多値カードを用いた秘密計算プロトコルの研究
～カードベース暗号の調査と研究の方向性について～

研究年度　平成 30 年度
研究代表者名　　松崎　なつめ

１．　はじめに

秘密計算プロトコルは，複数のプレーヤが共同で行う処理であって，各プレーヤの入力値は秘密にしたままで所定の処理を行い，特定の関数値のみを共有する．代表的な例として，投票がある．各自が誰に投票したのかが秘匿されたまま，それぞれの被投票者に合計何票投票されたのかのみが共有される．また，各病院で管理されている機密データ（例えば個人の疾患情報やゲノム情報など）を，相互に開示せずに結合・分析結果のみを求める応用も検討されている[1]．秘密計算プロトコルは，応用があり有用である一方，入力値の秘匿性や関数値の正当性など，直感的に理解しにくいとの課題がある．

この課題を解決する１アプローチとして，1989 年に den Boer により，カードを用いた秘密計算プロトコル（以降では，カードベース暗号と呼ぶ）が提案され[2]，以降盛んに研究が進められている．カードベース暗号は，暗号プロトコルの初心者にも取り組みやすく，論理的思考力が養われるため，教育的効果が期待される．

研究代表者は，当初，多値カードを用いた秘密計算プロトコルを研究する必要性を感じていた．多くの研究成果で想定している特殊なカードではなく，一般に入手しやすいカードを用いることで，可用性を向上する目的である．

本研究報告では，カードベース暗号の既存研究を調査し，研究方向性を整理する．この調査により，多値カードを用いる研究の方向性の妥当性を確認する．

２．　研究内容

今年度は，主には文献[2]を用いて，カードベース暗号の既存研究調査を実施した．以下内容を概説する．

2.1　カードベース暗号とは

カードベース暗号とは，トランプカードのような物理的なカード組を用いて，秘密計算プロトコルを，身近で手軽に実現するものである．プレーヤがその場で集まり，全員が見守る中で，カードを並べたり，シャッフルすることで，各プレーヤの入力値は秘密にしたままで所定の処理を行い，特定の関数値のみを求め共有する．

カードベース暗号の基本的な処理としては，おおむね次の通りである．まず，各プレーヤが保持するカードを，入力値に対応して，公開の場（プレーヤが囲むテーブル

を想定）に裏向けて並べる．その後，カードを裏向けたまま所定のシャッフルする．その後，出力値を確認して，特定の関数値を全プレーヤで確認する．場合によっては，このプロセスを複数回繰り返す．

2.2　Five-Card Trick[3]

Five-Card Trick は，1989 年に den Boer により提案されたカードベース暗号のプロトコルであり，ここからカードベース暗号の研究はスタートしている．2 名が，特別なカード（裏面で区別できない，クラブ（黒）とハート（赤）のみからなるカード，図１）を用いて，双方がカードを操作することにより，それぞれが入力する 1 ビットの入力値を秘密にしたまま，これらの AND 値（論理積）を求める． 2 名のプレーヤが入力する，1 ビットの入力値は， それぞれ 2 枚のカードを用いて表して，追加カード 1 枚を加えた 5 枚のカードで処理をする．

図 1　カードベース暗号用の特別カード

2.3　カードベース暗号研究の方向性

ここでは，2.2 で説明した Five-Card Trick を起点として，カードベース暗号の既存研究の方向性を次の８観点で述べる．

(1) 用いるカード

Five-Card Trick では，図１で示す，裏面が区別できないクラブ（黒）とハート（赤）のみからなる特別なカードを用いている． そして，2 枚のカードの並べ方により，1 ビットの値を表している．具体的には左から，クラブ-ハートを「0」，ハート-クラブを「1」とする（これを符号化方法と呼ぶ）．

これを拡張し，手軽に入手しやすい，通常のトランプを利用する方法も提案されている[4]．この方法では，1≦i＜j≦52 の i,j が表に記された 2 枚のカードを用いて，左から i,j と並べられた場合（左が小さい場合）は「0」を表し，j,i と並べられた場合（左が大きい場合）は「1」を表すものとする．[4]では，ランダム二等分割カットを用いて，AND，XOR を求めるプロトコルを提案している．

(2) 演算，シナリオ

Five-Card Trick では，求める演算は AND（論理積）である．2 名が「1」を入力した場合のみ，双方に両方が「1」を入力したことが共有できる．それ以外の場合は，例えば，自分が「0」を入力した場合は，相手が「0」を入力したのか，「1」を入力したのか分からない．その具体的なシナリオは，例えば，「気まずくならない告白」である．Yes と No をそれぞれ「1」と「0」で表すと，両方が Yes の場合のみ，そのことが分かり，交際成立となる．それ以外の場合は，相手が Yes としたのか No としたのかが分からない．そのため，その後も気まずくならず，友達を続けることができる．

AND 以外の演算として，XOR 演算や OR 演算，NOT 演算も提案されており，これらを組み合わせることで，加算や大小比較，ランキング計算等[5][6]の任意の演算が実現できる．

一方，1 ビットずつ論理演算を組み合わせるよりもシャッフルの数が少なく効率的な，それぞれの計算に特化したプロトコルの研究も提案されている．

(3) 出力の仕方

Five-Card Trick では，シャッフルの後，すべてのカードを表に返し，ハート（赤）が３つ並んでいる場合に AND 値が「1」，それ以外の場合は「0」であることを求める．これに対し，入力と同様の符号化方法（2 枚のカードの並べ方で 1 ビットを表す）で出力する方法を，コミット型プロトコルと言い，よりエレガントな方法として提案されている．

(4) 参加者人数

Five-Card Trick では，プレーヤは 2 名である．この人数を増やす場合について研究されていると考えられるが，論文については未調査である．

(5) シャッフルの仕方

Five-Card Trick では，巡回的なシャッフルを 2 者がそれぞれ何度でも任意の回数行う．このシャッフルはカードの並びを維持する．

一方，2009 年に，ランダム二等分割カットと呼ばれる，カード列をちょうど真ん中で半分に分割し，これら二つの部分列の位置を，50%の確率で入れ替える操作が提案された[7]．このシャッフル方法を導入することにより，効率的なコミット型 AND プロトコルや XOR プロトコルが構築できることが分かっている．

また，2016 年には，背面で秘密の置換を行う秘匿置換が提案された[8]．秘匿置換を用い，さらに効率的なプロトコルを実現できるのみならず，ルールに従わないプレーヤが存在した場合，そのことを検知することができる．しかしながら，見えないと

ころでシャッフルすることにより，もともとカードベース暗号が有する「プロトコルの動作を視覚的に把握可能であり，直感的に理解可能である」との利点が著しく損なわれていると考えられる．

(6) 余分なカード

Five-Card Trick では,2 人がそれぞれ入力となるカードを 2 枚づつ保持するに加え，追加のカードを 1 枚加え，合計で 5 枚のカードを用いる．2012 年に，ランダム二等分割カットを用いて，同じことを，4 枚のカードで実現できることが示されている[9]．

(7) ユーザの仮定

Five-Card Trick では，参加するユーザは,「0」を示すクラブ-ハート，あるいは「1」を示すハート-クラブの並びで入力すると仮定されている．これに対し，例えば，ハート-ハートと並べたり，決められた方法以外でカードをシャッフルするなど，ルールを守らないユーザを仮定し，それでも安全なプロトコルを考える研究がされている[10]．ルールを守るユーザを，semi-honest と言い，ルールを守らないユーザを malicious という．

(8) 直感的な理解

Five-Card Trick では，すべてを表に向け，決められたプロトコルどおりに入力すると，2 者が「1」を入力したときのみ，ハートが３つ続くことが容易に理解できる．巡回シャッフルでは，このカードの並びが維持される．ランダム二等分割カットの場合は，確率を考慮する必要があるため，多少理解度が下がる．さらに，秘匿置換となると，背面での置換が分からないため，理解度が下がると考えられる．ただし，理解度に関する，プレーヤの有する背景情報などに依存しない，定量的な評価基準の研究は今のところ見当たらない模様である．カードベース暗号以外での研究で，参考になるものを調査する必要がある．

2.4　最近のカードベース暗号研究

最近のカードベース暗号研究の動向は，秘匿置換を導入し，複雑な秘密計算を，できるだけ効率的に実現するカードベース暗号の提案が多い．さらに，背面で行う秘匿置換を導入することで生じる可能性のある malicious ユーザの不正は，これを検知する機能を有することで防止する．2019 年 1 月に開催された SCIS2019 では，カードベース暗号のセッションが設けられ，4 件の発表があった[11][12][13][14]．そのうち 3 件は秘匿置換を用いたものになっている．

３．　考察

今年度は，2 章で述べた既存研究の調査を通じ，研究の方向性を検討した．

当初，今年度の調査研究では，用いるカードとして通常のトランプのような多値カードを用いるカードベース暗号を研究する予定であった．しかしながら，調査の結果，手軽に入手しやすいカードであるとの利点，および学術的な興味はあるものの，すでに基本的な考えは提案されており，この改良を検討することは有用性に欠けると考えるに至った．

一方，最近のカードベース暗号研究は，多くの場合，複雑なシャッフル方法を導入することで，秘密計算の多機能性や効率化に注力している．このことによって，もともとカードベース暗号が有していた「直感的に理解可能」の利点が損なわれている気がする．また，「直感的に理解可能」と，多機能性や効率性などの関係についても，まだ十分研究の余地があると考える．ただし，「直感的に理解可能」の評価のためには，評価する人の背景知識に依存しない，妥当で定量的な指標が必要と考える．この指標については，未調査である．

４．　おわりに

ここでは，カードベース暗号の既存研究を調査して，その研究方向性を検討した．その結果，もともと考えていた多値カードを用いるプロトコルの研究よりも，カードベース暗号の「直感的に理解可能」といった利点と効率化等との関係についての研究が必要であると考えた．ただし，このためには，評価する人の背景知識に依存しない，妥当で定量的な指標が必要になる．

参考文献

[1] 佐久間，秘密計算による秘密データ利活用の社会応用に向けて，文科省 WG「グラフビッグデータ」講演 2013.12.5.
[2] 水木敬明，解説論文：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 IEICE Fundamentals Review, Vol.9, No.3, 179-187, 2016.
[3] B.denBoer, More efficient match-making and satisfiability: the five card trick, EUROCRYTPT’89, 1990.
[4] 水木，市販トランプカードを用いた安全な計算について，ISEC2014-103, 2015.
[5] 高島，阿部，佐々木，宮原，品川，水木，曽根，カード組を用いた秘匿ラインキング計算，ISEC2018-30,2018.
[6] 西田，林，水木，曽根，カード組を用いた任意の論理関数の安全な計算について，CSS2014,2014.
[7] T. Mizuki and H.Sone, Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, 2009.
[8] T. Nakai, Y. Tokushige, Y. Misawa, M. Iwamoto, and K. Ohta. Efficient card-based cryptographic protocols for millionaires’problem utilizing private permutations. In Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016,Proceedings, pages 500{517, 2016
[9] T.Mizuki, M.Kumamoto, and H.Sone, The five-card trick can be done with four cards, ASIACRYPT 2012, 2012.
[10] 水木，静谷，カードベース暗号プロトコルに対する攻撃に関する考察，ISEC2013.
[11] 品川，秘匿互換に基づくカードベース暗号プロトコル，SCIS2019.
[12] 安部，山本，岩本，太田，不正検知可能な 3 入力多数決カードプロトコル，SCIS2019.
[13] Yoshifumi Manbe, Hibiki Ono, Card-based cryptographic protocols for several Boolean functions using private operations, SCIS2019.
[14] 宮原，水木，曽根，カードベース安定マッチング，SCIS2019.