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

最小のカード枚数による対称関数の秘密計算について
Secure Computations of Symmetric Functions with Minimum Cards

四方 隼人 * 豊田 航大 * 宮原 大輝 †‡ 水木 敬明 *‡
Hayato Shikata Kodai Toyoda Daiki Miyahara Takaaki Mizuki

キーワード 物理的暗号，カードベース暗号，秘密計算，対称関数

あらまし

カードベース暗号は様々な研究者により発展を繰り返し，実用的なプロトコルから理論的な興味に基づく研究まで幅広く研究されている．そのうち，最も重要な問題の一つに「最小枚数のカードによるプロトコルの構成」がある．具体的には，1ビットを2枚のカードで符号化し，n 個のビットを示す $2n$ 枚のカード列だけが入力として与えられたときに，どのような論理関数が秘密計算できるか，という問題である．これまで AND [1] や XOR [2] 等の基本的な関数や，3 入力多数決関数等 [3] が最小枚数で秘密計算できることが知られているが，任意の関数に対して最小枚数で秘密計算できるかどうかは分かっていない．そこで本稿では，n 変数の対称関数を対象とし，最小枚数のプロトコルの構築を試みる（既存研究では，$2n+2$ 枚のプロトコルが提案されている [4]）．本稿で提案するプロトコルでは，特殊なケースを用いたシャッフル操作を計算過程に含み，入力数 n はある値以上である必要がある．今後本稿の成果を基に，これらの制約を取り除けるかどうかの検討が望まれる．

参考文献

[1] T. Mizuki, “Card-based protocols for securely computing the conjunction of multiple variables,” Theoretical Computer Science, vol.622, no.C, pp.34–44, 2016. https://doi.org/10.1016/j.tcs.2016.01.039

[2] T. Mizuki and H. Sone, “Six-card secure AND and four-card secure XOR,” Frontiers in Algorithmics, eds. by X. Deng, J.E. Hopcroft, and J. Xue, vol.5598, pp.358–369, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2009.

[3] K. Toyoda, D. Miyahara, and T. Mizuki, “Another use of the five-card trick: Card-minimal secure three-input majority function evaluation,” Progress in Cryptology – INDOCRYPT 2021, eds. by A. Adhikari, R. Küsters, and B. Preneel, pp.536–555, Springer International Publishing, Cham, 2021.

[4] T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, “Card-based protocols for any boolean function,” Theory and Applications of Models of Computation, eds. by R. Jain, S. Jain, and F. Stephan, vol.9076, pp.110–121, Lecture Notes in Computer Science, Springer, Cham, 2015.

* 東北大学, 宮城県仙台市青葉区荒巻字青葉 6-3, Tohoku University, 6-3 Aramaki-Aza-Aoba, Aoba, Sendai 980-8578, Japan
† 電気通信大学, 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, Japan
‡ 産業技術総合研究所, 東京都江東区青海 2-4-7, National Institute of Advanced Industrial Science and Technology (AIST), 2-4-7 Aomi, Koto, Tokyo 135-0064, Japan