DISCRETE LOGARITHMS IN GENERALIZED JACOBIANS

S. D. GALBRAITH AND B. A. SMITH

Abstract. Déchène has proposed generalized Jacobians as a source of groups for public-key cryptosystems based on the hardness of the Discrete Logarithm Problem (DLP). Her specific proposal gives rise to a group extension of an elliptic curve by the multiplicative group of a finite field. We explain why her proposal has no advantages over simply taking the direct product of groups. We then argue that generalized Jacobians offer poorer security and efficiency per bit than standard Jacobians.

1. Introduction

Recently, Déchène [4] has proposed generalized Jacobians as a source of groups for public-key cryptosystems based on the hardness of the Discrete Logarithm Problem (DLP). Generalized Jacobians offer a natural generalization of both torus-based and curve-based cryptography.

Déchène's specific proposal gives rise to a group extension of an elliptic curve $\mathcal{E}(k)$ by the multiplicative group of a finite field, $\mathbb{G}_m(k)$. She remarks in Section 6 of [4] that the DLP in such a generalized Jacobian "is at least as hard as a DLP in $\mathcal{E}(k)$ and at least as hard as a DLP in $\mathbb{G}_m(k)$".

Our main observation follows from applying the standard Pohlig-Hellman reduction and therefore reducing to the case of elements of prime order. It then immediately follows (see Proposition 2.1) that one can solve the DLP in the generalized Jacobian by solving a number of DLPs in $\mathcal{E}(k)$ and $\mathbb{G}_m(k)$ in parallel. One concludes that the generalized Jacobian DLP is **at most** as hard as the DLP in $\mathcal{E}(k)$ and the DLP in $\mathbb{G}_m(k)$. As we will explain, one can get the same security with greater efficiency by simply taking the direct product $\mathcal{E}(k) \times \mathbb{G}_m(k)$.

In our presentation we consider the DLP in the simpler and more general setting of extensions of algebraic groups. We will argue that extensions offer no advantages over the existing Jacobian or torus constructions for DLP-based cryptography.

Throughout this article, we let k be a finite field. All varieties are nonsingular k-varieties. We say that a morphism of algebraic groups is *explicit* if it may be evaluated in polynomial time. Algebraic groups are said to be *explicitly isomorphic* if there is an explicit isomorphism between them. All algebraic groups in this article are commutative, and written additively. We denote algebraic groups with script letters and their underlying varieties with capital letters: so if $\mathcal{A}$ is an algebraic group, then A denotes its underlying variety.

2. Discrete Logarithms in Extensions of Commutative Algebraic Groups

Fix a pair of algebraic groups $\mathcal{A}$ and $\mathcal{B}$. An *extension* of $\mathcal{A}$ by $\mathcal{B}$ is an algebraic group $\mathcal{C}$ together with separable homomorphisms $\iota : \mathcal{B} \to \mathcal{C}$ and $\pi : \mathcal{C} \to \mathcal{A}$, all defined over k, such that the following sequence is exact:

$$0 \to \mathcal{B} \xrightarrow{\iota} \mathcal{C} \xrightarrow{\pi} \mathcal{A} \to 0.$$

We will assume that the maps ι, π, and ι^{-1} (where it is defined) are explicit. A trivial example of an extension of $\mathcal{A}$ by $\mathcal{B}$ is the direct product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, with ι and π the obvious maps. The motivating example for this work is the case where $\mathcal{C}$ is a generalized Jacobian: here $\mathcal{A}$ is the Jacobian of an algebraic curve, $\mathcal{B}$ is a certain affine algebraic group,[1] and the group structure of

[1] The algebraic group in question is isomorphic to a product of multiplicative groups (i.e. a torus), together with a product of Witt groups (in which the DLP is trivial).

$\mathcal{C}$ is determined by a map $c_{\mathfrak{m}} : \mathcal{A}^2 \to \mathcal{B}$. The generalized Jacobians proposed for cryptography by Déchène are the special case where $\mathcal{A}$ is an elliptic curve and $\mathcal{B}$ is the multiplicative group.

We wish to assess the suitability of $\mathcal{C}$ as a source of groups for cryptography, compared with $\mathcal{A}$ and $\mathcal{B}$. Suppose we wish to solve a DLP in a subgroup $\mathcal{G}$ of $\mathcal{C}(k)$. The group $\mathcal{G}$ is necessarily finite, and without loss of generality we may assume that $\mathcal{G}$ is cyclic. By the standard reduction of Pohlig and Hellman [7], we may reduce to the case where the order of $\mathcal{G}$ is prime.

Proposition 2.1. *Let $\mathcal{G}$ be a subgroup of $\mathcal{C}(k)$, of prime order l. If $\mathcal{G}$ is contained in $\iota(\mathcal{B})$, then the DLP in $\mathcal{G}$ reduces to the DLP in a subgroup of order l in $\mathcal{B}(k)$. Otherwise, the DLP in $\mathcal{G}$ reduces to the DLP in a subgroup of order l in $\mathcal{A}(k)$.*

Proof. If $\mathcal{G}$ is a subgroup of $\iota(\mathcal{B})$, then it is explicitly isomorphic to the subgroup $\iota^{-1}(\mathcal{G})$ of $\mathcal{B}(k)$. Otherwise, $\mathcal{G}$ has trivial intersection with the kernel of π, so it is explicitly isomorphic to the subgroup $\pi(\mathcal{G})$ of $\mathcal{A}(k)$. □

Corollary 2.2. *The DLP in $\mathcal{C}(k)$ is no harder than the hardest DLP in $\mathcal{A}(k)$ and $\mathcal{B}(k)$.*

Proposition 2.1 shows that if $\mathcal{G}$ is not contained in $\iota(\mathcal{B})$, then the DLP in $\mathcal{G}$ reduces to the DLP in $\mathcal{A}(k)$. It is important to note that the absence of a natural projection from $\mathcal{C}$ to $\mathcal{B}$ does *not* preclude the existence of a homomorphism mapping $\mathcal{G}$ into $\mathcal{B}$; thus the DLP in $\mathcal{G}$ may, in some cases, be reduced to the DLP in $\mathcal{B}(k)$ as well. For many subgroups $\mathcal{G}$, therefore, the DLP in $\mathcal{G}$ is only as hard as the easier of the DLP in $\mathcal{A}(k)$ and the DLP in $\mathcal{B}(k)$. This means that we can have a relative loss in security in using extensions of $\mathcal{A}$ by $\mathcal{B}$ rather than using $\mathcal{A}$ and $\mathcal{B}$ independently.

Remark 2.3. Couveignes [2] shows that if $\mathcal{C}$ is a commutative algebraic group extension of $\mathcal{A}$ by $\mathcal{B}$, then there exists an algorithm to solve the DLP in $\mathcal{C}$ in subexponential time in the size of $\mathcal{C}$ if and only if there exists such algorithms for $\mathcal{A}$ and for $\mathcal{B}$ [2, Theorem 2]. This is due to the existence of a k-rational isogeny (not constructed in [2]) from $\mathcal{C}$ to the direct product $\mathcal{A} \times \mathcal{B}$.

3. Extensions Presented by Cocycles

Extensions $\mathcal{C}$ of $\mathcal{A}$ by $\mathcal{B}$ are effectively determined by the choice of a symmetric 2-cocycle (*cocycle* in the sequel): that is, a map $c : \mathcal{A}^2 \to \mathcal{B}$ satisfying the relations

$$c(P,Q) + c(P+Q,R) = c(Q,R) + c(P,Q+R) \quad \text{and} \quad c(P,Q) = c(Q,P) \tag{1}$$

for all P, Q and R in $\mathcal{A}$. Note that c is *not* required to be a homomorphism.

Given a cocycle $c : \mathcal{A}^2 \to \mathcal{B}$, we construct an extension $\mathcal{C}$ of $\mathcal{A}$ by $\mathcal{B}$ as follows. The underlying variety of $\mathcal{C}$ is the direct product $A \times B$, the identity element is $(0_\mathcal{A}, 0_\mathcal{B})$, and the group law and inverse maps are the morphisms $m_c : (A \times B)^2 \to A \times B$ and $i_c : A \times B \to A \times B$ defined by

$$m_c : ((P_\mathcal{A}, P_\mathcal{B}), (Q_\mathcal{A}, Q_\mathcal{B})) \longmapsto (P_\mathcal{A} + Q_\mathcal{A}, P_\mathcal{B} + Q_\mathcal{B} + c(P_\mathcal{A}, Q_\mathcal{A}))$$

and

$$i_c : (P_\mathcal{A}, P_\mathcal{B}) \longmapsto (-P_\mathcal{A}, -P_\mathcal{B} + c(P_\mathcal{A}, -P_\mathcal{A}))$$

(here $+$ and $-$ denote group operations in $\mathcal{A}$ and $\mathcal{B}$). Note that associativity and commutativity follow from the relations (1) above. If $\mathcal{C}$ is an algebraic group with group elements represented as $A \times B$ and group law given as above then we say that $\mathcal{C}$ is *presented by the cocycle c*. Generalized Jacobians (for background, see [9]) are examples of extensions which can be presented by cocycles; we will give an example below. The direct product group $\mathcal{A} \times \mathcal{B}$ is the extension presented by the zero cocycle, sending each element of $\mathcal{A}^2$ to $0_\mathcal{B}$. Our assumption that ι and π are explicit holds in any extension presented by a cocycle, as shown by the following easy lemma.

Lemma 3.1. *Let $0 \to \mathcal{B} \xrightarrow{\iota} \mathcal{C} \xrightarrow{\pi} \mathcal{A} \to 0$ be an extension presented by a cocycle $c : \mathcal{A}^2 \to \mathcal{B}$.*

(1) *The injection $\iota : \mathcal{B} \to \mathcal{C}$ is given by $\iota(P) = (0_\mathcal{A}, P)$. The subgroups of $\mathcal{C}$ in the image of ι are precisely those of the form $\{(0_\mathcal{A}, P) : P$ in some subgroup of $\mathcal{B}\}$, and in such groups the map ι^{-1} given by $\iota^{-1}((0_\mathcal{A}, P)) = P$ reduces the DLP to a DLP in $\mathcal{B}$.*

(2) *The projection $\pi : \mathcal{C} \to \mathcal{A}$ is given by $\pi(P_\mathcal{A}, P_\mathcal{B}) = P_\mathcal{A}$. This map reduces the DLP in any subgroup of $\mathcal{C}$ not in the image of ι to a DLP in $\mathcal{A}$.*

Lemma 3.1 implies that the difficulty of the DLP in $\mathcal{C}$ cannot be increased by a "clever" choice of c. Indeed, each prime-order subgroup $\mathcal{G}$ of any extension $\mathcal{C}$ either projects faithfully into $\mathcal{A}$ or can be pulled back to $\mathcal{B}$. In particular, the DLP in any extension of $\mathcal{A}$ by $\mathcal{B}$ is no harder than the DLP in the direct product $\mathcal{A} \times \mathcal{B}$.

Suppose $\mathcal{C}$ is an extension presented by a cocycle $c : \mathcal{A}^2 \to \mathcal{B}$. Computing the group law in $\mathcal{C}$ requires the same computations as computing the group law in $\mathcal{A} \times \mathcal{B}$, together with an application of the cocycle c and an extra group operation in $\mathcal{B}$ — so computing the group law in $\mathcal{C}$ requires at least as much space and time as computing the group law in $\mathcal{A} \times \mathcal{B}$. Further, $\mathcal{C}$ and $\mathcal{A} \times \mathcal{B}$ have the same underlying variety, so representing their elements requires the same space. Thus computing in $\mathcal{C}$ requires at least as much time and space as computing in $\mathcal{A} \times \mathcal{B}$.

For the purposes of DLP-based cryptography, the group $\mathcal{A} \times \mathcal{B}$ offers no advantages over $\mathcal{A}$ and $\mathcal{B}$. We have seen that the DLP in $\mathcal{A} \times \mathcal{B}$ can be no harder than the hardest DLP in $\mathcal{A}$ or $\mathcal{B}$, and computing in $\mathcal{A} \times \mathcal{B}$ requires at least as much space and time as computing in $\mathcal{A}$ and $\mathcal{B}$ separately. Therefore, using $\mathcal{A} \times \mathcal{B}$ in a DLP-based cryptosystem in place of $\mathcal{A}$ or $\mathcal{B}$ offers no advantage in security, while requiring more storage space and computing time. Similarly, using an extension $\mathcal{C}$ presented by a cocycle $c : \mathcal{A}^2 \to \mathcal{B}$ instead of $\mathcal{A}$ or $\mathcal{B}$ alone offers no increase in security, since it has no larger prime-order subgroups than those already present in $\mathcal{A}$ and $\mathcal{B}$, while requiring at least as much time and space as computing in $\mathcal{A}$ and $\mathcal{B}$. We have thus derived the following result.

Proposition 3.2. *If $\mathcal{C}$ is an extension of $\mathcal{A}$ by $\mathcal{B}$ presented by a cocycle, then any DLP-based cryptosystem based on a subgroup of $\mathcal{C}(k)$*

- *is no more secure,*
- *takes more space, and*
- *is less computationally efficient*

than the analogous cryptosystem based on $\mathcal{A}(k)$ or $\mathcal{B}(k)$ (whichever has the harder DLP).

Example 3.3. In [3] and [4], Déchène proposes certain generalized Jacobians of elliptic curves as a supply of cryptographic groups. Suppose $\mathcal{E}$ is an elliptic curve over k, and let O be the identity of $\mathcal{E}$. Let $\mathbb{G}_m$ denote the multiplicative group over k (we will write its group law multiplicatively). Fix points M and N (neither equal to O) on $\mathcal{E}$; the effective divisor $\mathfrak{m} = (M) + (N)$ is called the *modulus*. The generalized Jacobian $\mathcal{J}_{\mathcal{E},\mathfrak{m}}$ is defined to be the extension of $\mathcal{E}$ by $\mathbb{G}_m$ presented by the cocycle $c_\mathfrak{m}(P, Q) = f_{P,Q}(M)/f_{P,Q}(N)$, where $f_{P,Q}$ is any function on E with divisor $(P + Q) + (O) - (P) - (Q)$.[2] The group law on $\mathcal{J}_{\mathcal{E},\mathfrak{m}}$ is then given by

$$(P, \lambda) + (Q, \mu) = (P + Q, \lambda \cdot \mu \cdot f_{P,Q}(M)/f_{P,Q}(N)).$$

We remark that this group law was also used in Section 3 of [5].

The observations of Proposition 3.2 all apply to $\mathcal{J}_{\mathcal{E},\mathfrak{m}}$. We know that the DLP in $\mathcal{J}_{\mathcal{E},\mathfrak{m}}(k)$ is no harder than the hardest DLP in $\mathcal{E}(k)$ and $\mathbb{G}_m(k)$. Thus using cyclic subgroups of $\mathcal{J}_{\mathcal{E},\mathfrak{m}}(k)$ instead of subgroups of $\mathcal{E}(k)$ or $\mathbb{G}_m(k)$ requires extra work, and extra space, for no gain in security. Indeed, it is widely recognised that elliptic curves give better security and performance than multiplicative groups of finite fields. Hence, it would be better either to remove the $\mathbb{G}_m(k)$ and use only $\mathcal{E}(k)$ (saving space and time), or spending the extra bits on a larger ground field K and using a prime order elliptic curve $\mathcal{E}(K)$ instead (maximizing security).

Remark 3.4. Déchène suggests taking M and N to be defined over a finite extension K/k, so that the cocycle $c_\mathfrak{m}$ maps $\mathcal{E}(k)^2$ into $\mathbb{G}_m(K)$, and such that both $\mathcal{E}(k)$ and $\mathbb{G}_m(K)$ contains a subgroup of prime order l. Balasubramanian and Koblitz [1] have shown that for general elliptic curves, the degree of the smallest such extension (called the *embedding degree*) tends to grow with l, rendering computation in $\mathbb{G}_m(K)$ and $\mathcal{G}$ exponentially difficult. In practice, therefore, the suggestion requires $\mathcal{E}$ to be a so-called *pairing-friendly* curve, which means there is a homomorphism from $\mathcal{E}$ to $\mathbb{G}_m$ as used in the Frey–Rück and MOV attacks [5, 6]. As a result, this suggestion requires special curves $\mathcal{E}$ and it is not usually advised to use such curves unless one is taking advantage of the extra functionality of pairing-based cryptography. In fact, as noted above, the generalised Jacobian

[2]We may take $f_{P,Q} = v/l$, where l is the line through P and Q, and v is the vertical line through the third point of intersection of l with E.

group law is the same as the method proposed by [5] for computing the Tate pairing (except the function is inverted). Hence, if m is the least common multiple of the order of P and the order of $M - N$ in $\mathcal{E}(K)$, then computing m times $(P, 1)$ gives $(0, \langle P, M - N\rangle_m^{-1})$.

4. A practical example

Suppose one wants a group for cryptography such that solving the discrete logarithm problem requires at least 2^{80} operations. There are two natural solutions:

(1) One can use an elliptic curve of prime order over a finite field of size roughly 160 bits (or, more generally, the divisor class group of a hyperelliptic curve of genus 2 or 3).
(2) One can use a subgroup of prime order $l \approx 2^{160}$ of the torus $T_6(\mathbb{F}_q)$ over a field $\mathbb{F}_q$ where $q \approx 2^{170}$ (see [8] for a survey on tori).

Using point compression, the first solution requires roughly 160 bits to represent group elements and solving the discrete logarithm problem requires at least 2^{80} elliptic curve operations. This is essentially optimal. Elements of the torus $T_6(\mathbb{F}_q)$ are represented by two field elements, so require roughly 340 bits storage. It is believed that the discrete logarithm problem in such a group requires computation similar to the cost for the first solution.

One could take a group extension of an elliptic curve by $T_6(\mathbb{F}_q)$ using Déchène's method (to perform the group operations one must first decompress elements of $T_6(\mathbb{F}_q)$ to get elements in $\mathbb{F}_{q^6}^*$). Elements of the generalized Jacobian now require 500 bits to store and yet solving the DLP of a prime order element still takes 2^{80} operations. Hence, the the per-bit security of generalized Jacobians is much lower than elliptic curves.

Acknowledgements

We thank Isabelle Déchène for comments on the first draft of this paper.

References

[1] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm, *J. Cryptology* **11** (1998), 141–145.
[2] J.-M. Couveignes, Algebraic groups and discrete logarithms, in *Public-Key Cryptography and Computational Number Theory*, K. Alster, J. Urbanowicz, and H. C. Williams (editors), Walter De Gruyter, 2001.
[3] I. Déchène, *Generalized Jacobians in cryptography*, Ph.D. thesis, McGill University, 2005.
[4] I. Déchène, Arithmetic of generalized Jacobians, in F. Hess et al (eds.), ANTS VII, Springer LNCS 4076 (2006) 421–435.
[5] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.* **62** (1994) 865–874.
[6] A. J. Menezes, T. Okamoto, and S. A. Vanstone, Reducing elliptic curve logarithms to a finite field, IEEE Trans. Inf. Theory **39** (1993), 1639–1646.
[7] 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.
[8] K. Rubin and A. Silverberg, Using primitive subgroups to do more with fewer bits, in D. Buell (ed.), ANTS VI, Springer LNCS 3076 (2004) 18–41.
[9] J.-P. Serre, *Algebraic groups and class fields* , Graduate Texts in Mathematics **117**, Springer, 1997.

Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0EX, UK.
E-mail address: Steven.Galbraith@rhul.ac.uk, Ben.Smith@rhul.ac.uk