SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

非対称ペアリングを利用した対称ペアリングの構成
Symmetric Pairing based on Asymmetric Pairing

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

あらまし 楕円曲線のペアリングを応用した ID ベース暗号の提案以来、数多くのペアリングを利用した暗号技術が提案されてきた。楕円曲線のペアリングには大きく分けて非対称ペアリングと対称ペアリングがある。近年、非対称ペアリングの典型的な例である BN 曲線上のペアリング高速実装技術の研究が進んだことと、対称ペアリングの典型的な例である超特異曲線上のペアリング向け曲線への攻撃研究が進んだことから、非対称ペアリングが主流となりつつある。一方、ペアリング利用技術の中には対称ペアリングを前提とした方式もある。このようなアルゴリズムのために、非対称ペアリングを用いて対称ペアリングを実現する研究が行われているが、従来はハッシュ値を楕円曲線上の点に変換する関数 (MapToPoint) を行うことができなかった。本稿は、非対称ペアリングを用いて対称ペアリングを実現する際に MapToPoint を行う方法を提案し、性能の評価を行う。

キーワード ペアリング, 楕円曲線暗号, ID ベース暗号, MapToPoint

1 はじめに

ID ベース暗号 [4] の発表以降、楕円曲線上のペアリング $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ は、様々な暗号技術に用いられている。ここで、 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ は位数 l の群とする。

ここで、$\mathbb{G}_1 = \mathbb{G}_2$ であるペアリングを対称ペアリング（またはタイプ I のペアリング）と呼び、$\mathbb{G}_1 \neq \mathbb{G}_2$ であるペアリングを非対称ペアリングと呼ぶ。非対称ペアリングの中で distortion map: $\mathbb{G}_1 \to \mathbb{G}_2$ または $\mathbb{G}_2 \to \mathbb{G}_1$ が効率よく演算できるものをタイプ II と呼び、そうでないものをタイプ III と呼ぶ。

タイプ I のペアリングは G_1 として超特異楕円曲線を用いた Tate ペアリングや η_T ペアリングなどがある。タイプ II のペアリングおよびタイプ III のペアリングには MNT 曲線 [2] や BN[3] 曲線を用いた Tate ペアリングや Ate ペアリング [5] がある。

近年、超特異楕円曲線に対する解読研究が進展したことと、BN 曲線を用いた R-ate ペアリング [6] や Optimal-ate ペアリング [8] の研究が進展した [11] ことなどから、今後はタイプ III ペアリングが主流となると考えられる。

一方、ペアリングを利用するアルゴリズムによって、対称ペアリングを前提とするものと、非対称ペアリングを前提とするものが存在する。タイプ III ペアリングで対称ペアリングを実現する方法については [1] において白勢が研究を行なっており、タイプ III のペアリングをタイプ I のペアリングに変換する一般的な方法の提案を行なっているが、ID などのハッシュ値を楕円曲線上の点に変換する MapToPoint 関数についての検討が行われていなかった。

本稿は、タイプ III ペアリングを用いて対称ペアリングを実現する方法で、MapToPoint 関数も実現出来る方法について考察する。

* NTT 情報流通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 Information Sharing Platform Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585, Japan. kobayashi.tetsutaro@lab.ntt.co.jp

2 準備

2.1 楕円曲線

$p \geq 5$ を素数, q を p のべきとする。有限体 $\mathbb{F}_p$ 上の楕円曲線

$$E : y^2 = x^3 + ax + b$$

に対して E の $\mathbb{F}_q$ 上の有理点の集合を $E(\mathbb{F}_q)$ とする。

2.2 ペアリング

l を素数とする。写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, (ただし $\mathbb{G}_1, \mathbb{G}_2$ は位数 l の加法群、 $\mathbb{G}_T$ は位数 l の乗法群) が、非退化な双線形写像であるとき、写像 e をペアリングという。$\mathbb{G}_1 = \mathbb{G}_2$ であるとき e を対称ペアリングといい、$\mathbb{G}_1 \neq \mathbb{G}_2$ であるとき e を非対称ペアリングという。楕円曲線上のペアリングの場合、MNT 曲線 [2] や BN 曲

線 [3] のような通常楕円曲線を用いる場合は、対称ペアリングを構成することはできなかった。

たとえば Ate ペアリング [5] では、以下のような群を用いる。

$$\begin{aligned}\mathbb{G}_1 &= E[l] \cup ker(\phi_p - [1]) \\ \mathbb{G}_2 &= E[l] \cup ker(\phi_p - [p]), \\ &\quad \text{ただし } \phi_p \text{ は } p \text{ 乗フロベニウス写像とする}\end{aligned}$$

本稿の中では $\mathbb{G}_1, \mathbb{G}_2$ は上記の定義とする。

2.3 MapToPoint

[4] などの ID ベース暗号では、「ID を楕円曲線上の点に変換する演算」が重要であり、 MapToPoint 関数と呼ぶ。

非対称ペアリングでは、群 $\mathbb{G}_1$ 上の点 P と、群 $\mathbb{G}_2$ 上の点 Q の 2 つから、有限体上の元 $f = e(P, Q)$ への写像を行う。ハッシュ値を群 $\mathbb{G}_1$ 上の点や群 $\mathbb{G}_2$ 上の点に変換することは容易に実現することができ、IEEE P1363 [9] などで標準化が進んでいる。

一方、超特異でない楕円曲線 E 上の位数 l の巡回群 $\mathbb{G}$ を与えられたときに、$\mathbb{G} \neq \mathbb{G}_1, \mathbb{G}_2$ であれば ID を $\mathbb{G}$ 上の点に変換することは困難であり、[1] の方式では MapToPoint を実現する方法は示されていなかった。

したがって、MapToPoint を用いない対称ペアリングを用いる暗号アルゴリズムは [1] の方式で非対称ペアリングを用いるアルゴリズムに変換することが出来るが、MapToPoint が必要な方式の場合はこの方式では変換できない、という問題が残っていた。本稿は、この点に関する解決策を検討する。

3 従来法

この章では非対称ペアリングを用いて対称ペアリングを行なう従来法である白勢方式を説明する。この方式を元に改良した方式を 4 章に示す。

3.1 白勢方式

[1] の方式では $G_1 \in \mathbb{G}_1, G_2 \in \mathbb{G}_2$ をそれぞれ生成元とし、$G_1 + G_2$ で生成される群 $\mathbb{G}$ を考える。$\mathbb{G}$ 上の元 P, Q に対して、それぞれ G_1 成分と G_2 成分を取りだし、写像 $e' : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ を $e'(P, Q) = e(Q \text{ の } \mathbb{G}_1 \text{ 成分}, P \text{ の } \mathbb{G}_2 \text{ 成分})$ と定義する。これによって、対称ペアリングを非対称ペアリングによって実現することができる。

4 提案法

4.1 方式 1

本来困難であった超特異でない楕円曲線 E 上の位数 l の巡回群 $\mathbb{G}$ を与えられたときに ID を $\mathbb{G}$ の元に変換する方法として、Waters Hash [10] と呼ばれる方法がある。

方式 1 は Waters Hash を利用して、本来困難であった超特異でない楕円曲線 E 上の位数 l の巡回群 $\mathbb{G}$ を与えられたときに、ID を $\mathbb{G}$ 上の点に変換する。これによって、従来の MapToPoint を行なうことを可能とする。

Waters Hash では、 まず $\mathbb{G}$ の生成元 G 以外にあらかじめ $n+1$ 個の $\mathbb{G}$ 上の元 $G_0, \ldots, G_n$ を用意しておき、ID の i ビット目の値 を I_i とする。このときに ID に対応する点 $P = G_0 + \sum_{i=1}^{n} I_i G_i$ とする方法である。この方法ならば、いかなる $\mathbb{G}$ に対しても ID を $\mathbb{G}$ 上の点に変換することができる。ただし、 $G_0, \ldots, G_n$ を作成したエンティティは Waters Hash の逆写像を求めることができるなどの問題点がある。

ここでは、逆写像を行なう問題を解決するため、m 人のディーラー $(T_1, \ldots, T_m)$ が協力して G_i を生成する方式を述べる。ディーラーのうち少なくとも 1 人はハッシュの逆写像を求めることに加担しない、正直なディーラーであることを仮定している。

- 以下を $i = 0$ から n まで繰り返す。
  1. T_j は 乱数 r_j を生成し、$G_{ij} = r_j G$ および、G_{ij} のビットコミットメント $\mathrm{BC}(G_{ij})$ を求める。
  2. 全ての T_j が $\mathrm{BC}(G_{ij})$ を提出した後に G_{ij} をオープンする。
  3. ビットコミットメントと G_{ij} のチェックを行った後に、$G_i = \sum_{j=1}^{m} G_{ij}$ を求める。
  4. $e(G, G_i) = e(G_i, G)$ のチェックを行うことで $G_i \in \mathbb{G}$ を確認する。

4.2 方式 2

方式 2 と方式 3 は、事前にディーラーが点を生成していない場合でも MapToPoint を行なう方法である。白勢方式に若干の変更を加える。

ID を $\mathbb{G}_1$ 上の点に変換する関数を Hash_1 、$\mathbb{G}_2$ 上の点に変換する関数を Hash_2 とする。

$\mathbb{G}$ を $\mathbb{G}_1 \times \mathbb{G}_2$ であらわし、ID_1 を $\mathbb{G}$ 上の点に変換する関数を $\mathrm{Hash}(\mathrm{ID}_1) = P = (\mathrm{Hash}_1(\mathrm{ID}_1), \mathrm{Hash}_2(\mathrm{ID}_1)) \in \mathbb{G}$ と定義し、$\mathrm{Hash}(\mathrm{ID}_1)$ を $\mathbb{G}$ の生成元とする。

ID_2 を $\mathbb{G}$ 上の点に変換する際は $\mathrm{Hash}(\mathrm{ID}_2)$ を $Q = (\mathrm{Hash}_1(\mathrm{ID}_2), —) \in \mathbb{G}$ とする。Q の $\mathbb{G}_1$ 成分のみを求めることはできるが、$\mathbb{G}_2$ 成分を求めることはできない。

	ペアリング演算量	$\mathbb{G}$ 上の元を表すデータ量
方式 1	c	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$
方式 2	c	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$
方式 3	$2c$	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$

表 1: 方式の比較

$e'(P,Q) = e(\mathrm{Hash}_1(\mathrm{ID}_2), \mathrm{Hash}_2(\mathrm{ID}_1))$ と定義することで非対称ペアリング e を用いて対称ペアリング e' を求めることが出来る。

方式 2 の問題点として、$\mathrm{ID}_1, \mathrm{ID}_2$ の 2 つの ID のみで構成される暗号アルゴリズムであれば対称ペアリングを行なうことができるが、3 つ以上の ID が存在する場合、2 つめの点と 3 つめの点の間でペアリングを行なうことができない。また、最初の ID のみが特別で $\mathbb{G}_2$ の成分を求めることができるので、2 つの ID がある場合にどちらが $\mathbb{G}$ の生成元となるかについて、アルファベット順などのルールをあらかじめ合意しておく必要がある。

4.3 方式 3

ID を $\mathbb{G}_1$ 上の点に変換する関数を Hash_1 、$\mathbb{G}_2$ 上の点に変換する関数を Hash_2 とする。

$\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2$ とし、ID_1 を $\mathbb{G}$ 上の点に変換する関数を $\mathrm{Hash}(\mathrm{ID}_1) = P = (\mathrm{Hash}_1(\mathrm{ID}_1), \mathrm{Hash}_2(\mathrm{ID}_1)) \in \mathbb{G}$ と定義する。

ID_2 を $\mathbb{G}$ 上の点に変換する際は $\mathrm{Hash}(\mathrm{ID}_2)$ を $Q = (\mathrm{Hash}_1(\mathrm{ID}_2), \mathrm{Hash}_2(\mathrm{ID}_2)) \in \mathbb{G}$ とする。

$e'(P,Q) = e(\mathrm{Hash}_1(\mathrm{ID}_2),\ \mathrm{Hash}_2(\mathrm{ID}_1))^2$
$e(\mathrm{Hash}_1(\mathrm{ID}_1),\ \mathrm{Hash}_2(ID_2))^2$ と定義することで形式的に非対称ペアリング e を用いて対称ペアリング e' を求めることが出来る。

方式 3 の問題点として、P と Q は実際には同じ巡回群上の元になっていないため、暗号アルゴリズムによっては適切でない場合がある。

5 評価

4 章で提案した方式 1〜3 に関して、演算効率およびデータ量の評価を表 1 に示す。ただし、 c は非対称ペアリング 1 回の演算量、$|\mathbb{G}_i|$ は群 $\mathbb{G}_i$ の元をあらわすのに必要なデータ量をあらわす。

方式 3 以外は演算量、データ量ともに同等である。各方式ともに適用するための前提条件が異なっているため、条件によって使い分ける必要がある。

6 結論

非対称ペアリングを用いて対称ペアリングを実現する方式において、ID を楕円曲線上の点に変換する関数 (MapToPoint) を行う演算の必要性および、具体的な方式を 3 つ提案した。これによって、MapToPoint が必要な対称ペアリングを前提とした暗号アルゴリズムを非対称ペアリングを用いるアルゴリズムに変換することができるようになった。

ただし、提案した 3 方式とも適用可能でないケースが存在し、この問題が完全に解決したとはいえない。今後、任意の暗号アルゴリズムに適用できる方式を研究する必要がある。

参考文献

[1] 白勢政明, “通常楕円曲線上の対称ペアリング”, CSS'10.

[2] A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FRreduction,” IEICE Transactions on Fundamentals, Vol.E84-A, No.5, pp.1234-1243, 2001.

[3] Paulo S. L. M. Barreto, Michael Naehrig, “Pairing-Friendly Elliptic Curves of Prime Order,” Selected Areas in Cryptography – SAC'2005, LNCS 3897, Springer-Verlag (2006), pp 319–331. Preliminary version: Cryptology ePrint Archive, Report 2005/133.

[4] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” SCIS 2000, pp. (2000)

[5] F. Hess, N. P. Smart, and F. Vercauteren, “The Eta pairing revisited,” IEEE Transactions on Information Theory, Vol. 52, pp.4595-4602, 2006.

[6] E. Lee, H. Lee, and C. Park, “Efficient and generalized pairing computation on abelien varieties,” IEEE Transactions of Information Theory, Vol.55, No.4, pp.1793-1803, 2009.

[7] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, “Integer variable c-based Ate pairing,” Pairing 2008, LNCS 5209, pp.178-191, 2008.

[8] F. Vercauteren, “Optimal pairings,” IEEE Transactions on Information Theory, Vol. 56, pp.455-461, 2010.

[9] IEEE P1363.3: Identity-Based Public Key Cryptography `http://grouper.ieee.org/groups/1363/IBC/`

[10] B. Waters. “Efficient Identity-Based Encryption Without Random Oracles,” Eurocrypt 2005, LNCS 3494, Springer-Verlag, 2005.

[11] T. Hayashi, N. Shinohara, L. Wang, S. Matsuo, M. Shirase, T. Takagi, "Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n})", PKC 2010, LNCS 6056, pp.351-367, 2010.