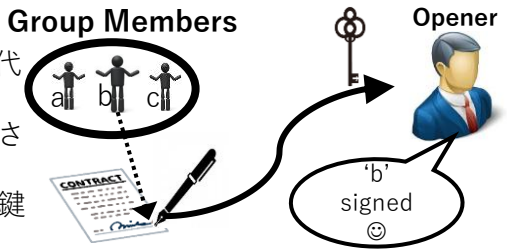
明治学院大学情報数理学部付属 情報数理科学研究所
Institute for Mathematical Informatics attached to Faculty of Mathematical Informatics, Meiji Gakuin University

穴田啓晃（教授）Hiroaki Anada, Professor
研究トピック　Research Topics

1．開封者を指定可能なグループ署名の提案･設計

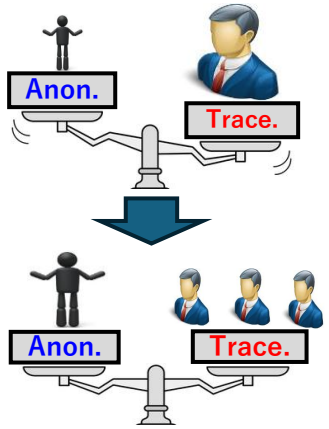
研究の背景

グループ署名 [1] は署名者が企業等のグループを代表して署名を生成できるディジタル署名方式
- 匿名性: 署名者はグループ内のどの者かを特定され得ない
- 追跡可能性: 開封者と呼ばれる権限機関が開封鍵を用いて署名者を特定できる



動機・問い

開封鍵を用いると全てのグループ署名に対し署名者を特定できる追跡可能性は，権限として強すぎる．匿名性との公平性をいかに実現するか？



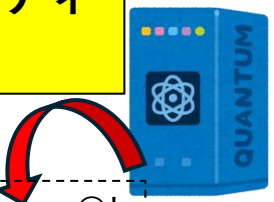
進展状況

署名者が開封者を属性で指定できるグループ署名 (GSdT)を提案[2]．開封されたくない属性の開封者を排除できる権限を署名者が持つ方式．提案では定義を与えるとともに，一般的構成を提示．具体的設計として，双線形群における構成[3]，対称鍵要素からの構成[4]，格子構造における構成[5]を与えた．

[1] David Chaum, Eugène van Heyst: “Group Signatures”. EUROCRYPT 1991: 257-265
[2] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa:“Group Signatures with Designated Traceability over Openers' Attributes”. Int. J. Netw. Comput. 12(2): 493-508 (2022)
[3] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa:“Group Signatures with Designated Traceability over Openers' Attributes in Bilinear Groups”. WISA 2022: 29-43
[4] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa:“Group Signatures with Designated Traceability over Openers' Attributes from Symmetric-Key Primitives”. PST 2024: 1-9
[5] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa:“Group Signatures with Designated Traceability over Openers' Attributes from Lattices”. CANDAR 2024: 1-10

2．耐量子計算機ディジタル署名のマルチパーティ計算からの設計，及び高機能化

研究の背景



量子計算機の研究開発が進むとともに，古典計算機を凌駕するその計算能力が暗号の危殆化をもたらしうる脅威となっている．このため，耐量子計算機暗号の研究が世界的に重要な課題であり，標準的な設計を米国立標準技術研究所(NIST)等が暗号研究者らに対し募っている．

動機・問い

マルチパーティ計算(MPC) [6]はn人の参加者(parties)の各々が個別に秘密を有している状況で秘密からの計算結果を得る暗号プロトコルである（例として，年収の降順順位を知る）．MPC-in-the-Head(MPCitH)はMPCをブラックボックスとして用いてゼロ知識対話証明系[7]を得るという理論計算機科学の提案方式である[8]．近年の研究（[9, 10]等）で，MPCitHが耐量子計算機ディジタル署名で時間計算効率の優れたものが構成できることが知られるようになっている．これらの構成をグループ署名やリング署名に高機能化できないか？

進展状況

対称鍵要素からの構成をGSdTや説明責任型リング署名へと拡張する設計（[4]等）を得ている．また，有限体の部分体の双線形衝突問題に基づく構成については現在も研究中[11]．
前者については高機能化固有の現象（問題）があることが判明しつつある．後者については有限体上の多変数２次連立方程式として耐量子計算機性を保証できるかが要所であり，その研究動向を追うとともに，高機能化の設計を進めている．

[6] Oded Goldreich, Silvio Micali, Avi Wigderson: “How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority”. STOC 1987: 218-229
[7] Shafi Goldwasser, Silvio Micali, Charles Rackoff:”The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract). STOC 1985: 291-304
[8] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Amit Sahai: “Zero-knowledge from secure multiparty computation”. STOC 2007: 21-30
[9] Jonathan Katz, Vladimir Kolesnikov, Xiao Wang: “Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures”. CCS 2018: 525-537
[10] Janik Huth, Antoine Joux: “MPC in the Head Using the Subfield Bilinear Collision Problem”. CRYPTO (1) 2024: 39-70
[11]穴田啓晃, 福光正幸, 長谷川 真吾:「リング署名の部分体双線形衝突問題に基づく構成に向けて」2025年暗号と情報セキュリティシンポジウム

明治学院大学情報数理学部付属 情報数理科学研究所
Institute for Mathematical Informatics attached to Faculty of Mathematical Informatics, Meiji Gakuin University

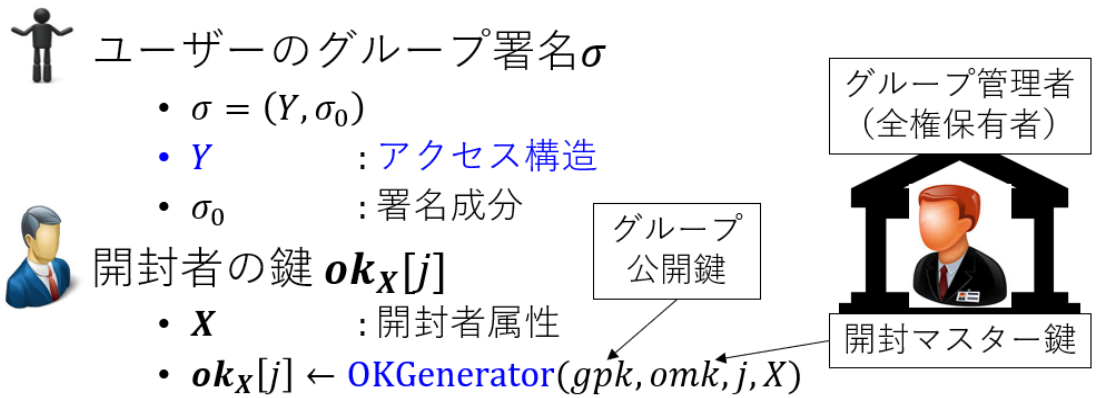
穴田啓晃（教授）　Hiroaki Anada, Professor
研究上の興味・疑問　Research Interests & Questions

社会情報学の問題に対し理論計算機科学の手法で

ネットワークを経由したサービスのユーザー，即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，社会で期待されている重要な要件です．例として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ります．その一方で，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す．この問題を対処するためには，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基づく開示請求で匿名を「開封」し，ユーザーを特定する必要があり，責任でもあります．つまり，追跡可能性は匿名性と表裏一体の要件です．

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ます．即ち，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ません．このように現在のネットワークサービス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ります．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社会情報学的に重要と考えています．

この課題は，理論計算機科学の一領域である暗号学では「匿名性と追跡可能性の両立するアルゴリズム」の問題と捉えられます．そのようなアルゴリズムを構築する際のアプローチとして「開封者を指定可能なグループ署名」（前ページ左および下図参照）の定義や設計に取り組んでいます．



データ科学・理論計算機科学で人間と機械が識別不可能に!?

中学３年生の頃に「数学ゲームⅠ」という本を読みました（[12]）．その中に「マッチ箱ゲーム思考機械」があり，その話はヘキサポーンというマス目の少ないチェスでマッチ箱に対戦相手を務めさせようというものでした．対戦経験を学習させるといずれ勝てるようになるというのですが，面白いというよりは大変奇妙な印象を持ちました．学習や思考は人間でなくても機械でもできるものなのか？数学で人間の思考をするような機械を設計できるか？

時を隔てること20年．あるきっかけからゼロ知識対話証明（前ページ[7]）を知りました．「証明者と検証者は対話型チューリング機械」という説明がありました．これを読んで中学生のときの奇妙な記憶を思い出したのが，その後暗号理論の領域あるいは学界で働くようになるトリガーです．お察しのように先述のマッチ箱は機械学習のおもちゃであり，ゼロ知識対話証明は計算の複雑さ理論に根源を持ちますから，話がずれています．が，どちらも人間の振る舞いのようなことを機械の動作として記述できることに惹かれています．

このような動機で研究をしているので，暗号理論の中でも対話証明，より一般的には暗号プロトコルが好きです。下図は前スライドのMPCitHの例です．いずれ，チューリングテストのような，暗号プロトコルの相手が人間なのか機械なのかを識別できなくなる時が来やしないか，ワクワクしたり心配したりしています．

[12] マーチン・ガードナー 著, 高木茂男 訳:「数学ゲームⅠ 楽しい数学へのアプローチ」, 講談社, 1974