氏名（本籍）	みずき　たかあき 水木　敬明　　（北海道）
学位の種類	博　士　（情報科学）
学位記番号	情博第151号
学位授与年月日	平成12年3月23日
学位授与の要件	学位規則第4条第1項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）システム情報科学専攻
学位論文題目	Sharing Unconditionally Secure Secret Keys （無条件に安全な秘密鍵共有法）
論文審査委員	（主査） 東北大学教授　西関　隆夫　　東北大学教授　丸岡　章 東北大学教授　根元　義章　　東北大学教授　静谷　啓樹

論文内容要旨

1 Introduction

Suppose that there are k (≥ 2) players $P_1, P_2, \cdots, P_k$ and a passive eavesdropper, Eve, whose computational power is unlimited. All players wish to share a common one-bit secret key that is unconditionally secure from Eve. Let C be a set of d distinct cards which are numbered from 1 to d. All cards in C are randomly dealt to players $P_1, P_2, \cdots, P_k$ and Eve. We call a set of cards dealt to a player or Eve a *hand*. Let $C_i \subseteq C$ be P_i's hand for each $1 \leq i \leq k$, and let $C_e \subseteq C$ be Eve's hand. We denote this *deal* by $\mathcal{C} = (C_1, C_2, \cdots, C_k; C_e)$. Clearly $\{C_1, C_2, \cdots, C_k, C_e\}$ is a partition of set C. We write $c_i = |C_i|$ for each $1 \leq i \leq k$ and $c_e = |C_e|$, where $|A|$ denotes the cardinality of a set A. We call $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ the *signature* of deal $\mathcal{C}$. We assume that $c_1 \geq c_2 \geq \cdots \geq c_k$. The set C and the signature γ are public to all the players and even to Eve, but the cards in the hand of a player or Eve are private to herself, as in the case of usual card games.

We consider a graph called a *key exchange graph*, in which each vertex i represents a player P_i and each edge (i, j) joining vertices i and j represents a pair of players P_i and P_j sharing a one-bit secret key $r_{ij} \in \{0, 1\}$. If the key exchange graph is a tree, then all the players can share a common one-bit secret key $r \in \{0, 1\}$ as follows: an arbitrary player chooses a one-bit secret key $r \in \{0, 1\}$, and sends it to the rest of the players along the tree.

Fischer and Wright give a class of protocols, called "key set protocols," to form a tree as the key exchange graph by using a random deal of cards. We say that a key set protocol *works for a signature* γ if the protocol always forms a tree as the key exchange graph for any deal $\mathcal{C}$ having the signature γ. Let Γ_k be the set of all signatures of deals for k players, and let $\Gamma = \bigcup_{k=2}^{\infty} \Gamma_k$. Define sets W and L as follows:

$$W = \{\gamma \in \Gamma \mid \text{there is a key set protocol working for } \gamma\}; \text{ and}$$

$$L = \{\gamma \in \Gamma \mid \text{there is no key set protocol working for } \gamma\}.$$

A signature in W is called a *winning* signature. We say that a key set protocol is *optimal* if it works for all winning signatures $\gamma \in W$.

For the case $k = 2$, Fischer and Wright give a simple necessary and sufficient condition for $\gamma \in W$. However, a simple necessary and sufficient condition for the case $k \geq 3$ has not been known so far. Furthermore, Fischer and Wright show that their so-called SFP protocol is optimal. However, a complete characterization of optimal key set protocols has not been known.

In this thesis, for the case $k \geq 3$, we give a simple necessary and sufficient condition for $\gamma \in W$. Furthermore, we give a complete characterization of optimal key set protocols. We also study our newly defined "Eulerian secret key exchange."

2 Preliminaries

In this chapter we explain the key set protocol formalized by Fischer and Wright.

We first define some terms. A *key set* $K = \{x, y\}$ consists of two cards x and y, one in C_i, the other in C_j with $i \neq j$, say $x \in C_i$ and $y \in C_j$. We say that a key set $K = \{x, y\}$ is *opaque* if $1 \leq i, j \leq k$ and Eve cannot determine whether $x \in C_i$ or $x \in C_j$ with probability greater than 1/2. If K is an opaque key set, then P_i and P_j can share a one-bit secret key $r_{ij} \in \{0, 1\}$, using the following rule agreed on before starting a protocol: $r_{ij} = 0$ if $x > y$; $r_{ij} = 1$, otherwise. We say that a card x is *discarded* if all the players agree that x has been removed from someone's hand, that is, $x \notin (\bigcup_{i=1}^{k} C_i) \cup C_e$. We say that a player P_i *drops out* of the protocol if she no longer participates in the protocol. We denote by V the set of indices i of all the players P_i remaining in the protocol.

The key set protocol has four steps as follows.

1. Choose a player P_s, $s \in V$, as a *proposer* by a certain procedure.
2. The proposer P_s determines in mind two cards x and y. The cards are randomly picked so that $x \in C_s$ and $y \in (\bigcup_{i \in V - \{s\}} C_i) \cup C_e$. Then P_s proposes $K = \{x, y\}$ as a key set to all the players.
3. If there exists a player P_t holding y, then P_t accepts K. Since K is an opaque key set, P_s and P_t can share a one-bit secret key r_{st} that is unconditionally secure from Eve. (In this case an edge (s, t) is added to the key exchange graph.) Both cards x and y are discarded. Let P_i be either P_s or P_t that holds a smaller hand; if P_s and P_t hold hands of the same size, let P_i be the proposer P_s. P_i discards all her cards and drops out of the protocol. Set $V := V - \{i\}$. Return to step 1.
4. If there exists no player holding y, that is, Eve holds y, then both cards x and y are discarded. Return to step 1. (In this case no new edge is added to the key exchange graph.)

These steps 1–4 are repeated until either exactly one player remains in the protocol or there are not enough cards left to complete step 2 even if two or more players remain.

Considering various procedures for choosing the proposer P_s in step 1, we obtain the class of *key set protocols*.

The *malicious adversary* determines who holds the card y contained in the proposed key set $K = \{x, y\}$. We use a function $\mathcal{A} : \Gamma_k \times V \to V \cup \{e\}$ to represent a malicious adversary, where e is Eve's index: $\mathcal{A}(\gamma, s) = t \neq e$ means that player P_t holds card y; and $\mathcal{A}(\gamma, s) = e$ means that Eve holds card y. We denote by $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ the current signature, and denote by $\gamma'_{(s,\mathcal{A})}$ the resulting signature after executing steps 1–4 under the assumption that P_s proposes a key set $K = \{x, y\}$ and $y \in C_{\mathcal{A}(\gamma,s)}$.

We say that player P_i is *feasible* if the following condition (i) or (ii) holds: (i) $c_i \geq 2$; and (ii) $c_e = 0$, $c_i = 1$ with $i = k$, and $c_{k-1} \geq 2$. We define a mapping $f : \Gamma \to \{0, 1, 2, \cdots, k\}$, as follows: $f(\gamma) = i$ if P_i is the feasible player with the smallest hand (ties are broken by selecting the player having the largest index); and $f(\gamma) = 0$ if there is no feasible player. Hereafter we often denote $f(\gamma)$ simply by f.

As an optimal key set protocol, Fischer and Wright give the *SFP (smallest feasible player) protocol* which chooses a proposer P_s as follows: $s = f(\gamma)$ if $1 \leq f(\gamma) \leq k$; $s = 1$ if $f(\gamma) = 0$.

3 Characterization of Winning Signatures

In this chapter, for the case $k \geq 3$, we give a complete characterization of winning signatures as in the following Theorems 1 and 2. Hereafter let $B = \{i \in V \mid c_i = 2\}$, and let $b = \lfloor |B|/2 \rfloor$.

Theorem 1 *Let $k = 3$. Then $\gamma \in W$ if and only if $c_3 \geq 1$ and $c_1 + c_3 \geq c_e + 3$.*

Theorem 2 *Let $k \geq 4$, $c_k \geq 1$ and $f \geq 1$. Then $\gamma \in W$ if and only if*

$$\sum_{i=1}^{k} \max\{c_i - h^+, 0\} \geq \tilde{f},$$

where

$$\bar{f} = f - \delta,$$
$$\tilde{f} = \bar{f} - 2\epsilon,$$
$$h = c_e - c_k + k - \bar{f},$$
$$h^+ = h + \epsilon,$$
$$\delta = \begin{cases} 0 & \textit{if } f = 1; \\ 1 & \textit{if } 2 \leq f \leq k-1; \\ 2 & \textit{if } f = k \textit{ and } c_{k-1} \geq c_k + 1; \textit{ and} \\ 3 & \textit{if } f = k \textit{ and } c_{k-1} = c_k, \end{cases}$$

and

$$\epsilon = \begin{cases} \max\{\min\{c_2 - h, b\}, 0\} & \textit{if } 5 \leq f \leq k-1; \\ \max\{\min\{c_2 - h, b-1\}, 0\} & \textit{if } 5 \leq f = k \textit{ and } c_e \geq 1; \textit{ and} \\ 0 & \textit{otherwise.} \end{cases}$$

4 Characterization of Optimal Key Set Protocols

In this chapter we give a complete characterization of optimal key set protocols.

We say that a player P_i is *selectable* for γ if $\gamma'_{(i,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$. Note that a key set protocol is optimal if and only if the protocol always chooses a selectable player as a proposer whenever such a player exists. Thus we shall characterize the set of all selectable players. If $\gamma \in L$, then there is no selectable player. Therefore it suffices to consider only the case where $\gamma \in W$..

For $k = 2$ and $k = 3$, we obtain the following Theorems 3 and 4.

Theorem 3 *Let $k = 2$ and $\gamma \in W$. Then a player P_i is selectable if and only if $c_i \geq 2$ or $c_e = 0$.*

Theorem 4 *Let $k = 3$ and $\gamma \in W$. Then a player P_i is selectable if and only if $1 \leq i \leq f$.*

Before giving a characterization for $k \geq 4$, we first give some definitions.

Let $V_r = \{i \in V \mid i = \max X \textit{ and } X \in V/R\}$, where V/R is the quotient set of V under the equivalence relation $R = \{(i,j) \in V \times V \mid c_i = c_j\}$. Hereafter we shall obtain a necessary and sufficient condition for a player P_i, $i \in V_r$, to be selectable. Of course, such a necessary and sufficient condition immediately yields a complete characterization of all selectable players (whose indices are not necessarily in V_r).

Define f_m, M and $\bar{\epsilon}$ as follows: $f_m = \min\{i \in V \mid c_i = c_f\}$, $M = \sum_{j=1}^{k} \max\{c_j - h^+, 0\}$, and

$$\bar{\epsilon} = \begin{cases} \max\{\min\{c_3 - h, b\}, 0\} & \textit{if } 5 \leq f \leq k-1; \\ \max\{\min\{c_3 - h, b-1\}, 0\} & \textit{if } 5 \leq f = k \textit{ and } c_e \geq 1; \textit{ and} \\ 0 & \textit{otherwise.} \end{cases}$$

Define *Conditions 1* and *2* as follows. Note that no signature satisfies both Conditions 1 and 2.

(Condition 1)

$5 \leq f = k$ and $c_{k-2} = c_{k-1} = c_k + 1$.

(Condition 2)

$c_{f_m - 2} = c_{f_m - 1} = 3$, $|B|$ is an odd number, and the following (i) or (ii) holds: (i) $6 \leq f \leq k-1$ and $c_2 - h \geq b + 1$; and (ii) $6 \leq f = k$, $c_e \geq 1$, $b \geq 1$ and $c_2 - h \geq b$.

Define λ and $\tilde{\epsilon}$ as follows:

$$\lambda = \begin{cases} 2 & if\ \gamma\ satisfies\ Condition\ 1; \\ 3 & if\ \gamma\ satisfies\ Condition\ 2;\ and \\ 0 & otherwise, \end{cases}$$

and

$$\tilde{\epsilon} = \begin{cases} \max\{\min\{c_2 - h - 1, b - 1\}, 0\} & if\ f \geq 8,\ c_k = 1\ and\ \lambda = 2;\ and \\ 0 & otherwise. \end{cases}$$

For $k \geq 4$, we obtain the following Theorem 5.

Theorem 5 *Let $k \geq 4$, $\gamma \in W$, $i \in V_r$ and $1 \leq i \leq f$. Then a player P_i is selectable if and only if*

$$\begin{cases} c_2 - h^+ \leq M - \tilde{f} - (\epsilon - \bar{\epsilon}) & if\ i \leq 2; \\ \sum_{j=1}^{\tilde{f} - \lambda - 2\tilde{\epsilon}} \max\{c_j - (h^+ + \tilde{\epsilon} + 1), 0\} \geq \tilde{f} - \lambda - 2\tilde{\epsilon} & if\ i = f_m - 1 \geq 4\ and\ \lambda \neq 0;\ and \\ c_i - h^+ \leq M - \tilde{f} & otherwise. \end{cases}$$

5 Protocols for Eulerian Key Exchange

We propose generalized key set protocols performing an *Eulerian secret key exchange*, in which the pairs of players sharing secret keys form an Eulerian circuit. Along the Eulerian circuit any designated player can send a message to the rest of players and the message can be finally sent back to the sender. Checking the returned message with the original one, the sender can know whether the message circulation has been completed without any false alteration. We then give three protocols. The first protocol requires the minimum number of cards when $c_1 = c_2 = \cdots = c_k$. The second requires the minimum number of cards dealt to all players. The third forms Eulerian circuits of length at most $\frac{3}{2}k$, and the time required to send the message to all players is minimum.

6 Average Length of Eulerian Circuits

In this chapter, we show that the average length of Eulerian circuits formed by the third protocol in the previous chapter is approximately $k + \ln k$.

7 Conclusions

This thesis deals with cryptographic protocols called key set protocols for unconditionally secure secret key sharing. We gave a necessary and sufficient condition for a key set protocol to work for a signature γ. Further, we completely characterized optimal key set protocols. We also introduced the notion of an Eulerian secret key exchange, and gave three efficient protocols performing it.

論文審査の結果の要旨

情報セキュリティの重要な技術として，無限の能力の計算機を使える盗聴者でさえも解読できない秘密鍵，すなわち無条件に安全な秘密鍵の共有法の開発が望まれている．何人かの秘密鍵を共有させたい人と盗聴者にカードをランダムに配布し，ある種のトランプゲームを実行することにより，無条件に安全な秘密鍵を共有させることができるが，そのために配布すべきカードの枚数に関する必要十分条件を求めることは未解決問題であった．著者はそのような条件を与えるとともに，ランダムに配布されたカードを用いて無条件に安全な秘密鍵を共有するための種々のプロトコルを設計している．本論文はこれらの成果をとりまとめたものであり，全編7章からなる．

第1章は序論である．

第2章では，無条件に安全な秘密鍵を共有するためのプロトコルに関する基本的な性質を示すとともに，従来のプロトコルの問題点を明らかにしている．

第3章では，無条件に安全な秘密鍵を共有するために配布すべきカードの枚数に関する必要十分条件を与えている．この結果は長年未解決であった問題を解決するもので，高く評価できる．

第4章では，最小のカード枚数で秘密鍵を必ず共有させることができるプロトコル，すなわち最適なプロトコルの完全な特徴付けを与えている．この特徴付けはいろいろな目的のプロトコルを設計するうえでも重要なもので，実用上も極めて有用である．

第5章では，オイラー閉路状鍵共有方式，すなわち秘密鍵を共有している人の対がオイラー閉路を構成するように秘密鍵を共有する方式を定式化し，そのためのプロトコルを設計している．オイラー閉路に沿ってメッセージを伝送することにより，送信者はメッセージが全員に正しく届いたことを確認できる．

第6章では，第5章のプロトコルで構成されるオイラー閉路の長さを確率的に解析し，その閉路の長さの期待値はハミルトン閉路の長さとほぼ同じであり，受領確認に要する時間が最小という意味でこのプロトコルが優れていることを示している．

第7章は結論である．

以上要するに本論文は，無条件に安全な秘密鍵を共有するために配布すべきカードの枚数に関する必要十分条件や最適なプロトコルの特徴付けを与えるとともに，新たにオイラー閉路状鍵共有方式を定式化し，それを実現するプロトコルを設計したものであり，暗号理論および理論計算機科学の発展に寄与するところが少なくない．

よって，本論文は博士(情報科学)の学位論文として合格と認める．