匿名性・追跡可能性・説明責任性を両立するデジタル署名とプライバシ保護の枠組の設計

代表研究者	穴田　啓晃	青森大学　ソフトウェア情報学部　教授
共同研究者	長谷川　真吾	東北大学　データ駆動科学・AI 教育研究センター　助教
共同研究者	福光　正幸	長崎県立大学　情報システム学部　准教授

1 はじめに

1-1 本研究の背景

ネットワークを経由したサービスのユーザー，すなわちヒトやモノが匿名で扱われ匿名性が保証されることは，期待される重要な性質である．ソーシャルネットワーキングサービス（SNS）では特に国内で大多数のユーザーが実名公開に抵抗感がある（図 1）．その一方，匿名での誹謗中傷の問題がここ 5 年程 SNS における深刻な社会問題である．この状況に対応するためには，不具合やトラブルが発生した際に SNS の運営事業者は，法に拠る開示請求に基づき匿名を「開封」しユーザーを特定する責任がある．つまり，追跡可能性は必要な性質と認知されている．

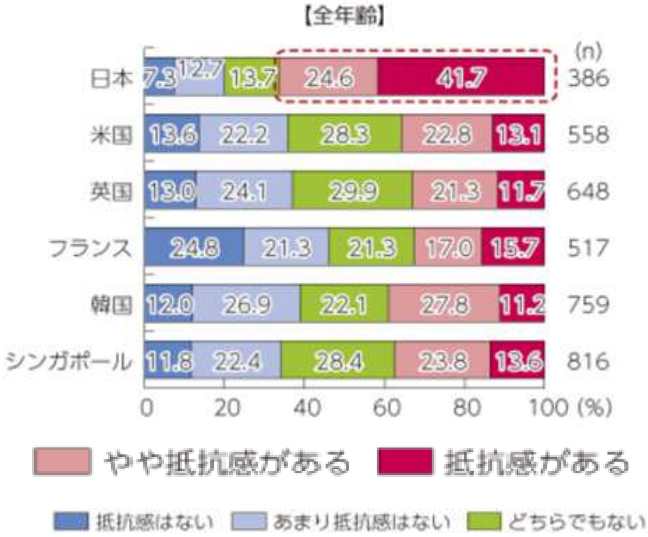

図 1　SNS での実名公開の抵抗感(総務省 H26)

しかしながら，インターネット上の通信の暗号化に対する盗聴の警鐘などで知られる「スノーデン事件」(2013 年)を機に「裏口鍵」の存在もまた脅威となっている．すなわち，請求が無いにも関わらず運営業者が追跡をしているのか否かをユーザーが知ることは難しく，追跡権限が濫用される懸念が排除できない．つまり，ネットワークサービスの社会では匿名性よりも追跡可能性に重点が置かれている現状がある（図 2）．この現状から「匿名性と追跡可能性をいかに公平にするか」という課題が重要と考えられる．この「匿名性と追跡可能性のフェアネスの保証」を課題とする状況に対し，サービスを運用する者が匿名を開封した事実を説明する責任を果たす場を設けることで保証を試みる方策が考えられる．この説明責任性とこれを果たす場の導入には，理論，技術，運用，ペナルティそして法といった幾つかのアプローチがありうる．従って，この課題に対する研究は，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．

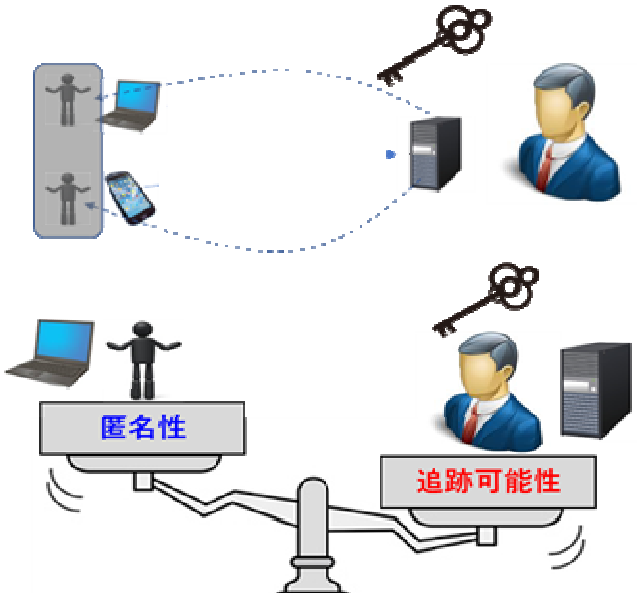

図 2　匿名性より追跡可能性が重視されている現状

本研究は，理論及び技術を含む暗号学のアプローチにより説明責任性を適切に導入し，匿名性・追跡可能性・説明責任性を両立する手法を構成しようとする動機に基づく．ここで暗号学は，理論計算機科学，数学，社会情報学，実装技術の共通分野に位置付けられる学際的な領域にあり，アプローチの一つとして適切と考えられる．特に上述の課題に対しては，一見困難な次の問いが浮上する：

「匿名性と追跡可能性を両立する暗号アルゴリズムの原理はどんなものか？」

1-2 本研究のアプローチ

この問いに対し、本研究では次の(1)(2)のアプローチを試みる.

「(1)サービスを管理する側（管理者側）の工夫と設計」. このアプローチは追跡権限の分権，あるいは，鍵発行の種別化などの切り口から解決を試みる．(1)のアプローチでは，管理者側が情報処理や通信のプロトコルに従うという前提に立つ.

「(2)ユーザー側のアルゴリズムの工夫と設計」. このアプローチは管理者側のみならずユーザー側をも追究するものである.

特に本研究では，グループ署名方式（group signature scheme [1]）と呼ばれる，デジタル署名に匿名性と追跡可能性の機能を付加した暗号スキームに着目する．グループ署名はグループ管理者の存在を前提とする．グループ管理者はマスター鍵を持ち，グループのメンバーの加入や失効を管理する．グループメンバーはグループを代表して署名を生成する．任意の検証者は，署名がそのグループのものであることを公開鍵で検証可能である．ただし，グループのどのメンバーが署名したかを特定することは計算量的に不可能とされる．この意味でグループ署名は匿名性を有すると言われる．一方，グループ署名には開封者の存在も前提とする．開封者はグループ管理者から開封鍵を渡される．開封者は，生成されたグループ署名に対し，開封鍵を用いることでグループのどのメンバーが署名したかを特定することが可能である．この意味でグループ署名は追跡可能性を有すると言われる．先述の「匿名性よりも追跡可能性に重点が置かれている現状」は，これらの意味で追跡可能性が匿名性より強いことに対応する.

1-3 本研究の成果

本研究では主にグループ署名方式を研究対象とし，主要な成果として次の三つの暗号スキームを提案した.

1. 開封者の属性で指定された追跡可能性を有するグループ署名の双線形群における例示（Group signatures with designated traceability over openers’ attributes in bilinear groups）
2. 非対話型署名生成機能を持つメッセージ依存開封型動的グループ署名（Dynamic group signatures with message dependent opening and non-interactive signing）
3. 署名者の等検査付きのグループ署名（Group signatures with equality test on signers）

以降，第 2 節では上記 1，第 3 節では上記 2，そして第 4 節では上記 3 の暗号スキームについて，それぞれの研究の背景と貢献，またスキームのアルゴリズムの要所と暗号学的な安全性を，要約して述べる（詳細については文中に示した文献を参照されたい）. 最後の第 5 節では，上記三つの暗号スキームに関する今後の課題を挙げる．なお，本研究課題は公益財団法人電気通信普及財団研究調査助成の 2020 年度採択（2021 年度実施）の「延長」であり，2021 年度採択（2022 年度実施）のものである.

2 開封者の属性で指定された追跡可能性を有するグループ署名の双線形群における例示（[13]）

2-1 研究の背景と貢献

（１）背景

Group signatures with designated traceability over openers’attributes in bilinear groups（以降 GSdT）は，署名者が開封者（追跡者）を指定することが可能なグループ署名スキームである．ここで，指定とは「追跡者の属性の全体集合に対するアクセス構造を能動的に選択できること」を指す．すなわち，グループ署名を生成する者が主体的に追跡可能性の一部分を制御出来る．2021 年度の研究の成果では GSdT のアルゴリズムのシンタックスと安全性定義を示し，また構成部品を組み合わせた一般的構成を与えた.

（２）貢献

2022 年度の本研究では，双線形群の構造を用いた GSdT の具体的構成を例示した（[13]）. なお，本稿の例は，双線形群の中でも“Type III pairing”（[3]）として特徴付けられたものを前提とする．その性能としては，追跡者（開封者）の数 L をスキームセットアップ時に決定する必要があるものの，L 及び追跡者属性の数 N に比例する程度の計算量及び署名長のコストで済むことが分かった.

2-2 提案方式の要約

（１）スキーム

GSdT の一般的構成（[2,11,12]）の構成要素は euf-cma secure なデジタル署名スキーム SIG，adaptive IND-CPA secure で only-payload-hiding な ciphertext-policy 属性ベース暗号スキーム ABE，そして simulation-sound な非対話型ゼロ知識証明系 NIZK である．具体例を構成する際に留意すべき点は，ABE の

先行研究はそのほとんどが双線形群のターゲット群においてblinding factorを乗じることで平文を暗号化する設計であるという制約がある点である（[5]）．この制約を満たそうとすると，SIGはターゲット群において署名を生成することとなり，このためソース群において署名を生成する“structure-preserving signatures (SPS)”（[4]）等とは相容れない．

そこで本研究では，ABEとしてペアリングフリーなもの（[6]）を用いる設計とする．すなわち，SIGとしてSPSを用いることを優先し，ソース群（という単独の群）において属性ベース暗号化する．ただし，[6]のABEには，ユーザー数の上限がABEのセットアップ時に固定されなければならないという別の制約がある．この制約から，提案する具体例の設計では開封者の数の上限をGSdTのセットアップ時に固定する必要が発生する．結果，具体例の構成要素は次の三つを選択するものとした．SIGは“compact structure-preserving signatures with almost tight security”（[4]），ABEは“pairing-free CP-ABE with limited number of users”（[6]），そしてNIZKは“Groth-Sahai NIZK”（[7,8]）である．

（2）安全性

上述の構成要素の選択に拠り，GSdTの安全性要件である正当性，匿名性，追跡可能性そして陥罪不可能性は，Type-IIIの双線形群に対するSXDH仮定（[4]）に帰着されることとなる．詳細は発表論文[13]を参照されたい．

3 非対話型署名生成機能を持つメッセージ依存開封型動的グループ署名（[14]）

3-1 研究の背景と貢献

（1）背景

Group signatures with message dependent opening（以降GS-MDO）は，グループ署名の変種であり，開封権限が開封者と承認者の二機関へと分権されたものである．この分権に拠り開封者のみによる開封権限の濫用を防ぐことが可能とされる．GS-MDOの先行研究を調査すると，そのほとんどの方式が静的モデルにおいて構成されていることが判る．ここで静的とは，スキームのセットアップ時にグループメンバーが固定され，その後グループメンバーが加入したり失効したりすることがないモデルを指す．動的モデルにおいて構成されている唯一の方式は，グループ署名生成時に署名者と承認者の間の対話が必要とされ，この特徴によって実際には匿名性が破綻していることが判明した．

（2）貢献

上述の調査を経て，本研究では動的モデルにおいてGS-MDOを提案した（[14]，DGS-MDO）．その特徴は，グループ署名生成時に署名者と承認者の間の対話を必要としないことである．本研究ではDGS-MDOのアルゴリズムのシンタックス，安全性定義，及び一般的構成を与えた．ただし，開封者匿名性と承認者匿名性の内，前者が「トークン発行回数がk回まで」（k-bounded tokens）という制約を有する．本研究では更に，具体例の構成について設計の一つを示した．

3-2 提案方式の要約

（1）スキーム

提案するシンタックス及び安全性を満たすようなDGS-MDOの一般的構成として，次の構成要素を用いるものを提案した．すなわち，デジタル署名スキームSIG，鍵カプセル化機構KEM，扱えるID文字列の数がk-resilientなID-KEM，計算量的ゼロ知識な非対話ゼロ知識証明系NIZK，そして更にシミュレーション健全な非対話ゼロ知識証明系SS-NIZKである．

（2）安全性

前述の通り，提案する一般的構成のDGS-MDOの長所は，再検討された意味での匿名性を実現したことである．すなわち，DGS-MDOの先行研究では署名生成時に対話が必要であったところ，提案スキームでは非対話で署名が生成され，これに拠り匿名性が破綻していた問題が解消されたことである．また別の観点での長所は，具体化した際に標準モデルでの安全性が得られること，また，グループメンバーの数に依存せず一定の署名長となることである．その一方，上述の“k-bounded tokens”の開封者匿名性という制約がある．詳細は発表論文[14,16]を参照されたい．

4 署名者の等検査付きのグループ署名（[15]）

4-1 研究の背景と貢献

（１）背景

グループ署名方式（[1]）は従来，単一のグループについてのみ種々の追究がなされてきた．しかしながら次の現実にありうるシナリオが考えられる．すなわち，グループ G の開封者 Oが，メッセージとグループ署名のペア(m, σ)に対し，m と類似した，疑義がありうる内容のメッセージ m'とそのグループ署名のペア(m', σ')，ただし別のグループ G'のもの，を見つけるというものである．このときに Oが G'の開封者 O'に次の問い合わせをするのは自然と考えられる：「σ'の署名者がσの署名者と同一か否かをテストさせてもらえないか？」．ただし，このテストにおいてσとσ'の有する匿名性は極力維持されるべきである．

（２）貢献

本研究では，上述のシナリオから期待される「署名者の等検査付きのグループ署名」(group signatures with equality test on signers，以降 GSET）の方式を提案した．この提案方式においてあるべき性質は，等検査の結果が false，すなわち「同一でない」と出力されたとき，それぞれの署名者の匿名性が保証される性質である．この性質を定式化するため，SemiOpen 及び EQ のアルゴリズムを導入し，シンタックス及び関連する安全性を定義した．また，一般的構成を与えた．

4-2 提案方式の要約

（１）スキーム

GSET のシンタックスは，従来のグループ署名方式のシンタックスである Bellare-Shi-Zhang[2]をベースに，SemiOpen 及び EQ のアルゴリズムが追加される設計とした．一般的構成においては，[2]の一般的構成の構成要素にハッシュ関数を加える形とした．

（２）安全性

本研究では，Bellare-Shi-Zhang[2]で定式化された正当性，匿名性，追跡可能性そして陥罪不可能性に（自然に）追加される形で“true-consistency（真一貫性）”及び“false-consistency（偽一貫性）”を新たに定義し提案した．これらの定義の下で，提案する一般的構成が安全性要件を全て満たすことを示した．ただし，グループが複数存在する前提での追跡可能性を扱うことから，グループメンバーが複数のグループに加入する際のアイデンティティが同一でなければ等検査ができない．このため，共通の公開鍵基盤に基づく一つのアイデンティティをメンバーが用いる前提とした．詳細は発表論文[15]を参照されたい．

5 今後の課題

第 2 節の提案方式:GSdT では，開封鍵を発行する者が「マスター鍵」という全権を持ち，発行者だけはマスター鍵を用いてどのグループ署名も開封できるという意味（「裏口鍵」），理想的でない．そこで今後の課題として，マスター鍵などの「全権」を有する実体を必要しない，ユーザー側の権限を強化する設計が挙げられる．この種の課題は，暗号学では 2000 年頃の ID ベース暗号の発明依頼，本質的には未解決とされている難題であり，解決すれば研究コミュニティへの波及が大きい．この難題に対し，今後は「匿名性 versus 追跡可能性」の設定に的を絞った形での解決を目指す．

第 3 節の提案方式：DGS-MDO では，一般的構成の構成部品である ID-KEM の k-resiliency に起因する，開封回数の制約の課題が残っている．この制約の解消は今後の課題である．

第 4 節の提案方式：GSET では，上述の《共通の公開鍵基盤》で管理された公開鍵と，一般的構成の部品である《公開鍵暗号》の公開鍵との，公開の範囲の違いに注意する必要がある．なぜなら，公開の範囲が同じであれば，ハッシュ値に対する辞書攻撃で匿名性が破綻する可能性があるからである．この点は今後追究すべき課題である．

他，「匿名性 versus 追跡可能性」についての最新の研究成果[19-22]も踏まえる必要がある．

【参考文献】

[1] D. Chaum and E. van Heyst: “Group Signatures”, in Proc. of EUROCRYPT ’91, 1991

[2] M. Bellare, H. Shi and C. Zhang: “Foundations of Group Signatures: The Case of Dynamic Groups”, in Proc. CT-RSA 2005

[3] S. D. Galbraith, K. G. Paterson and N. P. Smart: “Pairings for cryptographers”, Discrete Applied Mathematics, 156(16), pp.3113-3121, 2008.
[4] M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo and J. Pan: “Compact Structure-Preserving Signatures with Almost Tight Security”, CRYPTO 2017
[5] A. Sahai and B. Waters: “Fuzzy Identity-Based Encryption”, in Proc. EUROCRYPT 2005, 2005.
[6] J. Herranz: “Attribute-based versions of Schnorr and ElGamal”, Appl. Algebra Eng. Commun. Comput. 27(1), pp.17-57, 2016
[7] J. Groth and A. Sahai: “Efficient Non-interactive Proof Systems for Bilinear Groups”, EUROCRYPT ’08, 2008
[8] B. Libert and M. Yung: “Non-interactive CCA-Secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions”, in Proc. TCC 2012
[9] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda and K. Omote: “Group Signatures with Message-Dependent Opening”, in Proc. Pairing 2012
[10] H. T. Lee, S. Ling, J. H. Seo, H. Wang, and T.-Y. Youn: “Public key encryption with equality test in the standard model”, Inf. Sci., 516(C):89-108, 2020.
[11] H. Anada, M. Fukumitsu and S. Hasegawa: “Group Signatures with Designated Traceability”, CANDAR 2021
[12] H. Anada, M. Fukumitsu and S. Hasegawa: “Group Signatures with Designated Traceability over Openers’ Attributes”, Int. J. Networking and Computing, 493-508, vol.12(2), 2022
[13] H. Anada, M. Fukumitsu and S. Hasegawa: “Group Signatures with Designated Traceability over Openers' Attributes in Biliner Groups”, in Proc. Information Security Applications - 23rd International Conference (WISA 2022)
[14] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa: “Dynamic Group Signatures with Message Dependent Opening and Non-Interactive Signing”, in Proc. Tenth International Symposium on Computing and Networking (CANDAR 2022)
[15] Kyoya Anzai, Masayuki Fukumitsu, Hiroaki Anada, Shingo Hasegawa: “Group Signatures with Equality Test on Signers”, in Proc. 10th International Workshop on Information and Communication Security (WICS)
[16] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa: “Dynamic Group Signatures with Message Dependent Opening and Non-Interactive Signing”, to appear in Int. J. Networking and Computing, vol.13(2), 2022
[17] 穴田啓晃, 福光正幸, 長谷川真吾:「指定された追跡可能性を有するグループ署名の双線形群における例示」, 2022 年暗号と情報セキュリティシンポジウム予稿論文集, 2022 年
[18] 穴田啓晃, 安在恭弥:「署名者に対する等検査付きグループ署名の検討」, 電子情報通信学会情報セキュリティ研究会技術研究報告集, 2022 年 3 月
[19] M. Kohlweiss and I. Miers: “Accountable Metadata-Hiding Escrow: A Group Signature Case Study”, in Proc. Priv. Enhancing Technol. 2015
[20] S. Ling, K. Nguyen, H. Wang and Y. Xu: “Accountable Tracing Signatures from Lattices”, CT-RSA 2019
[21] J. Bootle, A. Cerulli, P. Chaidos, E. Ghadafi, J. Groth and C. Petit: “Short Accountable Ring Signatures Based on DDH”, in Proc. of ESORICS 2015
[22] B. Libert, K. Nguyen, T. Peters and M. Yung: “Bifurcated Signatures: Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme”, EUROCRYPT 2021

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Group Signatures with Designated Traceability over Openers' Attributes	International Journal of Networking and Computing	2022 年 7 月
Group Signatures with Designated Traceability over Openers' Attributes in Biliner Groups	Proceedings of Information Security Applications - 23rd International Conference (WISA 2022)	2022 年 8 月
Attribute-Based Signatures of Fiat-Shamir Type in Bilinear Groups: Scheme and Performance	Proceedings of The 2023 International Workshop on Future Security and Privacy (FSP 2022)	2022 年 8 月
Dynamic Group Signatures with Message Dependent Opening and Non-Interactive Signing	Proceedings of Tenth International Symposium on Computing and Networking (CANDAR 2022)	2022 年 11 月
Group Signatures with Equality Test on Signers	Proceedings of 10th International Workshop on Information and Communication Security (WICS)	2022 年 11 月
Dynamic Group Signatures with Message Dependent Opening and Non-Interactive Signing	International Journal of Networking and Computing	（to appear，2023 年 7 月）