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 １９ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８８

研究課題名（和文）電子書籍システムのための高機能暗号技術の研究

研究課題名（英文）Research of cryptography with advanced functionality for e-book system

研究代表者
白勢　政明（Shirase, Masaaki）

公立はこだて未来大学・システム情報科学部・准教授

研究者番号：７０５３０７５７

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：近年研究が盛んである高機能暗号技術を応用した電子書籍における著作権保護や貸借管理を実現するシステムの開発を目的として、サーバへのアクセスが不要な電子書籍の貸借システムを考案し、実験的実装により動作確認を行った。この方式に必要な楕円曲線のペアリング演算は重い処理であるため、ペアリング演算の代替となり計算が軽量なMe演算を提案し、Me演算の理論的性質を調べた。その結果、Me演算を用いた暗号はまだ実用化には至らないが、鍵長が等しい楕円曲線暗号と比較して攻撃がより困難であることが判明した。

研究成果の学術的意義や社会的意義
2000年以降研究が盛んであるが実用化はあまり進んでいない高機能暗号を初めて電子書籍システムに応用した点が本研究の学術的意義である。本研究で用いた高機能暗号は再代理人暗号であるが、類似手法のIDベース暗号、属性ベース暗号、放送型暗号といった別の高機能暗号も電子書籍システムへ応用することで暗号技術により電子書籍システムに新たな機能の付加が可能であることを示唆しており、電子書籍システムの発展に寄与できる点が本研究の社会的意義である。

研究成果の概要（英文）：In order to develop an e-book system that realizes copyright protection and lending and borrowing management that applies cryptography with advanced functionality, which has been actively researched in recent years, the research devised a lending and borrowing management system for e-books that does not require access to any server, and the system is experimentally confirmed the operation by mounting. Since pairing operation required for this method is a heavy process, an alternative to pairing operation is proposed, which is called Me operation, and the theoretical properties of Me operation are investigated. As a result, although encryption using Me operation is not yet put to practical use, it turned out that the attack is more difficult compared to the elliptic curve cryptosystem with the same key length.

研究分野：情報セキュリティ

キーワード：暗号　楕円曲線暗号　高機能暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

(1) 2012 年、電子図書の代表的なフォーマットある EPUB のための基準システムの開発を目的とするプロジェクト Readium において、電子書籍のための軽量な著作権保護技術の実装の必要性から Readium Lightweight Content Protection (LCP) が提案された[引用①]。(現在 LCP は Licensed Content Protection を意味する用語となった。) LCP では次のような方式を行う(図 1)。(a) 販売者は、デファクト・スタンダードな共通鍵暗号である AES でコンテンツを暗号化し、その暗号化ファイルを購入者に配布する。(b) 販売者は、AES 鍵を購入者の公開鍵を使って公開鍵暗号により暗号化し、購入者に配布する。(c) 購入者は自身の秘密鍵を使って AES 鍵を復元し、それを使ってコンテンツを復号する。このようにすることで、秘密鍵所有者のみがコンテンツの閲覧が可能となる。

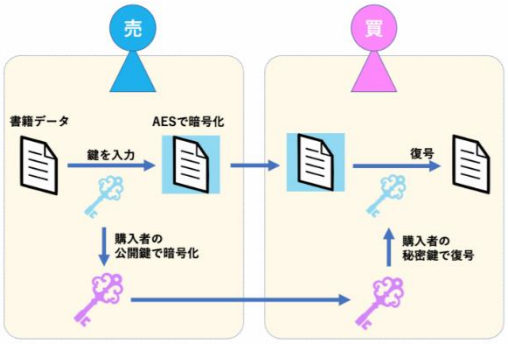

図 1　LCP の暗号化方式

(2) 2000 年のペアリング演算を用いた ID ベース暗号の提案を最初として、属性ベース暗号、放送型暗号、キーワード検索暗号、代理人暗号といった高機能暗号の研究が盛んであるが、実用化はあまり進んでいなかった。なお、ペアリング演算は楕円曲線上の演算であり、ペアリングを用いる高機能暗号は楕円曲線暗号の拡張と見なすことができる。

２．研究の目的

本研究の目的は、電子書籍における著作権保護(DRM)や貸借管理などを実現する軽量計算の暗号技術を研究し実装することである。電子書籍は著作者・出版社の立場では容易に書籍を製作できるという利点があるが、電子書籍はコピーも容易であることから著作権保護が不安視されている。また、読者の立場では購入の便利さはあるものの、紙の本では可能な友人間での貸借が難しく古本流通ができないといった不便さがある。従って電子書籍の更なる普及にはこれらの不安材料や不便さを解消する必要がある。高機能暗号技術は暗号技術のみでアクセス制御を可能としており、LCP での AES 鍵配布のための公開鍵暗号に高機能暗号を応用することで電子書籍システムの機能の拡充が期待できる。

３．研究の方法

(1) 電子書籍システムに求められる機能の調査：日本電子出版協会(JEPA)からの情報を収集し、高機能暗号で実現でき(当時の)LCP に準拠した機能を選別する。

(2) ペアリング演算のコスト削減：Complex Multiplication (CM)法などを用いて、高機能暗号で用いるペアリング演算を高速に行えるような楕円曲線の構成法を研究する。また、楕円曲線の点加算の方法の改良も行う。

(3) 安全で便利な電子書籍システムの開発：(1)による暗号プロトコルを(2)による手法を用いて、安全な電子書籍システムの実験的プログラムを作成し動作を確認する。

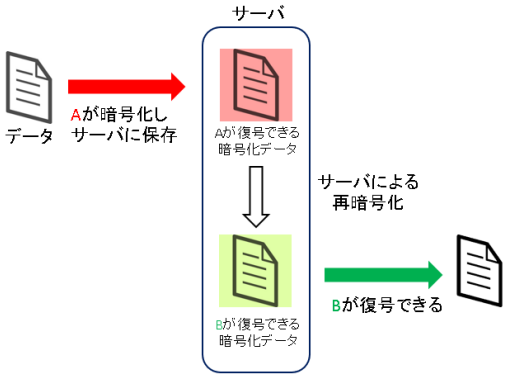

図 2　代理人暗号

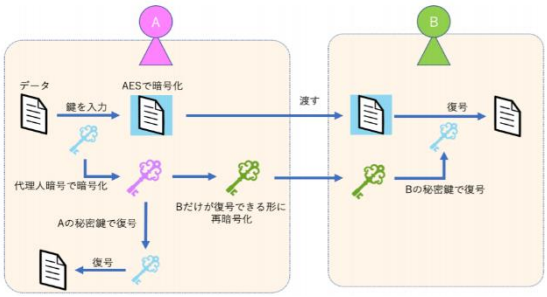

図 3　開発したシステム

４．研究成果

(1)　代理人暗号を用いた安全な貸借システムの研究開発

① 代理人暗号について：初めに、本研究で用いた代理人暗号を紹介する。代理人暗号とは、ユーザ A が暗号化したデータをサーバに保存し別のユーザ B がそのデータを必要とする時、データを復号せずに B が復号できる暗号化データに再暗号化できる技術である(図 2)。勿論、A 自身もデータを復号できる。

② 代理人暗号を用いた貸借システムの提案：代理人暗号を応用し、次の機能を有する電子書籍システムを開発した(図 3)。(a) コンテンツ販売者のサーバへアクセスせず、コンテンツの貸借が可能。(b) コンテンツ所有者はユーザ A に貸借させることは可能だが、A は別のユーザに貸借させることは不可。(c) (当時の)LCP に準拠しており、AES 鍵配布の方法以外は LCP で示されて

いる暗号方式と同じ方式。(d) 高機能暗号の１つである代理人暗号の技術を用いる。
なお代理人暗号には、楕円曲線の 2 点P、Qから有限体の元を計算するペアリング演算$e(P,Q)$を用いる。ペアリング演算は双線形$e(P,Q_0+Q_1)=e(P,Q_0)\cdot e(P,Q_1)$、$e(P_0+P_1,Q)=e(P_0,Q)\cdot e(P_1,Q)$を満たすことが重要な特徴である。
更に、本システムの実験的実装を行い、エラーなく動作することを確かめた。なお、ライブラリとして、多倍長精度の符号付き整数の演算を行うための GNU Multi-Precision Library(GMP)、ペアリング演算を行うための TEPLA、SSL/TLS プロトコルの基本的な暗号化関数とユーティリティ関数を提供する OpenSSL を用いた。

(2) Me 演算－代理人暗号や高機能暗号の高速化を目的とする演算－の提案
代理人暗号を含めいくつかの高機能暗号は、楕円曲線上のペアリング演算$e(P,Q)$を用いる。しかしながらペアリング演算は処理コストが大きいことが課題である。本研究では、双線形性の類似を持つ Me 演算および Me スカラー倍を提案し、これらの性質を調べた。
Me 演算は楕円曲線の点$P,Q\in E(\mathbb{F}_p)$に対して

$$P\oplus Q=Me(P,Q)=\begin{cases}P & P=Q\text{の時}\\ 2P-Q & P-Q\text{の}y\text{座標が}\mathbb{F}_p\text{の平方元の時}\\ 2Q-P & P-Q\text{の}y\text{座標が}\mathbb{F}_p\text{の非平方元の時}\end{cases}$$

と定義される。Pをベースポイント、Zを補助元とする Me スカラー倍は次のアルゴリズムによって定義される。

入力: $P,Z\in E(\mathbb{F}_p)$, 自然数nの 2 進数表現$(1,n_{l-2},n_{l-3},\dots,n_0)$

出力: $P_{n,Z}$

1. $Y=P$
2. for $i=l-2$ down to 0
3. $\quad Y=(Z+Y)\oplus Y$
4. $\quad$ if $n_i=1$ then $Y=Y\oplus P$
5. end for
6. return Y

従来の楕円曲線離散対数問題(ECDLP)の定義を模倣して、Me 演算の離散対数問題(MeDLP)を「$P,Q\in E(\mathbb{F}_p),z\in\mathbb{Z}$から$Q=P_{n,zP}$を満たす$n\in\mathbb{N}$を見つける問題」と定義できる。現時点で、Me 演算/スカラー倍、MeDLP に関して次の性質を持つことが判明した。

(a) $P\oplus P=P$	べき等律
(b) $P\oplus Q=Q\oplus P$	可換律
(c) $(P\oplus Q)+R=(P+R)\oplus(Q+R)$	分配律
(d) $P+(Q\oplus R)=(P+Q)\oplus(P+R)$	分配律
(e) $(P_{n,Z})_{m,Z}=(P_{m,Z})_{n,Z}=P_{n,Z}+P_{m,Z}-P$	Me 版 Diffie-Hellman 問題の非困難性
(f) MeDLP は ECDLP と同等に困難かより困難	
(g) 列$\{P_{n,Z}:n=1,2,3,\dots\}$は非周期的	(実験による)

性質(c)と(d)が双線形性と類似しており、ペアリング演算を Me 演算に置き換えた暗号プロトコルをいくつか考察したが、性質(e)により暗号の安全性が失われ、Me 演算を用いたディジタル署名を除いて攻撃法が発見された。しかしながら性質(f)は十分に安全な Me 演算を用いる暗号プロトコルが構成できる可能性があることを意味している。

(3) 楕円曲線探索
公開鍵暗号における暗号化・復号、ディジタル署名における署名生成・検証の処理を高速に行える楕円曲線の探索を行った。$p=2^{256}-58097$に対して、$\mathbb{F}_p$上楕円曲線$638y^2=x^3+10x^2+x$、$p=2^{256}-58097$がその一例である。

(4) 素因数分解のための楕円曲線法(ECM)の研究
CM 法による楕円曲線法による構成の研究の過程で、ECM により簡単に素因数できる素数が存在することが判明した。最初に、$p=(3V^2+1)/4$という形の素数を含む合成数は、j不変数が 0 の

楕円曲線を用いてECMを実行することで、簡単に素因数分解できることを示した。次に、この結果を改良し、$D = 11, 19, 35, 43, 51, 67, 91, 115, 123, 163, 187, 235, 267, 403, 427$に対する類多項式の根を$j$不変数とする楕円曲線を用いてECMを実行することで$p = (DV^2 + 1)/4$という素数を含む合成数が簡単に素因数分解できることを示した。最終的には、Dの範囲を更に拡げ、類多項式が計算できるようなDに対して、例えば50,000以下のDに対して、$p = (DV^2 + 1)/4$という形の素数を含む合成数が簡単に素因数分解できることを示した。RSA暗号の公開鍵の合成数Nが偶然このような素因数を持つ確率は無視できるほど小さいが、RSA暗号では公開鍵を簡単に素因数分解できると安全性が損なわれるため、気を付けたい結果である。

＜引用文献＞
①International Digital Publishing Forum、EPUB Lightweight Content Protection: Use Cases & Requirements、 http://idpf.org/epub-content-protection、2012 （最終アクセス2019/06/17）

５．主な発表論文等
〔雑誌論文〕（計２件）
① AIKAWA Yusuke、NUIDA Koji、SHIRASE Masaaki、Elliptic Curve Method Using Complex Multiplication Method、IEICE Transactions on Fundamentals of Electronics、Communications and Computer Sciences、査読有、E102.A、2019、74―80
② SHIRASE Masaaki、Search of Elliptic Curves Suitable for Signature、International Journal of informatics Society (IJIS)、査読有、2019、採録決定

〔学会発表〕（計１１件）
① 白勢政明、有限体上楕円曲線の新しい演算に基づくDLPとECDLPの関係、コンピュータセキュリティシンポジウム2018、2018
② SHIRASE Masaaki、Elliptic Curves Suitable for Elliptic Curve Signature、IWIN 2018、査読有、2018
③ SHIRASE Masaaki、New Operation and Problems on Elliptic curve and Their Application、IEEE 2018 ICCE-TE、査読有、2018
④ 白勢政明、有限体上楕円曲線の新しい演算に基づく離散対数問題の困難性とディジタル署名、情報セキュリティ研究会、2018
⑤ 白勢政明、新しい楕円曲線演算によるキーワード検索暗号、2018年暗号と情報セキュリティシンポジウム、2018
⑥ 白勢政明、有限体上M関数の有限体上楕円曲線への拡張とその応用、コンピュータセキュリティシンポジウム2017、2017
⑦ 白勢政明、有限体上M関数を用いたM-スカラー倍算の提案とその性質及び応用、日本応用数理学会2017年度年会、2017
⑧ YOSHIDA Tsutomu、SHIRASE Masaaki、A Digital Content Sharing Model Using Proxy Re-Encryption Without Server Access、IEEE 2017 ICCE-TW、査読有、2017
⑨ 白勢政明、特別な形の素因数を持つ合成数の楕円曲線法による素因数分解II、2017年暗号と情報セキュリティシンポジウム、2017
⑩ 白勢政明、特別な形の素因数を持つ合成数の楕円曲線法による素因数分解、情報セキュリティ研究会、2017
⑪ 白勢政明、$p = (3V^2 + 1)/4$を持つ合成数の楕円曲線法による素因数分解、日本応用数理学会2016年度年会、2016

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計０件）

名称：
発明者：

権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：

ローマ字氏名：

所属研究機関名：

部局名：

職名：
研究者番号（8桁）：

(2)研究協力者
研究協力者氏名：
ローマ字氏名：

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。