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

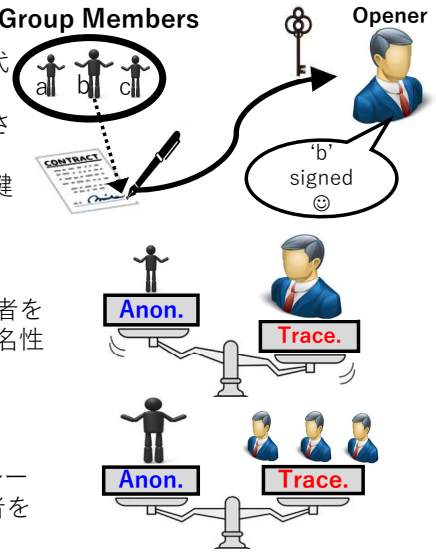
研究トピック　Research Topics

トピック１．開封者を指定可能なグループ署名

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

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。匿名性とのバランス取りを設計できないものか？

研究状況

署名者が開封者を，属性によって指定できるグループ署名を提案[2]。開封されたくない属性の開封者を排除できる権限を，署名者に☺

[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)

トピック２．耐量子計算機ディジタル署名の設計：NP問題，マルチパーティ計算，高機能化

[3] Jonathan Katz, Vladimir Kolesnikov, Xiao Wang: “Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures”. CCS 2018: 525-537
[4] Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa: “Group Signatures with Designated Traceability over Openers' Attributes from Symmetric-Key Primitives”. PST 2024: 1-9

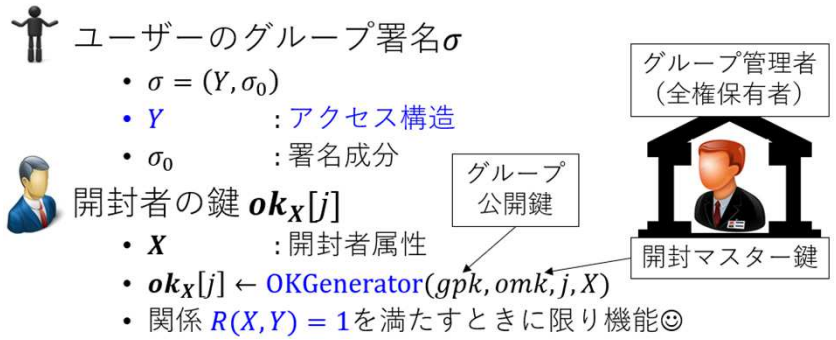
明治学院大学情報数理学部付属 情報数理科学研究所
Institute for Mathematical Informatics attached to Faculty of Mathematical Informatics, Meiji Gakuin University

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

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，期待される重要な性質です。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ります。つまり，追跡可能性は必要な性質と認知されています。

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。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」という課題が重要と考えられます。この課題に関し，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暗号学で，アルゴリズムとして一見困難な次の問いが浮上します。

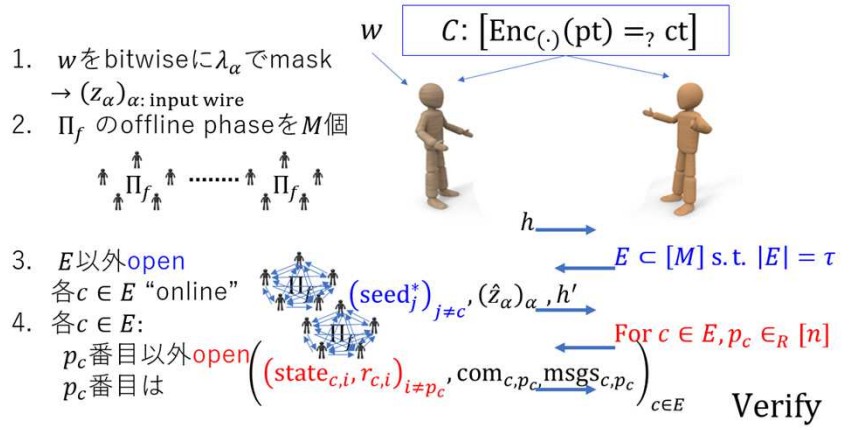
この問いに対する暗号学のアプローチは，《①サービスを管理する側（管理者側）の工夫と設計》と要約することができます。つまり，追跡権限の分権，あるいは，鍵発行の種別化などです（後述）。①のアプローチでは，管理者側が情報処理や通信のプロトコルに従うという前提に立ちます。これに対し，私の興味は，管理者側のみならず《②ユーザー側のアルゴリズムの工夫と設計》をも追究するところにあります。



一方，量子計算機の原理的解明と限界，また実物の開発が1990年代から（急速に）進展してきています。その正の面は，計算能力の飛躍的向上による種々の課題の解決です。しかし負の面は，悪意による安全性破壊です。特に懸念されているのが，インターネット上の暗号化通信やディジタル署名の脆弱化です。

耐量子計算機暗号という研究領域が1990年代後半から形成されていて，量子計算機の能力をもってしても原理的に堅牢な

[5]



[5] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Amit Sahai: Zero-knowledge from secure multiparty computation. STOC 2007: 21-30