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　４ 年　 ６ 月 ２０ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９６６

研究課題名（和文）高度楕円曲線暗号の研究開発

研究課題名（英文）Study and development of advanced elliptic curve cryptosystem

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・教授

研究者番号：７０５３０７５７

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：効率的に剰余算がなされハードウェア実装に適している楕円曲線を探索するアルゴリズムを提案し，そこで発見された曲線を用いた楕円曲線のスカラー倍算のFPGA実装を行った．また，楕円曲線上の2次と3次の指標を提案し，これらの指標を使う点の位数の偶奇性や3や4の倍数性の効率的な判定法を提案した．ペアリング暗号については，様々な埋め込み次数を持つペアリング・フレンドリー曲線を対象として，拡大体構成法と最終べき計算の改良を行った．同種写像暗号の1つであるSIDHについては，拡大体の構成の改良と同型写像を用いる計算法の改良を行った．楕円曲線の新しい演算であるMe演算を用いた疑似乱数生成法を提案した．

研究成果の学術的意義や社会的意義
電子署名ECDSAや鍵共有ECDHEを含む楕円曲線暗号は現在SSL/TLS通信やブロックチェーン等で広く普及している．IDベース暗号やグループ署名，属性ベース暗号などの機能性を有した暗号技術である高機能暗号は，その多くは楕円曲線上のペアリング写像を利用している．楕円曲線間の同種写像は，耐量子計算機の出現後も安全性が保たれる同種写像暗号の構成に利用される．このように楕円曲線は，様々なタイプの暗号技術の構成要素となっている．本研究はこれらの暗号の高速化や新しい演算Meの暗号技術への応用に対する成果を得ており，暗号技術や情報セキュリティ分野に貢献した．

研究成果の概要（英文）：For elliptic curve cryptography, the principal investigator proposed an algorithm to search for an elliptic curve suitable for hardware implementation because the remainder is efficiently calculated, and implemented scalar multiplication of an elliptic curve using the curve found by the algorithm on FPGA. He also proposed quadratic and cubic characteristics on elliptic curves, and suggested efficient methods for determining the evenness of the order of points and the ploidy of 3 or 4 using these characteristics. For pairing cryptosystems, he improved the extension field construction method and final exponentiation calculation for pairing-friendly curves with various embedded degrees. For SIDH, which is one of post-quantum cryptography, he improved the composition of the extension field and the calculation method using the isomorphism. He proposed a pseudo-random number generation method using the Me operation, which is a new operation of elliptic curves.

研究分野：情報セキュリティ

キーワード：暗号　楕円曲線　ペアリング　同種写像　高速実装

※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、研究者個人に帰属します。

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

SSL/TLS 通信や V2X 通信などで普及している楕円曲線暗号は，楕円曲線の群演算を利用している．ID ベース暗号や属性ベース暗号，グループ署名，時間指定暗号，放送型暗号，キーワード検索公開鍵暗号等の高機能暗号は，楕円曲線のペアリングと呼ばれる写像と群演算を利用している．耐量子計算機性を持つ同種写像暗号は，楕円曲線の同種写像の連続的な構成を利用している．このように楕円曲線は様々なタイプの暗号の構成要素となっているが，処理の高速化が課題となっている．更に，研究代表者は楕円曲線の Me 演算を提案しており，暗号への応用を試みていた．

２．研究の目的

楕円曲線のペアリング写像や同種写像，Me 演算，及びこれらの組み合わせが，低計算コスト公開鍵暗号の構成，高機能耐量子暗号の構成，全く新しい公開鍵暗号の構成に寄与できるかを研究し，これらのソフトウェア/ハードウェア高速実装を行うことが本研究の目的である．

３．研究の方法

(1)　本研究の開始前の時点で，Me 演算は群演算+との分配律を満たすこと，Me 演算離散対数問題は楕円曲線離散対数問題と同等かより困難であること，Me 演算 Diffie-Hellman 問題は楕円曲線 Diffie-Hellman 問題より顕著に簡単であることが判明していた．本研究では，更なる Me 演算の性質を調査し，群演算やペアリング計算，同種写像，並びに Me 演算を用いた暗号に関係するアルゴリズムを提案する．

(2) (1)で提案した暗号アルゴリズムに対して，その正当性を理論的及びプログラミングにより確認する．ハードウェア実装については，実際に FPGA 上で動作を確認し，Quartus Prime のような FPGA 開発メーカーが提供している開発ツールを使って動作の正当性を確認する．

４．研究成果

(1) 準備

初めに，本報告書全体に関係する有限体と楕円曲線について紹介する．具体的な本研究の成果は(2)節以降に記載する．

①　有限体

四則演算で閉じている集合を体と言い，体Kから$\{0\}$を除いた集合をK^*と表記する．素数pに対して集合$\mathbb{F}_p = \{0,1,2,\cdots,p-1\}$は体となる．$\mathbb{F}_p$での加減乗算は$a \pm b \bmod p$，$a \cdot b \bmod p$で定義される．$\mathbb{F}_p$での$a^{-1}$は$a^{-1} = a^{p-2} \bmod p$と計算される．なお$\mathbb{F}_p$では，不定方程式$ax + by = 1$の整数解を使って$a^{-1} = y$とすることもできる．除算は$a/b = a \cdot b^{-1}$とする．

「$\mathbb{F}_p$の元(g, y)に対して$y = g^n$を満たすnを求める」問題を離散対数問題(**DLP**)といい，「(g, g^a, g^b)からg^{ab}を計算する」問題を Diffie-Hellman 問題(**DHP**)という．pが 2048 ビット以上ならば DLP と DHP は十分に難しいと信じられている．例えば，SSL/TLS 通信でよく用いられている鍵共有 DHE は DHP の困難性を安全性の根拠としている．

素数pが奇数の時，$a \in \mathbb{F}_p$に対して，**Legendre 記号**(a/p)は$(a/p) = a^{p-1/2}$と定義される．$(a/p) \in \{-1, 0, 1\}$であり，「$(a/p) = 1 \Leftrightarrow a = b^2$を満たす$b \in \mathbb{F}_p^*$が存在する」が成り立つ．

適切な基底による$\mathbb{F}_p$のk次ベクトル空間は乗除算が定義され体を成す．例えば$\mathbb{F}_p$係数のk次既約多項式の根の 1 つをαとすると，集合$\{1, \alpha, \alpha^2, \cdots, \alpha^{k-1}\}$を基底とすれば良い．この体を$\mathbb{F}_{p^k}$と表記し，$\mathbb{F}_p$の$k$次**拡大体**と呼ぶ．$\mathbb{F}_{p^k}$の元$\alpha$に対して，$p$乗写像：$\alpha \to \alpha^p$は **Frobenius 写像**と呼ばれる．これはとても低コストで計算でき，基底の選び方によってはコストを無視できる場合もあり，暗号実装でよく利用される．$\mathbb{F}_p$や$\mathbb{F}_{p^k}$は有限集合かつ体なので**有限体**を呼ばれる．

②　楕円曲線

楕円曲線とは$E: y^2 = x^3 + ax + b$で与えられる 3 次曲線を指すことが多く，他にも Montgomery 曲線$by^2 = x^3 + ax^2 + x$等他の形式の楕円曲線も暗号実装の対象となる．いずれの形式の楕円曲線Eでも$P, Q \in E$に対して$P + Q \in E$が定義され，$(E, +)$は**無限遠点**Oを単位元とする群を成す．例えば，$E: y^2 = x^3 + ax + b$の場合，$P = (x_1, y_1)$，$Q = (x_2, y_2)$，$P + Q = (x_3, y_3)$とすると，$\lambda = (y_1 - y_2)/(x_1 - x_2)$，$x_3 = \lambda^2 - x_1 - x_2$，$y_3 = \lambda(x_3 - x_1) + y_1$により$(x_3, y_3)$を計算できる．言い換えると，$P + Q$の座標は$P$と$Q$の座標の四則演算で計算できる．

$P \in E$と自然数nに対して，$nP = P + P + \cdots + P$(n個の和)と表記する．PとnからnPを求める計算を**スカラー倍算**という．Eの係数a, bが$\mathbb{F}_p$の元である時，座標が$\mathbb{F}_p$であるEの点の集合を$E(\mathbb{F}_p)$と表記する．但し$O \in E(\mathbb{F}_p)$とする．$E(\mathbb{F}_p)$の点の個数を$\#\boldsymbol{E}(\mathbb{F}_p)$で表す．$P \in E(\mathbb{F}_p)$に対して，$nP = O$となる最小の自然数$n$を点$P$の**位数**という．

「$E(\mathbb{F}_p)$の 2 点(P, Q)から$Q = nP$を満たすnを見つける」問題を楕円曲線離散対数問題(**ECDLP**)といい，「(P, aP, bP)からabPを計算する」問題を楕円曲線 Diffie-Hellman 問題(**ECDHP**)という．pのサイズが 256 ビット以上ならば，ECDLP や ECDHP を解くことは困難であると信じられている．

SSL/TLS 通信でよく用いられている鍵共有 ECDHE や公開鍵暗号 ECElGamal を含む楕円曲線暗号は ECDHP の困難性を安全性の根拠としている．

(2) 楕円曲線署名のハードウェア実装に適した楕円曲線の探索とその実装
楕円曲線暗号の支配的な演算は$E(\mathbb{F}_p)$でのスカラー倍算であるが，これは$\mathbb{F}_p$の四則演算により計算される．特に$\mathbb{F}_p$での乗算，つまり$X \cdot Y \bmod p$の高速化が楕円曲線暗号の処理の高速化のキーとなる．

素数pが$p = 2^n \pm k$（kは小さな値）という形をしている時，この形の素数を擬メルセンヌ素数といい，高速に剰余$\bmod p$を計算できる．なお，$2^n - k$型の方が$2^n + k$型より剰余計算が効率的である．楕円曲線署名では点Pの位数lに対して，$\bmod l$の計算も必要となる．楕円曲線暗号の高速実装に適しているため人気がある Curve25519 は，pは$2^n - k$型の擬メルセンヌ素数，点の位数lは$2^n + k$型の擬メルセンヌ素数となる楕円曲線である．

本研究はpとlの両方が$2^n - k$型の擬メルセンヌ素数となる楕円曲線を探索するアルゴリズムを考案し，実際にそのような楕円曲線を 6 つ発見できた．ここではその 1 つの情報を記載する．

$$p = 2^{256} - 13497455,$$
$$E: 3y^2 = x^3 + 6x^2 + x,$$
$$l = (2^{256} - 2957934789948645541405169982804967901 24)/4$$

更に，この楕円曲線を使ったスカラー倍算の FPGA によるハードウェア実装を行った．

(3) 楕円曲線の指標の提案
素数pは 5 以上とし，楕円曲線Eは$E: y^2 = x^3 + ax^2 + bx$という形をしているとする．この時，$(0,0) \in E(\mathbb{F}_p)$は位数 2 を持つ．写像$\phi: E(\mathbb{F}_p) \to \{-1,1\}$を Legendre 記号を使って次のように定義する．

$$\phi(O) = 1, \phi((0,0)) = (b/p), \phi((x,y)) = (x/p)$$

すると，$\phi(P+Q) = \phi(P) \cdot \phi(Q)$を満たす．数学用語を用いると$\phi$は$E(\mathbb{F}_p)$の 2 次の指標となっている．

素数pは$p \equiv 1 \pmod 3$を満たすとする．楕円曲線Eは$E: y^2 + axy + by = x^3$という形をしているとする．この時，$(0,0)$は位数 3 を持つ．$\alpha \in \mathbb{F}_p$に対して，$\chi(\alpha) = \alpha^{p-1/3}$とする．$\phi': E(\mathbb{F}_p) \to$ {1 の 3 乗根}を次のように定義する．

$$\phi'(O) = 1, \phi'((0,0)) = \chi(b^2), \phi'((x,y)) = \chi(y)$$

すると，$\phi'(P+Q) = \phi'(P) \cdot \phi'(Q)$を満たす，つまり，$\phi'$は$E(\mathbb{F}_p)$の 3 次の指標である．

上記の 2 次及び 3 次の指標は，一般的な形式$y^2 = x^3 + ax + b$へ適用できるように簡単に改良できる．これらの指標は点の位数の偶奇性や 3,4 の倍数性の効率的な判定に用いることができ，ある種の暗号ハードウェアの攻撃の回避に用いられる可能性がある．

(4) ペアリングに関する成果
①ペアリングについて
$\mathbb{F}_p$係数の楕円曲線Eに対して，rを$\#E(\mathbb{F}_p)$の素因数とする．$r \mid p^k - 1$を満たす最小自然数kをrに関するEの埋め込み次数といい，この時写像$e: E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})[r] \to \mathbb{F}_{p^k}$で$e(P, Q+Q') = e(P,Q) \cdot e(P,Q')$と$e(P+P', Q) = e(P,Q) \cdot e(P',Q)$を満たすものを構成できる．このような写像はペアリングと呼ばれ，代表的なペアリングに Ate ペアリングが知られている．ペアリングを利用することで ID ベース暗号や属性ベース暗号，グループ署名，時間指定暗号，放送型暗号，キーワード検索公開鍵暗号等の高機能暗号を構成できる．$\log p / \log r$をロー値と呼ぶ．Ate ペアリングにおいて埋め込み次数kとロー値はペアリング計算の効率性に関係する重要パラメータである．

適切な埋め込み次数とロー値を持つ楕円曲線はペアリング・フレンドリー曲線と呼ばれる．代表的なペアリング・フレンドリー曲線として，BLS 曲線，BN 曲線，MNT 曲線等が著名である．本研究では BLS 曲線に注目する．例えば$k = 3^i$に対して，uを変数とする多項式

$$r(u) = \left(x^{2 \cdot 3^{i-1}} + x^{3^{i-1}} + 1\right)/3$$
$$m(u) = (u-1)^2$$
$$p(u) = m(u) \cdot r(u) + u$$

を考える．$r(u)$は円分多項式Φ_kを用いると$r(u) = \Phi_k(u)/3$と書ける．これらは多項式の計算として$r(u) \mid p(u)^k - 1$を満たす．$p(u)$と$r(u)$が共に素数となる$u = u_0$に対して，適切なbを選ぶと，楕円曲線$y^2 = x^3 + b$は$r(u_0)$に関する埋め込み次数kを持つ．

Ate ペアリングの計算は,Miller のアルゴリズムの実行とその出力を$(p^k - 1)/r$乗する部分(最終べき)に分けられる．最終べきの指数は

$$(p^k - 1)/r = (p^k - 1)/\Phi_k(p) \cdot \Phi_k(p)/r$$

と書ける．$(p^k - 1)/\Phi_k(p)$乗の計算は計算コストの低い Frobenius 写像と何回かの乗算で計算できるため，easy part と呼ばれる．残りの$\Phi_k(p)/r$乗の計算は hard part と呼ばれる．Hard part の効率化はペアリング計算の効率化にとって重要である．

②具体的な成果
最終べきの hard part の指数が$\lambda_s p^s + \lambda_{s-1} p^{s-1} + \cdots + \lambda_1 p + \lambda_0$と表現できる時，hard part は$\lambda_i$乗と Frobenius 写像，乗算，逆元計算($\lambda_i$が負の値の時に必要)で計算できる．本研究ではすべて

の BLS 曲線に対して集合$\{\lambda_i\}$はアルゴリズム 1 で与えられることを示した.

アルゴリズム 1
入力: BLS 曲線を定義するu, 埋め込み次数$k, m = m(u)$
出力: BLS 曲線の hard part の指数を与える集合$\{\lambda_i\}$
1. $k' = \phi(k)$（オイラーの関数）
2. $\Phi_k(x) = e_{k'}x^{k'} + e_{k'-1}x^{k'-1} + \cdots + e_1x + e_0$（円分多項式）
3. for $i = k' - 2$ down to 0
4. $\lambda_i = u\lambda_{i+1} + e_{i+1}\lambda_{k'-1}$
5. end for
6. $k = 3^i$の時 $\lambda_0 = \lambda_0 + 3$ その他の時 $\lambda_0 = \lambda_0 + 1$
7. return $\{\lambda_i\}$

更にペアリングに関して以下を行った.

1. 拡大体の演算に sparse multiplication を用いることで Miller のアルゴリズムを約 6%高速化した.
2. 現在の標準である 128 ビットセキュリティの埋め込み次数 15 のペアリングにおいて, AOPF という拡大体構成法を用いることで 10%ほど高速化した.
3. 埋め込み次数が$k = 2^i \cdot 3 (i > 1)$である BLS 曲線について, パラメータuが$u \equiv 7, 16, 31, 64 \pmod{72}$の時, 楕円曲線の係数を決定でき拡大体をシステム的に構成できることを示した. 同様に, 埋め込み次数6の BLS 曲線について, $u \equiv 7, 10, 16, 28, 31, 34 \pmod{36}$の時, 楕円曲線の係数を決定でき拡大体をシステム的に構成できることを示した.
4. 埋め込み次数 15 の BLS 曲線の最終べき計算法を改良した.
5. コンピュータによる探索を主とするペアリング・フレンドリー曲線の探索法を提案した. いくつか新しいペアリング・フレンドリー曲線を発見できたが, 既知のものより計算コストが削減される曲線は発見できていない.
6. Special TNFS という攻撃法に耐性のある埋め込み次数 10, 11, 13, 14 のペアリングの最終べき計算法を提案し計算コストを評価した.
7. $k \equiv 1 \pmod{6}$を満たす素数の場合に適用できる効率的な最終べき計算法を提案した.

(5) 同種写像暗号の効率化

①同種写像暗号について

2 つの楕円曲線E, E'間の写像$\phi: E \to E'$が任意の$P, Q \in E$に対して$\phi(P + Q) = \phi(P) + \phi(Q)$と$\phi(O) = O$を満たす時, ϕを同種写像という. Velu の公式を用いることで, Eと$P \in E$から核が$\{O, P, 2P, \dots\}$となるようなE'と同種写像ϕを構成できる. 同種写像暗号では, Velu の公式による同種写像の連続的な構成が支配的な処理となる. 同種写像暗号には SIDH や CSIDH 等がある.

②具体的な成果

SIDH の実装には$\mathbb{F}_p$の 2 次拡大体が必要となる. 本研究では, 2 次拡大体のいくつかの構成法について, 計算コストの比較行い, 拡大体の適切な構成や同型写像の利用による SIDH の計算法の効率化を提案した.

(6) Me 演算を用いる疑似乱数生成法の提案

①Me 演算について

写像 Me: $E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$を

$$Me(P, Q) = \begin{cases} P & P = Q\text{の時} \\ 2P - Q & sign(P - Q) = 1 \text{ の時} \\ 2Q - P & sign(Q - P)\text{の時} \end{cases}$$

と定義する. ここで, $sign(\cdot)$はLegendre 記号を使って$sign((x, y)) = (y/p)$と定義される. また, $P \oplus Q = Me(P, Q)$とも書くことにする. スカラー倍の Me 版を定義したいが, 単に$\oplus$の繰り返しでは$P \oplus P \oplus \cdots \oplus P = P$となりこの定義では意味がない. そのため先行研究では, $P, Z \in E(\mathbb{F}_p)$と自然数nに対して, Zを補助元とする Me スカラー倍$P_{n,Z}$をアルゴリズム 2 の出力として定義した.

Me 演算離散対数問題(MeDLP)を「(P, Q, Z)に対して$Q = P_{n,Z}$を満たすnを求める」問題と定義し, Me 演算 Diffie-Hellman 問題(MeDHP)を「$(P, Z, P_{n,Z}, P_{m,Z})$から$(P_{n,Z})_{m,Z}$を計算する」問題と定義する. 興味深いこと MeDLP と MeDHP は次の性質がある.

性質 1: MeDLP は ECDLP と同等かより困難である.

性質 2: MeDHP は簡単に解くことができる.

これは MeDLP の困難性を利用した暗号プロトコルを構成できる可能性はあるものの，ECDHE や ECElGamal 暗号のような ECDHP の困難性を利用している楕円曲線暗号の Me 版は全く安全でないものとなることを意味する．性質 2 が Me 演算の暗号応用を困難にしている理由である．

アルゴリズム 2
入力: $P \in E(\mathbb{F}_p)$，自然数nの 2 進数表現$n_{l-1}, n_{l-2}, \cdots, n_0$ 出力: $P_{n,Z}$
1. $Y = P$ 2. for $i = l - 2$ down to 0 3. $Y = (Z + Y) \oplus Y$ 4. if $n_i = 1$ then $Y = Y \oplus P$ 5. end for 6. return Y

②具体的な成果

DLP の困難性を利用した以下のような疑似乱数生成法が知られている．

$g \in \mathbb{F}_p^*$を生成元とし，自然数a_0を 1 つ選ぶ．再帰的に$a_i = g^{a_{i-1}} - 1$を計算する．$LSB(a_i)$の連結を疑似乱数とする．

この疑似乱数生成法は 2 つの演算，乗算と減算を必要とする．しかしながら従来は$E(\mathbb{F}_p)$には演算が$+$しかないため，この疑似乱数生成法の楕円曲線版は構成できなかった．

本研究は，$E(\mathbb{F}_p)$が位数 2 の点Tを持つ場合，Me 演算$\oplus$を$E(\mathbb{F}_p)$の 2 つ目の演算と見なすと，$\mathbb{F}_p$での「-1」という計算が$E(\mathbb{F}_p)$での「$\oplus T$」という計算に対応することを示した．これにより，ECDLP の困難性を利用した疑似乱数生成法は以下のようになる．

$G \in E(\mathbb{F}_p)$を生成元とし，自然数a_0を 1 つ選ぶ．再帰的に$a_i = a_{i-1}G \oplus T$のx座標とする．$LSB(a_i)$ の連結を疑似乱数とする．

残念ながらこの疑似乱数生成法は,ECDLP の困難性を利用した Me 演算を用いる手法であり,MeDLP の困難性を利用していない．今後は MeDLP の困難性を利用した暗号プロトコルを考案したい．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 NANJO Yuki、SHIRASE Masaaki、KUSAKA Takuya、NOGAMI Yasuyuki	４．巻 11
２．論文標題 Restrictions of Integer Parameters for Generating Attractive BLS Subfamilies of Pairing-Friendly Elliptic Curves with Specific Embedding Degrees	５．発行年 2021年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 383～411
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.11.2_383	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 NANJO Yuki、SHIRASE Masaaki、KUSAKA Takuya、NOGAMI Yasuyuki	４．巻 E104.A
２．論文標題 Improvement of Final Exponentiation for Pairings on BLS Curves with Embedding Degree 15	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 315～318
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAL2046	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 NANJO Yuki、SHIRASE Masaaki、KUSAKA Takuya、NOGAMI Yasuyuki	４．巻 E103.A
２．論文標題 A Construction Method of an Isomorphic Map between Quadratic Extension Fields Applicable for SIDH	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1403～1406
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020TAL0002	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 NANJO Yuki、SHIRASE Masaaki、KUSAKA Takuya、NOGAMI Yasuyuki	４．巻 10
２．論文標題 A Performance Analysis and Evaluation of SIDH Applied Several Implementation-Friendly Quadratic Extension Fields	５．発行年 2020年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 227～241
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.10.2_227	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計15件（うち招待講演　0件／うち国際学会　4件）

１．発表者名
白勢政明

２．発表標題
有限体上楕円曲線の3次の指標

３．学会等名
日本応用数理学会2021年度年会

４．発表年
2021年

１．発表者名
NANJO Yuki, SHIRASE Masaaki, KODERA Yuta, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
Efficient Final Exponentiation for Pairings on Several Curves Resistant to Special TNFS

３．学会等名
CANDAR 2021（国際学会）

４．発表年
2021年

１．発表者名
NANJO Yuki, SHIRASE Masaaki, KODERA Yuta, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
A Construction Method of Final Exponentiation for a Specific Cyclotomic Family of Pairing-Friendly Elliptic Curves with Prime Embedding Degrees

３．学会等名
CANDAR 2021（国際学会）

４．発表年
2021年

１．発表者名
白勢政明

２．発表標題
位数が4kの有限体上楕円曲線の点の位数の判定法

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
NANJO Yuki, SHIRASE Masaaki, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
Specific Congruence Classes of Integer Parameters for Generating BLS Curves for Fast Pairings.

３．学会等名
CANDAR (Workshops) 2020（国際学会）

４．発表年
2020年

１．発表者名
白勢政明，南條由紀

２．発表標題
任意のBLS曲線の最終べきのhard partについて

３．学会等名
情報セキュリティ研究会

４．発表年
2020年

１．発表者名
白勢政明

２．発表標題
Pairing-friendly曲線のファミリーの構成について

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
白勢政明

２．発表標題
偶数位数を持つ有限体上楕円曲線の2次の指標

３．学会等名
応用数理学会2019年度会

４．発表年
2019年

１．発表者名
NANJO Yuki, SHIRASE Masaaki, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
A Performance Analysis of Supersingular Isogeny Diffie-Hellman with Several Classes of the Quadratic Extension Fields

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
白勢政明

２．発表標題
楕円曲線のMe演算の負演算とその応用

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
NANJO Yuki, TAKAHASHI Yuto, SHIRASE Masaaki, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
Improvement of Miller's Algorithm of Pairing on Elliptic Curves with Embedding Degree 15 by Using Sparse Multiplication in Affine Coordinates

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
白勢政明

２．発表標題
有限体上の楕円曲線の指標と点の位数の偶奇性

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
NANJO Yuki, SHIRASE Masaaki, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
A Performance Analysis and Evaluation of SIDH with Implementation-Friendly Classes of Quadratic Extension Fields

３．学会等名
CANDAR2019（国際学会）

４．発表年
2019年

１．発表者名
白勢政明

２．発表標題
Curve25519より少し良いかもしれない楕円曲線とそのハードウェア実装の考察

３．学会等名
暗号と情報セキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
NANJO Yuki, KODERA Yuta, MATSUMURA Rikuya, SHIRASE Masaaki, KUSAKA Takuya, NOGAMI Yasuyuki

２．発表標題
Evaluation of Pairing on Elliptic Curves with Embedding Degree 15 with Type-II All-one Polynomial Extension Field of Degree 5

３．学会等名
暗号と情報セキュリティシンポジウム2020

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関