安全なデータ利活用に資するプライバシー保護暗号プロトコルの構成難易度に関する研究

代表研究者　　江村　恵太　　金沢大学　理工研究域電子情報通信学系　准教授

1 はじめに

情報セキュリティにおいて機密性（Confidentiality），完全性（Integrity），可用性（Availability）の3要素（CIA）が重要であるということは何十年も前から主張されており，現代のデジタル社会においてはもはや常識となっている．ここでCIAのみでは不十分である事例として，AIの進歩，とりわけLLM（大規模言語モデル）により一般にAIが普及した現状を鑑みる．AIの利用を通し，モデル作成に利用したデータを利活用していることに他ならないこと，特に機微なデータを扱う際にはCIAに加えてデータ提供者のプライバシーが重要になることに注意されたい．

プライバシー保護策として重要な役割を果たすのが暗号プロトコルである．しかし現在普及している安全な情報通信に資する暗号プロトコル，例えばオンラインショッピングの際のクレジットカード番号秘匿に用いる暗号化，情報の発信元とデータの改ざん防止に用いる署名などの基礎的な暗号を用いたプロトコルにプライバシー保護策を付加するには，追加のコスト（ここでは通信データ量や計算量を指す）を必要とすることは想像に難くない．そのコストがプライバシー保護に際し妥当であるかどうかの見積もりはプライバシー保護暗号プロトコルの普及に際し重要な課題と言える．

本調査では，このプライバシー保護に際し必要となる追加コストがどの程度なのかを測る指標として，プライバシー保護暗号プロトコルの構成難易度に関する研究を行った．まずプライバシー保護暗号プロトコルの構成には高機能暗号の利用が不可欠であることに着目する．なおどのような暗号方式を高機能暗号とするかは様々な定義が考えられるが，本研究調査においては[1]における定義「従来の暗号技術に対して，機能が追加・向上される等の優位性を主張する暗号技術，および，従来の暗号技術では困難であった事象を解決できる等の新規機能を有することを主張する暗号技術」を採用する．本調査では，高機能暗号における相互構成可能性，つまりある高機能暗号からある高機能暗号が構成可能/不可能であることを示す．例えば匿名性と追跡可能性を両立する高機能暗号として知られるグループ署名において，グループ署名から公開鍵暗号が構成できることが示されている．この結果より，グループ署名の構成には公開鍵暗号の利用が必要不可欠であることがわかると同時に，既に普及している公開鍵暗号の再利用が期待できることを示している．種々の高機能暗号間の関係性を調査することで，将来的なプライバシー保護暗号プロトコルの普及に資する．また対象のプライバシーが実利用に際し保護に値するものなのかの検討も必要不可欠であることから，本調査は理論計算機科学及び社会情報学の両方にまたがるものである．

本研究調査は「高機能暗号における構成可能性（項目１，2)」「高機能暗号のアプリケーション（項目３)」に分けて実施した．参考文献，発表資料はまとめて末尾に記載する．

2 項目 1: 高機能暗号における相互構成可能性: メッセージ依存開示可能グループ署名

2-1 グループ署名

グループ署名[5]とは匿名署名の一種である．グループに所属する署名者が作成した署名の検証にて，署名者がグループに属していることのみを検証し，グループの誰が署名したのかまでは特定しない．さらに複数の署名の作成者が同じ署名者か否かまでをも隠す．グループ管理者のみが自身の秘密鍵を用いて署名者を特定可能である．このように，グループ署名は匿名性と追跡可能性を両立した署名方式であるといえる．応用例として，マンション等のエントランス認証が挙げられる．グループ署名により住人であることのみを検証することで，帰宅時間等を秘匿することができる．ただし事件などが起きた場合に管理者がどの住人がこの時間に帰宅したのかなどを把握することが可能となる．なお，本来であれば管理者が住人を特定するのは事件などが起きた場合に限られるはずであるが，管理者は任意のグループ署名作成者を特定可能であることに注意されたい．この観点から，グループ署名における管理者の権限が強すぎると考えられる．

公益財団法人電気通信普及財団
研究調査助成報告書　第41号　2026年度

2-2 メッセージ依存開示可能グループ署名

グループ署名における管理者の権限を弱めた方式がメッセージ依存開示可能グループ署名[7]である．以下，GS-MDO（Group Signatures with Message-Dependent Opening）と表記する．GS-MDO では管理者の役割を分割する．アドミッターと呼ばれる管理者は署名するメッセージ M に依存したトークン tM を作成する．開示者と呼ばれる管理者は自身の秘密鍵とトークン tM を用いて署名者を特定する．ここでアドミッターと開示者は結託しないと仮定されることに注意されたい．先ほどのエントランス認証の例において，帰宅時間をメッセージとしてグループ署名を作成，事件等が起きた該当時間に対するトークンを作成することで，開示者は該当時間以外に帰宅した住人を特定することなく，該当時間に帰宅した住人のみを特定可能となる．安全性として，アドミッター単体，開示者単体では署名者の特定ができないことを保証するため，アドミッター匿名性，開示者匿名性が定義されている．さらに署名検証に通るグループ署名であればトークンと開示者秘密鍵を用いて署名者が特定できることを保証する追跡可能性が定義されている．

グループ署名に機能が追加されていることから，GS-MDO はグループ署名よりも構成が困難（強い暗号学的道具立てが必要）であると推察される．その理論的根拠として，グループ署名から公開鍵暗号が構成可能であること[2]，GS-MDO から ID ベース暗号が構成可能であること[7]，公開鍵暗号をいくら組み合わせても（ブラックボックス構成）ID ベース暗号は構成不可能であること[3]が示されている．しかしグループ署名の構成にはゼロ知識証明と呼ばれる暗号要素技術を通常利用すること，ゼロ知識証明は暗号要素技術のアルゴリズム入出力以外の情報を利用して構成する，すなわち非ブラックボックス構成であることから，GS-MDO が真にグループ署名より強い暗号要素技術であるとは結論付けられない．

2-3 タイムリリース暗号

通常の公開鍵暗号では，復号鍵を持つユーザが暗号文を入手した場合，即座に暗号文の復号が可能となる．しかし情報の解禁日を設けている場合など，場合によっては復号可能となる時間を規定したい場合が考えられる．規定時間に暗号文を送付する場合，データサイズなどに起因した遅延などを鑑みると，規定時間前に暗号文は送付し，規定時間に（送付遅延が考えにくい比較的小さなサイズの）トークンを時報局が配布，時刻トークンと復号鍵の両方が揃って初めて暗号文の復号が可能となる仕組みを実現するのがタイムリリース暗号である．トークン発行用の秘密鍵を持つ時報局であっても暗号文から平文の情報が得られないこと，該当トークンがない場合には復号鍵を持つユーザであっても暗号文から平文の情報が得られないことが要請される．

2-4 我々の成果

本研究調査では，GS-MDO がグループ署名より強い暗号要素技術である根拠を増やすことで GS-MDO の構成手法に関する知見を得ることを目的に，

(1) GS-MDO からタイムリリース暗号が構成可能であること，すなわち GS-MDO の構成にはタイムリリース暗号の機能性が不可欠であること
(2) トークンの偽造不可能性が開示者匿名性に含まれること，すなわち全ての GS-MDO 方式は暗にトークンの偽造不可能性を満たしていること

を明らかにした．

（2-4-1）メッセージ依存開示可能グループ署名からのタイムリリース暗号の一般的構成

以下，提案構成のアイディアを記載する．具体的な構成と安全性証明は煩雑であるため，発表資料を参照されたい．

まず GS-MDO とタイムリリース暗号の機能性が類似していることに着目する．すなわち，GS-MDO におけるアドミッターをタイムリリース暗号における時報局，GS-MDO における開示者をタイムリリース暗号における復号者とみなす．GS-MDO における匿名性（アドミッター匿名性，開示者匿名性）では，署名鍵が既知であっても匿名性が成り立つことを保証している．そこで GS-MDO における署名鍵 2 つをタイムリリース暗号の公開鍵とし，各署名鍵を平文 0 と 1 にそれぞれ割り当てる．暗号化時は平文に該当する署名鍵を用いて時刻 T に対するグループ署名を作成，タイムリリース暗号の暗号文とする．時報局はアドミッターの秘密鍵を用いてトークン tT を作成，時刻 T に配布する．復号者はトークンと GS-MDO の開示鍵を用いることで，どちらの署名鍵で作成されたグループ署名なのかを特定，復号結果を得る．なお GS-MDO のアドミッター匿名性により

時報局であっても暗号文から平文の情報が得られないこと，GS-MDO の開示者匿名性によりユーザであっても暗号文から平文の情報が得られないことが保証される．さらに暗号文がグループ署名であることから，グループ署名の署名検証アルゴリズムによる正当性の検証，すなわち暗号文の公開検証可能性が付与される．通常のタイムリリース暗号では要請されない機能が自動的に付加されることから，それだけGS-MDOは強い暗号要素技術であることが示唆される．

（2-4-2）トークンの偽造不可能性

GS-MDO の安全性モデルにおいては，トークンの偽造不可能性は明示的に定式化されていない．しかしアドミッターが作成したトークンを基に別のメッセージに対するトークンが偽造可能である場合，管理者たるアドミッターが発行していないトークンを用いたグループ署名の開示が可能になる．先ほどの応用例において，該当時間以外に帰宅した住人が特定されるとなると，GS-MDO の利用意義を揺るがす事態となる．そこで本調査研究ではトークンの偽造不可能性を定式化した．アドミッターの秘密鍵以外の全ての鍵を持つ攻撃者であったとしても，トークンの偽造が不可能であることを保証するものである．さらに，全ての GS-MDO 方式が満たすべき開示者匿名性にトークンの偽造不可能性が含まれることを示した．これはもしトークンの偽造不可能性を破る攻撃者が存在する場合，その偽造トークンを用いることで開示者匿名性を破ることが可能な帰着アルゴリズムを構成することで証明した．具体的な帰着アルゴリズムの構成と安全性証明は煩雑であるため，発表資料を参照されたい．

3 項目２: 高機能暗号における相互構成可能性: 公開鍵導出可能鍵隔離プライバシー保護署名

3-1 公開鍵導出可能鍵隔離プライバシー保護署名

ブロックチェーンを利用した暗号資産の送金には電子署名が利用される．送金者の署名検証鍵（のハッシュ値）をアドレスとして暗号資産を紐付ける．送金先や送金額などを記載したトランザクションに対し署名を作成，この署名の正当性がアドレスに対応する署名検証鍵を用いて確認できた場合，トランザクションに従って暗号資産が移動する．この際，送金/受金履歴が公となるため，同じアドレスを使用し続けるとプライバシー上の懸念が生じることも考えられる．そのため，ステルスアドレスという使い捨てアドレスを用いることで，送金/受金履歴を秘匿することが考えられる．ステルスアドレスの安全性を暗号理論的に証明するために公開鍵導出可能鍵隔離プライバシー保護署名 (PDPKS: Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key) が提案された[9]．PDPKS では，受金者がマスター公開鍵を生成，送金者がマスター公開鍵から使い捨ての導出公開鍵を作成する．このとき，どのマスター公開鍵から導出した導出公開鍵なのかを秘匿するリンク不可能性が定義されている．

これまでペアリングベース PDPKS 方式[9]，格子ベース PDPKS 方式[8]，公開鍵暗号と署名からの PDPKS の一般的構成[6]が提案されている．しかし PDPKS の実現可能性，すなわち PDPKS の構成に必要不可欠な暗号要素技術が何かについては明らかになっていない．署名は一方向性関数から構成可能である一方，一方向性関数から公開鍵暗号の構成不可能性が知られている．既存 PDPKS ではいずれも公開鍵暗号相当の暗号要素技術が使用されているが，署名であることから公開鍵暗号より弱い暗号要素技術から構成可能であれば，より効率的な構成も期待できる．

3-2 公開鍵暗号

公開鍵暗号では，公開鍵を用いて平文を暗号化，暗号文は公開鍵に対応する復号鍵を用いて復号され，平文を得る．公開鍵暗号は様々な用途で実用化されており，現代の情報化社会を支える重要な技術の一つである．例えばオンラインショッピングにおいて，クレジットカードの暗号化などに利用される．秘匿目的で公開鍵暗号を利用する場合は，選択暗号文攻撃（CCA: Chosen-Ciphertext Attack）に対する耐性を持つことが要請される．

3-3 我々の成果：公開鍵導出可能鍵隔離プライバシー保護署名からの公開鍵暗号の一般的構成

本研究調査では，PDPKS の構成に本質的に必要な暗号要素技術は何か?について検証を行った．具体的に，PDPKS から CCA 安全な公開鍵暗号が構成可能であることを示す．提案公開鍵暗号が CCA 安全であることは，PDPKS のリンク不可能性より証明される．PDPKS の目的がステルスアドレスの安全性向上であることから，リ

ンク不可能性が PDPKS の根幹を成す安全性であると位置づけられる．我々の結果により，PDPKS の根幹を成す安全性の達成には CCA 安全な公開鍵暗号相当の暗号要素技術が必要不可欠であることが明らかとなった．

以下，提案構成のアイディアを記載する．具体的な構成と安全性証明は煩雑であるため，発表資料を参照されたい．まず PDPKS では，受金者がマスター公開鍵 mpk を生成，送金者がマスター公開鍵から使い捨ての導出公開鍵 dpk を作成する．提案公開鍵暗号においては，2 つのマスター公開鍵（mpk0，mpk1）を公開鍵とし，平文 0 を暗号化する際には mpk0 を，平文 1 を暗号化する際には mpk1 を用いて dpk を作成，この dpk を暗号文とする．PDPKS では mpk に対応するマスター秘密鍵を用いることで，dpk が mpk から生成されたかどうかを検証するアルゴリズムが定義されている．そこで（mpk0，mpk1）に対応する 2 つのマスター秘密鍵（msk0，msk1）を公開鍵暗号の秘密鍵とする．dpk に対し，mpk0 から生成された場合は 0 を，mpk1 から生成された場合は 1 を復号結果として出力する．どのマスター公開鍵から導出した導出公開鍵なのかを秘匿するリンク不可能性により，暗号文 dpk から平文の情報は漏洩しない．さらにリンク不可能の安全性定義において，攻撃者は dpk の検証アルゴリズムにアクセス可能であることを利用し，公開鍵暗号の CCA 安全性における復号オラクルをシミュレートする．

4 項目 3: 高機能暗号のアプリケーション：成りすまし不可能性

4-1 グループ署名とその安全性

2-1 グループ署名にて述べたように，グループ署名[2]とは匿名署名の一種であり，グループに所属する署名者が作成した署名の検証にて，署名者がグループに属していることのみを検証し，グループの誰が署名したのかまでは特定しない．グループ管理者のみが自身の秘密鍵を用いて署名者を特定可能である．グループ署名の主な安全性として匿名性（Anonymity）と追跡可能性（Traceability）が定義されている．匿名性とは，グループ管理者の秘密鍵以外を持つ攻撃者に対し，グループ署名がどの署名鍵から生成されたものかという情報が漏れないことを保証する安全性であり，追跡可能性とは検証に通るグループ署名であれば，必ず署名者が特定可能であることを保証する安全性である．Bellare，Shi，Zhang（BSZ)[4]により導入された BSZ モデルでは，グループ公開鍵設定後の動的なユーザの追加を考慮した．さらにグループ管理者の役割をユーザの追跡（Opener）とユーザの追加（Issuer）に分離，匿名性においては Issuer が，追跡可能性においては Opener が攻撃者と結託する安全性モデルを定義した．さらに攻撃者が Opener と Issuer の両方と結託したとしても，追跡結果が攻撃者と結託していない正直なユーザとなる正当なグループ署名を生成できないことを保証する安全性として，成りすまし不可能性（Non-Frameability）が導入された．

定義から明らかなように，成りすまし不可能性は両グループ管理者（Opener と Issuer）が結託したとしても達成される，ユーザを守る安全性として導入された．ただし匿名性，追跡可能性というグループ署名の主となる安全性と比較して，その意義が多く評価されてきたとは言えない．そこで本研究調査では，グループ署名の応用として一般的な匿名オークションにおける成りすまし不可能性の意義を精査，新たな解釈を与える．

4-2 成りすまし不可能性の新たな解釈

匿名オークションでは落札額に対しグループ署名を作成することで，誰がいくら入札したのかという情報を隠すと共に，オークション管理者のみが落札者を追跡可能となる．ここで成りすまし不可能性を満たさないグループ署名方式を利用すると，例えばオークション管理者があるユーザに成りすまして虚偽の入札を行うことが可能となり，結果入札していないユーザに対し落札額を請求することが可能となる．さらに匿名性に起因して，いくらこのユーザが入札していないと主張したとしても，その事実を証明する術はない．しかしこのような不正をオークション管理者が行った場合，成りすまされたユーザが入札していないと主張することで，そのようなオークションにわざわざ参加するユーザはいないと考えるのが自然であろう．すなわち，このような社会的制裁を鑑みると，オークション管理者がわざわざ成りすましを行う動機はないと考えられる．では匿名オークションにおいて成りすまし不可能性は不必要な安全性なのであろうか．ここで本来の落札者が自分は入札していない，管理者が成りすましていると主張する場合を考える．後で落札を取りやめたい場合など，比較的起こりうる状況であると考えられる．この場合，グループ署名方式が成りすまし不可能性を満たすことで，オークション管理者は暗号理論的に成りすましていないことを主張可能となる．この状況を鑑みると，成りすまし不可能性はグループ管理者を守る役割を果たしており，成りすまし不可能性の新

たな解釈であると言える.

5 おわりに

本研究調査は「高機能暗号における構成可能性（項目１，2)」「高機能暗号のアプリケーション（項目３)」に分けて実施した．高機能暗号はその機能性や安全性により様々な応用が期待される．その一方で，どの高機能暗号を選べばよいのか，選ばれた高機能暗号方式は従来の暗号方式よりもどのような点で優れているのか，運用時にはどのようなことに注意することが必要か等，実際に利用する際には専門家以外では，判断基準がわからず，実運用の判断に困難な場合も多い（[1]はじめにに記載の文を引用)．本研究調査を通じ，高機能暗号の理解度が高まることで，高機能暗号の普及の一助となることを期待する.

【参考文献】

[1] CRYPTREC 暗号技術ガイドライン（高機能暗号）2023 年 3 月

[2] Michel Abdalla, Bogdan Warinschi: On the Minimal Assumptions of Group Signature Schemes. ICICS 2004: 1-13

[3] Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, Brent Waters: On the Impossibility of Basing Identity Based Encryption on Trapdoor Permutations. FOCS 2008: 283-292

[4] Mihir Bellare, Haixia Shi, Chong Zhang: Foundations of Group Signatures: The Case of Dynamic Groups. CT-RSA 2005: 136-153

[5] David Chaum, Eugène van Heyst: Group Signatures. EUROCRYPT 1991: 257-265

[6] Keita Emura: Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key, Revisited: Consistency, Outsider Strong Unforgeability, and Generic Construction. IACR Commun. Cryptol. 2(3): 17 (2025)

[7] Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, Kazumasa Omote: Group Signatures with Message-Dependent Opening. Pairing 2012: 270-294

[8] Wenling Liu, Zhen Liu, Khoa Nguyen, Guomin Yang, Yu Yu: A Lattice-Based Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key. ESORICS (2) 2020: 357-377

[9] Zhen Liu, Guomin Yang, Duncan S. Wong, Khoa Nguyen, Huaxiong Wang: Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key. EuroS&P 2019: 215-230

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
メッセージ依存開示可能グループ署名におけるトークンの偽造不可能性について	コンピュータセキュリティシンポジウム（CSS）2025	2025 年 10 月
公開鍵導出可能鍵隔離プライバシー保護署名からの CCA 安全な公開鍵暗号の一般的構成	暗号と情報セキュリティシンポジウム（SCIS）2026	2026 年 1 月
グループ署名における成りすまし不可能性の意義について	暗号と情報セキュリティシンポジウム（SCIS）2026	2026 年 1 月
Group Signatures with Message-Dependent Opening Directly Imply Timed-Release Encryption	24th International Conference on Cryptology and Network Security (CANS 2025)	2025 年 10 月
Group Signatures with Message-Dependent Opening Directly Imply Timed-Release Encryption	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2026	2026 年 9 月