様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 ２４ 日現在

機関番号：８２６２６
研究種目：若手研究(B)
研究期間：2016～2019
課題番号：１６Ｋ１６０６８

研究課題名（和文）多ユーザ関数型準同型署名の研究

研究課題名（英文）Study on multi-user homomorphic functional signatures

研究代表者
山田　翔太（Yamada, Shota）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究員

研究者番号：７０７５０８３４

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：従来の電子署名技術を拡張した高機能な暗号技術として，情報の真正性とプライバシを保証しつつ，データ処理を可能にする準同型署名技術が存在する．しかし，従来の準同型署名では，署名生成に関するアクセス制限ができないこと，他ユーザ環境でのデータ処理ができないという制限がある．本研究ではこの制限を取り払うことを目指して研究し，他ユーザ環境でのアクセス制御を考慮した高機能署名技術である属性ベース署名をはじめとして，グループ署名やゼロ知識証明など，関連する高機能暗号方式を複数提案した．

研究成果の学術的意義や社会的意義
本研究では，目的としていた「多ユーザ関数型準同型署名」の設計を目指して研究し，目標に近い技術である属性ベース署名やグループ署名の設計を提案した．グループ署名方式は，シンプルなアクセス制御機構と，追跡可能性を保持した高機能電子署名技術で，提案方式は初めての量子コンピュータに対しても安全な方式である．また，研究の過程で新たな暗号理論的テクニックを発見し，複数の新たな高機能暗号技術を提案した．これは今後の当該分野の理論的発展および真に実用的な高機能暗号技術の実社会への普及に向けて，一定程度の意義があるものと考えられる．

研究成果の概要（英文）：Homomorphic signature is an advanced form of conventional digital signatures where one can homomorphically evaluate on the signatures while preserving authenticity and privacy of data. In homomorphic signatures, there are two limitations. Firstly, in homomorphic signatures, there is no mechanism to control the signing capability of the signing entity. Secondly, homomorphic evaluation on signatures is available only when the signatures are generated by the same entity. In this research project, we tried to overcome these limitations and obtained new cryptographic schemes such as attribute-based signature, which is an advanced form of signature that allows access control over signing entities in the multi-use settings, as well as group signatures and non-interactive zero-knowledge protocols as partial results.

研究分野：暗号理論

キーワード：電子署名　準同型署名　属性ベース署名　グループ署名　格子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

健康情報や個人のゲノム情報をクラウド上で利活用することで，医療技術等の著しい進展が期待できる．この場合，データの機密性は非常に高く，情報漏洩は絶対に避けなければならない．一方で，有用な知見を引き出すためには，プライバシを守りつつもデータ処理を行う必要がある．加えて，データ処理によって得られた結果の真正性の保証が必要である．部分的にこれらを解決する既存技術として，準同型署名が知られている．準同型署名においては，メッセージと対応する電子署名に対して，演算を施し新たな電子署名を得ることができる．プライバシ要件としては処理前の署名と対応するメッセージの情報が漏れないこと，真正性の保証としては署名に対して正しい演算を施した場合にのみ検証に通る署名を生成することを保証できる．一方で，当該技術には，同じ署名鍵で正当性を保証されたデータ同士でしか，データ処理を実行できないという制約がある．例えば医療データの処理への応用を考えた場合，分散的に生成された異なる鍵により生成された署名に対してデータ処理が可能であることが望ましく，上記の制約は当該技術の利用を阻害する要因となり得る．また，もう一つの問題点として，既存の準同型署名においては，誰でもデータ処理ができてしまうことが挙げられる．言い換えると，データ処理を行い，対応する署名を準同型的に生成する際には秘密情報が必要ではない．そのため，データの真正性は準同型署名の安全性によって保たれはするが，データの処理が恣意的であったり，悪意はなくても杜撰であったりすることを防ぐことはできない．

２．研究の目的

上記の問題を解決すべく，当研究課題では，異なる署名鍵で分散的に生成された署名同士に関して準同型演算を行うことが可能であり，また，適用可能な準同型演算の種類がその演算を行うユーザの属性の関数として定まるという性質を持つ，新しい暗号技術である「多ユーザ準同型署名」の提案を目指して研究を行った．前者の性質により，上述の例で言えば，異なる病院から得た健康情報に関する署名の統合が可能である．また，後者の性質により，例えば，心臓外科医は心臓のデータに関する処理を行い，対応する電子署名の作成が可能だが，腎臓や呼吸器に関して同様のことはできないということが保証できる．すなわち，可能な準同型演算の種類に関してもアクセス制御がなされることになる．

３．研究の方法

上記の研究課題達成のため，(1)「多ユーザ関数型準同型署名」の機能要件を現実世界での実用に向けて洗い出し，当該技術の実現を目指す方法と，(2)既存研究の拡張を続けることにより当該技術達成に向かってボトムアップ的に研究を進める方法が考えられる．研究提案段階では両アプローチを混ぜて進めることを想定していたが，実際の研究活動を進めるにあたって，(2)のアプローチの方が成功したため，こちらを主とした．特に，既存の準同型署名方式の機能拡張[Gorbunov et al. STOC'15]に取り組み，「多ユーザ関数型準同型署名」そのものではないが，目的としていた技術に近い技術の開発に成功した．下に示すグループ署名や準同型署名に関する成果がこれにあたる．また，同問題に取り組む過程で，ID ベース暗号や放送型暗号やゼロ知識証明など，関連する要素技術に関しても新たな成果を得ることができた．

４．研究成果

以下，本研究で得られた成果で代表的なものを挙げる．

（１）　目的としていた「多ユーザ関数型準同型署名」に最も近い要素技術として，多ユーザ環境下で署名生成にアクセス制御が可能であるような要素技術である「属性ベース署名」の一種を格子構造を利用して構成可能であることを示した．提案方式の設計においては，格子の準同型性を利用しており，当該方式は属性ベース署名方式とも，一種の多ユーザ環境における準同型署名方式ともみなすことができる．この得られた方式を部品として，格子に基づくグループ署名の構成という関連する未解決問題の解決に成功した．グループ署名は，非常にシンプルなアクセス制御を可能とした署名技術の一種であり，署名を生成したユーザを必要な場合には開示することが可能な技術である．当該成果は国際会議 EUROCRYPT 2019 に採録された[KY19]．

（２）　上記のグループ署名の双対的な暗号技術として，「放送型暗号」と「追跡可能暗号」が存在する．本研究では，これらの技術に関しても研究を行い，それぞれに関して成果を得た．前者に関しては格子理論と双線形写像を用いて漸近的に最適な効率性を達成しつつ，暗号学的難読化を利用しない初めての構成を示すことに成功した．暗号学的難読化には安全性の懸念が複数指摘されているため，提案方式は，同様の効率性を達成した既存技術に比べ高い安全性を達成していると言える．当該成果は国際会議 EUROCRYPT 2020 に採録され，また Best paper award を受賞した[AY20]．後者に関しては，追跡可能性とユーザ無効化機能を両立しつつ漸近的に高い効率性を持つ方式を提案し，国際会議 ACM-CCS 2017 に採録がされた[ABP+17]．

（３） 本研究の初期段階では足がかりとして，格子構造の準同型性を利用した ID ベース暗号の設計に取り組み，新方式を提案した． ID ベース暗号は従来の公開鍵暗号と異なり，任意の文字列（メールアドレス等）に向けて暗号化が可能な技術であり，アクセス制御技術である関数型暗号の特殊なケースである．ID ベース暗号は，通常の電子署名に容易に変換が可能であり，その意味で電子署名とも深い関連のある技術である．具体的には．従来の ID ベース暗号は，信頼性の非常に高い数学的仮定に基づく安全性を達成しようとすると，(1)選択的安全性という弱い安全性のみを満たしているか，(2)適応的安全性という高い安全性を満たしているが，公開鍵等のパラメータが大きいか，のどちらかであった．当該研究では，適応的安全性を達成しつつも，公開鍵長が従来よりも漸近的に短い方式の設計に成功した．これらの結果は Asiacrypt 2016[KY16]および Crypto 2017 にて発表した[Yam17]．

（４） 非対話ゼロ知識証明は，情報の真正性を保証する暗号技術であり，準同型署名との関連も知られている．本研究では事前処理を許した状態での非対話ゼロ知識証明を考察し，ペアリング群を使わない群上の初めての構成を示した。また，その過程で，群構造を利用した準同型署名も提案した．当該研究は Eurocrypt 2019 にて発表した[KNYY19]．

引用文献

[AY20] Shweta Agrawal, Shota Yamada:
Optimal Broadcast Encryption from Pairings and LWE
Proc. of (Part 1) of EUROCRYPT 2020, LNCS 12105, pp. 13-43, Springer 2020.
[ABP+17] Shweta Agrawal, Sanjay Bhattacherjee, Duong Hieu Phan, Damien Stehlé, Shota Yamada:
Efficient Public Trace and Revoke from Standard Assumptions.
ACM-CCS 2017, pp. 2277-229
[KY16] Shuichi Katsumata, Shota Yamada:
Partitioning via Non-Linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps
Proc. (Part 2) of ASIACRYPT 2016, LNCS 10032, pp. 682-712, Springer, 2016.
[KNYY19] Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa
Designated Verifier/Prover and Preprocessing NIZKs from Diffie-Hellman Assumptions.
Proc. of (Part 2) of EUROCRYPT 2019, LNCS 11477 , pp. 622-651, Springer, 2019.
[KY19] Shuichi Katsumata, Shota Yamada:
Group Signatures without NIZK: From Lattices in the Standard Model.
Proc. of (Part 3) of EUROCRYPT 2019, LNCS 11478 , pp. 312-344, Springer, 2019
[Yam17] Shota Yamada:
Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques
Proc. (Part 3) of CRYPTO 2017, LNCS 10401, pp. 161-193, Springer, 2017.

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　15件／うち国際共著　4件／うちオープンアクセス　2件）

１．著者名 Shweta Agrawal, Shota Yamada	４．巻 12105
２．論文標題 Optimal Broadcast Encryption from Pairings and LWE	５．発行年 2020年
３．雑誌名 Advances in Cryptology - EUROCRYPT 2020	６．最初と最後の頁 13-43
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-45721-1	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa	４．巻 12107
２．論文標題 Compact NIZKs from Standard Assumptions on Bilinear Maps	５．発行年 2020年
３．雑誌名 Advances in Cryptology - EUROCRYPT 2020	６．最初と最後の頁 379-409
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-45727-3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro	４．巻 11694
２．論文標題 Exploring Constructions of Compact NIZKs from Various Assumptions	５．発行年 2019年
３．雑誌名 Advances in Cryptology - CRYPTO 2019	６．最初と最後の頁 639-669
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26954-8	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Shweta Agrawal, Monosij Maitra, Shota Yamada	４．巻 11693
２．論文標題 Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE	５．発行年 2019年
３．雑誌名 Advances in Cryptology - CRYPTO 2019	６．最初と最後の頁 765-797
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26951-7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Shweta Agrawal, Monosij Maitra, Shota Yamada	4．巻 11892
2．論文標題 Attribute Based Encryption for Deterministic Finite Automata from DLIN	5．発行年 2019年
3．雑誌名 Theory of Cryptography	6．最初と最後の頁 91-117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36033-7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa	4．巻 11477
2．論文標題 Designated Verifier/Prover and Preprocessing NIZKs from Diffie-Hellman Assumptions	5．発行年 2019年
3．雑誌名 Advances in Cryptology - EUROCRYPT 2019	6．最初と最後の頁 622-651
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17656-3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shuichi Katsumata, Shota Yamada	4．巻 11478
2．論文標題 Advances in Cryptology - EUROCRYPT 2019	5．発行年 2019年
3．雑誌名 Advances in Cryptology - EUROCRYPT 2019	6．最初と最後の頁 312-344
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17659-4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shuichi Katsumata, Shota Yamada	4．巻 11443
2．論文標題 Non-Zero Inner Product Encryption Schemes from Various Assumptions: LWE, DDH and DCR	5．発行年 2019年
3．雑誌名 Public-Key Cryptography - PKC 2019	6．最初と最後の頁 223-253
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17259-6	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yamakawa Takashi、Yamada Shota、Hanaoka Goichiro、Kunihiro Noboru	４．巻 820
２．論文標題 Generic hardness of inversion on ring and its relation to self-bilinear map	５．発行年 2020年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 60～84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2020.03.009	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Shuichi Katsumata, Takashi Yamakawa, Shota Yamada	４．巻 11273
２．論文標題 Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model.	５．発行年 2018年
３．雑誌名 Advances in Cryptology - ASIACRYPT 2018	６．最初と最後の頁 252-282
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-03329-3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa	４．巻 10992
２．論文標題 Constrained PRFs for NC1 in Traditional Groups.	５．発行年 2018年
３．雑誌名 Advances in Cryptology - CRYPTO 2018	６．最初と最後の頁 543-573
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-96881-0	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nuttapong Attrapadung, Goichiro Hanaoka, Shota Yamada	４．巻 Vol. E100-A
２．論文標題 New Security Proof for the Boneh-Boyen IBE: Tight Reduction in Unbounded Multi-Challenge Security	５．発行年 2017年
３．雑誌名 IEICE transaction EA	６．最初と最後の頁 1882-1890
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shota Yamada	4．巻 10401
2．論文標題 Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques	5．発行年 2017年
3．雑誌名 Advances in Cryptology - CRYPTO 2017	6．最初と最後の頁 161-193
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-63688-7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shweta Agrawal, Sanjay Bhattacherjee, Duong Hieu Phan, Damien Stehle, Shota Yamada	4．巻 2017
2．論文標題 Efficient Public Trace and Revoke from Standard Assumptions	5．発行年 2017年
3．雑誌名 ACM-CCS 2017	6．最初と最後の頁 277-2293
掲載論文のDOI（デジタルオブジェクト識別子） /10.1145/3133956.3134041	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Shuichi Katsumata, Shota Yamada	4．巻 10032
2．論文標題 Partitioning via Non-Linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps	5．発行年 2016年
3．雑誌名 Advances in Cryptology - ASIACRYPT 2016	6．最初と最後の頁 682-712
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-662-53887-6	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　14件）

1．発表者名 Shweta Agrawal, Shota Yamada
2．発表標題 Optimal Broadcast Encryption from Pairings and LWE
3．学会等名 Eurocrypt 2020（国際学会）
4．発表年 2020年

１．発表者名
Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro

２．発表標題
Compact NIZKs from Standard Assumptions on Bilinear Maps

３．学会等名
Eurocrypt 2020（国際学会）

４．発表年
2020年

１．発表者名
Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro

２．発表標題
Exploring Constructions of Compact NIZKs from Various Assumptions

３．学会等名
CRYPTO 2019（国際学会）

４．発表年
2019年

１．発表者名
Shweta Agrawal, Monosij Maitra, Shota Yamada

２．発表標題
Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE

３．学会等名
CRYPTO 2019（国際学会）

４．発表年
2019年

１．発表者名
Shweta Agrawal, Monosij Maitra, Shota Yamada

２．発表標題
Attribute Based Encryption for Deterministic Finite Automata from DLIN

３．学会等名
TCC2019（国際学会）

４．発表年
2019年

１．発表者名
Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa

２．発表標題
Designated Verifier/Prover and Preprocessing NIZKs from Diffie-Hellman Assumptions

３．学会等名
Eurocrypt 2019（国際学会）

４．発表年
2019年

１．発表者名
Shuichi Katsumata, Shota Yamada

２．発表標題
Group Signatures without NIZK: From Lattices in the Standard Model

３．学会等名
Eurocrypt 2019（国際学会）

４．発表年
2019年

１．発表者名
Shuichi Katsumata, Shota Yamada

２．発表標題
Non-Zero Inner Product Encryption Schemes from Various Assumptions: LWE, DDH and DCR

３．学会等名
PKC 2019（国際学会）

４．発表年
2019年

１．発表者名
Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa

２．発表標題
Constrained PRFs for NC1 in Traditional Groups.

３．学会等名
Crypto 2018（国際学会）

４．発表年
2018年

１．発表者名
Shuichi Katsumata, Takashi Yamakawa, Shota Yamada

２．発表標題
Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model.

３．学会等名
Asiacrypt 2018（国際学会）

４．発表年
2018年

１．発表者名
Shota Yamada

２．発表標題
Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques

３．学会等名
CRYPTO 2017（国際学会）

４．発表年
2017年

１．発表者名
Duong Phan Hieu

２．発表標題
Efficient Public Trace and Revoke from Standard Assumptions

３．学会等名
ACM-CCS2017（国際学会）

４．発表年
2017年

１．発表者名
Shuichi Katsumata

２．発表標題
Partitioning via Non-Linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps

３．学会等名
Asiacrypt 2017（国際学会）

４．発表年
2016年

１．発表者名 Shota Yamada
２．発表標題 Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters
３．学会等名 Eurocrypt 2016（国際学会）
４．発表年 2016年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考