様式 C-19

科学研究費補助金研究成果報告書

平成２３年　４月３０日現在

機関番号：１５３０１
研究種目：若手研究（B）
研究期間：2008～2010
課題番号：20760241
研究課題名（和文）高速なＡｔｅペアリング計算アルゴリズムの拡張とその世界最高速実装

研究課題名（英文）Extension of Efficient Ate Pairing and its Fastest Implementation

研究代表者
野上　保之（NOGAMI　YASUYUKI）
岡山大学・大学院自然科学研究科・准教授
研究者番号：60314655

研究成果の概要（和文）：
近年、情報セキュリティ技術に対する要求はより複雑かつ高度になってきており、とりわけプライバシを保護した認証技術が注目を浴びている。これをより現実的にするペアリング暗号の高速化手法として Xate ペアリングを提案しており、本研究では、これを適用できる楕円曲線を増やすことを主目的とし、それを用いて具体的に高速なペアリングを実装する。

研究成果の概要（英文）：
In the modern information oriented society, the demand of security technologies has become much more complicated and advanced. Especially, anonymous authentication with pairing operation has received much attention. In order to make its performance practical, an efficient pairing so called Xate pairing has been proposed. The main purpose of this research is to increase the number of Xate pairing curves and then develops an efficient implementation of those Xate pairings.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,400,000	420,000	1,820,000
2009 年度	1,000,000	300,000	1,300,000
2010 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：総合科目
科研費の分科・細目：情報学・情報学基礎
キーワード：応用数学、情報通信工学、セキュア・ネットワーク、代数学

１．研究開始当初の背景

現代情報化社会におけるセキュリティ技術、とりわけ情報の秘匿性を確保するための暗号化技術や、インターネットなどを介してユーザや機器を認証するための電子認証技術に対しての要求は、極めて高度かつ複雑なものとなっている。これは、一方で情報漏洩などの事件が後を絶たたず起こっているためである。このようなことを鑑み、総務省を中心に策定されているユビキタスネットワークセキュリティ（UNS）戦略 I・II においても、個人情報を保護しながら、高度に情報を暗号化し、またユーザ認証できる技術の開発を、2010 年代に完成させ、現実的な技術として提供できるようにすべきであるということが提唱されている。これに対し、2000 年に入り、日本を起源として、高度にそのような要求に応えるペアリングと呼ぶ技術が開発された。日本発の技術としてこれを世界に広めるため、とりわけ日本を中心に、その技術の改良・実装が進められている。

さてペアリングとは、まず拡大体と呼ぶ代数系の上で定義されるある特殊な形の楕円曲線暗号を考え、その上で定義される 2 入力 1 出力の双線形性を有する写像関数である。ペアリングを用いた高度な暗号技術を実現するためには、それが複雑な数学理論のもとで計算される写像であるため、その計算処理の遅さ・重さが足かせとなってきていた。それが故に、高度な暗号技術が実現できると分かっていながらも、その製品化・社会への技術としての還元が、総務省が提示する UNS 戦略ロードマップと対比しても遅れている。しかし一方で、ペアリング写像が理論的にどの程度まで高速化できるかという目安は既知の事実として示されており、数多くのペアリング暗号研究者は、その理論的な限界を達成するペアリング写像関数の発見・効率的な実装手法の開発を続けてきた。

そのような中、2005 年頃に入って、その理論的な限界に近づく成果が幾つか提案されている。例えば、Ate pairing, Twisted Ate pairing, ηT pairing, R-ate pairing, ptimal pairing, Xate pairing などである。その中で、ηT pairing, Twisted Ate pairing、Xate pairing は日本の研究者からの提案であり、これらはある特殊な楕円曲線上で定義でき、それをもって極めて高速かつ効率のよい計算処理によってペアリング計算を実現できることを示した。すなわち、近年の高度かつ複雑な情報セキュリティ技術、とりわけプライバシを保護した認証技術を実現するペアリング暗号においては、そのような効率のよいペアリング計算を、例えば PC 上などで実装することが必要となる。言い換えれば、そのようなペアリングを用いなければ、現実的に快適な処理を行うための計算速度を達成できず、さらに言えば、ユビキタス環境において重要な役割を果たす携帯端末など計算資源の限られた端末においては、言うまでもなく快適な処理時間を達成することは困難となる。したがって、そのような種々の計算端末、あるいは様々な情報源の重要度に対応する形で、幾通りもの組み合わせの状況が考えられ、そのような幾通りもの状況下においても、快適な暗号化処理を実現することが実用化に向けての要件となる。さらには、ペアリング計算の土台になる拡大体と呼ぶ代数系に対しても、そのような状況に対応するスケーラビリティと効率のよい基本演算（乗算、除算など）など、同様な効率化が要求され、これを実現する実装が求められる。

２．研究の目的

先に述べたような要求に対し、計算端末や情報の重要度など、色々な状況に高度なスケーラビリティをもって対応できるよう、本研究ではとくに Xate pairing に焦点を当て、これを適用できる楕円曲線の種類を増やすことを目的とする。具体的には、Xate pairing の提案時は、BN（Barreto-Naehrig）曲線と呼ぶ特殊なクラスの楕円曲線に対してのみ、その効率的な計算手法が示されていたため、本研究ではより広いクラスの楕円曲線に対してもこれを適用できるようにすることが主たる目的である。

それに合わせて、これを効率よく計算端末上に実装するために、ペアリング計算の効率化のみならず、その土台をなす拡大体と呼ぶ代数系に対しても、十分な効率性と高度なスケーラビリティを併せもって実現することを目的とする。具体的には、BN 曲線の場合には 12 次の拡大体が用いられるが、その他のペアリング曲線に対しては、他の次数の拡大体を準備する。それらをもって、現代情報化社会における高度かつ複雑化したセキュリティ要求に応えられるペアリング暗号技術の実現を目標とする。とりわけユビキタス端末として、スマートフォンなどの計算資源の限られた計算端末上でも、十分快適に動作することを検証することも重要である。

３．研究の方法

(1)ペアリング計算について

まずペアリング計算に関しては、Xate pairingを適用できる曲線のクラスを増やすことに実現する。そのためには、BN曲線がコンプリートファミリと呼ぶ曲線のクラスに属することをスタートとして、まず他のコンプリートファミリの楕円曲線へと拡張する。その結果を踏まえながら、それ以外のファミリへと拡張を試みる。その際には、理論的な計算量の限界を達成できているかが一つのチェックポイントとなる。

(2)拡大体計算について

拡大体については、より重要な実装項目となる。これは、上述のペアリング用の楕円曲線のクラスが、それぞれに拡大次数と呼ぶパラメータを異なった値でもつためであり、例えばBN曲線であれば、12次という次元数の拡大体を準備する必要がある。また、その上で計算効率を上げるためには、その部分体となる4次や6次といった次元数の代数系も効率よく実装しておく必要があり、そのような逐次的な効率化を積み重ねて行う必要がある。そして、それらを様々な次元数で、具体的には2次から20次の間での次元数で準備する必要があり、これを個別に準備するのではなく、やはり高度なスケーラビリティをもって、一つの計算プログラム・計算チップでこれらに対応できるような実装が求められる。これは、拡大体における演算は、四則演算に代表される基本的な演算を担うためであり、上位のペアリング計算からのパラメータ要求に柔軟に対応できる方が簡便となるからである。

(3)計算端末への実装について

近年のパーソナルコンピュータ（PC）は、安価で十分な計算能力をもっているものが多いため、実装のための実験や検証はPCを中心にして開発を進めるものの、一方でユビキタス社会において主として活躍するのは、スマードフォンなど、計算資源の限られた端末であり、そのような計算機上で快適に計算処理を行えるように実装することが重要であり、今回の研究開発においても幾つかのそのような計算端末を用いて、実際にユビキタス社会においても快適に動作するか否かを検証する。加えて、さらに上位の層となる認証プロトコ

ルに対しても実際にこれらを適用し、その性能を検証・評価する。

４．研究成果

(1)ペアリング計算について

本研究開発では、Xate pairingがBN曲線をから発案されたことをスタートとして、それをさらに多くのクラスのペアリング曲線に対しても、理論的な効率性の限界を達成しながら拡張できることを示した。具体的には、BW曲線、MNT曲線、一般のツイスト曲線などに対してであり、中でもFreeman曲線と呼ばれるクラスに対しては、BN曲線の場合と比べても十分な性能を有してペアリング写像を実現できることを示した。結果的には、適切なパラメータ設定と組み合わせながら、Xate pairingを大きく包含するAte pairingが適用できる楕円曲線のほぼすべてに対して拡張できることを確認した。これについては、業績[2]に示した国際会議において発表をしている。その他の曲線に対しての結果についても、下記に示すホームページにて紹介している。

(2)拡大体計算について

これまでの研究開発においてとくに感じていたことは、上位層のペアリング計算が効率的なアルゴリズムによって実現できることを示せたとしても、その土台をなす拡大体における種々の演算を、それに対応して十分な最適化を行った上で準備することが極めて重要となることである。しかしながら、先にも述べたように、これをそれぞれにカスタマイズして準備することは、今後のチップ化などへの展開を考えると不便であるため、そのような問題点を乗り越えるために本開発では、CVMAと呼ぶ拡大体における乗算アルゴリズムを、高度なスケーラビリティをもって拡張利用することを考えた。そして実際に実装して、効率性を確認した。主たる研究成果は業績の[1]、[4]にて発表している。例えばFreeman曲線の場合には、10次の次元数をもつ拡大体における四則演算を実装し、合わせてその部分体となる5次の次元数をもつ場合の演算についても実装を行った。その結果として、BN曲線の場合に劣らない計算処理速度を達成している。他の次元数に対しての実装結果は、同ホームページにて紹介をしている。

(3)計算端末への実装について

まず、拡大体における四則演算、ペアリング写像計算、プロトコルにおける各機能の計算処理時間について、PCを用いて実装、実験検証を行った。その際には、大きな桁数の整数演算が必要となるため、多倍長計算ライブラリであるGnuMPライブラリを用いて、C言語をベースに実装を行った。その結果として、PC上においては、拡大体における乗算1回を数マイクロ秒、ペアリング計算を数ミリ秒、そして例えば電子認証における署名の生成や検証などを、数十ミリ秒で行えることを確認した。これについては、その一部のデータに付いては、業績[3]において発表をしている。そして、これをスマートフォンなどの携帯端末において実装した場合の処理時間については、具体的にiPhone、iPadを用いて検証を行った。その結果、拡大体計算を数十マイクロ秒、ペアリング計算を数十ミリ秒、認証データの生成および検証を数百ミリ秒（具体的には百ミリ秒強）にて行えることを確認できた。これをもって十分に、現実的な処理を達成できていると結論づけるとともに、現代情報化社会において、とりわけユビキタス端末を用いたとしても、快適な処理時間をもって高度な暗号化および認証技術を実現できると言える。この最終的な成果については、国際学会などの場で発表する準備をしている。

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）
なし

〔学会発表〕（計 4 件）
[1] 湯浅 達也, 根角 健太, 野上 保之, 森川 良孝、“Type＜k,4＞GNB を用いた 2 次逐次拡大体 F_{{p^2}^2}の構成とその効率的な乗算の実装”、第 33 回情報理論とその応用シンポジウム（SITA2010）、査読無、2010/12/2.

[2] 根角 健太, 野上 保之, 森川 良孝、“Ultimately Customized Multiplication Algorithm in the Extension Field for Xate and R-ate Pairing with Freeman Curve”、IEEE TENCON2010, CD-ROM T4-3.3、査読有、2010/11/23.

[3] 竹内 翔一, 酒見 由美, 加藤 英洋, 野上 保之, 森川 良孝、“Thread Computing for Miller's Algorithm of Pairing Especially with Composite Order Pairing-Friendly Curves”、2010 年 暗号と情報セキュリティシンポジウム (SCIS 2010)、査読無、2010/1/20.

[4] 根角 健太, 湯浅 達也, 野上 保之, 森川良孝、“Freeman 曲線を用いた Xate および R–ate ペアリングのための定義体における乗算アルゴリズム”、コンピュータセキュリティシンポジウム 2009、査読無、2009/10/26.

〔図書〕（計 0 件）
なし

〔産業財産権〕
○出願状況（計 0 件）
なし

○取得状況（計 0 件）
なし

〔その他〕
ホームページ（研究成果の紹介）
http://www.trans.cne.okayama-u.ac.jp/~nogami

６．研究組織
(1)研究代表者
野上　保之（NOGAMI　YASUYUKI）
岡山大学・大学院自然科学研究科・准教授
研究者番号：60314655

(2)研究分担者
なし

(3)連携研究者
なし