SCIS 2005 The 2005 Symposium on Cryptography and Information Security
Maiko Kobe, Japan, Jan.25-28, 2005
The Institute of Electronics, Information and Communication Engineers

Pairing を用いた Revocable DDH とその応用
Revocable DDH by using Pairing and It's Application

星野 文学* 鈴木 幸太郎 * 小林 鉄太郎 *
Fumitaka Hoshino Koutarou Suzuki Tetsutaro Kobayashi

あらまし DDH に関する witness を CDH に関する witness から分離できるような群の family である revocable DDH group を提案し, そのセキュリティについて考察する. またそのアプリケーションとして, 任意の暗号文の同一性検証が可能となる検証鍵を秘密鍵から分離出来る暗号系を提案する. また楕円曲線上の点のある同型写像の一方向性に着目し 非 trace-2 の non-supersingular 楕円曲線を用いて安全な revocable DDH group を構成する方法を提案する.

キーワード 楕円曲線, pairing, revocable DDH, non-supersingular curve, 射影

1 はじめに

近年暗号分野にて楕円曲線, とりわけ pairing を用いた暗号系が注目されている. 元々 [MOV93] 以来 pairing は暗号分野では楕円曲線暗号を攻撃する為の道具として研究されてきた. しかし [SOK00, Jou00] の先駆的な仕事に始まる pairing を暗号に用いる方法論が [BF01, BLS02, MSK02] 等の発表によって次第に脚光をあびるようになった.

これら従来の pairing を用いた暗号系は, pairing のもつある一方向性に基づいて構成されている. この pairing の一方向性は楕円曲線上の CDH 問題に強い関連を持っており, [JN01] で CDH 問題と DDH 問題の間にギャップを持つ楕円曲線の存在が指摘されて以来関心が集まっている.

一方 楕円曲線上の DDH 問題と強い関連を持つ, pairing 可能な楕円曲線上で定義されるある同型写像の一方向性については, 最近まであまり関心をもたれる事が無かった [SHUK03, SHUK04].

本論文では, この一方向性を持つ特殊なクラスの楕円曲線に於いて, DDH に関する witness が CDH に関する witness から分離可能であることに注目し, そのような群の family を revocable DDH group として抽象化する. また, そのセキュリティを定義し, アプリケーションとして, 任意の暗号文の同一性検証が可能となる検証鍵を, 秘密鍵から分離出来る暗号系を提案する. そして pairing 可能な楕円曲線を用いた revocable DDH group の構成方法, 安全性及び効率等に関して議論する.

* 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所, 神奈川県横須賀市光の丘 1-1, NTT Information Sharing Platform Laboratories, 1-1 Hikarinooka Yokosuka-Shi Kanagawa 239-0847 Japan

2 Revocable DDH Group

revocable DDH group とは DDH 仮定 と CDH 仮定の両方が仮定され, DDH に関する witness を CDH に関する witness から分離できるような群の事である. 形式的には, 有限巡回群の family G_k ($g_0 \in G_k$: 生成元, $k = \lceil \log_2 \#G_k \rceil$: セキュリティパラメタ) で, 次の 3 つの k に関する多項式時間アルゴリズムをもつものを revocable DDH group と呼ぶ.

[Revocable DDH Group]

(1) **【鍵生成】**
$\mathrm{KeyGen}(g_0, G_k) \rightarrow (g_1, w_{\mathrm{DDH}}, w_{\mathrm{CDH}})$:
$g_1 \in_U G_k,\ w_{\mathrm{DDH}} \in \{0,1\}^*,\ w_{\mathrm{CDH}} \in \{0,1\}^*$

(2) **【Revoke】**
$\mathrm{Revoke}(g_0, g_1, g_2, g_3, G_k, w_{\mathrm{DDH}}) \rightarrow (g_3 \stackrel{?}{=} g_2^a)$
但し $g_1 = g_0^a$.

(3) **【鍵交換】**
$\mathrm{KeyEx}(g_0, g_1, g_2, G_k, w_{\mathrm{DDH}}, w_{\mathrm{CDH}}) \rightarrow g_2^a$
但し $g_1 = g_0^a$.

どのような有限巡回群の family でも多項式時間群演算アルゴリズムを持つなら離散対数を使って鍵交換アルゴリズムを構成できる. 従って $w_{\mathrm{DDH}} = w_{\mathrm{CDH}} = a$ としておけば, revocable DDH group にはなる. しかしながら, これでは DDH に関する witness が CDH に関する witness から分離出来ているとは云えない. witness の分離を議論する為には安全性の定義を導入しなくてはならない. revocable DDH group の安全性は, (2)〜(3) から

witness を 1 つづつ削ると攻撃者 $\mathcal{A}$ は問題が解けないと云う事によって定義される. 誤解を恐れずに表現すると

【DDH 仮定】 $\mathcal{A}(g_0, g_1, g_2, g_3, G_k) \not\to (g_3 \stackrel{?}{=} g_2^a)$
【CDH 仮定】 $\mathcal{A}(g_0, g_1, g_2, G_k, w_{\text{DDH}}) \not\to g_2^a$.

これらの形式的な定義は以下の (4),(5) となる. 即ち安全な revocable DDH group とは次の 2 つの仮定を満たす G_k の事である.

[安全な Revocable DDH Group]

$\forall Q(X) \in \mathbb{Z}[X] \setminus \{0\},\ \exists k_0 \in \mathbb{N},\ \forall k \in \mathbb{N}\ :\ k \geq k_0,$

(4) **【DDH 仮定】** $\forall \mathcal{A}$: p.p.t.(k),

$$\left| \Pr \left[\begin{array}{l} b \in_U \{0,1\}, \\ (g_2, g_3) \in_U D_b, \\ \mathcal{A}(g_0, g_1, g_2, g_3, G_k) = b \end{array} \right] - \frac{1}{2} \right| < \frac{1}{|Q(k)|}$$

$\alpha, \beta \in \mathbb{Z}/\ell\mathbb{Z},\ (\ell = \#G_k)$ として,
$D_0 = \{g_0^\alpha, g_1^\beta \mid \alpha \neq \beta\},\ D_1 = \{g_0^\alpha, g_1^\beta \mid \alpha = \beta\}$

(5) **【CDH 仮定】** $\forall \mathcal{A}$: p.p.t.(k),

$$\Pr \left[\begin{array}{l} g_2 \in_U G_k, \\ \mathcal{A}(g_0, g_1, g_2, G_k, w_{\text{DDH}}) = g_2^a \end{array} \right] < \frac{1}{|Q(k)|}$$

但し $g_1 = g_0^a$.

3 アプリケーション

安全な revocable DDH group を用いて任意の暗号文の同一性検証が可能となるような検証鍵を秘密鍵から分離できる公開鍵暗号系を構成することが出来る.

鍵生成者から 検証鍵 w_{DDH} を受け取った者は 秘密鍵 w_{CDH} を知らなくとも, 2 つの暗号文に対応する平文が一致するかしないかを多項式時間で判定することが出来る. 暗号の構成法自体は ElGamal 暗号そのものである. 下記のように構成された暗号系は準同型性を持ち, さらに witness 無しの再暗号化が可能である.

【鍵生成】 y: 公開鍵, w_{CDH}: 秘密鍵, w_{DDH}: 検査鍵
$(y, w_{\text{DDH}}, w_{\text{CDH}}) \leftarrow \text{KeyGen}(g, G_k)$

【暗号化】 $M \in_U G_k$:平文, (T, Y):暗号文 として,
$\text{Enc}(M, y) \to (T, Y)$:
$(T, r_0, r_1) \leftarrow \text{KeyGen}(g, G_k)$
$Y \leftarrow M \times \text{KeyEx}(g, T, y, G_k, r_0, r_1)$

【復号】 $(T, Y) = \text{Enc}(M, y)$ として
$\text{Dec}(T, Y, w_{\text{DDH}}, w_{\text{CDH}}) \to M$:
$M \leftarrow Y/\text{KeyEx}(g, y, T, G_k, w_{\text{DDH}}, w_{\text{CDH}})$

【検査】 $(T_b, Y_b) = \text{Enc}(M_b, y)$: $b \in \{0,1\}$ として
$\text{Test}(T_0, Y_0, T_1, Y_1, w_{\text{DDH}}) \to M_0 \stackrel{?}{=} M_1$:
$(M_0 \stackrel{?}{=} M_1) \leftarrow \text{Revoke}(g, y, T_0/T_1, Y_0/Y_1, G_k, w_{\text{DDH}})$

4 Revocable DDH Group の構成

ここでは, 楕円曲線を用いて revocable DDH group の構成を行う. 特殊な楕円曲線を用いると bilinear group と呼ばれる以下の同型写像 e, ψ をもつ巡回群の組 G_1, G_2, G_3 を作れる事がよく知られている.

1. e は非退化双線形写像 $e : G_1 \times G_2 \to G_3$.
2. ψ は同型写像 $\psi : G_2 \to G_1$.

e を pairing と呼ぶ. G_2 の生成元を $\mathcal{G}_0 \in G_2$ とし, $g_0 = \psi(\mathcal{G}_0)$ とする. 実際に revocable DDH group として機能するのは G_1 だけであるが, 群を指定するパラメタ G_k を $G_k = (G_1, G_2, G_3, \mathcal{G}_0)$ とする. 以下に構成法を示す.

【鍵生成】
$\text{KeyGen}(g_0, G_k) \to (g_1, w_{\text{DDH}}, w_{\text{CDH}})$:
$x \in_U \mathbb{Z}/\ell\mathbb{Z},\ (\ell = \#G_1),$
$g_1 \leftarrow g_0^x,\ w_{\text{DDH}} \leftarrow \mathcal{G}_0^x,\ w_{\text{CDH}} \leftarrow x$

【Revoke】
$\text{Revoke}(g_0, g_1, g_2, g_3, G_k, w_{\text{DDH}})$
$\to e(g_3, \mathcal{G}_0) \stackrel{?}{=} e(g_2, w_{\text{DDH}})$

【鍵交換】
$\text{KeyEx}(g_0, g_1, g_2, G_k, w_{\text{DDH}}, w_{\text{CDH}}) \to g_2^{w_{\text{CDH}}}$

5 G_1, G_2, ψ の構成方法

ここでは G_1, G_2, ψ をどう構成するか [SHUK03] に従って簡単に解説する.

5.1 楕円曲線

$a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ とし

$$E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

を満たす点 $x, y \in \overline{\mathbb{F}}_q$ の集合に無限遠点と呼ばれる特別の元 $\mathcal{O}$ を付加したものを $\mathbb{F}_q$ 上定義された楕円曲線と呼び $E/\mathbb{F}_q$ と記述する. 楕円曲線が楕円加算と呼ばれる演算に関して群をなすこと及び楕円加算を用いて楕円スカラー倍と呼ばれる演算が定義出来ることが良く知られている.

$E/\mathbb{F}_q$ のうち $x, y \in \mathbb{F}_q$ なる元の集合に $\mathcal{O}$ を付加したものを $E/\mathbb{F}_q$ の $\mathbb{F}_q$ 有理点とよび $E(\mathbb{F}_q)$ と記述する. $x, y \in \mathbb{F}_{q^m}$ の場合も同様に $E(\mathbb{F}_{q^m})$ と記述する. 楕円加算に関して $E(\mathbb{F}_{q^m})$ は $E/\mathbb{F}_q$ の部分群で, $E(\mathbb{F}_q)$ は $E(\mathbb{F}_{q^m})$ の部分群である.

$E/\mathbb{F}_q$ の元 P のうち楕円スカラー倍 ℓP が $\ell P = \mathcal{O}$ を満たす元の集合を $E/\mathbb{F}_q$ の ℓ 等分点と呼び, $E[\ell]$ と記述する. $E[\ell]$ は $E/\mathbb{F}_q$ の部分群である. ℓ と q が互いに素なら

$$E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$$

であり, $E[\ell]$ は 楕円加算を加法とし, 楕円スカラー倍をスカラー倍とする $\mathbb{Z}/\ell\mathbb{Z}$ 上線形空間となる事が良く知られている.

$E(\mathbb{F}_q)$ に含まれ, かつ $E[\ell]$ に含まれる元の集合を $E(\mathbb{F}_q)[\ell]$ と記述し, $E(\mathbb{F}_{q^m})$ に含まれ, かつ $E[\ell]$ に含まれる元の集合を $E(\mathbb{F}_{q^m})[\ell]$ と記述する. $E(\mathbb{F}_{q^m})[\ell]$ は $E(\mathbb{F}_{q^m})$ の部分群であり $E(\mathbb{F}_q)[\ell]$ は $E(\mathbb{F}_q)$ の部分群である.

暗号で pairing を用いる場合, 次の 2 条件を同時に満たす曲線のうち, なるべく q や m の小さいものを選ぶのが都合が良い.

(A) $\#E(\mathbb{F}_q)[\ell] = \ell$ で, ℓ は $E(\mathbb{F}_q)[\ell]$ 上の離散対数が困難な程大きい.

(B) $\#E(\mathbb{F}_{q^m})[\ell] = \ell^2$ で, m は $\mathbb{F}_{q^m}^*$ 上の位数 ℓ の部分群上の離散対数が困難な程に大きい.

5.2 フロベニウス写像

$E/\mathbb{F}_q$ の任意の元 $P = (x, y)$ または $\mathcal{O}$ に対し q 乗フロベニウス写像 ϕ は

$$\phi P = \begin{cases} (x^q, y^q) & \text{if } P \neq \mathcal{O} \\ \mathcal{O} & \text{if } P = \mathcal{O} \end{cases}$$

と定義される. ϕ は楕円加算及び楕円スカラー倍と可換な $E[\ell]$ 上の自己準同型写像であり, 従って $\mathbb{Z}/\ell\mathbb{Z}$ 上線形空間 $E[\ell]$ 上の線形写像であり, その特性方程式が楕円曲線 $E/\mathbb{F}_q$ のトレース t を用いて

$$\phi^2 - t\phi + q = 0 \pmod{\ell}$$

と書けることが良く知られている.

ここで 線形写像 ϕ による $E[\ell]$ の固有空間分解を考える. 暗号で pairing を用いる時 便利なセッティング (A) の場合には $E(\mathbb{F}_q)$ 上に $E[\ell]$ の非自明な部分群が存在している. $E(\mathbb{F}_q)$ 上で ϕ が恒等写像である事を思い出すと $E(\mathbb{F}_q)[\ell]$ が ϕ の一つの固有空間であり, その固有値は $\lambda_1 = 1$ である. 従って特性方程式よりもう一つの固有値は $\lambda_2 = \lambda_1 \times \lambda_2 = q \bmod \ell$ である.

5.3 固有空間への射影

簡単の為 ℓ を素数として ϕ の固有値が縮退していない場合を考える. 従って $t = \lambda_1 + \lambda_2 \neq 2 \pmod{\ell}$ である. この時, 固有値 λ_2 に対応する固有空間が, $E[\ell] \setminus E(\mathbb{F}_q)[\ell]$ の中に存在する. その生成元を Q とし, $E(\mathbb{F}_q)[\ell]$ の生成元を P とする. 従って,

$$E[\ell] = \langle P \rangle \oplus \langle Q \rangle$$

である. $E[\ell]$ 上の任意の点 R は $\alpha, \beta \in \mathbb{Z}/\ell\mathbb{Z}$ として, 必ず. $R = \alpha P + \beta Q$ と書ける. $\alpha \neq 0$ かつ $\beta \neq 0$ の任意の R を生成元とする巡回群 $\langle R \rangle$ を考えると, ϕ を用いた固有空間への射影を使って $\langle R \rangle$ から $\langle P \rangle$ や $\langle Q \rangle$ への同型写像を構成することが出来る. 例えば射影

$$\psi = \frac{\phi - \lambda_2}{\lambda_1 - \lambda_2}$$

は $\langle R \rangle$ から $\langle P \rangle$ への同型写像である. 我々が ψ に求めるのは $\langle R \rangle$ から $\langle P \rangle$ への同型写像であるから $c \in \mathbb{Z}/\ell\mathbb{Z}$: $c \neq 0$ として

$$\psi = c(\phi - \lambda_2), \quad \text{または} \quad \psi = c\left(\sum_{i=0}^{m-1} \phi^i\right)$$

等を ψ の定義としても良い. これら $E[\ell]$ からフロベニウス写像の固有空間への準同型写像も射影と呼ぶ事とする. 射影を使って revocable DDH group を作るには G_1, G_2, ψ を例えば次のようにとれば良い.

$$G_1 = E(\mathbb{F}_q)[\ell], \;\; G_2 = \langle R \rangle, \;\; \psi = \phi - \lambda_2$$

G_2 を構成するための R は $E[\ell]$ 上の適当な点をランダムに選べば $(\ell - 1)^2/\ell^2$ の確率で見つかる. $E[\ell]$ 上の適当な点は $E(F_{q^m})$ 上の適当な点を $\#E(F_{q^m})/\ell^2$ 倍すれば見つかる. $E(F_{q^m})$ 上の適当な点は適当な $x \in \mathbb{F}_{q^m}$ に対して楕円の定義式を満たす $y \in F_{q^m}$ がおよそ $1/2$ の確率で見つかる. $E(\mathbb{F}_q)[\ell]$ の生成元は $\psi(R)$ で見つかる. こうして作られた G_1 と G_2 の pairing は退化しない. 従って pairing の演算が可能な楕円曲線を見つければ, revocable DDH group を作る事は簡単である.

6 安全性について

安全な revocable DDH group を構成する為には, 条件 (4), 条件 (5) が必要である. pairing 使って暗号系を構成出来るような楕円曲線では, 上記の G_1 上の CDH 仮定, 即ち条件 (5) は一般に信じられている.

しかしながら, G_1 上の DDH 仮定, 即ち 条件 (4) は必ずしも正しくない. supersingular および trace-2 の curve では, G_1 上の DDH 問題を多項式時間で解く次のようなアルゴリズムが知られている.

$$\mathcal{A}(g_0, g_1, g_2, g_3, G_k) \\ \rightarrow e(g_3, \psi^{-1}(g_0)) \stackrel{?}{=} e(g_2, \psi^{-1}(g_1))$$

ここで登場する ψ^{-1} は, distorsion map と呼ばれるフロベニウス写像の固有空間の間の同型写像であり, supersingular あるいは trace-2 の curve では多項式時間アルゴリズムが知られている [JN01, Ver01]. 一方 non-supersingular curve に於いて distorsion map が如何なる単一の有理写像によっても構成できない事が何度も発見されている [Wat69, Sch87, Ver01]. この事を傍証として, ψ が一方向とみなせる G_1, G_2, ψ を非 trace-2 の non-supersingular 楕円曲線を用いて構成する方法が [SHUK03, SHUK04] で提案されている (上記の方法).

我々の提案は 単に 従来の楕円曲線暗号が求めていた安全な curve に多項式時間の pairing を要件として追加するのみである. 従って, 我々の提案を実現できる楕円曲線が比較的豊富に存在する事, 及び もし条件 (4) への攻撃が見つかったなら, 楕円曲線暗号の DDH 仮定への

新たな攻撃に直結する事が期待できる. pairing が計算可能な non-supersingular curve を効率的に生成する方法については [MNT01, SB04, BaLS02, DEM02] 等で議論されている.

7 性能について

本論文の暗号系に近い機能を RSA 暗号と ElGamal 暗号の Double Encryption で実現することが出来る. 一般に 160 bit の楕円離散対数と 1024 bit の素因数分解が同程度の強度と考えられており, この強度で暗号系を設計すると, 暗号文サイズは Double Encryption では 2048 bit 本論文の方法では 320 bit となる. 一方, 本論文の方法は検査に pairing を 2 回必要とするので, Double Encryption が 1024 bit のべき乗 2 回で済むのに比べて幾分重い. 但し暗号の準同型性は RSA 暗号と ElGamal 暗号の Double Encryption では実現できない.

8 まとめ

本論文では DDH に関する witness が CDH に関する witness から分離可能であるような群の family を revocable DDH group として抽象化し, そのセキュリティを定義した. 安全な revocable DDH group を用いて, 任意の暗号文の同一性検証が可能となる検証鍵を秘密鍵から分離出来る暗号系を提案した. そして pairing を用いた revocable DDH group の構成方法を示し, その安全性と効率に関して考察した. より詳細な安全性解析, 他の応用等は今後の課題である.

参考文献

[MOV93] A.J.Menezes, T.Okamoto, S.A.Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. IT,39, pp.1639-1646, 1993

[SOK00] R. Sakai, K. Ohgishi, M. Kasahara, "Cryptosystems based on pairing," Proc. SCIS 2000

[Jou00] A.Joux, "A one round protocol for tripartite Diffie-Hellman," Proc. ANTS IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000

[BF01] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," Proc. CRYPTO' 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001

[BLS02] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Proc. ASIACRYPT'2001, LNCS 2248, pp.514-532, Springer-Verlag 2002,

[MSK02] S. Mitsunari, R. Sakai, M. Kasahara, "A New Traitor Tracing," Traitor Tracing, IEICE Trans. Fundamentals, vol. E85-A, No. 2, pp.481-484, 2002

[JN01] A.Joux and K.Nguyen ,"Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups," http://eprint.iacr.org/2001/003/

[SHUK03] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Candidate One-Way Functions on Non-Supersingular Elliptic Curves," Technical Report of IEICE. ISEC 2003-65 (2003-09)

[SHUK04] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems," IEICE Trans. Fundamentals, VOL.E87-A, NO.5, pp.1203-1205, May 2004

[Wat69] W.C.Waterhouse, "Abelian varieties over finite fields," Ann. Sci. Ecole Norm. Sup., Ser.2, no.4, pp.521-560, 1969

[Sch87] R.Schoof, "Nonsingular plane cubic curves over finite fields," J.Comb. Theory A, vol.46, pp.183-211, 1987

[Ver01] E.R.Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," Proc. Eurocrypt 2001, LNCS 2045, pp.195-210, Springer-Verlag 2001

[MNT01] A.Miyaji, M.Nakabayashi, S.Takano, "New explicit conditions of elliptic curve traces for FR-Reduction," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1234-1243, May 2001

[SB04] M.Scott, P.S.L.M.Barreto, "Generating more MNT elliptic curves," http://eprint.iacr.org/2004/058/

[BaLS02] P.S.L.M.Barreto, B.Lynn, M.Scott, "Constructing elliptic curves with prescribed embedding degrees," Proc. SCN'2002, LNCS 2576, pp.257-267, Springer-Verlag, 2003

[DEM02] R.Dupont, A.Enge, F.Morain, "Building curves with arbitrary small MOV degree over finite prime fields," http://eprint.iacr.org/2002/094/