Arithmetic of Generalized Jacobians

Isabelle Déchène*

University of Waterloo
Department of Combinatorics and Optimization
Waterloo, Ontario, Canada N2L 3G1
idechene@uwaterloo.ca

Abstract. This paper aims at introducing generalized Jacobians as a new candidate for discrete logarithm (DL) based cryptography. The motivation for this work came from the observation that several practical DL-based cryptosystems, such as ElGamal, the Elliptic and Hyperelliptic Curve Cryptosystems, XTR, LUC as well as CEILIDH can all naturally be reinterpreted in terms of generalized Jacobians. However, usual Jacobians and algebraic tori are thus far the only generalized Jacobians implicitly utilized in cryptography. In order to go one step further, we here study the simplest nontrivial generalized Jacobians of an elliptic curve. In this first of a series of articles, we obtain explicit formulæ allowing to efficiently perform arithmetic operations in these groups. This work is part of our doctoral dissertation, where security aspects are considered in depth. As a result, these groups thus provide the first concrete example of semi-abelian varieties suitable for DL-based cryptography.

Keywords. Public-key cryptography, Discrete logarithm problem, generalized Jacobians, semi-abelian varieties, elliptic curves.

1 Introduction and Motivation

Groups where the discrete logarithm problem (DLP) is believed to be intractable are inestimable building blocks for cryptographic applications. They are at the heart of numerous protocols such as key agreements, public-key cryptosystems, digital signatures, identification schemes, publicly verifiable secret sharings, hash functions and bit commitments. The search for new groups with intractable DLP is therefore of great importance.

In 1985, the landmark idea of Koblitz [Kob87] and Miller [Mil86] of using elliptic curves in public-key cryptography would, to say the least, change the perception of many on the tools of number theory that can be of practical use to cryptographers. In 1988, Koblitz [Kob89] generalized this idea by considering Jacobians of hyperelliptic curves, which then led to the broader study of abelian

* The research for this paper was done while the author was a Ph.D. student at McGill University under the supervision of Henri Darmon and Claude Crépeau and was supported by the Bell University Laboratories (BUL).

varieties in cryptography. Nearly fifteen years later, Rubin and Silverberg [RS03] discovered that another family of algebraic groups, namely the algebraic tori, also are of great cryptographic interest.

Now on one hand, Jacobians of curves (of small genus) gained the favor of many over the years, mostly because of the smaller key size needed. This attractive characteristic is in fact possible since we can easily generate curves for which there are no known subexponential time algorithms for solving the corresponding discrete logarithm problem. On the other hand, rational algebraic tori over a finite field offer the convenient advantage of possessing a compact representation of their elements, which then decreases the amount of information needed to be exchanged.

In a nutshell, cryptographers like Jacobians of curves for their security and care about algebraic tori for their efficiency. Thus as far as we can tell, it appears that these two sub-families of algebraic groups somehow possess complementary cryptographic advantages. From a mathematical point of view, however, the overall picture looks quite different. Indeed, with a minimal background in algebraic geometry, they can both be seen as two realizations of a single concept: *generalized Jacobians*.

As a result, several existing DL-based cryptosystems, such as the ElGamal, the Elliptic and Hyperelliptic Curve Cryptosystems, XTR, the Lucas-based cryptosystem LUC as well as the torus-based cryptosystem CEILIDH all possess an underlying structure that can be naturally reinterpreted in terms of generalized Jacobians[1]. Figure 1 provides a simplified view of the interrelation between the cryptosystems and their underlying structures.

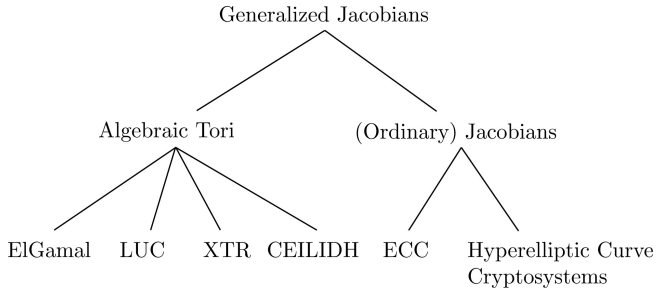

Fig. 1. Relation between DL-based cryptosystems and generalized Jacobians

This observation then raised the following question at the heart of our research:

[1] Recall that the interpretation of XTR and LUC in terms of tori is due to Rubin and Silverberg [RS03, Section 7].

Is it possible to use a generalized Jacobian that is neither a usual Jacobian nor an algebraic torus for DL-based cryptography?

An affirmative answer would then widen the class of algebraic groups that are of interest in public-key cryptography.

This existence result was established in our doctoral thesis [Déc05] by considering the simplest nontrivial generalized Jacobians of elliptic curves. These test groups are in fact semi-abelian varieties which are extensions (of algebraic groups) of an elliptic curve by the multiplicative group $\mathbb{G}_{\mathrm{m}}$.

Now recall that there are four main requirements for a group G to be suitable for DL-based cryptography. Namely,

- The elements of G can be easily represented in a compact form,
- The group operation can be performed efficiently,
- The DLP in G is believed to be intractable, and
- The group order can be efficiently computed.

We here address the first, second and fourth of these requirements. For security considerations, please refer to [Déc05, Section 5.5].

This paper is organized as follows. In the next section, we give a condensed introduction to generalized Jacobians. In Section 3, we derive a natural representation of the group elements. Using this compact representation, the group law algorithm is obtained in Section 4 and basic properties are presented in Section 5. An outlook is presented in Section 6.

2 Generalized Jacobians: The Essentials

We here present an extremely concise overview of generalized Jacobian varieties [Ros52,Ros54,Ser88]. A more detailed exposition in the context of cryptography can be found in [Déc05, Chapter 4]. The underlying idea behind the construction of generalized Jacobians is essentially the same as with the usual Jacobians. That is, starting with your favorite smooth algebraic curve C defined over an algebraically closed field K, one first considers the free abelian group whose elements are (a subgroup of) its divisors of degree zero. A *clever* equivalence relation on these divisors is then defined. The quotient group obtained is then naturally isomorphic to an algebraic group, which we hope to use for cryptographic applications.

Thus the key ingredient in these constructions is the equivalence relation one considers. Loosely speaking, the whole idea behind these equivalence relations is to somehow "measure" how much a divisor $D = \sum_{P \in C} n_P(P)$ differs from a divisor $D' = \sum_{P \in C} n'_P(P)$. Linear equivalence give rise to usual Jacobians. In this case, recall that two divisors D and D' are said to be *linearly equivalent* if $D - D'$ is a principal divisor, say $D - D' = \mathrm{div}(f)$ for some f in the function field $K(C)$ of C. In this case, we write $D \sim D'$. For generalized Jacobians, the equivalence relation will now depend on the choice of an effective divisor[2]

[2] That is, each m_P is a nonnegative integer and only finitely many of them are nonzero.

$\mathfrak{m} = \sum_{P \in C} m_P(P)$, thereafter called a *modulus*. For a given $f \in K(C)$, it is also a standard notation to write $f \equiv 1 \bmod \mathfrak{m}$ as a shorthand for the requirement $\mathrm{ord}_P(1-f) \geq m_P$ for each P in the support of $\mathfrak{m}$.

Definition 1. *Let $\mathfrak{m}$ be an effective divisor and let D and D' be two divisors of disjoint support with $\mathfrak{m}$. 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* $\mathrm{div}(f) = D - D'$ *and* $f \equiv 1 \bmod \mathfrak{m}$.

It is a small exercise to verify that this indeed defines an equivalence relation [Déc05, Section 4.2]. A motivation for this definition can also be found in [Déc05, Section 4.2], where $\mathfrak{m}$-equivalence is seen as a natural generalization of linear equivalence.

Now notice that if two divisors are $\mathfrak{m}$-equivalent, then they must be linearly equivalent as well. Therefore, if we denote by $[D]$ (respectively $[D]_{\mathfrak{m}}$) the class of D under linear equivalence (respectively $\mathfrak{m}$-equivalence), then $[D]_{\mathfrak{m}} \subseteq [D]$. This basic (but nevertheless fundamental) observation will play a key role in Sections 3 and 4, as our prior knowledge about the usual Jacobian will be our main tool for obtaining explicit formulæ for generalized Jacobians.

Next we wish to define the equivalent of the divisor class group for this new equivalence relation. Thus let $\mathrm{Div}_{\mathfrak{m}}(C)$ be the subgroup of $\mathrm{Div}(C)$ formed by all divisors of C of disjoint support with $\mathfrak{m}$. Let also $\mathrm{Div}^0_{\mathfrak{m}}(C)$ be the subgroup of $\mathrm{Div}_{\mathfrak{m}}(C)$ composed of divisors of degree zero. Moreover, let $\mathrm{Princ}_{\mathfrak{m}}(C)$ be the subset of principal divisors which are $\mathfrak{m}$-equivalent to the zero divisor[3]. It is a routine exercise[4] to show that $\mathrm{Princ}_{\mathfrak{m}}(C)$ is a subgroup of $\mathrm{Div}^0_{\mathfrak{m}}(C)$. As a result, the set of $\mathfrak{m}$-equivalence classes is indeed a group. We will therefore consider the quotient group $\mathrm{Div}^0_{\mathfrak{m}}(C)/\,\mathrm{Princ}_{\mathfrak{m}}(C)$, which will be denoted by $\mathrm{Pic}^{\,0}_{\mathfrak{m}}(C)$. At last, we can state the existence theorem of Maxwell Rosenlicht whose complete proof can be found in his original article [Ros54] as well as in [Ser88, Chapter V, in particular Prop. 2 and Thm 1(b)].

Theorem 1 (Rosenlicht). *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 $\mathrm{Pic}^0_{\mathfrak{m}}(C)$. The dimension π of $J_{\mathfrak{m}}$ is given by*

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

Definition 2. *The algebraic group $J_{\mathfrak{m}}$ is called the* generalized Jacobian *of the curve C with respect to the modulus $\mathfrak{m}$.*

Remark 1. We wish to emphasize that there are many $J_{\mathfrak{m}}$ associated to a fixed curve C, one for each choice of modulus $\mathfrak{m}$ in fact. This contrasts with the (usual) Jacobian J which is uniquely determined from C.

[3] The *zero divisor* $\mathbf{0} = \sum_{P \in C} 0(P)$ is the identity element of $\mathrm{Div}(C)$. Thus, $\mathrm{Princ}_{\mathfrak{m}}(C) = [\mathbf{0}]_{\mathfrak{m}} = \{\mathrm{div}(f) \,|\, f \in K(C)^* \text{ and } f \equiv 1 \bmod \mathfrak{m}\}$.

[4] See [Déc05, Section 4.3] for details.

Let's now take a closer look at the relationship between J and $J_{\mathfrak{m}}$. By construction, there are isomorphisms of groups $\varphi : \mathrm{Pic}^0(C) \to J$ and $\psi : \mathrm{Pic}^0_{\mathfrak{m}}(C) \to J_{\mathfrak{m}}$. Furthermore, there is a natural surjective homomorphism $\sigma : \mathrm{Pic}^0_{\mathfrak{m}}(C) \to \mathrm{Pic}^0(C)$ defined by $\sigma([D]_{\mathfrak{m}}) = [D]$. As a result, there is a surjective homomorphism $\tau := \varphi \circ \sigma \circ \psi^{-1}$ from $J_{\mathfrak{m}}$ to J.

An interresting object of study certainly is the kernel $L_{\mathfrak{m}}$ of the map τ since it might give us information about the structure of $J_{\mathfrak{m}}$. First notice that since τ is a homomorphism, then $L_{\mathfrak{m}}$ is a subgroup of $J_{\mathfrak{m}}$. We can then consider the following short exact sequence (of abelian groups[5]):

$$0 \longrightarrow L_{\mathfrak{m}} \overset{\text{inclusion}}{\longrightarrow} J_{\mathfrak{m}} \overset{\tau}{\longrightarrow} J \longrightarrow 0$$

As a result, *the generalized Jacobian $J_{\mathfrak{m}}$ is an extension of the usual Jacobian J by $L_{\mathfrak{m}}$*. The following theorem of Rosenlicht [Ros54] gives more information about $L_{\mathfrak{m}}$. The underlying ideas behind this proof are discussed in [Déc05, Section 4.5], while complete details can also be found in [Ser88, Sections V.13-V.17].

Theorem 2 (Rosenlicht). *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. Then, $L_{\mathfrak{m}}$ is an algebraic group isomorphic to the product of a torus $T = (\mathbb{G}_m)^{\#S_{\mathfrak{m}}-1}$ 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:

$$\begin{pmatrix} 1 & a_1 & a_2 & a_3 & \dots & a_{m_P-1} \\ 0 & 1 & a_1 & a_2 & \dots & a_{m_P-2} \\ 0 & 0 & 1 & a_1 & \dots & a_{m_P-3} \\ 0 & 0 & 0 & 1 & \dots & a_{m_P-4} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

This result allows us (among other things) to easily see why usual Jacobians and algebraic tori are two sub-families of generalized Jacobians.

Usual Jacobians are the generalized Jacobians corresponding to the case where the linear group $L_{\mathfrak{m}}$ is trivial. That is, if the modulus $\mathfrak{m} = \sum_{P \in C} m_P(P)$ with support $S_{\mathfrak{m}}$ was chosen to have degree zero or one. Indeed, if $\mathfrak{m} = \mathbf{0}$, then the condition $f \equiv 1 \bmod \mathfrak{m}$, i.e. $\mathrm{ord}_{P_i}(1-f) \geq m_i$ for each $P_i \in S_{\mathfrak{m}}$

[5] One can also see generalized Jacobians as extensions of *algebraic groups*, which are discussed in [Ser88, Chapter VII]. For the sequel, however, we shall only need to use properties of group extensions.

is vacuously true and therefore, $\mathfrak{m}$-equivalence coincides with linear equivalence. As well, if $\mathfrak{m} = (M)$, then the requirement $f \equiv 1 \bmod \mathfrak{m}$ reduces to $\mathrm{ord}_M(1-f) \geq 1$, which is equivalent to $f(M) = 1$. Hence, $\mathfrak{m}$-equivalence in this case reads $D \sim_{\mathfrak{m}} D'$ iff $\exists f \in K(C)^*$ such that $\mathrm{div}(f) = D - D'$ and $f(M) = 1$. But since $\mathrm{div}(c \cdot f) = \mathrm{div}(f)$ for any nonzero constant c, the condition $f(M) = 1$ is superfluous. It then follows that when $\mathfrak{m} = (M)$, linear and $\mathfrak{m}$-equivalence also define the same divisor classes.

If we are in the situation where $\mathfrak{m} = (P_0) + (P_1) + ... + (P_r)$ with the P_i's distinct, then $L_{\mathfrak{m}}$ is isomorphic to a torus T of dimension r. Moreover, since the usual Jacobian of $\mathbb{P}^1$ is trivial [Sil86, Example II.3.2], it then follows that the generalized Jacobian of $\mathbb{P}^1$ with respect to $\mathfrak{m}$ will be isomorphic to T. As a result, algebraic tori of any dimension can be seen as generalized Jacobians.

With these results at hand, we are now ready to explore the cryptographic potential of these algebraic groups.

3 Compact Representation of the Elements

The explicit family of generalized Jacobians that we consider can now be simply described as follows. Let E be a smooth elliptic curve defined over the finite field $K = \mathbb{F}_q$ with q elements[6] and let $B \in E(\mathbb{F}_q)$ be a point of prime order l. Let also $\mathfrak{m} = (M) + (N)$, where M and N are distinct nonzero points of $E(\mathbb{F}_{q^r})$, where $r \geq 1$ is a chosen integer. Hence, we can let $M = (X_M : Y_M : 1)$ and $N = (X_N : Y_N : 1)$. These are so far the only conditions we impose on $\mathfrak{m}$. Finally, let $J_{\mathfrak{m}}$ be the generalized Jacobian of E with respect to $\mathfrak{m}$. In the light of Theorem 2, this choice of parameters implies that this generalized Jacobian will be an extension of the elliptic curve E by the multiplicative group $\mathbb{G}_{\mathrm{m}}$, which is a nice simple case study since elliptic curves and finite fields already are cherished by cryptographers.

Now, the goal of this section is to obtain a compact representation of the elements of $J_{\mathfrak{m}}$. By a classical result on group extensions [Déc05, Theorem 4.7], we already know that there is a *bijection of sets* between $J_{\mathfrak{m}}$ and $\mathbb{G}_{\mathrm{m}} \times E$. Hence, each element of $J_{\mathfrak{m}}$ can be conveniently represented as a pair (k, P), where $k \in \mathbb{G}_{\mathrm{m}}$ and $P \in E$. Although the mere existence this bijection suffices to compactly represent the elements of $J_{\mathfrak{m}}$, understanding this correspondence in depth will prove to be useful in the next section when comes the time to work out explicit formulæ for the group operation on $\mathbb{G}_{\mathrm{m}} \times E$. Indeed, we have by construction that $J_{\mathfrak{m}}$ is isomorphic to $\mathrm{Pic}^0_{\mathfrak{m}}(E)$, and so an explicit bijection of sets $\psi : \mathrm{Pic}^0_{\mathfrak{m}}(E) \to \mathbb{G}_{\mathrm{m}} \times E$ could be used to *"transport"* the known group law on $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ to $\mathbb{G}_{\mathrm{m}} \times E$. Hence, exploring ψ can be seen as the first step towards the obtention of the group law algorithm on $\mathbb{G}_{\mathrm{m}} \times E$.

The official starting point of this exploration will of course be to take advantage of the fact that elliptic curves coincide with their Jacobians. Indeed,

[6] For the purpose of constructing the generalized Jacobian, we will view E as being defined over $\overline{\mathbb{F}}_q$, so that the results of the previous section directly apply here.

we have at our disposal the following well-known isomorphism between E and $\mathrm{Pic}^0(E)$, whose proof can be found for instance in [Sil86, Proposition III.3.4].

Theorem 3. *Let E be a smooth elliptic curve over a perfect field K. Then the map*

$$\begin{aligned} E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [(P) - (\mathcal{O})] \end{aligned}$$

is a group isomorphism with well-defined inverse

$$\begin{aligned} \mathrm{Pic}^0(E) &\to E \\ \left[\sum_{P\in E} n_P(P)\right] &\mapsto \sum_{P\in E} n_P P. \end{aligned}$$

Now let $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}^0_{\mathfrak{m}}(E)$ be given. Under the above isomorphism, the class $[D]$ is mapped to $S = \sum_{P\in E} n_P P \in E$. As a result, $[D] = [(S) - (\mathcal{O})]$, which implies that $D-(S)+(\mathcal{O})$ is a principal divisor, say $D = (S) - (\mathcal{O}) + \mathrm{div}(f)$ for some $f \in \overline{K}(E)^*$. This suggests that $\psi([D]_{\mathfrak{m}}) = (k, S)$, for some $k \in \mathbb{G}_{\mathrm{m}}$. As we will shortly see, the determination of k will involve the computation of $f(M)$ and $f(N)$. If $S \neq M, N$, then $\mathrm{ord}_M(f) = \mathrm{ord}_N(f) = 0$ since D has disjoint support with $\mathfrak{m}$. So in this case, $f(M)$ and $f(N)$ are both defined and nonzero. However, if $S \in \{M, N\}$, then $\mathrm{ord}_S(f) = -1$, which means that f has a pole at S. In this case, the strategy is to use, in place of $(S) - (\mathcal{O})$, another simple divisor linearly equivalent to D which will now have disjoint support with $\mathfrak{m}$. Such a divisor is easily found by appealing to the Abel-Jacobi theorem for elliptic curves, whose proof can be found in [Déc05, Section 3.3.5].

Theorem 4 (Abel-Jacobi). *Let E be a smooth elliptic curve defined over a perfect field K and $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}(E)$ be given. Then,*

$$D \text{ is principal if and only if } \deg(D) = 0 \text{ and } \sum_{P\in E} n_P P = \mathcal{O}.$$

We therefore have an easy criterion to decide if two divisors are linearly equivalent:

Corollary 1. *Let E be a smooth elliptic curve defined over a perfect field K and let $D_1 = \sum_{P\in E} n_P(P)$, $D_2 = \sum_{P\in E} m_P(P) \in \mathrm{Div}(E)$ be given. Then,*

$$D_1 \sim D_2 \text{ if and only if } \deg(D_1) = \deg(D_2) \text{ and } \sum_{P\in E} n_P P = \sum_{P\in E} m_P P.$$

Now observe that if we *translate* S by a point $T \in E$, we obtain by the above corollary that

$$D \sim (S) - (\mathcal{O}) \sim (S + T) - (T),$$

and thus if $T \notin \{\mathcal{O}, M, N, M-N, N-M\}$, then both $(M+T)-(T)$ and $(N+T)-(T)$ have disjoint support with $\mathfrak{m}$. So from now on, we will assume that such a *'translation point'* T is fixed and publicly known. We can now let

$$R = \begin{cases} \mathcal{O} \text{ if } S \notin \{M, N\}, \\ T \text{ otherwise,} \end{cases}$$

and so there is an $f \in \overline{K}(E)^*$ satisfying

$$D = (S+R) - (R) + \operatorname{div}(f), \tag{2}$$

where the property $\operatorname{ord}_M(f) = \operatorname{ord}_N(f) = 0$ is fulfilled since D has disjoint support with $\mathfrak{m}$. Since this way of writing out a divisor already highlights the point S of E corresponding to D, it thus remains to determine how to *'read'* the corresponding element of $\mathbb{G}_{\mathrm{m}}$ from (2).

Since any two divisors in an $\mathfrak{m}$-equivalence class are mapped to the same element of $\mathbb{G}_{\mathrm{m}} \times E$, our approach will be to unravel the definition of $\mathfrak{m}$-equivalence until we can clearly see how to associate an element of $\mathbb{G}_{\mathrm{m}} \times E$ to each class. So let $D_1 = (S_1+R_1)-(R_1)+\operatorname{div}(f_1)$, $D_2 = (S_2+R_2)-(R_2)+\operatorname{div}(f_2) \in \operatorname{Div}^0_{\mathfrak{m}}(E)$ be given such that

$$R_i = \begin{cases} \mathcal{O} \text{ if } S_i \notin \{M, N\}, \\ T \text{ otherwise,} \end{cases}$$

for $i = 1, 2$. We then have

$$\begin{aligned}
D_1 \sim_{\mathfrak{m}} D_2 \text{ iff } & \exists f \in \overline{K}(E)^* \text{ such that } \operatorname{div}(f) = D_1 - D_2 \text{ and } f \equiv 1 \bmod \mathfrak{m}, \\
\text{iff } & \exists f \in \overline{K}(E)^* \text{ such that } \operatorname{div}(f) = (S_1+R_1)-(S_2+R_2)+(R_2) \\
& -(R_1) + \operatorname{div}\left(\frac{f_1}{f_2}\right) \text{ and } \operatorname{ord}_M(1-f) \geq 1,\ \operatorname{ord}_N(1-f) \geq 1, \\
\text{iff } & S_1 + R_1 - (S_2+R_2) + R_2 - R_1 = \mathcal{O} \text{ and } \exists f \in \overline{K}(E)^* \text{ such that} \\
& \operatorname{div}(f) = \operatorname{div}\left(\frac{f_1}{f_2}\right) \text{ and } f(M) = f(N) = 1, \\
\text{iff } & S_1 = S_2,\ R_1 = R_2 \text{ and } \exists c \in \overline{K}^* \text{ such that } \frac{f_1(M)}{f_2(M)} = \frac{f_1(N)}{f_2(N)} = \frac{1}{c}, \\
\text{iff } & S_1 = S_2 \text{ and } \frac{f_1(M)}{f_2(M)} = \frac{f_1(N)}{f_2(N)}, \\
\text{iff } & S_1 = S_2 \text{ and } \frac{f_1(M)}{f_1(N)} = \frac{f_2(M)}{f_2(N)}.
\end{aligned}$$

That means that in order to check whether two given divisors are $\mathfrak{m}$-equivalent, we simply have to test two equalities, one in E and one in $\mathbb{G}_{\mathrm{m}}$. The obvious candidate for ψ is thus the map

$$\begin{aligned}
\psi : \operatorname{Pic}^0_{\mathfrak{m}}(E) &\longrightarrow \mathbb{G}_{\mathrm{m}} \times E \\
[D]_{\mathfrak{m}} &\longmapsto (k, S),
\end{aligned}$$

such that the $\mathfrak{m}$-equivalence class of $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}^0_{\mathfrak{m}}(E)$ corresponds to $S = \sum_{P \in E} n_P P$ and $k = f(M)/f(N)$, where $f \in \overline{K}(E)^*$ is any function satisfying

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

Notice that the existence of f is guaranteed by the Abel-Jacobi theorem and that ψ is well-defined since we have just shown that for $D_1 = (S_1 + R_1) - (R_1) + \mathrm{div}(f_1)$, $D_2 = (S_2 + R_2) - (R_2) + \mathrm{div}(f_2)$, $k_1 = f_1(M)/f_1(N)$ and $k_2 = f_2(M)/f_2(N)$, we have:

$$[D_1]_{\mathfrak{m}} = [D_2]_{\mathfrak{m}} \textit{ implies that } k_1 = k_2 \textit{ and } S_1 = S_2.$$

Morever, ψ is injective since we also already know that

$$(k_1, S_1) = (k_2, S_2) \textit{ implies that } [D_1]_{\mathfrak{m}} = [D_2]_{\mathfrak{m}}.$$

It therefore remains to show that ψ is surjective as well. So given $(k, S) \in \mathbb{G}_{\mathrm{m}} \times E$, we must find an $f \in \overline{K}(E)^*$ such that $f(M)/f(N) = k$. Using the idea behind the interpolation polynomial of Lagrange, or simply by inspection, we easily see that

$$f(X, Y, Z) = \begin{cases} \dfrac{k\,(X - X_N Z) + (X_M Z - X)}{(X_M - X_N)\,Z} & \text{if } X_M \neq X_N, \\ \dfrac{k\,(Y - Y_N Z) + (Y_M Z - Y)}{(Y_M - Y_N)\,Z} & \text{otherwise,} \end{cases}$$

fulfills the required conditions (notice that $X_M = X_N$ implies that $Y_M \neq Y_N$ since we assumed that $M \neq N$ and $Z_M = Z_N = 1$). Hence, the divisor

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

is mapped to (k, S), as wanted. We have therefore shown that ψ is the bijection we were looking for.

Proposition 1. *Let E be a smooth elliptic curve defined over $\mathbb{F}_q$, $T \in E \backslash \{\mathcal{O}, M, N, M - N, N - M\}$ and $\mathfrak{m} = (M) + (N)$ with $M, N \in E \setminus \{\mathcal{O}\}$, $M \neq N$ be given. Let also*

$$\begin{aligned} \psi : \mathrm{Pic}^0_{\mathfrak{m}}(E) &\longrightarrow \mathbb{G}_{\mathrm{m}} \times E \\ [D]_{\mathfrak{m}} &\longmapsto (k, S)\,, \end{aligned}$$

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

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

Then, ψ is a well-defined bijection of sets.

Remark 2. Notice that since the zero divisor can be written as

$$\mathbf{0} = (\mathcal{O}) - (\mathcal{O}) + \mathrm{div}(c),$$

where c is any nonzero constant, then $\mathbf{0}$ corresponds to the pair $(1, \mathcal{O})$. That is, $(1, \mathcal{O})$ is the identity element of $J_{\mathfrak{m}}$.

4 Group Law Algorithm

Using the explicit bijection between $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ and $\mathbb{G}_{\mathrm{m}} \times E$ that we just obtained, our next goal is to derive explicit formulæ for the group operation on $\mathbb{G}_{\mathrm{m}} \times E$ induced from $\mathrm{Pic}^0_{\mathfrak{m}}(E)$. First notice that by the theory of group extensions, we already know the basic structure of the addition on $J_{\mathfrak{m}}$ [Déc05, Theorem 4.7]. Indeed, we have for any k_1, $k_2 \in \mathbb{G}_{\mathrm{m}}$ and P_1, $P_2 \in E$,

$$(k_1, P_1) + (k_2, P_2) = (k_1 k_2 \cdot \mathbf{c}_{\mathfrak{m}}(P_1, P_2), P_1 + P_2)\,, \tag{3}$$

where $\mathbf{c}_{\mathfrak{m}} : E \times E \to \mathbb{G}_{\mathrm{m}}$ is a 2-cocycle depending on the modulus $\mathfrak{m}$. It thus suffices to make $\mathbf{c}_{\mathfrak{m}}$ explicit.

So given (k_1, P_1) and (k_2, P_2) in $J_{\mathfrak{m}}$, our task is then to compute their sum (k_3, P_3). Notice that there are two distinct cases to study, depending if the use of a *'translation point' T* is at all needed. Fortunately, there is an easy criterion to decide when it occurs. Indeed, suppose that the group we consider for cryptographic applications is the subgroup of $J_{\mathfrak{m}}$ generated by the element (k, P). By the addition rule (3), it immediately follows that

$$\textit{If } (j, Q) \in \langle (k, P) \rangle\,, \textit{ then } Q \in \langle P \rangle\,.$$

As a result, if neither M nor N is a multiple of P, then the group operation on $\langle (k, P) \rangle$ will *never* involve points of the form $(*, M)$ or $(*, N)$. Thus, there is no need to employ a translation point in this case. Of course, when either M or N lies in $\langle P \rangle$, then the corresponding addition formulæ will use translation points when appropriate in order to cover all possible cases. This motivates the following definition.

Definition 3. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and $B \in E(\mathbb{F}_q)$ be a given basepoint. Let also M, $N \in E(\overline{\mathbb{F}_q})$ be given. Then the modulus $\mathfrak{m} = (M) + (N)$ is said to be* B-unrelated *if M, $N \notin \langle B \rangle$. Otherwise, it will be called* B-related.

The aim of this section is to *transport* the addition on $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ to $\mathbb{G}_{\mathrm{m}} \times E$ in order to get explicit equations involving the group laws on $\mathbb{G}_{\mathrm{m}}$ and E in the case of a B-unrelated modulus $\mathfrak{m}$. So given (k_1, P_1), (k_2, P_2) and (k_3, P_3) in $J_{\mathfrak{m}}$ such that

$$(k_1, P_1) + (k_2, P_2) = (k_3, P_3) \text{ and } P_1,\ P_2,\ \pm P_3 \notin \{M, N\}\,,$$

our task is to express (k_3, P_3) in terms of (k_1, P_1) and (k_2, P_2). By the explicit bijection between $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ and $\mathbb{G}_{\mathrm{m}} \times E$, the elements (k_1, P_1) and (k_2, P_2) are respectively the image of the $\mathfrak{m}$-equivalence class of $D_1 = (P_1) - (\mathcal{O}) + \mathrm{div}(f_1)$ and $D_2 = (P_2) - (\mathcal{O}) + \mathrm{div}(f_2)$, for some $f_1, f_2 \in \overline{K}(E)^*$ such that $\mathrm{ord}_M(f_1) = \mathrm{ord}_N(f_1) = \mathrm{ord}_M(f_2) = \mathrm{ord}_N(f_2) = 0$, $f_1(M)/f_1(N) = k_1$ and $f_2(M)/f_2(N) = k_2$ (see proof of Proposition 1).

That being said, we can now endow $\mathbb{G}_{\mathrm{m}} \times E$ with the group operation inherited from $\mathrm{Pic}^0_{\mathfrak{m}}(E)$. So basically, all we need to know is to which element of $\mathbb{G}_{\mathrm{m}} \times E$ does $D_3 = D_1 + D_2$ correspond. First, we have by definition that

$$D_3 = (P_1) + (P_2) - 2(\mathcal{O}) + \mathrm{div}(f_1 \cdot f_2), \tag{4}$$

so in order to get the element of $\mathbb{G}_{\mathrm{m}} \times E$ we are looking for, the obvious stategy is to express the right hand side of (4) as $(P_3) - (\mathcal{O}) + \mathrm{div}(f_3)$. By the Abel-Jacobi theorem, we know that

$$(P_1) + (P_2) - 2(\mathcal{O}) \sim (P_1 + P_2) - (\mathcal{O}),$$

and so there is a function $L_{P_1,P_2} \in \overline{K}(E)^*$ satisfying

$$(P_1) + (P_2) - 2(\mathcal{O}) = (P_1 + P_2) - (\mathcal{O}) + \mathrm{div}(L_{P_1,P_2}). \tag{5}$$

Combining (4) and (5) yields

$$D_3 = (P_1 + P_2) - (\mathcal{O}) + \mathrm{div}(f_1 \cdot f_2 \cdot L_{P_1,P_2}).$$

We can thus set $P_3 = P_1 + P_2$ and $f_3 = f_1 \cdot f_2 \cdot L_{P_1,P_2}$. Hence, D_3 corresponds to (k_3, P_3), where

$$k_3 = \frac{f_3(M)}{f_3(N)} = \frac{f_1(M) \cdot f_2(M) \cdot L_{P_1,P_2}(M)}{f_1(N) \cdot f_2(N) \cdot L_{P_1,P_2}(N)} = k_1 \cdot k_2 \cdot \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)}.$$

That is,

$$(k_1, P_1) + (k_2, P_2) = \left(k_1 \cdot k_2 \cdot \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)}, P_1 + P_2 \right).$$

Moreover, notice that this addition rule so far agrees with the prediction (3) obtained from group extensions. Hence the 2-cocycle $\mathbf{c}_{\mathfrak{m}} : E \times E \to \mathbb{G}_{\mathrm{m}}$ we were seeking is now unveiled:

$$\mathbf{c}_{\mathfrak{m}}(P_1, P_2) = \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)}. \tag{6}$$

The very last step is to make L_{P_1,P_2} explicit. We are thus looking for a function L_{P_1,P_2} satisfying (5), or equivalently,

$$\mathrm{div}(L_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O}). \tag{7}$$

The natural approach is to consider the line ℓ_{P_1,P_2}, passing through P_1 and P_2, that will inevitably hit $-P_3 = -(P_1 + P_2)$ as well. Then,

$$\mathrm{div}\left(\frac{\ell_{P_1,P_2}}{Z} \right) = (P_1) + (P_2) + (-P_3) - 3(\mathcal{O}). \tag{8}$$

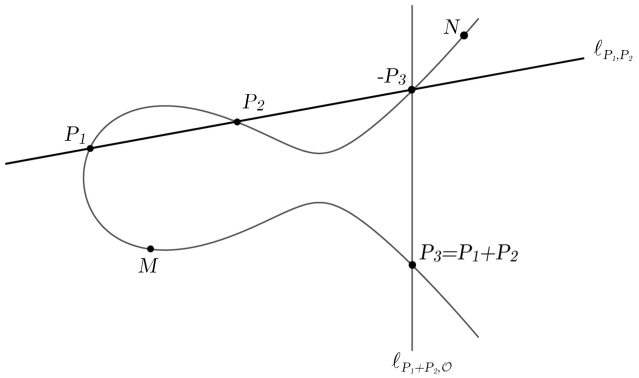

Fig. 2. Unveiling the 2-cocycle $\mathbf{c}_{\mathfrak{m}}$

Now in order to introduce the term $-(P_1 + P_2)$ and cancel out $(-P_3)$ at once, we may consider the line $\ell_{P_1+P_2,\mathcal{O}}$ passing through $P_1 + P_2$, $\mathcal{O}$, and a fortiori through $-P_3$. That is,

$$\operatorname{div}\left(\frac{\ell_{P_1+P_2,\mathcal{O}}}{Z}\right) = (P_1 + P_2) + (-P_3) - 2(\mathcal{O}). \tag{9}$$

Subtracting (9) from (8), we get

$$\operatorname{div}\left(\frac{\ell_{P_1,P_2}}{\ell_{P_1+P_2,\mathcal{O}}}\right) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O}). \tag{10}$$

Finally, (7) and (10) imply that L_{P_1,P_2} and $\ell_{P_1,P_2}/\ell_{P_1+P_2,\mathcal{O}}$ differ by a nonzero multiplicative constant:

$$\exists c \in \overline{K}^* \text{ satisfying } L_{P_1,P_2} = c \cdot \frac{\ell_{P_1,P_2}}{\ell_{P_1+P_2,\mathcal{O}}}. \tag{11}$$

Let's point out that our initial conditions M, $N \neq \mathcal{O}$ and P_1, P_2, $P_3 = P_1 + P_2 \notin \{M, N\}$ are sufficient to ensure that $L_{P_1,P_2}(M)$ and $L_{P_1,P_2}(N)$ will both be defined and nonzero, since (7) tells us that the only zeros and poles of L_{P_1,P_2} occur at P_1, P_2, $P_1 + P_2$ and $\mathcal{O}$. Furthermore, we can compute $L_{P_1,P_2}(M)$ and $L_{P_1,P_2}(N)$ by evaluating $\ell_{P_1,P_2}(M), \ell_{P_1+P_2,\mathcal{O}}(M), \ell_{P_1,P_2}(N)$ and $\ell_{P_1+P_2,\mathcal{O}}(N)$ separately since we also assumed that $-P_3 \neq M, N$.

Therefore, by (6) and (11), it is now legitimate to write

$$\mathbf{c}_{\mathfrak{m}}(P_1, P_2) = \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)} = \frac{\ell_{P_1,P_2}(M)}{\ell_{P_1+P_2,\mathcal{O}}(M)} \cdot \frac{\ell_{P_1+P_2,\mathcal{O}}(N)}{\ell_{P_1,P_2}(N)}, \tag{12}$$

and our goal is achieved since the 2-cocycle $\mathbf{c}_{\mathfrak{m}}$ is now completely determined. Lastly, since we have some freedom on both the equations of the lines (they are

determined up to a constant factor) and on the representatives for the homogeneous coordinates of M and N, we should verify that (12) is well-defined. That is, for $M = (X_M : Y_M : 1)$, $N = (X_N : Y_N : 1)$ and λ_1, λ_2, c_1, c_2 any nonzero constants, we have $M \sim (\lambda_1 X_M : \lambda_1 Y_M : \lambda_1)$, $N \sim (\lambda_2 X_N : \lambda_2 Y_N : \lambda_2)$ and $c_1 \cdot \ell_{P_1,P_2}$, $c_2 \cdot \ell_{P_1+P_2,\mathcal{O}}$ respectively defining the same line as ℓ_{P_1,P_2} and $\ell_{P_1+P_2,\mathcal{O}}$. Since ℓ_{P_1,P_2} and $\ell_{P_1+P_2,\mathcal{O}}$ are both homogeneous polynomials of degree one, it follows that

$$\frac{c_1 \cdot \ell_{P_1,P_2}(\lambda_1 X_M, \lambda_1 Y_M, \lambda_1)}{c_2 \cdot \ell_{P_1+P_2,\mathcal{O}}(\lambda_1 X_M, \lambda_1 Y_M, \lambda_1)} \cdot \frac{c_2 \cdot \ell_{P_1+P_2,\mathcal{O}}(\lambda_2 X_N, \lambda_2 Y_N, \lambda_2)}{c_1 \cdot \ell_{P_1,P_2}(\lambda_2 X_N, \lambda_2 Y_N, \lambda_2)} =$$
$$\frac{\lambda_1 \cdot \ell_{P_1,P_2}(X_M, Y_M, 1)}{\lambda_1 \cdot \ell_{P_1+P_2,\mathcal{O}}(X_M, Y_M, 1)} \cdot \frac{\lambda_2 \cdot \ell_{P_1+P_2,\mathcal{O}}(X_N, Y_N, 1)}{\lambda_2 \cdot \ell_{P_1,P_2}(X_N, Y_N, 1)} =$$
$$\frac{\ell_{P_1,P_2}(M)}{\ell_{P_1+P_2,\mathcal{O}}(M)} \cdot \frac{\ell_{P_1+P_2,\mathcal{O}}(N)}{\ell_{P_1,P_2}(N)},$$

which confirms that (12) was well-defined. Finally, we are ready to properly write down the group law we just obtained.

Theorem 5. *Let E be a smooth 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*

$$(k_1, P_1) + (k_2, P_2) = (k_1 k_2 \cdot \mathbf{c}_\mathfrak{m}(P_1, P_2), P_1 + P_2)\,, \tag{13}$$

where $\mathbf{c}_\mathfrak{m} : E \times E \to \mathbb{G}_m$ is the 2-cocycle given by

$$\mathbf{c}_\mathfrak{m}(P_1, P_2) = \frac{\ell_{P_1,P_2}(M)}{\ell_{P_1+P_2,\mathcal{O}}(M)} \cdot \frac{\ell_{P_1+P_2,\mathcal{O}}(N)}{\ell_{P_1,P_2}(N)},$$

and $\ell_{P,Q}$ denotes the equation of the straight line passing through P and Q (tangent at the curve if $P = Q$).

The group law for B-related moduli can also be obtained using a similar procedure. This case is fully treated in Section 5.3.2 of [Déc05], where the following result is presented.

Theorem 6. *Let E be a smooth elliptic curve defined over $\mathbb{F}_q$, $\mathfrak{m} = (M) + (N)$ be given such that M and N are distinct nonzero points of E and let $T \in E$ be any point such that $T \notin \{\mathcal{O}, M, N, M - N, N - M\}$. Given (k_1, P_1) and (k_2, P_2) in $J_\mathfrak{m}$, set $P_3 = P_1 + P_2$ and let, for $i = 1, 2, 3$,*

$$R_i = \begin{cases} T \text{ if } P_i \in \{M, N\}, \\ \mathcal{O} \text{ otherwise.} \end{cases}$$

Then,

$$(k_1, P_1) + (k_2, P_2) = \left(k_1 k_2 \cdot \frac{L(M)}{L(N)}, P_3\right),$$

where

$$L = \frac{\ell_{P_1,P_2}}{\ell_{P_3,\mathcal{O}}} \cdot \frac{\ell_{P_1+R_1,\mathcal{O}}}{\ell_{P_1,R_1}} \cdot \frac{\ell_{P_2+R_2,\mathcal{O}}}{\ell_{P_2,R_2}} \cdot \frac{\ell_{P_3,R_3}}{\ell_{P_3+R_3,\mathcal{O}}}.$$

As usual, $\ell_{P,Q}$ denotes the equation of the straight line passing through P and Q (tangent at the curve if $P = Q$).

5 Basic Properties

We here present a small collection of the basic properties of the group law in this generalized Jacobian. These properties are easily derived from Theorem 5.

Corollary 2. *Let E be a smooth 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. *$(1, \mathcal{O})$ is the identity element of $J_\mathfrak{m}$.*
2. *$\mathbf{c}_\mathfrak{m}(P_1, P_2) = \mathbf{c}_\mathfrak{m}(P_2, P_1)$ (This reflects the fact that $J_\mathfrak{m}$ is abelian).*
3. *If $M = (X_M : Y_M : 1)$ and $N = (X_N : Y_N : 1)$, then $\mathbf{c}_\mathfrak{m}(P, -P) = \ell_{P,\mathcal{O}}(M)/\ell_{P,\mathcal{O}}(N)$, and so the inverse of (k, P) is given by*

$$-(k, P) = \left(\frac{1}{k} \cdot \frac{\ell_{P,\mathcal{O}}(N)}{\ell_{P,\mathcal{O}}(M)}, -P\right)$$

4. *$\mathbf{c}_\mathfrak{m}(\mathcal{O}, P) = 1$ for all $P \in E\backslash\{M, N\}$. Hence,*

$$(k_1, \mathcal{O}) + (k_2, P) = (k_1 k_2, P).$$

5. *Futhermore, $J_\mathfrak{m}$ contains a subgroup isomorphic to $\mathbb{G}_\mathfrak{m}$, as*

$$(k_1, \mathcal{O}) + (k_2, \mathcal{O}) = (k_1 k_2, \mathcal{O}) \text{ for all } k_1, k_2 \in \mathbb{G}_\mathfrak{m}.$$

6. *If $B \in E(\mathbb{F}_q)$ and M, $N \in E(\mathbb{F}_{q^r})$ are such that $\mathfrak{m}$ is B-unrelated, then $\mathbb{F}_{q^r}^* \times \langle B\rangle$ is a subgroup of $J_\mathfrak{m}$.*

The only statement that might require a futher justification is property 6. Notice that it simply follows from properties 1 and 3, together with the observation that $\ell_{P_1,P_2}(M)$, $\ell_{P_1,P_2}(N) \in \mathbb{F}_{q^r}^*$ whenever P_1, $P_2 \in \langle B\rangle$. We have thus made completely explicit the finite group $\mathbb{F}_{q^r}^* \times \langle B\rangle$ of order $(q^r - 1) \cdot l$ that we wish to use for cryptographic applications.

6 Outlook

Given a smooth elliptic curve E defined over $\mathbb{F}_q$, a point $B \in E(\mathbb{F}_q)$ of prime order l and a B-unrelated modulus $\mathfrak{m} = (M) + (N)$ such that M and N are distinct points of $E(\mathbb{F}_{q^r})$ and $r \geq 1$ is a chosen integer, we now know that

$\mathbb{F}_{q^r}^* \times \langle B \rangle$, together with the group law of Theorem 5, is a finite subgroup of $J_{\mathfrak{m}}$ for which the elements are compactly represented, the group law efficiently computable and the group order readily determined.

Several other efficiency and security aspects were included in our doctoral dissertation[7] [Déc05]. On one hand, we considered various implementation issues, such as choosing a suitable modulus, speeding up scalar multiplications and selecting parameters such that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic group.

As for security, as soon as $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic subgroup of $J_{\mathfrak{m}}$, we obtained the following reductions among discrete logarithm problems:

The DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ *is at least as hard as the DLP in* $\langle B \rangle \subseteq E(\mathbb{F}_q)$ *and at least as hard as the DLP in* $\mathbb{F}_{q^r}^*$.

Thus from a practical point of view, this result implies that even though generalized Jacobians are newcomers in cryptography, we already know that solving their DLP cannot be easier than solving discrete logarithms in two of the most studied groups used in DL-based cryptography today.

Furthermore, we showed that extracting a discrete logarithm in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ can always be performed by *sequentially* computing a discrete logarithm in E followed by one in $\mathbb{F}_{q^r}^*$. Moreover, it is possible to proceed in parallel when $l \nmid (q^r - 1)$ while this is still an open question in the case of curves suitable for pairing-based cryptography.

Finally, we have also investigated several scenarios involving precomputations in order to further study the DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$. To this end, we empirically compared generalized Jacobians with the Classical Occupancy Problem. This preliminary study suggests that none of the proposed scenarios is faster than the known methods described above.

As a result, the generalized Jacobians we considered fulfill the basic requirements for a group to be suitable for DL-based cryptography. It thus provides the first concrete example of semi-abelian varieties that could be used in public-key cryptography.

Acknowledgments. I would like to thank my thesis co-supervisors Henri Darmon and Claude Crépeau for their guidance and advices. I would also like to thank the Centre for Applied Cryptographic Research (CACR) of the University of Waterloo for providing such a stimulating research environment.

References

[Déc05] Isabelle Déchène. *Generalized Jacobians in Cryptography.* PhD thesis, McGill University, 2005.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987.

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.

[7] For which the corresponding articles are currently in preparation.

[Mil86] Victor. S. Miller. Uses of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, Berlin, 1986. Springer-Verlag.

[Ros52] Maxwell Rosenlicht. Equivalence relations on algebraic curves. *Annals of Mathematics*, 56:169–191, July 1952.

[Ros54] Maxwell Rosenlicht. Generalized Jacobian varieties. *Annals of Mathematics*, 59:505–530, May 1954.

[RS03] Karl Rubin and Alice Silverberg. Torus-based cryptography. In Dan Boneh, editor, *Advances in Cryptology—CRYPTO '03*, volume 2729 of *Lecture Notes in Computer Science*, pages 349–365. Springer-Verlag, 2003.

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate texts in mathematics*. Springer-Verlag, New-York, 1988.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.