メッセージングアプリを用いて 物理オークションプロトコルを遠隔で行う方法

宮原 大輝[1,2,a)]　水木 敬明[3]　曽根 秀昭[3]

概要：カードベース暗号に代表される物理的暗号プロトコルは，代数学に関する知識を必要とせず，市販の道具などを用いて手軽に実行できることが特徴の 1 つである．しかし，物理的道具を用いる特性上，プロトコルの参加者は同一の場所にいる必要がある．本稿では，その容易に実行できるコンセプトを活かしつつ，遠隔でも実行できる暗号プロトコルを構築することを目的とする．具体的には，2014 年に Dreier らによって提案された封筒を用いる物理オークションプロトコルを発展させ，Facebook Messenger に代表されるメッセージングアプリを用いたオークションプロトコルを提案する．提案プロトコルでは，メッセージングアプリに搭載されている既読機能とグループチャット機能を活用している．提案プロトコルの安全性は，メッセージングアプリに脆弱性が無いこと（それを提供する第三者が恣意的に運用しないことも含む）を前提とした上で成り立ち，既存プロトコルの安全性も，用いる封筒に脆弱性が無いことを前提としており，両者の安全性要件の構造は同じである．メッセージングアプリを用いる提案方式は，参加者数や落札価格が大きな値であっても比較的容易に実行できる．

キーワード：暗号プロトコル，物理的暗号技術，オークション，メッセージングアプリ

How to Perform Physical Auction Protocol Remotely with Messaging App

Daiki Miyahara[1,2,a)]　Takaaki Mizuki[3]　Hideaki Sone[3]

Abstract: Cryptographic protocols using physical tools such as card-based cryptography enable us to easily achieve cryptographic tasks without the need for mathematical knowledge of algebra. However, all players participating in such a protocol are required to be in the same place because they use physical tools. In this paper, we focus on how to perform such a protocol remotely while keeping its property (i.e., it can be performed easily) consistent. Precisely, we propose an auction protocol with a messaging app such as Facebook Messenger, which extends the existing protocol with envelopes. Our idea is to utilize the read receipts and group chat features loaded in a messaging app. We note that security requirements between our proposed protocol and the existing protocol are similar; while our proposed protocol requires a messaging app used in the protocol to have no vulnerability, the existing protocol also requires physical tools to have no vulnerability.

Keywords: Cryptographic Protocol, Physical Cryptography, Auction, Messaging App

1. はじめに

物理的道具の特性を利用して秘密計算などの暗号機能を実現する方法として，カードベース暗号や Private PEZ プロトコルなどの**物理的暗号プロトコル**（娯楽暗号）が知ら

[1] 東北大学大学院情報科学研究科
Graduate School of Information Sciences, Tohoku University
[2] 産業技術総合研究所（AIST）
[3] 東北大学サイバーサイエンスセンター
Cyberscience Center, Tohoku University
[a)] daiki.miyahara.q4@dc.tohoku.ac.jp

れている．例えばカードベース暗号では，物理的なカード組の特性である裏になったカード列から表の絵柄は類推できないことを利用し，シャッフル操作やカードをめくる操作を巧みに組み合わせた暗号プロトコルが提案されている．

1.1 背景

物理的暗号プロトコルは，現代暗号で主に用いられる代数学の知識を一切用いず，親しみのある道具を用いて手軽に実行できることが大きな特徴である．しかしながら，物理的道具を用いる特性上，プロトコルに参加するプレーヤーは全員同一の場所にいなければならない．これまでの物理的暗号プロトコルに関する既存研究は，下で触れる Moran と Naor による方式 [1,2] 以外，全てこのことを仮定している．これは，物理的道具を用いて遠隔で実行するプロトコルを構築することが困難であることを意味している．

Moran と Naor は，不正開封防止シール（tamper-evident seal）付き封筒の送受信による否認可能なアンケート方式 [1] の提案と，その封筒を用いたコイントスと紛失通信方式の実現（不）可能性 [2] の証明を行った．彼らの提案方式は，汎用的結合可能性（Universal Composability）を満たす暗号プロトコルの構築における不正開封防止シールの有用性を示した反面，その構成は複雑である（実際に実行した結果もこれまで報告されていない[i]）．封筒の送受信を行うという観点からも，以下の 3 つの懸念事項が挙げられる．

第三者機関と費用　封筒の郵送を行う第三者の信頼できる機関（郵便局や運送会社など）が必要である．そのような郵送を行う公共機関が顧客の荷物を盗み見したり顧客と結託したりすることは通常考えられないので，そのような機関を無条件に信頼することは自然である．しかし，そのサービスを利用するにあたって生じる費用を誰が負担するのかという問題はある．

実行時間　プロトコルが終了するまでに多くの日数を必要とする．新特急郵便[ii]のように当日配送を行うサービス（地域は限られるが）を利用すれば 1 日でプロトコルを終了できる場合もあるが，プロトコルで封筒の通信回数が 2 回以上必要になる場合は，1 日でプロトコルを終了させることは不可能である．これは，気軽に実行できる物理的暗号プロトコルのコンセプトから逸脱する．

シール付き封筒の偽造　不正開封防止シールは，プロトコルで指定された場面以外で封筒が不正に開封されるのを防ぐ役割がある．しかし，送られてきたシール付き封筒そのものを受信者が偽造できたとしたら，プロトコルは根本的に成立しないことになる．例えば，2 つのシール付き封筒が受信者に届き，受信者はその内の 1 つをランダムに空け，もう 1 つは空けずに送信者に返す場面を想像しよう．受信者がもしもその封筒を偽造できたとしたら，受信者は送られてきた封筒を 2 つとも開封し，その内のどちらを送信者に返すか選ぶことができる．すなわち，不正開封防止シールの役割を根底から崩すことができてしまう．したがって，封筒の送受信を行うプロトコルには封筒の偽造不可能性（unforgeability）が要求される．[iii]

以上の懸念事項が Moran と Naor の方式に存在するが，これらは物理的道具を用いるという性質上避けられない問題であると考えられる．

1.2 貢献

上記の背景を鑑み，本研究では，物理的暗号プロトコルの「代数学を用いない」特徴は維持しつつ，遠隔でも容易に実行できる新たな方式の構築を目指す．主なアイデアは，**オンラインアプリ**を活用することである．市販されているカード組や PEZ ディスペンサを用いる既存研究と同様に，オンラインアプリはスマートフォンの普及によって今や当たり前に使われるほど親しみのある機能である．

本稿では，2014 年に Dreier ら [5] によって提案された封筒や特殊な木箱を用いる**物理オークションプロトコル**を発展させ，Facebook Messenger や LINE に代表される**メッセージングアプリ**を用いれば遠隔でプロトコルを実行できることを示す．提案方式は，メッセージングアプリに通常搭載されている既読機能とグループチャット機能を活用している．そのような機能を有するメッセージングアプリを $\mathcal{F}_{\mathrm{MA}}$ として 3 節で形式的に記述する．

後で触れるように，1.1 節で指摘した 3 つの懸念事項を提案方式は解決または改善している．実行するのに必要な費用は通信費用だけであり，実行時間は郵送の場合に比べ大幅に改善される（実行時間については 5 節で詳しく触れる）．送信するメッセージを偽造することは（送信元が常に通知されるので）原理的に不可能である．物理的暗号プロトコルに比べ，提案方式はプロトコルの参加者数や落札価格が大きい場合も対処できることを 5 節で述べる．

提案方式の安全性は，用いるメッセージングアプリに脆弱性が存在しないという仮定の下で安全である．加えて，メッセージングアプリを提供する第三者が恣意的に運用（例えば，メッセージの中身を盗み見したりユーザーと結託したりすること）しないことも含む．これは 1.1 節で述べたように，Moran と Naor による方式 [1,2] の安全性が，郵送を行う第三者が無条件に信頼できることや用いるシール付きの封筒が偽造不可能性を満たす仮定の下で成り立つという構造と同様である．したがって，両方式において前

[i] 例えばカードベース暗号では，実行時間の解析 [3] や置換エラーに基づく安全性解析 [4] が行われている．

[ii] 新特急郵便は 834 円で利用可能である（2020 年 8 月 20 日現在）．

[iii] Moran と Naor の文献 [1,2] では，この偽造不可能性については僅かしか触れられていない．

提となる安全性要件は大差ないことが言える．

なぜ秘密計算を対象にしないのか

カードベース暗号が主に扱う論理演算の秘密計算は，本研究の対象にしなかった．既読機能を有するメッセージは，暗号学におけるコミットメントと似た機能を持つと捉えられる．コミットメントの存在（すなわち一方向関数の存在）を仮定するだけでは任意の秘密計算を実現できないため，メッセージングアプリを用いて論理演算の秘密計算を行うカードベース暗号プロトコルを実現することは（カードベース暗号で用いられるシャッフル機能のような直接的な機能がアプリに搭載されない限り）不可能である．[iv]

1.3 構成

本稿の構成は以下の通りである．2 節では，Dreier らの既存方式 [5] を紹介し，オークションプロトコルが満たすべき性質を挙げる．3 節では，提案方式が用いるメッセージングアプリ機能 $\mathcal{F}_{\mathrm{MA}}$ を形式的に記述する．4 節では，メッセージングアプリを用いるオークションプロトコルを示す．5 節では，提案方式において参加者数や落札価格が大きい場合と，実行時間に関する考察を行う．6 節で本稿をまとめる．7 節に本研究における倫理的配慮を示す．

1.4 関連研究

本研究のようにオンラインアプリを用いて暗号プロトコルを構成する既存研究は，著者らの既存研究以外に存在しない．

Private PEZ プロトコルでは，2003 年の提案 [6] 以来初めての改善が Abe ら [7] によって成され，今後の発展が強く期待される．

カードベース暗号では，2020 年に著者らによってトランプカード組を用いる金持ち比べプロトコル [8]，ランダムカットのみを用いる 6 枚 XOR プロトコル [9]，数独パズルに対するゼロ知識証明プロトコルの改良版 [10]，タクズと縦横さんパズルに対するゼロ知識証明プロトコル [11] が提案されている．また，2020 年に Yasunaga [12] による効率的な 3 変数多数決関数プロトコル，Ruangwises と Itoh [13] によるナンバーリンクパズルに対するゼロ知識証明プロトコル，Koch と Walzer [14] による能動的安全なカードベースプロトコルが示されている．

2. 既存の物理オークションプロトコル

本節では，Dreier ら [5] が 2014 年に提案した物理オークション方式（Envelopako[v] と呼ばれる）の概要を説明し，オークションプロトコルが満たすべき性質を挙げる．

2.1 概要

この方式は封印入札方式であり，入札者は m 個の入札可能価格 $p_m > p_{m-1} > \cdots > p_1$ から 1 つを選んで入札を行う．オークションの開催者は，一番大きな価格を入札した人（勝者）とその価格を入札者と一緒に開示していく．プロトコルの流れは次の通りである．

準備　入札者はそれぞれ，m 枚の紙と m 個の封筒を準備する．i 枚目の紙の左側には価格 p_i が書かれていて，右側には “Yes” と “No” が書かれている．封筒は左側が透明であり，紙を入れると価格のみが見える．

入札　入札者は入札したい価格が書かれた紙の “Yes” にマークを付け，それ以外は “No” にマークを付ける．それら m 枚の紙を m 個の封筒にそれぞれ入れ，封筒を閉じ，それらをテーブルに置く．

開示　主催者は入札者の目の前で p_m に対応する封筒を全て開ける．もし “’Yes” にマークが付いた紙が出てきた場合，その封筒を置いた入札者が勝者[vi]である．全ての紙が “No” であった場合，p_{m-1} に対応する封筒を開け，同様のことを行っていく．

既存方式の原理は，入札者が入札価格を m 桁のビット列で表したとき，主催者は最上位ビットから開示していくことで一番大きな入札価格だけを見つけられることである．1999 年に Kikuchi ら [16] は，この原理に基づいた秘密分散方式を用いるプロトコルを提案している．

2.2 安全性

上で説明した既存方式 [5] は，主催者と入札者が semi-honest である仮定の下で，オークションプロトコルが満たすべき性質である**否認不可能性**，**公平性**，**検証可能性**及び**プライバシー**を以下に示すように全て満たしている．ただし，物理的暗号プロトコルではプレーヤーが不正に行動しないよう互いに監視できるため，semi-honest よりも弱い設定を仮定できる．例えば，不正を行った事実が他のプレーヤーに漏れることを避ける covert な設定が挙げられる．

否認不可能性　この性質は，プロトコルによって判明した勝者が落札価格を否定できないことを意味する．既存方式では，入札価格を表す封筒は公衆の場でテーブルに置かれるため，勝者が落札価格を否定することはできない．

公平性　この性質は，開示が行われるまで入札者が他の入札者の入札価格に関する情報を一切得られないことを意味する．既存方式では，入札者は他の入札者には見

[iv] Moran と Naor [2] が互いに区別のつく封筒では紛失通信を実現できないと証明したのと同じように，シャッフル操作が必要なカードベースプロトコルをメッセージングアプリを用いて実現するのは（現状）不可能である．本稿で対象にした物理オークションプロトコルは，後で見るように，シャッフル操作を用いずに実現できるため，メッセージングアプリを用いて実現できるのだと考えられる．

[v] Envelope を用いた Sako のプロトコル [15] の実装．

[vi] 勝者が複数いる場合は，価格設定を変えて勝者だけで再びオークションを行えば良い．

えないように紙にマークを付けるため，他の入札者に情報が漏れることはない．

検証可能性　この性質は，開示で得られる勝者と落札価格を入札者が検証できることを意味する．既存方式では，開示は公衆の場で行われるため，入札者は主催者と同じように勝者と落札価格を見つけられる．

プライバシー　この性質は，オークションの敗者の入札価格に関する情報が必要以上に漏れないことを意味する．既存方式では，勝者が判明した後に封筒を全て破棄すれば必ずプライバシーが保たれる．

3. メッセージングアプリの形式的記述

本節では，n 人のプレーヤー $P_1, P_2, \ldots, P_n$ 間で動作するメッセージングアプリの機能 $\mathcal{F}_{\mathrm{MA}}$ を定義する．本稿が対象とするメッセージングアプリは，メッセージの送受信に加え，既読機能とグループチャット機能を有する．すなわち，送信されたメッセージの内容を受信者が確認した途端に，送信者はそのことを（受信者の意思に関係なく）知ることができる．あらかじめプレーヤー間でグループを作成しておくと，送信者はグループに含まれているプレーヤー全員にメッセージを送信することができ，グループ内のプレーヤーはその内容を自由に確認できる．メッセージを受信したこと自体は内容を確認せずに受信者は知ることができることに注意されたい．

本稿では，**メッセージ**を組 $\mathsf{msg} = (c, Q)$ と定義する．ここで，$c \in \mathcal{M}$ は msg の内容であり，$\mathcal{M}$ はメッセージ空間である．$Q \subseteq \{P_1, \ldots, P_n\}$ は，msg を既に読んだ（すなわち，c を知っている）プレーヤーの集合を表す．後で示すように，送信者は Q そのものを知ることはできないが，その人数 $|Q|$ を常に知ることができる．

メッセージの定義を元に，n 人のプレーヤー $P_1, P_2, \ldots, P_n$ 間で動作するメッセージングアプリの機能 $\mathcal{F}_{\mathrm{MA}}$ を次のように定義する．

(Make, name, P_i, $\{P_{i_1}, P_{i_2}, \ldots, P_{i_\ell}\}$**)**　このコマンドは P_i によって開始される．P_i は集合 $\{P_{i_1}, P_{i_2}, \ldots, P_{i_\ell}\} \cup \{P_i\}$ から成るグループを作成する．そのグループの名前は name である．もし名前が name のグループが既に存在していた場合，$\{P_{i_1}, P_{i_2}, \ldots, P_{i_\ell}\}$ をそのグループに属するプレイヤーとして追加する．

(Send, id, name, P_i, msg**).**　このコマンドは P_i によって開始される．P_i は，id によってラベルされた msg を，名前が name のグループに送信する．そのグループに属するプレーヤーは，P_i が msg を送信した事実だけを知る．後に示すように，P_i は（いつでも）msg が何人に読まれたかどうかを検証できる．

(Read, name, P_j**)**　名前が name のグループに送信された全てのメッセージを

$$\mathsf{msg}_1 = (c_1, Q_1), \mathsf{msg}_2 = (c_2, Q_2), \ldots, \mathsf{msg}_t = (c_t, Q_t)$$

とする．このコマンドは（名前が name のグループに属する）P_j によって開始される．全ての $k \in \{1, 2, \ldots, t\}$ に対し，P_j は c_k を知り，$Q_k \leftarrow Q_k \cup \{P_j\}$ へと更新される[vii]．あるメッセージ msg_ℓ が既に削除されていた場合，P_j は c_ℓ を知ることができない（しかし msg_ℓ が送信者によって削除された事実を知る）．

(Verify, id, P_i**)**　id によってラベルされたメッセージを $\mathsf{msg} = (c, Q)$ とする．すなわち，(**Send**, id, name, P_i, msg) によって送信されたものとする．このコマンドは P_i によって開始される（そして msg の $|Q|$ を返す）．P_i は msg の $|Q|$（すなわち，名前が name のグループに属する何人のプレーヤーが c を知っているか）を知る．

(Delete, id, P_i**)**　$\mathsf{msg} = (c, Q)$ が (**Send**, id, name, P_i, msg) によって送信されたものとする．このコマンドは P_i によって開始される．P_i は id によってラベルされた msg を削除し，受信者が c を知ることを防げる．前述したように，そのグループに属するプレーヤーは既に P_i が msg を送信したことを知っているため，P_i は msg を送信した事実を隠すことができない．

1.2 節で述べたように，メッセージングアプリには脆弱性が存在しないと仮定しているため，上で定義した $\mathcal{F}_{\mathrm{MA}}$ に攻撃者が入り込む余地はなく，$\mathcal{F}_{\mathrm{MA}}$ は常に上の 5 つのコマンドによって動作する．

既読を付けずに読む方法について

例えば，送信されたメッセージを機内モードやポップアップ表示を介して確認することで，既読を付けずに内容を確認できると考える人もいるかもしれない．実際，送信するメッセージの形態がテキストや画像である場合は，そのような方法で既読を付けずに内容を確認できる．しかしながら，メッセージの形態を動画にすると，機内モードでは動画を再生できないことを第一著者は（Facebook Messenger と LINE で）確認している．これは，メッセージの形態が動画であった場合，利用者の帯域を節約するために，動画を再生するまでは動画はサーバに留まるためであると考えられる．[viii]

既読を付けずに送信と削除を行う方法について

$\mathcal{F}_{\mathrm{MA}}$ の **Send** コマンドと **Delete** コマンドでは，プレーヤーが既読を付けずにメッセージを送信及び削除できるとしている．しかしながら，それらの操作を行う際はグループチャットを開く必要があるため，そのグループチャット内に送信されたメッセージに自動的に既読が付いてしまうことが通常である．これを防ぐためには，メッセージを送

[vii] P_j はグループに送信された特定のメッセージの内容だけを知ることはできないことに注意しよう．

[viii] 最も有名なメッセージングアプリである WhatsApp では，動画であっても既読を付けずに再生できることを確かめられたため，$\mathcal{F}_{\mathrm{MA}}$ を実現できない．

信及び削除する際に，機内モードに設定してからグループチャットを開いて送信及び削除を行い，アプリを終了した後に機内モードを解除すれば，既読を付けずに送信及び削除できることを第一著者は確認している．

4. 提案方式

本節では，3 節で定義したメッセージングアプリの機能 $\mathcal{F}_{\mathrm{MA}}$ を利用したオークションプロトコルを提案する．オークションの勝者と落札価格を見つける原理は 2 節で紹介した既存方式 [5] と同様であり，最上位ビットから入札価格を開示していくことで計算を行う．封筒を用いる既存方式を単純に郵送で行えば遠隔で実行できると考える人もいるかもしれないが，郵送の場合，開示の場面で主催者が最上位ビットから正しく開示を行ったかどうかを検証するのが難しいことが直ちに分かる．すなわち，郵送では検証可能性を満たすのが難しい．提案方式のアイデアは，主催者と入札者から成るグループを価格毎にメッセージングアプリで作成することで，主催者が最上位ビットから開示したことを（同じグループに属する）入札者が後から検証できることである．

4.1 概要

主催者を A で表し，入札者を $S_1, S_2, \ldots, S_n$ で表す．入札可能価格は $p_m < p_{m-1} < \cdots < p_1$ とする．提案方式の流れを以下に自然言語で示し，3 節で定義した $\mathcal{F}_{\mathrm{MA}}$ を用いる厳密な記述を 4.3 節で行う．

準備 主催者 A は入札者 $S_1, S_2, \ldots, S_n$ と m 個のグループをメッセージングアプリ上で作成する．それぞれのグループの名前は p_i とする（$1 \leq i \leq m$）．

入札 入札者 S_j の入札価格を $p_{j'}$ とする（$1 \leq j \leq m$）．S_j は名前が $p_{j'}$ のグループに 1 を表すメッセージを（動画で）送信[ix]し，それ以外のグループには 0 を表すメッセージを送信する．

開示 主催者 A は名前が p_m のグループに送信されたメッセージを全て読む．もし 1 を表すメッセージがある場合，そのメッセージの送信者が勝者であり，勝者と落札価格を入札者に（任意の手段で）伝える．そうでない場合，名前が p_{m-1} のグループを確認し，同様のことを行っていく．もし削除されたメッセージが存在した場合，プロトコルを中止する．

検証 入札者 S_j は，落札価格以上の価格に対応するグループに送信された全てのメッセージを読み，勝者と落札価格を検証する．落札価格より小さい価格に対応するグループでは，既読が 0 であることを検証する．もしそうでない場合，プロトコルを中止する．

削除 入札者 S_j は，落札価格より小さい価格に対応するグループに送信した全てのメッセージを削除する．

4.2 安全性

上で示した提案方式は，covert な設定の下で，否認不可能性，公平性，検証可能性及びプライバシーを以下に示すように全て満たしている．

否認不可能性 送信するメッセージは偽造不可能であるため，勝者が落札価格を否定することはできない．

公平性 入札者は，自分が送信した（落札価格より小さい価格に対応する）メッセージを他の入札者が読んでいないことを既読機能を用いて検証できる．したがって，他の入札者が自分の入札価格に関する情報を元に入札していないことが保証される．

検証可能性 入札価格以上の価格に対応するグループに送信されたメッセージを開示後に読むことで，開示が正しく行われたことを入札者全員が検証できる．

プライバシー 公平性と同様に，入札者が，自分が送信した（落札価格より小さい価格に対応する）メッセージを誰も読んでいないことを検証できるため，敗者の入札価格に関する情報は漏れないことが保証される．それらのメッセージを削除すれば，誰も入札価格を知り得ない．ただし，既読を付けたプレーヤーを特定できないため，誰が不正を行ったか特定できない問題は存在する．

4.3 形式的な記述

提案方式の形式的な記述をアルゴリズム 1 に示す．ここで，$\mathsf{text} \in \mathcal{M}$ に対し，$(\mathbf{Tell}, P_i, P_j, \mathsf{text})$ は P_i が text を任意の手段で P_j に伝えることを意味する．

5. ディスカッション

本節では，4 節で示した提案方式の実行時間が，封筒を用いる既存方式 [5] に比べ大幅に改善されることと，参加者数や落札可能価格が大きい場合にも対処できることを述べる．

2 節で紹介した既存方式 [5] では，入札者は m 枚の紙と m 個の封筒を用意し，紙に印を付けた後にそれらを封筒に入れる必要があることを思い出そう．当然，m が大きいと時間を要し，そもそも必要な紙と封筒を揃える手間もかかる．（これは既存方式に限らず，物理的暗号プロトコル全般の課題である．）提案方式はメッセージングアプリを使用するため，メッセージとなる動画を（0 と 1 を表す 2 種類）準備するだけで良く，送信はコピー＆ペーストで十分である．開示では，主催者が封筒を実際に開けて確認する手間と，動画を再生する手間を詳細に検証する必要があり，今後の課題であるが，一般的には動画を再生する方が手間が少ないように考えられる．検証と削除についても詳細な検証が必要である．既存方式では敗者の封筒を除外する必

ix 例えば，1 を書いた紙を動画で撮影すれば良い．

Algorithm 1. Message-app-based auction protocol.

(1) **for** $i = 1$ to m **do**
(2) $\quad$ $(\mathbf{Make}, p_i, A, \{S_1, \ldots, S_n\})$
(3) **for** $i = 1$ to n **do**
(4) $\quad$ $\left(\mathbf{Send}, S_i^{i'}, p_{i'}, S_i, (1, \emptyset)\right)$ where $p_{i'}$ denotes the bid of S_i
(5) $\quad$ **for** $j = 1$ to m **do**
(6) $\quad\quad$ **if** $j \neq i'$ **then**
(7) $\quad\quad\quad$ $\left(\mathbf{Send}, S_i^j, p_j, S_i, (0, \emptyset)\right)$
(8) **for** $i = 0$ to $i = m - 1$ **do**
(9) $\quad$ $(\mathbf{Read}, p_{m-i}, A)$
(10) $\quad$ Let W be the set of sellers S_ℓ that performed $\left(\mathbf{Send}, S_\ell^{m-i}, p_{m-i}, S_\ell, (1, \emptyset)\right)$ for some $\ell \in \{1, \ldots, n\}$
(11) $\quad$ **if** $W \neq \emptyset$ **then**
(12) $\quad\quad$ **for** $j = 1$ to m **do**
(13) $\quad\quad\quad$ $(\mathbf{Tell}, A, S_j, W$ and $p_{m-i})$
(14) $\quad\quad$ A outputs W and p_{m-i}
(15) $\quad\quad$ Let k be $m - i$
(16) $\quad\quad$ **break**
(17) **for** $i = 1$ to $i = n$ **do**
(18) $\quad$ **for** $j = k$ to $j = m$ **do**
(19) $\quad\quad$ $(\mathbf{Read}, p_j, S_i)$
(20) $\quad\quad$ **if** there exists a seller S_ℓ that performed $\left(\mathbf{Send}, S_\ell^j, p_j, S_\ell, (1, \emptyset)\right)$ for some $\ell \in \{1, \ldots, n\}$ such that $j \neq k$ **then**
(21) $\quad\quad\quad$ S_i outputs $\perp$
(22) $\quad$ **for** $j = 1$ to $j = k - 1$ **do**
(23) $\quad\quad$ **if** $(\mathbf{Verify}, S_i^j, S_i) > 0$ **then**
(24) $\quad\quad\quad$ S_i outputs $\perp$
(25) **for** $i = 1$ to $i = n$ **do**
(26) $\quad$ **for** $j = 1$ to $j = k - 1$ **do**
(27) $\quad\quad$ $(\mathbf{Delete}, S_i^j, S_i)$
(28) $\quad$ S_i outputs W and p_k

要があるが，その除外方法は曖昧である．提案方式はメッセージを（**Delete** コマンドで）削除すれば良く，敗者の入札価格が漏れることはない．

送信 API[x]を用いれば，入札が簡便になると考えられる．API を使用して操作を自動化できるのはオンラインアプリの強みである．ただし，開示と検証は主催者と入札者が実際にメッセージを確認する必要があるため，自動化は不可能であるように思える．API を使用して提案方式を実行し，その詳細な実行時間を検証することは今後の課題である．

6. おわりに

本稿では，既読機能とグループチャット機能を有するメッセージングアプリの機能を定義し，それを用いるオークションプロトコルを提案した．提案プロトコルは，物理的暗号プロトコルの特徴（すなわち，代数学の知識を必要とせず気軽に実行できること）を維持しつつ遠隔で実行できる．メッセージングアプリなどのオンラインアプリを用いる魅力的な暗号プロトコルを構築していくことが今後の研究方針である．

7. 倫理的配慮のためのチェックリストについて

本稿では，実在するメッセージングアプリのサービス名を具体的に記述した．これは，3 節で定義した機能 $\mathcal{F}_{\mathrm{MA}}$ が実在するサービスによって実現可能であることを示すために必要であると考えたためである．本研究は実在するメッセージングアプリの脆弱性を示すものではなく，新たな活用方法を示す内容であるため，本研究がネガティブな影響をもたらすとは考えていない．

Facebook の利用規約[xi]に違反しないことも確認した．本研究が該当する恐れがある箇所として，利用規約 3「Facebook とコミュニティに対する利用者の誓約」における項目 2.2「ウイルスもしくは悪意あるコードをアップロードする、または弊社製品の正常な機能もしくは表示を停止させる、過負荷をかける、もしくは損傷させる行為は禁止されています。」が挙げられる．Facebook Messenger の月間利用者数（10 億以上と言われている）に比べ，本研究が過負荷を助長するとは到底言えないため，本研究は利用規約に違反していないと考えられる．

謝辞 本研究は JSPS 科研費 JP19J21153 の助成を受けたものです．

[x] 例えば，https://developers.facebook.com/docs/messenger-platform/reference/send-api/.

[xi] https://www.facebook.com/terms.php

参考文献

[1] T. Moran and M. Naor, "Polling with physical envelopes: A rigorous analysis of a human-centric protocol," Advances in Cryptology - EUROCRYPT 2006, ed. by S. Vaudenay, vol.4004, pp.88–108, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2006.

[2] T. Moran and M. Naor, "Basing cryptographic protocols on tamper-evident seals," Theoretical Computer Science, vol.411, no.10, pp.1283–1310, 2010.

[3] D. Miyahara, I. Ueda, Y. Hayashi, T. Mizuki, and H. Sone, "Analyzing execution time of card-based protocols," Unconventional Computation and Natural Computation, eds. by S. Stepney and S. Verlan, vol.10867, pp.145–158, Lecture Notes in Computer Science, Springer, Cham, 2018.

[4] T. Mizuki and Y. Komano, "Analysis of information leakage due to operative errors in card-based protocols," Combinatorial Algorithms, eds. by C. Iliopoulos, H.W. Leong, and W.-K. Sung, vol.10979, pp.250–262, Lecture Notes in Computer Science, Springer, Cham, 2018.

[5] J. Dreier, H. Jonker, and P. Lafourcade, "Secure auctions without cryptography," Fun with Algorithms, eds. by A. Ferro, F. Luccio, and P. Widmayer, vol.8496, pp.158–170, Lecture Notes in Computer Science, Springer, Cham, 2014.

[6] J. Balogh, J.A. Csirik, Y. Ishai, and E. Kushilevitz, "Private computation using a PEZ dispenser," Theoretical Computer Science, vol.306, no.1, pp.69–84, 2003.

[7] Y. Abe, M. Iwamoto, and K. Ohta, "Efficient private PEZ protocols for symmetric functions," Theory of Cryptography, eds. by D. Hofheinz and A. Rosen, vol.11891, pp.372–392, Lecture Notes in Computer Science, Springer, Cham, 2019.

[8] D. Miyahara, Y. Hayashi, T. Mizuki, and H. Sone, "Practical card-based implementations of Yao's millionaire protocol," Theoretical Computer Science, vol.803, pp.207–221, 2020.

[9] K. Toyoda, D. Miyahara, T. Mizuki, and H. Sone, "Six-card finite-runtime XOR protocol with only random cut," Proceedings of the 7th ACM on ASIA Public-Key Cryptography Workshop, pp.1–7, APKC'20, ACM, New York, NY, USA, to appear.

[10] T. Sasaki, D. Miyahara, T. Mizuki, and H. Sone, "Efficient card-based zero-knowledge proof for Sudoku," Theoretical Computer Science, pp.1–8, to appear.

[11] D. Miyahara, L. Robert, P. Lafourcade, S. Takeshige, T. Mizuki, K. Shinagawa, A. Nagao, and H. Sone, "Card-based ZKP protocols for Takuzu and Juosan," 10th International Conference on Fun with Algorithms (FUN 2020), pp.1–21, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, to appear.

[12] K. Yasunaga, "Practical card-based protocol for three-input majority," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp.1–3, to appear.

[13] S. Ruangwises and T. Itoh, "Physical zero-knowledge proof for Numberlink," 10th International Conference on Fun with Algorithms (FUN 2020), pp.1–11, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, to appear.

[14] A. Koch and S. Walzer, "Foundations for actively secure card-based cryptography," 10th International Conference on Fun with Algorithms (FUN 2020), pp.1–27, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, to appear.

[15] K. Sako, "An auction protocol which hides bids of losers," Public Key Cryptography, eds. by H. Imai and Y. Zheng, vol.1751, pp.422–432, Lecture Notes in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[16] H. Kikuchi, M. Hakavy, and D. Tygar, "Multi-round anonymous auction protocols," IEICE Transactions on Information and Systems, vol.E82-D, no.4, pp.769–777, Jan. 1999.