Sharing Secret Keys Along a Eulerian Circuit

Takaaki Mizuki, Hiroki Shizuya, and Takao Nishizeki

Graduate School of Information Sciences, Tohoku University, Sendai, Japan 980-8579

SUMMARY

A method for sharing secret keys that is information-theoretically secure is an important problem in the area of cryptography. By randomly distributing cards to players, it is possible to provide random information with which information-theoretically secure secret keys can be shared by players. This paper formulates sharing secret keys along a Eulerian circuit for information transmission for which the receipt can be confirmed and provides a protocol for its realization. The conditions for the success of the protocol for sharing secret keys along a Eulerian circuit are identified. Further, under the natural assumption that the same numbers of cards are distributed to each player, it is shown that the number of cards distributed is a minimum. 

Key words: Random distribution of cards; information-theoretically secure; sharing keys; Eulerian circuit.

1. Introduction

Let us assume that there are \( k \geq 2 \) players \( P_1, P_2, \ldots, P_k \) and an eavesdropper Eve with unlimited computation capability. It is desired to share a one-bit key among the players without its being known by Eve. Since Eve is assumed to have unlimited computational capability, let us consider an information-theoretically secure key sharing method. Let \( C \) be a set of \( n \) cards numbered from 1 to \( n \). First, the cards in \( C \) are randomly distributed to Eve and \( P_1, P_2, \ldots, P_k \). If the set of cards owned by \( P_j \) is \( C_j \subseteq C \) and that owned by Eve is \( C_e \subseteq C \), then this distribution is written as \( C = (C_1, C_2, \ldots, C_k; C_e) \). Here, \( C_1, C_2, \ldots, C_k \) and \( C_e \) are a partition of the set \( C \). Hence, the sets \( C_1, C_2, \ldots, C_k \) and \( C_e \) are pairwise disjoint and their union is equal to \( C \). For each \( p \) such that \( 1 \leq p \leq k \), let \( c_p = |C_p| \) and \( c_e = |C_e| \). Here, \( |A| \) denotes the cardinality of the set \( A \); \( c_p \) is the number of cards received by player \( P_p \), while \( c_e \) is the number Eve receives. Since \( n \) is the total number of cards distributed, \( n = \sum_{p=1}^{k} c_p + c_e \). Let us call \( \gamma = (c_1, c_2, \ldots, c_k; c_e) \) the signature of the distribution \( C \). Let us consider the problem of sharing an information-theoretically secure key by \( k \) players using this card distribution. Note that \( P_1, P_2, \ldots, P_k \) and Eve know the set \( C \) and the signature \( \gamma \), but do not know the cards held by others.

A problem of this kind arises in the following situation. It is intended to select \( k \) people out of \( k' \geq k \) people to carry out a certain project confidentially. Who will be selected is not known until the content of the project is determined. Let these \( k' \) people be players, and hand out cards as the initial information to these \( k' \) people. After the content of the project is determined, \( k \) people are selected from \( k' \). A problem then occurs with regard to having a key shared by the selected \( k \) people but without being noticed by the unselected \( k' - k \) people. To this end, the selected players are designated as \( P_1, P_2, \ldots, P_k \) and the remaining \( k' - k \) people as Eve as a whole. By using the card distribution \( C = (C_1, C_2, \ldots, C_k; C_e) \), let the information-theoretically secure key be shared by the players \( P_1, P_2, \ldots, P_k \) without being noticed by Eve [4].

Fischer, Paterson, and Rackoff [1] have proposed a method of sharing an information-theoretically secure one-bit key when there are two players (or \( k = 2 \)). Further, Fischer and Wright [2–4] have provided a protocol for
sharing a key such that one bit can be transmitted information-theoretically securely to k players. In this protocol, the players are considered as vertices. The graph obtained by using the pair of players sharing one-bit key as an edge constitutes a tree.

This paper gives the protocol to realize secret key sharing such that the graph G obtained with the pairs of players sharing a one-bit key as the edges forms a Eulerian circuit. (For the graph theory terminology, see Ref. 5.) Along this Eulerian circuit, secret information of one bit can be transmitted securely from one player to all the remaining players. By confirming the returned information, the secure and accurate delivery of the information can be confirmed. Hence, receipt confirmation is possible. The paper shows how the cards are distributed to the players in order for the protocol to succeed in sharing secret keys along a Eulerian circuit. It also shows that, under the natural assumption that all players receive the same number of cards, the protocol needs only the minimum of cards. Since we desire to reduce the number of cards to be distributed, the degrees of the vertices in the graph G should be as small as possible. However, it is not possible to form a Eulerian graph in which the degree of each vertex is 2, and thus, it is not possible to design a protocol with which is a Hamiltonian graph. In the paper, a protocol is given that forms a Eulerian graph G in which the degree of each vertex is 2 or 4.

2. Preliminaries

In this section, known methods [1, 2, 4] are explained in which the one-bit key is shared information-theoretically securely by k people by means of card distribution C = (C1, C2, . . . , Ck; C). Let us call the set K = {x, y} consisting of a card x of C1 and a card y of Ck as the key set. If Eve cannot discriminate at a probability exceeding 1/2 whether x ∈ C1 or X ∈ Ck then K is called a secret key set. Obviously, P1 and Pk know that x ∈ C1 and y ∈ Ck. If K is a secret key set, then P1 and Pk can share the one-bit key r information-theoretically securely in the following manner: One bit key r can be shared by predetermining r = 0 if x > y and r = 1 if x < y. Since Eve cannot discriminate whether r = 0 or r = 1 at a probability exceeding 1/2, the key r is information-theoretically secure.

In the following description, it is understood that discarding card x implies the elimination of x from someone’s hand containing x and agreement by all k players that x is not in any hand. Then, the players can construct a secret key set K by the following protocol.

(1) According to a certain procedure, the player Ps, 1 ≤ s ≤ k such that Cs ≠ φ is chosen as the proposer.

(2) Player Ps randomly selects his own card x and the other card y, and proposes to everyone the set K = {x, y} as the key set.

(3) If there exists a player Pt with y, then Pt informs that K can be accepted as a key set. (Then, P1 and Pk can share the one-bit key information-theoretically securely since K is a secret key set.) Then, x and y are discarded. Further, of Ps and Pt, the one with fewer cards in hand discards all the cards and leaves the protocol so that the process is returned to Step 1.

(4) If Eve has y, then x and y are discarded, and the process returns to Step 1.

This protocol is repeated until the number of players with cards in hand (and remaining in the protocol) becomes at most one.

In this protocol, the players are vertices, and the graph constructed by connecting two players sharing a one-bit key with an edge becomes a tree. By taking the exclusive OR of the key shared with the one bit to be transmitted and carrying out transmission along an edge of this tree, it is possible to transmit one bit from anyone to everyone information-theoretically securely. Fischer and Wright have provided the SFP procedure [2, 4] as the procedure in Step 1 and demonstrated that, if the SFP key set protocol by this procedure is followed, the key sharing graph necessarily becomes a tree for every distribution such that the signature γ = (c1, c2, . . . , ck; e) satisfies ci ≥ 1 for every i, 1 ≤ i ≤ k and max ci + min ci ≥ k + ε.

3. Eulerian Circuit Key Sharing and Key Set Protocol

In this paper, a protocol is provided that constructs a Eulerian circuit instead of a tree. If a Eulerian circuit can be constructed, then it is possible, as described below, to transmit information to all members and to confirm receipt.

It is desirable to send one bit information-theoretically securely from one player to all others, and to confirm that everyone has received it, because there may be damage and congestion in the network. In order to carry out transmission information-theoretically securely, it is necessary to share the one-bit key between two players if one bit is transmitted between them. The information is transmitted from the sending player with the key and is finally returned to the sending player. If it is identical to the original information, then it can be confirmed that transmission to everyone was successful. If different, falsification can be detected. Such information transmission can be carried out along a Eulerian circuit.

[Definition 1] When players P1, P2, . . . , Pk are the vertices, and Ps and Pj share m one-bit keys, the undirected
multigraph $G$ obtained by connecting the vertices $i$ and $j$ with $m$ multiple edges is called the key sharing graph.

[Definition 2] If the key sharing graph $G$ is a Eulerian graph, that is, it is connected and the degrees of all vertices are even, then this key sharing is called Eulerian circuit key sharing.

The following general protocol to realize Eulerian circuit key sharing is considered as an extension of the protocol introduced in the previous section.

1. According to a certain procedure (called “Procedure $A$”), player $P_s$ with $C_s \neq \emptyset$ is selected as the proposer.
2. Player $P_s$ randomly selects his own card $x$ and card $y$ for others, and proposes $K = \{x, y\}$ as the key set to everyone.
3. If there exists a player $P_t$ with $y$, then $P_t$ states that $K$ can be accepted as the key set and discards $x$ and $y$.
4. If eavesdropper Eve rather than a player has $y$, then $x$ and $y$ are discarded.
5. According to a certain procedure (called “Procedure $B$”), a set $X$ of several players is selected. These players are asked to discard all the cards they are holding. All players who are not holding cards are eliminated from the protocol, and the process returns to Step 1.

When Step 3 is carried out, $P_s$ and $P_t$ share one bit, and their cards are reduced by one each. When Step 4 is carried out, the cards held by $P_s$ and Eve are reduced by one each. This protocol is repeated until the number of players with nonempty hands (and hence who remain in the protocol) is at most one.

According to procedure $A$, a proposer is selected, while according to procedure $B$, a person to be eliminated from the protocol is determined. The protocol is confirmed by specifically determining these procedures. The protocol obtained by varying procedures $A$ and $B$ is called the key set protocol. The key set protocol determined by procedures $A$ and $B$ is called the (A,B)-key set protocol. The protocol introduced in the previous section is a special case.

In order to make the key sharing graph a tree, procedures $A$ and $B$ can be simple, as described in the previous section. However, in order to construct a Eulerian circuit, it is necessary to define procedures $A$ and $B$ so that they are dependent on the present number of cards in the hand and on the key sharing graph. Such procedures are not simple. In fact, procedures $A$ and $B$ provided in this paper are sophisticated, as seen in the next section.

The success of the protocol is defined as follows.

[Definition 3] The (A,B)-key set protocol succeeds in a Eulerian circuit key sharing for the signature $\gamma = (c_1, c_2, \ldots, c_k)$ if a Eulerian circuit key sharing is always possible for any card distribution $C$ with the signature $\gamma$ as long as the protocol is followed.

So that procedures $A$ and $B$ can be described easily, the procedure PROTOCOL to imitate the key set protocol is given as follows: Let the card distribution be $C = (C_1, C_2, \ldots, C_k)$, and the signature of $C$ be $\gamma = (c_1, c_2, \ldots, c_k)$. Let $V = \{1, 2, \ldots, k\}$ be the set consisting of the vertices corresponding to the players. In the following procedure PROTOCOL, $W$ denotes the set of the vertices corresponding to the players with non-empty hands. Also, $E$ indicates the set of the edges corresponding to the shared key, while $C_1, C_2, \ldots, C_k$ denote the sets of the cards held by the players and Eve. Further, $d(i)$ denotes the degree of the vertex $i \in V$ in the graph $G = (V, E)$, whereas $d_X(i)$ is the number of times a card in $C_i$ is included in the key sets $K = \{x, y\}$ proposed by $P_r$.

**Procedure PROTOCOL**

1. $W := \{1, 2, \ldots, k\}; E := \emptyset$;
2. for $i := 1$ to $k$ do $d(i) := 0$;
3. for $i := 1$ to $k$ do $d_X(i) := 0$;
4. while $|W| \geq 2$ do
5. According to procedure $A$, proposer $s \in W$ is selected;
   - Select proposer $P_s$;
   - Among $P_s$’s hand $C_s$, a card $x \in C_s$ is selected at random;
   - Select card $x$;
   - From those other than $C_x$, a card $y \in (\cup_{t \in W - \{s\}} C_t) \cup C_s$ is randomly chosen.
   - Select card $y$;
6. if there exists $t \in W$ such that $y \in C_t$ then
   - $P_t$ has $y$;
7. $E := E \cup \{(s, t)\}$;
8. Add the edge $(s, t)$ to graph $G$;
9. $d(s) := d(s) + 1; d(t) := d(t) + 1$;
10. $C_x := C_x - \{x\}; C_s := C_s - \{y\}$
   - Discard $x$, $y$;
11. else
   - Eve has $y$;
12. $d_X(s) := d_X(s) + 1$;
13. $C_x := C_x - \{x\}; C_s := C_s - \{y\}$
   - Discard $x$, $y$;
14. $\mathbf{fi}$
15. According to procedure $B$, $X \subseteq W$ is selected.
16. For all $i \in X$, let $C_i := \emptyset$.
   - Discard all hands of the player in the set $X$;
17. $W := W - \{i\}$
   - Eliminate players with empty hands;
18. elihw

If $G = (V, E)$ is a Eulerian graph at the completion of the procedure PROTOCOL, a Eulerian circuit key sharing has been achieved.

If $B = V - W$, then $W$ and $B$ are the partition of $V$. At any time in the execution of PROTOCOL, for all $p \in W$
If the vertex $p$ belongs to $B$ in the graph $G = (V, E)$, then no edge is connected to $p \in B$ in the subsequent while loops and $C_p = \phi$. Hence, for all $p \in B$
\[ c_p = |C_p| + d(p) + d_e(p) \tag{1} \]

Also,
\[ c_e = |C_e| + \sum_{p \in V} d_e(p) \tag{3} \]

4. Protocol to Realize a Eulerian Circuit Key Sharing

In this section, procedure $A$, to select the proposer, and procedure $B$, to select the players to be eliminated, are specifically determined to be procedures $A^1$ and $B^1$ so that the $(A^1, B^1)$-key set protocol is determined. Next, the condition is derived such that this protocol succeeds in a Eulerian circuit key sharing for the signature $\gamma = (c_1, c_2, \ldots, c_k; c_e)$. Hence, the following theorem is proved.

[Theorem 1] If the signature $\gamma = (c_1, c_2, \ldots, c_k; c_e)$ satisfies the following condition, then $(A^1, B^1)$-key set protocol succeeds in a Eulerian circuit key sharing for $\gamma$.

(Conditions) For every $i \in V$, the following are satisfied.

(a) For $k = 2$, $c_1, c_2 \geq 2$, $c_1 + c_2 \geq c_e + 4$.
(b) For $k = 3$,
\[ c_i \geq \begin{cases} c_e + 2 & (c_e \leq 1) \\ \left\lfloor c_e/2 \right\rfloor + 3 & (c_e \geq 2) \end{cases} \]
(c) For $k \geq 4$, $c_i \geq \left\lfloor c_e/2 \right\rfloor + 4$. \hfill $\square$

It is further shown that, for the case when all of the players receive the same number of cards, or for $\gamma = (c_1, c_2, \ldots, c_k; c_e)$ such that $c_1 = c_2 = \ldots = c_e$, this $(A^1, B^1)$-key set protocol is optimum in the sense that the number of necessary cards is the minimum. That is, we shall prove the following theorem.

[Theorem 2] For $\gamma = (c_1, c_2, \ldots, c_k; c_e)$ such that $c_1 = c_2 = \ldots = c_e$ the necessary and sufficient condition for the existence of a key set protocol succeeding in a Eulerian circuit key sharing is as follows.

For $k = 2$, $c \geq \left\lfloor c_e/2 \right\rfloor + 2$.
For $k = 3$,
\[ c_i \geq \begin{cases} c_e + 2 & (c_e \leq 1) \\ \left\lfloor c_e/2 \right\rfloor + 3 & (c_e \geq 2) \end{cases} \]
For $k = 4$, $c \geq \left\lfloor c_e/4 \right\rfloor + 4$. \hfill $\square$

4.1. Protocol

Specifically determining procedures $A$ and $B$ in the procedure PROTOCOL to be the following procedures $A^1$ and $B^1$ gives the $(A^1, B^1)$-key set protocol.

If $c_i \geq \left\lfloor c_e/2 \right\rfloor + 4$ for all $i \in V$ with $k \geq 4$, the connected components of graph $G = (V, E)$ take the forms in Fig. 1 during the execution of the protocol determined by procedures $A^1$ and $B^1$ described below. In the figure, the player with cards in hand, or the vertex in $W$, is indicated by a white dot, whereas the one with an empty hand, or the vertex in $B = V - W$, is indicated by a black dot. As shown later in Lemmas 1 and 4, note that the degree of each vertex is at most 4. Especially, the degree of the black vertex is 2 or 4, and is always even. In each connected component, one or two white vertices exist. If one exists [Fig. 1(a) and (c)], the degree of the white vertex is 0 or 2, and is even. On the other hand, if two exist [Fig. 1(b), (d), (e)], the degree of the white vertex is 1 or 3, and is odd.

Let us partition the set $W$ to the subsets $W_1, W_2,$ and $W_3$.

$W_1 = \{ i \in W | d(i) = 2 \text{ or } d(i) = 3 \text{ and another white vertex contained in the same connected component with } i \text{ is of degree 1} \}$.

$W_2 = \{ i \in W | d(i) = 0 \text{ or } d(i) = 1 \text{ and another white vertex contained in the same connected component with } i \text{ is of degree 1} \}$.

$W_3 = W - W_1 - W_2$.

Then,

$W_3 = \{ i \in W | d(i) = 1 \text{ and another white vertex contained in the same connected component with } i \text{ is of degree 3} \}$.

In procedure $A^1$, proposer $s$ is selected in the order of $W_1$, $W_2$, and $W_3$.

The white vertex of degree 2 in Fig. 1(a) and those of degree 3 in (b) are contained in $W_1$. The white vertices in
(c) and (d) are contained in $W_2$. Also, the white vertex of degree 1 in (b) and those in (e) are in $W_3$. From the preceding definitions of $W_1$ and $W_3$, if the proposer $s$ is $s \in W_1 \cup W_2$ and a new circuit is formed in $G$ by the edge $(s, t)$, or $s$ and $t$ are in the same connected component, then $t$ is of degree 1 and $d(t) = 2$ due to the new edge $(s, t)$. On the other hand, if the proposer $s$ is $s \in W_3$ and a new circuit is formed in $G$ by the new edge $(s, t), d(t) = 4$ by the new edge $(s, t)$. In addition, as seen later, then $t$ remains to be a white vertex. If the protocol were not completed, this vertex would have degree higher than 6.

First, procedure A is fixed to the following procedure $A^1$. In procedure $A^1$, proposer $s$ is selected in the order of $W_1$, $W_2$, and $W_4$. In addition, all white vertices $i \in W$ always satisfy $|C_i| + d(i) \geq 4$. If $|C_i| + d(k) \leq 3$, then the white vertex $i$ can no longer be of degree 4.

**Procedure $A^1$**

The proposer $s \in W$ is selected as follows.

- **Case A1:** $C_s \neq \phi$ and there exists $s \geq W_1 \cup W_2$ such that $|C_s| + d(s) \geq 5$.

  If there exists $s \in W_1$ such that $|C_s| + d(s) \geq 5$ [Fig. 1(a), (b)], then such an arbitrary $s$ is chosen. If not, an arbitrary $s \in W_2$ such that $|C_s| + d(s) \geq 5$ is chosen. [See Fig. 1(c) and (d)].

- **Case A2:** $C_s = \phi$ and $W_1 \cup W_2 \neq \phi$.

  If $W_1 = \phi$, an arbitrary vertex in $W_1$ is chosen as the proposer $s$. [See Figs. 1(a) and (b).] For $W_1 = \phi$, an arbitrary $s \in W_2$ is chosen [Fig. 1(c), (d)].

- **Case A3:** Other cases. (As shown in Lemma 4 later, it is already $W = W_3, |W| = 2$. The protocol is complete as soon as an edge connecting the two vertices in $W$ is added to $G$.)

Let us select $s \in W$ with a larger $|C_s|$.

Procedure B is fixed to the following procedure $B^1$. In procedure $B^1$, basically if the degrees of the vertices $s$ and $t$ become even, then $s$ and $t$ become black vertices and drop out of the protocol. If both $s$ and $t$ are in the same connected component before the edge $(s, t)$ is added, then only the proposer $s$ becomes a black vertex and drops out of the protocol. (If both become black vertices, all vertices in the connected component become black vertices so that the graph $G$ is no longer connected.)

**Procedure $B^1$**

The set $X \subseteq W$ of the players asked to discard the cards is chosen as follows.

- **Case B1:** For $y \in C_e$.

  Let $X := \phi$.

- **Case B2:** There is a circuit containing the edge $(s, t)$ in $G = (V, E)$. Hence, $y \in C_e$, $1 \leq t \leq k$, and $s$ and $t$ are already in the same connected component before the edge $(s, t)$ is added to $G$.

  Let $X := \{s\}$.

- **Case B3:** Other cases. Hence, $y \in C_e$, $1 \leq t \leq k$, and the connected component containing $s$ and the connected component containing $t$ are connected by the edge $(s, t)$.

  $X := \{i \mid d(i) \text{ is even}, i = s \text{ or } t\}$

In Fig. 2, an example is shown for the generation process of the graph containing the connected component in Fig. 1(e). Note that the degree of each vertex of the key sharing graph $G$ finally obtained is 2 or 4.

Let $\text{PROTOCOL}^1$ be the procedure to imitate the $(A^1, B^1)$-key set protocol.

### 4.2. Proof of Theorem 1

In this section, a proof of Theorem 1 is presented. First, the following Lemmas 1–3 are obtained.

[Lemma 1] Let $k \geq 4$. Assume that $c_x \geq \lfloor c_x/2 \rfloor + 4$ for all $i \in V$. If, in the execution of the procedure $\text{PROTOCOL}^1$, the proposer $s \in W$ is always selected by case A1 or A2 in the previous while loop, the following (a), (b), and (c) hold.

- (a) For all white vertices $i \in W, |C_i| + d(i) \geq 4$.
- (b) There are one or two white vertices in each connected component of $G = (V, E)$. If there is one [Fig. 1(a), (c)], the degree of such a vertex is 0 or 2. If there are

![Fig. 2. A generating process of $G$ containing the graph in Fig. 1(e).]
two [Fig. 1(b), (d), (e)], the degrees of these vertices are 1 or 3.
(c) For all black vertices \( i \in B = V - W, d(i) \) is either 2 or 4. (For proof, see Appendix 1.)

[Lemma 2] Let us assume that \( c_i \geq \left\lceil \frac{c_e}{2} \right\rceil + 4 \) for all \( i \in V \). If there are two white vertices \( i, j \in W \) such that \( |C_j| + d(i) \leq 4 \) and \( |C_j| + d(j) \leq 4 \) in the execution of the procedure PROTOCOL\(^1\), then \( C_e = \phi \). (For proof, see Appendix 2.)

[Lemma 3] Let \( k \geq 4 \). Assume that \( c_i \geq \left\lceil \frac{c_e}{2} \right\rceil + 4 \) for all \( i \in V \). The following (a) and (b) hold if proposer \( s \) is always selected by case A1 or A2 in the previous while loop during execution of the procedure PROTOCOL\(^1\).

(a) \( |W_i| \leq 2 \)
(b) There is at most one vertex \( i \) which is in \( W_i \) and is not selected as the proposer \( s \) (during the execution of PROTOCOL\(^1\)) and \( |C_j| + d(j) = 4 \). (For proof, see Appendix 3.)

From Lemmas 2 and 3, the following Lemma 4 can be proven. The proof is presented in Appendix 4.

[Lemma 4] Let \( k \geq 4 \). Assume that \( c_i \geq \left\lceil \frac{c_e}{2} \right\rceil + 4 \) for all \( i \in V \). Immediately before proposer \( s \) is selected for the first time by case A3 during the execution of the procedure PROTOCOL\(^1\), the graph \( G = (V, E) \) is connected and \( |W| = 2 \). Also, if \( W = \{i, j\} \), then \( |C_j| + |C_j| \geq |C_j| + 2 \).

By means of Lemmas 1 and 4, Theorem 1 can be proven as follows.

(Proof of Theorem 1) Let us provide a proof for \( k \geq 4 \). If \( k = 2 \) or \( k = 3 \), proof is possible by slightly modifying the procedures A\(^1\) and B\(^1\). Since \( |W| = 1 \) and \( G \) is connected. If \( W = \{i\} \) is assumed, \( d(i) = 0 \) or 2. Since \( |W| = k \geq 4 \) and \( G \) is connected, \( d(i) = 2 \). Also, the degree of the vertices other than \( i \), namely of all black vertices, is 2 or 4. Hence, \( G \) is a Eulerian graph.

Next, let us consider the case in which proposer \( s \) was selected by case A3. From Lemma 4, \( G \) was connected and \( |W| = 2 \) immediately before selection. Then, if the two white vertices are \( i \) and \( j \), then \( |C_j| + |C_j| \geq |C_j| + 2 \). Also, from Lemma 1, the degree of all black vertices is 2 or 4 while the degree of \( i \) and \( j \) is 1 or 3. Hence, if any edge is added between \( i \) and \( j \) prior to the completion of the procedure PROTOCOL\(^1\), then the degrees of all vertices become 2 or 4 and \( G \) becomes a Eulerian graph. From the choice of \( s \) in the case A3 and from \( |C_j| + |C_j| \geq |C_j| + 2 \), an edge must be added between \( i \) and \( j \) and \( G \) becomes a Eulerian graph so that PROTOCOL\(^1\) is complete.

### 4.3. Proof of Theorem 2

In this section, Theorem 2 is proven. To this end, the lower bound is given for the number of cards needed for the key set protocol to succeed in a Eulerian circuit key sharing. If a certain key set protocol succeeds in a Eulerian circuit key sharing for the signature \( \gamma = (c_1, c_2, \ldots, c_e; c_e) \), the key sharing graph always becomes a Eulerian graph for any card distributions \( C = (C_1, C_2, \ldots, C_e; C_e) \) with the signature \( \gamma \). Hence, in the procedure PROTOCOL to imitate this protocol, \( G = (V, E) \) is a Eulerian graph when the procedure is complete, no matter how card \( y \) is selected in (P7). In order to prove the lower bound of the number of cards, an adversary is determined so as to select \( y \) inconvenient to the players.

First, the following holds as a trivial lower bound on the necessary number of cards.

[Lemma 5] If there is a key set protocol succeeding in a Eulerian circuit key sharing for the signature \( \gamma = (c_1, c_2, \ldots, c_e; c_e) \), then \( c_p \geq 2 \) for all \( p \in V \) and \( \sum_{p=1}^k c_p \geq 2k + c_e \).

(Proof) If a Eulerian circuit key sharing is successful and the protocol is complete, then \( G \) is a Eulerian graph. Hence, for all \( p \in V, c_p \geq 2 \) and \( \sum_{p=1}^k c_p \geq \sum_{p=1}^k (d(p) + 0(p)) = 2k + c_e \). From this Lemma, the following corollary holds for the lower bound on the number of necessary cards when \( k = 2 \).

[Corollary 1] If there exists a key set protocol succeeding in a Eulerian circuit key sharing for \( \gamma = (c_1, c_2; c_e) \), then \( c_1, c_2 \geq 2 \) and \( c_1 + c_2 \geq c_e + 4 \).

(Proof) For \( k \geq 3 \), the following Lemma holds.

[Lemma 6] Let \( k \geq 3 \). If there exists a key set protocol succeeding in a Eulerian circuit key sharing for \( \gamma = (c_1, c_2, \ldots, c_e; c_e) \), then the following (a) and (b) hold.

(a) For \( k \geq 4 \), there exists either \( i \in V \) such that \( c_i \geq c_i + 4 \) for a pair \( i, j \in V \) such that \( c_i + c_j \geq c_e + 8 \).

(b) For \( k = 3 \), there exists a pair \( i, j \in V \) such that \( c_i + c_j \geq c_e + 6 \) if \( c_e \geq 2 \). (If \( c_e \leq 1 \), either \( c_i \geq c_i + 2 \) for all \( i \) or there exists a pair \( i, j \in V \) such that \( c_i + c_j \geq c_e + 6 \).)

(Proof) Let us provide the proof for (a). The proof for (b) is omitted due to space limitations. Let the partition of the set \( V \) be \( V_1 \) and \( V_1 \). Here, \( V_1 = V_1 \cup V_2 \) and \( V_1 \cap V_2 = \phi \). Since \( k \geq 4 \), there is a partition such that \( |V_1|, |V_2| \geq 2 \). Denote by \( G_i = (V_i, E_i) \) the subgraph of \( G \) induced by \( V_i \), \( i = 1, 2 \), where \( E_i \) is the set of the edges of \( G \) with both ends in \( V_i \). It is assumed that PROTOCOL is successful in an Eulerian circuit key sharing for \( \gamma = (c_1, c_2, \ldots, c_e; c_e) \). No matter how the card \( y \) is chosen at (P7) in PROTOCOL, \( G \) is a Eulerian graph when PROTOCOL terminates. Let us consider an adversary that selects \( y \) as follows.
Hence, Lemma holds for

For $c_e = 0$, it is found from (1) that $c_i + |C_i| + d(i) \geq c_e + 4$. Hence, Lemma holds.

For $c_e = 1$, if $d_i(i) = 1$, then $c_i + |C_i| + d(i) + d_i(j) \geq 4 + 1 \geq c_e + 4$. Hence, Lemma holds. If $d_i(i) = 1$ is not satisfied, then $d_i(i) = 0$ and $d_i(j) = 1$. The white vertex of $G_i$ is $j$ only. Similar to the case for $i$, $d(j) \geq 2$ and $|C_j| \geq 2$ as well as $c_j \geq c_e + 4$. Therefore, Lemma holds.

Finally, let us consider the case of $c_e \geq 2$. Assume that $c_p < c_e + 4$ for all $p \in V$. Then, $d_i(i) = c_i - (|C_i| + d(i)) < c_e + 4 - 4 = c_e$. Also, since $d_i(i) + d_i(j) = c_i$, $d_i(j) > 0$. Hence, the white vertex in $G_j$ is $j$ only. Therefore, arguments similar to those for $G_i$ above are applied to $G_2 = (V_2, E_2)$ so that $|C_1| + d(i) \geq 4$. From the above,

$$c_i + c_j + |C_i| + |C_j| + d(i) + d(j) \geq c_e + 8.$$ 

Hence, Lemma holds for $c_e \geq 2$. \hfill $\Box$

It is immediately obvious that Theorem 2 holds from Theorem 1, Corollary 1, and Lemma 6 for the signature $\gamma = (c_1, c_2, \ldots, c_e)$ such that $c_1 = c_2 = \ldots = c_e$ when all players receive the same number of cards. Thus, $(A^1, B^1)$-key set protocol is optimum in the sense that the number of necessary cards is the minimum.

5. Conclusions

In addition to sending information securely by sharing a secret key, it is important to confirm that the information has reached all members. Eulerian circuit key sharing was formulated, and the protocol for realization was provided, for information transmission enabling confirmation of receipt. The sufficient condition on the signature was given for the protocol to succeed in a Eulerian circuit key sharing. Under the natural assumption that every player receives the same number of cards, the lower bound for the necessary number of cards was given. It was shown that the protocol in this paper is optimum in the sense that the necessary number of cards is the minimum. Even for the protocols [2, 4] for which the graph is a tree, there is no non-trivial lower bound on the necessary number of cards. Since a tree needs to be simply formed in the protocols in Refs. 2 and 4, it is sufficient to place one white vertex at each connected component of the present key sharing graph. On the other hand, in the protocol in this paper in which a Eulerian circuit is formed, the number of white vertices of each connected component is one or two. For one, the degree is even, and for two, the degree is odd. The black vertices are always of even degree. Thus, the protocol in this paper is sophisticated.

In the case where every player may not receive the same number of cards, the total number of cards distributed can be made smaller. It is possible to provide an optimum protocol in the sense that the total number of necessary cards is the minimum [6]. The length of the Eulerian circuit corresponds to the time needed for confirmation of receipt. It is also possible to provide a protocol in which the key sharing graph has the shortest Eulerian circuit [7].

Acknowledgment. The authors thank Professor H. Suzuki of Ibaraki University for useful discussions.

REFERENCES

of the others. Hence, it is sufficient to show that its degree. Also, although the cards in the hand of
loop at the
Hence, (a) is proved.

d keys along an Eulerian circuit with the minimum number
7. Mizuki T, Shizuya H, Nishizeki T. Sharing secret
d keys along the shortest Eulerian circuit. Trans IEICE

Appendix

1. Proof of Lemma 1

In the following, \( G = (V, E) \), \( W, d(i), C_t \), and \( C_e \) immediately
carrying out the \textbf{while} loop in the \( l \)-th time are
written as \( G^l = (V, E^l) \), \( W^l, d^l(i), C^l_t \), and \( C^l_e \).

(Proof) An induction method in regard to the number
of the executions of the \textbf{while} loop is used for the proof.
Graph \( G^{l-1} = (V, E^{l-1}) \) immediately before the first execution
of the \textbf{while} loop is made of \( k \) isolated vertices. Hence, for
all \( i \in V, d(i) = 0 \) and \( |C^l_t| = c_t \) as well as \( V = W_2 \) so that
clearly (a), (b), and (c) hold. It is now assumed that (a), (b),
and (c) are satisfied immediately after execution of the
\textbf{while} loop in the \((l-1)\)-th time, namely immediately before
execution in the \( l \)-th time. It is then proven that these are
satisfied immediately after the \textbf{while} loop is executed in
the \( l \)-th time. Here, let \( l \geq 1 \).

(a) First, let us consider the case in which the card \( y \)
selected randomly from \( \cup_{p \in W^{l-1}} C_{p-1} \) is \( y \in C_{t-1}^l \).
Since \( C_{t-1}^l \neq \emptyset \), proposer \( s \) is selected not in case A2 but case
A1. Since \( y \in C_{t-1}^l \), \( G^{l-1} \) and no vertex has a change in
its degree. Also, although the cards in the hand of \( s \) are
reduced by one, there is no change in the cards in the hands
of the others. Hence, it is sufficient to show that
\( |C_j^l| + d^l(s) \geq 4 \). From the selection in case A1,
\( |C_{t-1}^l| + d^l(s) \geq 5 \). Also, since \( |C_j^l| = |C_{t-1}^l| = 1 \)
and \( d^l(s) = d^l(s) \), one finds \( |C_j^l| + d^l(s) \geq 4 \).

Next, let us consider the case of \( y \notin C_{t-1}^l \). Since the
degrees and the cards in the hands of others besides \( s \) and \( t \)
do not change, it is sufficient to show that \( |C_j^l| + d^l(s) \geq 4 \)
and \( |C_j^l| + d^l(t) \geq 4 \). By the assumption of the induction
method, \( |C_{t-1}^l| + d^l(s) \geq 4 \) and \( |C_{t-1}^l| + d^l(t) \geq 4 \). Also,
\( d^l(s) = d^l(s) \) and \( |C_j^l| = |C_{t-1}^l| - 1 \), \( d^l(t) = d^l(t) \) and
\( |C_j^l| = |C_{t-1}^l| - 1 \), \( |C_j^l| = |C_{t-1}^l| - 1 \), \( d^l(s) = d^l(s) \) and \( |C_j^l| + d^l(t) \geq 4 \).
Hence, (a) is proved.

(b), (c) First, consider \( y \in C_{t-1}^l \). Then, \( G^l = G_{t-1}^l \), and
there is no change in the degree of any vertex. From (a),
\( |C_j^l| + d^l(s) \geq 4 \) immediately after the execution of the \textbf{while}
loop at the \( l \)-th time. Also, in \( G^l \), (b) is satisfied, and \( s \) is
a white vertex. Hence, \( d^l(s) \leq 3 \). Therefore,
\( d^l(s) = d^l(s) \leq 3 \) and \( |C_j^l| \geq 1 \), so that proposer \( s \) remains
a white vertex in \( G^l \). Hence, (b) and (c) are satisfied.

Next, let us consider the case with \( y \in C_{t-1}^l \). There are
the following two cases.

(Case 1) In \( G^l \), \( s \) and \( t \) are in the same connected
component.

In regard to graph \( G^l \) immediately after execution of
the \textbf{while} loop at the \( l-1 \)-th time, (b) is satisfied. Since the
white vertices \( s \) and \( t \) are in the same connected component,
\( d^l(s) \) and \( d^l(t) \) are 1 or 3. Since proposer \( s \) was selected
in Case A1 or A2, \( s \in W_1 \cup W_2 \). [See Fig. 1(b), (d)] Since
\( s \) and \( t \) are in the same connected component, \( d^l(t) = 1 \)
from the definition of \( W_1 \) and \( W_2 \). If the \textbf{while} loop
is executed at the \( l \)-th time, the vertices \( s \) and \( t \) are connected
by an edge so that \( d^l(s) \) becomes 2 or 4 while \( d^l(t) \) becomes
2. By Case B2, \( X = \{ s \} \) is selected and \( s \) becomes a black
vertex. Since \( d^l(s) = 1 \) and \( |C^l_j| + d^l(s) \geq 4 \), \( |C^l_{t-1}| \geq 3 \).
Hence, \( |C^l_j| = |C^l_{t-1}| - 1 \geq 2 \) while \( t \) is still a white vertex in \( G^l \).
In this manner, (b) and (c) are satisfied in \( G^l \).

(Case 2) In \( G^l \), \( s \) and \( t \) are in different connected
components.

First, let us assume that both \( d^l(s) \) and \( d^l(t) \) are odd
numbers. Then, \( d^l(s) \) and \( d^l(t) \) are 0 or 2. Also, \( s \) is the
only white vertex in the connected component containing \( s \)
in \( G^l \) while \( t \) is the only white vertex in the connected
component containing \( t \). Since \( |C^l_{t-1}| + d^l(s) \geq 4 \) and
\( |C^l_{t-1}| + d^l(t) \geq 4 \), one finds \( |C^l_{t-1}| \geq 4 \). Hence,
\( |C^l_{t-1}| \geq 1 \). Also, since \( d^l(s) \) and \( d^l(t) \) are 1 or 3, \( X = \phi \) in
Case B3. Therefore, \( s \) and \( t \) are black vertices in \( G^l \). The
white vertices in the connected components containing
them are \( s \) and \( t \) only. Hence, (b) and (c) hold.

Next, assume that both \( d^l(s) \) and \( d^l(t) \) are even numbers.
Then, \( d^l(s) \) and \( d^l(t) \) are 0 or 2. Also, \( s \) is the
only white vertex in the connected component containing \( s \)
in \( G^l \) while \( t \) is the only white vertex in the connected
component containing \( t \). Since \( |C^l_{t-1}| + d^l(s) \geq 4 \) and
\( |C^l_{t-1}| + d^l(t) \geq 4 \), one finds \( |C^l_{t-1}| \geq 4 \). Hence,
\( |C^l_{t-1}| \geq 1 \). Also, since \( d^l(s) \) and \( d^l(t) \) are \( 1 \) or \( 3 \), \( X = \phi \) in
Case B3. Therefore, \( s \) and \( t \) remain white vertices in \( G^l \). The
white vertices in the connected components containing
them are \( s \) and \( t \) only. Hence, (b) and (c) hold.

Next, let us assume that \( d^l(s) \) is odd and \( d^l(t) \) is
even. Then, \( d^l(s) \) is 1 or 3 while \( d^l(t) \) is 0 or 2. There is
another white vertex \( v \) in the connected component in which
the white vertex \( s \) of \( G^l \) is contained, and \( d^l(v) \) is 1 or 3.
On the other hand, \( t \) is the only white vertex in the connected
component of \( G^l \) containing \( t \). Since \( |C^l_{t-1}| + d^l(t) \geq 4 \) and
\( |C^l_{t-1}| + d^l(t) \geq 2 \) and \( |C^l_{t-1}| \geq 1 \). Also, since \( d^l(s) \) is 2 or 4,
while \( d^l(t) \) is 1 or 3, \( X = \{ s \} \) in Case B3 while \( s \) becomes a black
vertex in \( G^l \) and \( t \) remains a white vertex. Only \( t \) and \( v \) are
the white vertices in the connected component containing
\( s \) and \( t \) in \( G^l \). Since \( d^l(v) = d^l(t), d^l(v) \) is 1 or 3. Hence, (b)
and (c) hold.
Hence, from Lemma 2,

\[ C_e \neq \phi \] and \[ \|C\| + d(i) = 4 \]. Therefore, the white vertex \( i \) of the graph \( G \) is either in \( W_3 \) or in \( W_1 \cup W_2 \), and \( C_e \neq \phi \) and \[ \|C\| + d(i) = 4 \] are satisfied. Hence, as shown in Fig. 1(d), \( G \) has two white vertices. There is no connected component in which the degrees of these vertices are both 1. The reason is as follows. If such a component exists, and the two white vertices contained are \( i \) and \( j \), it is necessary from \( i, j \in W_2 \) that \( C_e \neq \phi \) and \[ \|C\| + d(i) = 4 \]. However, since \[ \|C\| + d(i) = \|C\| + d(j) = 4 \], \( C_e \neq \phi \) from Lemma 2 and contradicts the above. Therefore, all connected components of \( G \) satisfy the following condition (C-i), (C-ii), or (C-iii).

(C-i) There are two white vertices in the connected component, and the degree for each is 3. [See Fig. 1(e).]

(C-ii) \( C_e \neq \phi \), and exactly one white vertex exists in the connected component. If such a vertex is \( i \), then \[ \|C\| + d(i) = 4 \]. [Fig. 1(a), (c).]

(C-iii) \( C_e \neq \phi \), and there are two white vertices in the connected component. If these vertices are \( i \) and \( j \), then \[ \|C\| = 1, d(i) = 3 \] and \( d(j) = 1 \). [See Fig. 1(b).]

Next, let us prove that there is only one connected component satisfying (C-i), (C-ii), or (C-iii) and that \( G \) is connected.

First, it is shown that \( G \) is connected if there exists a connected component satisfying (C-i). It is assumed that the connected component satisfying (C-i) is formed the first time when the \textbf{while} loop is executed at the \( l \)-th time in PROTOCOL\(^1\). (See the transformation second from the last in Fig. 2.) Let the two white vertices contained in this connected component be \( i \) and \( j \). Also, the connected component of \( G' \) containing the vertex \( i \) is written as \( D_i' \). Since \( D_i' \) satisfies (C-i), \[ d(i) = d(j) = 3 \]. Since \[ d^{-1}(i) \geq 2 \] and \[ d^{-1}(j) \geq 2 \] immediately before the execution of the \textbf{while} loop at the \( l \)-th time, one finds \( i, j \notin W_1 \). Also, \( i, j \notin W_1 \).

The reason is as follows. If \( i \in W_1 \), then \[ d^{-1}(i) = 3 \] from the definition of \( W_1 \). The other white vertex in the connected component \( D_i' \) in which \( i \) of \( G' \) is contained is also degree 3, and \( D_i' \) satisfies (C-i) even immediately after execution of the \textbf{while} loop in the \( (l-1) \)-th time.

This contradicts the above assumption. From the above, \( i, j \in W_1 \). From Lemma 3(a), \( W_1 = \{i, j\} \). When the \textbf{while} loop is executed in the \( l \)-th time, it is possible to assume without loss of generality that \( j \) but not \( i \) is selected as the proposer \( s \) and that the edge (\( s, i \)) is added to \( G' \).

The graph third from the last in Fig. 2 represents \( G' \) and the lowest white vertex indicates \( j \) while the highest white vertex indicates \( i \). \( D_j' \) satisfies (C-i) and \( i, j \in W_3 \). When in order to form a connected component other than \( D_j' \) satisfying (C-i) when the \textbf{while} loop is executed at the \( (l'+1) \)-th time with \( l' > 1 \), two white vertices \( v, v' \in W_1 \) not contained in \( D_j' \) need to be formed. However, from Lemma 3(b), the vertex in \( W_1 \) other than \( i \) is always selected as the proposer, and there is at most one vertex in \( W_1 \) other than \( i \). Hence, it is not possible for the condition (C-i) to be...
satisfied except by $D_i^t$. Also, when the while loop is executed at the $l$-th time, $i$, the vertex in $W_{l-1}^1$ is not selected as the proposer. Therefore, from Lemma 3(b), $|C_l^t| + d_i^{l-1}(i) = 4$. It is now assumed that there is at least one connected component not including $i$, or that satisfying (C-ii) or (C-iii), immediately before the proposer $s$ is selected for the first time by Case A3, then $C_e \neq \emptyset$ and the white vertex $j$ such that $|C_j| + d(j) = 4$ exists in the connected component. Then, there exist two white vertices $i, j$ such that $|C_i| + d(i) = |C_j| + d(j) = 4$. From Lemma 2, $C_e \neq \emptyset$ that contradicts $C_e \neq \emptyset$. Therefore, if there exists a connected component satisfying (C-i), then $G$ has only such a connected component so that $G$ is connected.

Next, let us show that $G$ is connected if there exists a connected component satisfying (C-ii) or (C-iii). If it is assumed that more than two of such components exist, $C_e \neq \emptyset$ and there exist two white vertices $i, j$ such that $|C_i| + d(i) = |C_j| + d(j) = 4$. Hence, from Lemma 2 $C_e = \emptyset$ that contradicts $C_e \neq \emptyset$.

From the above, it is concluded that there is only one connected component in $G$ so that $G$ is connected. Then, since PROTOCOL$^1$ is not completed, $|W| = 2$.

If $W = \{i, j\}$, then $c_e - |C_e| = \sum_{p=1}^{k} d_e(p) \geq d_e(i) + d_e(j), c_i + c_j \geq c_e + 8$ and $d(i) + d(j) \leq 6$. Hence,

$$|C_i| + |C_j| = c_i + c_j - d(i) - d(j) - d_e(i) - d_e(j) \geq c_e + 8 - 6 - (c_e - |C_e|) = |C_j| + 2. \quad \Box$$

**AUTHORS** (from left to right)

Takaaki Mizuki (student member) graduated from the Department of Computer Science, Tohoku University, in 1995 and is now in a doctorate course. He is engaged in research on information-theoretically secure key sharing.

Hiroki Shizuya (member) graduated from the Department of Communication Engineering, Tohoku University, in 1981 and completed a doctoral course in 1987. He then obtained a D.Eng. degree and became an assistant at the same university, where he is now a professor. He is engaged in research and education on cryptography, complexity theory, and fundamental information science. He is a member of ACM, IACR, IEEE, and SITA.

Takao Nishizeki (member) graduated from the Department of Communication Engineering, Tohoku University, in 1969, and completed a doctoral course in 1974. He then received a D.Eng. degree and became an assistant at the same university, where he is now a professor. He is engaged in research and education on algorithm, cryptography, graph theory, and VLSI layout design. He is an IEEE Fellow and an ACM Fellow, and a member of the Information Processing Society and the Japan Applied Mathematics Society.