Skew Frobenius Map on Binary Edwards Curves

Ahmed Youssef Ould Cheikh¹ & Demba Sow¹

¹ Ecole Doctorale de Mathématiques et Informatique, Laboratoire d'Algèbre de Cryptologie de Géométrie Algèbrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal

Correspondence: Ahmed Youssef Ould Cheikh, Ecole Doctorale de Mathématiques et Informatique, Laboratoire d'Algèbre de Cryptologie de Géométrie Algèbrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal. E-mail: youssef@ucad.sn

Received: November 27, 2013	Accepted: December 19, 2013	Online Published: February 20, 2014
doi:10.5539/jmr.v6n1p93	URL: http://dx.doi.org/10.5539/jmr.v6n1p93	

Abstract

This paper introduces the Frobenius endomorphism on the the binary Edwards elliptic curves proposed by Bernstein, Lange and Farashahi in 2008 and by Diao and Lubicz (2010). To speed up the scalar multiplication on binary Edwards curves, we use the GLV method combined with the Frobenius endomorphism over the curve.

Keywords: Frobenius endomorphism, elliptic curves, binary Edwards Curves, scalar multiplication

1. Introduction

In 2007, H. Edwards introduced a new elliptic curve model. This model, called Edwards curves later, gain more interest and is widely investigated during the last six years. The binary version of the curve were proposed by Bernstein et al. (2008) and by Diao et al. (2010).

In this paper, we defined and study the Frobenius endomorphism over the Edwards elliptic curves model on a field of characteristic 2. It's well known that such an endomorphism can be used to derive fast algorithm to perform scalar multiplication over elliptic curves.

In the next section, we recall some basic notions on Edwards curves and Frobenius endomorphism. We also give the expression of the group law and the birational equivalence between elliptic curves in Edwards model and elliptic curves in Weierstrass model when considering a finite field of characteristic 2.

In section 2, we introduce the Frobenius endormphism for Edwards models cited above.

2. Preliminaries

This section recall some definitions and notations related to Edwards elliptic curve in characteristic 2.

2.1 Binary Edwards Curves

2.1.1 Binary Edwards Curves of Bernstein and Lange (2008)

Edwards curves was introduced by Harold Edwards in 2007. Bernstein and Lange generalize this work to twisted Edwards curve in (Bernstein & Lange, 2008). In 2008, they introduce the binary version of Edwards curves in (Bernstein et al., 2008). In the following we recall the main results for binary Edwards curves.

Definition 2.1 (Binary Edwards curve) Consider a finite field *K*, with $\#K = 2^n$ ($n \ge 1$) and let $d_1, d_2 \in K$ such that $d_1 \ne 0$ and $d_2 \ne d_1^2 + d_1$. The Edwards model in *K* with elements d_1 and d_2 is given by the affine equation

$$E_{B,d1,d2}: d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points of E_{B,d_1,d_2} , then $P_1 + P_2 = P_3 = (x_3, y_3)$, where

$$x_{3} = \frac{d_{1}(x_{1} + x_{2}) + d_{2}(x_{1} + y_{1})(x_{2} + y_{2}) + (x_{1} + x_{1}^{2})(x_{2}(y_{1} + y_{2} + 1) + y_{1}y_{2})}{d_{1} + (x_{1} + x_{1}^{2})(x_{2} + y_{2})}$$
$$y_{3} = \frac{d_{1}(y_{1} + y_{2}) + d_{2}(x_{1} + y_{1})(x_{2} + y_{2}) + (y_{1} + y_{1}^{2})(y_{2}(x_{1} + x_{2} + 1) + x_{1}x_{2})}{d_{1} + (y_{1} + y_{1}^{2})(x_{2} + y_{2})}.$$

If the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero, then the sum (x_3, y_3) is a point on E_{B,d_1,d_2} : i.e., $d_1(x_3 + y_3) + d_2(x_3^2 + y_3^2) = x_3y_3 + x_3y_3(x_3 + y_3) + x_3^2y_3^2$.

Birational Equivalence

Generally, elliptic curves are defined by the Weierstrass model. When considering a finite field of characteristic 2, the curve defined by the equation

$$v^2 + uv = u^3 + a_2u^2 + a_6$$

with $a_6 \neq 0$ is an elliptic curve in short Weierstrass model. Addition law has the point at infinity as neutral element and the inverse element of the point (u_1, v_1) is $-(u_1, v_1) = (u_1, v_1 + u_1)$.

Consider the elliptic curve *E* defined by: $v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4(d_1^4 + d_1^2 + d_2^2)$ with *j*-invariant $1/(d_1^4(d_1^4 + d_1^2 + d_2^2))$ $d_1^2 + d_2^2)$).

Then, we have a birational equivalence between E and E_{B,d_1,d_2} via the map φ defined by $\varphi(x, y) = (u, v)$ with

$$\begin{cases} u = \frac{d_1(d_1^2 + d_1 + d_2)(x + y)}{xy + d_1(x + y)}, \\ v = d_1(d_1^2 + d_1 + d_2) \left(\frac{x}{xy + d_1(x + y)} + d_1 + 1\right) \end{cases}$$

The inverse of φ is defined as follows:

$$\begin{cases} x = \frac{d_1(u+d_1^2+d_1+d_2)}{u+v+(d_1^2+d_1)(d_1^2+d_1+d_2)}, \\ y = \frac{d_1(u+d_1^2+d_1+d_2)}{v+(d_1^2+d_1)(d_1^2+d_1+d_2)}. \end{cases}$$

By putting $\varphi(0,0) = P_{\infty}$, and $P \in E_{B,d_1,d_2}$, then the function φ can be extended on P, see Bernstein et al. (2008). **Theorem 2.2** Consider K a field with $\#K = 2^n (n \ge 3)$ and d_1, d_2 in K such that $d_1 \ne 0$. Let $s \in K$, with $s^2 + s + d_2 = 0$. Then the completeness of the addition law on the Edwards model $E_{B,d_1,d_2}(K)$ in K is satisfied. \square

Proof. See Bernstein et al. (2008).

Definition 2.3 Consider K a field with $\#K = 2^n$ ($n \ge 3$) and d_1, d_2 in K such that $d_1 \ne 0$. Suppose that $s^2 + s + d_2 \ne 0$ for all $s \in K$. Then, the complete Edwards elliptic curve with elements d_1 and d_2 is given by the equation

$$E_{B,d_1,d_2}: d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

Theorem 2.4 Consider $n \in \mathbb{N}$ and $n \ge 3$. Let E be an elliptic curve in Weierstrass model over \mathbb{F}_{2^n} and E_{B,d_1,d_2} be a complete Edwards model over \mathbb{F}_{2^n} . Then $E_{B,d_1,d_2} \simeq E$ over \mathbb{F}_{2^n} .

Proof. See Bernstein et al. (2008).

2.1.2 Binary Edwards Curves of Diao and Lubicz (2010)

Definition 2.5 In Diao and Lubicz (2010), Diao and Lubicz introduce the following Edwards model:

$$x^2 + y^2 + \frac{1}{c}xy = 1 + x^2y^2,$$

 $c \in K^*$, with K a field of characteristic 2. We denote this curve $E_{DL,c}$ and consider the point (0,1) as neutral element of the following group law.

The addition law can be performed as follows:

Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be two points on the curve.

If $P_1 \neq P_2$ then, $P_1 + P_2 = P_3(x_3, y_3)$ with

$$x_3 = \frac{(x_1 + x_2)(1 + y_1y_2)}{(y_1 + y_2)(1 + x_1x_2)},$$

And if
$$P_1 = P_2$$
 then,

$$y_{3} = \frac{(x_{1} + y_{2})(y_{1} + x_{2})}{(1 + x_{1}y_{2})(1 + y_{1}x_{2})}.$$
$$x_{3} = \frac{x_{1}(y_{1} + 1)^{2}}{y_{1}(x_{1} + 1)^{2}},$$
$$y_{3} = \frac{(x_{1} + y_{1})^{2}}{(x_{1}y_{1} + 1)^{2}}.$$

Birational Equivalence

Every Edwards model defined over a field K of characteristic 2 is birationally equivalent to an ordinary elliptic curve defined by the equation: $z^2 + tz = t^3 + c^4$ of *j*-invariant $\frac{1}{c^4}$ via (the change of coordinates) the map

$$\begin{split} \varphi:(x,y)\longmapsto(t,z), & \left\{ \begin{array}{l} t=\frac{c}{x},\\ z=c(y+cx(y+1))/(x(y+1)). \end{array} \right.\\ \varphi^{-1}:(t,z)\longmapsto(x,y), & \left\{ \begin{array}{l} x=\frac{c}{t},\\ y=(z+c^2)/(t+z+c^2). \end{array} \right. \end{split} \end{split}$$

The map φ is not defined at point (0, 1) and we have $\varphi(0, 1) = P_{\infty}$.

2.2 Frobenius Map on Elliptic Curves

Let \mathbb{F}_q be a finite field of characteristic two with q elements $(q = 2^k)$ and $\overline{\mathbb{F}}_q$ be its algebraic closure. We consider nonsingular elliptic curves defined over \mathbb{F}_q

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

with $a, b \in \mathbb{F}_q, b \neq 0$.

The symbol $E(\overline{\mathbb{F}}_q)$ is denoted as the additive abelian group of $\overline{\mathbb{F}}_q$ -rational points on E with identity P_{∞} .

This is the groupe on which most public-key protocols are performed. The Frobenius endomorphism ϕ on $E(\overline{\mathbb{F}}_q)$ is given by

$$\phi: E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q)$$
$$(x, y) \longmapsto (x^q, y^q).$$

The map ϕ satisfies the equation

$$\phi^2 - c\phi + q = 0$$

where *c* is the trace of ϕ so that $|c| \leq 2\sqrt{q}$ is odd.

This means

$$\phi^2(P) - c\phi(P) + qP = P_\infty$$

for all points $P \in E(\overline{\mathbb{F}}_q)$.

3. Frobenius Map on Binary Edwards Curves

3.1 Diao and Lubicz's Binary Edwards Curve

In this subsection, we introduce the Frobenius endomorphism for the Edwards model proposed by Diao and Lubicz (2010).

Let \mathbb{F}_q be a finite field with $q = 2^k$ and $E_{DL,c}$ defined. In this section, we consider the q-Frobenius map π_q of $E_{DL,c}$

$$\pi_q: E_{DL,c} \longrightarrow E_{DL,c}$$
$$(x, y) \longmapsto (x^q, y^q).$$

The following theorem is the core of this section.

Theorem 3.1 Let \mathbb{F}_q be a finite field with $q = 2^k$ and let $E_{DL,c}$ be an Edwards model defined over \mathbb{F}_q and π_q the Frobenius map defined above. Then, we have

$$(\pi_q^2 - t\pi_q + q)P = P_{\infty}$$

for all $P \in E_{DL,c}$.

Before proving the Theorem 3.1, we give the following important lemmas.

Lemma 3.2 Let K be a finite field with $\#K = 2^n$ ($n \ge 3$). Every Edwards model defined over K is birationally equivalent over k to a Weierstrass elliptic curve given by equation: $z^2 + tz = t^3 + c^4$ of *j*-invariant $\frac{1}{c^4}$.

By Lemma 3.2, there exists an elliptic curve E over \mathbb{F}_q defined by $z^2 + tz = t^3 + c^4$, which verifies $E_{DL}(\overline{\mathbb{F}}_q) \cong E(\overline{\mathbb{F}}_q)$. Let φ be the isomorphism. Then,

$$\varphi: (x, y) \longmapsto (t, z) = \left[\frac{c}{x}, \frac{c(y + cx(y + 1))}{x(y + 1)}\right]$$

is a birational equivalence from $E_{DL,c}$ to E, with inverse

$$\varphi^{-1}: (t,z)\longmapsto (x,y) = \left[\frac{c}{t}, \frac{z+c^2}{t+z+c^2}\right].$$

Lemma 3.3 Let $E_{DL,c}$ an Edwards model over \mathbb{F}_q $(q = 2^k)$ which is birationally equivalent to Weierstrass curve E over \mathbb{F}_q . Let N be the cardinal of the group of rational points of $E_{DL,c}$ (N = q - t + 1) and let φ a birational map from $E_{DL,c}$ to E. Consider π_q as the q^{th} -pow Frobenius map of E. Put $\psi = \varphi^{-1} \circ \pi \circ \varphi$. Thus

- ψ is in $End(E_{DL,c})$, the endomorphism group of $E_{DL,c}$;
- $\forall P \in E_{DL,c}(\overline{\mathbb{F}}_q),$ $\psi^2(P) - [t]\psi(P) + [q](P) = O_{E_{DL,c}}.$

Proof. φ is isomorphism from $E_{DL,c}$ to E (see Bernstein, Birkner, Joye, Lange, & Peters, 2008), therefore we can see that ψ is an isogeny of E_{DL} to itself, since π_q is an isogeny.

Let *P* in $E_{DL}(\overline{\mathbb{F}}_q)$ and let $Q = \varphi(P)$ in $E(\overline{\mathbb{F}}_q)$, then

$$(\pi_q^2 - t\pi_q + q)Q = O_E.$$

Since

$$\varphi^{-1}(\pi_q^2 - t\pi_q + q)\varphi(P) = E_{DL}$$

we can deduce that

$$\psi^2(P) - [t]\psi(P) + [q](P) = O_{E_{DI}}.$$

Proof of Theorem 3.1. Let E_{DL} be a binary Edwards model and let E be the Weierstrass elliptic curve such that $E_{DL}(\mathbb{F}) \simeq E(\mathbb{F})$ and let ψ be the endomorphism defined in Lemma 3.2. Then, for all $P \in E_{DL}(\overline{\mathbb{F}}_q)$, we have:

$$\begin{split} \psi(x,y) &= (\varphi^{-1} \circ \pi_q \circ \varphi)(x,y) \\ &= (\varphi^{-1} \circ \pi_q) \left[\frac{c}{x}, \frac{c(y + cx(y + 1))}{x(y + 1)} \right] \\ &= \varphi^{-1} \left[\left(\frac{c}{x} \right)^q, \left(\frac{c(y + cx(y + 1))}{x(y + 1)} \right)^q \right] \\ &= \varphi^{-1} \left[\frac{c^q}{x^q}, \frac{c^q(y^q + c^q x^q(y^q + 1))}{x^q(y^q + 1)} \right] \\ &= (x^q, y^q) \end{split}$$

3.2 Bernstein and Lange's Binary Edwards Curve

We consider now the Bersntein and Lange's model (2008).

Consider \mathbb{F}_q) as a finite field with $q = 2^k$ and let E_{B,d_1,d_2} be a binary Bersntein and Lange's model defined over \mathbb{F}_q). Let q-Frobenius map π_q of E_{B,d_1,d_2} ,

$$\pi_q : E_{B,d_1,d_2} \longrightarrow E_{B,d_1,d_2}$$
$$(x, y) \longmapsto (x^q, y^q).$$

The following theorem is the core of this section.

Theorem 3.4 Consider E_{B,d_1,d_2} be a binary Edwards model defined over \mathbb{F}_q with $q = 2^k$ and let N be the cardinal of the group of rational points of E_{B,d_1,d_2} (N = q - t + 1). The Frobenius map π_q of E_{B,d_1,d_2} verifies

$$(\pi_q^2 - t\pi_q + q)P = P_\infty = (0, 1), \quad \forall P \in E_{B, d_1, d_2}.$$

Before proving the Theorem 3.4, we give the following lemmas.

Lemma 3.5 Let K be a finite field with $\#K = 2^n$ ($n \ge 3$). Every Edwards model defined over K is birationally equivalent over K to a Weierstrass elliptic curve given by the equation: $z^2 + tz = t^3 + c^4$ of *j*-invariant $\frac{1}{c^4}$.

By Lemma 3.5, there exists a Weierstrass elliptic model E over \mathbb{F}_q which verifies $E_{B,d_1,d_2}(\overline{\mathbb{F}}_q) \cong E(\overline{\mathbb{F}}_q)$. Consider φ as the isomorphism, thus $E(\mathbb{F}_q)$ can be defined as $z^2 + tz = t^3 + c^4$.

The map

$$\varphi: (x, y) \longmapsto (u, v) = \left[\frac{d_1(d_1^2 + d_1 + d_2)(x + y)}{xy + d_1(x + y)}, d_1(d_1^2 + d_1 + d_2)\left(\frac{x}{xy + d_1(x + y)} + d_1 + 1\right)\right]$$

is a birational equivalence from E_{B,d_1,d_2} to E, and the inverse map is defined by

$$\varphi^{-1}: (u,v) \longmapsto (x,y) = \left[\frac{d_1(u+d_1^2+d_1+d_2)}{u+v+(d_1^2+d_1)(d_1^2+d_1+d_2)}, \frac{d_1(u+d_1^2+d_1+d_2)}{v+(d_1^2+d_1)(d_1^2+d_1+d_2)}\right].$$

Lemma 3.6 Let E_{B,d_1,d_2} be a Edwards model defined over \mathbb{F}_q with $q = 2^k$ and let E the birationally equivalent in Weierstrass model of E_{B,d_1,d_2} over \mathbb{F}_{2^k} . Let N be the cardinal of the group of rational points of $E(\mathbb{F}_q)$, i.e. (N = q - t + 1) and let φ be a birational map. Consider π_q as the q^{th} -pow Frobenius endomorphism of E. Put $\psi = \varphi^{-1} \circ \pi \circ \varphi$, thus

- ψ is in $End(E_{B,d_1,d_2})$, the endomorphism group of E_{B,d_1,d_2});
- $\forall P \in E_{B,d_1,d_2}(\overline{\mathbb{F}}_q),$

$$\psi^{2}(P) - [t]\psi(P) + [q](P) = O_{E_{Bd_{1}d_{2}}}$$

Proof. φ is an isomorphism from E_{B,d_1,d_2} to E (see Bernstein, Birkner, Joye, Lange, & Peters, 2008). Therefore we can see that ψ is an isogeny of E_{B,d_1,d_2} to itself defined over \mathbb{F}_q since π_q : $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$ is an isogeny from E to itself defined over \mathbb{F}_q .

Let $P \in E_{B,d_1,d_2}(\overline{\mathbb{F}}_q)$ and let $Q = \varphi(P) \in E(\overline{\mathbb{F}}_q)$, then

$$(\pi_q^2 - t\pi_q + q)Q = O_E$$

Since

$$\varphi^{-1}(\pi_q^2 - t\pi_q + q)\varphi(P) = E_{B,d_1,d_2}$$

we can deduce that

$$\psi^2(P) - [t]\psi(P) + [q](P) = O_{E_{B,d_1,d_2}}.$$

Proof of Theorem 3.4. Let *E* be a Weierstrass elliptic curve and let E_{B,d_1,d_2} be the binary Edwards model such that $E_{B,d_1,d_2}(\mathbb{F}_q) \simeq E_{B,d_1,d_2}(\mathbb{F}_q)$, and let ψ be the endomorphism defined in *Lemma 3.5.* Then, $\forall P = (x, y) \in E_{B,d_1,d_2}(\overline{\mathbb{F}}_q)$

$$\begin{split} \psi(x,y) &= (\varphi^{-1} \circ \pi_q \circ \varphi)(x,y) \\ &= (\varphi^{-1} \circ \pi_q)(u,v) \\ &= (\varphi^{-1} \circ \pi_q) \left(\frac{d_1(d_1^2 + d_1 + d_2)(x+y)}{xy + d_1(x+y)}, \frac{d_1(d_1^2 + d_1 + d_2)}{x(xy + d_1(x+y)) + d_1 + 1} \right) \\ &= \varphi^{-1} \left[\left(\frac{d_1(d_1^2 + d_1 + d_2)(x+y)}{xy + d_1(x+y)} \right)^q, \left(d_1(d_1^2 + d_1 + d_2) \left(\frac{x}{xy + d_1(x+y)} + d_1 + 1 \right) \right)^q \right] \\ &= \varphi^{-1} \left[\frac{d_1^q(d_1^{2q} + d_1^q + d_2^q)(x^q + y^q)}{x^{qyq} + d_1^q(x^q + y^q)}, d_1^q(d_1^{2q} + d_1^q + d_2^q) \left(\frac{x^q}{x^{qyq} + d_1^q(x^q + y^q)} + d_1^q + 1 \right) \right] \\ &= \varphi^{-1} \left[\frac{d_1(d_1^2 + d_1 + d_2)(x^q + y^q)}{x^{qyq} + d_1(x^q + y^q)}, d_1(d_1^2 + d_1 + d_2) \left(\frac{x^q}{x^{qyq} + d_1(x^q + y^q)} + d_1 + 1 \right) \right] \\ &= (x^q, y^q) \end{split}$$

4. Conclusion

We have successfully introduced Frobenius map on elliptic curves of characteristic 2 in particulary on Binary Edwards curves of T. Lange and D. J. Bernstein and on Binary Edwards curves of O. Diao and D. Lubucz.

These two endomorphisms can be used to speed up the scalar multiplication over Edwards models in characteristic two, using the GLV method for example.

References

- Arene, C., Lange, T., Naehrig, M., & Ritzenthaler, C. (2011). Faster computation of the Tate pairing. Journal of Number Theory, 131(5), 842-857. http://dx.doi.org/10.1016/j.jnt.2010.05.013
- Avanzi, R., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., & Vercauteren, F. (2006). *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall.
- Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards curves. In S. Vaudenay (Ed.), Progress in Cryptology–AFRICACRYPT 2008, Lecture Notes in Computer Science, 5023, 389-405. http://dx.doi.org/10.1007/978-3-540-68164-9_26
- Bernstein, D. J., Lange, T., & Farashahi, R. R. (2008). Binary edwards curves. Cryptographic Hardware and Embedded Systems-CHES 2008, Lecture Notes in Computer Science, 5154, 244-265. http://dx.doi.org/10.1007/978-3-540-85053-3_16
- Blake, I., Murty, V. K., & Xu, G. (2008). Nonadjacent radix-expansions of integers in Euclidean imaginary quadratic number fields. *Canadian Journal of Mathematics*, 60, 1267-1282. http://dx.doi.org/10.4153/CJM-2009-055-6
- Diao, O., & Lubicz, D. (2010). Quelques aspects de l'arithmétique des courbes hyperelliptiques de genre 2. Retrieved from http://tel.archives-ouvertes.fr/docs/00/50/60/25/PDF/FinalRapport.pdf
- Edwards, H. M. (2007). A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(2007), 393-422. http://dx.doi.org/10.1090/S0273-0979-07-01153-6
- Galbraith, S., Lin, X. B., & Scott, M. (2011). Endomophisms for faster elliptic curve cryptography on a large class of curves. *Journal of Cryptology*, 24(3), 446-469. http://dx.doi.org/10.1007/s00145-010-9065-y
- Gallant, R. P., Lambert, R. J., & Vanstone, S. A. (2001). Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In J. Kilian (Ed.), Advances in Cryptology–CRYPTO 2001, Lecture Notes in Computer Science, 2139, 190-200. http://dx.doi.org/10.1007/3-540-44647-8_11
- Hisil, H., Wong, K. K. H., Carter, G., & Dawson, E. (2008). Twisted edwards curves revisited. Advances in Cryptology–ASIACRYPT 2008, Lecture Notes in Computer Science, 5350, 326-343. http://dx.doi.org/10.1007/978-3-540-89255-7_20
- Iijima, T., Matsuo, K., Chao, J., & Tsujii, S. (2002). Construction of Frobenius maps of twist elliptic curves and

its application to elliptic scalar multiplication. In Proc. of SCIS 2002, 699-702.

- Joux, A. (2004). A one round protocol for tripartite Diffe-Hellman. Journal of Cryptology, 17(4), 263-276. http://dx.doi.org/10.1007/s00145-004-0312-y
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Math. Comp.*, 48, 203-209. http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5

Silvermann, J. (1986). The Arithmetique of Elliptic Curves. Springer.

Solinas, J. (1997). An improved algorithm for arithmetic on a family of elliptic curves. *Advances in Cryptology– CRYPTO'97, Lecture Notes in Computer Science, 1294*, 357-371. http://dx.doi.org/10.1007/BFb0052248

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).