret key. The former situation can be formalized by using a hypergraph (V, E) whose vertices correspond to persons and whose hyperedge $e \subseteqq V$ represents which persons share the same prior secret key.

文　献

[1] M. J. Fischer and R. N. Wright, "Multiparty secret key exchange using a random deal of cards," *Proc. CRYPTO 91*, LNCS 576, pp. 141–153, 1991.

[2] M. J. Fischer and R. N. Wright, "Bounds on secret key exchange using a random deal of cards," *Journal of Cryptology* 9, pp. 71–99, 1996.

[3] M. Franklin and M. Yung, "Secure hypergraphs: privacy from partial broadcast," *Proc. 27th STOC*, pp. 36–44, 1995.

[4] Y. Wang and Y. Desmedt, "Secure communications in multicast channels: the answer to Flanklin and Wright's question," *Journal of Cryptology* 14, pp. 121–135, 2001.

[5] D. B. West, "Introduction to Graph Theory, 2nd edition," Prentice Hall, 2001.

[6] S. Zhu, S. Xu, S. Setia and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach," *Proc. ICNP03*, pp. 326–335, 2003.