様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年４月１１日現在

機関番号：１７１０２
研究種目：基盤研究（B）
研究期間：2010～2012
課題番号：22300026
研究課題名（和文）ペアリング暗号方式の基礎数理および実装方法の研究

研究課題名（英文）Mathematical Foundation and Implantation Methods for Pairing-Based Cryptography

研究代表者
高木　剛（TAKAGI TSUYOSHI）
九州大学・マス・フォア・インダストリ研究所・教授
研究者番号：60404802

研究成果の概要（和文）：ペアリング暗号は、従来の公開鍵暗号では実現が困難であった新たな暗号プロトコルが構成できる。本研究課題では、高速実装が可能なペアリング関数として知られているη_Tペアリングと R-Ate ペアリングを様々な計算環境において高速実装を行い、ペアリング暗号は RSA 暗号や楕円曲線暗号と同程度の演算処理性能を得ることを示した。また、ID ベース暗号の高機能化の研究を進め、標準モデルで安全性証明可能な ID ベース型の署名付き暗号化方式などを提案した。

研究成果の概要（英文）：Pairing-based cryptography (PBC) provides us new cryptographic protocols which cannot be constructed by the conventional public-key cryptosystems. In this research, we implemented η_T pairing and R-ate pairing on real-life computing environments such as mobilephones and GPGPU, and eventually we showed that PBC has become as efficient as RSA or elliptic curve cryptography on those devices. Moreover, we investigated the further development of ID-based encryption, and then we proposed an ID-based signcryption which is provably secure in the standard model.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	3,600,000	1,080,000	4,680,000
２０１１年度	3,700,000	1,110,000	4,810,000
２０１２年度	3,200,000	960,000	4,160,000
２０１３年度	0	0	0
２０１４年度	0	0	0
総　計	10,500,000	3,150,000	13,650,000

研究分野：計算機システム・ネットワーク
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：暗号・認証、公開鍵暗号、ペアリング暗号、高速実装、暗号プロトコル

１．研究開始当初の背景

(1)次世代暗号であるペアリング暗号は、従来の公開鍵暗号（RSA 暗号や楕円曲線暗号）では実現困難であったセキュリティ技術を、効率的に提供でき、更に将来のユビキタス社会に適した暗号プロトコル（暗号文キーワード検索方式、放送型暗号等）も構成できる。

(2)ペアリング暗号とその応用研究では、数学的基礎、暗号実装、暗号プロトコルなどの研究課題が独立に行われてきた。その結果、双線形ペアリング関数をブラックボックスとして実計算環境での実装を考慮しない暗号プロトコルなど、実用化が困難と思われる方式が多く提案されてきた。

２．研究の目的

本研究課題では、ペアリング暗号の基礎理論から実装技術までを含めた以下の 3 点に関して研究を進める。

① 暗号プロトコル: 安全性証明技術による安全性の考察や新たなペアリング暗号プロトコルの提案

② 暗号実装: 効率的な実装アルゴリズムの考察や異なるプラットフォームにおけるペアリング暗号の高速実装

③ 数学的基礎: 新しいペアリング関数の構成や、理論的及び計算機実験による安全性の検証

３．研究の方法

(1)本研究課題のテーマを、暗号プロトコル、暗号実装研究、数学的基礎研究という 3 つの階層に分け推進する。数学基礎研究において効率的な双線形ペアリング写像の構成法を研究し、暗号実装研究で得られる異なる計算プラットフォームでの実装データを踏まえた上で、暗号プロトコルの研究では新たなペアリング暗号方式を提案する。

(2)双線形ペアリング写像には、標数 3 の有限体上で構成される η_Tペアリング、256 ビットの素数 p に対して有限体 GF(p^{12})で構成される R-Ate ペアリングなどがある。利用する双線形ペアリング関数の違いにより、暗号プロトコルの安全性や実計算環境での実装性能などがどのように異なってくるかを考察する。

４．研究成果

(1) ペアリングを利用した暗号プロトコルの研究を進め、Lu-Dong-Cao によって提案されたモバイル通信に向いた効率的な代理署名方式に対する脆弱性を指摘した。複数のバイオメトリ情報から秘密鍵を抽出することが可能な暗号化認証方式をペアリング関数により構成した。

(2) 幾何領域ベースの鍵生成方法と関数型暗号に関する研究を進めた。秘密鍵を平面領域の点として表現し、暗号化ポリシを直線や凸体に対応させる暗号化方式を提案した。また、階層型 ID ベース暗号を拡張した方式として部分順序委任暗号を考察し、暗号文のサイズが定数となる匿名暗号を構成した。

(3) 標準モデルにおいて ID ベース署名付き暗号化方式 (ID-based signcryption) を提案した。この提案方式は、変形双線形 DH 判定仮定の下で、適応型暗号文攻撃に対して識別不可能性(IND-CCA)かつ適応型平文攻撃に対して存在的署名偽造不可能性(EUF-CMA)を有することを証明できる。また、安全性証明可能な暗号方式に関して議論する国際会議 ProvSec 2012 の予稿集を出版した。

(4)128 ビット AES のセキュリティレベルにおける R-ate ペアリングを BREW 携帯電話においてソフトウェア実装を行った。高速化にあたり最終冪に Addition Chain を適用した結果 GF(p)の乗算回数を約 8%削減し、BREW 携帯電話 (ARM9 225MHz) における R-ate ペアリングの演算時間は 1.60 秒となった。また同じセキュリティレベルにおける BREW 携帯電話上で RSA と ECC との時間比較を行った結果、R-ate ペアリングは RSA と ECC 同等の演算時間であった。

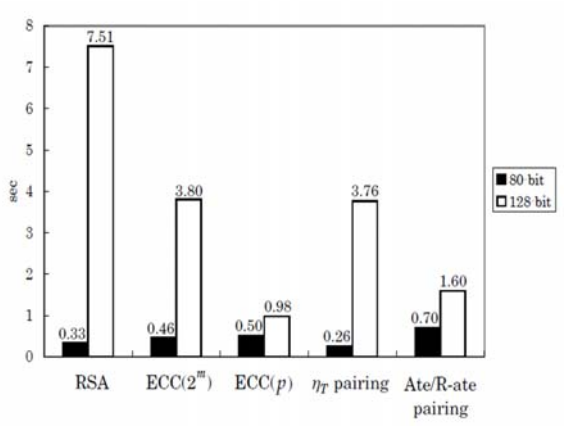

図１．ペアリング暗号の計算時間比較

(5)近年盛んに研究されている GPGPU を用いて、標数 3 の η_T ペアリングを高速実装し暗号化演算の性能を評価した。特に、NVIDIA 社の GPU である GTX285, GTX480, Tesla C1060, Tesla C2050 を用いて、複数の η_T ペアリン

グを並列計算する実装を行った。その結果、有限体 GF(3^{97})上の η_T ペアリングは、GTX 285 上で 1.47msec で計算可能であり、GTX 480 上において 1 秒間で 33710 回の η_T ペアリング演算が実行可能である結果を得た。本実装は GPU 上に η_T ペアリングの実装を行った最初の実装結果である。

	Curve	Architecture	#cores	Freq. (GHz)	Time (ms)
Beuchat *et al.* [13]	$E(F_{397})$	Intel Core 2	2	2.6	0.090
This work	$E(F_{397})$	NVIDIA GTX 480	480	1.4	0.029
Beuchat *et al.* [13]	$E(F_{3193})$	Intel Core 2	2	2.6	0.550
This work	$E(F_{3193})$	NVIDIA GTX 480	480	1.4	0.201
Aranha *et al.* [1]	$E(F_{21223})$	Intel Xeon 45nm	8	2.0	1.51
Beuchat *et al.* [13]	$E(F_{3509})$	Intel Core 2	4	2.4	2.94
Beuchat *et al.* [13]	$E(F_{3509})$	Intel Core i7	8	2.9	1.87
This work	$E(F_{3509})$	NVIDIA GTX 480	480	1.4	3.01

図 3. ペアリング暗号の実装比較

(6) ペアリング暗号の高速な実装を目的として、128 ビットセキュリティレベルの R-ate ペアリングおよび η_T ペアリングを Android 携帯電話において実装評価を行った。Java ベースの Android 携帯電話の実装では、BigInteger の加減算におけるネイティブ関数の呼び出し回数の削減などにより、ペアリングの演算時間を約 13%高速できる方式を提案した。また、ペアリング演算とべき乗演算との比較データや、すでに実用化されている公開鍵暗号である RSA 暗号との実装スピードの比較も行った。

Degree	97	193	353	509
Multiplication	0.806	1.765	3.244	4.624
Cubing	0.056	0.107	0.167	0.211
Square Root	11.75	36.71	95.63	178.30
Matrix	1.90	4.56	9.15	16.03
1/3-trace	6.40	22.88	64.39	115.52

AMD Opteron 2.2 GHz (μsec)

図 2. MapToPoint の速度比較

(7) MapToPoint は楕円曲線上の点の片方の座標から点を生成するアルゴリズムである。η_T ペアリングでは GF(3^n)上の超特異楕円曲線 $y^2=x^3-x+b$, b=1,-1 の一方の座標が入力され点を生成する。本研究では、1/3-trace を提案し、y 座標から x 座標を構成するアルゴリズムを構成した。1/3-trace は $x^3-x=c$ の解 x を乗算なしで計算可能なため、必要な乗算の回数を従来法(Square Root)より削減している。更に、有限体 GF(3^n)の線形変換の行列をメモリに格納する従来法(Matrix)と異なり、提案方式では予備計算の必要がない。

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 10 件）

① Fagen Li, Mingwu Zhang, Tsuyoshi Takagi, Efficient Signcryption in the Standard Model, Concurrency and Computation: Practice and Experience, 査読有, Vol.24, No.17, 2012, pp. 1977-1989.
DOI: 10.1002/cpe.1823

② 井山政志, 清本晋作, 福島和英, 田中俊昭, 高木剛, 携帯電話におけるペアリング暗号の実装, 電子情報通信学会和文論文誌, 査読有, Vol.J95-A, No.7, 2012, pp.579-587,
http://ci.nii.ac.jp/naid/10031083671

③ Fagen Li, Yongjian Liao, Zhiguang Qin, Tsuyoshi Takagi, Further Improvement of an Identity-Based Signcryption Scheme in the Standard Model, Computers & Electrical Engineering, 査読有, Vol.38, No.2, 2012, pp.413-421.
DOI: 10.1016/j.compeleceng.2011.11.001

④ Mingwu Zhang, Tsuyoshi Takagi, GeoEnc: Geometric Area based Keys and Policies in Functional Encryption Systems, 16th Australasian Conference on Information Security and Privacy, ACISP 2011, 査読有, LNCS 6812, 2011, pp.241-258.
DOI: 10.1007/978-3-642-22497-3_16

⑤ Yosuke Katoh, Yun-Ju Huang, Chen-Mou Cheng, Tsuyoshi Takagi, Efficient Implementation of the η_T Pairing on GPU, 9th International Conference on Applied Cryptography and Network Security, ACNS 2011, 査読有, Industrial Track, 2011, pp.119-133.
http://eprint.iacr.org/2011/540.pdf

⑥ Mingwu Zhang, Takashi Nishide, Bo Yang, Tsuyoshi Takagi, Anonymous Encryption with Partial-Order Subset Delegation Functionality, Fifth International

Conference on Provable Security, ProvSec 2011, 査読有, LNCS 6980, 2011, pp.154-169.
DOI: 10.1007/978-3-642-24316-5_12

⑦ Fagen Li, Fahad Bin Muhaya, Mingwu Zhang, Tsuyoshi Takagi, Efficient Identity-Based Signcryption in the Standard Model, Fifth International Conference on Provable Security, ProvSec 2011, 査読有, LNCS 6980, 2011, pp.120-137.
DOI: 10.1007/978-3-642-24316-5_10

⑧ Yuto Kawahara, Tetsutaro Kobayashi, Gen Takahashi, Tsuyoshi Takagi, Faster MapToPoint on Supersingular Elliptic Curves in Characteristic 3, 査読有, IEICE Transaction, Vol.E94-A, No.1, 2011, pp.150-155.
DOI: 10.1587/transfun.E94.A.150

⑨ Tadashi Iyama, Shinsaku Kiyomoto, Kazuhide Fukushima, Toshiaki Tanaka, Tsuyoshi Takagi, Efficient Implementation of Pairing-based Cryptography on BREW Mobile Phones, The 5th International Workshop on Security, IWSEC 2010, 査読有, LNCS 6434, 2010, pp.326-336.
DOI: 10.1007/978-3-642-16825-3_22

⑩ Fagen Li, Masaaki Shirase, Tsuyoshi Takagi, Cryptanalysis of Efficient Proxy Signature Schemes for Mobile Communication, Science China Information Sciences, Vol.53, No.10, 査読有, 2010, pp.2016-2021.
DOI: 10.1007/s11432-010-4012-y

〔学会発表〕(計2件)

① 高木剛, センサノードMICAzにおけるペアリング暗号の高速実装, 2012年暗号と情報セキュリティシンポジウム, チュートリアル講演, 2012年2月1日, 金沢エクセルホテル.

② Tsuyoshi Takagi, Fault Attacks on Multivariate Public-Key Cryptosystems, International Conference on Coding and Cryptography, 招待講演, 2011年8月26日, Ewha Womans University, ソウル, 韓国.

〔図書〕(計1件)

① Tsuyoshi Takagi, Guilin Wang, Zhiguang Qin, Shaoquan Jiang, Yong Yu, Springer Verlag, 6th International Conference on Provable Security - ProvSec 2012, 2012, 335.

〔その他〕

ホームページ
http://imi.kyushu-u.ac.jp/~takagi/

５．研究組織

(1) 研究代表者

高木　剛 (TAKAGI TSUYOSHI)
九州大学・ﾏｽ・ﾌｫｱ・ｲﾝﾀﾞｽﾄﾘ研究所・教授
研究者番号：60404802