日本応用数理学会論文誌
Vol. 25, No. 2, 2015, pp. 117～133

楕円曲線暗号の進展

高島 克幸 †
† 三菱電機株式会社 情報技術総合研究所

概要. 楕円曲線暗号は，Koblitz, Miller によって独立に 1985 年に提案されて以来，新たな応用を生み出しながら，現在まで発展している．本稿では，私が関わったトピックを中心にして，誕生 30 年を迎える楕円曲線暗号の進展を，数論アルゴリズム的な側面から振り返る．特に，スカラー倍算，ペアリング演算，同種写像計算という 3 つの一方向性関数と，それらに基づく Diffie-Hellman 型鍵共有法に焦点を当てながらサーベイを行う．

The Evolution of Elliptic Curve Cryptography

Katsuyuki Takashima†
†Information Technology R&D Center, Mitsubishi Electric Corporation

Abstract. Elliptic curve cryptography was proposed independently by Koblitz and Miller in 1985. Since then, it has evolved into a powerful tool for new applications. Here, I will survey the evolution of elliptic curve cryptography in terms of three central one-way functions, i.e., scalar multiplication, pairing operation, and isogeny sequence computation, and associated Diffie-Hellman type key exchanges.

1. はじめに

暗号技術の良し悪しを測るには，安全性・効率性・機能性の 3 つの側面があり，それらを出来るだけ高める努力が行われてきた[*1]．本稿では，楕円曲線暗号が，それら 3 側面でそれぞれ固有な特性を示しながらここまで進んできていることを概観する[*2]．これは楕円曲線暗号研究が既に豊かな研究分野に成長していることを示している．また，本稿では，楕円曲線暗号の進展を，数論アルゴリズム的な課題と共に振り返る．2005 年以前の研究動向は，全般的に事典 [10] を参照する．また，本稿では，広い範囲の読者を想定して可読性を優先して記述した．より厳密な数学的取り扱いに関しては，標準的な教科書，例えば，[10, 19, 52, 59] を参照されたい．

本サーベイ論文は，2014 年度日本数学会年会 企画特別講演アブストラクト「楕円曲線暗号の進展」を，加筆・修正したものである．

[*1] 例えば，「安全性」改善と一口に言っても，実際に解読時間を短くするような改善もあれば，安全性証明の根拠となる計算量仮定をより望ましいものにする改善もあり，各性質の意味するところは多岐に渡るが，ここでは，その点には深入りしない．

[*2] ペアリング暗号，同種写像暗号を含めずに，楕円曲線離散対数問題の困難性に基づく暗号を狭義に楕円曲線暗号と呼ぶことも多いが，本稿では，その狭義楕円曲線暗号を従来型楕円曲線暗号と呼び，上記の先進暗号も含めて楕円曲線を用いた暗号を広義に（単に）楕円曲線暗号と呼ぶ．

暗号方式は，秘密鍵暗号と公開鍵暗号に大別される．秘密鍵暗号では送受信者間で秘密保持された同じ鍵を使って暗号化と復号が行われるのに対し，公開鍵暗号では暗号化と復号に別の鍵を使い，しかも暗号化鍵を（インターネット上に）公開しても安全性が保たれるという特長を持つ．一方，秘密鍵暗号の特長は，一般的に公開鍵暗号より暗号化・復号処理が高速であることである．従って，通常よく使われているインターネット標準セキュリティプロトコル SSL/TLS（最新版 TLS 1.2 [15]）などでは，実際のデータ暗号化（及び復号）には秘密鍵暗号を使い，その秘密鍵暗号で用いる鍵を共有するために公開鍵暗号を使う．更に，標準化・実用化状況を知るためには，例えば [48] を参照されたい．

公開鍵暗号の一種である楕円曲線暗号は，Koblitz [32], Miller [35] によって独立に 1985 年に提案されて以来，新たな応用を生み出しながら，現在まで発展してきている．その提案当初は，「効率性」の観点から，先行提案されていた RSA 暗号に比べて，短いデータサイズ，効率的な処理性能を実現する公開鍵暗号として注目された．そして，楕円曲線パラメータ生成法や効率的な演算法という現実的な課題から，数論アルゴリズムの研究分野としても広がって行った．次に，2000 年前後から，ペアリング演算が 3 者間鍵共有 [27], ID ベース暗号 [5,41]，属性ベース暗号 [23,44]，述語暗号 [30] という新機能暗号を構成できるという「機能性」の観点から注目され，暗号学的な応用研究と共に，ペアリング暗号を高速に実装するための数論アルゴリズム研究が進展した．そして，2006 年頃 [8,13,43] から，複数の楕円曲線を扱う同種写像も暗号演算に取り込まれて，楕円曲線（同種写像）という数論的要素を使いながらも，量子計算機に耐性を持つ公開鍵暗号が構成できるという「安全性」の観点から注目されている．

その 3 側面は，第 2.1 節で示す 3 つの一方向性関数の特性にそれぞれ対応しており，それらを順次説明する．では，公開鍵暗号の源流である Diffie-Hellman（DH）鍵共有法 [16] から始める．大素数 p に関する有限体乗法群 $\mathbb{F}_p^\times$ とその巡回群生成元 g を Alice と Bob の共有情報（公開パラメータ）として使う．以下，$x \xleftarrow{\cup} X$ は，x が集合 X から一様にサンプリングされることを示す．

Diffie-Hellman（DH）鍵共有

Alice		**Bob**
$\alpha \xleftarrow{\cup} \mathbb{Z}/(p-1)\mathbb{Z}$: Alice の秘密鍵, $K_{\mathrm{Alice}} := B^\alpha$	$\xrightarrow{A:=g^\alpha}$ $\xleftarrow{B:=g^\beta}$	$\beta \xleftarrow{\cup} \mathbb{Z}/(p-1)\mathbb{Z}$: Bob の秘密鍵, $K_{\mathrm{Bob}} := A^\beta$

$K := K_{\mathrm{Alice}} = K_{\mathrm{Bob}}$ が Alice と Bob の共有鍵である．良く知られているように，有限体乗法群 $\mathbb{F}_p^\times$ の離散対数（DL）問題が容易に解けてしまえば，その群を使った DH 鍵共有は安全でなくなる．本稿では，次章で掲げる 3 つの一方向性関数に即して，DH 鍵共有が，どのように発展していくのか辿ることで楕円曲線暗号の進展を跡付ける．

2. 楕円曲線に付随する3つの一方向性関数

2.1 3つの一方向性関数

本稿では，話しを簡便にするために，有限素体 $\mathbb{F}_p$ s.t. $p \geq 5$ 上定義された楕円曲線 $E: Y^2 = X^3 + aX + b$ $(a, b \in \mathbb{F}_p,\ 4a^3 + 27b^2 \neq 0)$ を専ら考える．無限遠点は O_E とする．良く知られたように2点の加算 $P_3 := P_1 + P_2$ を，$P_1 = O_E$（又は $P_2 = O_E$）の場合には，$P_3 := P_2$（又は $P_3 := P_1$）と定め，P_1, P_2 共に O_E でない場合は，$P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ を使って，$P_3 = (x_3, y_3)$ を

もし $x_1 \neq x_2$ 又は（$x_1 = x_2$ かつ $y_1 = y_2 \neq 0$）であれば，
$x_3 := \lambda^2 - x_1 - x_2$, $y_3 := \lambda(x_1 - x_3) - y_1$,
但し，もし $x_1 \neq x_2$ であれば，$\lambda := (y_2 - y_1)/(x_2 - x_1)$,
もし $x_1 = x_2$ かつ $y_1 = y_2 \neq 0$ であれば，$\lambda := (3x_1^2 + a)/2y_1$,
それ以外の場合は，$P_3 := O_E$

と定めれば代数群になる（幾何学的には Fig. 2 の右半部を参照）．$\overline{\mathbb{F}}_p := \cup_{k=1}^{\infty} \mathbb{F}_{p^k}$ を $\mathbb{F}_p$ の代数閉包，その任意の部分体 $\mathbb{F} \subseteq \overline{\mathbb{F}}_p$ に対し，$E(\mathbb{F})$ を x, y 座標が $\mathbb{F}$ に入る E 上の点と O_E がなす加法群とする．

この加算構造を基にして次の3種の一方向性関数が得られる．一方向性関数とは，順方向は効率的に計算できるが，逆方向は現実的に計算困難な関数である．暗号構成のための数学的原石と言うべきものであり，これを加工・洗練することで興味深い暗号が作り上げられる．以下では素数 r に関し r ねじれ点群を $E[r] := \{P \in E(\overline{\mathbb{F}}_p) \mid rP = O_E\}$ として，$P(\neq O_E) \in E[r] \cap E(\mathbb{F}_p)$ とする．

(2.1) スカラー倍算 $(P, \alpha) \underset{\text{困難}}{\overset{\text{容易}}{\rightleftarrows}} (P, \alpha P)$, 但し $\alpha \overset{\cup}{\leftarrow} \mathbb{Z}/r\mathbb{Z}$,

(2.2) ペアリング演算 $(P, Q) \underset{\text{困難}}{\overset{\text{容易}}{\rightleftarrows}} (P, e(P, Q))$, 但し $Q \overset{\cup}{\leftarrow} E[r]$, 定義は第2.3節参照,

(2.3) 同種写像計算 $(E, \phi) \underset{\text{困難}}{\overset{\text{容易}}{\rightleftarrows}} (E, \phi(E))$, 定義は第4.3節参照.

上の3演算の逆関数計算問題を，それぞれ楕円曲線離散対数（ECDL）問題，ペアリング逆関数（PI: Pairing Inversion）問題，同種写像（ISOG）問題と呼ぶ．それらに対し一般には多項式時間解法は知られていない．

順方向関数の効率的な計算法 スカラー倍算は，スカラーを2進展開したビット値に応じて加算，2倍算を組み合わせて計算する標準的な方法で行う．その効率化研究は，例えば

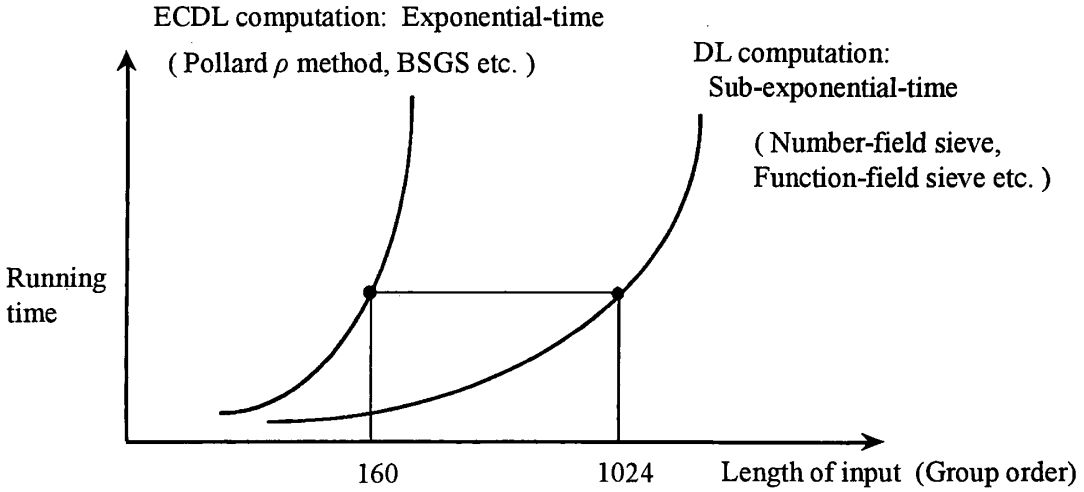


Fig. 1. Running time comparison of DL problem and ECDL problem

最近の [24] を参照されたい．ペアリング演算は，Miller アルゴリズム（第 2.3 節の Fig. 2）に基づき，同種写像計算は，Vélu の公式（第 4.2 節の式 (4.1)）に基づいて効率的に計算される．詳細は，それぞれの個所を参照されたい．

逆関数（ECDL，PI，ISOG）問題の困難性 これら逆関数問題の困難性の検討は，暗号の安全性と直結するため最重要である．まず，有限体乗法群上の DL 問題には，それらを持ちあげた代数体整数環や多項式環での素イデアルによるふるい法を用いることで準指数時間での解法があるのに対し，（大標数素体上の）ECDL 問題に対しては，有効な持ちあげ型解法が現在までに得られていないため，指数時間での解法しか知られていない（Fig. 1）．DL 問題解法に関する最近の進展は [28]，ECDL 問題持ちあげ型解法研究の現状は [53] を参照されたい．この DL 問題と ECDL 問題の困難性の定性的相違は，第 3 章でペアリング暗号用の曲線を生成する場合に重要な要素となる．特殊な曲線上の ECDL 解法（MOV 帰着法 [34]，SASS 法 [45,49,54]）も存在する．PI 問題に関しては，[20] を，ISOG 問題に関しては，[9,17] 等を参照されたい．

2.2 従来型 楕円曲線暗号の概要

前節で触れたように，効率的に計算可能なスカラー倍算（式 (2.1)）を使うことで DH 型の鍵共有法が得られ，それは ECDH（Elliptic Curve DH）鍵共有と呼ばれる．

楕円曲線 Diffie-Hellman（ECDH）鍵共有

Alice		**Bob**
$\alpha \xleftarrow{\cup} \mathbb{Z}/r\mathbb{Z}$: Alice の秘密鍵, $K_{\mathrm{Alice}} := \alpha B$	$\xrightarrow{A:=\alpha P}$ $\xleftarrow{B:=\beta P}$	$\beta \xleftarrow{\cup} \mathbb{Z}/r\mathbb{Z}$: Bob の秘密鍵, $K_{\mathrm{Bob}} := \beta A$

$K := K_{\mathrm{Alice}} = K_{\mathrm{Bob}}$ が Alice と Bob の共有鍵である．

Algorithm 1 Miller Algorithm

Input : Integer r, $P \in E[r], Q \in E$
(binary expansion of $r = \sum_{j=0}^{L} r_j 2^j, r_L = 1$),
Output : Miller variable $f_{r,P}(Q)$.
$T \leftarrow P, f \leftarrow 1$.
for $j = L-1$ downto 0 **do**
Calculate lines $l_{T,T}$ and v_{2T} for doubling T.
$f \leftarrow f^2 \cdot l_{T,T}(Q)/v_{2T}(Q)$.
$T \leftarrow 2T$.
if the j-th bit r_j of r is 1 **then**
Calculate lines $l_{T,P}$ and v_{T+P}
for adding T and P.
$f \leftarrow f \cdot l_{T,P}(Q)/v_{T+P}(Q)$.
$T \leftarrow T + P$.
end if
end for
Output f.

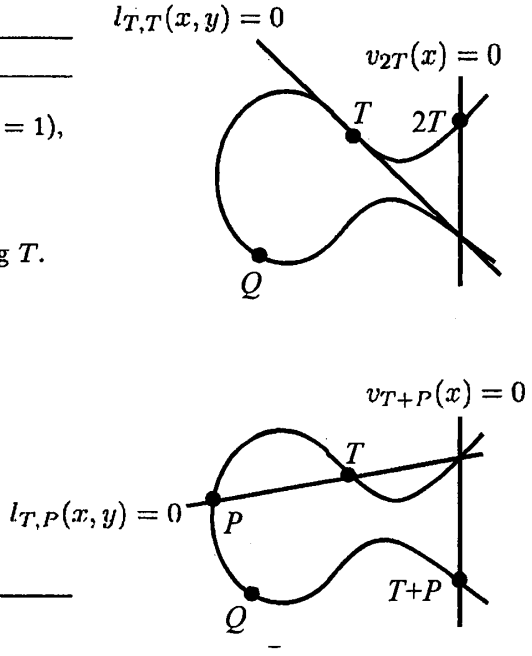


Fig. 2. Miller algorithm. Equations $l_{T,T}, v_{2T}, l_{T,P}, v_{T+P}$ in Algorithm 1 are defined geometrically as in the right hand part.

Fig. 1 では，1024 ビットサイズの DL 問題と 160 ビットサイズの ECDL 問題が同程度に困難であることを示している．これにより，DL 問題困難性に根拠を置く DH 鍵共有と ECDL 問題困難性に根拠を置く ECDH 鍵共有は，それぞれ 1024 ビット，160 ビットサイズで同程度に安全となる．つまり，同じ安全性レベルで，ECDH 鍵共有は，DH 鍵共有より短いデータサイズ，効率的な暗号化・復号処理を実現する．よって，ECDH 鍵共有は，楕円曲線ディジタル署名 ECDSA [1, 40] と共に，セキュリティプロトコル SSL/TLS の最新版 TLS 1.2 [15] で規定されている．

ECDH 鍵共有の安全性は，次の ECDH 問題の困難性に基づく．

ECDH 問題 入力 $(P, \alpha P, \beta P)$ に対し，$\alpha\beta P$ を計算せよ．ここで，$P \xleftarrow{U} E[r], \alpha, \beta \xleftarrow{U} \mathbb{Z}/r\mathbb{Z}$ とする．

明らかに，ECDH 問題が困難であるためには，少なくとも，その楕円曲線上の ECDL 問題が困難でなければならない．次節では，ペアリング暗号の安全性のためには，ECDH 問題の 2 つの一般化問題（BDH，LIN 問題）が良く使われていることを述べ，第 4.3 節では，同種写像を使った DH 型鍵共有の場合にその類似形が定義される．

2.3 ペアリング暗号の概要

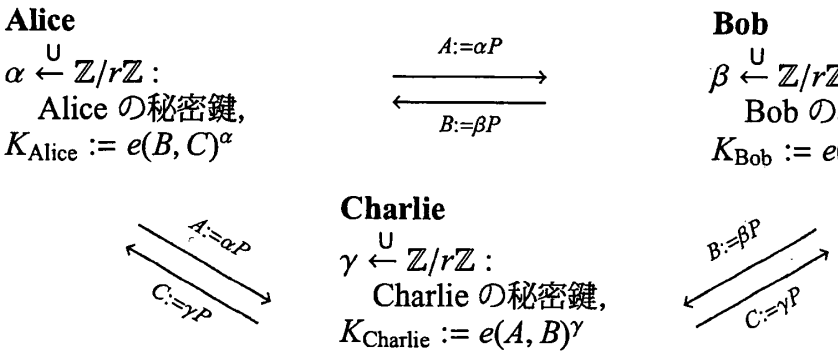
楕円曲線上の点 P, Q に対して効率的に計算できるペアリング関数 $e(P, Q)$ で $e(aP, bQ) = e(P, Q)^{ab}$, ある P, Q に対して $e(P, Q) \neq 1$，かつ PI 問題が困難になるものを利用した暗号をペアリング暗号と総称する．このようなペアリング関数 e は複数提案されている

が，それらの基本となるのは Weil ペアリングと Tate ペアリングであり，その計算の核は次の $f_{r,P}(Q)$ 計算である．$P \in E[r]$ より Abel の定理から $(f_{r,P}) = r((P) - (O_E))$ と（定数倍を除いて）決まる有理関数 $f_{r,P}$ の Q での値を $f_{r,P}(Q)$ とする．それは，Fig. 2 の Miller アルゴリズム [36] で効率的に計算できる．$f_{r,P}$ を因子 D 上の関数 $f_{r,P}(D)$ に線形に拡張して定義する．Weil ペアリング $e_{r,\mathrm{weil}} : E[r] \times E[r] \to \mu_r := \{1 \text{ の } r \text{ 乗根}\} \subset \overline{\mathbb{F}}_p$ は $e_{r,\mathrm{weil}}(P,Q) = f_{r,P}(D_Q)/f_{r,Q}(D_P)$ で与えられる．ここで，D_P, D_Q はそれぞれ $f_{r,Q}(D_P)$ 及び $f_{r,P}(D_Q)$ が零又は ∞ にならないように線形同値類の中で適切に選んだ因子 $D_P \sim (P) - (O_E), D_Q \sim (Q) - (O_E)$ である[*1]．また，$\mu_r \subset \mathbb{F}_{p^k}^{\times}$ となる最小の k は埋め込み次数と呼ばれる．Tate ペアリング $e_{r,\mathrm{tate}} : E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \to \overline{\mathbb{F}}^{\times}/(\overline{\mathbb{F}}^{\times})^r$ は Miller アルゴリズムと $\mathbb{F}_{p^k}^{\times}$ 内のべき乗算で計算される．また，実際には Tate ペアリングを応用した Optimal Ate ペアリングが通常良く使用されている．ペアリング暗号用の曲線として最初に使用されたのは，次に与える超特異楕円曲線であった[*2]：

$$E/\mathbb{F}_p : Y^2 = X^3 + b, \text{ ここで，素数 } p \equiv 2 \bmod 3 \tag{2.4}$$

その埋め込み次数 $k = 2$ で $\sharp E(\mathbb{F}_p) = \Phi_2(p) = p+1$ である．$r \mid \sharp E(\mathbb{F}_p)$ として，$\zeta (\neq 1 \in \mathbb{F}_{p^2}^*)$ s.t. $\zeta^3 = 1$ とする．ζ を使い $\psi : E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2})$ を $P = (x,y) \mapsto (\zeta x, y) = \psi(P) \notin \langle P \rangle$ とすると，$e(P,P) := e_{\mathrm{weil}}(P, \psi(P)) \neq 1$ となり，この $\langle P \rangle \times \langle P \rangle$ 上のペアリング e は，暗号研究において対称ペアリングと呼ばれ，素体上の有理点群 $\langle P \rangle$ で定義されたペアリングとなり，効率的に計算できる．対称ペアリングを用いて，3 者（Alice, Bob, Charlie）間で $K := e(P,P)^{\alpha\beta\gamma}$ を共有する DH 型鍵共有が以下のように実現できる [27].

3 者間 DH 鍵共有



3 者間で鍵を共有する方式は，[27] 以前にも知られていたが，それらはいずれも少なくとも 2 ラウンド通信を必要とした．1 ラウンド通信で 3 者間鍵共有を実現したのは上記方式が初めてであり，それは実用上有用であると共に，それ以後の様々な高機能ペアリング暗号の嚆矢となったことから理論的にも意義深いものであった．

[*1] 正確には，因子の台（Support）が $\mathrm{Supp}(D_P) \cap (f_{r,Q}) = \mathrm{Supp}(D_Q) \cap (f_{r,P}) = \emptyset$ となるように選択する．

[*2] ペアリング暗号が提案される以前から，k が小さくて MOV 帰着法 [34] が適用可能な曲線としてよく知られていたからペアリング暗号用曲線（ペアリングフレンドリ曲線）として最初に使用された．

3 者間 DH 鍵共有の安全性は，3 者版の DH 問題である次の双線形 DH（BDH）問題の困難性に基づく．

双線形 DH（BDH: Bilinear DH）問題 入力 $(P, \alpha P, \beta P, \gamma P)$ に対し，$e(P,P)^{\alpha\beta\gamma}$ を計算せよ．
ここで，$P \xleftarrow{\cup} E[r], \alpha, \beta, \gamma \xleftarrow{\cup} \mathbb{Z}/r\mathbb{Z}$ とする．

また，BDH 問題とは別の DH 問題の一般化として次の問題がある．

線形（LIN）問題 入力 $(P, \alpha P, Q = \beta P, R, \gamma R)$ に対し，$(\alpha+\gamma)Q = (\alpha+\gamma)\beta P$ を計算せよ．
ここで，$P, R \xleftarrow{\cup} E[r], \alpha, \beta, \gamma \xleftarrow{\cup} \mathbb{Z}/r\mathbb{Z}$ とする．

DL 問題が解ければ，DH 問題が解けたように，PI 問題が解ければ，BDH 問題と LIN 問題が解ける．我々 [42] は，判定版 LIN 問題の困難性という標準的な仮定に基づいて適応的安全な関数型暗号方式を初めて構成した[*1]．

2.4 同種写像暗号の概要

従来，同種写像は，パラメータ生成（SEA アルゴリズム [46,47]），効率化（GLV [22], GLS 法 [21] など）や安全性帰着（同種楕円曲線間 [26]，種数 3 超楕円ヤコビアンから高種数非超楕円ヤコビアンへ [55]）など様々な暗号応用を有してきた．最近になって積極的に新暗号構成に応用する動きが出てきた．量子計算機が出現すれば，Shor のアルゴリズム [51] により現在実用化している素因数分解問題や離散対数（DL）問題に基づいた公開鍵暗号が破れる（特に，式 (2.1),(2.2) は一方向でなくなる）．よって，量子計算機でも破れない一方向性関数に基づいた公開鍵暗号の構成が活発に研究されている．その候補として，格子ベース暗号や多変数多項式ベース暗号などいくつか提案されているが，同種写像一方向性関数（式 (2.3)）も量子計算機での多項式時間解法がこれまで知られておらず，同種写像ベース暗号は，耐量子計算機公開鍵暗号として期待されている．

3. ペアリング暗号の数理

3.1 ペアリング曲線生成法

ペアリング暗号を実装するのに適した楕円曲線を探す必要がある．特に，小さい埋め込み次数 k と大きい素数位数 r を有する楕円曲線が必要である．ペアリング暗号では，ECDL 問題と共に，ペアリングで移された先の有限体乗法群の DL 問題の困難性も考慮しなければいけないので，次の 3 条件を満たす楕円曲線が必要である．

1. $E[r]$ 上の離散対数問題が困難である．

[*1] 関数型暗号（特に，属性ベース暗号）は，復号条件（復号関数）を復号鍵の中に埋め込み可能な公開鍵暗号であり，[42] 方式は線形スパンプログラムと内積述語の複合関数を復号条件に使用できる．

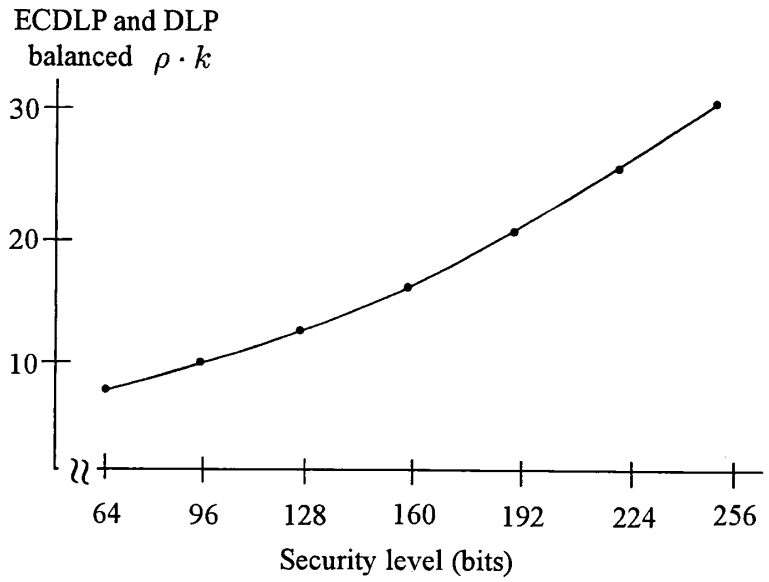


Fig. 3. Balancing $\rho \cdot k$ for ECDLP and DLP. Here, (EC)DLP stands for (Elliptic Curve) Discrete Logarithm Problem.

2. $\mathbb{F}_{p^k}^{\times}$ ($\supset \mu_r$) 上の離散対数問題が困難である.
3. ペアリング計算が効率的である.

これらをペアリングフレンドリ (pairing-friendly) 曲線と呼び，様々な構成方法が提案されて，研究されている．Freeman らによる [18] は，そのような曲線構成法に関する 2010 年より前の結果の詳細なサーベイ論文であり，Costello による [11] は，ペアリング暗号に対する丁寧な入門を与えている．ここでは，ペアリングフレンドリ曲線の生成法に焦点を当てて説明する．特に，超特異曲線，MNT 曲線 [37]，BN 曲線 [2]，KSS-18 曲線 [29] に関して説明する.

次にパラメータ選択にとって重要な値 $\rho := \frac{\log p}{\log r}$ を定義する（但し，以下の MNT，BN，KSS 曲線など r, p が多項式表示 $r = r(x), p = p(x)$ される場合は，$\rho := \frac{\lim_{x\to\infty} \log p(x)}{\lim_{x\to\infty} \log r(x)} = \frac{\deg p(x)}{\deg r(x)}$ と定義する)．鍵，暗号文，署名などのデータは r ねじれ点 (即ち $E[r]$ の点) に関係するので，データサイズを小さくするために ρ 値は小さい方が望ましい．通常，得られる ρ は $1 \le \rho \le 2$ を満たし，$\rho \approx 1$ となる場合が最も望ましい.

また，Fig. 1 から入力サイズ $\log r$ の ECDL 問題と入力サイズ $k \log p = \log(p^k)$ の DL 問題の解読時間関数の違いから，安全性レベルに応じて最適なパラメータ選択をするためには，$\rho \cdot k = \frac{k \log p}{\log r}$ を変更する必要がある (Fig. 3)．通常使用されるパラメータでは，$(\log r, k \log p)$ は $(160, 1024)$ 又は $(256, 3072)$ で与えられる．異なる安全性レベルに対する $\rho \cdot k$ を得るために，異なる 楕円曲線生成法を使うのが望ましい（例えば，[12]）．式 (2.4) で定義された超特異楕円曲線は，$k = 2$ に固定されているので，安全性レベルに応じて $\rho \cdot k$ を変更するのに制限がある．よって，通常（ordinary）楕円曲線でペアリングフレンドリ曲線を生成する必要があり，それは CM（虚数乗法：Complex Multiplication）

法 [38] に基づき次の 2 ステップで生成される.

1. 固定した k に対して，素数位数 r と埋め込み次数 k を持つ楕円曲線 $E/\mathbb{F}_p$ が存在する p と r を見つける.
2. そのパラメータ (k,p,r) を実現する楕円曲線 E を CM 法に基づいて構成する.

Frobenius 写像のトレース t を $t := p+1-\sharp E(\mathbb{F}_p)$ で，CM 判別式 D を $D := 4p-t^2$ で定義する．平方因子を持たない $D>0$ に対し，CM 判別式 D を有する楕円曲線を Hilbert 類多項式 $H_D(X) := \prod_{i=1}^{h}(X-j(\tau_i))$ の法 p 還元の根 j を j-不変量とする楕円曲線として構成する．$H_D(X)$ の次数 $h := h_D$ がそれほど大きくない場合には CM 法計算（ステップ 2）は効率的に実行できる．計算実行時間は，$O(h_D^2) = O(D)$ であり，Sutherland [56] によれば，現在 CM 法で扱える上限は $h_D \approx 10^7, D \approx 10^{16}$ である.

上記曲線を生成するために，埋め込み次数 k (e.g., $2 \le k \le 50$) に対し，以下の条件を満たす $(k,t,p,r) \in \mathbb{Z}^4$ を探す必要がある.

ペアリングフレンドリ曲線の存在条件 埋め込み次数 k，Frobenius 写像のトレース t，有限体位数 p，巡回群素数位数 r に対して，

1. p,r は共に素数.
2. r は $p+1-t$ を割り切る.
3. r は $\Phi_k(p)$ (又は $\Phi_k(t-1)$) を割り切る，但し，Φ_k は k 次円分多項式.
4. ある十分小さい $D \in \mathbb{Z}$ と $f \in \mathbb{Z}$ に対し $4p-t^2 = Df^2$ が成立.

これらの条件を満たす曲線生成法は様々あるが，以下には，代表的な MNT,BN,KSS-18 曲線のパラメータ (k,t,p,r) を示す.

- **MNT 曲線:** MNT 曲線の (k,t,p,r) は以下の多項式で与えられる：

$$\begin{aligned} &k=3 \text{ に対して}, \quad t(x) = -1 \pm 6x, \quad p(x) = 12x^2 - 1, \\ &k=4 \text{ に対して}, \quad t(x) = -x, x+1 \quad p(x) = x^2 + x + 1, \\ &k=6 \text{ に対して}, \quad t(x) = 1 \pm 2x \quad p(x) = 4x^2 + 1, \end{aligned}$$

  かつ $r(x) = p(x) + 1 - t(x)$．あとは，x を動かして条件 1 と 4 を満たすものを探す．条件 4 を満足する場合は，それほど多くないことから MNT 曲線族は「疎な族」と呼ばれる.
- **BN 曲線:** BN 曲線の (k,t,p,r) と条件 4 の (f,D) は以下の多項式で与えられる：

$$\begin{aligned} p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1, \qquad f(x) = 6x^2 + 4x + 1, \end{aligned}$$

  かつ $k=12, D=3$．x を動かして条件 1 を満たすものを探す．条件 1 のみが探索条件で，豊富に得られるので「完全族」と呼ばれる．また，BN 曲線は $\rho = 1$ であ

り，$\rho \cdot k = 12$ なので，Fig. 3 から，128 ビットの安全性レベル曲線の選択に適する．

- **KSS-18 曲線:** KSS-18 (k,t,p,r) と条件 4 の (f,D) は以下の多項式で与えられる：

$$p(x) = (x^8+5x^7+7x^6+37x^5+188x^4+259x^3+343x^2+1763x+2401)/21,$$
$$r(x) = (x^6+37x^3+343)/343,$$
$$t(x) = (x^4+16x+7)/7, \quad f(x) = (5x^4+14x^3+94x+259)/21,$$

かつ $k = 18, D = 3$．BN 曲線同様の完全族に属する．$\rho = 4/3, \rho \cdot k = 24$ なので，Fig. 3 から，224 ビットの安全性レベル曲線の選択に適する．

3.2 BN, KSS 曲線の個数見積もり

BN, KSS 曲線は，$(p(x), r(x))$ が共に素数なら，ペアリングフレンドリ曲線になるので，その場合を数え上げることを考える．完全族といっても，実際に豊富にあるかどうかは自明でなく，その検証を行う必要がある．それに基づき豊富に好条件の曲線が得られる生成法を使うことで，高効率実装できる楕円曲線パラメータを生成することが可能になる．例えば，r や t を低ハミング重み にする (2 進展開中の 1 の個数を少なくする) ことで高速演算が実装できる．そのために，ペアリングフレンドリ曲線数の勘定は有用である．以下では，[7,39] に従い，Bateman-Horn 予想 [3] を用いる．十分大きい整数 y に対して，個数 $\sharp\{x \in \mathbb{Z}_{>0} \mid 1 \le x \le y, p(x), r(x) : \text{素数}\}$ は次の式でヒューリスティックに評価される[*1]：

$$Q(y) = \frac{C}{\deg p \cdot \deg r} \int_2^y \frac{1}{(\log x)^2} \mathrm{d}x \text{ ここで, } C = \prod_{q:\text{素数}} \left[\left(1-\frac{1}{q}\right)^{-2} \left(1-\frac{N_q}{q}\right) \right],$$

ここで，N_q は $p(x)r(x) \equiv 0 \bmod q$ の解の個数で与えられる．定数 C は Hardy-Littlewood (HL) 定数と呼ばれる．しかし，上記の無限積は収束が遅いため，より正確な数値を得るには，収束の速い無限積を与える Davenport-Schinzel の公式を用いる．D を $p(x) \cdot r(x)$ の判別式，K_p, K_r はそれぞれ $p(x), r(x)$ で定義される代数体とする．HL 定数は，

$$C = \frac{\xi(D)}{\sigma(K_p) \cdot \sigma(K_r)} \prod_{q \nmid D \text{ なる素数 } q} \left[\left(1-\frac{N_q}{q}\right) \left(1-\frac{1}{q}\right)^{-N_q} \prod_{j \ge 2} \left(1-\frac{1}{q^j}\right)^{-N_q^{(j)}} \right]$$

で与えられる．ここで，

$$\xi(D) = \prod_{q \mid D \text{ なる素数 } q} \left[\left(1-\frac{N_q}{q}\right) \prod_{j \ge 1} \left(1-\frac{1}{q^j}\right)^{-N_q^{p,(j)}-N_q^{r,(j)}} \right],$$

[*1] KSS 曲線に関しては，有理数係数 $(p(x), r(x))$ に適当な変数変換を施して整数係数化した多項式 $(p^+(x), r^+(x))$ に対して Bateman-Horn 予想を適用する必要があるが，ここでは，その点には深入りしない．[31] を参照されたい．

$\sigma(K)$ は代数体 K の Dedekind ゼータ関数の 1 での留数，$N_q^{(j)}$ は $p(x)r(x) \bmod q$ の j 次の既約因子の個数，$N_q = N_q^{(1)}$, $N_q^{p,(j)}$ は K_p での q の j 次素イデアル因子の個数，$N_q^{r,(j)}$ は K_r に対して同様に定義される値とする．

[7,39] では，BN 曲線に関して HL 定数を具体的に計算し個数見積もり値 Q を計算すると共に，小区間で BN 曲線を実際に数え上げた値との比較を行い，BH 予想に基づく曲線数数え上げの妥当性も検証している．我々は，数式処理ソフト MAGMA [6] を使って KSS 曲線の場合に個数見積もりの正しさを検証する課題に取り組んだ [57]．その正しさを検証すると共に，実用的に十分な個数の KSS 曲線が得られることを確かめた [31]．

4. 同種写像暗号の数理

4.1 同種写像グラフ

以下では，特に，超特異楕円曲線とその同種写像のなすグラフを扱い，[8] に従って同種写像暗号の数理を説明する．また，以下では，無向で正則な有限グラフのみを扱う．

p, ℓ を 2 つの素数として，$\mathbb{F}_{p^2}$ 上定義された超特異楕円曲線の ($\overline{\mathbb{F}}_p$-) 同型類全体を頂点集合 $\mathcal{V}(G)$，それら頂点間の ℓ-同種写像全体を辺集合 $\mathcal{E}(G)$ とする（無向な）$(\ell+1)$-正則グラフ $G = G(p,\ell)$ は，Pizer グラフと呼ばれて，エクスパンダーグラフ（特に，Ramanujan グラフ）という応用上良い性質をもつことが知られている．つまり，エクスパンダーグラフ上でのランダムウォークにより，少ない乱数性でグラフ頂点のほぼ一様なサンプリングを実現するので，暗号理論を含む計算機科学で様々な応用を有する [25]．以下では，[8] に従い，それを概観する．

エクスパンダーグラフの定義： $N := \sharp\mathcal{V}$ として，グラフ G が拡張率 $c > 0$ のエクスパンダーグラフであるとは，任意の $\sharp\mathcal{U} \le N/2$ となる部分集合 $\mathcal{U} \subset \mathcal{V}$ に対しその境界集合 $\Gamma(\mathcal{U}) := \{v \in \mathcal{V} \mid \exists u \in \mathcal{U}, \{u,v\} \in \mathcal{E}\} - \mathcal{U}$ のサイズは，$\sharp\Gamma(\mathcal{U}) \ge c \cdot \sharp\mathcal{U}$ を満たす．

エクスパンダーグラフ上で $O(\log(N))$ ステップのランダムウォークをさせると，その終点の分布はグラフ上の一様分布を良い精度で近似する．それは，以下の急撹拌性（rapid mixing property）によって保証される．

急撹拌性定理： X_i をランダムウォークが i 番目に到達する頂点とする．任意の $\delta > 0$ に対して，全ての頂点 $v \in \mathcal{V}$ に関して $\left|\Pr[X_i = v] - \frac{1}{N}\right| < \delta$ となるようなインデックス $i = O(\log(1/\delta))$ が存在する．

同種写像との関係では，以下の隣接行列固有値を用いた特徴付けが重要である：グラフ G の各頂点の次数を k として，$k > \mu_1 \ge \mu_2 \ge \cdots \ge \mu_{N-1}$ をその隣接行列固有値とすると，μ_1 と拡張率 c との間には，$c \ge \frac{2(k-\mu_1)}{3k-2\mu_1} =: f(\mu_1)$ が成り立つ．右辺の関数 $f(\mu_1)$ は，$\mu_1 < k$ の範囲で狭義単調減少なので，μ_1 が小さければ拡張率 c に対するより大きい下界が得られ，応用上，より望ましいエクスパンダーグラフが得られる．$\lambda(G) := \max(|\mu_1|, |\mu_{N-1}|)$ とする．Alon-Boppana は，$\sharp\mathcal{V}(G_m) \to \infty$ となる連結 k-正則グラフの族 $\{G_m\}$ に関して，

$\liminf_{m\to\infty}\lambda(G_m)\geq 2\sqrt{k-1}$ を示した．この事実は次の定義を動機づける．

Ramanujan グラフの定義 [33]： $\lambda(G)\leq 2\sqrt{k-1}$ となるグラフ G を Ramanujan グラフと呼ぶ．

実際に，2 つの異なる素数 p,ℓ に関し，Pizer グラフ $G(p,\ell)$ が Ramanujan グラフであることは，Eichler, Shimura によって証明された Ramanujan-Petersson 予想の特別な場合から導かれる．これで，$G(p,\ell)$ が暗号応用向きであることがわかった．

4.2 同種写像計算

楕円曲線 E とその上の位数 ℓ の巡回群 C を入力として，Vélu の公式 [58] は同種な曲線 E/C の定義式とそこへの同種写像 $E\ni(x,y)\mapsto(X,Y)\in E/C$ を具体的に与える．まず，$E: y^2=x^3+ax+b$ と C の点 $Q=(x_Q,y_Q)\neq O_E\in C$ に対して，$g_Q^x=3x_Q^2+a, g_Q^y=-2y_Q, t_Q=2g_Q^x$ if $Q\in E[2]$, $t_Q=g_Q^x$ if $Q\notin E[2]$, $u_Q=(g_Q^y)^2$. $S=(C-\{O_E\})/\pm 1$ として，$t=\sum_{Q\in S}t_Q, w=\sum_{Q\in S}(u_Q+x_Qt_Q), a'=a-5t, b'=b-7w$ とすれば，

$$E/C: Y^2=X^3+a'X+b',\quad X=x+\sum_{Q\in S}\left(\frac{t_Q}{x-x_Q}+\frac{u_Q}{(x-x_Q)^2}\right),$$

$$Y=y+\sum_{Q\in S}\left(\frac{2u_Qy}{x-x_Q}+\frac{t_Q(y-y_Q)-g_Q^xg_Q^y}{(x-x_Q)^2}\right) \tag{4.1}$$

と表わされる．Charles らは，Vélu の公式を使って，2-同種写像列を利用したハッシュ関数を構成した [8]．我々は，2-同種写像列を計算する時に更に効率的な演算法を提案し Charles らのハッシュ関数計算の改善を図った [60]．

4.3 同種写像を用いた耐量子計算機 DH 型鍵共有 [17]

2 つの小素数 ℓ_A,ℓ_B（例えば，$\ell_A=2,\ell_B=3$）に対して，$p+1=f\cdot\ell_A^{e_A}\ell_B^{e_B}$ となる大素数 p を選ぶ．有理点群が $E(\mathbb{F}_{p^2})\simeq(\mathbb{Z}/(p+1)\mathbb{Z})^2\supseteq(\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2\oplus(\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2$ となる $\mathbb{F}_{p^2}$ 上定義された超特異楕円曲線 E を選ぶ．次数が $\ell_A^{e_A},\ell_B^{e_B}$ の巡回群をそれぞれ核とする同種写像 ϕ,ψ を利用する．下の可換図式を Alice と Bob の間の DH 型鍵交換に利用する．

$$\begin{array}{ccc} E & \xrightarrow{\ \phi\ } & E_A:=E/\langle R_A\rangle \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi'} \\ E_B:=E/\langle R_B\rangle & \xrightarrow{\ \phi'\ } & E/\langle R_A,R_B\rangle \end{array}$$

但し，$\ker\phi=\langle R_A\rangle\subset E[\ell_A^{e_A}]$,
$\ker\psi=\langle R_B\rangle\subset E[\ell_B^{e_B}]$,
$\ker\phi'=\langle\psi(R_A)\rangle\subset E_B[\ell_A^{e_A}]$,
$\ker\psi'=\langle\phi(R_B)\rangle\subset E_A[\ell_B^{e_B}]$.

以下では，$E[\ell_A^{e_A}]=\langle P_A,Q_A\rangle, E[\ell_B^{e_B}]=\langle P_B,Q_B\rangle$ となる生成元 P_A,Q_A,P_B,Q_B を選び，超特異楕円曲線 $E/\mathbb{F}_p$ と共に公開パラメータとする．

耐量子計算機 DH 型鍵共有

Alice		**Bob**
$m_A, n_A \xleftarrow{\cup} (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^\times$:		$m_B, n_B \xleftarrow{\cup} (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^\times$:
Alice の秘密鍵,		Bob の秘密鍵,
$R_A := m_A P_A + n_A Q_A$,	$\xrightarrow{E_A, \phi(P_B), \phi(Q_B)}$	$R_B := m_B P_B + n_B Q_B$,
$\phi : E \to E_A := E/\langle R_A \rangle$,	$\xleftarrow{E_B, \psi(P_A), \psi(Q_A)}$	$\psi : E \to E_B := E/\langle R_B \rangle$,
$K_{\text{Alice}} :=$		$K_{\text{Bob}} :=$
$E_B/\langle m_A \psi(P_A) + n_A \psi(Q_A) \rangle$		$E_A/\langle m_B \phi(P_B) + n_B \phi(Q_B) \rangle$

ここで, $\langle m_A \psi(P_A) + n_A \psi(Q_A) \rangle = \langle \psi(R_A) \rangle = \ker \phi'$, $\langle m_B \phi(P_B) + n_B \phi(Q_B) \rangle = \langle \phi(R_B) \rangle = \ker \psi'$ であるので $K_{\text{Alice}} = E_B/\ker \phi' = E/\langle R_A, R_B \rangle = E_A/\ker \psi' = K_{\text{Bob}}$ となり, $K := K_{\text{Alice}} = K_{\text{Bob}}$ が共有鍵である. Alice の出力には E_A と共に $\phi(P_B), \phi(Q_B)$ も含まれているので, この耐量子計算機 DH 型鍵共有の安全性は, それらの補助入力を含む次の ISOG 型問題（式 (2.3)）と ISOG DH 型問題が, 量子計算機を用いても多項式時間で解けないという仮定に基づく.

超特異 ISOG 型問題 上記 DH 型鍵共有で定義された超特異楕円曲線とその上の点の入力 $(E, E_A, \phi(P_B), \phi(Q_B))$ に対し, $\langle m_A P_A + n_A Q_A \rangle$ の生成元 R_A を計算せよ.

超特異 ISOG DH 型問題 上記 DH 型鍵共有で定義された超特異楕円曲線とその上の点の入力 $(E, E_A, \phi(P_B), \phi(Q_B), E_B, \psi(P_A), \psi(Q_A))$ に対し, $E_{AB} := E/\langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B \rangle$ を計算せよ.

最後に, 2014 年に, Biasse らにより得られた結果を述べる [4]. それ以前は, 超特異楕円曲線に関する ISOG 問題を解く量子計算アルゴリズムの最良計算量は, $O(p^{1/2})$ であったが, 彼らは, Delfs らの結果 [14] に基づき, それを $O(p^{1/4})$ に改良したアルゴリズムを提案した.

5. 結語

本稿執筆中にも, Semaev による最新 ECDL 問題解法が, Cryptology ePrint Archive に挙がった [50]. 本稿では（主としては）扱わなかった標数 2 の拡大体 $\mathbb{F}_{2^k}$ 上の ECDL 問題に対するアルゴリズム提案だが, 拡大次数 $k > 310$ の場合に, 一般解法である Pollard ρ 法より少ない演算量で解けると見積もられている. その真偽・有効性の検証は, 今後の研究にゆだねられるが, 従来法は $k > 2000$ の場合に有効とされていたことからすると, 現実のパラメータ選択にも影響を与え得る興味深い内容である.

楕円曲線暗号研究は今も進展し続けており, 今後も, 応用数理研究者（数論アルゴリズム研究者, 暗号理論研究者など）の寄与が益々期待できる面白い研究分野である.

謝辞 本稿に関して貴重なコメントを頂きました平野貴人氏, Mehdi Tibouchi 氏, ならび

に匿名査読者の方々に深く感謝致します.

参考文献

[1] ANSI. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). *ANS*, X9.62-2005, November 2005.

[2] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *SAC 2006*, pages 319–331, 2006.

[3] P.T. Bateman and R.A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[4] J.F. Biasse, D. Jao, and A. Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *INDOCRYPT 2014*, pages 428–442, 2014.

[5] D. Boneh and M.K. Franklin. Identity-based encryption from the Weil pairing. In *CRYPTO 2001*, pages 213–229, 2001.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[7] J. Boxall. Heuristics on pairing-friendly elliptic curves. *J. Math. Crypt.*, 6(2):81–104, 2012.

[8] D.X. Charles, K.E. Lauter, and E.Z. Goren. Cryptographic hash functions from expander graphs. *J. Crypt.*, 22(1):93–113, 2009. Preliminary version: *IACR Cryptology eprint Archiv*, 2006:021, 2006.

[9] A.M. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Crypt.*, 8(1):1–29, 2014.

[10] H. Cohen and G. Frey, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[11] C. Costello. *Pairings for beginners*. a part of PhD thesis (*Fast Formulas for Computing Cryptographic Pairings,* Queensland Univ. of Tech.), 2012.

[12] C. Costello. Particularly friendly members of family trees. *IACR Cryptology ePrint Archive*, 2012:72, 2012.

[13] J.M. Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006:291, 2006.

[14] C. Delfs and S.D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbf{F}_p$. *Math. arXiv*, 1310:7789, 2013. To appear in Designs, Codes and Cryptography.

[15] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol, version 1.2.

RFC, 5246, August 2008.

[16] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[17] L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Crypt.*, 8(3):209–247, 2014.

[18] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *J. Crypt.*, 23(2):224–280, 2010.

[19] S.D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge Univ. Press, 2012.

[20] S.D. Galbraith, F. Hess, and F. Vercauteren. Aspects of pairing inversion. *IEEE Trans. Information Theory*, 54(12):5719–5728, 2008.

[21] S.D. Galbraith, X. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. *J. Crypt.*, 24(3):446–469, 2011.

[22] R.P. Gallant, R.J. Lambert, and S.A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *CRYPTO 2001*, pages 190–200, 2001.

[23] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS 2006*, pages 89–98, 2006.

[24] H. Hisil. *Elliptic Curves, Group Law, and Efficient Computation.* PhD thesis, Queensland Univ. of Tech., 2010.

[25] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their application. *Bulletin of AMS*, 43(4):439–561, 2006.

[26] D. Jao, S.D. Miller, and R. Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *ASIACRYPT 2005*, pages 21–40, 2005.

[27] A. Joux. A one round protocol for tripartite diffie-hellman. In *ANTS-IV*, pages 385–394, 2000.

[28] A. Joux, A. Odlyzko, and C. Pierrot. The past, evolving present and future of discrete logarithm. In *Open Problems in Mathematical and Computational Sciences*, pages 5–36, 2014.

[29] E.J. Kachisa, E.F. Schaefer, and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In *Pairing 2008*, pages 126–135, 2008.

[30] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *J. Crypt.*, 26(2):191–224, 2013. Preliminary version

appeared at EUROCRYPT 2008.

[31] Y. Kiyomura, N. Iwamoto, S. Yokoyama, K. Hayasaka, Y. Wang, T. Yasuda, K. Takashima, and T. Takagi. Heuristic counting of Kachisa-Shaefer-Scott curves. *JSIAM Letters*, 6:73–76, 2014.

[32] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[33] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica.*, 8(3):261–277, 1988.

[34] A. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Information Theory*, 39(5):1639–1646, 1993.

[35] V.S. Miller. Use of elliptic curves in cryptography. In *CRYPTO '85*, pages 417–426, 1985.

[36] V.S. Miller. The Weil pairing, and its efficient calculation. *J. Crypt.*, 17(4):235–261, 2004.

[37] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, E84-A(5):1234–1243, 2001.

[38] F. Morain. Building elliptic curves modulo large primes. In *EUROCRYPT '91*, pages 328–336, 1991.

[39] M. Naehrig. BN curves revisited. invited talk at the Mini-Workshop on Computational aspects of elliptic and hyperelliptic curves, K.U. Leuven, Belgium, October 2009.

[40] NIST. Digital Signature Standard (DSS). *FIPS-PUB*, 186-4, July 2013.

[41] 大岸聖史, 境隆一, 笠原正雄. 楕円曲線上の ID 鍵共有方式の基礎的考察. 電子情報通信学会 ISEC 研究会 *ISEC99-57*, ページ 37–42, 1999.

[42] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO 2010*, pages 191–208, 2010. Full version: *IACR Cryptology eprint Archiv*, 2010:563, 2010.

[43] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.

[44] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT 2005*, pages 457–473, 2005.

[45] T. Satoh and K. Araki. Fermat quotients and the polynomial time dicrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998.

[46] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 48:203–209, 1987.

[47] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie de Nombres Bordeaux*, 7:219–254, 1995.

[48] 清藤武暢, 四方順司. 公開鍵暗号を巡る新しい動き： RSA から楕円曲線暗号へ. 金融研究, 32(3), July 2013.

[49] I. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67:353–356, 1998.

[50] I. Semaev. New algorithm for the discrete logarithm problem on elliptic curves. *IACR Cryptology ePrint Archive*, 2015:310, 2015.

[51] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[52] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, 2nd edition, 2009.

[53] J.H. Silverman. The four faces of lifting for the elliptic curve discrete logarithm problem. In *11th Workshop on Elliptic Curve Cryptography, ECC 2007*, September, 2007.

[54] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Crypt.*, 12(3):193–196, 1999.

[55] B.A. Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves. *J. Crypt.*, 22(4):505–529, 2009.

[56] A. Sutherland. Accelerating the CM method. *LMS J. Comp. and Math.*, 15:171–204, 2012.

[57] K. Takashima, et al. Generating pairing-friendly elliptic curves (in cryptography). In *Study Group Workshop 2013, MI Lecture Note vol.52, Kyushu Univ*, pages 39–71, 2013.

[58] J. Vélu. Isogénies entre courbes elliptiques. *C.R. Acad. Sc. Paris, Séries A.*, 273:238–241, 1971.

[59] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press, 2nd edition, 2008.

[60] R. Yoshida and K. Takashima. Computing a sequence of 2-isogenies on supersingular elliptic curves. *IEICE Trans. Fundamentals*, 96-A(1):158–165, 2013.

高島 克幸 (正会員)　〒247-8501 神奈川県鎌倉市大船 5-1-1

1995 年京都大学大学院理学研究科修士課程修了. 1997 年三菱電機株式会社入社. 以後, 情報セキュリティ, 特に暗号の研究に従事. 2000 年度電子情報通信学会情報セキュリティ研究会 SCIS 論文賞, 2003 年度日本応用数理学会論文賞受賞. 博士（情報学）.

（2014年11月28日受付）
（2015年4月22日最終稿受付）