International Journal of Pure and Applied Mathematics
Volume 108 No. 4 2016, 801-807
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v108i4.6

ijpam.eu

SOME REMARKS ON A DISTANCE BETWEEN TWO ORDINARY ELLIPTIC CURVES OVER THE FINITE FIELD $\mathbb{F}_{2^5}$

Keisuke Hakuta

Interdisciplinary Graduate School of Science and Engineering
Shimane University
1060 Nishikawatsu-cho, Matsue-shi, Shimane 690-8504, JAPAN

Abstract: Rishivarman and Parthasarathy (2013) have constructed a map from the direct product of two copies of the set of ordinary elliptic curves with short Weierstrass equation over $\mathbb{F}_{2^5}$ to non-negative real numbers (plus infinity), and they have claimed that the map is a metric. In this paper we point out that the proof of the claim contains several flaws. Even worse, we shall show that the map is not a metric.

AMS Subject Classification: 14H52, 11G20
Key Words: elliptic curves, metric, isomorphism

1. Introduction

Elliptic curve cryptosystems (ECC for short) have been proposed independently by Miller [7] and Koblitz [5]. The most dominant operation in ECC is scalar multiplication (or point multiplication), which computes $[k]P \in E$ for a given integer k and a point $P \in E$, where E is an elliptic curve over a finite field. Scalar multiplication requires the secret information as an input. Side channel attacks are exploit (whole or partial) secret information that leaks from cryptographic modules. We need scalar multiplication algorithms to resist side channel attacks.

In order to resist side channel attacks on scalar multiplication, several au-

Received: January 27, 2016
Published: August 16, 2016

url: www.acadpubl.eu

thors have found an interesting property of the set of elliptic curves with short Weierstrass equation over a finite field. The interesting property is that one can induce metrics on the set of elliptic curves with short Weierstrass equation over a prime field of characteristic greater than three. The property has been firstly found by Mishra and Gupta [8]. Thereafter, Vetro [11] has proposed some other metrics on the set of elliptic curves with short Weierstrass equation over a prime field of of characteristic greater than three. Recently, Hakuta [1] has proposed metrics on the set of ordinary elliptic curves with short Weierstrass equation over any finite field of characteristic two. In [8] and [11], the authors have proposed potential applications of the metrics to the protection of side channel attacks (especially, fixed table attack [3]). A similar method to protect cryptographic modules against side channel attacks has also been proposed by Joye and Tymen [4].

In our knowledge, the method [1] is the first systematic approach to construct metrics on the set of ordinary elliptic curves with short Weierstrass equation over any finite field of characteristic two. However, this method seems not to be suitable for protection against side-channel attacks such as [8] and [11]. On the other hand, Rishivarman and Parthasarathy [9] have constructed a map from the direct product of two copies of the set of ordinary elliptic curves with short Weierstrass equation over $\mathbb{F}_{2^5}$ to non-negative real numbers (plus infinity), and they have claimed that the map is a metric. In addition, they have claimed that the map can be used to resist side channel attacks on scalar multiplication same as [8] and [11].

In this paper we point out that the proof of the claim contains several flaws. Even worse, we shall show that the map is not a metric. The rest of this paper is organized as follows. In Section 2, we collect the basic background on elliptic curves which will be necessary for our investigations. In Section 3, we briefly review the map proposed by Rishivarman and Parthasarathy in [9]. Section 4 gives some remarks on the map proposed by Rishivarman and Parthasarathy in [9]. Section 5 concludes the paper.

2. Preliminaries

This section provides the basic background on elliptic curves which will be necessary for our investigations. Further details can be seen in [2, Section 3.5], [6, Chapter 3], and [10, Appendix A].

Let K be a field and $p = \mathrm{char}(K)$ the characteristic of K. We denoted the set of rational integers, the set of real numbers, and a finite field with q

elements, by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{F}_q$, respectively, where $q = p^m$ $(m \geq 1)$, $p = \mathrm{char}(\mathbb{F}_q)$. We denote by $\sharp S$ the cardinality of a finite set S. For a group $(\mathbb{G}, \circ)$, the order of $a \in \mathbb{G}$ is denoted by $\mathrm{ord}_{\mathbb{G}}(a)$.

Let $E/K : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ be an elliptic curve over K. Two elliptic curves E_1 and E_2 are called isomorphic if there exist morphisms (as algebraic varieties) from E_1 to E_2 and from E_2 to E_1 which are inverses of each other. More precisely, two elliptic curves E_1/K and E_2/K given by the equations

$$\begin{aligned} E_1 : y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6, \\ E_2 : y^2 + \bar{a}_1xy + \bar{a}_3y &= x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \end{aligned}$$

are isomorphic over K (or K-isomorphic), denoted by $E_1/K \cong E_2/K$, if and only if there exist $u \in K^*$ and $r, s, t \in K$ such that the change of variables

$$(x, y) \longmapsto (u^2x + r, u^3y + u^2sx + t)$$

transforms equation E_1 to equation E_2. The relationship of isomorphism is an equivalence relation.

An elliptic curve E/K $(p = \mathrm{char}(K))$ is called *supersingular* if $E[p] = \{ \mathcal{O} \}$, and the curve E/K is called *ordinary* (or *non-supersingular*) if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. It is well-known that if $K = \mathbb{F}_q$ and $p = 2$ or $p = 3$, then E is supersingular if and only if $j(E) = 0$. In other words, if $p = 2$ or $p = 3$, E is ordinary if and only if $j(E) \neq 0$. Remark that if $E/K : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$ is an elliptic curve with $\mathrm{char}(K) = 2$ and $j(E) \neq 0$, then the admissible change of variables

$$(x, y) \longmapsto \left(\bar{a}_1^2x + \frac{\bar{a}_3}{\bar{a}_1}, \bar{a}_1^3y + \frac{\bar{a}_1^2\bar{a}_4 + \bar{a}_3^2}{\bar{a}_1^3} \right) \tag{2.1}$$

transforms E to the ordinary elliptic curve

$$E'/K : y^2 + xy = x^3 + a_2x^2 + a_6. \tag{2.2}$$

Equation (2.2) is called *short Weierstrass equation*. Let $E_1/\mathbb{F}_{2^m}, E_2/\mathbb{F}_{2^m}$

$$\begin{aligned} E_1 : y^2 + xy &= x^3 + a_2x^2 + a_6 \quad (a_6 \neq 0), \\ E_2 : y^2 + xy &= x^3 + \bar{a}_2x^2 + \bar{a}_6 \quad (\bar{a}_6 \neq 0) \end{aligned}$$

be ordinary elliptic curves with short Weierstrass equation (2.2) over $\mathbb{F}_{2^m}$. If $E_1/\mathbb{F}_{2^m} \cong E_2/\mathbb{F}_{2^m}$, then we have $a_6 = \bar{a}_6$ and the isomorphism is given by

$$\phi_s : E_1 \longrightarrow E_2, \quad (x, y) \longmapsto (x, y + sx), \tag{2.3}$$

where s is an element in $\mathbb{F}_{2^m}$ and satisfies the equation

$$s^2 + s = a_2 + \bar{a}_2 \tag{2.4}$$

(See [6, Section 3.3]).

Remark that if s_1 is a solution of Equation (2.4) then $s_2 := s_1 + 1$ is the other solution. Furthermore, ϕ_s is an automorphism if and only if $s \in \{0, 1\}$ ([10, Appendix A, Proposition 1.2]).

3. A Map Proposed by Rishivarman and Parthasarathy

Here we briefly review a map from the direct product of two copies of the set of ordinary elliptic curves with short Weierstrass equations over $\mathbb{F}_{2^5}$ to non-negative real numbers (plus infinity) proposed by Rishivarman and Parthasarathy in [9]. Let X be an indeterminate over the finite field $\mathbb{F}_2$. Since the polynomial $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ is irreducible, the finite field $\mathbb{F}_{2^5}$ can be seen as the quotient ring $\mathbb{F}_2[X]/(X^5 + X^2 + 1)$ over the ideal $(X^5 + X^2 + 1) \subsetneq \mathbb{F}_2[X]$ generated by $X^5 + X^2 + 1$. Let g be a generator of the multiplicative group $\mathbb{F}_{2^5}^*$. Let $\mathcal{E}$ be the set of ordinary elliptic curves with short Weierstrass equations over $\mathbb{F}_{2^5}$.

The map $d_g : \mathcal{E} \times \mathcal{E} \to \mathbb{R} \cup \{ \infty \}$ which depends on the choice of the generator $g \in \mathbb{F}_{2^5}^*$, is constructed as follows. Put

$$\mathcal{R}' := \{ -2^4/2 + 1, -2^4/2 + 2, \ldots, -1, 0, 1, \ldots, 2^4/2 \}. \tag{3.1}$$

According to [9], it satisfies that

$$\mathbb{F}_{2^5}^* = \langle g \rangle = \left\{ g^k \;\middle|\; 0 \le k \le 2^4 \right\} = \left\{ g^k \;\middle|\; k \in \mathcal{R}' \right\}. \tag{3.2}$$

From Equation (3.2), the set $\mathcal{R}'$ is called a standard index set of a generator g. Let $E_i : y^2 + xy = x^3 + a_i x^2 + b_i \in \mathcal{E}$ for $i = 1, 2$. In [9], two elliptic curve E_1 and E_2 are called isomorphic if there exist a $t \in \mathbb{F}_{2^5}$ such that

$$a_2 = t^4 a_1 \tag{3.3}$$

and

$$b_2 = t^6 b_1. \tag{3.4}$$

The map $d_g : \mathcal{E} \times \mathcal{E} \to \mathbb{R} \cup \{ \infty \}$ proposed in [9] is defined as follows:

$$\begin{array}{rccc} d_g : & \mathcal{E} \times \mathcal{E} & \to & \mathbb{R} \cup \{ \infty \} \\ & \cup & & \cup \\ & (E_1, E_2) & \mapsto & |r| \qquad E_1 \overset{\phi_t}{\cong} E_2, \\ & (E_1, E_2) & \mapsto & \infty \qquad \text{otherwise}, \end{array}$$

where $\phi_t : E_1 \to E_2$, $(x, y) \mapsto (t^2x, t^3y)$ is an $\mathbb{F}_{2^5}$-isomorphism and $t = g^r$ for some $r \in \mathcal{R}'$.

4. Remarks on the Map d_g

In this section, we shall point out that there are three errors in Section 3. The first one is that Equation (3.2) is incorrect.

Claim 1. It does not hold Equation (3.2). Namely, we have

$$\mathbb{F}_{2^5}^* \neq \left\{ g^k \;\middle|\; 0 \leq k \leq 2^4 \right\} \tag{4.1}$$

and

$$\mathbb{F}_{2^5}^* \neq \left\{ g^k \;\middle|\; k \in \mathcal{R}' \right\} \tag{4.2}$$

for

$$\begin{aligned} \mathcal{R}' &= \{ -2^4/2 + 1, -2^4/2 + 2, \ldots, -1, 0, 1, \ldots, 2^4/2 \} \\ &= \{ -7, -6, \ldots, -1, 0, 1, \ldots, 8 \} = \{ 0, \pm 1, \ldots, \pm 7, 8 \}. \end{aligned}$$

Let $\mathcal{R} := \{ 0, \pm 1, \pm 2, \ldots, \pm 15 \}$. Then we have

$$\begin{aligned} \mathbb{F}_{2^5}^* &= \left\{ g^k \;\middle|\; 0 \leq k \leq 2^5 - 2 \right\} \\ &= \left\{ g^k \;\middle|\; 0 \leq k \leq 30 \right\} \\ &= \left\{ g^k \;\middle|\; k \in \mathcal{R} \right\}. \end{aligned} \tag{4.3}$$

From now on, we use Equation (4.3) instead of Equation (3.2), in order to remove the flaw (Claim 1).

The second one (resp. the third one) is that Equation (3.3) (resp. Equation (3.4)) is incorrect.

Claim 2. An $\mathbb{F}_{2^5}$-isomorphism is given by the form (2.3). Equation (3.3) and Equation (3.4) do not give any $\mathbb{F}_{2^5}$-isomorphism.

Finally, we consider whether or not d_g is a map from $\mathcal{E} \times \mathcal{E}$ to non-negative reals (plus infinity) or not. We can see that d_g is indeed not a map.

Main Claim. d_g is not a map. Namely, d_g is not a metric.

Proof. The latter part follows immediately from the former part. We show the former part by proving that d_g is not defined over $\mathcal{E} \times \mathcal{E}$. Let $E_i : y^2 + xy = x^3 + a_i x^2 + b_i \in \mathcal{E}$ for $i = 1, 2$. Suppose that $E_1 \cong E_2$ for some $\mathbb{F}_{2^5}$-isomorphism of form (2.3). Since $d_g(E_1, E_2)$ is defined using Equation (3.3) and Equation (3.4), there must exists $t \in \mathbb{F}_{2^5}$ such that $a_2 = t^4 a_1$ and $b_2 = t^6 b_1$. On the other hand, by $E_1 \cong E_2$, there exists $s \in \mathbb{F}_{2^5}$ satisfying Equation (2.3). Thus there must exist $s, t \in \mathbb{F}_{2^5}$ satisfying the following simultaneous equations:

$$\begin{cases} s^2 + s = a_1 + a_2 & (4.4) \\ b_1 = b_2 & (4.5) \\ a_2 = t^4 a_1 & (4.6) \\ b_2 = t^6 b_1. & (4.7) \end{cases}$$

Let us show that there do not exist $s, t \in \mathbb{F}_{2^5}$ satisfying Equation (4.4)–(4.7). Since we have

$$\alpha^{2^5 - 1} = \alpha^{31} = 1 \tag{4.8}$$

for any $\alpha \in \mathbb{F}_{2^5}^*$ and the number 31 is prime, it holds

$$\mathrm{ord}_{\mathbb{F}_{2^5}^*}(\alpha) = 1 \tag{4.9}$$

or

$$\mathrm{ord}_{\mathbb{F}_{2^5}^*}(\alpha) = 31. \tag{4.10}$$

Substituting Equation (4.7) for Equation (4.5) yields $t^6 = 1$. It follows that $\mathrm{ord}_{\mathbb{F}_{2^5}^*}(t)$ divides 6. By Equation (4.9) and Equation (4.10), the order of t is one ($\mathrm{ord}_{\mathbb{F}_{2^5}^*}(t) = 1$), namely, $t = 1$. By substituting Equation (4.6) for $t = 1$, we have $a_2 = a_1$. Finally, from $a_2 = a_1$ and Equation (4.4), we obtain $s(s+1) = 0$. Therefore, $s = 0$ or $s = 1$. This shows that $E_1 = E_2$. Hence, if $E_1 \neq E_2$ and $E_1 \cong E_2$, d_g is not defined. Thus d_g is not a map from $\mathcal{E} \times \mathcal{E}$ to $\mathbb{R} \cup \{ \infty \}$. □

5. Conclusion

In this paper, we have given some remarks on the map proposed by Rishivarman and Parthasarathy in 2013. More precisely, we have pointed out that it is indeed not a map, and thus not a metric. Our results show that the map proposed by Rishivarman and Parthasarathy can not be used to resist side channel attacks on scalar multiplication. Our results also show that no analogous result of the metric proposed by Mishra and Gupta which can be used to resist side channel attacks on scalar multiplication, is known in the characteristic two case.

Acknowledgements

This work was partially supported by a grant for young researchers from Shimane University in 2015.

References

[1] K. Hakuta, Metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two, *Internat. J. Math. Math. Sci.*, **2015**, Article ID 597849 (2015), 597849:1–597849:5.

[2] D. Husemöller, *Elliptic Curves*, second edition, Springer-Verlag, USA (2004).

[3] T. Izu, B. Möller, and T. Takagi, Improved elliptic curve multiplication methods resistant against side channel attacks, In: *Progress in Cryptology – INDOCRYPT 2002*, LNCS **2551** (2002), 296–313.

[4] M. Joye and C. Tymen, Protections against differential analysis for elliptic curve cryptography: An algebraic approach, In: *Cryptographic Hardware and Embedded Systems – CHES 2001*, LNCS **2162** (2001), 377–390.

[5] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, **48**, No. 177 (1987), 203–209.

[6] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, USA (1993).

[7] V. Miller, Uses of elliptic curves in cryptography, In: *Advances in Cryptology – CRYPTO '85*, LNCS **218** (1986), 417–426.

[8] P.K. Mishra and K.C. Gupta, A metric on the set of elliptic curves over $\mathbb{F}_p$, *Appl. Math. Lett.*, **21**, No. 12 (2008), 1330–1332.

[9] A.R. Rishivarman and B. Parthasarathy, An elliptic curve metric on the fundamental group over $GF(2^5)$, *Int. J. Pure Appl. Math.*, **89**, No. 4 (2013), 547–552.

[10] J.H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Springer-Verlag, USA (2009).

[11] F. Vetro, Metrics on the set of elliptic curves over $\mathbb{F}_p$, *Int. J. of Contemporary Math. Sciences*, **1**, No. 1 (2011), 22–24.