ON THE SECURITY OF GENERALIZED JACOBIAN CRYPTOSYSTEMS

ISABELLE DÉCHÈNE

Abstract. Generalized Jacobians are natural candidates to use in discrete logarithm (DL) based cryptography since they include the multiplicative group of finite fields, algebraic tori, elliptic curves as well as all Jacobians of curves. This thus led to the study of the simplest nontrivial generalized Jacobians of an elliptic curve, for which an efficient group law algorithm was recently obtained. With these explicit equations at hand, it is now possible to concretely study the corresponding discrete logarithm problem (DLP); this is what we undertake in this paper. In short, our results highlight the close links between the DLP in these generalized Jacobians and the ones in the underlying elliptic curve and finite field.

1. Introduction

Throughout this past year, cryptographers proudly celebrated three decades of public-key cryptography. In a word, concrete public-key cryptosystems exist *because* we know computational problems which, despite our greatest joint efforts, remain very hard to solve. We could thus say that Diffie and Hellman [4] taught us how to be optimistic by turning our incapacity of solving these problems into an amazingly elegant and powerful technique.

In addition of being the first such problem to be used in public-key cryptography, the discrete logarithm problem (DLP) remains without a doubt one of the most popular choices used nowadays to design cryptographic protocols.

Definition 1. Let G be a finite group and g be an element of G. Given $h \in \langle g \rangle$, the smallest non-negative integer k such that $g^k = h$ is called the *discrete logarithm of* h (to the base g) and is denoted $\log_g h$.

Generalized Jacobians are a good source of groups where this problem seems intractable. Indeed, recall that the ElGamal, Elliptic and Hyperelliptic Curve Cryptosystems as well as XTR, LUC and CEILIDH can all be understood in terms of generalized Jacobians [11, 3]. So from a cryptographic point of view, two remarkable subfamilies of generalized Jacobians are algebraic tori and usual Jacobians.

In order to *explicitly* study the cryptographic properties of a family of generalized Jacobians that are neither Jacobians nor tori, the simplest nontrivial generalized Jacobians of an elliptic curve was recently put forward [3]. In particular, it was shown

Date: First submitted on September 29, 2006 and revised on March 24, 2007.

2000 *Mathematics Subject Classification.* Primary 14L35, 94A60; Secondary 68Q17.

Key words and phrases. Public-key cryptography, discrete logarithm problem, generalized Jacobians, semi-abelian varieties, elliptic curves, finite fields, pairing-friendly curves.

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).

in this article how to obtain a compact representation of the elements, efficiently compute the group law and readily determine the cardinality of these groups.

The present article is the natural continuation of this work. Indeed, using completely elementary techniques, we here investigate the corresponding discrete logarithm problem. From the point of view of algebraic geometry, these specific generalized Jacobians are extensions of an elliptic curve by the multiplicative group $\mathbb{G}_{\mathrm{m}}$. We thus expect that this study will involve discrete logarithms in *three* different groups, namely, the generalized Jacobian, an elliptic curve and the multiplicative group of a finite field.

Thus the overall goal of this paper is to gain further insight on the precise relationships between these three problems. We emphasize that the objective of this work is not to claim nor demonstrate any *practical* advantages over previously proposed groups.

This article is based on Section 5.5 of our doctoral dissertation [2]. We first show that extracting a DL in these generalized Jacobians can always be performed by *sequentially* solving an instance of the DLP in the underlying elliptic curve E followed by one in the chosen finite field F. On the other hand, we demonstrate that the DLP in such cyclic generalized Jacobians is at least as hard as the DLP in E *and* at least as hard as the DLP in F. As a result, extracting a DL in those generalized Jacobians is polynomial-time equivalent to solving a DL in E and a DL in F.

Galbraith and Smith [6] recently made similar observations by working with extensions of algebraic groups "presented by a cocycle". Although this more general setting extends some of the results of this paper, we believe that our explicit approach has the advantage of being more insightful. For instance, these techniques enabled us to highlight an apparent distinct behaviour of generalized Jacobians of pairing-friendly curves (see Section 6 for more details).

This paper is organized as follows. In the next section, we review the construction of generalized Jacobians and recall the group law for the explicit family we consider. In Section 3, we obtain a closed expression involving three different DLPs, from which follows a natural solution to the DLP in these generalized Jacobians. Two reductions among discrete logarithm problems are then obtained in Section 4. In the following two sections, we apply the ideas of Pohlig and Hellman, both to curves used in classical ECC as well as to pairing-friendly curves. Lastly, an outlook is presented in Section 7.

2. Generalized Jacobians of an Elliptic Curve

The goal of this section is to present a minimalist aide-mémoire of the construction of generalized Jacobians as well as of the explicit group law for the family we are studying. For a complete treatment, please refer to the classical texts by Maxwell Rosenlicht [9, 10] and Jean-Pierre Serre [12, 13]. Although the underlying theory truly sheds some light on the intrinsic structure of these groups, the utterly simple equations for the group operation is all that will be needed for the sequel.

Let C be a smooth algebraic curve defined over an algebraically closed field K and $\mathfrak{m} = \sum_{P \in C} m_P(P) \in \mathrm{Div}(C)$ be an effective divisor[1], thereafter called a *modulus*. Two divisors D and D' of disjoint support with $\mathfrak{m}$ are said to be $\mathfrak{m}$-*equivalent*, and we write $D \sim_{\mathfrak{m}} D'$, if there exists an f in the function field of

[1]That is, each m_P is a non-negative integer and only finitely many of them are nonzero.

C such that $\mathrm{div}(f) = D - D'$ and $\mathrm{ord}_P(1-f) \geq m_P$ for each P in the support of $\mathfrak{m}$. Let $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ be the group of $\mathfrak{m}$-equivalence classes of degree zero divisors having disjoint support with $\mathfrak{m}$. Then, there exists a commutative algebraic group $J_{\mathfrak{m}}$, called the *generalized Jacobian* of C with respect to $\mathfrak{m}$, which is isomorphic to $\mathrm{Pic}^0_{\mathfrak{m}}(C)$.

The explicit family of generalized Jacobians we consider can now be described as follows. Let E be a smooth elliptic curve defined over the finite field $\mathbb{F}_q$ with q elements and let $B \in E(\mathbb{F}_q)$ be a point of prime order l. Let also $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus with M and N distinct points of $E(\mathbb{F}_{q^r})$, where $r \geq 1$ is a chosen integer (to fix ideas, r can be picked to be relatively small, say $r \leq 50$). Recall that a modulus $\mathfrak{m} = (M) + (N)$ is said to be *B-unrelated* if M, $N \notin \langle B \rangle$ [3, Definition 3].

For the purpose of constructing the corresponding generalized Jacobian $J_{\mathfrak{m}}$, we view E as being defined over $\overline{\mathbb{F}}_q$. This algebraic group $J_{\mathfrak{m}}$ is then a semi-abelian variety, which is an extension of algebraic groups of E by the multiplicative group $\mathbb{G}_{\mathrm{m}}$. Background material on extensions of algebraic groups can be found in [13, Chapter VII].

Remark 1. Recall that a commutative algebraic group S is called a *semi-abelian variety* if there exists a short exact sequence of algebraic groups

$$1 \to T \to S \to A \to 1,$$

where T is an algebraic torus and A is an abelian variety.

In order to obtain a compact and convenient representation for the elements of $J_{\mathfrak{m}}$ and a group law algorithm using this representation, the first step followed in [3] was to obtain an explicit bijection ψ of sets between $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ and $\mathbb{G}_{\mathrm{m}} \times E$. Thus in this particular case, an element of $J_{\mathfrak{m}}$ can be viewed as a pair (k, P), where $k \in \mathbb{G}_{\mathrm{m}}$ and $P \in E$. The known addition on $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ could then be used to endow, via ψ, the set $\mathbb{G}_{\mathrm{m}} \times E$ with the desired group structure.

More explicitly, let (k_1, P_1) and (k_2, P_2) be elements of $J_{\mathfrak{m}}$ such that P_1, P_2, $\pm(P_1 + P_2) \notin \{M, N\}$. Then,

$$(k_1, P_1) + (k_2, P_2) = (k_1 k_2 \cdot \mathbf{c}_{\mathfrak{m}}(P_1, P_2), P_1 + P_2)\,, \tag{2.1}$$

where $\mathbf{c}_{\mathfrak{m}} : E \times E \to \mathbb{G}_{\mathrm{m}}$ 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 $P = Q$) [3, Theorem 5].

Several basic properties can be easily derived from these explicit equations [3, Section 5]. In particular, the set

$$\mathbb{F}^*_{q^r} \times \langle B \rangle = \left\{ (k, P) \,\middle|\, k \in \mathbb{F}^*_{q^r}, P \in \langle B \rangle \right\},$$

together with the group law (2.1), is a subgroup of $J_{\mathfrak{m}}$ with identity $(1, \mathcal{O})$. Also, for all $(k_1, \mathcal{O}), (k_2, P) \in \mathbb{F}^*_{q^r} \times \langle B \rangle$, we have that

$$(k_1, \mathcal{O}) + (k_2, P) = (k_1 k_2, P)\,. \tag{2.2}$$

This last property will turn out to play a central role in our study of the DLP.

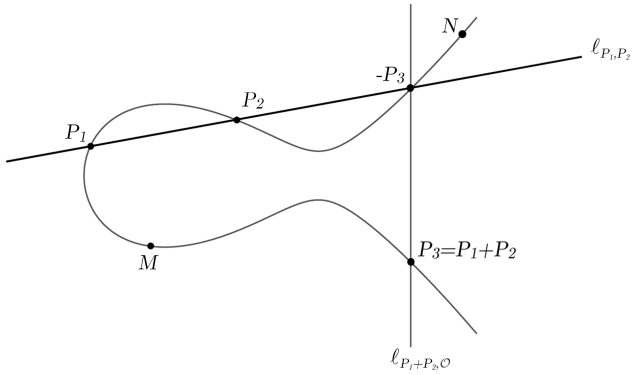

FIGURE 1. Group law in the generalized Jacobian

Next we make some useful remarks on the order of the elements in $\mathbb{F}_{q^r}^* \times \langle B \rangle$. So let $(k, P) \in \mathbb{F}_{q^r}^* \times \langle B \rangle$ be given such that $P \neq \mathcal{O}$. We are then looking for the smallest positive integer m such that $m(k, P) = (1, \mathcal{O})$. Since $m(k, P) = (*, mP)$, we must have $mP = \mathcal{O}$, from which we get that m is a multiple of $l = \operatorname{ord}(P)$. There is then a positive integer n such that $m = n \cdot l$. Hence,

$$(1, \mathcal{O}) = m(k, P) = n \cdot l(k, P) = n(\lambda, \mathcal{O}) = (\lambda^n, \mathcal{O}),$$

where $\lambda \in \mathbb{F}_{q^r}^*$ satisfies $l(k, P) = (\lambda, \mathcal{O})$. It thus follows that $\lambda^n = 1$, for which the least solution is $n = \operatorname{ord}(\lambda)$. As a result,

$$\textit{The order of } (k, P) \textit{ equals } \operatorname{ord}(\lambda) \cdot l. \tag{2.3}$$

So in particular,

$$(k, P) \textit{ generates } \mathbb{F}_{q^r}^* \times \langle B \rangle \textit{ if and only if } \lambda \textit{ generates } \mathbb{F}_{q^r}^*. \tag{2.4}$$

This last property can also be used to show, using an elementary counting argument, that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a *cyclic* group as soon as $l \nmid (q^r - 1)$ [2, Section 5.4.4]. Moreover, Balasubramanian and Koblitz showed that for a random prime q and a random E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = l$, the case $l \mid (q^r - 1)$ was very unlikely to arise [1, Theorem 2]. Thus in practice, it is easy to generate a generalized Jacobian $\mathbb{F}_{q^r}^* \times \langle B \rangle$ which is a cyclic group.

To sum up, $\mathbb{F}_{q^r}^* \times \langle B \rangle$ together with the induced group law (2.1) is a finite subgroup of $J_{\mathfrak{m}}$ of order $(q^r - 1) \cdot l$ for which the elements are compactly represented and the group law is efficiently computable. That being said, we are now ready to study the discrete logarithm problem in $\mathbb{F}_{q^r}^* \times \langle B \rangle$.

3. A Natural Solution

The purpose of this section is to present a natural method to extract discrete logarithms in $\mathbb{F}_{q^r}^* \times \langle B \rangle$. To do so, the first step will be to take a closer look at the scalar multiplication in this group.

So given $(k, P) \in \mathbb{F}_{q^r}^* \times \langle B \rangle$ and a non-negative integer n, we are here looking for an efficient way to compute the scalar multiple $n(k, P)$. First remark that a repeated application of the group law yields $n(k, P) = (*, nP)$. Thus if we set $n_0 = n \bmod l$, we get $n(k, P) = (*, n_0 P)$. So instead of computing $n(k, P)$ directly, we could make

use of the value of $n_0(k,P)$. Indeed, if we let $n_1 = \lfloor n/l \rfloor$, then $n = n_1 l + n_0$ and so $n(k,P) = n_1 l(k,P) + n_0(k,P)$. Therefore, if we let $l(k,P) = (\lambda, \mathcal{O})$ and $n_0(k,P) = (\nu_{n_0}, n_0 P)$, we obtain

$$\begin{aligned} n(k,P) &= n_1 l(k,P) + n_0(k,P) \\ &= n_1(\lambda, \mathcal{O}) + (\nu_{n_0}, n_0 P) \\ &= (\lambda^{n_1}, \mathcal{O}) + (\nu_{n_0}, n_0 P) \\ &= (\nu_{n_0} \cdot \lambda^{n_1}, n_0 P) \end{aligned} \tag{3.1}$$

by repeated applications of (2.2). Hence, evaluating $n(k,P)$ using this method essentially requires to compute λ, λ^{n_1} and $n_0(k,P)$. Of course, if several scalar multiples of the *same* element (k,P) need to be performed, then the value of λ may be precomputed in order to speed up the computations. We have therefore shown:

Lemma 2. *Let E be a smooth elliptic curve defined over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order l and $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus, where M and N are distinct points of $E(\mathbb{F}_{q^r})$. For $(k,P) \in \mathbb{F}_{q^r}^* \times \langle B \rangle$ and a non-negative integer n, let $n_0 = n \bmod l$, $n_1 = \lfloor n/l \rfloor$, $l(k,P) = (\lambda, \mathcal{O})$ and $n_0(k,P) = (\nu_{n_0}, n_0 P)$. Then,*

$$n(k,P) = (\nu_{n_0} \cdot \lambda^{n_1}, n_0 P).$$

Notice that this simple equality in fact relates three instances of the discrete logarithm problem in three different groups, namely a generalized Jacobian, an elliptic curve and a finite field. Next we see how this observation provides a natural solution to compute discrete logarithms in $\mathbb{F}_{q^r}^* \times \langle B \rangle$. The goal of this exercise is to give an upper bound on the overall complexity of this problem.

So given $(k,P) \in \mathbb{F}_{q^r}^* \times \langle B \rangle$ and an element (j,Q) in the subgroup generated by (k,P), we need to determine the least non-negative integer n such that $n(k,P) = (j,Q)$. Using the above notations, first notice that knowing n is equivalent to knowing both n_0 and n_1 (since l is public and $n = n_1 l + n_0$), where $0 \leq n < \mathrm{ord}(\lambda) \cdot l$, $0 \leq n_0 < l$ and $0 \leq n_1 < \mathrm{ord}(\lambda)$. Lemma 2 then yields

$$(j,Q) = n(k,P) = (\nu_{n_0} \cdot \lambda^{n_1}, n_0 P).$$

Thus, given the values of

$$j = \nu_{n_0} \cdot \lambda^{n_1} \text{ and } Q = n_0 P,$$

our task is to recover n. Observe that Q is independent of n_1 while j depends on both n_0 and n_1.

The obvious strategy is then to start by solving an instance of the discrete logarithm problem in E in order to recover n_0 from $Q = n_0 P$. Once n_0 is known, the value of ν_{n_0} can be easily computed, as $n_0(k,P) = (\nu_{n_0}, n_0 P)$. Next derive the value of λ^{n_1} by computing[2] $\nu_{n_0}^{-1} \cdot j$. Then recover n_1 by extracting the discrete logarithm of λ^{n_1} to the base λ. At last, set $n = n_1 l + n_0$. Figure 2 illustrates this sequence of computations while the following proposition summarizes the result just obtained.

Proposition 1. *Let E be a smooth elliptic curve defined over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order l and $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus, where M and N are distinct points of $E(\mathbb{F}_{q^r})$. Then, the discrete logarithm problem in any cyclic*

[2]Notice that $\nu_{n_0} \neq 0$ since by construction, $\nu_{n_0} \in \mathbb{F}_{q^r}^*$.

subgroup of $\mathbb{F}_{q^r}^* \times \langle B \rangle$ *is no harder than* ***sequentially*** *solving a discrete logarithm in* E *followed by one in* $\mathbb{F}_{q^r}^*$.

$\mathbb{F}_{q^r}^*$	E
	$n_0 P$
	$\downarrow$
	n_0
	$\downarrow$
$\nu_{n_0} \cdot \lambda^{n_1}$	ν_{n_0}
$\downarrow$	
λ^{n_1}	
$\downarrow$	
n_1	

FIGURE 2. Natural solution to a DLP in the generalized Jacobian

Informally speaking, the next step is to ask whether it is possible to find a quicker way to solve this DLP. In particular,

- *If we know how to solve the DLP in* $\mathbb{F}_{q^r}^* \times \langle B \rangle$*, do we necessarily know how to solve it in* E*?*
- *If we know how to solve the DLP in* $\mathbb{F}_{q^r}^* \times \langle B \rangle$*, do we necessarily know how to solve it in* $\mathbb{F}_{q^r}^*$*?*
- *Is it possible to solve a DLP in* $\mathbb{F}_{q^r}^* \times \langle B \rangle$ *by solving one in* E *and one in* $\mathbb{F}_{q^r}^*$ *in* ***parallel****?*
- *Can some precomputations be made in order to speed up the extraction of a DL in* $\mathbb{F}_{q^r}^* \times \langle B \rangle$*?*

The remainder of this paper focuses on the first three questions, while a discussion around the last question can be found in [2, Section 5.5.3].

4. Reductions among Discrete Logarithm Problems

To ease the exposition, we will assume throughout this section that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic subgroup of $J_{\mathfrak{m}}$ generated by (k, P). In short, the goal is now to show that any given algorithm that solves DLPs in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ may be used as a subroutine to solve DLPs in E as well as in $\mathbb{F}_{q^r}^*$. In other words, if anyone ever discovers an efficient way to solve DLPs in $\mathbb{F}_{q^r}^* \times \langle B \rangle$, he or she could use it to efficiently solve instances of the DLP in E and in $\mathbb{F}_{q^r}^*$.

Since we are concerned in this section with lower bounds on the difficulty of solving the DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$, the proofs we provide here are written formally in order to be as rigorous as possible. For completeness, a review of fundamental properties of discrete logarithms needed to prove these results is included in the appendix.

Proposition 2. *Let* E *be a smooth elliptic curve over* $\mathbb{F}_q$*,* $B \in E(\mathbb{F}_q)$ *be a point of prime order* l*,* $\mathfrak{m} = (M) + (N)$ *be a* B*-unrelated modulus, where* M *and* N *are distinct points of* $E(\mathbb{F}_{q^r})$ *such that* $\mathbb{F}_{q^r}^* \times \langle B \rangle$ *is a cyclic subgroup of* $J_{\mathfrak{m}}$*. Then, the discrete logarithm problem in* $\mathbb{F}_{q^r}^* \times \langle B \rangle$ *is at least as hard as the discrete logarithm problem in* $\langle B \rangle \subseteq E(\mathbb{F}_q)$*.*

Proof. Let $\mathcal{A}_{J_\mathfrak{m}}$ be an algorithm having a non-negligible probability of solving discrete logarithms in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ to the base (k, P), where (k, P) is a generator of $\mathbb{F}_{q^r}^* \times \langle B \rangle$. We wish to show that there is an algorithm $\mathcal{A}_E$ having a non-negligible probability of solving discrete logarithms in $\langle B \rangle$ to the base P. So let $Q = n_0 P$ be an instance of the discrete logarithm problem in $\langle B \rangle$, where $0 \leq n_0 < l$. By the random self-reducible property of discrete logarithms[3], we can assume without loss of generality that given *any* element of $\mathbb{F}_{q^r}^* \times \langle B \rangle$, its discrete logarithm (to the base (k, P)) has a non-negligible probability of being obtained with $\mathcal{A}_{J_\mathfrak{m}}$. Now, for a randomly chosen element $j \in \mathbb{F}_{q^r}^*$, invoke $\mathcal{A}_{J_\mathfrak{m}}$ on input (j, Q). With non-negligible probability, a non-negative integer n such that $n(k, P) = (j, Q)$ will be obtained, yielding $n_0 = n \bmod l$. □

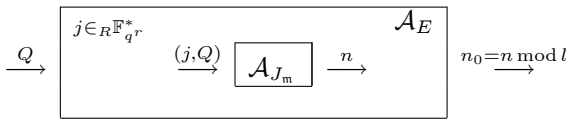

FIGURE 3. Converting an instance of the DLP in $\langle B \rangle$ into one in $\mathbb{F}_{q^r}^* \times \langle B \rangle$

Next we show a similar reduction from the discrete logarithm problem in $\mathbb{F}_{q^r}^*$ to the one in $\mathbb{F}_{q^r}^* \times \langle B \rangle$.

Proposition 3. *Let E be a smooth elliptic curve over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order l, $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus, where M and N are distinct points of $E(\mathbb{F}_{q^r})$ such that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic subgroup of $J_\mathfrak{m}$. Then, the discrete logarithm problem in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is at least as hard as the discrete logarithm problem in $\mathbb{F}_{q^r}^*$.*

Proof. Let $\mathcal{A}_{J_\mathfrak{m}}$ be an algorithm having a non-negligible probability of solving discrete logarithms in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ to the base (k, P), where (k, P) is a generator of $\mathbb{F}_{q^r}^* \times \langle B \rangle$. We want to show the existence of an algorithm $\mathcal{A}_{\mathbb{F}_{q^r}^*}$ having a non-negligible probability of solving discrete logarithms in $\mathbb{F}_{q^r}^*$ to the base λ, where $l(k, P) = (\lambda, \mathcal{O})$. Recall that by (2.4), λ must generate all of $\mathbb{F}_{q^r}^*$ since (k, P) is a generator of $\mathbb{F}_{q^r}^* \times \langle B \rangle$. Thus let $h = \lambda^n$ be an instance of the discrete logarithm problem in $\mathbb{F}_{q^r}^*$, with $0 \leq n < q^r - 1$. As usual, thanks to the random self-reducible property, we can assume without loss of generality that given *any* element of $\mathbb{F}_{q^r}^* \times \langle B \rangle$, its discrete logarithm (to the base (k, P)) has a non-negligible probability of being obtained with $\mathcal{A}_{J_\mathfrak{m}}$. Invoking $\mathcal{A}_{J_\mathfrak{m}}$ on input $(h, \mathcal{O})$ will yield with non-negligible probability an integer a satisfying $(h, \mathcal{O}) = a(k, P)$ and $0 \leq a < (q^r - 1) l$. We have in particular that $aP = \mathcal{O}$, which implies that a must be divisible by l. There is thus an integer b such that $a = b \cdot l$ and $0 \leq b < (q^r - 1)$. As a result,

$$(\lambda^n, \mathcal{O}) = (h, \mathcal{O}) = a(k, P) = bl(k, P) = b(\lambda, \mathcal{O}) = (\lambda^b, \mathcal{O}),$$

which yields $n = b$. □

As a result, the two propositions of this section imply that even though generalized Jacobians are newcomers in cryptography, we already know that solving their

[3]This property is described in the appendix.

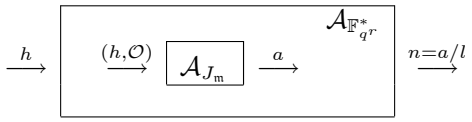

FIGURE 4. Converting an instance of the DLP in $\mathbb{F}_{q^r}^*$ into one in $\mathbb{F}_{q^r}^* \times \langle B \rangle$

DLP cannot be easier than solving discrete logarithms in two of the most studied groups used in DL-based cryptography today.

5. A Parallel Solution à la Pohlig-Hellman

Now that we have strong evidences that the discrete logarithm problem in the generalized Jacobians we consider is a computationally difficult problem, we further investigate the natural solution proposed in Section 3. Recall that Proposition 1 showed that an instance of the DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ can be solved by sequentially extracting a discrete logarithm in E followed by one in $\mathbb{F}_{q^r}^*$. We next try to determine under which circumstances the DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ could be performed any faster.

For simplicity, we will also assume here that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic subgroup of $J_\mathfrak{m}$ generated by (k, P). As usual, let $(j, Q) = n(k, P)$ be an instance of the DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ to be solved, where $0 \leq n < (q^r - 1)\, l$. By Lemma 2, we know that

$$(j, Q) = n(k, P) = (\nu_{n_0} \cdot \lambda^{n_1}, n_0 P), \tag{5.1}$$

where we keep the notation $n = n_1 l + n_0$, $0 \leq n_0 < l$, $0 \leq n_1 < q^r - 1$ as well as $l(k, P) = (\lambda, \mathcal{O})$ and $n_0(k, P) = (\nu_{n_0}, n_0 P)$. Notice that the sequential solution of Section 3 performs computations involving $j = \nu_{n_0} \cdot \lambda^{n_1}$ *only* once ν_{n_0} is known, as depicted in Figure 2.

We could instead attempt to extract a discrete logarithm in $\mathbb{F}_{q^r}^*$ in *parallel* with the one in the elliptic curve. On one hand, using (5.1), one can start to solve $Q = n_0 P$ for n_0 by extracting a discrete logarithm in E. In the meantime, we could also start to extract a discrete logarithm in the finite field as follows. This time, let

$$n_2 = n \bmod (q^r - 1)\,.$$

Then compute $l\,(j, Q)$ which will equal, say, $(j', \mathcal{O})$. We now have:

$$(j', \mathcal{O}) = l\,(j, Q) = l \cdot n\,(k, P) = n \cdot l\,(k, P) = n\,(\lambda, \mathcal{O}) = (\lambda^n, \mathcal{O}) = (\lambda^{n_2}, \mathcal{O})\,.$$

Since j' and λ are known, we can then solve the following DLP in $\mathbb{F}_{q^r}^*$ in order to get n_2:

$$j' = \lambda^{n_2}.$$

Remark that this can be done in *parallel* with the computation of n_0.

Finally, try to combine n_0 and n_2 using the Chinese remainder theorem in order to recover n. However, we *must* have $\gcd(l, q^r - 1) = 1$ to fully recover n with this method. We summarize this observation below.

Proposition 4. *Let E be a smooth elliptic curve over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order l and $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus, where M and N are distinct points of $E(\mathbb{F}_{q^r})$. If $l \nmid (q^r - 1)$, then the discrete logarithm problem in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is no harder than solving a discrete logarithm in E and one in $\mathbb{F}_{q^r}^*$ in* ***parallel****.*

Remark 2. Notice that in this proposition, there is no need to add the hypothesis that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ must be a cyclic group. Indeed, as mentioned in Section 2, the condition $l \nmid (q^r - 1)$ already ensures that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ will be cyclic.

6. Generalized Jacobians of Pairing-friendly Curves

We now turn our attention to the case $l \mid (q^r - 1)$, and thus to pairing-friendly curves. Recall that we now know several techniques allowing to efficiently generate suitable curves for various values of r of cryptographic interest. A thorough classification of these methods was recently made by Freeman, Scott and Teske [5].

An interesting case arises when we work in a cyclic subgroup $\langle (k, P) \rangle \subseteq \mathbb{F}_{q^r}^* \times \langle B \rangle$ of order $d \cdot l^\alpha$, where $\alpha \geq 2$ and $l \nmid d$. Indeed, we will see here that the natural solution of Section 3 is then still faster than a straightforward application of the ideas of Pohlig and Hellman. It therefore seems that the DLP in generalized Jacobians of pairing-friendly curves can behave distinctly.

Remark 3. Recall that the MOV attack [7] allows in this case to reduce the DLP in $\langle B \rangle \subseteq E(\mathbb{F}_q)$ to the DLP in $\mathbb{F}_{q^r}^*$, thanks to the Weil pairing. Thus for pairing-based applications, the embedding degree r is usually chosen such that these two DLPs are (roughly) of equal difficulty. We shall assume that this also holds here, so that there is no practical advantage of transforming an instance of the DLP in the elliptic curve into one in the finite field.

Just as before, let $(j, Q) = n\,(k, P)$ be the instance of the DLP we wish to solve. In order to use the Chinese remainder theorem to recover n, we now compute

$$\begin{cases} n_\alpha := n \bmod l^\alpha \\ n_d := n \bmod d \end{cases}.$$

This can be achieved as follows.

(1) We here want to compute n_d. To do so, first evaluate $l^\alpha\,(j, Q)$, which will equal, say, $(j', \mathcal{O})$. Now,

$$\begin{aligned}(j', \mathcal{O}) = l^\alpha\,(j, Q) = l^\alpha n\,(k, P) = nl^{\alpha-1} \cdot l\,(k, P) \\ = nl^{\alpha-1}\,(\lambda, \mathcal{O}) = \left(\left(\lambda^{l^{\alpha-1}}\right)^n, \mathcal{O}\right) = \left(\left(\lambda^{l^{\alpha-1}}\right)^{n_d}, \mathcal{O}\right),\end{aligned}$$

which means that

$$j' = \left(\lambda^{l^{\alpha-1}}\right)^{n_d},$$

where j' and $\lambda^{l^{\alpha-1}}$ are known. It thus suffices to solve a DLP in $\mathbb{F}_{q^r}^*$ in order to recover n_d.

(2) While performing Step 1, we can also start to determine n_α in parallel.
   (a) First let $n_0 = n \bmod l$ $(= n_\alpha \bmod l)$. Since $(j, Q) = n\,(k, P) = (*, nP) = (*, n_0 P)$, we have $Q = n_0 P$. The value of n_0 can thus be obtained by solving a DLP in the elliptic curve[4].
   (b) Next we compute

$$n_1 = \frac{n - n_0}{l} \bmod l.$$

[4]Notice that we have now retrieved *all* the information about n that Q contained. That is, we should expect that *all* other discrete logs that we have to solve from this point on will be in the finite field $\mathbb{F}_{q^r}^*$.

To do so, write n as $n_0 + n_1 l + m l^2$ for some (unknown) integer m and compute $dl^{\alpha-2}(j, Q)$ to get, say, $\left(j'', dl^{\alpha-2}Q\right)$. Then,

$$\begin{aligned}\left(j'', dl^{\alpha-2}Q\right) &= dl^{\alpha-2}(j, Q) = dl^{\alpha-2} \cdot n(k, P) \\ &= dl^{\alpha-2}\left(n_0 + n_1 l + m l^2\right)(k, P) \\ &= dl^{\alpha-2} n_0 (k, P) + n_1 dl^{\alpha-2} \cdot l(k, P) + m \cdot dl^{\alpha}(k, P) \\ &= dl^{\alpha-2}(\nu_{n_0}, n_0 P) + n_1 dl^{\alpha-2}(\lambda, \mathcal{O}) + m(1, \mathcal{O}) \\ &= \left(\left(\nu_{n_0}\right)^{dl^{\alpha-2}} \cdot \mu, dl^{\alpha-2}Q\right) + \left(\left(\lambda^{dl^{\alpha-2}}\right)^{n_1}, \mathcal{O}\right) \\ &= \left(\left(\nu_{n_0}\right)^{dl^{\alpha-2}} \cdot \mu \cdot \left(\lambda^{dl^{\alpha-2}}\right)^{n_1}, dl^{\alpha-2}Q\right),\end{aligned}$$

where μ is simply the product of the 2-cocycles from repeated applications of the group law. Notice that μ can be computed directly from Q and $dl^{\alpha-2}$. It therefore follows that

$$\frac{j''}{\mu \cdot \left(\nu_{n_0}\right)^{dl^{\alpha-2}}} = \left(\lambda^{dl^{\alpha-2}}\right)^{n_1},$$

where the only unknown is n_1. Thus, n_1 can be obtained by solving a DLP in $\mathbb{F}_{q^r}^*$.

(c) If $\alpha = 2$, then we are done since $n_\alpha = n_0 + n_1 l$. Otherwise, proceed to compute n_2 such that

$$n_2 = \frac{n - n_0 - n_1 l}{l^2} \bmod l,$$

and repeat this process for n_3, n_4, ..., $n_{\alpha-1}$. Finally, get $n_\alpha = n_0 + n_1 l + n_2 l^2 + ... + n_{\alpha-1} l^{\alpha-1}$.

(3) Combine n_d and n_α using the Chinese remainder theorem to get n.

The remarkable property of this method[5] is that *the value of ν_{n_0} is used to compute n_1*. This thus suggests that the value of n_0, obtained by solving a DLP in E, should be known prior to the computation of n_1. In other words, to compute n_α, the discrete logarithm in the elliptic curve should be performed *first*, and be followed by discrete logarithm(s) in $\mathbb{F}_{q^r}^*$.

Therefore, the natural solution of Section 3 is still preferable to the above method *à la* Pohlig-Hellman in the case of pairing-friendly curves. In particular, we are left with the following open question.

Question. Let E be a smooth elliptic curve defined over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order l and $\mathfrak{m} = (M) + (N)$ be a B-unrelated modulus, where M and N are distinct points of $E(\mathbb{F}_{q^r})$ such that $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is a cyclic subgroup of $J_\mathfrak{m}$. If $l \mid q^r - 1$, is it possible to solve a DLP in $\mathbb{F}_{q^r}^* \times \langle B \rangle$ significantly faster than with the sequential solution of Section 3?

7. Outlook

This paper was devoted to the study of the DLP in the simplest nontrivial generalized Jacobians of an elliptic curve. Thanks to the explicit equations for this group law from [3], it was not only possible to give an upper bound on the difficulty

[5] To the best of our knowledge, there is no version of the above process that allows to retrieve n_1 without computing n_0 first.

of this problem, but most importantly, to show that when $\mathbb{F}_{q^r}^* \times \langle B \rangle$ is cyclic, it is at least as hard as two well-studied computational problems, namely the DLP in elliptic curves and in finite fields.

As a result, the abelian group $\mathbb{F}_{q^r}^* \times \langle B \rangle$ in principle fulfills the four basic requirements for a group to be suitable for DL-based cryptography, as its elements are easily represented in a compact form, its group law is efficiently computable, its order is readily determined and its DLP is believed to be intractable.

This therefore shows that the family of generalized Jacobians that are suitable for cryptographic applications *strictly* contains algebraic tori and Jacobians of curves.

Acknowledgments. I would like to thank my thesis co-supervisors Henri Darmon and Claude Crépeau for their guidance and advices. I am also grateful to Edlyn Teske and Alfred Menezes, who always find time for me in their busy schedules.

References

[1] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 10(11):141–145, 1998.

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

[3] Isabelle Déchène. Arithmetic of Generalized Jacobians. In *Algorithmic Number Theory Symposium - ANTS VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 421–435. Springer-Verlag, 2006.

[4] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[5] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. `http://eprint.iacr.org/`.

[6] S. D. Galbraith and B. A. Smith. Discrete logarithms in generalized jacobians. Cryptology ePrint Archive, Report 2006/333, 2006. `http://eprint.iacr.org/`.

[7] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

[8] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press series on discrete mathematics and its applications. CRC Press, Boca Raton, 1996.

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

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

[11] 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.

[12] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Hermann, Paris, 1975.

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

Appendix: Properties of Discrete Logarithms

We here review fundamental properties of discrete logarithms in an arbitrary (multiplicatively written) cyclic group G of order n generated by an element g.

We begin with the *random self-reducible* property of discrete logarithms, which is based on the equality

$$g^a \cdot g^r = g^{a+r}. \tag{7.1}$$

We say that an algorithm $\mathcal{A}$ has a *non-negligible probability of solving the DLP in* G (to the base g) if for an input h uniformly chosen at random in G, there is a non-negligible probability[6] that $\mathcal{A}$ outputs $\log_g h$. But in practice, it is often desirable to learn the discrete logarithm of a *specific* element s of the group. It is however possible that the probability that $\mathcal{A}$ yields $a = \log_g s$ on input s equals zero[7]. The strategy is then to *disguise* s using (7.1). Indeed, if we uniformly pick an integer r in $\{0, 1, \ldots, n-1\}$, then

$$s \cdot g^r = g^a \cdot g^r = g^{a+r}.$$

Then notice that if r is uniformly selected, then so is $a + r$. So on input $s \cdot g^r$, there is now a non-negligible probability that $\mathcal{A}$ yields the value of $(a + r) \bmod n$. If so, then a can be recovered since r is known. Thus, $\mathcal{A}$ implies the existence of a randomized algorithm $\mathcal{A}'$ such that for *any* input $s \in G$, there is a non-negligible probability that $\mathcal{A}'$ outputs $\log_g s$.

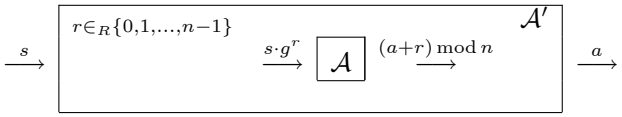

Figure 5. Constructing $\mathcal{A}'$ from $\mathcal{A}$

The second property concerns the choice of the generator of the group. Namely, if g_1 and g_2 are distinct generators of G, then any algorithm $\mathcal{A}_1$ that has a non-negligible probability of solving discrete logarithms in G to the base g_1 can readily be turned into an algorithm $\mathcal{A}_2$ having non-negligible probability of solving discrete logarithms in G to the base g_2.

Indeed, let $h = g_2^a$ be an instance of the DLP in G to be solved. By the random self-reducible property of discrete logarithms, we can assume without loss of generality that for any $s \in G$, $\mathcal{A}_1$ has a non-negligible probability of producing $\log_{g_1} s$. So first invoke $\mathcal{A}_1$ on input g_2 in order to get, with non-negligible probability, an integer b such that $g_2 = g_1^b$ and $0 < b < n$. Since g_1 and g_2 are both generators, it follows that $\gcd(n, b) = 1$, and so b is an invertible element of $\mathbb{Z}/n\mathbb{Z}$. Then compute an integer c such that $bc \equiv 1 \pmod n$ and $0 < c < n$ using, for instance, the extended Euclidean algorithm [8, Algorithm 2.107]. Then,

$$g_2^c = \left(g_1^b\right)^c = g_1^{bc} = g_1.$$

[6] That is, there is a polynomial p such that this probability is greater than $1/p(\log n)$.

[7] For instance, the algorithm could solve all instances for which the discrete logarithm is even, but fail otherwise.

Next, we can obtain with non-negligible probability an integer d such that $h = g_1^d$ and $0 \leq d < n$ by invoking $\mathcal{A}_1$ on input h. Finally,

$$h = g_1^d = (g_2^c)^d = g_2^{cd},$$

and so $a = cd \bmod n$, which completes the argument.

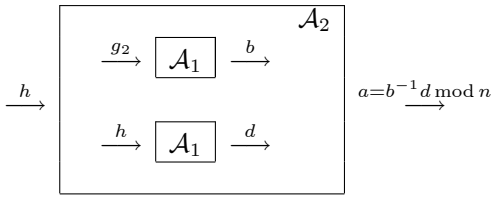

FIGURE 6. Constructing $\mathcal{A}_2$ from $\mathcal{A}_1$

DEPARTMENT OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA N2L 3G1

E-mail address: idechene@uwaterloo.ca