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

シャッフル 1 回のみの秘密計算に必要なカード枚数について
A Note on the Number of Cards Required for Secure Computations with Single Shuffle

葛馬 知紀 * 豊田 航大 * 五十鈴川 頼宗 * 宮原 大輝 †‡
Tomoki Kuzuma Kodai Toyoda Raimu Isuzugawa Daiki Miyahara
水木 敬明 *‡
Takaaki Mizuki

キーワード 物理的暗号，カードベース暗号，秘密計算

あらまし

カードベース暗号では，秘密計算を実現するプロトコルにおいて,「カード枚数」と「シャッフル回数」がその複雑さの尺度となり，これらの値は小さいほどよい．後者の尺度を最小とする既存研究として，Shinagawa と Nuida [1] は Garbled Circuit のアイデアを基に，任意の n 変数論理関数は 1 回のシャッフルで秘密計算できることを示した．必要なカード枚数は，計算したい n 変数論理関数が q 個のゲートで表現できるとき，$2n+24q$ 枚である．例えば，n 変数の AND 関数や XOR 関数に適用すると，それらのゲート数は $n-1$ なので，$26n-24$ 枚のカードを使うことになる．本稿では，これら 2 つの具体的な関数に着目すると，必要なカード枚数が削減できることを示す．具体的には，n 変数 AND 関数は $4n-2$ 枚，XOR 関数は $2n$ 枚のカードでシャッフル 1 回のみを用いて秘密計算できる．

参考文献

[1] K. Shinagawa and K. Nuida, “A single shuffle is enough for secure card-based computation of any Boolean circuit,” Discrete Applied Mathematics, vol.289, pp.248–261, 2021.

* 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