カードゲームLove Letterへの秘密計算の応用

小泉 康一[1,a)]　水木 敬明[2]

概要：カードゲーム Love Letter は 1 から 8 までの数字の付いた 16 枚のカードで遊ぶゲームである．2 人から 4 人で遊ぶことができ，各プレイヤーは手札を 1 枚持つ．手番ごとに山札からカードを 1 枚引き，ゲームのルールに従って手札 2 枚のうち 1 枚を場に出す．最終的に手札の数字が最も大きいプレイヤーが勝利する．場に出されたカードごとに異なる特殊処理を行うため，これによりゲームに面白みを与えている．本稿では，このゲームにおいて仮想的なプレイヤーをコンピュータ無しで実現することを考える．そのためには，仮想プレイヤーの手札の中身を見ずに適切な 1 枚を選択し場に出す必要がある．カードベース暗号のテクニックを用いて，2 枚のうちどちらを選ぶべきか（あるいは負けが確定しているか）の戦略を行列として与え，仮想プレイヤーの手札の 1 枚を秘密に選択するカードベースプロトコルを構成する．仮想プレイヤーの手札にゲームのルール処理を施すカードベースプロトコルは，これまでにババ抜きや UNO に対して構築されてきたが，本稿はそれらに続くものとなる．

キーワード：カードベース暗号，秘密計算，カードゲーム

Application of Secure Computation to the Love Letter Card Game

Koichi Koizumi[1,a)]　Takaaki Mizuki[2]

Abstract: The Love Letter card game is played with 16 cards numbered from 1 to 8. It can be played by 2 to 4 players, with each player holding one card in their hand. On each turn, a player draws one card from the deck and, following the rules of the game, plays one of the two cards in their hand. The player with the highest number in their hand at the end of the game wins. Each card played triggers a different special effect, adding to the fun of the game. In this paper, we explore the implementation of a virtual player in this game without relying on a computer. To do this, we must select an appropriate card from the hand of the virtual player without seeing their hand. Using card-based cryptography techniques, we construct a card-based protocol that secretly selects one card from the virtual player's hand by providing a matrix representing the strategy for choosing between the two cards (or determining when defeat is certain). Card-based protocols that apply game rule processing to the virtual player's hand have been constructed for Old Maid and UNO, and this paper follows them.

Keywords: Card-based cryptography, Secure computation, Playing cards

1. はじめに

本稿ではカードゲーム，*Love Letter* を取り扱う．Love Letter はカナイセイジ氏が考案したカードゲームで，1 から 8 までの数字が描かれた 16 枚の数字付きカードを用いて，2 人から 4 人のプレイヤーで遊ぶゲームであり，ルールが比較的簡単で短時間で遊べる．初版は 2012 年であり，国内外の複数の出版社からいくつかのバージョンが販売されており，人気を博している．図 1 は国内版のバージョンの 1 つ（株式会社アークライト製）である．本稿ではプレイヤーを 4 人とし，ゲームのルール説明から始める[i]．

[1] 福島工業高等専門学校
National Institute of Technology, Fukushima College
[2] 東北大学サイバーサイエンスセンター
Cyberscience Center, Tohoku University
[a)] koizumi@fukushima-nct.ac.jp

[i] プレイヤーが 2 人および 3 人の場合も同じルールである．

図 1: Love Letter のセット

図 2: Love Letter の数字付きカード

1.1 Love Letter のゲームルール

Love Letter では，図 2 の 8 種のカードを用いる．1 から 8 までの数字と，各数字に 1 対 1 に対応するカード名，カードの効果が描かれているが，本稿ではカード名を用いず数字のみで**数字付きカード**として表現する．各カード枚数には偏りがあり，1 のカードが 5 枚，2，3，4，5 が 2 枚，6，7，8 が 1 枚ずつである．すなわち，ゲームには次の 16 枚のカードを用いる．

1	1	1	1	1	2	2	3	3	4	4	5	5	6	7	8

裏面は共通の絵柄（本稿では ? とする）で裏からカードの表面を特定できない．また，同じ数字のカードはお互いに区別できない．

ゲーム開始前に，これらの 16 枚のカードを裏向きにしてかき混ぜ，各プレイヤーへランダムに 1 枚が手札として配布される．手札でないカード（4 人プレイヤーなので 12 枚）のうち，1 枚は非公開で取り除かれ，残りのカードで山札が作られる．

基本的なゲームの流れを示す．各プレイヤーが順に以下の手番を行う．

(1) 山札から 1 枚引き，手札に加える．
(2) 手札に持つと発揮するカードの効果を処理する[ii]．
(3) 手札 2 枚のうち，選択可能な 1 枚を場に出す．
(4) 場に出したカードの持つ効果を処理する[iii]．
(5) 場に出したカードを捨て札にする．

カードの効果によりプレイヤーがゲームから脱落することがあり，脱落したプレイヤーは手札を表にし，以降の手番は飛ばされる．山札がなくなるまで上記の手番を繰り返し，ゲームは終了する．脱落せずに残っている各プレイヤーは，手札 1 枚を公開し，最も大きい数字のプレイヤーが勝利する[iv]．

カードの効果を表 1 にまとめる[v]．カードの効果はゲームのバージョンにより異なるが，本稿では最初のバージョンのものを採用している．

表 1: カードの効果

数	名称	カードが持つ効果
1	兵士	他のプレイヤーを 1 人選び，その手札を予想し 1 以外の数字を 1 つ言う．当たった場合，そのプレイヤーは脱落する．
2	道化	他のプレイヤーを 1 人選び，その手札を見る．
3	騎士	他のプレイヤーを 1 人選び，ひそかに手札の数字を比べ，数字の小さいプレイヤーは脱落する．
4	僧侶	あなたの次の手番が始まるまで，あなたへのカードの効果は無効になる．
5	魔術師	プレイヤーを 1 人選ぶ（あなたでもよい）．そのプレイヤーは手札を捨て札にし，山札から 1 枚引いて新たな手札にする．
6	将軍	他のプレイヤーを 1 人選び，手札を交換する．
7	大臣	手札が 2 枚のとき，もう片方の手札の数字が 5 以上であればあなたは脱落する．
8	姫	（5 のカードの効果で捨てる場合でも）このカードを捨て札にする場合あなたは脱落する．

なお，このゲームではプレイヤーは全員正直である必要がある．

1.2 Love Letter の手札非公開処理

Love Letter において仮想プレイヤーを作ることを考えよう．仮想プレイヤーの手番になったら手札の 2 枚からランダムに 1 枚をめくって場に出す，という手法は誰でも思いつく．しかしながら，手札の内訳により 2 枚から選択すべ

ii 本稿で紹介するカードでは，7 のみこのタイミングで処理する．ここで脱落した場合，以降のステップを省略する．
iii 場に出したカードの効果を処理したことによって連鎖的に発生する効果もここで処理する．具体的には 5 の効果で捨てた 8 の効果が相当する．
iv 最大の数字のカードを持つプレイヤーが複数存在する場合は，そのすべてが勝利する．脱落していないプレイヤーがちょうど 1 人になった場合，そのプレイヤーがただちに勝利する．
v カードに記載されている本来の文面とは若干異なるが，本質的な違いはない．

き適切な手が変化するため，残念ながらこの手法を適用することはできない．

さらに，Love Letter では一部のカードの処理に手札情報が必要となる．仮想プレイヤーの作成を考えるにあたり，ここで手札情報を用いる必要のあるすべての処理を列挙する．

(1) 仮想プレイヤーが手札に 7 と 5 以上のカードを持った場合，7 の効果により直ちに脱落しなければならない．
(2) 仮想プレイヤーが別の仮想プレイヤーに対して 3 の効果を適用する場合，仮想プレイヤーの手札を見ずに大小比較を行わなければならない．
(3) 仮想プレイヤーに対して 1 の効果を適用する場合，宣言する数字が合っているかどうか，手札を見ずに判断できなければならない．

以下では（仮想ではない）通常のプレイヤーはすべて正直であると仮定するが，仮想プレイヤーの手番では，通常のプレイヤーが代わりにカードの操作を行うことになり，単純な仮想プレイヤーを想定するだけでは手札情報が必要となる上記の処理は実行不可能である．なお，これら 3 つ以外のカードの効果は，対象の手札情報を知らなくても，すなわち効果の対象が仮想プレイヤーであっても，問題なく処理できる．

まとめると，仮想プレイヤーの手札情報を秘密にしたまま Love Letter を実行するために必要な機能は，以下の 2 つに大別される．本稿ではこれらを実現することを考えたい．

- 仮想プレイヤーの 2 枚の手札の中身を見ずに適切な 1 枚を選択し場に出す
- 必要なカードの効果処理を手札の中身を見ずに実行する

なお本稿では，仮想プレイヤーが行うカードの効果において，対象プレイヤーの選択および任意の数の選択は一様ランダムに行うものとする（戦略的な選択手法については今後の課題とする）．

1.3 本稿の貢献

本稿では，2 枚の手札からルール上合法な，適切な 1 枚を秘密に選ぶことができ，カードの処理を秘密に行うことのできるような仮想プレイヤーを実現するプロトコルを与える．ゲームの流れとしては，通常プレイヤーと仮想のプレイヤーが混在しているとし，通常プレイヤーは自身で手番を行い，仮想プレイヤーの手番では，本稿で与えるプロトコルを用いて，手札を見ることなく通常プレイヤーが代わりに実行する．さらに，仮想プレイヤーの手札情報が必要なカード効果の適用については，本稿で与えるプロトコルを用いることで手札を見ることなく実行できる．**カードベース暗号** [5,7] の技術を活用し，以下の秘密計算プロトコルを構成する．

(1) **戦略適用プロトコル** 戦略に従って手札 2 枚から，表面の情報を秘匿したまま適切な 1 枚を選択でき，それを場に出すことができる．具体的には，2 枚のうちルール上出さなくてはならないカードや，明らかに出すべきカードがある場合はそれを選択でき，そうでない場合はランダムにいすれかを選択する．また，脱落が確定している場合はそのことを知る．
(2) **カード効果処理プロトコル** 相手手札の情報を見ることなく，手札情報に依存したカードの効果処理を適切に行うことができる．具体的には，1 と 3 のカードの効果処理を秘密に行う．

設計の主な方針は以下の通りである．ゲーム用の 16 枚の数字付きカードに，その数字に対応するような 8 枚の黒赤カードを紐つける．この束を**九枚束**と呼び，ゲーム中はこれを数字付きカード 1 枚とみなす．16 個の九枚束のセットを用いて，通常のようにゲームを行う．仮想プレイヤーの持つ手札は，通常プレイヤーが代わりとなってカードを秘匿したまま操作する．仮想プレイヤーの手番では山札から九枚束 1 つを引いた後，2 つの九枚束から，それぞれに紐付けられた 8 枚の黒赤カードを表面を見ずに取り出し，それらを入力としてどちらを出すべきか，戦略適用プロトコルを実行する．プロトコルにより選択された九枚束に含まれる数字付きカードを表向きにして公開し，その効果を処理する．仮想プレイヤーの手札情報が必要な効果を適用する場合，カード効果処理プロトコルを実行する．

ゲーム開始前に 16 個の九枚束を作成する．これは，図 3 のように，九枚束を 1 つのスリーブに入れることで簡単に実装できる．

図 3: カード束の実装例

提案手法では，ゲーム用数字付きカード 16 枚に紐付けられる黒赤カード $8 \times 16 = 128$ 枚のほかに，戦略適用プロトコルで使用する追加カードとして，黒のカード ♣ 28 枚と赤のカード ♥ 28 枚，数字カード 0 を 8 枚，1 から 8 を各 2 枚用いる（追加カード合計 80 枚）．カード効果処理プロトコルでは追加カード 80 枚の一部を再利用する．

また，必要なシャッフル回数は，戦略適用プロトコルを実行するごとに最大 4 回，カード効果処理プロトコルを実行するごとに最大 3 回である．

1.4 関連研究

カードベース暗号は物理的なカードを用いて様々な暗号機能を実現する技術であり，その応用としてカードゲームとの親和性が高いと考えられる．以下にそのような既存の応用例を列挙する．

まず，カードベース暗号を利用した，カードゲームの仮想プレイヤーを作り出すことのできるプロトコルとして，ババ抜きゲームに対するもの [11] がある．これは，手札の中に同じ数字のカードペアが存在すれば，それ以外の情報を隠したまま見つけることができ，ババ抜きで必要な処理を各プレイヤーの手札を見ずに行うことのできるものである．ババ抜きのようなゲームを一人でも楽しむことができる最初のゲームプレイヤープロトコルである．続いて，Ruangwises と Shinagawa はババ抜きプロトコルの発展型として，UNO カードゲームにおいて仮想プレイヤーを作り出すプロトコル [9] を提案した．

カードゲームではないが，Ikeda と Shinagawa は，本来出題者と解答者に分かれて最低 2 名で遊ぶことのできるヒットアンドブローゲームを，カードベース暗号の技術を用いて，出題者なしで遊ぶ手法 [3] を提案している．

ゲームの一部に利用するという点においては，人狼ゲームなどで使うことのできる，複数のプレイヤー集合を秘密に作成できるプロトコル [2]，タギロンというゲームにおいて一部の処理をカード公開せずに行うことのできるプロトコル [14] がある．また，2 人用ゲームの先手後手を決める際に，各プレイヤーの希望を秘密にしたまま，お互いの希望がうまく合えばその通りに決定し，そうでなければランダムに決めることのできるプロトコル [12] がある．

カードゲームのルール自体を新たに作り出す，という方向への応用例に，カードベース暗号による秘密計算を用いた新しいカードゲーム Gakmoro [6] がある．また，既存ゲームのインスタンスを新たに作り出す応用例に，15 パズルやルービックキューブに対して，必ず解くことのできる問題のみを生成できるプロトコル [10] がある．

1.5 本稿の構成

本稿の以下の構成は次の通りである．2 節では，カードベースプロトコルで使用するカードや，カード束のシャッフル操作，整数符号化について説明する．3 節では，1 つの戦略に対応して 2 つの手札から 1 つを秘密に選択することのできる戦略適用プロトコルを構成する．4 節では，Love Letter のための仮想プレイヤーを実現するために，カード効果処理プロトコルを構築し，プロトコルの全体を与える．最後に 5 節で本稿をまとめる．

2. 準備

本節では，本稿で提案するプロトコルで使用するカードと，使用するシャッフルであるパイルスクランブルシャッフル，既存の大小比較プロトコルを説明する．

2.1 使用カードと整数コミットメント

本稿で登場するプロトコルで用いられるカードは，1 節で見たように，黒カード（♣ ♣ ···）と赤カード（♥ ♥ ···）と，（ゲーム用数字付きカードとは異なるプロトコル用）数字カード（本稿では 0 から 8 を用いる）である．同じ表面絵柄のカードは互いに区別できないとし，これらのカードの裏面はすべて同じ模様 ? であるとする[vi]．以下では，裏に置かれたカード，例えば裏に置かれた 3 枚のカード ♣ 0 ♥ は，

? ? ?
♣ 0 ♥

のように書く．

本稿では 1 から 8 までの整数を，8 枚のカード ♣ ♥ の並びを用いて

♥ ♣ ♣ ♣ ♣ ♣ ♣ ♣ = 1
♣ ♥ ♣ ♣ ♣ ♣ ♣ ♣ = 2
♣ ♣ ♥ ♣ ♣ ♣ ♣ ♣ = 3
♣ ♣ ♣ ♥ ♣ ♣ ♣ ♣ = 4
♣ ♣ ♣ ♣ ♥ ♣ ♣ ♣ = 5
♣ ♣ ♣ ♣ ♣ ♥ ♣ ♣ = 6
♣ ♣ ♣ ♣ ♣ ♣ ♥ ♣ = 7
♣ ♣ ♣ ♣ ♣ ♣ ♣ ♥ = 8 (1)

の符号化ルールで扱うものとする [1]．符号化ルール (1) に従って，8 枚のカードを用いて整数 $x \in \{1,2,3,4,5,6,7,8\}$ が裏向きで表されているとき，裏に置かれた 8 枚のカードを x の**整数コミットメント**と呼ぶ．プロトコルに応じて，整数コミットメントは縦向きで並べられることもあり，左側から右側への並びが上から下になるように転置される．

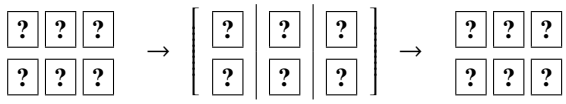
先に示したように，ゲーム開始前にゲーム用の数字付きカードに書かれた数と，符号化ルール (1) を対応させて九枚束を作成することになる．

2.2 パイルスクランブルシャッフル

本稿で登場するプロトコルで使用されるメインのシャッフルは，**パイルスクランブルシャッフル** [4] である．パイルスクランブルシャッフルは，大きさが等しい複数のカード束があるとき，各束を構成するカードの順序を変えずに束そのものを一様ランダムにかきまぜる．

例えば，2 枚のカード束 3 つに対してパイルスクランブルシャッフルを適用する場合，

[vi] 本稿で登場する黒赤カード，数字カードはそれぞれ同じ裏面模様とするが，16 枚のゲーム用数字付きカードとは裏面が異なっていてもよい．



のように書く[vii]．（ここでは縦に並んだ 2 枚が束である．）3 つの束を p_1, p_2, p_3 とし，元の並びが順に $p_1\ p_2\ p_3$ であれば，ランダムに 6 つのうちいずれかの並びになる．

$$p_1p_2p_3 \quad p_1p_3p_2 \quad p_2p_1p_3 \quad p_2p_3p_1 \quad p_3p_1p_2 \quad p_3p_2p_1$$

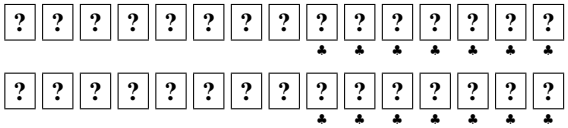
このシャッフルの具体的な実装方法としては，束 1 つ分のカード組を収容可能なカードスリーブを束の数だけ用意し，それぞれにカードを束ごと入れ，各スリーブの元の位置がわからなくなるまでかき混ぜればよい．

2.3 大小比較プロトコル

3 の効果を秘密に処理するためには，2 つの整数コミットメントの大小比較が必要となる．本稿では既存の手法 [6] を利用する．2 つの整数コミットメントを入力とし，どちらが大きいか（等しいか）を知ることができる．

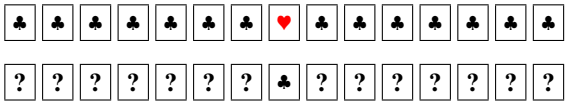
大小比較プロトコル [6]

(1) 2 つの整数コミットメントを 2 段に並べ，各段の右にダミーカードとして ♣ 7 枚を裏にして置く．



(2) 縦 2 枚の束 15 列に対して**パイルシフティングシャッフル** [8] を適用する．パイルシフティングシャッフルとは，各束を構成するカードの順序を変えずに，束そのものを巡回的に並べ替える操作である．

(3) 上の 15 枚をめくる．めくって唯一存在する ♥ の下のカードをめくり，♥ なら 2 つの整数コミットメントの表す値が同じことを知りプロトコルを終了する．
そうでなければ，上の ♥ が中央になるように列の構成を維持したまま巡回シフトして以下の列を得る．



(4) 下段でめくられている ♣ より左の 7 枚をシャッフルしてからすべてめくる．この中に ♥ があれば，上の整数コミットメントの値が大きいと知る．そうでなければ，下の整数コミットメントの値が大きいと知る．

シャッフル回数は，ステップ (2) と (4) でそれぞれ 1 回なので，2 つの入力が同値である場合は 1 回，そうでなければ合計 2 回である．

3. 戦略適用プロトコル

この節では，手札の 2 つの九枚束から戦略に応じて 1 つを選択できるプロトコルを与える．これを**戦略適用プロトコル**と呼ぶ．以下では手札のうち 1 つの九枚束を束 1，もう 1 つを束 2 と呼ぶ．九枚束は数字付きカード 1 枚とその数に対応する整数コミットメント 8 枚で構成されていることに注意する．

このプロトコルでは，まず前処理として 8 行 8 列の行列風に 64 通りの戦略を表として作成する．行は束 1，列は束 2 に対応している[viii]．各セルには束 1，束 2 のうちどちらを選択すべきか，基本的に 1 または 2 の数字で示される．片方が 7 で，手札にある時点で脱落が確定している（負ける）とき，この表では 0 と表現する．2 つのうちどちらを選んでも戦略的に違いがない場合はランダムに選択することとし，この表では $*$ と表現する．本稿では，こちらを選ぶと比較的有利になるだろう，とわかるもののみ選択を指定するが，実際のゲームでは，ゲームの前半，中盤，最終手番により取るべき戦略が変化する．これらに対応することは今後の課題である．

Pile 1 \ Pile 2	1	2	3	4	5	6	7	8
1	*	*	1	*	*	1	*	1
2	*	*	1	*	*	*	*	1
3	2	2	*	2	*	1	1	1
4	*	*	1	*	*	1	1	1
5	*	*	*	*	*	1	0	1
6	2	*	2	2	2	*	0	1
7	*	*	2	2	0	0	0	0
8	2	2	2	2	2	2	0	0

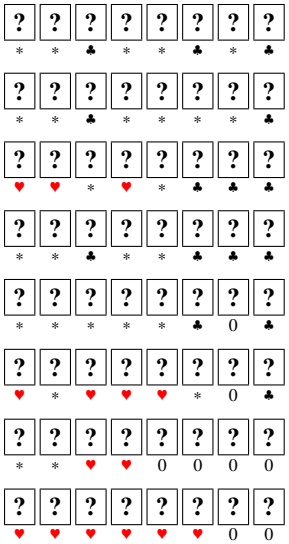
このような戦略を表にしたものを用いて，戦略適用プロトコルを実行する．

[vii] 左側のシャッフル前，右側のシャッフル後の（カード束たちの）記述は省略することもある．

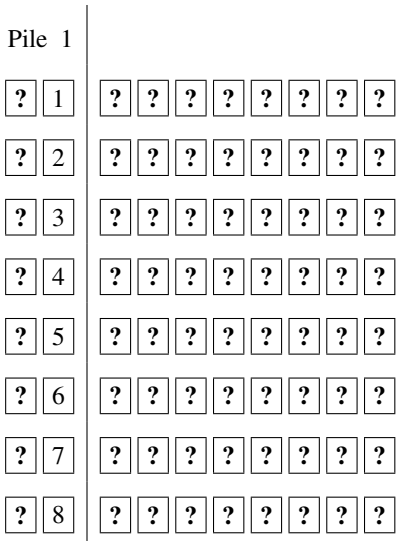
[viii] 6，7，8 についてはそれぞれ数字付きカードが 1 枚しか存在しないので手札の 2 つの九枚束が両方同じになることはあり得ないが，秘密漏洩を防ぐためすべてのセルを作成する．

戦略適用プロトコル

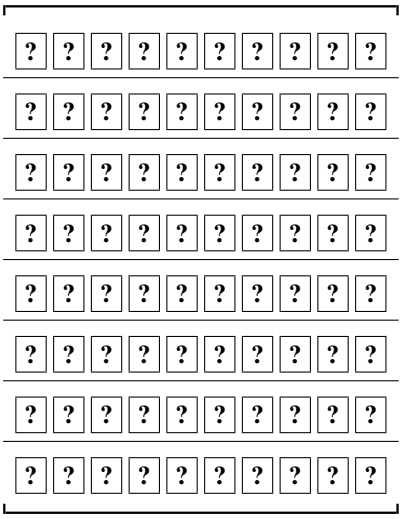
(1) 戦略表に従って，追加カード 64 枚を 8×8 の行列風に並べる．表のセルの 1 の箇所には ♣ を，2 の箇所には ♥ を，0 の箇所には 0 を，＊ の箇所にはランダムになるようにシャッフルしてから ♣ または ♥ を，それぞれ裏向きで置く[ix]．



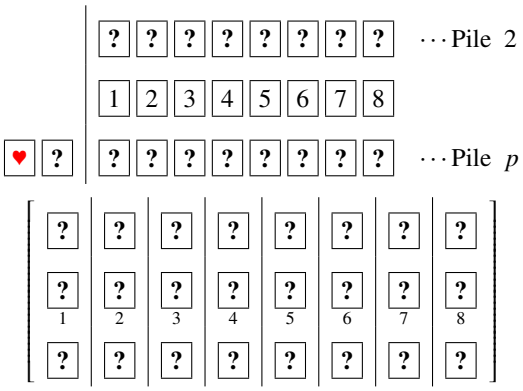
(2) 束 1 の整数コミットメントを構成するカードと，1 から 8 までの数字カードを対応させて縦向きで行列の左に並べる．各行をカード束として行 8 つに対してパイルスクランブルシャッフルを適用する．



[ix] 実装上は，♣ ♥ をそれぞれ*セル数の半分の枚数だけ用意してシャッフルし，ランダムになるように置けばよい．

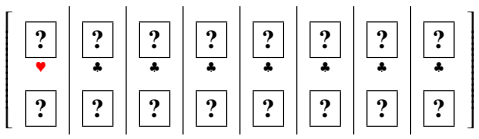


(3) 各行の左のカードをめくり ♥ が出現するカード束を Pile p とする．束 2 の整数コミットメント，1 から 8 までの数字カード，Pile p の右 8 枚のカードの順に上下に並べる．各列 3 枚をカード束として列 8 つに対してパイルスクランブルシャッフルを適用する．



(4) 一番上のカード 8 枚をめくり ♥ となるカード束の一番下のカードもめくる．♣ であれば束 1 の数字付きカードを，♥ であれば束 2 のものを，それぞれ選択対象とする．下のカードが 0 であれば，(7 の効果を処理したものとして) 束 1，束 2 (の数字付きカード) を両方ともめくって捨て札にし，その仮想プレイヤーを脱落させる．

(5) 仮想プレイヤーが脱落していなければ，選択対象とならなかったカードを九枚束として手札に戻す必要がある．そのため，以下のようにして秘匿したまま元に戻す．手札に戻す整数コミットメントの構成カード (表になっているものはめくって裏向きにする) とそれに対応する裏向きの 1 から 8 までの (プロトコル用) 数字カードのペア 2 枚 8 組に対して，パイルスクランブルシャッフルを適用する．



その後，数字カードのみをめくり，数字の順に整数コ

ミットメントの構成カードを裏向きのまま並べ直し，元の九枚束を復元する．

プロトコル終了後，使用したすべての裏面の追加カードをシャッフルしてからめくり，それ以降の別のプロトコル実行時の追加カードとして再利用する．

戦略適用プロトコル 1 回の実行に必要なシャッフル回数は，ステップ（1）で 1 回，ステップ（2），ステップ（3），ステップ（5）でそれぞれパイルスクランブルシャッフル 1 回の合計 4 回となり，ステップ（5）を実行しない場合は合計 3 回となる．

4. Love Letter の仮想プレイヤープロトコル

この節ではまず Love Letter のカード効果を秘密に処理できるプロトコルを与える．具体的には，4.1 節で与えるプロトコルを適用することで，1 の効果を手札を見ることなく秘密に処理する．2 の効果は手札を見るだけであり，3 の効果は大小比較プロトコルを適用する．7 の効果は戦略適用プロトコルにより処理し，残りの 4 5 6 8 の効果の処理には手札情報を必要としない．

これと，前節の戦略適用プロトコルを組み合わせて 4.2 節で仮想プレイヤーが存在する場合のゲーム全体のプロトコルを与える．

4.1 カード効果処理プロトコル

この節では，1 の効果の対象のプレイヤーが仮想プレイヤーであっても，その手札情報を秘匿したまま処理できるプロトコルを示す．また，3 の処理について言及する．

1 の処理では，効果の対象となったプレイヤーの手札が，宣言した数と等しいかどうかを知る必要がある．以下の通りにして，手札の九枚束に含まれる整数コミットメント 8 枚を用いて，シャッフル操作なしで実行できる．

整数コミットメント 8 枚のうち，左から宣言した数に等しい順番のカード 1 枚をめくり表にする．その絵柄が ♥ であれば（宣言数が合っていたことになるので）対象のプレイヤーの手札を公開し捨て，そのプレイヤーを脱落させる．♣ であれば（宣言数が異なっていたことになるので）再度めくり裏向きにして，8 枚の整数コミットメントを元の九枚束に戻す．

3 の処理は，2 人のプレイヤーの手札の九枚束の整数コミットメント 8 枚それぞれを入力とし，2.3 節で示した大小比較プロトコル [6] を実行すればよい．詳細は省略するが，既存プロトコルに，整数コミットメントを元に戻すテクニックを追加することにより，シャッフル回数最大 3 回で実行できる．

4.2 プロトコルの全体

以下に，提案する Love Letter の仮想プレイヤープロトコルの全体を示す．

***Love Letter* の仮想プレイヤープロトコル**

16 個の九枚束のセットを裏向きのままかき混ぜ，各プレイヤーに対して手札として 1 つ配布する．通常プレイヤーは手札を自分だけ確認する．仮想のプレイヤーの手札は伏せたままにしておく．余りの九枚束のセットから 1 つ取り除き，その残りで山札を作成する．手番プレイヤーをランダムに決めてゲームを開始する．ゲームの途中で，カード効果によりいずれかのプレイヤーが脱落した場合，そのプレイヤーの手札があれば表にして捨て札にする．そのプレイヤーが手番プレイヤーであれば直ちに次のプレイヤーの手番となる．

(1) 手番プレイヤーが通常プレイヤーであれば，山札から九枚束を 1 つ引いて手札に加えてから手番を行う．仮想プレイヤーに対して 2 3 5 6 のいずれかの効果を使用する場合，カード効果に従って手番プレイヤーが仮想プレイヤーの手札を操作する．仮想プレイヤーに対して 1 の効果を使用する場合，カード効果処理プロトコルに従って手札を操作する．

(2) 手番プレイヤーが仮想プレイヤーであれば，通常プレイヤーの 1 人が代わりとなって，山札から引いた九枚束 1 つを裏向きのまま手札に加え，以下のように動く．

(a) 手札の九枚束 2 つに紐付けられた整数コミットメントを使用して，戦略適用プロトコルを実行する．

(b) 戦略適用プロトコルにより選択された数字付きカードを場に出し，そのカード効果を処理する[x]．1 または 3 の効果を別の仮想プレイヤーに使用する場合は，カード効果処理プロトコルに従う．

(3) 脱落せずに残ったプレイヤーが 1 人となった場合はそのプレイヤーが直ちに勝利する．山札がなくなった場合はそのプレイヤーの手番終了後，脱落せずに残った全プレイヤーの手札を公開し，最も数字の大きいプレイヤー（たち）が勝利する．いずれでもない場合は，次のプレイヤーの手番として最初のステップに戻る．

シャッフル回数は，戦略適用プロトコルの実行には最大 4 回必要で，カード効果処理プロトコルの実行には最大 3 回必要となるので，仮想プレイヤーが 1 つの手番を実行するごとに最大 7 回となる．

5. おわりに

本稿では，カードベース暗号のカードゲームに対する応用の 1 つとして，Love Letter における仮想プレイヤープロトコルを構成した．提案手法は正直なプレイヤーを仮定したが，少しのプロトコルを追加することにより、通常プレイヤーが不正を行う可能性のある場合であっても，不正行為を完全に見つけることのできるモデルに変更することが

[x] 前述した通り，本稿ではカードの効果の対象プレイヤーや，1 の効果で宣言する数はランダムに選ばれるものとする．

可能である．

提案プロトコルは，使用するカード枚数は少なくはないが簡単な構成で，非専門家に対しても分かりやすいと考えられ，秘密計算の仕組みや安全性についての直感的な理解を促すツール [13] として有用であり，教育的な価値が期待できる．より直接的には，世界の各地に存在する Love Letter のユーザコミュニティに秘密計算技術の存在をアピールできることが期待できる．

本文でも示したが，場面に応じた手札選択の戦略や，カード効果の使用時に選択すべきプレイヤーの戦略を組み込むことは今後の課題である．

謝辞 本研究の一部は JSPS 科研費 JP23H00479 と JP24K02938 の助成を受けている．

参考文献

[1] Crépeau, C. and Kilian, J.: Discreet Solitary Games, *Advances in Cryptology—CRYPTO' 93*, LNCS, Vol. 773, Berlin, Heidelberg, Springer, pp. 319–330 (1994).

[2] Hashimoto, Y., Shinagawa, K., Nuida, K., Inamura, M. and Hanaoka, G.: Secure Grouping Protocol Using a Deck of Cards, *IEICE Trans. Fundam.*, Vol. E101.A, No. 9, pp. 1512–1524 (2018).

[3] Ikeda, S. and Shinagawa, K.: How to Play Mastermind without Game Master, *Theory and Applications of Models of Computation*, LNCS, Cham, Springer (2025, to appear).

[4] Ishikawa, R., Chida, E. and Mizuki, T.: Efficient Card-Based Protocols for Generating a Hidden Random Permutation Without Fixed Points, *Unconventional Computation and Natural Computation*, LNCS, Vol. 9252, Cham, Springer, pp. 215–226 (2015).

[5] Koch, A.: The Landscape of Security from Physical Assumptions, *IEEE Information Theory Workshop*, NY, IEEE, pp. 1–6 (2021).

[6] Mizuki, T., Kuzuma, T., Hirano, T., Oshima, R. and Yasuda, M.: Gakmoro: An Application of Physical Secure Computation to Card Game, *Unconventional Computation and Natural Computation*, LNCS, Cham, Springer (2025, to appear).

[7] Mizuki, T. and Shizuya, H.: Computational Model of Card-Based Cryptographic Protocols and Its Applications, *IEICE Trans. Fundam.*, Vol. E100.A, No. 1, pp. 3–11 (2017).

[8] Nishimura, A., Hayashi, Y., Mizuki, T. and Sone, H.: Pile-shifting scramble for card-based protocols, *IEICE Trans. Fundam.*, Vol. 101, No. 9, pp. 1494–1502 (2018).

[9] Ruangwises, S. and Shinagawa, K.: Simulating Virtual Players for UNO without Computers, *Unconventional Computation and Natural Computation*, LNCS, Cham, Springer (2025, to appear).

[10] Shinagawa, K., Kanai, K., Miyamoto, K. and Nuida, K.: How to Covertly and Uniformly Scramble the 15 Puzzle and Rubik's Cube, *Fun with Algorithms*, LIPIcs, Vol. 291, Dagstuhl, Germany, Schloss Dagstuhl, pp. 30:1–30:15 (2024).

[11] Shinagawa, K., Miyahara, D. and Mizuki, T.: How to Play Old Maid with Virtual Players, *Theory of Computing Systems*, Vol. 69, No. 1 (2025).

[12] Shinoda, Y., Miyahara, D., Shinagawa, K., Mizuki, T. and Sone, H.: Card-Based Covert Lottery, *Innovative Security Solutions for Information Technology and Communications*, LNCS, Vol. 12596, Cham, Springer, pp. 257–270 (2021).

[13] 花岡悟一郎，岩本　貢，渡邉洋平，水木敬明，安部芳紀，品川和雅，新井美音，矢内直人：高機能暗号の社会展開を促進する物理・視覚暗号，電子情報通信学会論文誌 A, Vol. J106-A, No. 8, pp. 214–228 (2023).

[14] 小泉康一，水木敬明：タギロンカードゲームへの秘密計算の応用，信学技報，ISEC2025-10, pp. 40–47 (2025).