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　　元 年　　６ 月 ２６ 日現在

機関番号：８２６３６
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９８

研究課題名（和文）次世代暗号の実用化を支える新たな高度鍵更新手法の設計と安全性評価

研究課題名（英文）Research on Advanced Key Update Technique for Practical Applications of Advanced Cryptosystem

研究代表者

江村　恵太（Keita, Emura）

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所セキュリティ基盤研究室・主任研究員

研究者番号：３０５９７０１８

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：電子データを安全にやり取りする上で必要不可欠な技術の一つとして，暗号理論が知られている．ただし暗号自体は秘密鍵が漏洩しない状況での安全性を保証しているに過ぎないため，鍵漏洩対策は必須であるといえる．そこで本研究では，次世代暗号に適用可能な鍵管理方式の提案を行う．具体的には，効率的な鍵失効機能を持つIDベース暗号/属性ベース暗号/グループ署名を提案する．

研究成果の学術的意義や社会的意義
次世代暗号では，既存暗号に比べ秘密鍵を様々な用途に使用可能であるがゆえに，鍵漏洩が及ぼす影響が甚大であるという懸念がある．実際に問題が発生した例として,不正コピー防止技術HDCPおける鍵漏洩事件が知られている．これはTwitter上でIntel Global PRと名乗るユーザがHDCP用製品のデバイス鍵を作成可能なマスター鍵を拡散した事件である．ここで問題なのは，たかが一つのマスター鍵漏洩が全てのユーザに影響し，そのため攻撃者の鍵入手利益が非常に大きいという点である．この事例から明らかなように，適切な鍵管理対策を行うことは急務である．

研究成果の概要（英文）：Cryptography is widely recognized for realizing secure communication. We remark that cryptosystems are guaranteed to be security only when secret keys are suitably maintained. Thus, it is quite important to consider secret key exposure. In this research, we propose advanced key update/revocation techniques for practical applications of advanced cryptosystems. Concretely, we propose revocable identity-based encryption, revocable attribute-based encryption, and revocable group signatures.

研究分野：暗号理論

キーワード：鍵失効機能付きIDベース暗号　鍵失効機能付き属性ベース暗号　署名鍵有効期限付きグループ署名　鍵失効機能付きグループ署名

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

電子データを安全にやり取りする上で必要不可欠な技術の一つとして，暗号理論が知られている．ただし暗号自体は秘密鍵が漏洩しない状況での安全性を保証しているに過ぎないため，鍵漏洩対策は必須であるといえる．また最近では，高機能な次世代暗号が数多く提案され，クラウドへの応用などその実用化が進められている．次世代暗号では，既存暗号に比べ秘密鍵を様々な用途に使用可能であるがゆえに，鍵漏洩が及ぼす影響が甚大であるという懸念がある．例えばクラウド上の暗号化データ管理システムでは，鍵漏洩発生時に個人情報 (医療情報など) が閲覧し放題となる．

２．研究の目的

上述の背景を鑑み，次世代暗号に適用可能な鍵管理方式の提案を行う．具体的には，効率的な鍵失効機能を持つ ID ベース暗号/属性ベース暗号/グループ署名を提案する．

３．研究の方法

まず次世代暗号の中で最も基礎的な ID ベース暗号に対し，効率的な鍵失効機能を付加する．次に ID ベース暗号の上位概念である属性ベース暗号について鍵失効機能を付加する．さらに鍵漏洩問題を解決する新たな方策として鍵に有効期限を設定することで，鍵漏洩の影響を有効期限内にのみ限定可能なグループ署名方式の提案を進める．本研究計画においては，国立研究開発法人情報通信研究機構 江村 恵太 主任研究員を研究代表者，同主任研究員 林 卓也，国立研究開発法人産業技術総合研究所研究チーム長・花岡 悟一郎，同チーム長・Nuttapong Attrapadung，同主任研究員 松田隆弘を研究分担者として，研究に取り組むものとする．

４．研究成果

素数位数を持つ非対称双線型群上での構成，かつ復号鍵漏洩耐性を持ち，公開パラメータ長がユーザ数に依存しないという点でこれまで提案された鍵失効機能付き ID ベース暗号の中で最も効率的な鍵失効機能付き ID ベース暗号を提案した．本成果をコンピュータセキュリティシンポジウム 2016 (CSS2016) で発表するとともにプレプリントサーバにも展開，また国際会議 CT-RSA2017 で発表した．さらに改良を加え効率化した方式を国内会議 SCIS2019 にて発表した．また非常に広いクラスの属性ベース暗号方式に鍵失効機能を付加する一般的構成を提案し，国内会議 SCIS2017，国際会議 ESORICS2017，英文論文誌 IEICE にて発表した．Pair encoding フレームワークを用いた一般的構成を与えたことから，用途に応じた様々な鍵失効機能付き属性ベース暗号が構成できる．本一般的構成から得られる属性ベース暗号は適応的安全性を満たすことが保証される．正規言語を扱う方式，属性サイズが無制限である方式，暗号文長や秘密鍵長が定数である方式について，これまで適応的安全である方式が提案されていなかったが，本研究成果により全ての方式が得られるため，その意義は大きいと評価する．次に鍵に有効期限を持たせるグループ署名方式の提案について，国内会議 SCIS2017，国際会議 AsiaCCS2017，英文論文誌 IEEE Transactions on Dependable and Secure Computing にて発表した．既存方式において署名長がユーザ数に依存していたという問題を解決し，はじめて署名長が定数である方式を構成した．さらに署名生成と検証コストがユーザ数に依存しない鍵失効機能付きグループ署名，国内会議 SCIS2018，国際会議 ISC2018 にて発表した．

５．主な発表論文等

〔雑誌論文〕（計 3 件）

1　Keita Emura, Takuya Hayashi, Ai Ishida: Group Signatures with Time-bound Keys Revisited: A New Model, an Efficient Construction, and its Implementation. IEEE Transactions on Dependable and Secure Computing. 査読有. DOI: 10.1109/TDSC.2017.2754247. (採録決定)

2　Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka: Generic Constructions for Fully Secure Revocable Attribute-Based Encryption. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences. 2019. PP: 1456-147. 査読有. DOI: 10.1587/transfun.E101.A.1456.

3　Yohei Watanabe, Keita Emura, Jae Hong Seo: New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters. 2016. 査読なし.

〔学会発表〕（計 9 件）

1　Keita Emura, Takuya Hayashi: A Revocable Group Signature Scheme with Scalability

from Simple Assumptions and Its Implementation. ISC 2018. 査読有.
2 高安 敦, 渡邉 洋平, 江村恵太: より効率的で適応的に安全な鍵失効機能付き ID ベース暗号の構成. 暗号と情報セキュリティシンポジウム (SCIS) 2019. 査読なし.
3 江村 恵太: 標準的な仮定で安全かつスケーラブルなメンバ削除可能グループ署名. 暗号と情報セキュリティシンポジウム (SCIS) 2018. 査読なし.
4 Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka: Generic Constructions for Fully Secure Revocable Attribute-Based Encryption. ESORICS 2017. 査読有.
5 Keita Emura, Takuya Hayashi, Ai Ishida: Group Signatures with Time-bound Keys Revisited: A New Model and an Efficient Construction. AsiaCCS 2017. 査読有.
6 Yohei Watanabe, Keita Emura, Jae Hong Seo: New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters. CT-RSA 2017. 査読有.
7 山田 古都子, アッタラパドゥン・ナッタポン, 江村 恵太, 花岡 悟一郎, 田中 圭介: 適応的安全な無効化可能属性ベース暗号の一般的構成. 暗号と情報セキュリティシンポジウム (SCIS) 2017. 査読なし.
8 江村 恵太, 林 卓也, 石田 愛: 署名鍵有効期限付きグループ署名の効率化とその実装評価. 暗号と情報セキュリティシンポジウム (SCIS) 2017. 査読なし.
9 渡邉 洋平, 江村 恵太: 素数位数群における効率的な鍵失効機能付き ID ベース暗号の構成法. コンピュータセキュリティシンポジウム 2016. 査読なし.

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況 (計 0 件)
○取得状況 (計 0 件)

〔その他〕
ホームページ等: なし

６. 研究組織

(1)研究分担者

研究分担者氏名：花岡　悟一郎

ローマ字氏名：Goichiro Hanaoka

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：サイバーフィジカル研究センター高機能暗号研究チーム

職名：研究チーム長

研究者番号 (8 桁)：30415731

研究分担者氏名：Attrapadun Nutt

ローマ字氏名：Attrapadun Nutt

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：イバーフィジカル研究センター暗号プラットフォーム研究チーム

職名：研究チーム長

研究者番号 (8 桁)：40515300

研究分担者氏名：松田　隆宏

ローマ字氏名：Takahiro Matsuda

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：サイバーフィジカル研究センター高機能暗号研究チーム

職名：主任研究員

研究者番号 (8 桁)：60709492

研究分担者氏名：林　卓也

ローマ字氏名：Takuya Hayashi

所属研究機関名：国立研究開発法人情報通信研究機構

部局名：サイバーセキュリティ研究所セキュリティ基盤研究室

職名：主任研究員
研究者番号（8 桁）：70739995

(2)研究協力者
該当なし