Iranian Journal of Mathematical Sciences and Informatics
Vol. 4, No. 2 (2009), pp. 55-64
DOI: 10.7508/ijmsi.2009.02.006

Generalized Jacobian and Discrete Logarithm Problem on Elliptic Curves

H. Daghigh* and M. Bahramian

Department of Mathematics, Faculty of Science, University of Kashan, I. R. Iran

E-mail: hassan@kashanu.ac.ir
E-mail: bahramianh@kashanu.ac.ir

Abstract. Let E be an elliptic curve over the finite field $\mathbb{F}_q$, P a point in $E(\mathbb{F}_q)$ of order n, and Q a point in the group generated by P. The discrete logarithm problem on E is to find the number k such that $Q = kP$. In this paper we reduce the discrete logarithm problem on $E[n]$ to the discrete logarithm on the group $\mathbb{F}_q^*$, the multiplicative group of nonzero elements of $\mathbb{F}_q$, in the case where $n \mid q-1$, using generalized jacobian of E.

Keywords: Elliptic Curve, Discrete Logarithm Problem, Generalized Jacobian.

2000 Mathematics subject classification: 14H22, 14H40, 14L35.

1. Introduction

Let G be an additive finite group, $x \in G$ and $y \in \langle x \rangle$. The discrete logarithm problem (DLP) on G is to find the number k such that $y = kx$. The integer k is called the discrete logarithm of y to the base x. If G is the group of points on an elliptic curve over a finite field, then the discrete logarithm problem on G is called the elliptic curve discrete logarithm problem ($ECDLP$).

*Corresponding Author

Received 21 July 2009; Accepted 26 September 2009

Koblitz [6] and Miller [7] in 1985 independently proposed using the group of points on an elliptic curve defined over a finite field to devise discrete logarithm cryptographic schemes. The security of these cryptosystems is based upon the presumed intractability of computing logarithms in the elliptic curve group.

Our main result is the following theorem which reduces the $ECDLP$ to DLP on the underlying field.

Theorem Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and $E(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$ rational points of E. Also let $E[n](\mathbb{F}_q)$ be the group of n-torsion points of E defined over $\mathbb{F}_q$. If $n \mid q-1$, then solving the discrete logarithm problem on $\mathbb{F}_q^*$ is at least as hard as solving the discrete logarithm problem on $E[n](\mathbb{F}_q)$.

The remainder of the paper is organized as follows. The next section provides the definition of the usual and generalized jacobians and necessary results about them. We will prove the above theorem in section 3 (Theorem 3.3) using the theory of generalized jacobian of the elliptic curve E. Finally an example, which shows how to apply our method is given in the last section.

2. Usual and Generalized Jacobians

Déchène [1, 2, 3] has proposed generalized jacobians as a source of groups for public key cryptosystems based on the hardness of the Discrete Logarithm Problem. We will obtain a relation that presents a way to reduce the discrete logarithm in the n-torsion part of an elliptic curve E over the finite field $\mathbb{F}_q$ to the multiplicative group $\mathbb{F}_q^*$ where $n \mid q-1$ using generalized jacobian. First we need some definitions and properties.

let C be a smooth algebraic curve defined over an algebraically closed field K. Also let $Div(C)$ be the free abelian group of all divisors of C and $Princ(C)$ be the group of all principal divisors. The quotient group $Div(C)/Princ(C)$ is called the Picard group or the divisor class group of C and is denoted by $Pic(C)$. The degree zero part of the Picard group, $Pic^0(C)$, is simply $Div^0(C)/Princ(C)$. For elliptic curves, we have the following result which says that the class group of divisors of degree zero on E is simply isomorphic to the group E.

Theorem 2.1. *Let E be an elliptic curve over a field K. Then the map $P \longrightarrow [(P)-(\mathcal{O})]$ is a group isomorphism between E and $Pic^0(E)$with well-defined inverse $[\sum_{P\in E} n_P(P)] \longrightarrow \sum_{P\in E} n_P P$.*

Proof. See ([12] Proposition III.3.4) □

The following theorem introduces the (usual) jacobian.

Theorem 2.2. *Let C be a smooth algebraic curve of genus g defined over an algebraically closed field. Then, there exists an abelian variety $J(C)$ of* *dimension g and an isomorphism of groups*

$$Pic^0(C) \longrightarrow J(C).$$

The variety $J(C)$ is called the jacobian of C.

Proof. The proof of this theorem can be found in ([13] Proposition III.2.6). For a more complete treatment, one can see [16]. □

Now we present an overview of generalized jacobian varieties. For more information see [9, 10, 11]. Generalized jacobians offer a natural generalization of both torus-based and curve-based cryptography. Starting with a smooth algebraic curve C defined over an algebraically closed field K, two divisors $D = \sum_{P \in C} n_P(P)$ and $D' = \sum_{P' \in C} n_{P'}(P')$ are said to be linearly equivalent if $D - D'$ is a principal divisor, i.e. $D - D' = div(f)$ for some f in the function field $K(C)$ of C. In this case, we write $D \sim D'$. The quotient group obtained is then the usual jacobian $J(C)$. To define the generalized jacobian, let $\mathfrak{m} = \sum_{P \in C} m_P(P)$ be an effective divisor on the curve C. For a given $f \in K(C)$ we write $f \equiv 1 \ (mod\ \mathfrak{m})$ as a shorthand for the requirement $Ord_P(1-f) \geq m_P$ for each P in the support of $\mathfrak{m}$.

Definition 2.3. Let $\mathfrak{m}$ be an effective divisor and let D and D' be two divisors with supports disjoint from the support of $\mathfrak{m}$. We say that D and D' are $\mathfrak{m}$-equivalent, and write $D \sim_{\mathfrak{m}} D'$, if there is a function $f \in K(C)^*$ such that $div(f) = D - D'$ and $f \equiv 1 \ (mod\ \mathfrak{m})$.

It is easy to see that the above definition defines an equivalence relation on $Div(C)$. Also if two divisors are $\mathfrak{m}$-equivalent, then they must be linearly equivalent. Therefore, if we denote by $[D]$ the class of the divisor D under linear equivalence and by $[D]_{\mathfrak{m}}$ the class of the divisor D under $\mathfrak{m}$-equivalence, then $[D]_{\mathfrak{m}} \subseteq [D]$.

Now let $Div_{\mathfrak{m}}(C)$ be the subgroup of $Div(C)$ formed by all divisors of C with supports disjoint from $\mathfrak{m}$. Let also $Div^0_{\mathfrak{m}}(C)$ be the subgroup of $Div_{\mathfrak{m}}(C)$ of divisors of degree zero. Moreover, let $Princ_{\mathfrak{m}}(C)$ be the subset of principal divisors which are $\mathfrak{m}$-equivalent to the zero divisor. It is easy to see that $Princ_{\mathfrak{m}}(C)$ is a subgroup of $Div^0_{\mathfrak{m}}(C)$. Therefore, the set of $\mathfrak{m}$-equivalence classes in $Div^0_{\mathfrak{m}}(C)$ is indeed the quotient group $Div^0_{\mathfrak{m}}(C)/Princ_{\mathfrak{m}}(C)$, which will be denoted by $Pic^0_{\mathfrak{m}}(C)$. Since $[D]_{\mathfrak{m}} \subseteq [D]$ for all divisor D, there exists an epimorphism $\sigma : Pic^0_{\mathfrak{m}}(C) \longrightarrow Pic^0(C)$.

The following theorem is an analogue of Theorem (2.2).

Theorem 2.4. *Let K be an algebraically closed field and C be a smooth algebraic curve of genus g defined over K. Then for every modulus $\mathfrak{m}$, there exists* *a commutative algebraic group $J_{\mathfrak{m}}$ isomorphic to the group $Pic^0_{\mathfrak{m}}(C)$. The dimension π of $J_{\mathfrak{m}}$ is given by*

$$\pi = \begin{cases} g & \text{if } \mathfrak{m} = 0, \\ g + deg(\mathfrak{m}) - 1 & \text{otherwise.} \end{cases}$$

Proof. See [10] and ([11] chapter V. Proposition 2. and Theorem 1.) □

Definition 2.5. The algebraic group $J_{\mathfrak{m}}$ is called the generalized jacobian of the curve C with respect to the modulus $\mathfrak{m}$.

To obtain a representation of the elements of the generalized jacobian we need the following theorem.

Theorem 2.6. *Let $(G, +)$ be a group and $(A, \cdot)$ be an abelian group. Let also*

$$1 \longrightarrow A \longrightarrow \overline{G} \xrightarrow{p} G \longrightarrow 0$$

be a short exact sequence defining a group extension $\overline{G}$ of G by A. Denote by $\oplus$ the group operation on $\overline{G}$. Then,

1: *Let $s : G \longrightarrow \overline{G}$ be a (set-theoretic) section for p (i.e. $p \circ s = 1_G$). Then the map*

$$\begin{aligned} A \times G &\longrightarrow \overline{G} \\ (a, \sigma) &\rightsquigarrow a \oplus s(\sigma) \end{aligned}$$

is a bijection of sets. Hence, each element of $\overline{G}$ can be represented as a pair (a, σ), where $a \in A$ and $\sigma \in G$.

2: *There is a well-defined natural action of G on A given by*

$$\begin{aligned} A \times G &\longrightarrow A \\ (a, \sigma) &\rightsquigarrow a^{\sigma} := x \oplus a \ominus x \end{aligned}$$

where x is any element of $\overline{G}$ satisfying $p(x) = \sigma$ and $\ominus x$ denotes the inverse of x in $\overline{G}$.

3: *In fact, the group operation $\oplus : \overline{G} \times \overline{G} \longrightarrow \overline{G}$ can be expressed in terms of this action:*

$$(a, \sigma) + (b, \tau) = (a \cdot b^{\sigma} \cdot c(\sigma, \tau), \sigma + \tau)$$

where $c : G \times G \longrightarrow A$ must satisfy the following condition

$$c(\sigma, \tau) \cdot c(\sigma + \tau, \rho) = c(\tau, \rho)^{\sigma} \cdot c(\sigma, \tau + \rho). \tag{2.1}$$

(A function c satisfying (2.1) is called a 2-cocycle on G with values in A.)

Proof. see ([4] chapter III) and ([17] chapter 5) □

In the case that $\overline{G}$ is commutative, (2.1) can be rewritten as

$$c(\sigma, \tau) \cdot c(\sigma + \tau, \rho) = c(\tau, \rho) \cdot c(\sigma, \tau + \rho).$$

Moreover we have the following Lemma.

Lemma 2.7. *With the notation of the above theorem*

$$c(\sigma,\tau)\cdot c(-\sigma,\sigma+\tau)=1$$

for all $\sigma,\tau \in G$.

Proof. See ([5] Lemma 7.1) and [14] for a more complete treatment. □

Theorems 2.2 and 2.4 and the epimorphism $\sigma : Pic^0_{\mathfrak{m}}(C) \longrightarrow Pic^0(C)$ implies that there exists an epimorphism $\tau : J_{\mathfrak{m}} \longrightarrow J$. Let $L_{\mathfrak{m}}$ be the kernel of τ, then the short exact sequence

$$1 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \xrightarrow{\tau} J \longrightarrow 0$$

defines the group extension $J_{\mathfrak{m}}$ of J by $L_{\mathfrak{m}}$. It then follows from Theorem 2.6 that the elements of $J_{\mathfrak{m}}$ could be seen as pairs (k,P), where $k \in L_{\mathfrak{m}}$ and $P \in J$. Using this representation, the group law on $J_{\mathfrak{m}}$ could be expressed in terms of the group laws on $L_{\mathfrak{m}}$ and on J, and also involves a 2-cocycle on J with values in $L_{\mathfrak{m}}$.

Moreover the short exact sequence

$$1 \longrightarrow L_{\mathfrak{m}} \xrightarrow{\iota} L_{\mathfrak{m}} \times J \xrightarrow{\rho} J \longrightarrow 0$$

with obvious maps ι and ρ also defines another group extension $L_{\mathfrak{m}} \times J$ of J by $L_{\mathfrak{m}}$. But can $J_{\mathfrak{m}}$ be the direct product $L_{\mathfrak{m}} \times J$? Rosenlicht answers this question in the following theorem.

Theorem 2.8. *Let C be a smooth algebraic curve of genus g defined over an algebraically closed field and let $J_{\mathfrak{m}}$ be the generalized jacobian of C with respect to a modulus $\mathfrak{m}$. If $g \geq 1$ and $deg(\mathfrak{m}) \geq 2$, then $J_{\mathfrak{m}}$ is not a trivial direct product.*

Proof. This is a corollary of Theorem 13 in [10]. □

Theorem 2.9. *Let C be a smooth algebraic curve defined over an algebraically closed field, J be the jacobian of C and $J_{\mathfrak{m}}$ be the generalized jacobian of C with respect to a modulus $\mathfrak{m} = \sum_{P\in C} m_P(P)$ of support $S_{\mathfrak{m}}$. Let also $L_{\mathfrak{m}}$ be the kernel of the natural homomorphism τ from $J_{\mathfrak{m}}$ onto J, and let $\mathbb{G}_m \simeq \{x \in \mathbb{A}^1 | x \neq 0\}$. Then, $L_{\mathfrak{m}}$ is an algebraic group isomorphic to the product of a torus $T = \mathbb{G}_m^{\sharp S_{\mathfrak{m}}-1}$ by a unipotent group V of the form $V = \prod_{P\in S_{\mathfrak{m}}} V_{(m_P)}$ where each $V_{(m_P)}$ is isomorphic to the group of matrices of the form*

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & a_{m_P-1} \\ 0 & 1 & a_1 & \dots & a_{m_P-2} \\ 0 & 0 & 1 & \dots & a_{m_P-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Proof. See ([11] Chapter V). □

Now let E be an elliptic curve defined over the finite field $K = \mathbb{F}_q$ with q elements and let $\mathfrak{m} = (M) + (N)$, where M and N are distinct nonzero points of $E(\mathbb{F}_q)$.

Finally, let $J_{\mathfrak{m}}$ be the generalized jacobian of E with respect to $\mathfrak{m}$. In the light of Theorems 2.8 and 2.9, this choice of parameters implies that this generalized jacobian will be an extension of the elliptic curve E by the multiplicative group $\mathbb{G}_m$. We already know that there is a bijection of sets between $J_{\mathfrak{m}}$ and $\mathbb{G}_{\mathfrak{m}} \times E$. Hence, each element of $J_{\mathfrak{m}}$ can be represented as a pair (k, P), where $k \in \mathbb{G}_m$ and $P \in E$ Indeed, we have by construction that $J_{\mathfrak{m}}$ is isomorphic to $Pic^0_{\mathfrak{m}}(E)$, and so an explicit bijection of sets $\varphi : Pic^0_{\mathfrak{m}}(E) \longrightarrow \mathbb{G}_{\mathfrak{m}} \times E$ could be used to transport the known group law on $Pic^0_{\mathfrak{m}}(E)$ to $\mathbb{G}_{\mathfrak{m}} \times E$.

Déchène ([1] Chapter 5, Propositions 5.1 and 5.4) has proved the following two theorems which represent the elements of $J_{\mathfrak{m}}$ using the isomorphism between $Pic^0_{\mathfrak{m}}(E)$ and $\mathbb{G}_m \times E$ and obtaining a formula for the group operation on $\mathbb{G}_m \times E$.

Theorem 2.10. *Let E be an elliptic curve defined over $\mathbb{F}_q$, $\mathfrak{m} = (M) + (N)$ with $M, N \in E\backslash\{\mathcal{O}\}$, $M \neq N$ and $T \in E\backslash\{\mathcal{O}, M, N, M - N, N - M\}$, be given. Let also*

$$\psi : Pic^0_{\mathfrak{m}}(E) \longrightarrow \mathbb{G}_m \times E$$
$$[D] \longrightarrow (k, S)$$

be such that the $\mathfrak{m}$-equivalence class of $D = \sum_{P \in E} n_P(P)$ corresponds to $S = \sum_{P \in E} n_P P$ and $k = f(M)/f(N)$, where $f \in K(E)^*$ is any function satisfying

$$div(f) = \begin{cases} D - (S) + (\mathcal{O}) & \textit{if } S \notin \{M, N\}\ , \\ D - (S + T) - (T) & \textit{otherwise.} \end{cases}$$

Then ψ is a well-defined bijection of sets.

Theorem 2.11. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $\mathfrak{m} = (M) + (N)$ be given such that M and N are distinct nonzero points of E. If (k_1, P_1) and (k_2, P_2) are elements of $J_{\mathfrak{m}}$ fulfilling $P_1, P_2, \pm(P_1 + P_2) \notin \{M, N\}$ then $(k_1, P_1) + (k_2, P_2) = (k_1 k_2 \mathbf{c}_{\mathfrak{m}}(P_1, P_2), P_1 + P_2)$ where $c_{\mathfrak{m}} : E \times E \longrightarrow \mathbb{G}_m$ is a 2-cocycle depending on the modulus $\mathfrak{m}$ and*

$$\mathbf{c}_{\mathfrak{m}}(P_1, P_2) = \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)}$$

where $L_{P_1,P_2}(M) = c \cdot \frac{l_{P_1,P_2}}{l_{P_1+P_2,\mathcal{O}}}$ for some $c \in \overline{K}^*$ (that we can suppose that $c = 1$). Also $l_{P,Q}$ denotes the equation of the line passing through P and Q (tangent at the curve if $P = Q$).

We here present a small collection of the basic properties of the group law in these generalized jacobians, which are easily derived from Theorem (2.11).

Corollary 2.12. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $\mathfrak{m} = (M) + (N)$ be given such that M and N are distinct nonzero points of E. Let also $(k, P), (k_1, P_1), (k_2, P_2) \in J_\mathfrak{m}$ be given such that $P_1, P_2, \pm(P_1 + P_2) \notin \{M, N\}$. Then,*

1: $\mathbf{c}_\mathfrak{m}(P_1, P_2) = \mathbf{c}_\mathfrak{m}(P_2, P_1)$ *(This reflects the fact that $J_\mathfrak{m}$ is abelian).*

2: $\mathbf{c}_\mathfrak{m}(\mathcal{O}, P) = 1$ *for all $P \notin \{M, N\}$. Hence, $(k_1, \mathcal{O}) + (k_2, P) = (k_1 k_2, P)$.*

3: $(1, \mathcal{O})$ *is the identity element of $J_\mathfrak{m}$.*

4: *Furthermore, $J_\mathfrak{m}$ contains a subgroup isomorphic to $\mathbb{G}_m$, as $(k_1, \mathcal{O}) + (k_2, \mathcal{O}) = (k_1 k_2, \mathcal{O})$ for all $k_1, k_2 \in \mathbb{G}_m$.*

3. Discrete Logarithm Problem

Definition 3.1. (Discrete Logarithm Problem) Let G be a finite cyclic group of order n generated by an element g . Given $h \in G$, determine the integer $k \in [0, n-1]$ such that $g^k = h$. This integer is called the discrete logarithm of h (to the base g), and is denoted $\log_g(h)$.

In this section we will reduce the discrete logarithm problem in the n-torsion subgroup of an elliptic curve E over a finite field K with q elements, where $n \mid q - 1$ to the discrete logarithm problem in multiplicative group of K.

Remark 3.2. Given a group G, an element $g \in G$ and a natural number t, we can compute g^t very fast using the known (left-to-right) "square-and-multiply" algorithm. If $t = (t_m \cdots t_1 t_0)_2$ is the binary representation of t, then

$$\begin{aligned} g^k &= g^{2^m t_m + 2^{m-1} t_{m-1} + \cdots + 2t_1 + t_0} \\ &= ((\cdots((g^2 g^{t_{m-1}})^2 g^{t_{m-2}})^2 \cdots)^2 g^{t_1})^2 g^{t_0}. \end{aligned}$$

Theorem 3.3. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and $E(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$ rational points of E. Also let $E[n](\mathbb{F}_q)$ be the group of n-torsion points of E defined over $\mathbb{F}_q$. If $n \mid q - 1$, then solving the discrete logarithm problem on $\mathbb{F}_q^*$ is at least as hard as solving the discrete logarithm problem on $E[n](\mathbb{F}_q)$.*

Proof. Let $P \in E$ be a point of order n, and $\mathfrak{m} = (M) + (N)$ be a divisor prime to all prime divisors (rP) for those $0 < r < n$ which occur in the "square-and-multiply" algorithm, as noted in Remark 3.2. Also let $\alpha_t(P)$ be the first component of $t(1, P)$ where $(1, P) \in J_\mathfrak{m}$. We prove that

$$\alpha_n(kP)^{\frac{q-1}{n}} = (\alpha_n(P)^{\frac{q-1}{n}})^k \tag{3.1}$$

for all integer k.

The case $k = 0$ is clear. For $k > 0$, let $Q = kP$ and calculate $\alpha_{nk}(P)$, the first component of $nk(1, P)$ in two ways. From Theorem 2.11, we know

$$\alpha_t(P) = \mathbf{c}_\mathfrak{m}(P, P)\mathbf{c}_\mathfrak{m}(P, 2P) \cdots \mathbf{c}_\mathfrak{m}(P, (t-1)P).$$

At first

$$\begin{aligned} nk(1,P) &= n(k(1,P)) = n(\alpha_k(P), kP) = n(\alpha_k(P), Q) \\ &= (\alpha_k(P)^n \alpha_n(Q), nQ) = (\alpha_k(P)^n \alpha_n(Q), \mathcal{O}) \end{aligned}$$

thus $\alpha_{nk}(P) = \alpha_k(P)^n \alpha_n(Q)$. Also

$$\begin{aligned} nk(1,P) &= k(n(1,P)) = k(\alpha_n(P), nP) \\ &= k(\alpha_n(P), \mathcal{O}) = (\alpha_n(P)^k, \mathcal{O}) \end{aligned}$$

thus $\alpha_{nk}(P) = \alpha_n(P)^k$. Comparing these two last equation implies that

$$\alpha_k(P)^n \alpha_n(Q) = \alpha_n(P)^k \tag{3.2}$$

and from this we have

$$\alpha_n(Q)^{\frac{q-1}{n}} = (\alpha_n(P)^{\frac{q-1}{n}})^k.$$

Now let $k < 0$. From Lemma 2.7 $\mathbf{c}_\mathfrak{m}(R,S)\mathbf{c}_\mathfrak{m}(-R, R+S) = 1$ for all $R, S \in E$ then

$$\begin{aligned} &\mathbf{c}_\mathfrak{m}(Q,Q)\mathbf{c}_\mathfrak{m}(-Q,2Q) = 1 \\ &\mathbf{c}_\mathfrak{m}(Q,2Q)\mathbf{c}_\mathfrak{m}(-Q,3Q) = 1 \\ &\vdots \\ &\mathbf{c}_\mathfrak{m}(Q,(n-1)Q)\mathbf{c}_\mathfrak{m}(-Q,\mathcal{O}) = 1 \\ &\mathbf{c}_\mathfrak{m}(Q,\mathcal{O})\mathbf{c}_\mathfrak{m}(-Q,Q) = 1. \end{aligned}$$

Multiplying the above equations gives $\alpha_n(Q)\alpha_n(-Q) = 1$ that implies $\alpha_n(-Q) = (\alpha_n(Q))^{-1}$ and the proof is now complete. □

Remark 3.4. Using the above theorem, discrete logarithm on E is reduced to discrete logarithm on $\mathbb{F}_q$. Note that by the standard reduction of Pohlig and Hellman [8] we can assume that n is prime. For, let $n = \prod_i p_i^{e_i}$ be the prime factorization of n. To find k from $Q = kP$, the idea of Pohlig-Hellman is to find $k \pmod{p_i^{e_i}}$ for each i, then use the Chinese Remainder theorem to combine these and obtain $k \pmod{n}$ ([15], Section 5.2.3). Therefore we can assume that n is prime. Now assuming $\alpha_n(P)^{\frac{q-1}{n}} \neq 1$, from $(\alpha_n(P)^{\frac{q-1}{n}})^n = 1$ we deduce that $Ord_{\mathbb{F}_q^*}(\alpha_n(P)^{\frac{q-1}{n}}) = n$. Since $k < n$, if one can solve discrete logarithm on $\mathbb{F}_q^*$ then k will be obtained uniquely.

Remark 3.5. In the generalized jacobian $J_\mathfrak{m}$ let (a,P) and (b,Q) be the representation of two elements of $J_\mathfrak{m}$ such that $(b,Q) = k(a,P)$. Also let $Ord(P) = n$. In this case $b = a^k\alpha_k(P)$ and therefore from (3.2)
$b^n\alpha_n(Q) = a^{kn}\alpha_k(P)^n\alpha_n(Q) = a^{kn}\alpha_n(P)^k = (a^n\alpha_n(P))^k$. If $a^n\alpha_n(P)$ is a primitive root of unity in $\mathbb{F}_q^*$, then the equation $b^n\alpha_n(Q) = (a^n\alpha_n(P))^k$ gives a discrete logarithm problem in $\mathbb{F}_q^*$.

4. An Example

With a simple PARI program we can calculate $\alpha_n(P)$ and $\alpha_n(Q)$ very fast (in logarithmic time).

Consider the elliptic curve

$$E : y^2 + xy + y = x^3 + 2x^2 + 6x + 7$$

defined over the finite field $\mathbb{F}_q$ with $q = 152617819$ elements. We reduce the discrete logarithm problem on this elliptic curve to a discrete logarithm problem in $\mathbb{F}_q^*$.

Consider $P = (23658750, 133471885) \in E(\mathbb{F}_q)$, $Q = kP = (129045381, 133258769)$ with $k = 4276384$. The order of P is $Ord(P) = 25436303$. The points $M = 4P$ and $N = 5P$ do not occur in the calculation $\alpha_n(P)$ and $\alpha_n(Q)$ by repeated doubling process. We get

$$\alpha_n(P)^{\frac{q-1}{n}} = \alpha_n(P)^6 = 76904832,$$
$$\alpha_n(Q)^{\frac{q-1}{n}} = \alpha_n(Q)^6 = 95183794.$$

Hence in order to compute k we have to solve the discrete logarithm problem

$$95183794 \equiv 76904832^k \pmod{q}. \tag{4.1}$$

Of course one can check in this example that k is a solution of the equation (4.1).

References

[1] Isabelle Déchène, *Generalized Jacobians in Cryptography*, PhD thesis, McGill University, 2005.

[2] Isabelle Déchène, *Arithmetic of generalized Jacobians, in "Algorithmic Number Theory Symposium ANTS VII" (eds. F. Hess, S. Pauli and M. Post)*, 4076, Springer-Verlag, 2006, 421-435.

[3] Isabelle Déchène, On the security of generalized jacobian cryptosystems, *Advances in Mathematics of Communications*, **1** (4) (2007), 413-426.

[4] Peter Hilton and Urs Stammbach, *Course in Homological Algebra*, Number 4 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1971.

[5] J. Scott Carter, Daniel Jelsovsky, Seiichi Kamada, Laurel Langford and Masahico Saito, Quandle Cohomology and State-sum Invariants of Knotted Curves and Surfaces, *Trans. Amer. Math. Soc.*, **355** (2003), 3947-3989.

[6] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987), 203-209.

[7] V. Miller, Use of elliptic curves in cryptography, *Advances in CryptologyCRYPTO*, **85** (LNCS 218, [483]) (1986), 417-426.

[8] G. C. Pohlig and M. E. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Trans. Info. Theory*, **24** (1978), 106-110.

[9] Maxwell Rosenlicht, Equivalence relations on algebraic curves, *Annals of Mathematics*, **56** (1952), 169-191.

[10] Maxwell Rosenlicht, Generalized Jacobian varieties, *Annals of Mathematics*, **59** (1954), 505-530.

[11] Jean-Pierre Serre, *Algebraic groups and class fields*, Vol. 117 of Graduate texts in mathematics, Springer-Verlag, New-York, 1988.

[12] Joseph H. Silverman, *The arithmetic of elliptic curves*, Vol. 106 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1986.

[13] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Vol. 151 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1994.

[14] M. Wakui, On Dijkgraaf-Witten invariant for 3-manifolds, *Osaka J. Math.*, **29** (1992), 675-696.

[15] L. C. Washington, *Elliptic Curves*, Number Theory and Cryptography, Chapman and Hall / CRC, 2003.

[16] André Weil, *Variétés abéliennes et courbes algébriques*, Vol. 1064 of Actualités Sci. Ind. Hermann and Cie, Paris, 1948.

[17] Edwin Weiss, *Cohomology of groups*, Pure and Applied Mathematics, Vol. 34, Academic Press, New York, 1969.