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　３ 年　 ５ 月 ２７ 日現在

機関番号：１４４０１
研究種目：若手研究
研究期間：2018～2020
課題番号：１８Ｋ１８０４９

研究課題名（和文）省計算能力デバイスでの利用に向けた更新機能を持つ高機能暗号の研究

研究課題名（英文）Research on Advanced Cryptography with Updatability for Devices with Low Computational Resources

研究代表者
矢内　直人（Yanai, Naoto）

大阪大学・情報科学研究科・助教

研究者番号：３０７３７８９６

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：高機能暗号として、独立に生成された電子署名を互いに集約できる集約署名について、緊密な帰着を持つ安全性証明を実現するとともに、そのネットワーク応用としてソフトウェアルータに搭載したプロトタイプを実装した。これにより、理論から実装に至るまで、集約署名のクラスとして高機能暗号の一貫した検討を行っている。また、データを暗号化した状態で検索できる検索可能暗号について、多人数での設定において暗号化ファイルごとにユーザアクセスを柔軟に制御する鍵集約検索可能暗号を、安全性を計算量理論の観点から証明できる方式を初めて構成した。鍵集約検索可能暗号についても実装評価を行っており、実装をGitHub に公開している。

研究成果の学術的意義や社会的意義
応用が不透明である高機能暗号について、理論から応用技術まで一貫して検討を行ったことに重要な学術的意義と社会的意義がある。理論研究の面からは社会的課題を踏まえた暗号理論を示しており、また、応用研究からは従来技術ではなしえなかった性能や仕様を達成するに至っている。とくに実装面に至る成果はプログラムを公開することで、再現性も確保している。

研究成果の概要（英文）：For aggregate signatures, which are an advanced cryptographic primitive to aggregate individual signatures, a security proof with a tight reduction was presented, and then a prototype implementation on a software router was provided as an application to networks. Hence, from theory to implementation, advanced cryptography had been discussed through a class of aggregate signatures. Meanwhile, searchable encryption that allows a user to search encrypted data was discussed. In particular, a key-aggregate searchable encryption scheme that can provide user-level access control for each file in the multi-user setting was proposed. The proposed scheme is the first scheme whose security can be proven in the multi-user setting. The scheme was also implemented, and source code is publicly available from GitHub.

研究分野：情報セキュリティ

キーワード：高機能暗号　ネットワーク　暗号化状態検索　コンピュータセキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Internet-of-Things (IoT) 機器は今日の社会において家電・医療機器・自動車など様々な用途・環境で幅広く利用されている。これらの機器の中には、ユーザの生活改善を提言すべく連続的にサーバにデータ発信を続けるセンサや、ユーザ自身が重要な情報をスマートフォンを用いてクラウドに保存する管理するなど、ユーザ個人の生活に強く紐づけられたものも少なくない。このような状況においては、ユーザ個人に密接に関連する情報がインターネットを介して外部とやりとりされることから、多くのユーザにとってセキュリティおよびプライバシーの保護が極めて重要となる。事実として、IoT 機器に関するセキュリティおよびプライバシー上の問題が多数報告されている（¥url{https://www.ipa.go.jp/security/iot/}）。

このような実情に対し、暗号技術の IoT 機器への適用が強く望まれている。
とくに、暗号文に対し平文の復号条件の埋め込みや電子署名の生成対象となる平文の指定など、暗号文や電子署名を介して平文を操作・制御する高機能暗号が高い関心を受けている。

しかしながら、一般に暗号技術は処理負荷が高く、IoT 機器によっては導入が難しい場合がある。とくにセンサ系で使われるようなマイコン 32-bit CPU など小型のアーキテクチャで設計されていることから、その負荷は無視できない。まして高機能暗号は、その演算負荷が従来の暗号よりも極めて高く、導入可能なセンサ機器は皆無といってよい。前述の通り、このような小型のアーキテクチャにおいても高機能暗号の利用は望まれることから、この計算負荷の問題を如何に解決するかが IoT 社会における重要な社会的問題といえる。

２．研究の目的

本研究では高機能暗号において、高速計算可能かつ安全性を保証可能な方式を実現することにある。とくに IoT などリソースが限られた機器に対し、各機器の使用状況や目的ごとにおける最適な機能と設定についても調査する。

３．研究の方法

本研究ではまず高機能暗号の中でも暗号文に平文を復号できるユーザの指定や平文の取得条件などを関数として埋め込める関数型暗号として、IoT など計算リソースが限られたデバイスに適した構成を明らかにする。つぎに、リソースが限られたデバイス上で実際に計算を行わせることで、計算性能および機器への影響を評価する。これらの検討を通じて、無数に存在しうる IoT 機器において、その用途ごとに指標となる鍵長などのパラメータも明らかにする。

以下に、その詳細について、具体的な研究手法と各年度の目標を含めて記載する。

3.1.　関数型暗号の構成と安全性証明

研究の第一段階として、リソースが限られたデバイスでも利用可能な関数型暗号を提案する。従来の関数型暗号は格子ベクトル空間に基づいて構成される。ここでいう格子ベクトル空間とは、基底ベクトル及びその基底から生成されるベクトルを用いて定義されるベクトル集合として定義される。このとき、二つのベクトル空間を入力にとり一つのベクトル空間に写像する関数として、互いに対をなす特定のベクトル以外は関数の計算結果が常に 0 になる性質を持つ関数を定義する。この関数を用いて暗号化と復号を行う。しかし、この格子ベクトル空間を伴う演算は負荷が大きい。このため、格子ベクトル空間を用いることなく方式を構成する。また、安全性については、暗号文から情報が洩れないことを数学的に証明することで、提案方式の安全性を明らかにする。とくに、汎用的な組み合わせによる構成と安全性の本質となる数学的性質を解明することで、任意の既存方式を通じた更新機能付き関数型暗号・関数型署名の構成も示す。

3.2.　関数型暗号の参照実装

研究の第二段階として、第一段階で提案した方式を実装する。既存のライブラリでは mcl (https://github.com/herumi/mcl) が任意の鍵長におけるパラメータ生成機能を有しており、まずは汎用計算機上で mcl ライブラリを利用して実装する。その後に、ラズベリーパイおよび TWELITE を仮想 IoT 機器として導入し、これらのプラットフォームに合わせた速度も計算する。また、本実装により、各プラットフォームにおける性能評価はもちろん、提案方式の実在性を机上検討の域を越えて示すことにもなる。

４．研究成果

本研究の成果は大きく三点である。まず高機能暗号の文脈として、(1)集約署名の緊密な帰着の構成、(2)鍵集約検索可能暗号の構成をそれぞれ示した。詳細は後述するがこれらはいずれも関数型暗号の局所系とみなせる。次に、(3)参照実装として、それぞれの実装に加え、集約署名は IoT 機器としてルータへの搭載を行った。それぞれの詳細を以下に述べる。

4.1.　集約署名の緊密な帰着の構成

集約署名は独立して生成された電子署名を互いに集約することで、電子署名の保存に係るメ

モリ量を削減する方式である。その集約できる特性を一種の関数とみなすことで、関数型署名の局所的な方式といえる。また、署名の集約により IoT 機器への導入やブロックチェーンへの応用など、近年では盛んに研究されている技術である。

この集約署名に関して、安全性の根拠となる Diffie-Hellman 計算仮定と緊密な帰着を持つ方式を構成した。緊密な帰着を持つ方式自体はこれまでにも知られていたが、申請者の結果ではどのような構成にすれば緊密な帰着となるか、原理を解き明かしたことが新しい。すなわち、従来の研究では偶発的に緊密な帰着を持つ方式が得られていたが、申請者はフルドメインハッシュ関数を持ち、かつ、署名者間で三回対話処理をはさむような構成であれば緊密な帰着を実現できることを示している。また、そのような条件に従う既存方式に対しても実際に緊密な帰着を実現できることも示している。当該成果については論文誌 IEICE Transactions に掲載されている。

さらにこの検討を進めていく中で、ネットワーク技術に向けた応用として、集約署名の機能を拡張することも検討した。とくに、集約署名から一部の署名検証機能を切り出す手法、及び、安全性を損なうことなく平文に対して一意に署名を生成する手法を、それぞれ考案した。前者の手法はインターネット経路制御、後者の手法は無線ネットワーク経路制御にそれぞれ適している。

具体的に、集約署名から一部の署名検証機能を切り出す手法は、署名の検証式の一部を検証式に変換することで実現した。一般に、検証式は各署名に対して一意に定まる構成となる。このため、検証式の一部を署名の要素として切り出し、また、その該当する署名を検証式の中で再度呼び出すことで、切り出された部分のみの署名を集約署名から検証することが可能となる。これは例えばインターネット経路制御において、新たに参入したネットワーク事業者に関連事業者の経路情報を送信する際などに有効である。この成果を国内の権威的会議である 2020 年コンピュータセキュリティシンポジウムに発表したところ高い評価を受け、論文賞（108 件中 9 件）を受賞している。また、通信分野を代表する査読付き国際会議 ICC 2021 にて発表を予定している。

一方、安全性を損なうことなく平文に対して一意に署名を生成する手法は、与えられた入力から一意に乱数を生成する疑似ランダム関数を用いることで実現した。疑似ランダム関数は代表的な暗号技術として知られる要素技術であるが、これを集約署名の文脈の中で用いることで安全性を低下させることなく、平文に対して一意に署名が定まる構成が新しい。とくに無線ネットワークのように通信環境を動的に再構成するような状況では、以前に用いた署名を再び生成することで、ネットワーク経路を速やかに再構築することが期待できる。この成果については、途中経過の成果を無線通信技術を代表する査読付き国際会議 WCNC 2019 にて発表し、また、理論的証明と無線環境での実験含めた評価を国際論文誌に現在投稿中である。

4.2. 鍵集約検索可能暗号の構成

鍵集約検索可能暗号は、多人数設定において、暗号化されたデータの検索とユーザアクセス制御を両立させる技術であり、検索を関数とみなした局所的な関数型暗号といえる。暗号化した状態で検索できる性質から、クラウドを用いたデータ共有を想定した検討が盛んである。しかしながら、既存の鍵集約検索可能暗号は厳密な安全性証明が付いておらず、安全性については直観的な議論を行っているか、あるいは証明が不完全なままであった。

本研究では Diffie-Hellman 計算仮定への帰着証明を伴う方式を示すことで、厳密に安全性を証明できる方式を初めて提案した。本研究の着想は大まかには集約署名の形式でユーザ鍵を発行し、かつ、限られたユーザ集合だけが暗号文にアクセスできる放送暗号のように暗号文を構成することである。具体的には、各データの暗号文に対し一意のインデックスを付与し、各データの暗号文の検索鍵は電子署名のように構成する。このとき、ユーザがもつ検索用の集約鍵をデータのインデックスを束ねた集約署名のように構成する。また、暗号文は放送暗号の構成とすることで、各暗号文のインデックスを含む集約鍵であれば、その暗号文に対する検索が可能となる。

既存方式も同様の構成をしていたが、本研究では上述した背景理論に従うことで、各要素技術に従う帰着証明を与えている。これに対し、既存方式では雑多な構成と言え、証明が得られなかった。この成果は国内の権威的会議である 2019 年コンピュータセキュリティシンポジウムに発表している。また、高インパクトファクターの国際論文誌 IEEE Access に掲載されている。

4.3. 参照実装

4.1 集約署名の緊密な帰着の構成で述べた方式をソフトウェアルータ BIRD に搭載し、実験評価を行った。BIRD は C 言語で記述された仮想ルータを提供するソフトウェアであり、実際のインターネット運用でも利用されている。本研究では IoT 想定機器として BIRD に提案方式を搭載することで、提案方式のプロトタイプをルータ上で実装している。

実験を通じて性能を評価したところ、ルータの処理時間については搭載前と比べて大幅に遅延していた。やはり高機能な暗号技術は計算時間への負荷も大きく、適用が難しいように思われる。一方で、確実に動作はしていたことから、計算の回数がそこまで多くない機器であれば導入できるユースケースも存在するように見受けられた。本成果については集約署名の構成と同様、2020 年コンピュータセキュリティシンポジウムに発表したところ高い評価を受け、論文賞（108 件中 9 件）を受賞している。また、通信分野を代表する査読付き国際会議 ICC 2021 にて発表を予定している。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Hideharu Kojima, Naoto Yanai, Jason Paul Cruz	４．巻 7
２．論文標題 ISDSR+: Improving the Security and Availability of Secure Routing Protocol	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 74849-74868
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2916318	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 －

１．著者名 Shimamoto Hayato, Naoto Yanai, Shingo Okamura, Jason Paul Cruz, Shouei Ou, Takao Okubo	４．巻 7
２．論文標題 Towards Further Formal Foundation of Web Security: Expression of Temporal Logic in Alloy and Its Application to A Security Model with Cache	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 74941-74960
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2920675	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 －

１．著者名 Masahiro Kamimura, Naoto Yanai, Shingo Okamura, Jason Paul Cruz	４．巻 8
２．論文標題 Key-Aggregate Searchable Encryption, Revisited: Formal Foundations for Cloud Applications, and Their Implementation	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 24153-24169
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.2967793	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13件（うち招待講演　1件／うち国際学会　4件）

１．発表者名 ゲッテ ヤン，矢内 直人，森 達哉
２．発表標題 SecureHID:USBインタフェースのセキュリティ
３．学会等名 コンピュータセキュリティ
４．発表年 2019年

１．発表者名
上村 真弘，矢内 直人，クルズ ジェイソン　ポール，岡村 真吾

２．発表標題
証明可能安全な鍵集約検索可能暗号の構成と実装評価

３．学会等名
コンピュータセキュリティシンポジウム2019（CSS 2019）

４．発表年
2019年

１．発表者名
王 晶栄，矢内 直人，大久保 隆夫，岡村 真吾

２．発表標題
sslstrip攻撃の脅威に関する検討

３．学会等名
コンピュータセキュリティシンポジウム2019（CSS 2019）

４．発表年
2019年

１．発表者名
Naoto Yanai

２．発表標題
On Security of Anonymous Invitation-Based System

３．学会等名
the 13th DPM International Workshop on Data Privacy Management (DPM 2018)（国際学会）

４．発表年
2018年

１．発表者名
Hideharu Kojima

２．発表標題
Implementation and Evaluation of ISDSR in Emulation Environments

３．学会等名
Proc. of the IEEE Wireless Communications and Networking Conference(WCNC) 2019（国際学会）

４．発表年
2019年

１．発表者名
清水 真之介

２．発表標題
Mininet-wifiを用いたISDSRの性能評価に関する研究

３．学会等名
IEICE 2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
Ouyang Junjie

２．発表標題
アグリゲート署名を用いたBGPsec AS_PATH検証手法の提案と実装評価

３．学会等名
コンピュータセキュリティシンポジウム2017（CSS 2017）

４．発表年
2018年

１．発表者名
Ouyang Junjie

２．発表標題
アグリゲート署名を用いたBGPsecの改良

３．学会等名
JANOG43ミーティング

４．発表年
2019年

１．発表者名
矢内直人

２．発表標題
ブロックチェーンで解決すべき応用課題やアプリケーション

３．学会等名
第21回 KECテクノフォーラム（招待講演）

４．発表年
2018年

１．発表者名
Tatsuya Takemura

２．発表標題
APVAS+: A Practical Extension of BGPsec with Low Memory Requirement

３．学会等名
2021 IEEE International Conference on Communications (ICC 2021)（国際学会）

４．発表年
2021年

１．発表者名
Naoki Umeda

２．発表標題
SQUAB: A Virtualized Infrastructure for Experiments on BGP and Its Extensions

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications (AINA 2021)（国際学会）

４．発表年
2021年

１．発表者名
竹村達也

２．発表標題
APVAS+: 集約署名を用いたAS パス検証プロトコルの改良とフルルート情報を想定した実験評価

３．学会等名
コンピュータセキュリティシンポジウム2020 (CSS 2020)

４．発表年
2020年

１．発表者名
梅田直希

２．発表標題
BGPsecの展開可能性に向けたBGPとの同時運用の検討

３．学会等名
コンピュータセキュリティシンポジウム2020 (CSS 2020)

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

大阪大学 大学院情報科学研究科 マルチメディア工学専攻 セキュリティ工学講座 http://www-infosec.ist.osaka-u.ac.jp/publications.html Naoto Yanai Web ページ http://www-infosec.ist.osaka-u.ac.jp/~yanai/yanaiweb.html 大阪大学 大学院情報科学研究科 マルチメディア工学専攻 セキュリティ工学講座 http://www-infosec.ist.osaka-u.ac.jp/publications.html Naoto Yanai Web ページ http://www-infosec.ist.osaka-u.ac.jp/~yanai/

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

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関