Efficient Generation of a Card-based Uniformly Distributed Random Derangement[⋆]

Soma Murata[1], Daiki Miyahara[1,3], Takaaki Mizuki[2], and Hideaki Sone[2]

[1] Graduate School of Information Sciences, Tohoku University
6–3–09 Aramaki-Aza-Aoba, Aoba-ku, Sendai 980–8578, Japan
[2] Cyberscience Center, Tohoku University
6–3 Aramaki-Aza-Aoba, Aoba-ku, Sendai 980–8578, Japan
[3] National Institute of Advanced Industrial Science and Technology
2–3–26, Aomi, Koto-ku, Tokyo 135-0064, Japan

Abstract. Consider a situation, known as Secret Santa, where n players wish to exchange gifts such that each player receives exactly one gift and no one receives a gift from oneself. Each player only wants to know in advance for whom he/she should purchase a gift. That is, the players want to generate a hidden uniformly distributed random derangement. (Note that a permutation without any fixed points is called a derangement.) To solve this problem, in 2015, Ishikawa *et al.* proposed a simple protocol with a deck of physical cards. In their protocol, players first prepare n piles of cards, each of which corresponds to a player, and shuffle the piles. Subsequently, the players verify whether the resulting piles have fixed points somehow: If there is no fixed point, the piles serve as a hidden random derangement; otherwise, the players restart the shuffle process. Such a restart occurs with a probability of approximately 0.6. In this study, we consider how to decrease the probability of the need to restart the shuffle based on the aforementioned protocol. Specifically, we prepare more piles of cards than the number n of players. This potentially helps us avoid repeating the shuffle, because we can remove fixed points even if they arise (as long as the number of remaining piles is at least n). Accordingly, we propose an efficient protocol that generates a uniformly distributed random derangement. The probability of the need to restart the shuffle can be reduced to approximately 0.1.

Keywords: Card-based cryptography · Derangement (Permutation without fixed points) · Exchange of gifts · Secret Santa

1 Introduction

Let $n\,(\geq 3)$ be a natural number, and consider a situation, known as Secret Santa, where n players $P_1, P_2, \ldots, P_n$ wish to exchange gifts such that each player receives exactly one gift and no one receives a gift from oneself. Every player wants to

[⋆] This paper appears in Proceedings of WALCOM 2021. The final authenticated version is available online at https://doi.org/10.1007/978-3-030-68211-8_7.

know in advance for whom he/she should purchase a gift. Mathematically, an assignment of a gift exchange can be regarded as a permutation, *i.e.*, an element in S_n, which is the symmetric group of degree n; in this context, a permutation $\pi \in S_n$ indicates that a player P_i for every i, $1 \leq i \leq n$, will purchase a gift for $P_{\pi(i)}$. Such a permutation $\pi \in S_n$ must not have any fixed points, *i.e.*, $\pi(i) \neq i$ for every i, $1 \leq i \leq n$, to prevent each player from receiving a gift from himself/herself. Note that a permutation is called a *derangement* if it has no fixed point. Therefore, the players want to generate a uniformly distributed random derangement. Furthermore, to make the exchange fun, it is necessary for each player P_i to know only the value of $\pi(i)$. Thus, we aim to generate a "hidden" uniformly distributed random derangement.

Physical cryptographic protocols are suitable for resolving this type of problem because they can be easily executed by using familiar physical tools without relying on complicated programs or computers.

1.1 Background

The problem of generating a hidden derangement was first studied by Crépeau and Kilian [1] in 1993. Since then, several solutions with physical tools have been proposed. (Refer to [17] for the non-physical solutions.) As practical protocols, Heather *et al.* [6] proposed a protocol with envelopes and fill-in-the-blank cards in 2014; Ibaraki *et al.* [7] proposed a protocol with two sequences of cards representing player IDs and gift IDs in 2016. The common feature of these two practical protocols is that the generated derangement is not uniformly distributed; it always includes a cycle of a specific length.

Let us focus on generating a *uniformly distributed* random derangement. A protocol that generates a uniformly distributed random derangement was proposed by Crépeau and Kilian [1] with a four-colored deck of $4n^2$ cards. Ishikawa, Chida, and Mizuki [8] subsequently improved the aforementioned protocol by introducing a *pile-scramble shuffle* that "scrambles" piles of cards. Their improved protocol, which we refer to as the *ICM protocol* hereinafter, uses a two-colored deck of n^2 cards. It is described briefly as follows. (Further details will be presented in Section 2.5.)

1. Prepare n piles of cards, each of which corresponds to a player.
2. Apply a pile-scramble shuffle to the n piles to permute them randomly.
3. Check whether there are fixed points in the n piles somehow.
   - If there is at least one fixed point, restart the shuffle process, *i.e.*, go back to Step 2.
   - If there is no fixed point, the piles serve as a hidden random derangement.

Thus, the ICM protocol is not guaranteed to terminate within a finite runtime, because it restarts the shuffle process whenever a fixed point arises. The probability that at least one fixed point appears in Step 3 is $1 - \sum_{k=0}^{n} (-1)^k/k! \approx 1 - 1/e \approx 0.63$ (where e is the base of the natural logarithm), which will be described later in Section 2.5.

In 2018, Hashimoto *et al.* [4] proposed the first finite-runtime protocol for generating a uniformly distributed random derangement by using the properties of the types of permutations. While their proposed protocol is innovative, its feasibility to be performed by humans has not been studied, as it requires a shuffle operation with a nonuniform probability distribution.

1.2 Contributions

In this study, we also deal with generating a uniformly distributed random derangement and propose a new card-based protocol by improving the ICM protocol. Specifically, we devise a method to reduce the probability of the need to restart in the ICM protocol. Recall that, after one shuffle is applied in Step 2, the ICM protocol returns to Step 2 with a probability of approximately 0.6. In card-based protocols, it is preferable to avoid repeating shuffle operations because players manipulate the deck of physical cards by hand. Here, we prepare more piles of cards than the number n of players, *i.e.*, we prepare $n + t$ piles for some $t \geq 1$. This potentially helps us remove fixed points (if they arise); hence, we can reduce the probability of the need to restart the shuffle. In the same manner as the ICM protocol, the proposed protocol generates a hidden uniformly distributed random derangement. The probability of the need to restart the shuffle is reduced by increasing the number t of additional piles. Specifically, the probability of the need for such a restart can be reduced to approximately 0.1 by setting $t = 3$.

The remainder of this paper is organized as follows. In Section 2, we introduce the notions of card-based cryptography, the properties of permutations, and the ICM protocol. In Section 3, we present our protocol. In Section 4, we demonstrate the relationship between the number t of additional piles and the probability of the need to restart the shuffle; we illustrate how the probability can be reduced by increasing the number t.

1.3 Related Works

Card-based cryptography involves performing cryptographic tasks, such as secure multi-party computations, using a deck of physical cards; since den Boer [2] first proposed a protocol for a secure computation of the AND function with five cards, many elementary computations have been devised (e.g., [11, 14]). For more complex tasks, millionaire protocols [9, 12, 13] that securely compare the properties of two players, a secure grouping protocol [5] that securely divides players into groups, and zero-knowledge proof protocols for pencil puzzles [3, 10, 15, 16, 18] were also proposed.

2 Preliminaries

In this section, we introduce the notions of cards and the pile-scramble shuffle used in this study, and the properties of permutations. Furthermore, we introduce the ICM protocol proposed by Ishikawa *et al.* [8].

2.1 Cards

In this study, we use a two-colored (black $\boxed{\clubsuit}$ and red $\boxed{\heartsuit}$) deck of cards. The rear sides of the cards have the same pattern $\boxed{?}$. The cards of the same color are indistinguishable. Using n cards consisting of $n-1$ black cards and one red card, we represent a natural number i, $1 \leq i \leq n$, using a sequence such that the i-th card is red and the remaining cards are black:

$$\overset{1}{\boxed{\clubsuit}}\,\overset{2}{\boxed{\clubsuit}}\cdots\overset{i}{\boxed{\heartsuit}}\cdots\overset{n-1}{\boxed{\clubsuit}}\,\overset{n}{\boxed{\clubsuit}}.$$

If a sequence of face-down cards represents a natural number i according to the above encoding rule, we refer to it as a *commitment to* i and express it as follows:

$$\underbrace{\overset{1}{\boxed{?}}\,\overset{2}{\boxed{?}}\cdots\overset{n}{\boxed{?}}}_{i}.$$

2.2 Pile-scramble Shuffle

A *pile-scramble shuffle* is a shuffle operation proposed by Ishikawa *et al.* [8]. Let $(\mathsf{pile}_1, \mathsf{pile}_2, \ldots, \mathsf{pile}_n)$ be a sequence of n piles, each consisting of the same number of cards. By applying a pile-scramble shuffle to the sequence, we obtain a sequence of piles $(\mathsf{pile}_{\pi^{-1}(1)}, \mathsf{pile}_{\pi^{-1}(2)}, \ldots, \mathsf{pile}_{\pi^{-1}(n)})$ where $\pi \in S_n$ is a uniformly distributed random permutation. Humans can easily implement a pile-scramble shuffle by using rubber bands or envelopes.

2.3 Properties of Permutations

An arbitrary permutation can be expressed as a product of disjoint cyclic permutations. For example, the permutation

$$\tau = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,5\,6\,4\,2\,7\,1 \end{pmatrix}$$

can be expressed as the product of three disjoint cyclic permutations $\tau_1 = (4), \tau_2 = (25), \tau_3 = (1367)$: $\tau = \tau_1\tau_2\tau_3 = (4)(25)(1367)$. The lengths of the cyclic permutations τ_1, τ_2, and τ_3 are 1, 2, and 4, respectively. A cycle of length one is a fixed point.

Let d_n denote the number of all derangements in S_n; then, d_n can be expressed as follows:

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

for $n \geq 2$, and $d_1 = 0$. The number of permutations (in S_n) having exactly f fixed points is ${}_n\mathrm{C}_f \cdot d_{n-f}$, where we define $d_0 = 1$.

2.4 Expression of Permutation Using Cards

Hereinafter, we use the expression $[1:m]$ to represent the set $\{1,2,\ldots,m\}$ for a positive integer m. Remember that a commitment to $i \in [1:n]$ consists of one red card at the i-th position and $n-1$ black cards at the remaining positions. In this paper, we represent a *hidden permutation* $\pi \in S_n$ using a sequence of n distinct commitments $(X_1,\ldots,X_n)$ such that

$$\begin{aligned} X_1 &: \underbrace{\boxed{?}\,\boxed{?}\cdots\boxed{?}}_{\pi(1)} \\ &\;\vdots \\ X_n &: \underbrace{\boxed{?}\,\boxed{?}\cdots\boxed{?}}_{\pi(n)}\,. \end{aligned} \tag{1}$$

Given a hidden permutation $\pi \in S_n$ in the above form (1), to check whether an element $i \in \pi$ is a fixed point, it suffices to reveal the i-th card of the i-th commitment: if the revealed card is red, the element is a fixed point, *i.e.*, $\pi(i) = i$.

2.5 The Existing Protocol

We introduce the ICM protocol [8], which generates a uniformly distributed random derangement using n^2 cards with the pile-scramble shuffle, as follows.

1. Arrange n distinct commitments corresponding to the identity permutation (in S_n) according to the form (1). That is, all the cards on the diagonal are red $\heartsuit$ and the remaining cards are black $\clubsuit$.
2. Apply a pile-scramble shuffle to the sequence of n commitments. Note that the resulting n commitments correspond to a certain permutation $\pi \in S_n$; moreover, π is uniformly randomly distributed.
3. Turn over the n cards on the diagonal to check whether there are fixed points in the permutation π.
   - If at least one red card appears, return to Step 2.
   - If all the revealed cards are black, π has no fixed point; hence, π is a uniformly distributed random derangement.

After n players $P_1, P_2, \ldots, P_n$ obtain a hidden derangement (consisting of n commitments) through this protocol, Secret Santa can be implemented by P_i receiving the i-th commitment; he/she reveals the commitment privately to confirm the value of $\pi(i)$, and then purchases a gift for $P_{\pi(i)}$.

Whenever a generated permutation π is not a derangement, the protocol returns to Step 2. The probability that a generated permutation uniformly randomly chosen from S_n is a derangement is $d_n/n! = \sum_{k=0}^{n}(-1)^k/k!$. As $\lim_{n\to\infty}\sum_{k=0}^{n}(-1)^k/k! = 1/e$, the probability of the need to restart the shuffle in the ICM protocol is approximately $1 - 1/e \approx 0.63$.

Note that Ishikawa *et.al.* [8] also showed that the number of required cards can be reduced from n^2 to $2n\lceil\log_2 n\rceil + 6$ by arranging each pile of cards corresponding to a player based on a binary number.

3 Proposed Protocol for Generating a Derangement

In this section, we improve the ICM protocol [8] described in Section 2.5 so that the probability of the need to restart the shuffle is decreased. Here, we prepare more piles of cards than the number n of players.

3.1 Overview of the Proposed Protocol

Let us provide an overview of the proposed protocol.

We first prepare $n+t$ commitments instead of n commitments, and apply a pile-scramble shuffle to them. These t additional commitments provide a buffer that absorbs any fixed points that may arise. By revealing the cards on the diagonal, we determine all the fixed points; let f be their number. If the fixed points are too many to be absorbed, *i.e.*, $f > t$, restart the shuffle. If $f \leq t$, we apply the "fixed-point removal" operation (described in Section 3.2), resulting in $n+t-f$ commitments. Subsequently, we apply the "reduction" operation (described in Section 3.2) to eliminate the $t-f$ extra commitments.

We explain both the fixed-point removal and reduction operations in the following subsection.

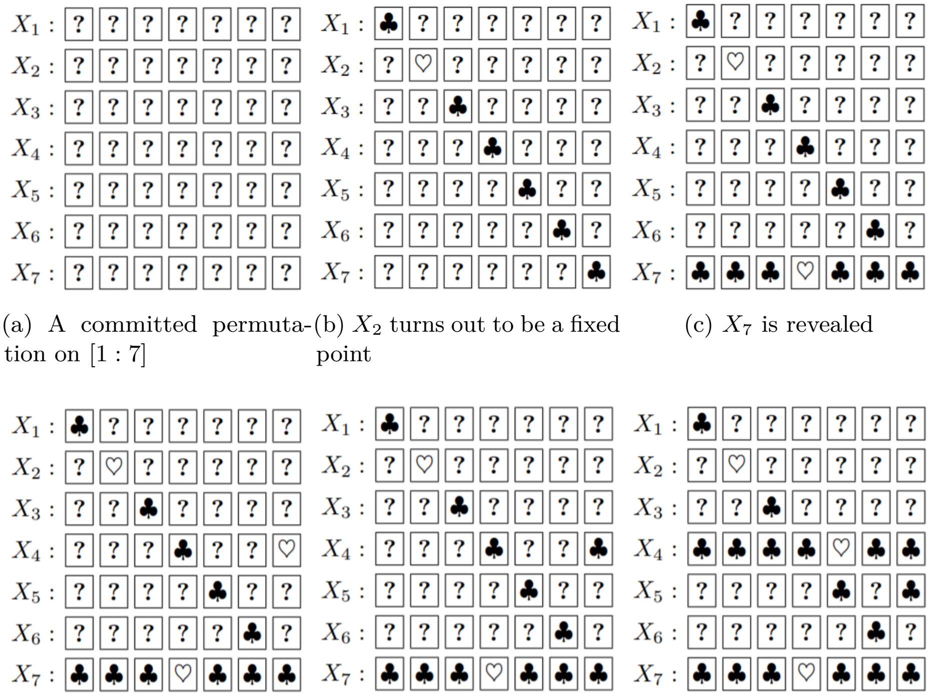
3.2 Definitions of the Two Operations

Suppose that we execute Steps 1 and 2 in the ICM protocol (shown in Section 2.5), starting with the identity permutation of degree $n+t$ (instead of degree n). Then, we obtain a sequence of $n+t$ commitments corresponding to a uniformly distributed random permutation in S_{n+t}: we refer to such a sequence of commitments as a *committed permutation on* $[1:n+t]$.

Fixed-point Removal Operation. For the above committed permutation on $[1:n+t]$, let us reveal all the $n+t$ cards on the diagonal as in Step 3 of the ICM protocol. Subsequently, we determine all the fixed points in the permutation. Let I_{FP} be the set of indices of these fixed points. Ignoring the commitments corresponding to the fixed points, namely, the commitments whose positions are in I_{FP}, the sequence of the remaining commitments corresponds to a derangement uniformly distributed on $[1:n+t]\backslash I_{\mathrm{FP}}$: we refer to this sequence as a *committed derangement on* $[1:n+t]\backslash I_{\mathrm{FP}}$.

Through the fixed-point removal operation, a committed permutation of degree $n+t$ is transformed into a committed derangement on $[1:n+t]\backslash I_{\mathrm{FP}}$ of degree $n+t-|I_{\mathrm{FP}}|$.

Consider the case of $(n,t)=(4,3)$ as an example. Let us transform a committed permutation shown in Figure 1a. Then, after the fixed-point removal operation is applied to the committed permutation of degree seven, all the seven cards on the diagonal are revealed as shown in Figure 1b. In this example, the commitment X_2 is a fixed point; hence, we have $I_{\mathrm{FP}}=\{2\}$ and the sequence of the remaining six commitments $(X_1, X_3, X_4, X_5, X_6, X_7)$ is a committed derangement on $[1:7]\backslash\{2\}=\{1,3,4,5,6,7\}$ of degree six.



(a) A committed permutation on $[1:7]$ (b) X_2 turns out to be a fixed point (c) X_7 is revealed

(d) Case 1: The seventh card of X_4 is red (e) Case 2: The seventh card of X_4 is black (f) X_4 is revealed and the seventh card of X_5 is turned over

Fig. 1: Example of execution of the proposed protocol

As $n = 4$, the current committed derangement (depicted in Figure 1b) has two "extra" commitments, *i.e.*, we aim to reduce the degree by two. To this end, we turn over the last commitment, *i.e.*, the seventh commitment X_7. Assume that the revealed value of X_7 is 4 as illustrated in Figure 1c, indicating a mapping $7 \mapsto 4$, which we refer to as a *bypass*. That is, let us ignore the seventh revealed commitment and regard mapping to 7 as virtually mapping to 4 (via the bypass $7 \mapsto 4$). Consequently, we obtain a committed permutation on $\{1, 3, 4, 5, 6\}$ of degree five, which has been reduced by one.

We now have the committed permutation of degree five (as in Figure 1c). It may not be a derangement because if $4 \mapsto 7$, it (virtually) has a fixed point (due to the cycle $7 \mapsto 4 \mapsto 7$). Therefore, we turn over the seventh card of the fourth commitment X_4 to check whether it is a fixed point.

- If a red card appears as shown in Figure 1d, we have the cycle $7 \mapsto 4 \mapsto 7$, indicating a fixed point. Let I_{cycle} denote the set of all the indices of the cycle, *i.e.*, $I_{\text{cycle}} = \{4, 7\}$. Ignoring this cycle, namely, the commitments X_4 and X_7, the sequence of the remaining commitments (X_1, X_3, X_5, X_6) becomes

a committed derangement uniformly distributed on $[1:7]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}}) = \{1,3,5,6\}$. Thus, we obtain a committed derangement of degree four, as desired. Note that, in this case, the degree decreases by two.
- If a black card appears as shown in Figure 1e, there is no fixed point; hence, this committed permutation $(X_1, X_3, X_4, X_5, X_6)$ is a uniformly distributed derangement of degree five under the bypass $7 \mapsto 4$. In this case, the degree decreases by one.

In the above example, if a black card appears, we obtain a derangement of degree five; hence, we need to reduce the degree further (because $n = 4$). Therefore, we are expected to reveal another commitment (in this case, we reveal the fourth commitment X_4 because of the bypass $7 \mapsto 4$, as illustrated in Figure 1f; we will revisit it later).

In general, we define the reduction operation for a committed derangement on $[1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}} \cup I_{\mathrm{BP}})$ as follows, where I_{FP} is the set of fixed points, I_{cycle} is the set of indices in cycles, there is a bypass $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_{\ell-1} \mapsto i_\ell$, and $I_{\mathrm{BP}} = \{i_1, i_2, \ldots, i_{\ell-1}\}$.

Reduction Operation. If $I_{\mathrm{BP}} \neq \phi$, turn over the i_ℓ-th commitment X_{i_ℓ} (which is the end of the bypass). If $I_{\mathrm{BP}} = \phi$, turn over the last of the remaining commitments, *i.e.*, the $(\max([1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}})))$-th commitment; in this case, we set $i_\ell = i_1 = \max([1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}}))$ for the sake of convenience. In either case, let $i_{\ell+1}$ be the value of the turned over commitment. Then, turn over the i_1-th card of the $i_{\ell+1}$-th commitment $X_{i_{\ell+1}}$.

- If a red card appears, this committed permutation has the cycle $i_1 \mapsto \cdots \mapsto i_{\ell+1} \mapsto i_1$. The indices $i_1, \ldots, i_{\ell+1}$ of this cycle, namely, all the elements in set $I_{\mathrm{BP}} \cup \{i_\ell, i_{\ell+1}\}$, are added to the set I_{cycle}, and the bypass disappears; hence, we set $I_{\mathrm{BP}} = \phi$. Ignoring all the commitments whose positions are in $I_{\mathrm{FP}} \cup I_{\mathrm{cycle}}$, the sequence of the remaining commitments becomes a committed derangement on $[1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}})$. Note that the degree of the committed derangement has been reduced by two (because of ignoring X_{i_ℓ} and $X_{i_{\ell+1}}$).
- If a black card appears, the sequence of the remaining commitments is a committed derangement uniformly distributed on $[1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}} \cup I_{\mathrm{BP}})$ under the bypass $i_1 \mapsto \cdots \mapsto i_\ell \mapsto i_{\ell+1}$ (where $I_{\mathrm{BP}} = \{i_1, i_2, \ldots, i_\ell\}$). In this case, the degree of the committed derangement has been reduced by one.

3.3 Description of the Proposed Protocol

We describe the proposed protocol using the two aforementioned operations. This protocol uses $n+t$ piles (whereas the ICM protocol [8] uses n piles), as follows.

1. Arrange $n+t$ distinct commitments corresponding to the identity permutation (in S_{n+t}) according to the form (1). That is, all the $n+t$ cards on the diagonal are red ♡ and the remaining cards are black ♣.

2. Apply a pile-scramble shuffle to the sequence of $n+t$ commitments, and the resulting $n+t$ commitments become a committed permutation on $[1:n+t]$.
3. Apply the fixed-point removal operation described in Section 3.2 to the committed permutation obtained in Step 2. Let I_{FP} be the set of fixed points and $f = |I_{\mathrm{FP}}|$. We obtain a committed derangement on $[1:n+t]\backslash I_{\mathrm{FP}}$ of degree $n+t-f$.
   - In the case of $f > t$, the committed derangement is insufficient because its degree is less than the number n of players. Therefore, turn all the cards face-down, and return to Step 2.
   - In the case of $f = t$, the degree of the committed derangement is n, as desired. Therefore, proceed to Step 5.
   - In the case of $f < t$, proceed to Step 4.
4. Repeatedly apply the reduction operation described in Section 3.2 to the committed derangement on $[1:n+t]\backslash I_{\mathrm{FP}}$ obtained in Step 3, until its degree becomes n or less. Recall that each application of the reduction operation reduces the degree by one or two.
   - If a committed derangement of degree $n-1$ is obtained, turn all the cards face-down, and return to Step 2.
   - If a committed derangement of degree n is obtained, proceed to Step 5.
5. We have a committed derangement of degree n on $[1:n+t]\backslash(I_{\mathrm{FP}} \cup I_{\mathrm{cycle}} \cup I_{\mathrm{BP}})$, as desired.

After we obtain a committed derangement in Step 5, we renumber the players based on the remaining n commitments. If there is a bypass $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_\ell$, a player who turns over the commitment to i_1 should purchase a gift for the player corresponding to i_ℓ. For example, consider the committed derangement illustrated in Figure 1f, which is obtained from Figure 1e by revealing X_4 and the seventh card of X_5. We renumber the four players such that $P_1 = P'_1$, $P_2 = P'_3$, $P_3 = P'_5$, and $P_4 = P'_6$, and make P'_1, P'_3, P'_5, and P'_6 receive commitments X_1, X_3, X_5, and X_6, respectively. Each player secretly turns over the assigned commitment to know for whom he/she should purchase a gift. Because of the bypass $7 \mapsto 4 \mapsto 5$, the player who reveals the commitment to 7 should purchase a gift for P'_5.

Thus, the proposed protocol generates a committed derangement. As there is a trade-off between the number t of additional piles and the probability of returning to Step 2, we comprehensively analyze the probability of the need to restart the shuffle in the following section.

4 Probability of the Need to Restart the Shuffle

In the proposed protocol presented in the previous section, the probability of the need to restart the shuffle depends on the number $t\,(\geq 1)$ of additional piles. In this section, we analyze this probability. Recall that the restart occurs when either more than t fixed points appear in Step 3 or a derangement of degree $n-1$ is obtained in Step 4.

Let f be the number of fixed points determined in Step 2. A restart from Step 3 occurs if $t+1 \leq f \leq n+t$. As the probability that a uniformly distributed random permutation in S_{n+t} has exactly f fixed points is ${}_{n+t}\mathrm{C}_f \cdot d_{n+t-f}/(n+t)!$, the following equation holds:

$$\Pr[\text{Restart from Step 3}] = \sum_{f=t+1}^{n+t} \frac{{}_{n+t}\mathrm{C}_f \cdot d_{n+t-f}}{(n+t)!}. \tag{2}$$

Next, we consider a restart from Step 4. Suppose that we have a committed derangement of degree $n+x$ for a non-negative integer x. Let $\epsilon(n,x)$ be the probability that repeated applications of the reduction operation result in a committed derangement of degree $n-1$ and we return to Step 2. Each application of the reduction operation to the committed derangement of degree $n+x$ produces a committed derangement of degree either $n+x-2$ or $n+x-1$. The former occurs when the commitment to be revealed is included in a cycle of length two; therefore, its occurrence probability is $(n+x-1)d_{n+x-2}/d_{n+x}$. The latter occurs with a probability of $1-(n+x-1)d_{n+x-2}/d_{n+x}$. Thus, $\epsilon(n,x)$ can be expressed recursively as follows:

$$\begin{aligned}\epsilon(n,x) = &\left(1 - \frac{(n+x-1)d_{n+x-2}}{d_{n+x}}\right) \cdot \epsilon(n,x-1)\\ &+ \frac{(n+x-1)d_{n+x-2}}{d_{n+x}} \cdot \epsilon(n,x-2),\end{aligned}$$

where $\epsilon(n,0) = 0$ and $\epsilon(n,1) = n \cdot d_{n-1}/d_{n+1}$. As Step 4 occurs when f lies between 0 and $t-1$ with a probability of ${}_{n+t}\mathrm{C}_f \cdot d_{n+t-f}/(n+t)!$, the following equation holds:

$$\Pr[\text{Restart from Step 4}] = \sum_{f=0}^{t-1} \frac{{}_{n+t}\mathrm{C}_f \cdot d_{n+t-f}}{(n+t)!} \cdot \epsilon(n,t-f). \tag{3}$$

The probability of the need to return to Step 2 for the entire proposed protocol, denoted by $\Pr[\text{Restart}^{(n,t)}]$, is the sum of Eqs. (2) and (3). Figure 2 shows the relationship between $t\,(\leq 10)$ and the probability $\Pr[\text{Restart}^{(n,t)}]$ for the number of players from $n=3$ to $n=20$. $\Pr[\text{Restart}^{(n,0)}]$ is the same as the probability for the ICM protocol. The proposed protocol improves significantly as t increases. If we prepare t additional piles, the number of required cards increases by $t(t+2n)$; considering an unnecessarily large t is not realistic. Even if we set t to a small value such as 2 or 3, the probability can be reduced to approximately 0.1 compared with that of the ICM protocol (approximately 0.6).

5 Conclusion

In this paper, we proposed a new efficient protocol that generates a uniformly distributed random derangement. We prepared more piles of cards than the number n of players to suppress the need to restart the shuffle process. There is a trade-off between the number t of additional piles and the probability of the

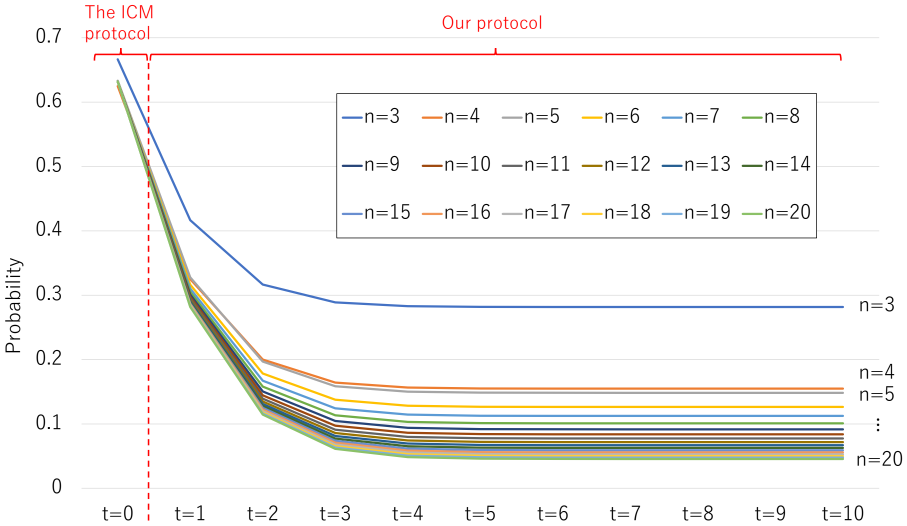


Fig. 2: Relationship between the number t of additional piles and the probability of the need to restart $\Pr[\mathrm{Restart}^{(n,t)}]$

need to restart the shuffle. When executing the proposed protocol, it is better to set $t = 2$ or $t = 3$, as shown in Figure 2.

The proposed technique can also be applied to the existing protocol based on the binary expression of the indices of players [8].

Acknowledgement

We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. This work was supported in part by JSPS KAKENHI Grant Number JP19J21153.

References

1. Crépeau, C., Kilian, J.: Discreet solitary games. In: Stinson, D.R. (ed.) Advances in Cryptology—CRYPTO' 93. LNCS, vol. 773, pp. 319–330. Springer, Berlin, Heidelberg (1994), https://doi.org/10.1007/3-540-48329-2_27
2. Den Boer, B.: More efficient match-making and satisfiability the five card trick. In: Quisquater, J.J., Vandewalle, J. (eds.) Advances in Cryptology—EUROCRYPT '89. LNCS, vol. 434, pp. 208–217. Springer, Berlin, Heidelberg (1990), https://doi.org/10.1007/3-540-46885-4_23
3. Gradwohl, R., Naor, M., Pinkas, B., Rothblum, G.N.: Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles. Theory of Computing Systems **44**(2), 245–268 (2009), https://doi.org/10.1007/s00224-008-9119-9

4. Hashimoto, Y., Nuida, K., Shinagawa, K., Inamura, M., Hanaoka, G.: Toward finite-runtime card-based protocol for generating a hidden random permutation without fixed points. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E101.A**(9), 1503–1511 (2018), https://doi.org/10.1587/transfun.E101.A.1503
5. Hashimoto, Y., Shinagawa, K., Nuida, K., Inamura, M., Hanaoka, G.: Secure grouping protocol using a deck of cards. In: Shikata, J. (ed.) Information Theoretic Security. LNCS, vol. 10681, pp. 135–152. Springer, Cham (2017), https://doi.org/10.1007/978-3-319-72089-0_8
6. Heather, J., Schneider, S., Teague, V.: Cryptographic protocols with everyday objects. Formal Aspects Comput. **26**(1), 37–62 (2014), https://doi.org/10.1007/s00165-013-0274-7
7. Ibaraki, T., Manabe, Y.: A more efficient card-based protocol for generating a random permutation without fixed points. In: Mathematics and Computers in Sciences and in Industry (MCSI). pp. 252–257 (2016), https://doi.org/10.1109/MCSI.2016.054
8. Ishikawa, R., Chida, E., Mizuki, T.: Efficient card-based protocols for generating a hidden random permutation without fixed points. In: Calude, C.S., Dinneen, M.J. (eds.) Unconventional Computation and Natural Computation. LNCS, vol. 9252, pp. 215–226. Springer, Cham (2015), https://doi.org/10.1007/978-3-319-21819-9_16
9. Miyahara, D., ichi Hayashi, Y., Mizuki, T., Sone, H.: Practical card-based implementations of Yao's millionaire protocol. Theor. Comput. Sci. **803**, 207–221 (2020), https://doi.org/10.1016/j.tcs.2019.11.005
10. Miyahara, D., Robert, L., Lafourcade, P., Takeshige, S., Mizuki, T., Shinagawa, K., Nagao, A., Sone, H.: Card-based ZKP protocols for Takuzu and Juosan. In: Farach-Colton, M., Prencipe, G., Uehara, R. (eds.) Fun with Algorithms. Leibniz International Proceedings in Informatics (LIPIcs), vol. 157, pp. 20:1–20:21. Schloss Dagstuhl, Dagstuhl, Germany (2020), https://doi.org/10.4230/LIPIcs.FUN.2021.20
11. Mizuki, T., Sone, H.: Six-card secure AND and four-card secure XOR. In: Deng, X., Hopcroft, J.E., Xue, J. (eds.) Frontiers in Algorithmics. LNCS, vol. 5598, pp. 358–369. Springer, Berlin, Heidelberg (2009), https://doi.org/10.1007/978-3-642-02270-8_36
12. Nakai, T., Tokushige, Y., Misawa, Y., Iwamoto, M., Ohta, K.: Efficient card-based cryptographic protocols for millionaires' problem utilizing private permutations. In: Foresti, S., Persiano, G. (eds.) Cryptology and Network Security. LNCS, vol. 10052, pp. 500–517. Springer, Cham (2016), https://doi.org/10.1007/978-3-319-48965-0_30
13. Ono, H., Manabe, Y.: Efficient card-based cryptographic protocols for the millionaires' problem using private input operations. In: Asia Joint Conference on Information Security (AsiaJCIS). pp. 23–28 (2018), https://doi.org/10.1109/AsiaJCIS.2018.00013
14. Ono, H., Manabe, Y.: Card-based cryptographic logical computations using private operations. New Gener. Comput. **39**(1), 19–40 (2021), https://doi.org/10.1007/s00354-020-00113-z
15. Robert, L., Miyahara, D., Lafourcade, P., Mizuki, T.: Physical zero-knowledge proof for Suguru puzzle. In: Devismes, S., Mittal, N. (eds.) Stabilization, Safety, and Security of Distributed Systems. LNCS, vol. 12514, pp. 235–247. Springer, Cham (2020), https://doi.org/10.1007/978-3-030-64348-5_19
16. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for Numberlink puzzle and k vertex-disjoint paths problem. New Gener. Comput. **39**(1), 3–17 (2021), https://doi.org/10.1007/s00354-020-00114-y

17. Ryan, P.Y.A.: Crypto santa. In: Ryan, P.Y.A., Naccache, D., Quisquater, J.J. (eds.) The New Codebreakers. LNCS, vol. 9100, pp. 543–549. Springer, Berlin, Heidelberg (2016), https://doi.org/10.1007/978-3-662-49301-4_33
18. Sasaki, T., Miyahara, D., Mizuki, T., Sone, H.: Efficient card-based zero-knowledge proof for Sudoku. Theor. Comput. Sci. **839**, 135–142 (2020), https://doi.org/10.1016/j.tcs.2020.05.036