アルゴリズム 62－10
（1998．5．20）

1ビットの鍵共有に必要十分なカード配布枚数について

水木 敬明　静谷 啓樹　西関 隆夫
東北大学大学院 情報科学研究科

概要． プレーヤーと無制限の計算能力をもつ盗聴者にカードを配布し，そのカードを用いてプレイさせ，プレーヤー全員に1ビットの共通な秘密鍵を情報理論的に安全に共有させたい．そのためには，何組かのプレーヤーの対の間に1ビットの秘密鍵を共有させ，そのようなすべてのプレーヤー対が全域木をなすようなプロトコルがあればよい．本論文では，そのようなプロトコルが存在するためのカードの配布枚数に関する必要十分条件を与える．

On dealing necessary and sufficient numbers of cards to share a one-bit key

Takaaki Mizuki　Hiroki Shizuya　Takao Nishizeki
Graduate School of Information Sciences, Tohoku University

Abstract. Using a random deal of cards to players and a computationally unlimited eavesdropper, all players wish to share a one-bit information-theoretically secure secret key. This can be done by a protocol to make several pairs of players share one-bit secret keys so that all these pairs form a spanning tree over players. In this paper we obtain a necessary and sufficient condition on the number of cards for the existence of such a protocol.

1　まえがき

k (≥ 2) 人のプレーヤー $P_1, P_2, \cdots, P_k$ および無制限の計算能力をもった盗聴者 Eve がいるとする．プレーヤー全員に1ビットの共通な秘密鍵を情報理論的に安全に共有させたい．1から d まで番号の付いた d 枚のカードの集合を C とする．最初に C のカードを $P_1, P_2, \cdots, P_k$ と Eve にランダムに配布する．各プレーヤーあるいは Eve が受け取るカードの集合を手札と呼ぶ．P_i の手札が $C_i \subseteq C$ であり，Eve の手札が $C_e \subseteq C$ であるとき，この配布を $C = (C_1, C_2, \cdots, C_k; C_e)$ と書く．ここで $C_1, C_2, \cdots, C_k, C_e$ は集合 C の分割であるとする．よって，$1 \leq i \leq k$ なる各 i に対し $c_i = |C_i|$ とし，$c_e = |C_e|$ としたとき，$d = \sum_{i=1}^{k} c_i + c_e$ である．但し，$|A|$ は集合 A の基数（要素数）を表す．$c_1, c_2, \cdots, c_k$ および c_e は，それぞれ $P_1, P_2, \cdots, P_k$ および Eve が受け取る手札の枚数であることに注意しよう．$\gamma = (c_1, c_2, \cdots, c_k; c_e)$ を配布 C の**符号数**と呼ぶ．本論文では，一般性を失うことなく $c_1 \geq c_2 \geq \cdots \geq c_k$ と仮定する．すなわち，プレーヤー $P_1, P_2, \cdots, P_k$ は手札の枚数によって降順に並んでいるとする．なお，$P_1, P_2, \cdots, P_k$ および Eve は集合 C と符号数 γ を知っているが，他人の手札は知らないとする．

図1のように，プレーヤーを点とし，1ビットの秘密鍵を情報理論的に安全に共有しているプレーヤーの対を辺として得られるグラフを**鍵共有グラフ**と呼ぶ．(グラフ理論の用語は文献[8]参照.) 図1(e)のように鍵共有グラフが全域木であるならば，任意の1人のプレーヤーが1ビット $r \in \{0,1\}$ をランダムに決め，そのプレーヤーを根とする全域木に沿って r を送ることにより k 人のプレーヤー全員は1ビットの共通な秘密鍵 r を情報理論的に安全に共有できる．但し，r

を全域木の辺 (i,j) に沿って送るとき，P_i は辺 (i,j) に対応する 1 ビットの秘密鍵 $r_{ij} \in \{0,1\}$ と r との排他的論理和 $r_{ij} \oplus r$ を取って，P_j に送るとし，それを受け取った P_j は r_{ij} との排他的論理和を取って r を得るものとする．Fischer, Paterson, Rackoff は，$k=2$ のときに鍵共有グラフが全域木，すなわち 1 本の辺からなるグラフになるような，カードの配布を用いたプロトコルを与えた [2]．また，Fischer, Wright は，このプロトコルを任意の k に一般化して，鍵共有グラフが全域木になるようなプロトコルのクラスを定式化した [3, 6]．そのクラスに含まれるプロトコルは“鍵集合プロトコル”と呼ばれる．プレーヤーが鍵集合プロトコルを実行するとき，符号数が γ であるようなどんな配布 C に対しても鍵共有グラフが必ず全域木になるならば，そのプロトコルは**符号数 γ に対して成功する**と定義されている [2, 3, 4, 5, 6]．鍵共有グラフが全域木であるならば，上述のようにして k 人のプレーヤーは全員で 1 ビットの共通な秘密鍵 r を情報理論的に安全に共有できる．

Fischer, Wright は，鍵集合プロトコルの 1 つとして“SFP プロトコル”というものを与えた．符号数全体の集合を Γ とする．但し，プレーヤーの人数 k および配布するカードの合計枚数 d はどんな値でもよいとする．Γ の分割 W, L を

$W = \{\gamma \in \Gamma \mid \gamma$ に対し成功する鍵集合プロトコルが存在する $\}$

$L = \{\gamma \in \Gamma \mid \gamma$ に対し成功する鍵集合プロトコルが存在しない $\}$

と定義しよう．SFP プロトコルは $\gamma \in W$ なるすべての γ に対し成功することが知られている [3, 6]．また彼らは，$c_k \geq 1$ かつ $c_1 + c_k \geq c_e + k$ がそのプロトコルが符号数 $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ に対し成功するための十分条件，すなわち $\gamma \in W$ であるための十分条件であることを示した．更に，$k=2$ のときにはこの条件が $\gamma \in W$ であるための必要十分条件であることを示した [3, 6]．しかし，一般の $k \geq 3$ のときの $\gamma \in W$ であるための必要十分条件は知られていなく，簡潔な必要十分条件を求めることは未解決の問題であった [3, 6]．

本論文では，$k \geq 3$ のときの $\gamma \in W$ であるための簡潔な必要十分条件を与える．符号数 γ がその条件を満足するかどうかは線形時間で容易に調べることができる．本文の条件は，与えられた次数列がグラフ実現できるための必要十分条件 [1, 7, 8, 12] と似た形をしており，本文の証明は次数列条件の証明と同様にかなり複雑である．

なお，文献 [9, 10, 11] は，全域木ではなくオイラー閉路であるような鍵共有グラフを作るプロトコルを与えており，特定の条件下においてではあるが，そのプロトコルが成功するための必要十分条件も与えている．

2 準備

本節では，Fischer, Wright が定式化した鍵集合プロトコルを説明し，このプロトコルに関する既知の結果を紹介する [2, 3, 6]．

まず，いくつかの用語を定義する．プレーヤー P_i の 1 枚のカード $x \in C_i$ とプレーヤー P_j の 1 枚のカード $y \in C_j$ からなる集合 $K = \{x, y\}$ を**鍵集合**と呼ぶ．但し，$1 \leq i, j \leq k$ かつ $i \neq j$ とする．無論，プレーヤー P_i と P_j は $x \in C_i$ かつ $y \in C_j$ なることを知っている．$x \in C_i$ であるか $x \in C_j$ であるかを Eve が 1/2 を超えた確率では識別できないとき，K は**秘密鍵集合**であると言い，P_i と P_j は 1 ビットの秘密鍵 r_{ij} を情報理論的に安全に共有できる．すなわち，$x > y$ ならば $r_{ij} = 0$，$x < y$ ならば $r_{ij} = 1$ と決めておけばよい．プロトコルにおいてカー

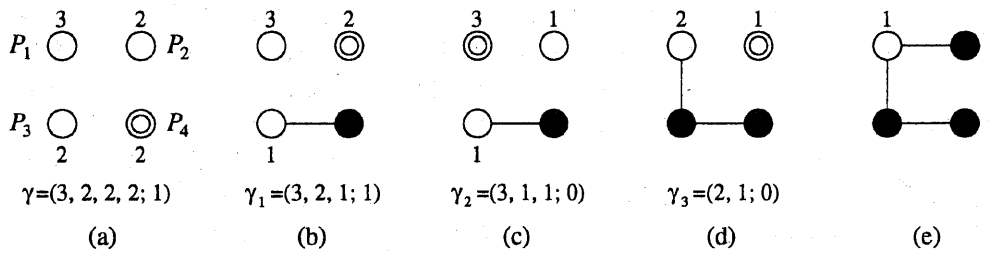

図 1: 鍵共有グラフの生成過程の例

ド x を捨てるとは，x が入っている手札 $C_1, C_2, \cdots, C_k$ または C_e から x を除去し，k 人のプレーヤー全員がカード x が手札にないということに合意することである．プレーヤーがプロトコルから抜けるとは，そのプレーヤーがそれ以降はプロトコルに参加しないことである．

鍵集合プロトコルは次の 4 つのステップからなる．以下で集合 V はプロトコルに現在残っているプレーヤーの添字番号からなるとする．よって，プロトコルの開始前には $V = \{1, 2, \cdots, k\}$ であることに注意しよう．

1. ある手順に従い，プロトコルに残っているプレーヤーの 1 人 P_s，$s \in V$，を提案者として選ぶ．

2. 提案者 P_s は自分のカード $x \in C_s$ と自分以外のカード $y \in (\bigcup_{i \in V-\{s\}} C_i) \cup C_e$ をランダムに選び，集合 $K = \{x, y\}$ を鍵集合として全員に提案する．(K は集合として提案されていることに注意しよう．)

3. カード y をもっているプレーヤー P_t が存在すれば，P_t は K を鍵集合として受け入れられることを告げる．K は秘密鍵集合であるので，P_s と P_t は 1 ビットの秘密鍵 r_{st} を情報理論的に安全に共有できる．(このとき鍵共有グラフに点 s と点 t とを結ぶ辺 (s,t) が付加される．) カード x と y を捨てる．更に，P_s と P_t のうち手札の枚数の少ない方 (等しいときは P_s) が手札を全部捨てて，プロトコルから抜ける．プロトコルから抜けたプレーヤーが P_i，$i \in \{s, t\}$，であるとき，$V := V - \{i\}$ としてステップ 1 に戻る．

4. カード y をもっているプレーヤーが存在しないとき，すなわち Eve が y をもっているならば，カード x と y を捨て，ステップ 1 に戻る．(このとき鍵共有グラフに新しい辺は付加されない．)

このステップ 1-4 をプロトコルに残っているプレーヤーがちょうど 1 人になるか，あるいはプロトコルに 2 人以上残っていてもステップ 2 を実行するだけのカードが残っていなくなるまで繰り返す．前者のとき鍵共有グラフは全域木になり，後者のときプロトコルは失敗したことになる．

鍵集合プロトコルの動きの一例を示そう．プロトコルの開始前の符号数を $\gamma = (3, 2, 2, 2; 1)$ とする．すなわち，4 人のプレーヤー P_1, P_2, P_3, P_4 と Eve がいて，P_1 の手札は 3 枚であり，

P_2, P_3 および P_4 の手札は各々2枚であり，Eve の手札は1枚であるとする．プロトコルを開始するとき図1(a)のように鍵共有グラフは4個の孤立点からなり，辺は1本もない．図1では，プロトコルに残っているプレーヤーに対応する点を白丸で描き，白丸に付けられている数字は対応するプレーヤーの手札の枚数である．まずステップ1が実行される．ここでは P_4 が提案者として選ばれたとしよう．なお，図1では，提案者のプレーヤーに対応する点は二重の白丸で描かれている．ステップ2に進み，P_4 は $x \in C_4$ かつ $y \notin C_4$ なる $K = \{x, y\}$ を提案する．たまたま $y \in C_3$ であったとしよう．このときステップ3が実行され，P_3 と P_4 は1ビットの秘密鍵 r_{34} を共有し，図1(b)のように鍵共有グラフに辺 (3,4) が付加される．カード x と y は捨てられるので，P_3 および P_4 の手札はちょうど1枚減る．このとき P_3 と P_4 の手札の枚数は等しいので，提案者であった P_4 は手札を全部捨てて，P_4 はプロトコルから抜ける．よって，このときの符号数を γ_1 とすると，$\gamma_1 = (3,2,1;1)$ である．なお，図1では，プロトコルから抜けたプレーヤーに対応する点を黒丸で描いている．ステップ3が終了したので，ステップ1に戻る．今度は提案者が P_2 であり，たまたま $y \in C_e$ であったとしよう．このときステップ4が実行され，P_2 と Eve の手札がそれぞれ1枚減る．よって，このときの符号数を γ_2 とすると，$\gamma_2 = (3,1,1;0)$ である．また，図1(c)のように鍵共有グラフに新しい辺は付加されない．ステップ4が終了したので，ステップ1に戻る．今度は提案者が P_1 であり，たまたま $y \in C_3$ であったとしよう．このとき図1(d)のように鍵共有グラフに辺 (1,3) が付加される．P_1 の手札はちょうど1枚減り，P_3 はプロトコルから抜けるので，このときの符号数を γ_3 とすると，$\gamma_3 = (2,1;0)$ である．ステップ1に戻る．今度は P_2 が提案者として選ばれたとしよう．このとき Eve の手札は空なので，必ず $y \in C_1$ であり，図1(e)のように鍵共有グラフに辺 (1,2) が付加され，鍵共有グラフは全域木になり，プロトコルは終了する．このようにプロトコルの実行中，鍵共有グラフの各連結成分にはプロトコルに残っているプレーヤー（白丸）がちょうど1人だけいることに注意しよう．

ステップ1における提案者 P_s を選ぶ手順を具体的に決めることによりプロトコルは確定する．その手順の決め方によりいろいろなプロトコルが考えられる．そのようなプロトコルを**鍵集合プロトコル**と呼ぶ．

まず $k = 2$ のときのステップ1における手順について考えよう．Fischer, Paterson, Rackoff は，P_1 と P_2 のうち手札の多い方を提案者として選ぶように手順を決めたとき，その鍵集合プロトコルは $c_2 \geq 1$ かつ $c_1 + c_2 \geq c_e + 2$ なる符号数 $\gamma = (c_1, c_2; c_e)$ に対し成功することを示した [2]．このことは次のように明らかである．もし P_1 と P_2 の手札の合計枚数が Eve の手札より2枚以上多いならば，運悪く $y \in C_e$ であることが c_e 回続いても，いずれ必ず $y \in C_t$ となり，P_1 と P_2 は秘密鍵 r_{12} を共有できる．また，$\gamma = (c_1, c_2; c_e)$ に対し成功する鍵集合プロトコルがあるならば，$c_2 \geq 1$ かつ $c_1 + c_2 \geq c_e + 2$ であることも明らかである．よって，$k = 2$ のとき次の定理1が成立する [3]．

定理 1 $k = 2$ とする．$\gamma \in W$ であるための必要十分条件は，$c_2 \geq 1$ かつ $c_1 + c_2 \geq c_e + 2$ である [3]．

次に $k \geq 3$ のときのステップ1における手順について考えよう．Fischer, Wright は，次に説明する“適切な（feasible）”プレーヤーの中で，手札の枚数が最小なものを提案者 P_s として選ぶ SFP（smallest feasible player）手順というものを与えた [3, 6]．現在の符号数を $\gamma =$

$(c_1, c_2, \cdots, c_k; c_e)$ とする．もし $c_e \geq 1$ のときに $c_i = 1$ なるプレーヤー P_i を提案者として選んでしまうと，たまたま $y \in C_e$ であるときに P_i はプロトコルに残っているにもかかわらず手札が空になり，鍵共有グラフは全域木になり得なくなってしまう．一方，$c_e = 0$ ならば，$y \in C_e$ ということはないので，$c_i = 1$ なるプレーヤー P_i を提案者として選んでもよさそうであるが，手札が1枚しかないプレーヤーが2人以上いるときに，すなわち $c_{k-1} = c_k = 1$ であるときに，P_k を提案者として選び，しかも $y \in C_{k-1}$ であると，P_{k-1} はプロトコルに残っているにもかかわらず手札が空になってしまう．$c_1 \geq c_2 \geq \cdots \geq c_k$ と仮定していたことに注意しよう．よって，提案者として次の“適切な”プレーヤーを選ばなければならない．このようにして，次の (1) あるいは (2) が成立するとき，プレーヤー P_i は**適切**であると言うことにする．

(1) $c_i \geq 2$.

(2) $c_i = 1$．但し，$i = k$，$c_e = 0$ かつ $c_{k-1} \geq 2$.

プロトコルに現在残っているプレーヤー全員の手札が空でなく（すなわち $c_k \geq 1$ であり），提案者 P_s が適切なプレーヤーであるならば，ステップ 1–4 の繰返しループを次に実行するときにプロトコルに残っているプレーヤー全員の手札が空でないことに注意しよう．

適切なプレーヤーで手札の枚数が最小なプレーヤーを P_i とし，そのようなプレーヤーが複数いる場合は添字番号が最大なプレーヤーを P_i とし，$f(\gamma) = i$ と書くことにする．但し，適切なプレーヤーが存在しないときは $f(\gamma) = 0$ と書くことにする．例えば，$\gamma = (4,3,2,2,1,1;3)$ ならば，$f(\gamma) = 4$ である．$\gamma = (4,4,3,3,1;0)$ ならば，$c_k = 1$，$c_{k-1} \geq 2$ かつ $c_e = 0$ なので，$f(\gamma) = k = 5$ である．$\gamma = (1,1,1;2)$ ならば，適切なプレーヤーがいないので，$f(\gamma) = 0$ である．以後，文脈から明らかなときには $f(\gamma)$ を単に f と書くことがある．

f の定義により次の補題が直ちに成立することに注意しよう．補題 1(a) は $\gamma \in W$ であるための自明な必要条件を与えている．なお，以下本論文では $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ とする．

補題 1 次の (a) および (b) が成立する．

(a) $k \geq 3$ かつ $\gamma \in W$ ならば，$c_k \geq 1$ かつ $f(\gamma) \geq 1$ である [3].

(b) $c_k \geq 1$ ならば，$f(\gamma) + 1 \leq i \leq k$ なるすべての $i \in V$ に対し $c_i = 1$ である．

SFP 手順は次のように提案者 P_s の添字番号 $s \in V$ を選ぶ．

$$s = \begin{cases} f(\gamma) & (1 \leq f(\gamma) \leq k \text{ のとき}) \\ 1 & (f(\gamma) = 0 \text{ のとき}) \end{cases}$$

なお，SFP 手順は $k = 2$ のときも f を同様に定義して s を選んでいる．この手順によって得られる鍵集合プロトコルを **SFP プロトコル**と言う．このプロトコルに関し次の定理が成立することが知られている [3, 6].

定理 2 符号数 $\gamma \in \Gamma$ に対し成功する鍵集合プロトコルが存在する，すなわち $\gamma \in W$ であるための必要十分条件は，γ に対し SFP プロトコルが成功することである [3, 6].

また，$\gamma \in W$ であるための十分条件として次の補題 2 が証明されている [3, 6].

補題 2 $c_k \geq 1$ かつ $c_1 + c_k \geq c_e + k$ ならば，$\gamma \in W$ である [3, 6].

上の十分条件は $\gamma \in W$ であるための必要条件とは限らない．例えば $\gamma = (3,3,2,1;1)$ は補題 2 の条件を満足しないが，SFP プロトコルはこの γ に対して成功するので，$\gamma \in W$ である [3, 6]．本論文では，任意の $k \geq 3$ に対して $\gamma \in W$ であるための簡潔な必要十分条件を与える．後で示すように $\gamma = (3,3,2,1;1)$ はその必要十分条件を満足する．

3 必要十分条件

$k = 3$ のときは，次の定理 3 に示すように，補題 2 の $\gamma \in W$ であるための十分条件が実は必要十分条件である．定理 3 の証明は紙面の都合上割愛する．

定理 3 $k = 3$ とする．$\gamma \in W$ であるための必要十分条件は，$c_3 \geq 1$ かつ $c_1 + c_3 \geq c_e + 3$ である．

$k \geq 4$ のときの $\gamma \in W$ であるための必要十分条件は次の定理 4 のとおりである．なお，$B = \{i \in V \mid c_i = 2\}$ とし，$b = \lfloor |B|/2 \rfloor$ としている．補題 1(a) により $c_k \geq 1$ かつ $f \geq 1$ は $\gamma \in W$ であるための自明な必要条件であることに注意しよう．定理 4 の証明は紙面の都合上割愛する．

定理 4 $k \geq 4$，$c_k \geq 1$，かつ $f \geq 1$ とする．このとき $\gamma \in W$ であるための必要十分条件は

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

である．但し，

$$\bar{f} = f - \delta$$

$$\tilde{f} = \bar{f} - 2\epsilon$$

$$h = c_e - c_k + k - \bar{f}$$

$$h^+ = h + \epsilon$$

$$\delta = \begin{cases} 0 & (f = 1 \text{ のとき}) \\ 1 & (2 \leq f \leq k-1 \text{ のとき}) \\ 2 & (f = k \text{ かつ } c_{k-1} \geq c_k + 1 \text{ のとき}) \\ 3 & (f = k \text{ かつ } c_{k-1} = c_k \text{ のとき}) \end{cases}$$

$$\epsilon = \begin{cases} \max\{\min\{c_2 - h, b\}, 0\} \\ \qquad (5 \leq f \leq k-1 \text{ のとき}) \\ \max\{\min\{c_2 - h, b-1\}, 0\} \\ \qquad (5 \leq f = k \text{ かつ } c_e \geq 1 \text{ のとき}) \\ 0 \qquad (\text{その他のとき}) \end{cases}$$

である．

なお，$c_1 \geq c_2 \geq \cdots \geq c_k$ なので，明らかに式(1)は

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

と同値である．

前に述べたように符号数 $\gamma = (3,3,2,1;1)$ に対し SFP プロトコルは成功するが，γ は補題2の十分条件を満足しない [3, 6]．このγに対し，$2 \leq f = 3 = k-1$ なので，$\delta = 1$ である．また，$b = 0$ なので，$\epsilon = 0$ である．よって，$\tilde{f} = \bar{f} = f - \delta = 2$ かつ $h^+ = h = 1-1+4-2 = 2$ である．従って，$\sum_{i=1}^{\tilde{f}} \max\{c_i - h^+, 0\} = (3-2)+(3-2) = 2 = \tilde{f}$ である．このように $\gamma \in W$ は定理4の必要十分条件を満足する．

定理1，3および4から次の系が得られる．この系は，すべてのプレーヤーが同じ枚数の手札を受け取るという自然な仮定の下での $\gamma \in W$ であるための必要十分条件を与えている．なお，証明の詳細は紙面の都合上割愛する．

系 1 $k \geq 2$ かつ $c_1 = c_2 = \cdots = c_k$ とする．このとき $\gamma \in W$ であるための必要十分条件は

$$c_1 \geq \begin{cases} c_e/2+1 & (k=2 \text{ のとき}) \\ c_e/2+3/2 & (k=3 \text{ のとき}) \\ c_e/2+2 & (k \geq 4 \text{ のとき}) \end{cases}$$

である．

4 むすび

本論文では，成功する鍵集合プロトコルが存在するための符号数 $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ に関する簡潔な必要十分条件を与えた．言い換えると，集合 W および L の完全な特徴付けを行った．

SFP プロトコルはすべての $\gamma \in W$ に対し成功するので（定理2），ある符号数 γ が $\gamma \in W$ であるかどうかは，SFP プロトコルを実際にシミュレーションすることにより決定することも可能である．しかし，このときすべてのアドバーサリーに対しシミュレーションする必要があり，そのシミュレーションにかかる計算時間は k に関する指数関数であり，現実的ではない．無論，本論文で与えた必要十分条件を使えば，$\gamma \in W$ であるかどうかは $O(k)$ 時間で直ちに決定できる．

参考文献

[1] T. Asano, "An $O(n \log\log n)$ time algorithm for constructing a graph of maximum connectivity with prescribed degrees," J. Comput. and Syst. Sci., vol. 51, pp. 503–510, 1995.

[2] M. J. Fischer, M. S. Paterson and C. Rackoff, "Secret bit transmission using a random deal of cards," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 2, pp. 173–181, 1991.

[3] M. J. Fischer and R. N. Wright, "An application of game-theoretic techniques to cryptography," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 13, pp. 99–118, 1993.

[4] M. J. Fischer and R. N. Wright, "An efficient protocol for unconditionally secure secret key exchange," Proceedings of the 4th Annual Symposium on Discrete Algorithms, pp. 475–483, 1993.

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

[6] M. J. Fischer and R. N. Wright, "Multiparty secret key exchange using a random deal of cards," Proc. Crypto '91, Lecture Notes in Computer Science, vol. 576, pp. 141–155, 1992.

[7] S. L. Hakimi, "On realizability of a set of integers as degrees of the vertices of a linear graph. I," J. SIAM Appl. Math., vol. 10, no. 3, pp. 496–506, 1962.

[8] F. Harary, "Graph Theory," Addison-Wesley, Reading, Mass., 1969.

[9] 水木敬明, 静谷啓樹, 西関隆夫, "カードの配布によるオイラー閉路状鍵共有," 信学論 (A), vol. J81-A, no. 4, 1998.

[10] 水木敬明, 静谷啓樹, 西関隆夫, "最小枚数のカードの配布によるオイラー閉路状鍵共有," 信学論 (A), vol. J81-A, no. 4, 1998.

[11] 水木敬明, 静谷啓樹, 西関隆夫, "最短なオイラー閉路状鍵共有," 信学論 (A), vol. J81-A, no. 4, 1998.

[12] E. F. Schmeichel and S. L. Hakimi, "On planar graphical degree sequences," SIAM J. Appl. Math., vol. 32, no. 3, pp. 598–609, 1977.