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

同一のカードを用いた秘密計算
Secure Multi-Party Computations Using Identical Cards

高橋 俊彦 *
Toshihiko Takahashi

キーワード カードベース暗号，秘密計算

あらまし

カードベース暗号プロトコルはトランプのようなカードを用いて秘密計算を実現する方法である [1]．カードベース暗号の起源は 1989 年に発表された den Boer の Five-Card Trick とされる [2]. Five-Card Trick は赤と黒の 2 種類のカードを 5 枚用いて, Alice と Bob が選んだビットの論理積 AND を秘密計算する方法である.

裏向きのカードあるいはカードの組がある論理値 x を表しているとき，このカードを x のコミットメントと呼ぶ. 出力をコミットメントで与えるようなプロトコルはコミット型と呼ばれる．最初のコミット型 AND プロトコルは, 1994 年に Crépeau and Kilian によって発表された [3]. その後, 使用するカードの枚数やシャフル (カット) 回数がより少ないプロトコル, 有限回で終了するプロトコルなどの改案が次々と発表されていった [4, 5].

一方, こうしたプロトコルの実現にはランダム 2 等分割カット (random bisection cut)[6] などの特殊なシャフル (カット) の導入や, カードの並べ替えなどの操作が必要であり, プロトコルを実現するために人間が行う操作は複雑なものとなっていった.

これまでのカードベース暗号の符号化ルールは基本的に赤 (♡) と黒 (♣) の 2 種類のカードを用い, ♣♡ を 0, ♡♣ を 1 と定義するものであった.

これに対し，本研究では同一カード—ただし表面が one-way(上下非対称) であり, 本稿中では↑で表わす—のみを用いた非常にシンプルなカードベース暗号プロトコルを提案する.

最初に 3 枚のカードを用いた非コミット型 AND プロトコルを示す. 続いて，コミット型の NOT プロトコル, XOR プロトコル, COPY(コミットメントの複製) プロトコル, および使用するシャフルの異なる 2 種類の AND プロトコルを順に紹介する. これらを組み合せることで, 同一のカードを用いて任意の論理関数を秘密計算するプロトコルが得られる.

* 新潟大学工学部, 新潟市西区五十嵐二ノ町 8050, Faculty of Engineering, Niigata University, 8050 Ikarashi 2-no-cho, Nishi-ku, Niigata, 950-2181, JAPAN

参考文献

[1] 水木 敬明, “カード組を用いた秘密計算,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 9 巻, 3 号, pp.179–187, 2016.

[2] B. den Boer, “More Efficient Match-Making and Satisfiability The Five Card Trick,” Advances in Cryptology—EUROCRYPT ’89, pp. 208–217, 1989.

[3] C. Crépeau and J. Kilian, “Discreet Solitary Games,” Advances in Cryptology—CRYPTO ’93, pp 319–330, 1993.

[4] Y. Abe, Y. Hayashi, T. Mizuki, and H. Sone, “Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles,” New Generation Computing, Springer, Vol.39, No.1, pp.97-114, 2021.

[5] Y. Abe, T. Mizuki, and H. Sone, “Committed-format AND protocol using only random cuts,” Natural Computing, Springer, Vol. 20, pp. 639—645, 2021.

[6] T. Mizuki and H. Sone, “Six-Card Secure AND and Four-Card Secure XOR,” Frontiers in Algorithmics (FAW 2009), Lecture Notes in Computer Science, Springer-Verlag, Vol.5598, pp.358–369, 2009.