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

3 値入力可能な可換半群の条件を満たす非コミットメント型 AND 演算拡張カードベースプロトコルの構成

Constructions of non-commitment card-based 3-inputs extended-AND protocols that satisfy the conditions of commutative semi-group

須賀 祐治 *
Yuji SUGA

Keywords: Card-based cryptography, Secure multi-party computation, non-committed format, Five-Card Trick, Commutative Semi-group

あらまし

2 者の AND 演算によるマッチングはカードベースプロトコルにおける一般的なアプリケーションであり，気まずくならない告白ができることが知られている．2 者間の秘密計算によって AND 演算出力が 0 である場合，入力が 0 だったのか 1 だったのかを秘匿できる意味で，相手に入力がバレないことから気まずくならないとされている．本稿は $0,1$ という 2 択の入力を持つ通常の AND 演算を拡張し，0 でも 1 でもない第 3 の値「不定」を入力可能な拡張 AND プロトコルを考える．ビルディングブロックとして 2 者間の拡張 AND 演算プロトコルを用い，複数のプロトコルを連続して実行することを想定すると，この拡張演算は推移律を満たす必要がある．さらに AND 演算は可換であることから，位数 3 の半群がここで扱うべき対象となる．本稿は $0,1,\theta$ を入力とする 3 元の半群としてどのようなバリエーションがあるか完全に分類を行う．また，その一部については 既存の 5 Card Trick をベースとしてプロトコルを構成することを試みた．簡便で十分実現可能な実装法として，裏面にして入力する際に裏面の識別不可能性を持つ同一カード束（名刺など）を用いれば，その上限の位置関係に応じた入力方式を提案する．

* 株式会社インターネットイニシアティブ〒 102 − 0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan. suga@iij.ad.jp

参考文献

[1] J. Heather, S. Schneider, and V. Teague, Cryptographic Protocols with Everyday Objects, Formal Aspects of Computing 26(1), pp.37-62, 2014.

[2] K. Shinagawa, T. Mizuki, The Six-Card Trick: Secure Computation of Three-Input Equality, ICISC 2018.

[3] B. denBoer, More efficient match-making and satisability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.

[4] T. Mizuki, H.Shizuya, Practical Card-Based Cryptography, FUN2014, pp.313-324, 2014.