Impossibility Results for Single-Cut Full-Open Card-Based Protocols with Any Number of Cards

Koji Nuida[12] Kazumasa Shinagawa[312] Yasuhide Numata[41]

[1] Kyushu University (nuida@imi.kyushu-u.ac.jp)
[2] National Institute of Advanced Industrial Science and Technology (AIST)
[3] University of Tsukuba
[4] Hokkaido University

November 20, 2026

Abstract

Card-based protocols are cryptographic protocols using a deck of physical cards instead of electronic computers, where information is encoded into a sequence of face-down cards and decoded by opening the cards, and random operations are realized by shuffles of cards. In this research area, there are known impossibility results for protocol construction, but most of the existing results (except for one result for a specific function under a non-standard encoding rule) are conditional on the number of cards used in a protocol, i.e., just giving lower bounds for the number of cards. In contrast, in this paper we give impossibility results, unconditional on the number of cards, for some kind of protocols computing wide classes of functions. Technically, our result is given by deepening a recently explored connection between card-based protocols and combinatorics on words.

Specifically, we consider card-based protocols with the following two properties: (1) just a single random cut is used as shuffles; (2) an opening operation is used just once, where all cards are opened at the same time. It has been known that an arbitrary function can be computed by slightly relaxing (1) to "a single shuffle" (not necessarily a random cut) or (2) to "a part of cards are opened". As opposed to them, in this paper we prove that for protocols satisfying both (1) and (2), for the case of symmetric Boolean functions and Boolean functions without redundant variables, the currently known protocols are essentially all of the possible cases; for any other function (in the sense of NPN non-equivalence), such a protocol is shown to be impossible regardless of the number of cards. We also partially extend the impossibility result to functions with non-binary outputs.

1 Introduction

1.1 Background

Secure computation [6, 22] enables ℓ parties $P_1, \ldots, P_\ell$, each holding a private input $x_1, \ldots, x_\ell \in X$, to compute the output value $y = f(x_1, \ldots, x_\ell) \in Y$ of a function $f\colon X^\ell \to Y$ on their inputs without revealing any additional information on the inputs beyond what is implied by the output value y. While secure computation is usually assumed to be implemented on electronic computers, it is known that secure computation can be realized using a deck of physical cards. This line of research is called *card-based cryptography* [2, 3, 14].

In card-based cryptography, a bit $x \in \{0, 1\}$ is usually encoded as $\clubsuit\heartsuit = 0$ and $\heartsuit\clubsuit = 1$, and a pair of face-down cards representing $x \in \{0, 1\}$ is called a *commitment* to x. If we identify the symbols $\clubsuit$ and $\heartsuit$ with bits as $\clubsuit = 0$ and $\heartsuit = 1$, then a commitment to a bit x can be represented as $(x, \overline{x})$ where $\overline{x}$ is the negation of x. The starting point of our work is the *five-card trick* [2], which is the first card-based protocol in the literature proposed in 1989, for computing the logical AND value $x_1 \wedge x_2$ while keeping the input bits

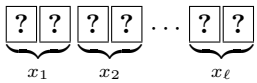
x_1 and x_2 secret. An input sequence of cards is given by $(x_1, \overline{x_1}, x_2, \overline{x_2}, \heartsuit) \in \{\clubsuit, \heartsuit\}^5$ (where all cards are faced down) where the fifth card $\heartsuit$ is a constant *helping card*. Then the protocol proceeds as follows.

1. Rearrange the sequence as $(c_0, c_1, c_2, c_3, c_4) := (\overline{x_1}, x_1, \heartsuit, x_2, \overline{x_2})$.
2. Apply a *random cut* to the sequence $(c_0, c_1, c_2, c_3, c_4)$, which results in $(c_r, c_{r+1}, c_{r+2}, c_{r+3}, c_{r+4})$ for a uniformly random number $r \in \{0, 1, 2, 3, 4\}$ (where the indices are considered modulo 5).
3. Open all cards. Output 0 if they are $\heartsuit\clubsuit\heartsuit\clubsuit\heartsuit$ up to cyclic shifts, and 1 if they are $\heartsuit\heartsuit\heartsuit\clubsuit\clubsuit$ up to cyclic shifts.

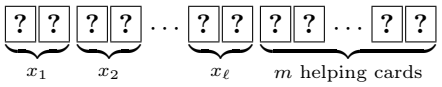
A natural generalization of the five-card trick is the following class of card-based protocols.

Definition 1 (Single-cut full-open (SCFO) protocol)**.** A *single-cut full-open (SCFO) protocol* for a function $f\colon \{0,1\}^\ell \to Y$, where Y is some set, is a protocol that proceeds as follows:

1. For an input $x = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$ of the protocol, given a sequence of commitments to the input bits as

   put a number (say, m) of face-down helping cards, where the symbols ($\clubsuit$ or $\heartsuit$) of the helping cards are fixed and publicly known:

2. Rearrange the card sequence $(c_0, c_1, \ldots, c_{n-1})$ (where $n := 2\ell + m$) by applying a fixed and publicly known permutation $\pi \in \mathsf{Sym}_n$ where Sym_n denotes the set of permutations over $\{0, 1, \ldots, n-1\}$.
3. (The *single-cut* property.) Apply a random cut to the whole of the card sequence; if the original card sequence is $(c_0, c_1, \ldots, c_{n-1})$, then the random cut results in $(c_r, c_{r+1}, \ldots, c_{r+n-1})$ (where the indices are considered modulo n) for a uniformly random and unknown number $r \in \{0, 1, \ldots, n-1\}$.
4. (The *full-open* property.) Open all cards, and determine the output $y \in Y$ of the protocol based on the opened symbols.

Here we suppose that an SCFO protocol must satisfy the following conditions:

Correctness: The output y of the protocol is always equal to $f(x)$.

Security: For any two inputs $x, x' \in \{0,1\}^\ell$ with $f(x) = f(x')$, the probability distribution of the opened symbols at the end of the protocol for input x is identical to that for input x'.

From a practical viewpoint, SCFO protocols are desirable because of their simple protocol designs and of the following facts:

- A random cut is one of the easiest-to-implement shuffles among those used in card-based cryptography.
- For a protocol without the full-open property, we should be careful about the face-down cards remained at the end of the protocol when we put them away; opening them naively may cause leakage of some secret information. On the other hand, we do not need such care when the protocol has the full-open property.

From a theoretical viewpoint, it has been shown in [4] that a protocol for an arbitrary function exists if either the single-cut property is slightly relaxed to a single shuffle (not necessarily a random cut) or the full-open property is slightly relaxed to open only a part of cards at the end of the protocol. In contrast, for protocols with both of the single-cut and the full-open properties, to the authors' best knowledge, only the following SCFO protocols[1] have been discovered in the literature (we note that any SCFO protocol for a Boolean function $f\colon \{0,1\}^\ell \to \{0,1\}$ can be easily converted into an SCFO protocol for the negation of f):

(F1) A 5-card SCFO protocol for $x_1 \wedge x_2$ [2].

(F2) A 4-card SCFO protocol for $x_1 \oplus x_2$ [3, 16].

(F3) A 6-card SCFO protocol for the equality function $\mathsf{EQ}(x_1, x_2, x_3)$ [8, 16].

(F4) An 8-card SCFO protocol for $(x_1 \wedge x_2) \vee (\overline{x_1} \wedge x_3)$ [20].

(F5) An 8-card SCFO protocol for $\overline{x_1}x_2\overline{x_4} \vee \overline{x_2}x_3\overline{x_4} \vee x_1\overline{x_2}x_4 \vee x_2\overline{x_3}x_4$ [20].

In particular, the known SCFO protocols are sporadic, and no unified construction of SCFO protocols for some class of functions has been obtained. Based on the extreme gap of these situations, it is natural to be interested in the (im)possibility of SCFO protocols for other functions.

The goal of this paper is to establish impossibility results for SCFO protocols for a large class of functions. As for the previous work on impossibility of SCFO protocols, Shinagawa and Nuida [19] showed that any SCFO protocol for an n-input Boolean function requires at least 2^{n-1} cards. Ikeda and Shinagawa [9] proved the nonexistence of SCFO protocols for all three-input Boolean functions except for the equality function, in the setting where only ♣ cards are allowed as helping cards. However, here we are interested in impossibility results that are unconditional on the number of cards; no such results have been given in the literature. In fact, as explained in Section 1.3, most of the known impossibility results for card-based protocols are conditional on the numbers of cards (the only exception is the result of [14], but it was given under a non-standard encoding rule for information and therefore the technique cannot be applied to our case). Hence, we need a new technique in order to establish impossibility results unconditional on the numbers of cards.

1.2 Our Contribution

In this paper, we first prove the following impossibility result for SCFO protocols.

Theorem 1. *Let $\ell \geq 3$, and let $f\colon \{0,1\}^\ell \to Y$ be a function for some set Y. Then there does not exist an SCFO protocol for the function f if f satisfies the following condition:*

> *There exist a sequence $b = (b_0, \ldots, b_{\ell-1}) \in \{0,1\}^\ell$ and three indices $i_1 < i_2 < i_3$ in $\{0, 1, \ldots, \ell-1\}$ satisfying that $f(b) = f(b^{(1)}) = f(b^{(2)}) = f(b^{(3)})$, where for each $j \in \{1,2,3\}$, $b^{(j)}$ denotes the sequence obtained from b by changing the i_j-th bit b_{i_j} to $\overline{b_{i_j}}$.*

From Theorem 1, we obtain the following impossibility result for SCFO protocols for a class of symmetric functions.

Corollary 1. *Let $\ell \geq 3$ and consider a symmetric function $f\colon \{0,1\}^\ell \to Y$ for some set Y; now there exists a function $\varphi\colon \{0, 1, \ldots, \ell\} \to Y$ satisfying that $f(b) = \varphi(\mathsf{wt}(b))$ for every $b \in \{0,1\}^\ell$, where $\mathsf{wt}(b)$ denotes the Hamming weight of b. Then there does not exist an SCFO protocol for the function f if there exists an integer $\mu \in \{0, 1, \ldots, \ell - 1\}$ satisfying that $\varphi(\mu) = \varphi(\mu + 1)$ and $(\ell, \mu) \neq (3, 1)$.*

Moreover, for the case of symmetric Boolean functions (i.e., with binary outputs), Corollary 1 can be specialized as follows.

[1] One may also consider SCFO protocols in which multiple commitments to some input bit x_i are given as input. For example, if two commitments to x_1 and one commitment each to x_2 and x_3 are given, then an SCFO protocol for $x_1 \oplus x_2 \oplus x_3$ can be constructed [20]. Such SCFO protocols are outside the scope of this paper.

Corollary 2. *Let $\ell \geq 3$ and consider a symmetric Boolean function $f\colon \{0,1\}^\ell \to \{0,1\}$. Then there does not exist an SCFO protocol for the function f if f is not one of the following functions:*

- *The XOR function $f(b_0, \ldots, b_{\ell-1}) = b_0 \oplus \cdots \oplus b_{\ell-1}$, or its negation.*
- *When $\ell = 3$, the equality function $f(b_0, b_1, b_2) = 1 \Leftrightarrow b_0 = b_1 = b_2$, or its negation.*

For the first excluded case of XOR functions (and their negations) in Corollary 2, we also give the following impossibility result.

Theorem 2. *Let $\ell \geq 3$. Then there does not exist an SCFO protocol for the ℓ-input XOR function.*

On the other hand, for the remaining symmetric Boolean functions, we recall that an SCFO protocol for the three-input equality function has been obtained ((F3) in Section 1.1), and SCFO protocols for symmetric Boolean functions with at most two inputs can be constructed as explained in Section 7. By combining these results, we obtain the following characterization of symmetric Boolean functions that admit an SCFO protocol.

Corollary 3. *Let f be a symmetric Boolean function $\{0,1\}^\ell \to \{0,1\}$. Then there exists an SCFO protocol for f if and only if f is either with at most two inputs (i.e., $\ell \leq 2$) or the three-input equality function or its negation.*

The proof technique for Theorem 2 can in fact be extended to prove the following stronger result. Recall that two Boolean functions are said to be *NPN equivalent* if one of them can be converted into the other by negations of inputs, permutations of variables, and the negation of output. We also say that a variable x_i in a Boolean function $f(x_1, \ldots, x_\ell)$ is *redundant* if $f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_\ell)$ and $f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_\ell)$ are the same function.

Theorem 3. *Let $f\colon \{0,1\}^\ell \to \{0,1\}$ be a Boolean function with no redundant variables. Then there exists an SCFO protocol for f if and only if f is NPN equivalent to the zero function 0, the univariate identity function x_1, or one of the functions (F1)–(F5) in Section 1.1.*

This theorem shows that the seemingly sporadic list of the known SCFO protocols in Section 1.1 in fact exhausts all the possible cases for Boolean functions with no redundant variables. We emphasize again that our impossibility results are unconditional on the number of cards. In contrast, most of the existing proofs for impossibility of card-based protocols, such as those based on KWH diagrams [10, 11, 13], gave only lower bounds on the number of cards; see Section 1.3 for more details.

1.3 Related Work

Card-Based Protocols for Any Function with a Single Shuffle. Shinagawa and Nuida [17] proposed (by using the technique of garbled circuits) the first card-based protocol that uses only a single shuffle (not a random cut) to compute any function, where cards are opened sequentially and adaptively depending on the symbols of the previously opened cards. Subsequent work [15, 21] improved the required number of cards in their protocol. Recently, Eriguchi and Shinagawa [4] proposed (by establishing a generic conversion from private simultaneous messages (PSM) protocols to card-based protocols) two protocols for any function, one of which uses a single shuffle (not a random cut) and with the full-open property, and the other of which is with the single-cut property but the opening operations are adaptive.

Impossibility Proofs in Card-Based Cryptography. Several impossibility proofs for card-based protocols have been given, such as proofs based on KWH diagrams [10, 11, 13], based on formal verification [5, 11, 12], based on the abc conjecture [7], and based on a conversion from card-based protocols to PSM protocols [18]. These impossibility results provide only lower bounds on the number of cards, whereas our impossibility results are independent of the number of cards. One exception is the impossibility result for COPY protocols by Mizuki and Shizuya [14]. They proved the nonexistence of COPY protocols based on

Shannon entropy. However, their proof technique is specialized to COPY protocols under the single-card encoding, which is a special type of encoding. In contrast, our results apply to a class of symmetric functions under the standard encoding (i.e., $\clubsuit\heartsuit = 0$ and $\heartsuit\clubsuit = 1$), while restricting the protocols under consideration to SCFO protocols. As for the impossibility of SCFO protocols, Shinagawa and Nuida [19] gave a lower bound on the number of required cards by using the notion of cyclic equalizability of bit sequences. Ikeda and Shinagawa [9] studied SCFO protocols for three-input Boolean functions based on mathematical optimization and gave an impossibility result in the setting where only $\clubsuit$ cards are allowed as helping cards. Our result is the first to show the nonexistence of SCFO protocols regardless of the number of cards. Moreover, even beyond SCFO protocols, this is the first non-trivial impossibility result for protocols using the standard encoding regardless of the number of cards.

1.4 Notations

In this paper, we sometimes identify the set $\{0,1\}$ of bits naturally with the binary field $\mathbb{F}_2$. We write the negation of $b \in \{0,1\}$ as $\overline{b}$, i.e., $\overline{b} := 1 - b$; and define $\{0,1\}^* := \bigcup_{n\geq 0}\{0,1\}^n$. For any vector w (over some field), let w_i denote the i-th entry of w, where the index i starts from 0 (unless otherwise specified). For any $w \in \{0,1\}^n$, let $\mathsf{wt}(w)$ denote the Hamming weight of w, i.e., the number of indices i with $w_i = 1$; and let

$$\Phi_w(x) := \sum_{i=0}^{n-1} w_i x^i \in \mathbb{F}_2[x] \ .$$

For any polynomial $f(x) \in \mathbb{F}_2[x]$, the coefficient of x^i in f is denoted by $[x^i]f$, and the number of monomials x^i having coefficient $[x^i]f = 1$ is denoted by $\mathsf{wt}(f)$. We note that for any $w \in \{0,1\}^n$, we have $\mathsf{wt}(\Phi_w) = \mathsf{wt}(w)$. For any sets A and B, let $|A|$ denote the cardinality of A, and let $A \,\Delta\, B := (A \cup B) \setminus (A \cap B)$ denote the symmetric difference of A and B. For an integer $n \geq 2$, let ω_n denote a primitive n-th root of unity in $\mathbb{C}$.

In this paper, we write the $(m \times n)$-matrix over $\mathbb{F}_2$ consisting of m rows $w_0, w_1, \ldots, w_{m-1} \in (\mathbb{F}_2)^n$ from top to bottom as ${}^t[w_0, w_1, \ldots, w_{m-1}]$. For any integer $n \geq 1$, let Sym_n denote the set of permutations over $\{0, 1, \ldots, n-1\}$. Then for any sequence $v = (v_0, v_1, \ldots, v_{n-1})$ and any permutation $\pi \in \mathsf{Sym}_n$, let $\pi(v)$ denote the sequence obtained by permuting the components of v according to π; that is, $\pi(v) := (v_{\pi^{-1}(0)}, v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n-1)})$. Moreover, for any $(m \times n)$-matrix $M = {}^t[w_0, w_1, \ldots, w_{m-1}]$ over $\mathbb{F}_2$ and any permutation $\pi \in \mathsf{Sym}_n$, let $\pi(M)$ denote the matrix obtained by applying π to each row of M; i.e.,

$$\pi(M) = {}^t[\pi(w_0), \pi(w_1), \ldots, \pi(w_{m-1})] \ .$$

2 Our Techniques

2.1 Relation between SCFO Protocols and Cyclic Equalizability of Words

Our argument in this paper is based on the relation between SCFO protocols and cyclic equalizability of words explained below; the latter is a notion in combinatorics on words recently introduced in [19].

First, we say that two sequences $w, w' \in (\mathbb{F}_2)^n$ are *cyclically equal* if there is an integer r satisfying that $w'_h = w_{h+r \bmod n}$ for every $h \in \{0, 1, \ldots, n-1\}$; and a number of bit sequences are *cyclically equal* if any two of them are cyclically equal.

Let M be an $(m \times n)$-matrix ${}^t[w_0, w_1, \ldots, w_{m-1}]$ with each row being $w_i = (w_{i,0}, w_{i,1}, \ldots, w_{i,n-1}) \in (\mathbb{F}_2)^n$. Then we call a collection of $n+1$ sequences $u_0, u_1, \ldots, u_n \in \{0,1\}^*$ an *assignment*. Now we define the *insertion* of assignment $(u_0, u_1, \ldots, u_n)$ to M as the process of performing the following for each row w_i:

- Append u_0 to the left of the leftmost bit $w_{i,0}$ of w_i.
- For each $j = 1, \ldots, n-1$, insert u_j into between the $(j-1)$-th bit $w_{i,j-1}$ and the j-th bit $w_{i,j}$ of w_i.
- Append u_n to the right of the rightmost bit $w_{i,n-1}$ of w_i.

We often indicate an inserted bit by putting a dot on the top of it. For example, when $M = {}^t[01, 10]$, the result of the insertion of assignment $(01, 10, 111)$ to M is ${}^t[\dot{0}\dot{1}0\dot{1}\dot{0}1\dot{1}\dot{1}\dot{1}, \dot{0}1\dot{1}1\dot{0}0\dot{1}\dot{1}\dot{1}]$. Moreover, we say that a number of rows $w_{i_1}, \ldots, w_{i_\ell}$ of a matrix $M = {}^t[w_0, w_1, \ldots, w_{m-1}]$ are *cyclically equalizable* [19] if there is an assignment with the property that for the result M' of the insertion of this assignment to M, for any two indices $h, h' \in \{1, \ldots, \ell\}$, the i_h-th row and the $i_{h'}$-th row of M' are cyclically equal.

Now we consider an SCFO protocol for a function $f\colon \{0,1\}^\ell \to Y$ as in Definition 1 where we identify the symbols with bits as $\clubsuit = 0$ and $\heartsuit = 1$. For an input $x \in \{0,1\}^\ell$, let $s(x) \in \{0,1\}^{2\ell+m}$ denote the sequence of front symbols of the face-down cards at the end of Step 2, and let $\widetilde{s}(x) \in \{0,1\}^{2\ell+m}$ denote the sequence of the opened symbols at the end of Step 4. Then, owing to the random cut in Step 3, if $s(x)$ and $s(x')$ for inputs x and x' are cyclically equal, then the probability distributions of $\widetilde{s}(x)$ and $\widetilde{s}(x')$ are identical. On the other hand, if $s(x)$ and $s(x')$ are not cyclically equal, then we always have $\widetilde{s}(x) \neq \widetilde{s}(x')$. Consequently, the correctness and the security of an SCFO protocol are equivalent to the following condition: for $x, x' \in \{0,1\}^\ell$, $s(x)$ and $s(x')$ are cyclically equal if and only if $f(x) = f(x')$.

On the other hand, as the symbols of the helping cards in Step 1 and the permutation π in Step 2 are both fixed and publicly known, the first two steps of an SCFO protocol is equivalent to the following: Given commitments to the input bits, the card sequence is firstly rearranged by a fixed and publicly known permutation $\pi' \in \mathsf{Sym}_{2\ell}$, and then m face-down helping cards are inserted into fixed and publicly known positions in the permuted card sequence. Now we observe that the latter insertion of helping cards can be regarded as an insertion of assignment to a matrix of possible permuted inputs in the sense above. By this and the result of the previous paragraph, the (non)existence of SCFO protocols can be interpreted as follows:

Lemma 1. *Let $f\colon \{0,1\}^\ell \to Y$ be a function for some set Y. Let M denote the $(2^\ell, 2\ell)$-matrix over $\mathbb{F}_2$ with rows indexed by the ℓ-bit sequences, where for each $x = (x_0, x_1, \ldots, x_{\ell-1}) \in \{0,1\}^\ell$, the x-th row of M is $x_0\overline{x_0}x_1\overline{x_1}\cdots x_{\ell-1}\overline{x_{\ell-1}}$. Then there exists an SCFO protocol for f if and only if there exist a permutation $\pi \in \mathsf{Sym}_{2\ell}$ and an assignment $(u_0, u_1, \ldots, u_{2\ell})$ with the property that the result M' of the insertion of this assignment to $\pi(M)$ satisfies the following conditions:*

- *For any two sequences $x, x' \in \{0,1\}^\ell$ with $f(x) = f(x')$, the x-th row and the x'-th row of M' are cyclically equal.*
- *For any two sequences $x, x' \in \{0,1\}^\ell$ with $f(x) \neq f(x')$, the x-th row and the x'-th row of M' are not cyclically equal.*

In particular, in the situation of Lemma 1, if there is some $y \in Y$ satisfying the following:

> for any permutation π, the x-th rows of the matrix $\pi(M)$ for the inputs $x \in \{0,1\}^\ell$ with $f(x) = y$ are not cyclically equalizable,

then there is no SCFO protocol for the function f. We will use this fact for showing the impossibility of SCFO protocols for a large class of functions.

2.2 Interpretation of Cyclic Equality by Polynomial Rings

Then we exploit the fact that cyclic shifts of n-bit sequences can be expressed as multiplication by monomials in the quotient ring $R = R_n := \mathbb{F}_2[x]/(x^n + 1)$. Although this fact has been frequently used in cryptography, this is (to the authors' best knowledge) the first time to apply this fact to card-based cryptography. In the following, we often identify the ring R naturally with the set of polynomials over $\mathbb{F}_2$ of degree at most $n-1$. Then, for any $f \in R$ and any indices $i, j \in \{0, 1, \ldots, n-1\}$, we have $[x^i](x^j f) = [x^{i-j \bmod n}]f$.

Specifically, for an n-bit sequence $w \in (\mathbb{F}_2)^n$ and the corresponding polynomial $\Phi_w(x)$ (see Section 1.4 for the notation), the result w' of cyclically shifting w to the right by α bits satisfies that $\Phi_{w'}(x) = x^\alpha \cdot \Phi_w(x)$ in R. This implies that for any $w, w' \in (\mathbb{F}_2)^n$, w and w' are cyclically equal if and only if there is an integer α with $\Phi_{w'}(x) = x^\alpha \cdot \Phi_w(x)$ in R. Moreover, as we have $\Phi_w(x) + \Phi_{w'}(x) = \Phi_{w+w'}(x)$ in R, w and w' are cyclically equal if and only if there is an integer α satisfying

$$\Phi_{w+w'} = (x^\alpha + 1)\Phi_w(x) \quad (\text{in } R)\ . \tag{1}$$

Our Theorem 1 will be proved by exploiting Eq.(1).

2.3 Evaluating Polynomials at a Root of Unity

Although we have also proved our Theorem 2 solely by the technique of Section 2.2, the proof was too lengthy and based on a computer-based case-by-case analysis. Then the authors tried to use a generative AI tool for shortening our original proof, and the AI tool output a shorter proof of Theorem 2 (described in Section 5) based on another technique explained below. Moreover, the AI tool also suggested and proved a stronger result in Theorem 3 with the same technique.

The strategy here is to consider evaluations of polynomials Φ_w appearing in Section 2.2 at a root of unity, where the coefficients of Φ_w are considered in $\{0,1\} \subseteq \mathbb{R}$ instead of $\mathbb{F}_2$. Specifically, for any sequence $w \in \{0,1\}^n$, we consider

$$\Phi_w(\omega) = \sum_{j=0}^{n-1} w_j \omega^j \in \mathbb{C}$$

where $\omega = \omega_n \in \mathbb{C}$ is a primitive n-th root of unity, and define

$$Q(w) := |\Phi_w(\omega)|^2 \in \mathbb{R} \ .$$

Now if $w, w' \in \{0,1\}^n$ are cyclically equal, then we have $\Phi_{w'}(\omega) = \omega^\alpha \cdot \Phi_w(\omega)$ for some integer α, therefore we have

$$Q(w') = |\omega^\alpha \cdot \Phi_w(\omega)|^2 = |\omega^\alpha|^2 \cdot |\Phi_w(\omega)|^2 = |\Phi_w(\omega)|^2 = Q(w) \ .$$

Hence the quantity $Q(w)$ is invariant for the relation of cyclic equality of words. The shorter proof of Theorem 2 and the proof of Theorem 3 are obtained by exploiting this invariant $Q(w)$.

3 Proof of Theorem 1

In this section, we give a proof of Theorem 1. We deduce a contradiction by assuming that there exists an SCFO protocol as in the statement. Then by Lemma 1, there are a permutation $\pi \in \mathsf{Sym}_{2\ell}$ and an assignment with the property that the result M' of the insertion of this assignment to $\pi(M)$, where M is the matrix in the statement of Lemma 1, satisfies the conditions as in Lemma 1. In particular, the b-th row, the $b^{(1)}$-th row, the $b^{(2)}$-th row, and the $b^{(3)}$-th row of M' are all cyclically equal. Now we extract these four rows of M' and generate a $(4 \times n)$-matrix M'' where n denotes the number of columns of M'; all rows of M'' are cyclically equal as above. Then by the definition of the sequences $b^{(j)}$, we observe that for the following (4×6)-matrix

$$\widehat{M} := \begin{pmatrix} b_{i_1} & \overline{b_{i_1}} & b_{i_2} & \overline{b_{i_2}} & b_{i_3} & \overline{b_{i_3}} \\ \overline{b_{i_1}} & b_{i_1} & b_{i_2} & \overline{b_{i_2}} & b_{i_3} & \overline{b_{i_3}} \\ b_{i_1} & \overline{b_{i_1}} & \overline{b_{i_2}} & b_{i_2} & \overline{b_{i_3}} & b_{i_3} \\ b_{i_1} & \overline{b_{i_1}} & b_{i_2} & \overline{b_{i_2}} & \overline{b_{i_3}} & b_{i_3} \end{pmatrix} \ ,$$

there are a permutation $\widehat{\pi} \in \mathsf{Sym}_6$ and an assignment with the property that the result of the insertion of this assignment to $\widehat{\pi}(\widehat{M})$ is equal to M''.

Now let $w'_0, w'_1, w'_2, w'_3 \in \{0,1\}^n$ be the four rows of M'' from top to bottom. Moreover, let $j_0, \ldots, j_5$ be the six (distinct) indices in $\{0, 1, \ldots, n-1\}$ satisfying that for each $k \in \{0, \ldots, 5\}$, the j_k-th column of M'' originates from the k-th column of $\widehat{M}$. By this choice of indices $j_0, \ldots, j_5$, we have

$$\Phi_{w'_1} = \Phi_{w'_0} + x^{j_0} + x^{j_1} \ , \ \Phi_{w'_2} = \Phi_{w'_0} + x^{j_2} + x^{j_3} \ , \ \Phi_{w'_3} = \Phi_{w'_0} + x^{j_4} + x^{j_5} \ .$$

Now, as all rows of M'' are cyclically equal, by combining Eq.(1) with the relations above, it follows that there are integers $\alpha_1, \alpha_2, \alpha_3$ satisfying (in the ring $R = R_n$)

$$(x^{\alpha_1} + 1)\Phi_{w'_0} = x^{j_0} + x^{j_1} \ , \ (x^{\alpha_2} + 1)\Phi_{w'_0} = x^{j_2} + x^{j_3} \ , \ (x^{\alpha_3} + 1)\Phi_{w'_0} = x^{j_4} + x^{j_5} \ .$$

Moreover, these integers α_k can be chosen from the set $\{0, 1, \ldots, n-1\}$ by the definition of R, and these integers α_k are all non-zero and distinct since the indices $j_0, \ldots, j_5 \in \{0, 1, \ldots, n-1\}$ are all distinct. However, this contradicts Lemma 2 given below (with $g := \Phi_{w'_0}$). This completes the proof of Theorem 1.

Lemma 2. *Let $n \geq 1$. Then there do not exist distinct integers $\gamma_1, \gamma_2, \gamma_3 \in \{1, 2, \ldots, n-1\}$, distinct integers $\nu_0, \nu_1, \nu_2, \nu_3, \nu_4, \nu_5 \in \{0, 1, \ldots, n-1\}$, and an element $g \in R = R_n$ satisfying the following conditions:*

$$(x^{\gamma_1} + 1)g = x^{\nu_0} + x^{\nu_1} \ , \tag{2}$$
$$(x^{\gamma_2} + 1)g = x^{\nu_2} + x^{\nu_3} \ , \tag{3}$$
$$(x^{\gamma_3} + 1)g = x^{\nu_4} + x^{\nu_5} \ . \tag{4}$$

Proof. We assume that such elements exist and deduce a contradiction.

First, under the assumption, we prove that for each $j \in \{1, 2, 3\}$, we have $\gamma_j = n/2$ or $\gamma_{j'} + \gamma_{j''} \equiv 0 \pmod{n}$ where j' and j'' are the two indices in $\{1, 2, 3\} \setminus \{j\}$. By symmetry, it suffices to prove the claim for $j = 1$. By combining Eq.(2) and Eq.(3), we have

$$(x^{\gamma_2} + 1)(x^{\nu_0} + x^{\nu_1}) = (x^{\gamma_1} + 1)(x^{\gamma_2} + 1)g = (x^{\gamma_1} + 1)(x^{\nu_2} + x^{\nu_3}) \ . \tag{5}$$

Similarly, by combining Eq.(2) and Eq.(4), we have

$$(x^{\gamma_3} + 1)(x^{\nu_0} + x^{\nu_1}) = (x^{\gamma_1} + 1)(x^{\gamma_3} + 1)g = (x^{\gamma_1} + 1)(x^{\nu_4} + x^{\nu_5}) \ . \tag{6}$$

Now we introduce the following set

$$S := \{(i, j) \in \{2, 3, 4, 5\}^2 \mid x^{\gamma_1 + \nu_i} = x^{\nu_j} \text{ in } R\} = \{(i, j) \in \{2, 3, 4, 5\}^2 \mid \gamma_1 \equiv \nu_j - \nu_i \pmod{n}\} \ ;$$

intuitively, the set S involves information on how the monomials are overlapped when expanding the right-hand sides of Eq.(5) and Eq.(6) and comparing them. Then we analyze the possibility of elements of S in the following manner:

- As $\gamma_1 \not\equiv 0 \pmod{n}$, we have $(2, 2), (3, 3), (4, 4), (5, 5) \notin S$.
- We have $(4, 2), (4, 3), (5, 2), (5, 3) \notin S$. Indeed, if such a pair, say (i, j), were in S, then a contradiction is deduced as follows. First, by Eq.(6), we have

  $$x^{\nu_0} + x^{\nu_1} + x^{\nu_4} + x^{\nu_5} = x^{\gamma_3 + \nu_0} + x^{\gamma_3 + \nu_1} + x^{\gamma_1 + \nu_4} + x^{\gamma_1 + \nu_5} \ .$$

  As $\mathsf{wt} = 4$ in the left-hand side, we must have $\mathsf{wt} = 4$ in the right-hand side as well. Therefore the monomials in the right-hand sides are not canceled in the sum. Now by the current assumption that $(i, j) \in S$ where $(i, j) \in \{(4, 2), (4, 3), (5, 2), (5, 3)\}$, we have $x^{\gamma_1 + \nu_4} \in \{x^{\nu_2}, x^{\nu_3}\}$ or $x^{\gamma_1 + \nu_5} \in \{x^{\nu_2}, x^{\nu_3}\}$. In any case, the right-hand side above involves a monomial x^{ν_2} or x^{ν_3}, so does the left-hand side above as well, contradicting the fact that the integers ν_k are all distinct.
- We have $(2, 4), (2, 5), (3, 4), (3, 5) \notin S$: this follows from the same argument as the previous item applied to the following relation implied by Eq.(5):

  $$x^{\nu_0} + x^{\nu_1} + x^{\nu_2} + x^{\nu_3} = x^{\gamma_2 + \nu_0} + x^{\gamma_2 + \nu_1} + x^{\gamma_1 + \nu_2} + x^{\gamma_1 + \nu_3} \ .$$

Summarizing these properties, we have $S \subseteq \{(2, 3), (3, 2), (4, 5), (5, 4)\}$. Now if $\{(2, 3), (3, 2)\} \subseteq S$, then we have $\gamma_1 \equiv \nu_3 - \nu_2 \equiv \nu_2 - \nu_3 \pmod{n}$ and hence $2(\nu_2 - \nu_3) \equiv 0 \pmod{n}$. Therefore, as $\nu_2 \neq \nu_3$, we have $\nu_2 - \nu_3 = \pm n/2$. This implies that $\gamma_1 = \nu_2 - \nu_3 \bmod n = n/2$ as in the current statement. By the same argument, the current statement is also implied in the case $\{(4, 5), (5, 4)\} \subseteq S$. From now, we consider the remaining case that $\{(2, 3), (3, 2)\} \not\subseteq S$ and $\{(4, 5), (5, 4)\} \not\subseteq S$.

In this case, by adding Eq.(5) and Eq.(6), we have

$$\begin{aligned}(x^{\gamma_2} + x^{\gamma_3})(x^{\nu_0} + x^{\nu_1}) &= (x^{\gamma_1} + 1)(x^{\nu_2} + x^{\nu_3} + x^{\nu_4} + x^{\nu_5}) \\ &= (x^{\gamma_1 + \nu_2} + x^{\gamma_1 + \nu_3} + x^{\gamma_1 + \nu_4} + x^{\gamma_1 + \nu_5}) + (x^{\nu_2} + x^{\nu_3} + x^{\nu_4} + x^{\nu_5}) \ .\end{aligned}$$

As we have $\mathsf{wt} \leq 4$ in the left-hand side, we must have $\mathsf{wt} \leq 4$ in the right-hand side as well, therefore at least two cancellations must occur between the former part and the latter part of the right-hand side. Hence

we have $|S| \geq 2$. By this and the current conditions $S \subseteq \{(2,3),(3,2),(4,5),(5,4)\}$, $\{(2,3),(3,2)\} \not\subseteq S$, and $\{(4,5),(5,4)\} \not\subseteq S$ for the set S, we can express the set S as $S = \{(i_1,j_1),(i_2,j_2)\}$ where $(i_1,j_1) \in \{(2,3),(3,2)\}$ and $(i_2,j_2) \in \{(4,5),(5,4)\}$. Now the right-hand side of Eq.(5) can be expressed as

$$(x^{\nu_{j_1}-\nu_{i_1}}+1)(x^{\nu_{i_1}}+x^{\nu_{j_1}}) = x^{2\nu_{j_1}-\nu_{i_1}}+x^{\nu_{i_1}} \ ,$$

therefore by Eq.(5), we have

$$(x^{\gamma_2+\nu_0}+x^{\gamma_2+\nu_1})+(x^{\nu_0}+x^{\nu_1}) = x^{2\nu_{j_1}-\nu_{i_1}}+x^{\nu_{i_1}} \ .$$

As $\mathsf{wt} \leq 2$ in the right-hand side, we must have $\mathsf{wt} \leq 2$ in the left-hand side as well, therefore a cancellation must occur between the former part and the latter part of the left-hand side. By this and the fact that $\gamma_2 \neq 0$, we have

$$\gamma_2 = \nu_0 - \nu_1 \bmod n \text{ or } \gamma_2 = \nu_1 - \nu_0 \bmod n \ . \tag{7}$$

Similarly, the right-hand side of Eq.(6) can be expressed as

$$(x^{\nu_{j_2}-\nu_{i_2}}+1)(x^{\nu_{i_2}}+x^{\nu_{j_2}}) = x^{2\nu_{j_2}-\nu_{i_2}}+x^{\nu_{i_2}} \ ,$$

therefore by Eq.(6), we have

$$(x^{\gamma_3+\nu_0}+x^{\gamma_3+\nu_1})+(x^{\nu_0}+x^{\nu_1}) = x^{2\nu_{j_2}-\nu_{i_2}}+x^{\nu_{i_2}} \ .$$

Hence by an argument similar to the above, we have

$$\gamma_3 = \nu_0 - \nu_1 \bmod n \text{ or } \gamma_3 = \nu_1 - \nu_0 \bmod n \ . \tag{8}$$

By Eq.(7), Eq.(8), and the fact that $\gamma_2 \neq \gamma_3$, it follows that $\gamma_2+\gamma_3 \equiv 0 \pmod n$ as in the current statement.

Thus the statement at the beginning of this proof has been proved. Now, as $\gamma_1,\gamma_2,\gamma_3$ are distinct, there is at most one of $\gamma_1,\gamma_2,\gamma_3$ that is equal to $n/2$. By symmetry, we assume without loss of generality that $\gamma_1,\gamma_2 \neq n/2$. Then the statement at the beginning of this proof implies that $\gamma_2+\gamma_3 \equiv 0 \pmod n$ and $\gamma_1+\gamma_3 \equiv 0 \pmod n$. Therefore $\gamma_2 \equiv -\gamma_3 \equiv \gamma_1 \pmod n$ and hence $\gamma_2 = \gamma_1$, contradicting the fact that $\gamma_1 \neq \gamma_2$. This concludes the proof of Lemma 2. □

4 Proofs of Corollary 1 and Corollary 2

Proof of Corollary 1. First we note that $\mu \leq \ell-3$ or $\mu \geq 2$. When $\mu \leq \ell-3$, by putting $b_j := 1$ for $3 \leq j \leq \mu+2$ and $b_j := 0$ for $\mu+3 \leq j \leq \ell-1$, and by writing $\vec{\beta} := (b_3,\ldots,b_{\ell-1})$, we have $\mathsf{wt}(\vec{\beta}) = \mu$, therefore $\mathsf{wt}(0,0,0,\vec{\beta}) = \mu$ and $\mathsf{wt}(1,0,0,\vec{\beta}) = \mathsf{wt}(0,1,0,\vec{\beta}) = \mathsf{wt}(0,0,1,\vec{\beta}) = \mu+1$. Hence by the assumption $\varphi(\mu) = \varphi(\mu+1)$, we have $f(0,0,0,\vec{\beta}) = f(1,0,0,\vec{\beta}) = f(0,1,0,\vec{\beta}) = f(0,0,1,\vec{\beta})$. Now the claim is implied by Theorem 1.

Similarly, when $\mu \geq 2$, by putting $b_j := 1$ for $3 \leq j \leq \mu$ and $b_j := 0$ for $\mu+1 \leq j \leq \ell-1$, and by writing $\vec{\beta} := (b_3,\ldots,b_{\ell-1})$, we have $\mathsf{wt}(\vec{\beta}) = \mu-2$, therefore $\mathsf{wt}(1,1,1,\vec{\beta}) = \mu+1$ and $\mathsf{wt}(0,1,1,\vec{\beta}) = \mathsf{wt}(1,0,1,\vec{\beta}) = \mathsf{wt}(1,1,0,\vec{\beta}) = \mu$. Hence by the assumption $\varphi(\mu) = \varphi(\mu+1)$, we have $f(1,1,1,\vec{\beta}) = f(0,1,1,\vec{\beta}) = f(1,0,1,\vec{\beta}) = f(1,1,0,\vec{\beta})$. Now the claim is implied by Theorem 1. □

Proof of Corollary 2. It suffices to show that if the function f does not satisfy the assumption of Corollary 1, then f is the XOR function or its negation, or the three-input equality function or its negation.

When $\ell \geq 4$, the only cases where the assumption fails are the followings:

$$(\varphi(0),\varphi(1),\ldots,\varphi(\ell)) = (0,1,0,1,0,1,\ldots) \text{ or } (1,0,1,0,1,0,\ldots) \ .$$

The former corresponds to the XOR function, and the latter corresponds to the negation of the XOR function.

When $\ell = 3$, the only cases where the assumption fails are $(\varphi(0),\varphi(1),\varphi(2),\varphi(3)) = (0,1,0,1)$, $(1,0,1,0)$, $(0,1,1,0)$, or $(1,0,0,1)$. These correspond to the XOR function, the negation of the XOR function, the negation of the equality function, and the equality function, respectively. This completes the proof. □

5 Proofs of Theorem 2 and Theorem 3

In this section, we prove Theorem 2 and Theorem 3. First we suppose, in general, that a Boolean function $f\colon \{0,1\}^\ell \to \{0,1\}$ admits an SCFO protocol, and study necessary conditions for f. Now let M be the matrix as in the statement of Lemma 1. Then by Lemma 1, there are a permutation π and an assignment for which the result M' of the insertion of this assignment to $\pi(M)$ satisfies the following condition, where n denotes the number of columns of M' and for each $x \in \{0,1\}^\ell$, $w(x) \in \{0,1\}^n$ denotes the x-th row of M': for any two sequences $x, x' \in \{0,1\}^\ell$ with $f(x) = f(x')$, $w(x)$ and $w(x')$ are cyclically equal.

By the construction of $w(x)$, there are distinct indices $\nu_1, \ldots, \nu_\ell, \nu'_1, \ldots, \nu'_\ell$ in $\{0, 1, \ldots, n-1\}$ and a constant vector $a \in \{0,1\}^n$ satisfying that $w(x) = a + \sum_{i=1}^{\ell}(x_i e_{\nu_i} + (1-x_i)e_{\nu'_i})$ for any $x \in \{0,1\}^\ell$, where $e_j \in \mathbb{R}^n$ denotes the j-th unit vector for $j = 0, 1, \ldots, n-1$. Now the value $\Phi_{w(x)}(\omega)$ introduced in Section 2.3 can be written as

$$\Phi_{w(x)}(\omega) = \Phi_a(\omega) + \sum_{i=1}^{\ell}(x_i\omega^{\nu_i} + (1-x_i)\omega^{\nu'_i}) = A + \sum_{i=1}^{\ell} u_i x_i$$

where $A := \Phi_a(\omega) + \sum_{i=1}^{\ell}\omega^{\nu'_i} \in \mathbb{C}$ is a constant independent of x and $u_i := \omega^{\nu_i} - \omega^{\nu'_i} \in \mathbb{C}$ for each $i \in \{1, \ldots, \ell\}$. We note that $u_i \neq 0$, as $\nu_i \neq \nu'_i$ and ω is a primitive n-th root of unity. Then the invariant $Q(w(x))$ introduced in Section 2.3 can be written as

$$\begin{aligned} Q(w(x)) = |\Phi_{w(x)}(\omega)|^2 &= \left(A + \sum_{i=1}^{\ell} u_i x_i\right)\left(\overline{A} + \sum_{i=1}^{\ell} \overline{u_i} x_i\right) \\ &= |A|^2 + \sum_{i=1}^{\ell}((A\overline{u_i} + \overline{A}u_i)x_i + |u_i|^2 {x_i}^2) + \sum_{1\le i<j\le \ell}(u_i\overline{u_j} + \overline{u_i}u_j)x_i x_j \qquad (9) \\ &= |A|^2 + \sum_{i=1}^{\ell}(2\,\mathrm{Re}(A\overline{u_i}) + |u_i|^2)x_i + 2\sum_{1\le i<j\le \ell}\mathrm{Re}(u_i\overline{u_j})x_i x_j \end{aligned}$$

where we used the relation ${x_i}^2 = x_i$ for $x_i \in \{0,1\}$ at the last equality.

Now recall that $Q(w(x))$ is invariant for the relation of cyclic equality of words. By this and the argument in the first paragraph of this section, if $x, x' \in \{0,1\}^\ell$ and $f(x) = f(x')$, then we have $Q(w(x)) = Q(w(x'))$. Therefore, there are elements $q_0, q_1 \in \mathbb{R}$ satisfying that $Q(w(x)) = q_{f(x)}$ for any $x \in \{0,1\}^\ell$.

In order to show that $Q(w(x))$ is not constant for $x \in \{0,1\}^\ell$, we use the following known fact; we include its proof for the sake of completeness. Here an expression for a function $g\colon \{0,1\}^\ell \to \mathbb{R}$ of the form $\sum_{I\subseteq\{1,\ldots,\ell\}} c_I \prod_{i\in I} x_i$ with $c_I \in \mathbb{R}$ is called a *polynomial expression* of g.

Lemma 3. *Any function $g\colon \{0,1\}^\ell \to \mathbb{R}$ has a unique polynomial expression.*

Proof. First, as for the existence of a polynomial expression for g, note that the Kronecker delta function $\delta_a(x) := \mathsf{Ind}(x = a)$ for any constant vector $a \in \{0,1\}^\ell$ can be expressed as $\prod_{i\,;\,a_i=0}(1-x_i)\prod_{i\,;\,a_i=1} x_i$. Now a polynomial expression for g can be obtained by taking the linear combination $\sum_{a\in\{0,1\}^\ell} g(a)\delta_a(x)$.

On the other hand, as for the uniqueness of a polynomial expression for g, we suppose that g has two expressions of the form

$$g(x) = \sum_{I\subseteq\{1,\ldots,\ell\}} c_I \prod_{i\in I} x_i = \sum_{I\subseteq\{1,\ldots,\ell\}} c'_I \prod_{i\in I} x_i \qquad (10)$$

with coefficients $c_I, c'_I \in \mathbb{R}$, and show that $c_I = c'_I$ for any $I \subseteq \{1, \ldots, \ell\}$. Now it suffices to consider the case that $c'_I = 0$ for every I and show that $c_I = 0$ for every I. We use recursion on ℓ. The base case $\ell = 0$ is obvious (now the two polynomials are $c_\emptyset$ and $c'_\emptyset$, therefore $c_\emptyset = c'_\emptyset$). When $\ell \geq 1$ and the claim holds for the case of smaller ℓ, the middle part of Eq.(10) can be written as

$$\left(\sum_{I\subseteq\{1,\ldots,\ell-1\}} c_I \prod_{i\in I} x_i\right) + \left(\sum_{I\subseteq\{1,\ldots,\ell-1\}} c_{I\cup\{\ell\}} \prod_{i\in I} x_i\right) x_\ell \ .$$

As this is a constant zero function, both of the two functions in the parentheses are zero functions as well, therefore all of the coefficients c_I and $c_{I\cup\{\ell\}}$ must be zero by the claim for smaller ℓ. Hence the claim for this ℓ holds. Therefore a polynomial expression for g is unique. This completes the proof of Lemma 3. □

Now we show the property of $Q(w(x))$ mentioned above.

Lemma 4. *In this setting, suppose that $\ell \geq 3$. Then $Q(w(x))$ is not a constant function for $x \in \{0,1\}^\ell$. In particular, we have $q_0 \neq q_1$.*

Proof. Assume, for the sake of contradiction, that $Q(w(x))$ is constant. Then by Lemma 3, every monomial of positive degree has coefficient 0 in Eq.(9). In particular, we have $\mathrm{Re}(u_i\overline{u_j}) = 0$ for any $1 \leq i < j \leq \ell$. Now we note that $\mathrm{Re}(u_i\overline{u_j})$ is equal to the standard inner product $\langle u_i, u_j\rangle$ on $\mathbb{R}^2$ via the natural identification $\mathbb{C} \simeq \mathbb{R}^2$. Then $\mathbb{R}^2$ involves $\ell \geq 3$ mutually orthogonal non-zero vectors $u_1, \ldots, u_\ell$, a contradiction. □

When $\ell \geq 3$, as $q_0 \neq q_1$ by Lemma 4, the function f can be expressed as

$$f(x) = \frac{Q(w(x)) - q_0}{q_1 - q_0} \ . \tag{11}$$

By this and Eq.(9), $f(x)$ (as well as $Q(w(x))$) admits a polynomial expression of degree at most two. Thus we have obtained the following necessary condition for a Boolean function f to admit an SCFO protocol (note that when $\ell \leq 2$, f always has a polynomial expression of degree at most two).

Proposition 1. *Let $f\colon \{0,1\}^\ell \to \{0,1\}$ be a Boolean function. If f admits an SCFO protocol, then f has a polynomial expression of degree at most two.*

Now we focus on the case of the ℓ-input XOR function f with $\ell \geq 3$ as in Theorem 2. We observe that the XOR function f has the following (unique) polynomial expression $f(x) = (1 - \prod_{i=1}^{\ell}(1-2x_i))/2$. Indeed, the term $\prod_{i=1}^{\ell}(1-2x_i)$ becomes 1 and -1 if the numbers of 1's in x are even and odd, respectively; therefore the right-hand side of the expression becomes 0 and 1 if the numbers of 1's in x are even and odd, respectively, as desired. Now this polynomial expression of f has degree $\ell \geq 3$ (as the coefficient of $x_1x_2\cdots x_\ell$ does not vanish), therefore f does not satisfy the necessary condition in Proposition 1. Hence f does not admit an SCFO protocol. This completes the proof of Theorem 2.

To prove Theorem 3, we use the following known list of NPN equivalence classes of Boolean functions with polynomial expressions of degree at most two.

Proposition 2 (See e.g., [1, Section 3])**.** *A Boolean function $g\colon \{0,1\}^\ell \to \{0,1\}$ has a polynomial expression of degree at most two if and only if g is NPN equivalent to one of the following: (G1) 0, (G2) x_1, (G3) $x_1 \wedge x_2$, (G4) $x_1 \oplus x_2$, (G5) $\mathsf{Ind}(x_1 = x_2 = x_3)$, (G6) $(x_1 \wedge x_2) \vee (\overline{x_1} \wedge x_3)$, and (G7) $\mathsf{Ind}((x_1 \leq x_2 \leq x_3 \leq x_4) \vee (x_1 \geq x_2 \geq x_3 \geq x_4))$, where $\mathsf{Ind}(P) := 1$ if P is true and $\mathsf{Ind}(P) := 0$ if P is false.*

We note that the functions (G3), (G4), (G5), and (G6) are nothing but the functions (F1), (F2), (F3), and (F4) in Section 1.1. On the other hand, an exhaustive search shows that (G7) is the negation of (F5) in Section 1.1 (see Table 1). Hence the list in Proposition 2 is equivalent to 0, x_1, and (F1)–(F5) in Section 1.1. As described in Section 1.1 and Section 7, all of those functions admit an SCFO protocol (if there are no other redundant variables).

Now let $f\colon \{0,1\}^\ell \to \{0,1\}$ be a Boolean function with no redundant variables. If f admits an SCFO protocol, then Proposition 1 and Proposition 2 imply that f is NPN equivalent to 0, x_1, or (F1)–(F5). Conversely, if f is NPN equivalent to 0, x_1, or (F1)–(F5), then f admits an SCFO protocol by the argument in the previous paragraph. This completes the proof of Theorem 3.

6 Discussion on the Two Approaches

The two approaches in the proofs of our main theorems, based on the techniques of Section 2.2 and of Section 2.3, have their own advantages and limitations. First, we explain why a proof of Theorem 2 based on the

Table 1: Truth tables for functions (F5) and (G7)

x_1	x_2	x_3	x_4	(F5)	(G7)
0	0	0	0	0	1
0	0	0	1	0	1
0	0	1	0	1	0
0	0	1	1	0	1
0	1	0	0	1	0
0	1	0	1	1	0
0	1	1	0	1	0
0	1	1	1	0	1
1	0	0	0	0	1
1	0	0	1	1	0
1	0	1	0	1	0
1	0	1	1	1	0
1	1	0	0	0	1
1	1	0	1	1	0
1	1	1	0	0	1
1	1	1	1	0	1

technique of Section 2.2 becomes lengthy. We recall that in the proof of Theorem 1 based on the technique of Section 2.2, it was sufficient to focus on some inputs corresponding to a single output value. In contrast, in the case of the XOR function, say with $\ell = 3$ inputs, for the four rows 010101, 011010, 100110, and 101001 of the matrix M in Lemma 1 corresponding to inputs $x = (0,0,0)$, $(0,1,1)$, $(1,0,1)$, and $(1,1,0)$ having output value $f(x) = 0$, by permuting them by a cyclic permutation $\pi = (0\ 1\ 3\ 4\ 5)$, the resulting sequences 100110, 001101, 010011, and 111000 are cyclically equalizable as $10\dot{0}0110$, $00\dot{0}1101$, $01\dot{0}0011$, and $11\dot{0}1000$. The situation is similar for the four inputs having output value $f(x) = 1$. This implies that we cannot deduce a contradiction by just focusing on inputs corresponding to a single output value, and dealing with input sets for the two output values simultaneously makes the argument more complicated.

On the other hand, in the proofs of Theorem 2 and Theorem 3 based on the technique of Section 2.3, an essential property was that the elements q_0 and q_1 are distinct, which is the core of an expression of f as in Eq.(11). Now if the range of the function f is not binary, say $f\colon \{0,1\}^\ell \to \{0,1,\ldots,N-1\}$ for $N \geq 3$, the non-constantness of $Q(w(x))$ in Lemma 4 is not sufficient for ensuring that $q_0, q_1, \ldots, q_{N-1}$ are all distinct. Consequently, the present technique is effective for the case of binary outputs only, in contrast to the technique of Section 2.2 that yielded Theorem 1 for functions with possibly non-binary outputs.

7 Constructions of SCFO Protocols for Small Functions

Here we consider the case of symmetric Boolean functions $f\colon \{0,1\}^\ell \to \{0,1\}$ with $\ell \leq 2$. First, when $\ell = 1$, the possible functions f are $f(b_0) := b_0$ and $f(b_0) := 0$ (and their negations). An SCFO protocol for the former f is obtained by using helping cards ♣♡ (as 0101 and 1001 are not cyclically equal), while an SCFO protocol for the latter f is obtained by using the fact that the two sequences 01 and 10 themselves are cyclically equal (a random cut can conceal the information on the input b_0 completely).

Secondly, when $\ell = 2$, the possible functions f are the AND function, the OR function, the XOR function, and $f(b_0, b_1) := 1$ (and their negations). SCFO protocols for AND and OR functions are given by the five-card trick and De Morgan's law. An SCFO protocol for the XOR function is given in [3, 16]. Moreover, an SCFO protocol for the constant function $f(b_0, b_1) := 1$ is obtained by using the fact that, starting from the matrix $M = {}^t[0101, 0110, 1001, 1010]$ and exchanging the zeroth and the third columns, we have the following matrix $\pi(M) = {}^t[1100, 0110, 1001, 0011]$ where all the four rows are cyclically equal. Summarizing, every symmetric Boolean function with at most two inputs admits an SCFO protocol.

8 Conclusion

In this paper, we studied a subclass of card-based protocols, called single-cut full-open (SCFO) protocols, which is a generalization of the five-card trick for the AND function to other functions; it consists of only a single random cut as the shuffle operation and opens all cards at the end of the protocol, while it may use an arbitrary number of helping cards. For symmetric Boolean functions, and for Boolean functions without redundant variables, we showed that the SCFO protocols already obtained are essentially all of the possible cases; an SCFO protocol for any other function (in the sense of NPN non-equivalence) is shown to be impossible. We also partially extended this impossibility result to the case of non-binary outputs.

One interesting direction for future research is to consider a relaxed model in which multiple commitments for the same input variable are allowed. Indeed, there exists an SCFO protocol for the three-input XOR function using two commitments for one of the input variables [20], whereas our impossibility result rules out this function in the present model with only one commitment per variable. Thus, it would be interesting to clarify how allowing multiple commitments affects the class of functions that admit SCFO protocols. Other directions for future research include exploring the case of Boolean functions with redundant variables and the case of non-Boolean functions further by enhancing our proof techniques.

Acknowledgements. This work is supported in part by JSPS KAKENHI Grant Numbers JP21K17702, JP25K14994, and JP26K21162, Japan, and JST CREST Grant Number JPMJCR22M1, Japan.

AI Disclosure: We used ChatGPT, powered by GPT-5.6 Sol Pro, to assist with developing the root-of-unity-based proof technique and deriving the resulting non-computer-assisted impossibility proof for the XOR function. The tool materially affected Sections 1.2, 2.3 and 5. More details can be found in the first paragraph of Section 2.3. The authors verified the correctness and originality of all content including references.

References

[1] Jan De Beule, Jozefien D'haeseleer, Ferdinand Ihringer, and Jonathan Mannaert. Degree 2 Boolean functions on Grassmann graphs. *Electronic Journal of Combinatorics*, 30(1):1–23, February 2023.

[2] Bert Den Boer. More efficient match-making and satisfiability *The Five Card Trick*. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology – EUROCRYPT' 89*, volume 434 of *LNCS*, pages 208–217, Heidelberg, 1990. Springer.

[3] Claude Crépeau and Joe Kilian. Discreet solitary games. In Douglas R. Stinson, editor, *Advances in Cryptology—CRYPTO' 93*, volume 773 of *LNCS*, pages 319–330, Berlin, Heidelberg, 1994. Springer.

[4] Reo Eriguchi and Kazumasa Shinagawa. Single-shuffle full-open card-based secure computation protocols for any function. In Yi Li, Frank Stephan, and Xiaoming Sun, editors, *Computing and Combinatorics*, volume 16835 of *Lecture Notes in Computer Science*, pages 15–27, Cham, 2026. Springer.

[5] Kazuhiro Fujita, Shota Ikeda, Kazumasa Shinagawa, and Kazuki Yoneyama. Formal verification and proof of impossibility for four-card XOR protocols using only random cuts. In Keita Emura and Hiraku Morita, editors, *ACM ASIA Public-Key Cryptography Workshop*, pages 9–16, New York, 2025. ACM.

[6] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 218–229. ACM, 1987.

[7] Yuji Hashimoto, Koji Nuida, Kazumasa Shinagawa, Masaki Inamura, and Goichiro Hanaoka. Toward finite-runtime card-based protocol for generating a hidden random permutation without fixed points. *IEICE Trans. Fundam.*, E101.A(9):1503–1511, 2018.

[8] James Heather, Steve Schneider, and Vanessa Teague. Cryptographic protocols with everyday objects. *Formal Aspects Comput.*, 26(1):37–62, 2014.

[9] Shunnosuke Ikeda and Kazumasa Shinagawa. Impossibility results of card-based protocols via mathematical optimization. In *Information Security and Cryptology*, LNCS, Singapore, 2025. Springer.

[10] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. The minimum number of cards in practical card-based protocols. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology—ASIACRYPT 2017*, volume 10626 of *LNCS*, pages 126–155, Cham, 2017. Springer.

[11] Alexander Koch, Michael Schrempp, and Michael Kirsten. Card-based cryptography meets formal verification. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology–ASIACRYPT 2019*, volume 11921 of *LNCS*, pages 488–517, Cham, 2019. Springer.

[12] Alexander Koch, Michael Schrempp, and Michael Kirsten. Card-based cryptography meets formal verification. *New Gener. Comput.*, 39(1):115–158, 2021.

[13] Alexander Koch, Stefan Walzer, and Kevin Härtel. Card-based cryptographic protocols using a minimal number of cards. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology—ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 783–807, Berlin, Heidelberg, 2015. Springer.

[14] Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. *Int. J. Inf. Secur.*, 13(1):15–23, 2014.

[15] Tomoki Ono, Kazumasa Shinagawa, Takeshi Nakai, Yohei Watanabe, and Mitsugu Iwamoto. Single-shuffle card-based protocols with six cards per gate. In Hwajeong Seo and Suhri Kim, editors, *Information Security and Cryptology*, volume 14562 of *LNCS*, pages 157–169, Singapore, 2024. Springer.

[16] Kazumasa Shinagawa and Takaaki Mizuki. The six-card trick: Secure computation of three-input equality. In Kwangsu Lee, editor, *Information Security and Cryptology*, volume 11396 of *LNCS*, pages 123–131, Cham, 2018. Springer.

[17] Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any Boolean circuit. *Discrete Applied Mathematics*, 289:248–261, 2021.

[18] Kazumasa Shinagawa and Koji Nuida. Card-based protocols imply PSM protocols. In Olaf Beyersdorff, Michał Pilipczuk, Elaine Pimentel, and Nguyên Kim Thàng, editors, *Theoretical Aspects of Computer Science*, volume 327 of *LIPIcs*, pages 72:1–72:18, Dagstuhl, 2025. Schloss Dagstuhl.

[19] Kazumasa Shinagawa and Koji Nuida. Cyclic equalizability of words and its application to card-based cryptography. In Artur Jez and Jan Otop, editors, *Fundamentals of Computation Theory*, volume 16106 of *Lecture Notes in Computer Science*, pages 406–419, Singapore, 2025. Springer.

[20] Kazumasa Shinagawa and Koji Nuida. A note on single-cut full-open protocols. arXiv: 2507.03323, 2025.

[21] Kazunari Tozawa, Hiraku Morita, and Takaaki Mizuki. Single-shuffle card-based protocol with eight cards per gate and its extensions. *Natural Computing*, 24(1):131–147, 2025.

[22] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, 1982.