**SCIS 2022** 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers



# 秘匿置換を用いた効率的な $n$ 入力多数決カードプロトコル
# Efficient Card-Based Majority Voting Protocol with $n$ Inputs Using Private Permutations

安部芳紀 * 中井雄士 * 渡邉洋平 * † 岩本貢 * 太田和夫 * †
Yoshiki Abe Takeshi Nakai Yohei Watanabe Mitsugu Iwamoto Kazuo Ohta

**キーワード** マルチパーティ計算・カードベース暗号・$n$ 入力多数決

## あらまし

カードベース暗号とは，物理的なカードを用いて秘密計算を実現する暗号技術である．カードベース暗号プロトコルは，使用する操作により 2 種類に分類することができる．一つが，全てのカード操作を公開の場で行う「シャッフル」ベースのプロトコルであり，もう一つが，他のプレーヤから見えないプライベートな場所でカード操作を行う「秘匿置換」ベースのプロトコルである．シャッフルを用いるプロトコルでは 2 枚のカードで 1-bit の入力を表現するため，$n$ 入力の場合は少なくとも $2n$ 枚のカードが必要となるが，秘匿置換を用いるプロトコルの場合はその限りではなく，$2n$ 枚より少ないカード枚数でプロトコルを構成できることが知られている [1–3]．しかし，入力数 $n$（入力の合計 bit 数が $n$-bit）のプロトコルにおいて，$n$ 枚未満のカードしか使用しないプロトコルは金持ち比べプロトコルなど，一部の例を除き知られておらず，$n$ 入力多数決を計算できるプロトコルでは $n$ 枚以上のカードが必要であった [1–4]．本研究では，秘匿置換を用いて，$n$ ($\geq 3$) 入力多数決を $\lceil n/2 \rceil + 1$ 枚のカードで実現するプロトコルを提案する（表 1）．特に，$n$ ($> 3$) 入力の場合は入力数 $n$ を下回る約 $n/2$ 枚のカードで多数決を計算可能である．本研究は，Watanabe らが提案した，3 枚のカードで 3 入力多数決を行うプロトコル [3] を元に，出力となるカードの位置に着目して分析を行い，$n$ 入力へと拡張している．

表 1: $n$ 入力多数決プロトコルの比較.

| プロトコル | カード枚数 | 操作回数 | 通信回数 |
|---|---|---|---|
| [1, 2] | $n+1$ | $n$ | $n-1$ |
| [4] | $2n+4$ | $O(2^n)$ | $O(2^n)$ |
| [4] | $2^{n+1}$ | $O(2^n)$ | 2 |
| 本研究 | $\lceil n/2 \rceil + 1$ | $2n-1$ | $2n-2$ |
| [3][a] | 3 | 5 | 4 |

[a] [3] は 3 入力多数決プロトコルである．

## 参考文献

[1] 品川和雅. カードと封筒とチェーンを用いた能動的安全な決定的暗号プロトコル. SCIS2018, 3B1–3, 2018.

[2] 中井雄士，徳重佑樹，岩本貢，太田和夫． 秘匿置換を用いたカードベースしきい値関数プロトコル. SCIS2021, 2F1–3, 2021.

[3] Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, and Kazuo Ohta. Card-based majority voting protocols with three inputs using three cards. In International Symposium on Information Theory and Its Applications, ISITA 2018, Singapore, October 28–31, 2018, pp. 218–222. IEEE, 2018.

[4] Hibiki Ono and Yoshifumi Manabe. Card-based cryptographic logical computations using private operations. New Gener. Comput., Vol. 39, No. 1, pp. 19–40, 2021.

* 電気通信大学，〒 182-8585 東京都調布市調布ヶ丘 1-5-1，The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585 {yoshiki, t-nakai, watanabe, mitsugu, kazuo.ohta}@uec.ac.jp
† 産業技術総合研究所，〒 135-0064 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064