様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 6 月 1 日現在

研究種目：基盤研究（B）
研究期間：２００６～２００９
課題番号：１８３４０００５
研究課題名（和文）　ペアリングに基づく楕円暗号の安全性の数論的研究

研究課題名（英文）　On security of pairing based elliptic curve cryptosystems in view of number theory

研究代表者：
佐藤　孝和 (SATOH　TAKAKAZU)
東京工業大学・大学院理工学研究科・准教授
研究者番号：７０２１５７９７

研究成果の概要（和文）：
ペアリングに基づく楕円暗号に特有の解読法としてペアリング反転を解く方法が知られている。本研究ではヴェイユペアリングの反転写像の明示公式を与えた。この式は密な有理式であり、このペアリング反転公式をそのまま計算してしまう方法に対してはペアリングに基づく楕円暗号は安全であることが示された。また、ペアリングに基づく暗号に適する超楕円暗号をペアリングに基づく暗号に適さないある種の楕円暗号から構成する方法を開発した。

研究成果の概要（英文）：
A pairing inversion formula is considered to be a possible pairing based elliptic curve cryptography specific cryptanalysis. In this research, we gave explicit formulae for the Weil pairing inversion. The result is a dense rational formula and therefore pairing based cryptosystems are not vulnerable to evaluation of the explicit formula. We also constructed pairing friendly hyperelliptic curves from certain pairing non-friendly elliptic curves.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2006年度	2,100,000	630,000	2,730,000
2007年度	1,500,000	450,000	1,950,000
2008年度	1,500,000	450,000	1,950,000
2009年度	1,500,000	450,000	1,950,000
年度			
総　計	6,600,000	1,980,000	8,580,000

研究分野：数論
科研費の分科・細目：数学・代数学
キーワード：ペアリング、楕円曲線暗号、離散対数問題

1. 研究開始当初の背景

本研究が主な対象としたのは楕円曲線上のペアリングに基づく楕円暗号通信手順の安全性である。ペアリングは実用的な三者間鍵共有、短い電子署名、識別情報に基づく暗号等に不可欠である。その際、ペアリングフレンドリーという特殊な楕円曲線が用いられる。一般の楕円曲線を用いる楕円暗号は安全であろうという仮定は楕円曲線暗号研究者の間では広く受け入れられている。しかしペアリングフレンドリー曲線は特殊な性質を持つのでそれを利用した解読法があるかもしれない。

研究代表者が本研究の応募に際し、楕円曲線暗号界を代表する欧米の研究者たちにペアリングに基づく楕円曲線暗号の安全性を照会したところ**ペアリングに基づく楕円曲線暗号の安全性の根拠である離散対数問題は、研究代表者の知り得た限りにおいて、誰も、何も、示していない**ということが判明した。このような状況でペアリングに基づく暗号の実装研究や規格化が先行するのは極めて憂慮された。

2. 研究の目的

本研究ではペアリングに基づく暗号の安全性に何らかの理論的な帰結を出すことを目的とする。具体的にはペアリングフレンドリーであることが一番影響を受けると思われるペアリング反転に関して、何らかのアルゴリズムを与え、その計算量を評価することを主目的とした。

3. 研究の方法

(1) ペアリング反転ができればその値域を共有するすべてのペアリングを用いた暗号は多項式時間で解読されることは従前より知られていた。ペアリング反転アルゴリズムの構成には種々の方法が考えられるが、本研究ではWeil ペアリング反転の明示式による表示がどうなるかを検証することとした。楕円曲線の数論的性質および形式群の性質を利用した。

(2) 理論的に得られた明示式を検証するため、有限体のサイズを落としたところで数値計算を行った。

(3) 上記の所見を踏まえてペアリング暗号に適する楕円暗号の構成をゼータ関数論用いて試みた。

4. 研究成果

(1) Weil ペアリングに対してペアリング反転公式を構成した。その種の結果に関しては従来は次数のみの評価しか得られていなかったが、本研究の結果として、そのような多項式の係数を明示的に与え特に重みについては最良の結果を得た。楕円曲線が関連する多項式補間で簡明な明示公式はないだろうというおおかたの予想を覆す研究成果である。この導出には Lagrange 分解式を用いて Kummer 理論をペアリング反転に適用するという手法が用いられ、従来の組み合わせ論的手法では到底得られなかった成果をあげることができた。

標数 2 及び 3 の超特異曲線に対しては公式は若干簡単な形となる。具体的には q が 2 のベキで $E/\mathbf{F}_q$ を

$$Y^2+a_3Y = X^3+a_4X+a_6$$

により定義された $\mathbf{F}_q$ 上の楕円曲線とする（標数 2 の超楕円曲線はかならずこの形に表わされる）。$A\in E[l]$ に対し $G:=\langle A\rangle$ とおき $\varphi_G: E\to E/G$ を標準的準同型とする。1 の l 乗根のなす群 μ_l の要素 ω に対し

$$V_A(\omega) := \begin{cases} \mathcal{O} & (\omega = 1) \\ (x_\omega, y_\omega) & (\omega \neq 1) \end{cases}$$

ここで

$$x_\omega := u_2 + \frac{a_3^2}{\Omega_2}\sum_{n=2}^{(l-1)/2}\frac{\Omega_{2n}}{(u_1-u_n)^2},$$

$$y_\omega := \frac{(u_2^2+a_4)}{a_3}(u_4+u_2)+v_2+\frac{\omega^4 a_3}{\Omega_4} + \frac{a_3(u_2^2+a_4)}{\Omega_4}\sum_{n=2}^{(l-1)/2}\frac{\Omega_{4n}}{(u_2-u_{2n})^2} + \frac{a_3^3}{\Omega_4}\sum_{n=2}^{(l-1)/2}\frac{\Omega_{4n}}{(u_2-u_{2n})^3}$$

ただし

$$\Omega_n := \omega^n+\omega^{-n}, u_n := (nA)_X, v_n := (nA)_Y$$

とおく。このとき以下が成立する：

① V_A は μ_l から $(E/G)[l]$ への単射準同型

② e_l を l 分点に対する Weil ペアリングとする。$B\in(E/G)[l]-\mathrm{Ker}\,\widehat{\varphi_G}$ に対し $e_l(B, V_{\widehat{\varphi_G}(B)}(\omega))=\omega.$

非超特異曲線に対しては式の形は上記よりも複雑となるが本質的な構造は類似している明示式が得られた。直接の結論として、ペアリングに基づく楕円暗号は上のペアリング反転公式をそのまま計算する解読法に対して安全であることが分かった。現時点ではこの結果は超特異曲線を用いたペアリングに基づく楕円暗号が非超特異曲線を用いたペアリングに基づく楕円暗号に比べて実用上の安全性が劣るという事を意味しないが、今後超特異曲線の安全性に関して一層の研究が必要であることが明らかにされた。

(2) 得られた反転公式を検証検証する際、算術演算ライブラリーのメモリー管理を改良した。この過程で、副産物として Shanks 予想に関する結果を得た。Shanks 予想とは「整数環上の Euclid 素数列は全ての素数を表わすであろう」というものでこの報告書作成時点でも未解決問題として残っている。Shanks 予想は有限体上の一変数多項式環でも定式化されるが、その場合には予想を否定的に解決した。他方、もとの整数環上の場合の Shanks 予想の正しさを示唆する計算例を得た。

(3) 頂切離散附値環の拡大についての Deligne の定理を、剰余体が必ずしも完全でない場合に一般化した。これは例へば一般の完備離散附値環上のアーベル多様体の等分点から生ずる分岐の研究などに応用が期待される。

(4) ペアリングフレンドリーではない楕円曲線から種数 2 のペアリングフレンドリーである超楕円曲線を構成した。ここではこれらのゼータ関数が同種写像により関連づけられることが重要である。しかも、この超楕円曲線を用いた暗号は多項式時間帰着の差を除いて楕円曲線暗号と同等以上の安全性をもつことが証明された。

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 12 件）

① T. Hiranouchi, Y. Taguchi, Flat modules and Gröbner bases over truncated discrete valuation rings, Interdisciplinary Information Sciences 16, 33–37 (2010), 査読有

② T. Satoh, Generating Genus Two Hyperelliptic Curves over Large Characteristic Finite Fields, Advances in Cryptology – Eurocrypt 2009, Lect. Notes in Comput. Sci., 5479, 536–553 (2009), 査読有

③ N. Kurokawa Automorphy of the principal Eisenstein series of weight 1: an application of the double sine function, Kodai Math. J. 32, 391–403 (2009), 査読有

④ N. Kurokawa, H. Ochiai, A multivariable Euler product of Igusa type and its applications, J. Number Theory 129, 1919–1930 (2009), 査読有

⑤ G. Bisson, T. Satoh, More discriminants with the Brezing-Weng method, Progress in cryptology – INDOCRYPT 2008, Lect. Notes in Comput. Sci., 5365, 389–399 (2008), 査読有

⑥ N. Kurokawa, T. Satoh, Euclid prime sequences over unique factorization domains, 17, 145–152 (2008), 査読有

⑦ T. Satoh, Closed formulae for the Weil pairing inversion, Finite fields and their appl., 14, 743–765 (2008), 査読有

⑧ N. Kurokawa, Limit values of Eisenstein series and multiple cotangent functions, J. Number Theory, 128, 1775–1783 (2008), 査読有

⑨ S. Koyama, N. Kurokawa, Multiple Eisenstein series and multiple cotangent functions, J. Number Theory 128, 1769–1774 (2008), 査読有

⑩ T. Hiranouchi, Y. Taguchi, Extensions of truncated discrete valuation rings, Pure and Applied Mathematics Quarterly, 4, 1205–1214 (2008), 査読有

⑪ H. Moon, Y. Taguchi, On the finiteness and non-existence of certain mod 2 Galois representations of quadratic fields, Kyungpook Math. J., 48, 323–330 (2008), 査読有

⑫ H. Moon, Y. Taguchi, The nonexistence of certain mod 2 Galois representations of some small quadratic fields, Proc. Japan Acad. Ser. A Math. Sci., 84, 63–67 (2008), 査読有

〔学会発表〕（計 19 件）

① T. Satoh, Explicit formulae for certain primitive varieties associated to elliptic curves, 2009 KMS-AMS joint meeting, 2009.12.19, Seoul

② N. Kurokawa, Absolute zeta functions, absolute Riemann hypothesis and absolute Casimir energies, Casimir force, Casimir operators and Riemann hypothesis, 2009.11.13, Fukuoka, Japan

③ T. Satoh, Generating genus two hyperelliptic curves over large characteristic finite fields, 13th Workshop on elliptic curve cryptography, 2009.08.26, Calgary, Canada

④ T. Satoh, Simple but not absolutely simple Jacobians in cryptography, 1st PRIMA congress, 2009.07.08, Sydney, Australia

⑤ Y. Taguchi, Extensions of truncated discrete valuation rings, Modular Forms and Function Field Arithmetic, a conference in honor of Jing Yu's 60th birthday, 2009.05.20, National Taiwan University, Taiwan.

⑥ T. Satoh, Generating genus two hyperelliptic curves over large characteristic finite fields, Eurocrypt 2009, 2009.04.30, Cologne, Germany

⑦ N. Kurokawa, Absolute modular forms, Non commutative geometry and geometry over the field with one element, 2009.03.26, Baltimore, U.S.A.

⑧ N. Kurokawa, Zeta functions over $\mathbf{F}_1$, ibid. 2009.03.24, Baltimore, U.S.A.

⑨ 佐藤孝和、超楕円暗号に適したある種の種数 2 の超楕円曲線の生成法、2009 暗号と情報セキュリティーシンポジウム、2009.01.23, 大津。

⑩ Y. Taguchi, Extensions of truncated discrete valuation rings (joint work with Toshiro Hiranouchi) Pan Asian Number Theory Conference, 2009.01.10, Pohang, Korea.

⑪ Y. Taguchi, Groebner bases over truncated discrete valuation rings, 1st POSTECH-Kyushu U. Joint Workshop, 2009.01.06, Pohang, Korea.

⑫ 田口雄一郎、頂切離散付値環のガロア理論 (平之内俊郎氏との共同研究)、ガロア理論とその周辺、2008.09.10 徳島、日本。

⑬ T. Satoh, Inversion Problems on the Weil pairing, Intensive Lectures in Mathmatical Problems in cryptography, 2008.01.28, Seoul, Korea

⑭ Y. Taguchi, The non-existence of certain mod 2 Galois representations of some small quadratic fields, East Asia Number Theory Conference, 2008.01.21, Daejeon, Korea.

⑮ T. Satoh, On Pairing Inversion Problems, Pairing conference, 2007.07.04, Tokyo, Japan

⑯ Y. Taguchi, Moduli of Galois representations and their applications, P-adic method and its applications in arithmetic geometry 2007, 2007.06.12, Tokyo, Japan.

⑰ Y. Taguchi, Problems on q-Specht modules, The 19th PNU-POSTECH Algebraic Combinatorics Seminar, 2007.06.02, Pohang, Korea.

⑱ T. Satoh, On Euclid prime sequences (joint work with Nobushige Kurokawa), Workshop on computational challenges arising in algorithmic number theory and cryptography, 2006.11.03, Canada, Toronto.

⑲ Y. Taguchi, On extensions of truncated discrete valuation rings (joint work with T. Hiranouchi), 2006.09.27, Number Theory Seminar, Seoul, Korea.

６．研究組織

(1) 研究代表者

佐藤　孝和 (SATOH TAKAKAZU)
東京工業大学・大学院理工学研究科・准教授
研究者番号：70215797

(2) 研究分担者

該当なし

(3) 連携研究者

黒川　信重 (KUROKAWA NOBUSHIGE)
東京工業大学・大学院理工学研究科・教授
研究者番号：70114866

川内　毅 (KAWACHI TAKESHI)
東京工業大学・大学院理工学研究科・助教
研究者番号：30323778

田口　雄一郎 (TAGUCHI YUICHIRO)
九州大学・数理学研究院・准教授
研究者番号：90231399