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

手札に関する不正者を検出可能な新しい秘密計算カードプロトコルの提案
Proposition of New Secure Multiparty Computation Protocols for Unfair Player Using a Deck of Cards

小泉 康一 * 大槻 正伸 *
Koichi Koizumi Masanobu Ohtsuki

キーワード Secure multiparty computation, Physical zero-knowledge proof, card game

あらまし

手札を持つようなカードゲームにおいて各プレイヤーの持つ手札の内容は非公開であるために，ゲーム中にいくつかの不正が起こりうる．たとえばほとんどのゲームにおいて，あるカードを手札に持っていないことを示す際にはその事実のみを口頭で示せば良い．ここで，不正なプレイヤーがいるとすると，手札に持つにもかかわらず，持っていないとうそをついてその後のゲーム展開を有利にするかもしれない．このような不正を低コスト，短時間で発見できる手法があると不正行為の抑止力となるだろう．そこで本稿では，このような不正を発見できるようなカードを用いた物理的秘密計算の手法を提案手法１として提案する．提案手法１はゲームで使用する本来の全カード数 N の高々2 倍である 2*N 枚の物理的なカードを用いることで，自分の手札に特定の種類のカードを１枚も含まないことをその他すべてのプレイヤーに対して証明できる．この手法は比較的簡単な手順からなっており，カードゲームを行うことのできるようなすべての人が実行可能である．2*N 枚の物理的なカードのうち半分の N 枚を用いて通常のゲームを行いつつも，必要に応じてゲームを一時中断し，残りの N 枚を用いて提案手法１を実行し，その後すぐにゲームを再開できる．提案手法１を応用することで他のいくつかの手札に関する秘密計算が可能である．

２人のプレイヤーがお互いに手札のカード１枚を同時にオープンして勝敗比べをするようなゲームがある．このゲームをお互いに出す手札をオープンせずに実行したい．これを実現するためには既存の，カードによる金持ち財産比べプロトコル[1]を用いるのが良いかもしれない．ただし，既存版ではカードの数値の大小比べのみが可能であると思われる．そこで，本稿では既存の金持ち比べを変更したものと提案手法１を組み合わせたものを提案手法２として提案する．これにより，単純な大小比べのみでなくじゃんけんのように出す手の価値が異なるような，たとえば通常なら最弱だが特定の相手の手には勝てるような特殊な判定を含む場合でも勝敗が判定できる．さらにお互いに出す手自体は公開しないので簡単に不正が実現できてしまうがそのような不正ができないような新手法を提案手法２として提案する．

ただし，厳密に提案手法２を実行しようとすると使用する全カード枚数が膨大になり，特殊なシャッフル手法が必要になるため実行にかかる時間もだいぶ大きくなる．そのため，今のところ実用的な時間内で提案手法２を適用できるのは，出せる手の種類が少ないようなシンプルなゲームに限られてしまう．

一連の提案手法は，ほぼ同じ大きさの複数枚のカードの表面，裏面が同一デザインであるとき，どのような人間であっても誰も区別ができない，という仮定を安全性の根拠としている．現実には全く同じカードを複数枚用意することは不可能であるが，カジノのように常に新品のカードを使用することや，カードを覆うスリーブなどを活用することで理想的な環境に近づけることができる．

参考文献

[1] 宮原大輝，水木敬明，曽根秀昭，“トランプカードを用いた金持ち比べプロトコル，” 信学技報，COMP2018-38, pp. 39--45, 2018.

* 福島工業高等専門学校 電気電子システム工学科, 9708034 福島県いわき市平上荒川字長尾 30