SCIS 2015 The 32nd Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 20 - 23, 2015
The Institute of Electronics,
Information and Communication Engineers

Barreto-Naehrig 曲線に関して
On Barreto-Naehrig Curves

星野 文学 *
Fumitaka Hoshino

あらまし 最も代表的な pairing-friendly 楕円曲線の一つである Barreto-Naehrig 曲線における hash to point に関して考察し、高速化の検討を行なう.

キーワード Barreto-Naehrig 曲線, ペアリング, hash to point

1 はじめに

楕円曲線暗号において, 平文やハッシュ値といった任意の文字列をどのように楕円曲線上の点へ埋め込むかという問題について, 長い間関心が注がれていた. 例えば Koblitz の教科書 [10] の 163 ページには次のような記述がある.

> there is no polynomial time (in $\log p$) *deterministic* algorithm known for writing down a large number of points on an arbitrary elliptic curve E over $\mathbb{F}_q$.

この問題に関して, 近年幾つかの重要な進展があった. Boneh らは j 不変量 0 の超特異楕円曲線において, 3 乗根が定義体上で全単射と見なせる事実に基づき, `MapToPoint` と呼ばれる確定多項式時間アルゴリズムを提案している [2]. Icart はこの方法を拡張し, より広い楕円曲線のクラスへ適用した [8]. Sato らは円錐曲線上の点から j 不変量非零の楕円の定義体の 2 次拡大上の有理点を生成し, そのトレース写像により定義体上の有理点を生成する方法を提案した [12]. Skałba は定義体標数が 2 でも 3 でもない, j 不変量非零の楕円曲線において, 少なくとも 1 つは定義体上有理点となる 3 つの点の組を生成する方法を提案し [15], Shallue らはこの方法を改善した [14]. 最も重要な pairing-friendly 楕円曲線の一つである Barreto-Naehrig 曲線 (BN 曲線)[1] では上記の方法がいずれも適用できないと考えられ, 暫く open problem とされていたが, Tibouchi がそれが実現可能であることを指摘し [16], Fouque らによって厳密なアルゴリズムが与えられた [6].

* NTT セキュアプラットフォーム研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Secure Platform Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585 Japan

Fouque らの方法は BN 曲線における拡大体側の巡回群 (いわゆる G_2) においても, 些末な違いを除いて概ね適用可能であるが, 素体側の巡回群 (いわゆる G_1) の時と幾分状況が変わるので, その違いについて本論文で考察する.

2 準備

2.1 Barreto-Naehrig 曲線

BN 曲線は 2005 年に Barreto らによって提案された pairing friendly 曲線で, 代数閉体上では同型となる二つの楕円曲線

$$E/\mathbb{F}_p : \quad y^2 = x^3 + b$$
$$E'/\mathbb{F}_{p^2} : \quad y^2 = x^3 + b'$$

によって定義される. $n = \#E(\mathbb{F}_p), m = \#E'(\mathbb{F}_{p^2})/\#E(\mathbb{F}_p)$, と定義し $\Phi_n(x)$ を n 次の円分多項式とする. BN 曲線においては, ある媒介変数 $u \in \mathbb{Z}$ により

$$\begin{aligned} p &= 36u^4 + 36u^3 + 24u^2 + 6u + 1 \\ n &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \\ m &= 36u^4 + 36u^3 + 30u^2 + 6u + 1 \\ s &= \Phi_{12}(p)/n \end{aligned}$$

と定められる. p が素数となることは必須の要件であるが, 安全性や効率のため, これらの値が全て素数となるような u を選ぶのが望ましい. たとえば CertiVox 社の M-Pin なる認証系では

$$u = -4611686018490307249$$

なる 253 bit の BN 曲線が利用されているが, このとき上記の p, n, m, s は全て素数である [4]. BN 曲線を用いてペアリング

$$e : G_1 \times G_2 \to G_T$$

を定義するとき

$$\begin{aligned} G_1 &= E(\mathbb{F}_p)\ (= E(\mathbb{F}_p)[n]) \\ G_2 &= E'(\mathbb{F}_{p^2})[n] \\ G_T &= \mu_n\ (\subset \mathbb{F}_{p^{12}}) \end{aligned}$$

とするのが慣例となっているので, 本論文でもそのように G_1, G_2, G_T を定義する.

2.2 Fouque らの BN 曲線の符号化

(x_0, y_0) を $E(\mathbb{F}_q) \setminus \mathcal{O}$ 上の $x_0 y_0 \neq 0$ なる適当な点とし, ξ を 1 の原始 3 乗根とする. $t \in \mathbb{F}_q$ に対して,

$$\begin{aligned} x_1(t) &= \left(\frac{1+\xi t^2}{1+t^2}\right) \cdot \xi x_0, \\ x_2(t) &= \left(\frac{1+\xi^2 t^2}{1+t^2}\right) \cdot \xi^2 x_0, \\ x_3(t) &= \left(1 - \frac{y_0^2}{3x_0^3}\left(\frac{1+t^2}{t}\right)^2\right) \cdot x_0. \end{aligned}$$

のうち, 最低一つは $E(\mathbb{F}_q)$ 上の点の x 座標である [14]. $g(x) = x^3 + b$ とすると x_1, x_2, x_3 を使って概ね次のような符号化が提案されている [6].

名称: $F' : \mathbb{F}_q \to E(\mathbb{F}_q)$

入力: $t \in \mathbb{F}_q$

出力: $(x, y) \in E(\mathbb{F}_q)$

手続:

1. if $t = 0$ then $i = 1$,
   else if $1 + t^2 = 0$ then $i = 3$,
   else $i = \min j \in \{1, 2, 3\}$
   s.t. $\sqrt{g(x_j(t))} \in \mathbb{F}_q$.
2. return $\left(x_i(t),\ \chi(t)\sqrt{g(x_i(t))}\right)$.

但し $\chi : \mathbb{F}_q \to \{-1, 1\}$ は

$$\begin{aligned} &\forall t \in \mathbb{F}_q^\times,\ \chi(-t) = -\chi(t). \\ &\chi(0) = 1. \end{aligned}$$

を満たすとする. さらに概ね以下の標本アルゴリズムが提案されている [6].

名称: $I' : E(\mathbb{F}_q) \xrightarrow{\$} \mathbb{F}_q$

入力: $(x, y) \in E(\mathbb{F}_q)$

出力: $L \subset \mathbb{F}_q$

手続:

1. $L \leftarrow \emptyset$
2. t に関する方程式
   $$(x - \xi^2 x_0)t^2 + (x - \xi x_0) = 0$$
   が $\mathbb{F}_q$ 上に根を持つなら $y = \chi(t)\sqrt{g(x)}$ を満たす方の根を t_1 とし, $L \leftarrow L \cup \{t_1\}$ とする.
3. t に関する方程式
   $$(x - \xi x_0)t^2 + (x - \xi^2 x_0) = 0$$
   が $\mathbb{F}_q$ 上に根を持つなら $y = \chi(t)\sqrt{g(x)}$ を満たす方の根を t_2 とし, $\sqrt{g(x_1(t_2))} \notin \mathbb{F}_q$ ならば $L \leftarrow L \cup \{t_2\}$ とする.
4. t に関する方程式
   $$t^4 + \left(2 + \frac{3x_0^2(x - x_0)}{y_0^2}\right)t^2 + 1 = 0$$
   が, $\mathbb{F}_q$ 上に 4 つの根を持つなら $y = \chi(t)\sqrt{g(x)}$ を満たす 2 つの根を t_3, t_4 とし, $\mathbb{F}_q$ 上に 2 つの根を持つなら $y = \chi(t)\sqrt{g(x)}$ を満たす根を t_3 とする. t_3 が存在し, $\sqrt{g(x_1(t_3))} \notin \mathbb{F}_q$ かつ $\sqrt{g(x_2(t_3))} \notin \mathbb{F}_q$ ならば $L \leftarrow L \cup \{t_3\}$ とする. t_4 が存在し, $\sqrt{g(x_1(t_4))} \notin \mathbb{F}_q$ かつ $\sqrt{g(x_2(t_4))} \notin \mathbb{F}_q$ ならば $L \leftarrow L \cup \{t_4\}$ とする.
5. L を出力する.

2.3 強識別不可能性と許容符号化

ここでは [3] に従い, 強識別不可能性と許容符号化を紹介する. 強識別不可能性は Maurer ら によって導入された次のような概念である [11].

定義 1 暗号学的理想原始関数 h への神託照会が許されるチューリング機械 C に関し, C の理想原始関数 H への神託照会が許される実行時間 t_S の h の模倣器 S が存在し, どのような最大実行時間 t_D, 最大照会回数 q_D の識別器 D に対しても

$$\left|\Pr\left[D^{C^h, h} = 1\right] - \Pr\left[D^{H, S^H} = 1\right]\right| < \varepsilon$$

であるなら, C^h は H と $(t_D, t_S, q_D, \varepsilon)$-強識別不可能という. 安全変数 k に関して, 多項式限度の t_D, t_S, q_D に対して ε が無視可能関数であるなら C^h は H と強識別不可能という.

許容符号化とは次のような符号化の事である [3].

定義 2 S, R を有限集合とする. 次の 3 つの性質を満たす関数 $F : S \to R$ を ε-許容符号化という.

1. 計算可能性: F は確定多項式時間で計算可能

2. 正規性: S 上で一様に分布する確率変数 s に対して $F(s)$ が R 上の一様分布と ε-統計的識別不可能である.

3. 標本可能性: あらゆる $r \in R$ に対して効率的な乱択アルゴリズム I が存在し, $I(r)$ の分布が $F^{-1}(r)$ と ε-統計的識別不可能である.

次のような定理が知られている.

定理 1 ([3]) $h : \{0,1\}^* \to S$ がランダムオラクルであり, $F : S \to R$ が ε-許容符号化であるとする. t_I を I の最大実行時間とし, $t_S = 2q_D \cdot t_I$, $\varepsilon' = 4q_D\varepsilon$ とする. このとき $F(h(\cdot)) : \{0,1\}^* \to R$ はランダムオラクル $H : \{0,1\}^* \to R$ と $(t_D, t_S, q_D, \varepsilon')$-強識別不可能である.

Fouque らの F' には明らかな分布の偏りがある為, 上記の定理を用いランダムオラクル h を使って $F'(h(\cdot))$ を構成しても ε を安全変数の無視可能関数にする事が出来ない. 代わりに Fouque らは h_1, h_2 をランダムオラクルとして, 次のような符号化 $F : \{0,1\}^* \to E(\mathbb{F}_q)$ を提案した [5, 6].

$$F : x \mapsto F'(h_1(x)) + F'(h_2(x))$$

3 基本的なアイディア

G_1 上で Fouque らの関数を実装すると, ε が安全変数の無視可能関数となるような ε-許容符号化を実現する事が出来ないので, 上記のように関数を 2 回評価する必要があった. Fouque らの関数は $g(x) = x^3 + b'$ と読み替えて, 出力を n 等分点に潰せば G_2 にも適用可能であるが, G_2 においてはこの制約を回避出来る可能性がある. 即ち $F' : \mathbb{F}_{p^2} \to E'(\mathbb{F}_{p^2})$ が何らかの良い分布を持っていると仮定すると $E'(\mathbb{F}_{p^2})$ の元を $E'(\mathbb{F}_{p^2})[n]$ の元に潰す際に大数の法則に従うような分布の平均化が起こると考えられる.

$$F' : \mathbb{F}_{p^2} \to E'(\mathbb{F}_{p^2})$$

を Fouque らの関数とし, $N : E'(\mathbb{F}_{p^2}) \to \mathbb{N}$ を

$$N(P) = \#\{x | F'(x) = P, x \in \mathbb{F}_{p^2}\}$$

と定義する. $N(P)$ の $P \in E'(\mathbb{F}_{p^2})$ に関する平均値

$$\overline{N} = \frac{1}{\#E'(\mathbb{F}_{p^2})} \sum_{P \in \#E'(\mathbb{F}_{p^2})} N(P)$$

は

$$\overline{N} = \frac{\#\mathbb{F}_{p^2}}{\#E'(\mathbb{F}_{p^2})}$$

である. $N(P)$ の $P \in E'(\mathbb{F}_{p^2})$ に関する標準偏差 σ を

$$\sigma = \sqrt{\frac{1}{\#E'(\mathbb{F}_{p^2})} \sum_{P \in \#E'(\mathbb{F}_{p^2})} (N(P) - \overline{N})^2}$$

と定義する. F' による $\mathbb{F}_{p^2}$ から $E'(\mathbb{F}_{p^2})$ への写像は, 同じ点への重複が整定数 $d = 4$ で抑えられるので,

$$\sigma < d - \overline{N}$$

とすることができる. 今 $N(\cdot)$ の m 個の点に関する和 N' を

$$N'(P) = \sum_{Q \in \#E'(\mathbb{F}_{p^2})[m]} N(P + Q)$$

と定義する. そして, N' の $P \in E'(\mathbb{F}_{p^2})$ に関する分布が大数の法則を満たすと仮定する. 即ち N' の平均 $\overline{N'}$ および標準偏差 σ' は

$$\begin{aligned} \overline{N'} &= m \cdot \overline{N} \\ \sigma' &= \sqrt{m} \cdot \sigma \end{aligned}$$

を満たすと仮定する. $F : \mathbb{F}_{p^2} \to E'(\mathbb{F}_{p^2})[n]$ を

$$F : x \mapsto [m](F'(x))$$

と定義すると, $\mathbb{F}_{p^2}$ 上に一様分布する確率変数 x による $F(x)$ の分布と $E'(\mathbb{F}_{p^2})[n]$ 上の一様分布の統計距離

$$\Delta = \sum_{P \in E'(\mathbb{F}_{p^2})[n]} \left| \Pr_{x \in \mathbb{F}_{p^2}} [F(x) = P] - \frac{1}{n} \right|$$

は,

$$\Delta < \frac{(\#E'(\mathbb{F}_{p^2})[n])\sigma'}{\#\mathbb{F}_{p^2}} < \frac{n\sqrt{m}}{p^2} \left(d - \frac{p^2}{nm} \right)$$

が期待できる. 符号化関数 F の一様分布との統計距離がセキュリティパラメタの無視可能関数 $\sim 1/\sqrt{m}$ を使って抑えられる事が期待できる. さらに, 上記の仮定の下で次の乱択アルゴリズムにより標本可能性はクリア出来る.

入力: $R \in E'(\mathbb{F}_{p^2})[n]$

出力: $t \in \mathbb{F}_{p^2}$

手続:

1. $Q \xleftarrow{\$} E'(\mathbb{F}_{p^2})[m]$.
2. $P \leftarrow Q + R$.
3. $L \leftarrow I'(P)$.
4. $i \xleftarrow{\$} \{1, \ldots, d\}$.
5. $i \leq \#L$ なら $t \xleftarrow{\$} L$ を出力して終了.
6. 1 に戻る.

4 歪みフロベニウス写像を用いた符号化

F' を用いた G_2 上の符号化 $F : \mathbb{F}_{p^2} \to E'(\mathbb{F}_{p^2})[n]$ において, 上記では位数の余因子 m によるスカラー倍

$$F : x \mapsto [m](F'(x))$$

を用いた. この部分は歪みフロベニウス写像 [9] $\pi : E'(F_{p^2}) \to E'(F_{p^2})$

$$\pi : (x, y) \mapsto (v_1\overline{x}, v_2\overline{y})$$

(但し,$\overline{x}, \overline{y}$ はそれぞれ x, y の $\mathbb{F}_p$ 上共役元, v_1, v_2 はそれぞれ $\mathbb{F}_{p^2}$ 上の元) を用いて幾らか高速化できる. 例えば

$$F : x \mapsto [6u - \pi^3 + 3\pi^2 - \pi](F'(x))$$

など [13, 7].

参考文献

[1] P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In B. Preneel and S. E. Tavares, editors, *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2005.

[2] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[3] E. Brier, J. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. In T. Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 237–254. Springer, 2010.

[4] CertiVox UK Ltd. CertiVox M-Pin Client and Server Libraries. https://github.com/CertiVox/M-Pin-Python-RP-v0.2, 2013.

[5] R. R. Farashahi, P. Fouque, I. Shparlinski, M. Tibouchi, and J. F. Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Math. Comput.*, 82(281), 2013.

[6] P. Fouque and M. Tibouchi. Indifferentiable hashing to barreto-naehrig curves. In A. Hevia and G. Neven, editors, *Progress in Cryptology - LATINCRYPT 2012 - 2nd International Conference on Cryptology and Information Security in Latin America, Santiago, Chile, October 7-10, 2012. Proceedings*, volume 7533 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2012.

[7] L. Fuentes-Castañeda, E. Knapp, and F. Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In A. Miri and S. Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 412–430. Springer, 2011.

[8] T. Icart. How to hash into elliptic curves. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 303–316. Springer, 2009.

[9] T. Iijima, K. Matsuo, J. Chao, and S. Tsujii. Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication . SCIS 2002 The 2002 Symposium on Cryptography and Information Security, 10B-3, Shirahama,Japan, Jan. 29-Feb. 1, 2002.

[10] N. Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer, 1987.

[11] U. M. Maurer, R. Renner, and C. Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In M. Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[12] H. Sato and K. Hakuta. An efficient method of generating rational points on elliptic curves. *Journal of Math-for-Industry*, 1:33–44, 2009.

[13] M. Scott, N. Benger, M. Charlemagne, L. J. D. Perez, and E. J. Kachisa. Fast hashing to G_2 on pairing-friendly curves. In H. Shacham and B. Waters, editors, *Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings*, volume 5671 of *Lecture Notes in Computer Science*, pages 102–113. Springer, 2009.

[14] A. Shallue and C. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In F. Hess, S. Pauli, and M. E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 510–524. Springer, 2006.

[15] M. Skałba. Points on elliptic curves over finite fields. *Acta Arithmetica*, 117:293–301, 2005.

[16] M. Tibouchi. A Note on Hashing to BN Curves. SCIS 2012 The 2012 Symposium on Cryptography and Information Security, 1B2-1, Kanazawa, Japan, Jan. 30-Feb. 2, 2012.