様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 ２０ 日現在

機関番号：３２６６１
研究種目：若手研究(B)
研究期間：2013～2014
課題番号：２５７３００８２

研究課題名（和文）新世代型暗号における鍵管理手法の研究

研究課題名（英文）Key management schemes for new-era cryptography

研究代表者
金岡　晃（KANAOKA, Akira）

東邦大学・理学部・講師

研究者番号：００４５５９２４

交付決定額（研究期間全体）：（直接経費）　　1,500,000円

研究成果の概要（和文）：RSAやECCなど従来型の公開鍵暗号と異なりさまざまな機能が利用可能なIDベース暗号に代表される高機能暗号の研究が盛んである。ここではそれらを新世代暗号と呼ぶ。新世代型暗号の実用化はまだまだ途上であるが重要な点として鍵管理の検討がある。鍵の安全性に論拠した理論的な安全が実用面で毀損されることを割けるため、新世代暗号に関しても鍵管理を考えなければならない。本研究では従来型暗号と新世代暗号での鍵管理の共通性の調査検討や新世代型暗号に必要な鍵管理手法の提案とソフトウェア実装による試作を行った。

研究成果の概要（英文）：New type public key encryption schemes has been studied in these years. Such schemes has useful functions conventional public key encryption schemes does not have. In this research, we call these new schemes as "new-era cryptography".
It is still on the way to the practical use of new-era cryptography. One of most significant point to be practical is cryptographic key management. To avoid compromising new-era cryptography which has rational security proof by practical scene, we have to study cryptographic key management for new-era cryptography. In this research, firstly we compare between conventional public key cryptography and new-era cryptography and pick up common part and different part. Then we propose new key management method for new-era cryptography and develop prototype implementation using identity based encryption schemes.

研究分野：情報セキュリティ

キーワード：暗号技術　暗号鍵管理　新世代暗号

１．研究開始当初の背景

1984 年に Shamir によって ID ベース暗号はそのコンセプトが提案された。RSA や楕円曲線エルガマル暗号とはことなり、公開鍵のデータを任意に設定が可能という特徴を持つ。しかし現実的な実現方法は提案されておらず長くコンセプトのみとなっていたが、2000 年になり境らにより双線形写像ペアリングを用いた方式が提案され、また Boneh らによる方式が提案されるなど近年研究が活発になっている。ID ベース暗号研究の本質は「任意データによる暗号化」を可能とするものであり、ID による暗号化を越えて属性ベース暗号、特定時刻による復号を可能にする Timed-Release Encryption（TRE）、暗号化されたデータ中の検索を可能にする検索可能暗号などがその後相次いで発表され、さらに暗号化されたデータ同士の演算を可能にする完全準同型暗号（Fully Homomorphic Encryption）の実現がされるなど、これまでの公開鍵暗号とは異なる用途を持つ新世代型暗号の研究開発が非常に盛んである。

近年では新世代型暗号の皮切りとなった ID ベース暗号の標準化が IEEE や IETF といった標準化団体で進むなど新世代型暗号は実用化に向けた段階に進みつつあると言える。

しかし手法が標準化されるだけでは暗号は実用化には至らない。実用化に向けて特に重要となる課題が鍵管理である。鍵管理は鍵の生成から配送・保管・バックアップ・失効・廃棄・回復など技術と管理手法が多岐にわたっており、そのいずれか 1 つが毀損するだけでも暗号鍵の安全性は失われることから、数学的な鍵の安全性と同様に鍵管理の技術と管理手法は暗号技術にとって重要な要素となっている。新世代型暗号ではこの鍵管理に関する技術と管理手法についての研究がほとんどされていない

２．研究の目的

ID ベース暗号や属性ベース暗号、さらに完全準同型暗号といった既存の公開鍵暗号の用途を大幅に変える暗号方式（本研究ではそれらを新世代型暗号と呼ぶ）が近年急速に研究されている。新世代暗号の特徴は、機能に応じて ID 基盤や属性基盤など他の基盤を活用して暗号サービスを提供する部分にあり、暗号鍵の管理は活用する基盤との連携のもと果たされなければならない。しかし新世代暗号の鍵管理に関する研究はほとんど行なわれていない。そこで本研究では以下 3 つの研究を行うことを目的とした：(1) 既存公開鍵暗号との鍵管理手法の共通性調査・検討、(2) 新世代型暗号に独自に必要な鍵管理手法の提案、(3) ソフトウェア実装によるモジュール化と管理環境試作

３．研究の方法

米国の標準技術局（NIST）では、SP 800-57 において鍵管理の推奨ガイドラインを定めており、そこでは公開鍵暗号方式の鍵管理は以下の項目に細分化されている。

鍵生成、鍵配送、鍵の利用（鍵の変更、導出含む）、鍵の保管/バックアップ、鍵の期限切れ/失効/廃棄、鍵の回復

本研究では最初に「(1) 既存公開鍵暗号との鍵管理手法の共通性調査・検討」を行う。

新世代型暗号方式はその特徴から既存の公開鍵暗号系とは異なる部分が多い。例えば鍵生成において、既存の RSA や DSA、楕円曲線暗号（ECC）といった公開鍵暗号系では公開鍵と秘密鍵（Private Key）の鍵ペア生成者は「利用者または信頼できる第三者（認証局など）」であるが、ID ベース暗号や属性ベース暗号、TRE は、利用者は既に暗号鍵となる情報（ID や属性、時刻）をもっているが利用者自身では ID 情報に対応した秘密鍵生成を行うことができず信頼できる第三者（ID ベース暗号では鍵生成センタと呼ぶ）が行わなければならない。このことから、鍵生成センタへの公開鍵情報送付や公開鍵情報の被付与者であることの証明（認証）を行わなければならず、既存公開鍵手法と異なる鍵生成の運用が必要となる。このように新世代型暗号における鍵管理は SP 800-57 で挙げられた項目の多くで既存公開鍵暗号手法と異なる技術と管理手法を行わなければならない可能性があるため、その共通性調査と検討を行う。

上記(1)において得られた結果から「(2) 新世代型暗号に独自に必要な鍵管理手法の提案」を行う。新世代型暗号は従来の公開鍵暗号を超えたさまざまな用途で利用されるために、(1)の結果が多岐にわたる場合は項目を絞り(2)に臨むこととする。しかしいかなる用途であろうと「鍵生成」「鍵保管/バックアップ」「鍵の期限切れ/失効/廃棄」については暗号鍵の管理において欠かせない項目とされているものであり、用途によっては必要ないとされる部分でもその不必要な性質を十分に説明する必要があるため、重点的に研究を行う。

(1)・(2)により得られた結果の中で特に ID ベース暗号、を対象に「(3)ソフトウェア実装によるモジュール化と管理環境試作」を行う。

４．研究成果

（1）既存公開鍵暗号との鍵管理手法の共通性

既存公開鍵暗号を RSA 暗号、ECDH（Elliptic Curve Diffie-Helman）鍵交換や ECDSA（Elliptic Curve Disigal Signature Algorithm）、ECMQV（Elliptic Curve Menezes-Qu-Vanstone）を合わせた ECC（Elliptic Curve Cryptography、楕円曲線暗号）の 2 種類とし、新世代暗号で最も歴史が深く実用化に近い ID ベース暗号について、その共通性の比較を行い、4 点の差異を明確にした。

<1> 鍵生成のタイミング
ID ベース暗号では、プライベート鍵（復号鍵）は暗号文生成時（暗号化時）には必要ない。そのため、プライベート鍵の事後発行が可能になる。

<2> 鍵と ID の紐づけ
RSA や ECC ではその暗号プロトコルの特徴から公開鍵とプライベート鍵のペアは任意に設定できず、乱数をもとにそれぞれの特徴で生成されたデータとなる。鍵の利用者は、他人の公開鍵の所有が実際に所有者によりなされているかの確認が鍵データを見るだけでは判断ができないため何らかの紐づけの必要性がでる。ID ベース暗号では、識別子（Identifier、ID）のような任意のデータを公開鍵データに設定することが可能であるため、紐づけが不要となる。

<3>プライベート鍵の生成者
RSA や ECC では、鍵ペアの生成は権威サーバ（Authority）による発行と利用者自身による発行のいずれも可能である。プライベート鍵の利用者による所持の信頼担保するために暗号アルゴリズムとは異なる仕組みが必要となる。PKI（Public Key Infrastructure、公開鍵基盤）はそういった仕組みを提供する仕組みである。
ID ベース暗号では、プライベート鍵は権威サーバ（ID ベース暗号では KGC（Key Generation Center、鍵生成センタ）あるいは PKC（Private Key Generator、プライベート鍵生成者）と言われる）の持つサーバシークレットと利用者 ID により生成されるため、利用者自身による生成は不可能である。

<4>鍵の失効と ID の失効
RSA や ECC では、暗号鍵を失効する場合には利用者 ID を失効する必要はない。その代わり、その紐づけをしている情報の失効が必要となる。これらも暗号アルゴリズムでは達成されず、PKI の 1 つの機能として実現される。具体的には公開鍵証明書でその保証がされている。
ID ベース暗号では、プライベート鍵を失効する場合は公開鍵にした情報も併せて失効しなければならない。公開鍵にした情報が ID そのものである場合は、ID を失効しなければならない。

（2）新世代型暗号に独自に必要な鍵管理手法の提案

NIST SP800-57 による暗号鍵の状態と遷移を図 1 に示す。また鍵状態とは別に、以下の 4 つのフェーズを持つ
・運用前フェーズ
・運用フェーズ
・運用後フェーズ

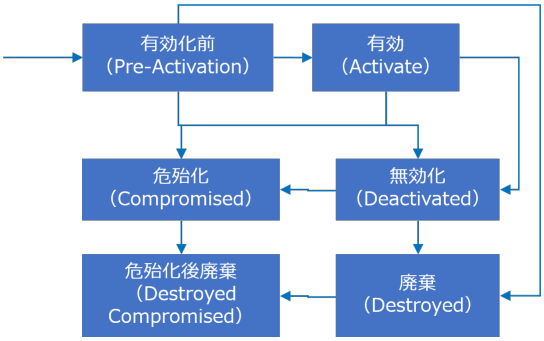

図 1 NIST SP 800-57 における鍵状態遷移

・廃棄フェーズ
これらを直接新世代型暗号に当てはめるのは、その鍵ペアの独立性から難しい。そこで（1）と同様に ID ベース暗号に焦点をあて、その独立性から暗号鍵の状態遷移とフェーズについて鍵ペアの関連性を考察し、まとめた。表 1 は ID と鍵の各フェーズにおける依存関係を示したものである。表中の「○」はその状態を許容し、「△」は暗号用途に依存する。そして「×」は状態が許容されない。「△」の場合、電子署名と暗号化でその許容が変わる。

表 1 鍵と ID のフェーズ間依存関係

		ID 情報			
		運用前	運用	運用後	廃棄
プライベート鍵	運用前	○	○	○	×
	運用	×	○	△	△
	運用後	○	○	○	○
	廃棄	○	○	○	○

表 2、3、4、5 は ID とプライベート鍵の各フェーズ・状態における依存関係を示したものである。表 1 と同様に、表中の「○」はその状態を許容し、「△」は暗号用途に依存する。そして「×」は状態が許容されない。「△」の場合、電子署名と暗号化でその許容が変わる。

これらのことから、ID ベース暗号では鍵管理において公開鍵となる ID の管理と密接に連携しなければならないことが判明した。それらの関係性は単純ではなく、新世代型暗号ではその管理がより複雑になることが示された。

表 2　フェーズ・状態間依存関係（1）

			ID 情報	
			運用前	
			生成	有効化前
秘密鍵	運用前	生成	○	○
		有効化前	-	○
	運用	有効	-	×
		一時停止	-	×
		失効	-	×
	運用後	無効化	-	×
		危殆化	-	○
	廃棄	廃棄	-	○
		危殆化後廃棄	-	○

表 3 フェーズ・状態間依存関係（2）

			ID 情報		
			運用		
			有効	一時停止	失効
秘密鍵	運用前	生成	○	○	×
		有効化前	○	○	×
	運用	有効	○	×	△
		一時停止	○	○	△
		失効	○	○	○
	運用後	無効化	○	○	○
		危殆化	○	○	○
	廃棄	廃棄	○	○	○
		危殆化後廃棄	○	○	○

表 4 フェーズ・状態間依存関係（3）

			ID 情報	
			運用後	
			無効化	危殆化
秘密鍵	運用前	生成	×	×
		有効化前	×	×
	運用	有効	△	△
		一時停止	△	△
		失効	○	○
	運用後	無効化	○	○
		危殆化	○	○
	廃棄	廃棄	○	○
		危殆化後廃棄	○	○

表 5 フェーズ・状態間依存関係（4）

			ID 情報	
			廃棄	
			廃棄	危殆化後廃棄
秘密鍵	運用前	生成	×	×
		有効化前	×	×
	運用	有効	△	△
		一時停止	△	△
		失効	○	○
	運用後	無効化	○	○
		危殆化	○	○
	廃棄	廃棄	○	○
		危殆化後廃棄	○	○

（3）ソフトウェア実装によるモジュール化と管理環境試作

鍵の状態管理とデータ表現等の現実化とその利用における検討点抽出のために、新世代型暗号のソフトウェア実装を行った。本研究では、(1)(2)と同様に新世代型暗号の中で代表的な ID ベース暗号に焦点をあて、実装を行った。実装は Boneh-Franklin の方式（以後 BF 方式と記載）と Waters の方式（以後 Waters 方式と記載）の 2 種類を実装した。

実装は C 言語で行い、ペアリング関数や関連する楕円曲線上の点の演算等は、C 言語ライブラリである TEPLA を利用した。各実装はそれぞれの ID ベース暗号の 4 つの関数である setup、extract、encrypt、decrypt の 4 つの関数を持っている。

図 2 は BF 方式の各関数の実行時間を示したものとなっている。平均実行時間だけでなく、最大実行時間と最少実行時間も併せてしめしている。

図 3 は Waters 方式の各関数の実行時間を示したものとなっている。BF 方式の図 2 とは異なる表現となっているが、Waters 方式では ID として扱うデータの長さ（ビット長）に応じて処理の時間が異なるため、横軸にビット長を設定し、複数のビット長でその性能を評価している。

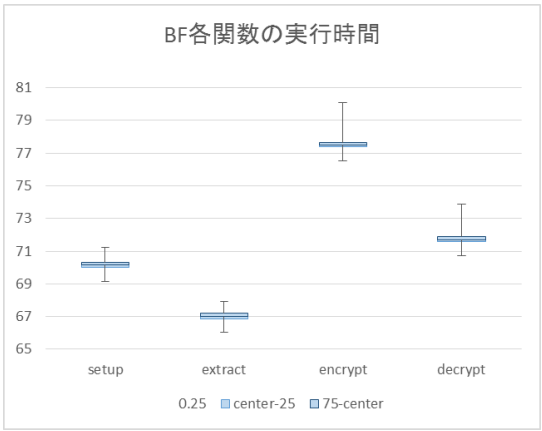

図 2　BF 方式の実行時間

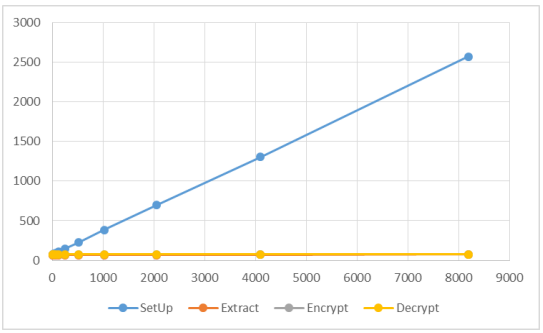

図 3 Waters 方式の実行時間

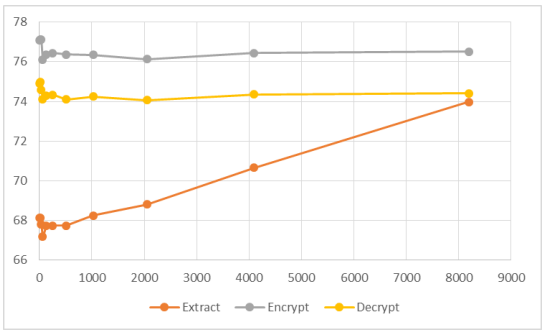

図 4 Waters 方式の実行時間

図 4 は図 3 のうち setup を除いた時間を示したものである。
setup と extract が ID のビット長に比例して実行時間が増加していることに対して、encrypt と decrypt は ID のビット長にかかわらずほぼ一定の値になっていることが分かる。
プライベート鍵のデータ出力は方式に応じたものとした。BF 方式では楕円曲線上の点 1 つでプライベート鍵が構成されるが、Waters 方式では 2 つの点でプライベート鍵が構成される。
実装は汎用性を考慮して作成したため広い用途で利用可能となっている。そのことから、それぞれの方式のソースプログラムは全世界からアクセス可能な GitHub に公開をした。またその適用を容易にするためにサンプルプログラムも併せて公開している。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0　件）

〔学会発表〕（計　1　件）
[1] 金岡晃、“ID ベース暗号の概観と今後の展望”，次世代セキュア情報基盤ワークショップ、2013 年 8 月 29 日、広島大学、広島県東広島市

〔図書〕（計　0　件）

〔その他〕
作成ソフトウェア公開ページ：
Boneh-Franklin 方式 ID　ベース暗号
https://github.com/KlabIBEDevTeam/BonehFranklinCode
Waters 方式 ID ベース暗号
https://github.com/KlabIBEDevTeam/WatersCode

６．研究組織
(1)研究代表者
金岡　晃（KANAOKA, Akira）
東邦大学・理学部・講師
研究者番号：00455924

(2)研究分担者
なし

(3)連携研究者
なし