General Conversion Scheme of Card-based Protocols for Two-colored Cards to Updown Cards

— the number of cards for computing an arbitrary function

Takumi Sakurai, Yuichi Kaji
Nagoya University, JAPAN

tentative edition

NAGOYA UNIVERSITY

IARIA

Takumi Sakurai

- Takumi Sakurai is a student of the Graduate School of Informatics in Nagoya University, Japan.
- His research is about card-based cryptography.

Summary

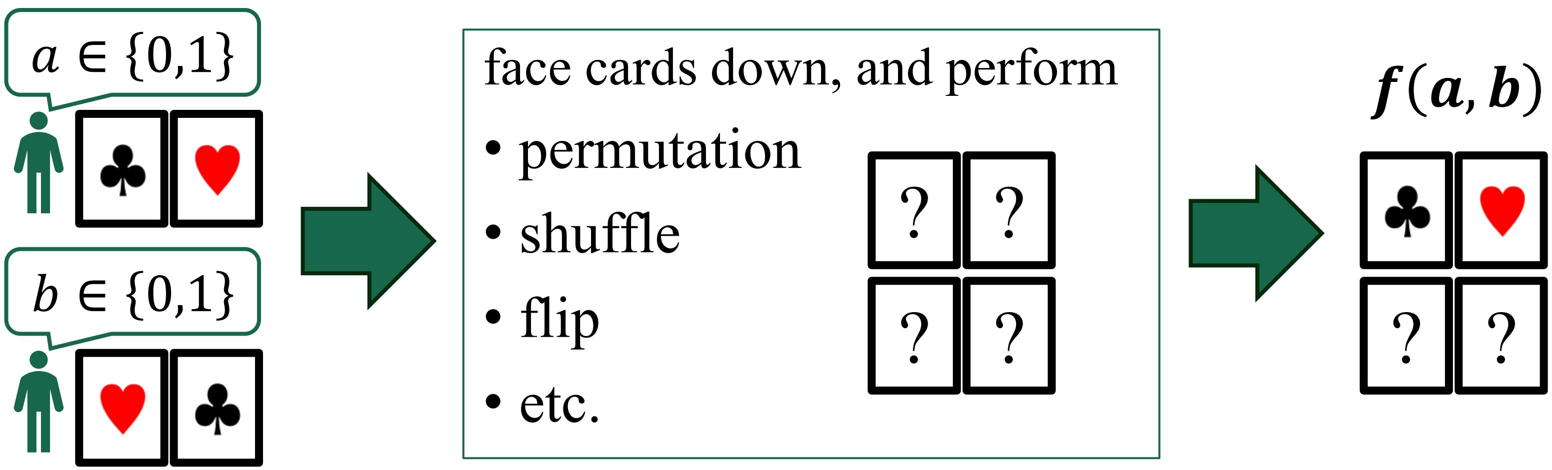
In card-based cryptography, we will …

- discuss the sufficient condition of two-colored cards protocols that can be converted to updown cards.
- clarify the number of updown cards that compute an arbitrary Boolean function by the conversion.

- This study is a compilation of many known results, rather than a novel proposal based on a new idea.

Card-based cryptography

- a technique for secure multi-party computation using physical cards

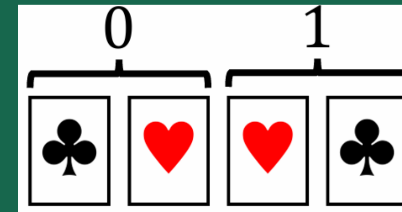


  - without specialized knowledge or equipment
  - lectures of security, zero-knowledge proof for puzzles [Gradwohl 07][Shinagawa 22]

Example: AND protocol [Mizuki 09]

- two-colored cards
  - printed with either “♣” or “♥” on front and “?” on back
    front: ♥ ♣ back: ? ?
  - Cards with the same symbol are not distinguished.
  - placed on a table. We can see only the upper side of cards.
  - A bit is encoded as a *commitment*, a pair of two cards.
    ♣ ♥ = 0, ♥ ♣ = 1
  - The negation bit is obtained by swapping cards in a commitment.

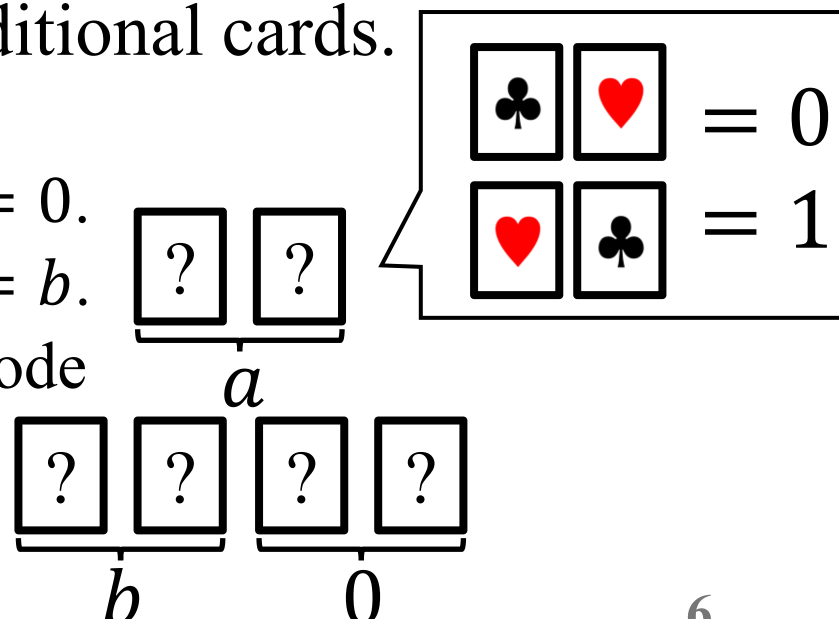
Example: AND protocol [Mizuki 09]



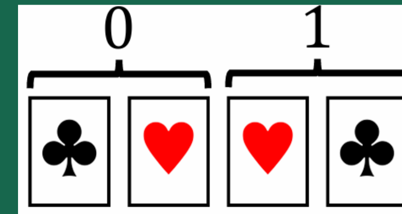
- Alice has $a \in \{0,1\}$. Bob has $b \in \{0,1\}$.
- They obtain only the result of $a \wedge b$.
- Alice and Bob want to compute secure AND.

protocol's procedure

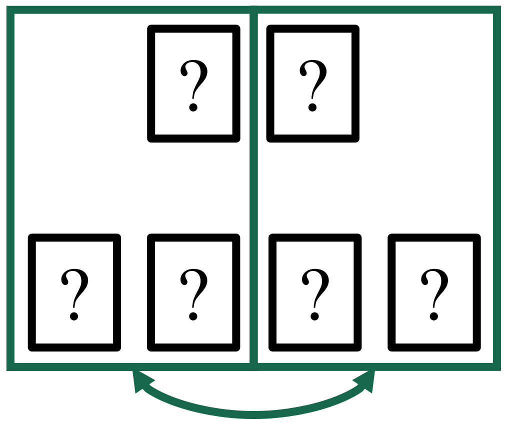
1. Put the input cards and additional cards.
   - Keep the cards face down.
   - When $a = 0$, $a \wedge b = 0 \wedge b = 0$.
   - When $a = 1$, $a \wedge b = 1 \wedge b = b$.
   - The cards under the heart encode the result of the computation.



Example: AND protocol [Mizuki 09]

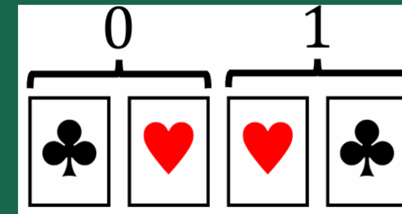


2. Shuffle the left and right sides of the cards.
    - We can use card sleeves or clips.

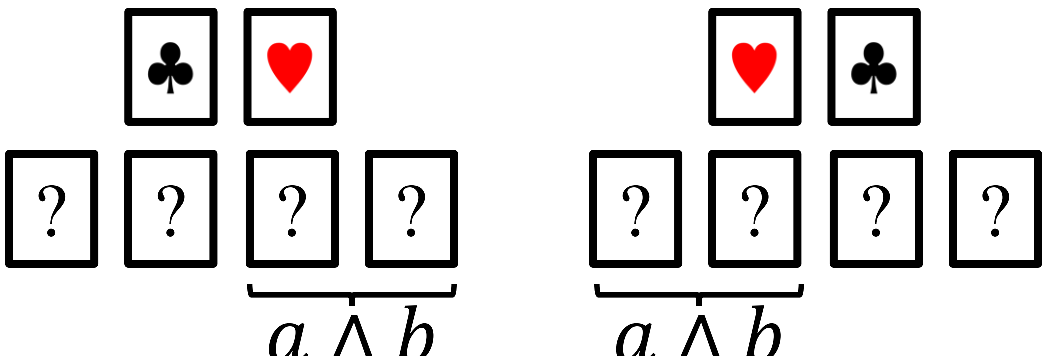


- Participants don’t know whether the cards are swapped.
- Probability of swapping the cards is 1/2.

Example: AND protocol [Mizuki 09]



3. Open the top two cards, and determine the position of the result.
   - The result is the commitment under the heart.
   - By the shuffle, the bit a is not identified.



- To obtain the value, open the resulting cards.
- We can keep the resulting cards face down, and use them for the subsequent computation.

Two-colored protocols

- 6 cards AND protocol [Mizuki 09]
- 4 cards XOR protocol [Mizuki 09]

These basic protocols construct the below protocols

[Nishida 14]

- $2n + 6$ cards
  arbitrary n-variable Boolean function
- $2n + 2$ cards
  arbitrary n-variable symmetric Boolean function

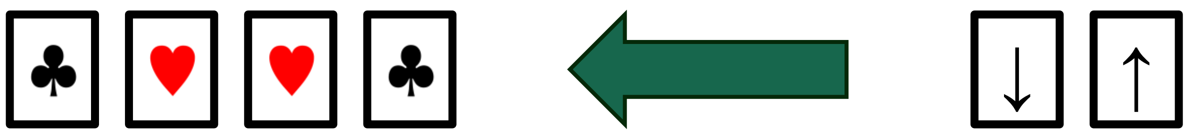
Updown cards

- Updown cards
  - printed with a single symbol of an arrow
  - front: $\boxed{\uparrow}$ back: $\boxed{}$
  - A bit is encoded by the direction of the arrow.

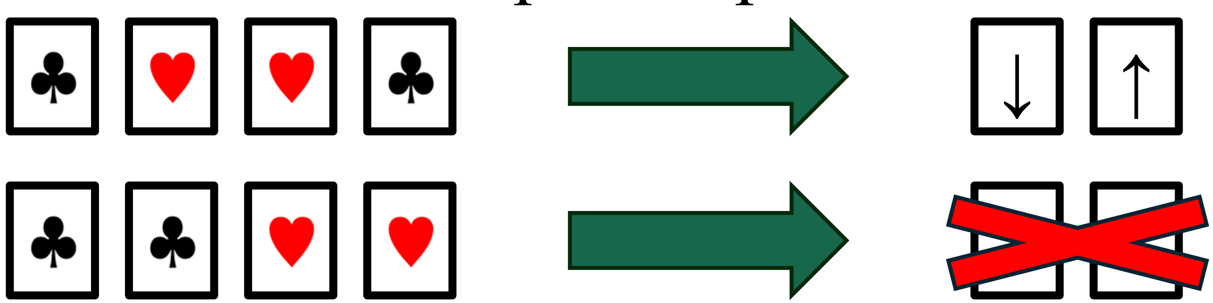
    $\boxed{\downarrow} = 0,\quad \boxed{\uparrow} = 1$
  - The negation bit is obtained by rotating the card.
  - Updown protocols require fewer cards than two-colored.
  - Investigations for updown cards is not enough.
  - There is no updown protocols computing an arbitrary Boolean function.

Main idea

- Given an arbitrary updown protocol, it is clearly possible to construct two-colored protocol.[Shinagawa 23]
  - Retain the expressions of bits.



- Two-colored protocol that preserves commitments can be converted to updown protocol.



Conversion scheme

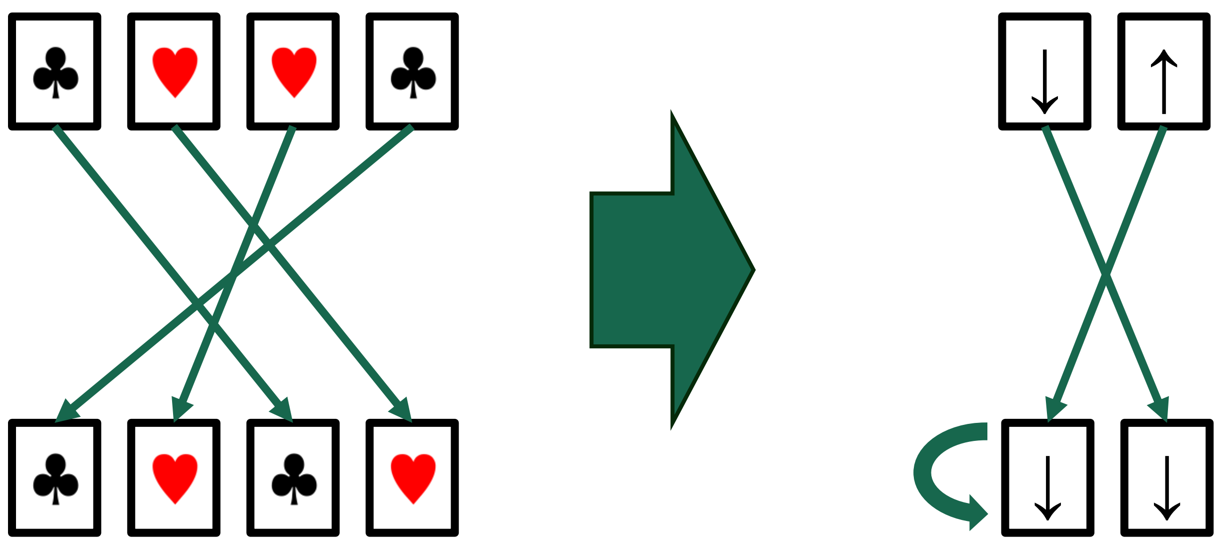
The two-colored protocol using only the following operations can be converted to updown protocol with half the number of cards.

- permutation not destroying the commitment
- shuffle not destroying the commitment
- flip that turns a card face up or face down
- NOT operation

These operation can be simulated by updown cards.

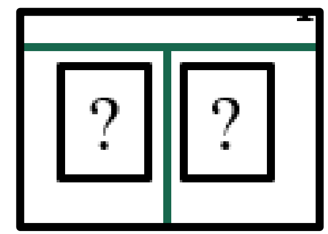
Example of conversion

- with two-colored cards
  - permutation not destroying the commitment
- with updown cards
  - permutation and NOT operations



Logical operations

- Two-colored protocols computing an arbitrary Boolean function destroy the commitment.
  - AND and XOR protocols have the operations separating two cards of a bit.



- With updown cards, AND and XOR protocols were proposed with half the number of cards.
  - 3 cards AND protocol [Mizuki 14][Shinagawa 16]
  - 2 cards XOR protocol [Mizuki 14]

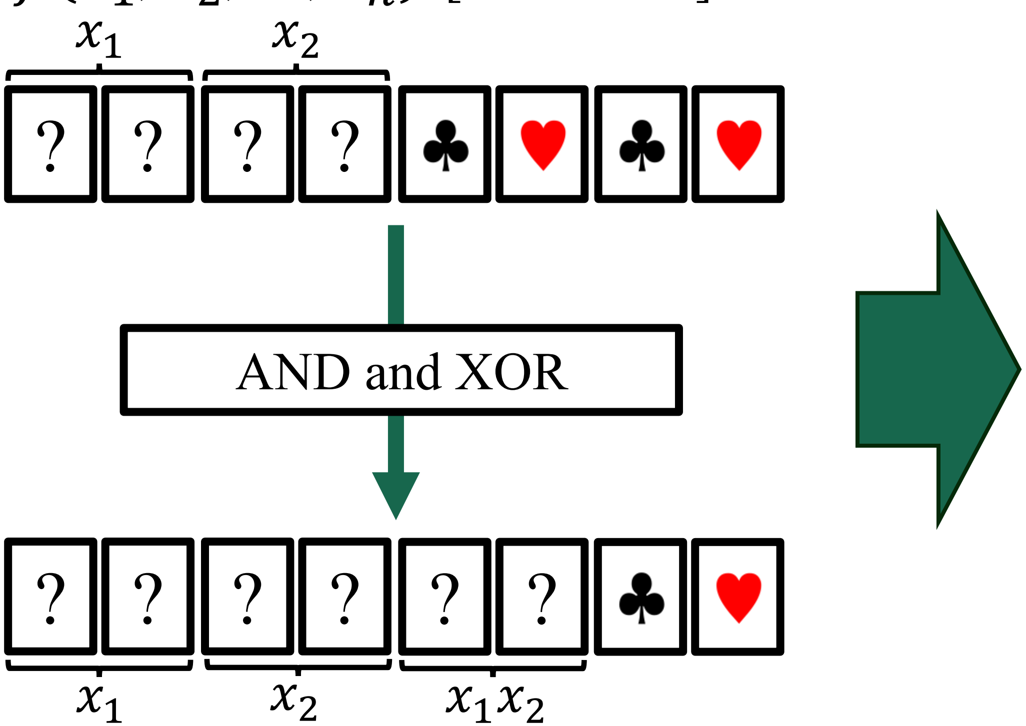
Conversion scheme

The two-colored protocol using only the following operations can be converted updown protocol with half the number of cards.

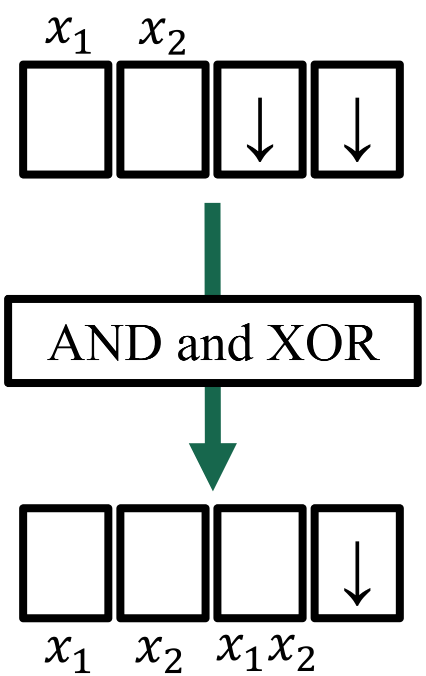
- permutation not destroying the commitment
- shuffle not destroying the commitment
- flip that turns a card face up or face down
- NOT operation
- 6 cards AND protocol
- 4 cards XOR protocol

Example of applications

- with two-colored cards arbitrary n-variable Boolean function $f(x_1, x_2, \ldots, x_n)$ [Nishida 14]



- with updown cards



Arbitrary Boolean function

These basic protocols construct the below protocols

[Nishida 14]

- $2n+6$ cards
  arbitrary n-variable Boolean function
- $2n+2$ cards
  arbitrary n-variable symmetric Boolean function

Convert two-colored protocols to updown protocols.

- $n+3$ cards
  arbitrary n-variable Boolean function
- $n+1$ cards
  arbitrary n-variable symmetric Boolean function

Conclusion and future work

- Conclusion
  - conversion scheme for the two-colored protocol to the updown protocol
  - Boolean function with $n+3$ updown cards
    symmetric function with $n+1$ updown cards

- Future work
  - about other protocols destroying the commitment
  - The minimum number of cards is still unresolved.
    - Use the relationship between updown and two-colored cards…

References

[1] R. Gradwohl, M. Naor, B. Pinkas, and G. N. Rothblum, “Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles,” Internatinal Conference on Fun with Algorithms, pp. 166–182, 2007.
[2] S. Iino, Y. Li, K. Sakiyama, and D. Miyahara, “On the impossibility of n-card and protocols,” 42nd Symposium on Cryptography and Information Security, 4D2-3, 2025 (in Japanese).
[3] A. Koch, S. Walzer, and K. Härtel, “Card-based cryptographic protocols using a minimal number of cards,” International Conference on the Theory and Application of Cryptology and Information Security, pp. 783–807, 2015.
[4] T. Mizuki and H. Shizuya, “A formalization of card-based cryptographic protocols via abstract machine,” International Journal of Information Security, 13, pp. 15–23, 2014.
[5] T. Mizuki and H. Shizuya, “Practical card-based cryptography,” International Conference on Fun with Algorithms, pp. 313–324, 2014.
[6] T. Mizuki and H. Sone, “Six-card secure and and four-card secure xor,” International Workshop on Frontiers in Algorithmics, pp. 358–369, 2009.
[7] T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, “Card-based protocols for any boolean function,” 12th Annual Conference on Theory and Applications of Models of Computation, pp. 110–121, 2015.
[8] T. Nishida, T. Mizuki, and H. Sone, “Securely computing the three-input majority function with eight cards,” Second International Conference on Theory and Practice of Natural Computing, pp. 193–204, 2013.
[9] T. Sasao, “Switching theory for logic synthesis,” Kluwer Academic Publishers, 1999.
[10] H. Shikata, K. Toyoda, D. Miyahara, and T. Mizuki, “Card minimal protocols for symmetric boolean functions of more than seven inputs,” International Colloquium on Theoretical Aspect of Computing, pp. 388–406, 2022 (in Japanese).
[11] K. Shinagawa, “Card types and encodings of card-based cryptography,” presentation slide, Organizing Mathematical Unsolved and New Problems in Card-based Cryptography through Industry-academia Collaboration. [Online]. Available from: https://joint.imi.kyushu-u.ac.jp/wp content/uploads/2023/06/IMI_shinagawa.pdf (accessed 2025 07-03) (in Japanese)
[12] K. Shinagawa, K. Nuida, T. Nishide, G. Hanaoka, and E. Okamoto, “Committed AND protocol using three cards with more handy shuffle,” 2016 International Symposium on Information Theory and Its Applications, pp. 700–702, 2016.
[13] K. Shinagawa, “A report on a lecture for elementary and junior high school using card-based cryptography,” 39th Symposium on Cryptography and Information Security, 2F4-4, 2022 (in Japanese).

Thanks for your attention!