Index Calculus Attacks on Hyperelliptic Jacobians with Effective Endomorphisms

Sulamithe Tsakou and Sorina Ionica

Laboratoire MIS, Université de Picardie Jules Verne, Amiens, France
{sulamithe.tsakou, sorina.ionica}@u-picardie.fr

Abstract. For a hyperelliptic curve defined over a finite field $\mathbb{F}_{q^n}$ with $n > 1$, the discrete logarithm problem is subject to index calculus attacks. We exploit the endomorphism of the curve to reduce the size of the factorization basis and hence improve the complexity of the index calculus attack for certain families of ordinary elliptic curves and genus 2 hyperelliptic Jacobians defined over finite fields. This approach adds an extra cost when performing operation on the factor basis, but the experiences show that reducing the size of the factor basis allows to have a gain on the total complexity of index calculus algorithm with respect to the generic attacks.

Keywords: Discrete Logarithm Problem · Index Calculus · Endomorphism.

1 Introduction

The security of many public key cryptographic implementations relies on the difficulty of solving the discrete logarithm problem in the Jacobian of a hyperelliptic curve. In a general setting, this problem is stated as follows: given a finite cyclic group G generated by g and an element $h \in G$, find an integer k such that $h = kg$. In this paper, we take G to be the group of rational points of an elliptic curve E defined over a finite field $\mathbb{F}_{q^n}$ or the Jacobian $J(H)$ of a hyperelliptic curve H of genus $g > 1$ defined over $\mathbb{F}_{q^n}$.

In a generic group, the discrete logarithm problem can be solved by using Pollard's rho algorithm or the baby-step-giant-step algorithm. When the group is known to have a certain algebraic structure, this may be exploited to improve the performance of generic algorithms. For instance, Duursma, Gaudry, Morain [8] used the automorphisms of the curve to speed up Pollard's rho method on elliptic curves and Jacobians of hyperelliptic curves. Another example is that of elliptic curves defined over extension fields, where the index calculus method yields a faster attack than generic algorithms. Once a convenient factor basis on the curve is decided, the index calculus algorithm has three steps: the collection of relations in which a random point is decomposed as sum of points in the factor basis, the linear algebra step and the descent phase in which the discrete logarithm of h is deduced. The choice of the factor basis depends on the curve and its field of definition. The complexity of the algorithm crucially depends on the size of the factor basis, since this determines the probability for a point to be decomposed over the basis and also the cost of the linear algebra step.

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$. In [7, 18], the authors suggest, if q is a large prime and n small, to take the factor basis as :

$$\mathcal{F} = \{P \in E : x(P) \in \mathbb{F}_q\} \tag{1}$$

which has approximately q elements. Defining the factor basis like Gaudry does, a natural observation is that $-P \in \mathcal{F}$ whenever $P \in \mathcal{F}$. So, one can construct the equivalence class $\{P, -P\}$ in the factor basis and thus reduce its size by a factor 2. Going further in this direction, the authors of [11, 12, 15] exploit small torsion points to reduce the size of the factor basis.

We generalize the reduction of the factor basis based on the use of the automorphism $[-] : P \mapsto -P$ by considering an efficient computable endomorphism ϕ of the curve whose action on the basis is closed (i.e. $\phi(P) \in \mathcal{F}$ for all $P \in \mathcal{F}$). This allows us to consider equivalence classes of larger size than those proposed by Gaudry. We focus on ordinary elliptic curves and hyperelliptic curves of genus greater than 1 defined over finite fields with small characteristic and on GLV, GLS and GLV-GLS families of hyperelliptic curves. In the relation search step of the index calculus algorithm, each time a point decomposition is computed, we obtain a new line in the matrix of relations whose coefficients are powers of the eigenvalue of the endomorphism. Along the way, for elliptic curves with rational 2-torsion, we show that our definition of equivalent classes on the factor basis is compatible to the one in [12], resulting into an improved algorithm for some of these curves as well. We implemented this decomposition algorithm using the computer algebra system MAGMA [3] and obtained a speed up factor close to the size of our equivalence classes.

Our work is organized as follows: In Section 2, we recall the background on the index calculus on elliptic curves. In Section 3, we present our reduction on the size of the factor basis for elliptic curves defined over $\mathbb{F}_{q^n}$, $q \geq 2$ and the additional cost of the look up in equivalence class. In Section 4 we show a similar approach for hyperelliptic curves. In Section 5 we briefly describe our MAGMA implementation on elliptic curves defined over extension fields of composite degree, on binary hyperelliptic curves of genus greater than 1 defined over a prime degree extension fields and show benchmarks for our experiments.

2 Background on index calculus

We recall here the principle of the index calculus algorithm as presented in [18]. Consider a finite additive group G of prime order r and 2 elements $h, g \in G$. Our goal is to find an integer k such that $h = kg$. The index calculus algorithm consists of 4 main steps:

1. The computation of a convenient factor basis $\mathcal{F} = \{g_1, g_2, \cdots, g_N\}$ consisting of some elements of G which generate whole G.

2. The relation collection: Choose random integers α_i modulo r and try to decompose $[\alpha_i]g$ into the factor basis, that is, $[\alpha_i]g = \sum_{j=1}^{N} \lambda_{i,j} g_j$. This equation is called a relation. The process is repeated until N relations are collected.

3. The linear algebra phase : Once N linearly independant relations were found, construct the vector $A = (\alpha_i)_{1 \leq i \leq N}$ and the matrix $M = (\lambda_{i,j})_{1 \leq i,j \leq N}$ and find a vector X such that $MX = A$. This vector contains all the logarithms of the basis elements with respect to g.

4. The descent phase : Choose random integers α and $\beta \neq 0$ and try to decompose $\alpha g + \beta h$ in the factor basis, i.e. $\alpha g + \beta h = \sum_{j=1}^{N} \lambda_j g_j$ and deduce the logarithm of h with respect to g. By taking $X = (x_1, x_2, \cdots, x_N)$, we get that $h = ((\sum_{j=1}^{N} \lambda_j x_j) - \alpha)\beta^{-1} g$.

Index calculus attack over an elliptic curve. We consider an elliptic curve E defined over the finite field $\mathbb{F}_{q^n}$. Let $G = \langle P \rangle$ the subgroup of $E(\mathbb{F}_{q^n})$ of order r, where r is the greatest prime divisor of the order N of E. For cryptographic purposes, $r \sim N$. To define the factor basis, we follow the approach in [12] which is useful for our purposes. Let $\mathbb{P}^1$ be the projective space. Consider the morphism

$$\begin{aligned} \mu :\ & E \to \mathbb{P}^1 \\ & P \mapsto \mu(P), \end{aligned} \tag{2}$$

defined over $\mathbb{F}_{q^n}$.

Definition 1. *We define the factor basis with respect to* μ *as*

$$\mathcal{F}_{E,\mu} = \{P \in E(\mathbb{F}_{q^n}) : \mu(P) \in \mathbb{F}_q\}.$$

To find a relation of the form

$$R = P_1 + P_2 + \cdots + P_n,$$

we use the so called Semaev's summation polynomial associated to the morphism μ, introduced in [12, Proposition 2].

The m^{th}-Semaev's summation polynomial $S_{m,\mu}$ associated to the morphism μ is a multivariate polynomial with coefficients in $\mathbb{F}_{q^n}$ such that given $P_1, P_2, \cdots, P_m \in E(\mathbb{F}_{q^n})$ we have

$$P_1 + P_2 + \cdots + P_m = 0 \iff S_{m,\mu}(\mu(P_1), \mu(P_2), \cdots, \mu(P_m)) = 0. \tag{3}$$

Example 1. Let E is defined by the equation $y^2 = x^3 + Ax + B$ defined over a finite field. When the morphism μ is defined by

$$\begin{aligned} x :\ & E \to \mathbb{P}^1 \\ & P \mapsto x(P), \end{aligned}$$

where $x(P)$ is the x-coordinate of the point P. Semaev's summation polynomial associated to x is given by:

1. $S_{2,x}(x_1, x_2) = x_1 - x_2$;
2. $S_{3,x}(x_1, x_2, x_3) = (x_1 - x_2)^2 x_3^2 - 2((x_1 + x_2)(x_1x_2 + A) + 2B)x_3 + ((x_1x_2 - A)^2 - 4B(x_1 + x_2))$;
3. $S_{n,x}(x_1, x_2, \cdots, x_n) = Res_x(S_{n-k,x}(x_1, \cdots, x_{n-k-1}, x), S_{k+2,x}(x_{n-k}, \cdots, x_n, x)$ for any $n \geq 4$ and $1 \leq k \leq n-3$.

Given $R \in E(\mathbb{F}_{q^n})$, the usual approach to find a relation $R = P_1 + P_2 + \cdots + P_n$ with $P_i \in \mathcal{F}$ is to solve the equation

$$S_{n+1,\mu}(\mu(P_1), \mu(P_2), \cdots, \mu(P_n), \mu(R)) = 0, \tag{4}$$

where $\mu(P_1), \mu(P_2), \cdots, \mu(P_n)$ are the unknowns. After replacing $\mu(R)$ by its value, we perform a Weil descent with respect to a vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and obtain a polynomial system of n equations and n unknowns which can be tackled using Gröbner basis algorithms [9, 10]. For a random morphism μ, the expected degree of $S_{n,\mu}$ in each of the variables is bounded by $(\deg \mu)^{n-1}$.

For completeness, we give an upper bound for the complexity of the Gröbner basis computation of the system $\mathcal{S} = \{f_1, f_2, \cdots, f_n\}$ that we obtain. Under the assumption that $\mathcal{S}$ is regular, the maximum degree of polynomials occurring during the computation of the Gröbner basis is bounded by the degree of regularity d_{reg} of the homogenized system, which in turn is smaller than the Macaulay bound $d = \sum_{i=1}^{n}(deg f_i - 1) + 1$.

Using the fact that the system $\mathcal{S}$ is composed of n polynomials of degree $(\deg \mu)^{n-1}$ in n variables, we have $d = n(\deg \mu)^{n-1} - n + 1$. The number of columns of the d-Macaulay matrix is at most the number of monomials of degree smaller than or equal to d which in our case is bounded by

$$\binom{d+n}{n} = \binom{n(\deg \mu)^{n-1} - n + 1 + n}{n} = \binom{n(\deg \mu)^{n-1} + 1}{n} \simeq \binom{n(\deg \mu)^{n-1}}{n}.$$

Then the complexity of computation of the Gröbner basis of the system $\mathcal{S}$ is in

$$\tilde{\mathcal{O}}\left(\binom{n(\deg \mu)^{n-1}}{n}^{\omega}\right),$$

where $\omega < 3$ is the complexity exponent of matrix multiplication. As n is negligible compared to $n2^{n-2}$ and using the Stirling's formula, we get:

$$\binom{n(\deg \mu)^{n-1}}{n} \sim \frac{(n(\deg \mu)^{n-1})^n}{n!} \sim (\deg \mu)^{n(n-1)} e^n (2\pi n)^{-1/2}.$$

Finally, the complexity of Gröbner basis computation is

$$\tilde{\mathcal{O}}\left(\left((\deg \mu)^{n(n-1)} e^n n^{-1/2}\right)^{\omega}\right), \tag{5}$$

where ω is the factor occurring in the complexity of matricial product. Consequently, to be able to solve the system resulting from Equation (4), Faugère *et al.* focus on the case where $\deg \mu = 2$.

3 Our contribution

Let $\mathbb{F}_{q^n}$ be a finite field, E an ordinary elliptic curve defined over $\mathbb{F}_{q^n}$, and $\#E(\mathbb{F}_{q^n}) = hr$, with h small and r a large prime number. For cryptographic applications, we work in the group $G = \langle P \rangle$, where P is an element of $E(\mathbb{F}_{q^n})$ of order r. If ϕ is an endomorphism of $E(\mathbb{F}_{q^n})$ and $\gcd(r, \#Ker(\phi)) = 1$, then $\phi(P)$ is also of order r. Since E is ordinary, $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_{q^n}}(E)$. This implies that $\phi(P) \in G$ and in particular, that there exists an integer β such that $\phi(P) = \beta P$.

We exhibit several examples of curves and endomorphisms ϕ with the property that if $P \in \mathcal{F}$, then $\phi(P) \in \mathcal{F}$. Then we construct an equivalence class $\{P, \phi(P), \phi^2(P), \cdots, \phi^{k-1}(P)\}$, where $k \in \mathbb{Z}$ will be chosen such that $\phi^k(P) = P$ for all $P \in \mathcal{F}$. By considering one representant of each equivalence class in the factor base, we reduce its size by a factor k.

Note that the eigenvalue β may be obtained by computing the roots of the characteristic polynomial of ϕ in $\mathbb{F}_r$. During the decomposition phase, whenever a relation $R = P_1 + P_2 + \ldots + P_m$ is computed, one searches first the representatives of the equivalence classes to which these points belong to. Let us denote these representatives by $\hat{P}_i$, $i = 1, \ldots, m$. Then by computing β^{j_i} such that $\phi^{j_i}(P_i) = \hat{P}_i = \beta^{j_i} P_i$, one modifies the matrix of relations by adding a line whose coefficients are β^{-j_i} for the columns corresponding to $\hat{P}_i$, $i = 1, \ldots, m$ and 0 otherwise. Note that this approach is effective as long as the size of the equivalence class is small, since computing the discrete logarithm value β^{j_i} by exhaustive search is costly otherwise. In all examples considered in this paper, k is of size $O(\log r)$.

Definition 2. *For a given endomorphism ϕ of E defined over a finite field $\mathbb{F}_{q^n}$ such that $\phi^k = \pm 1$ and a morphism $\mu : E \to \mathbb{P}_1$ such that $\mu(P) = \mu(-P)$ for $P \in E(\mathbb{F}_{q^n})$, we define respectively the trace and norm of μ with respect to ϕ :*

$$\begin{aligned} \mathrm{Tr}_\phi(\mu) : E &\to \mathbb{P}^1 \\ Q &\mapsto \mu(Q) + \mu(\phi(Q)) + \cdots + \mu(\phi^{k-1}(Q)). \end{aligned}$$

and

$$\begin{aligned} N_\phi(\mu) : E &\to \mathbb{P}^1 \\ Q &\mapsto \mu(Q) \cdot \mu(\phi(Q)) \cdot \cdots \cdot \mu(\phi^{k-1}(Q)). \end{aligned}$$

Lemma 1. *Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mu : E \to \mathbb{P}_1$ such that $\mu(P) = \mu(-P)$ for all points $P \in E(\mathbb{F}_{q^n})$ and $\phi : E \to E$ and endomorphism of E such that $\phi^k = \pm 1$. Consider $\mathrm{Tr}_\phi(\mu) : E \to \mathbb{P}^1$ the trace morphism with respect to ϕ. The factorization basis $\mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$ is invariant with respect to the endomorphism ϕ, i.e. for every point $Q \in E(\mathbb{F}_{q^n})$, $\phi(Q) \in \mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$ whenever $Q \in \mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$.*

Proof. Let $Q \in \mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$, i.e. $\mathrm{Tr}_\phi(\mu)(Q) \in \mathbb{F}_q$. We have that

$$\begin{aligned}\mathrm{Tr}_\phi(\mu)(\phi(Q)) &= \mu(\phi(Q)) + \mu(\phi^2(Q)) + \cdots + \mu(\phi^k(Q))\\ &= \mu(\phi(Q)) + \mu(\phi^2(Q)) + \cdots + \mu(Q) \quad (\text{since} \quad \phi^k \equiv \pm 1 \pmod r)\\ &= \mathrm{Tr}_\phi(\mu)(Q).\end{aligned}$$

Hence, $\mathrm{Tr}_\phi(\mu)(\phi(Q)) \in \mathbb{F}_q$ since $\mathrm{Tr}_\phi(\mu)(Q) \in \mathbb{F}_q$. Consequently, $\phi(Q) \in \mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$. The proof that $\mathcal{F}_{E,N_\phi(\mu)}$ is invariant under ϕ is similar. □

3.1 Curves defined over an extension field of composite degree

Let $\mathbb{F}_{q^n}$ be a finite field with $q \geq 2$ and $n = m_1 m_2$. Usually, m_1 is small (i.e. $m_1 \in \{2,3,4\}$) and m_2 is a large prime number. Let E be an ordinary elliptic curve defined over $\mathbb{F}_{q^{m_1}}$ and assume that $\#E(\mathbb{F}_{q^n}) = hr$, with h small and r a prime number. We would like to perform an index calculus attack in the group $E(\mathbb{F}_{q^n})$.

Note that the curve E admits a Frobenius endomorphism π_{m_1} defined by

$$\pi_{m_1} : P = (x,y) \mapsto \pi_{m_1}(P) = (x^{q^{m_1}}, y^{q^{m_1}}). \tag{6}$$

There exists an integer μ such that for all Q of order r in $E(\mathbb{F}_{q^n})$, $\pi_{m_1}(Q) = \mu Q$. The integer μ is a root of the characteristic polynomial χ_E of π_{m_1}, defined by:

$$\chi_E(T) = T^2 - tT + q^{m_1}, \tag{7}$$

where t is the trace of the Frobenius endomorphism.

To perform index calculus on the curve E, we define our factor base by $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_{q^{m_2}}\}$. We observe that, if $P = (x,y) \in \mathcal{F}$, then $\pi_{m_1}(P) = (x^{q^{m_1}}, y^{q^{m_1}}) \in \mathcal{F}$. In fact, $(x(\pi_{m_1}(P)))^{q^{m_2}} = (x^{q^{m_1}})^{q^{m_2}} = (x^{q^{m_2}})^{q^{m_1}} = x^{q^{m_1}} = x(\pi_{m_1}(P))$, since $x^{q^{m_2}} = x$. We conclude that, if $P \in \mathcal{F}$ then $\pi_{m_1}(P), \pi_{m_1}^2(P), \cdots, \pi_{m_1}^{m_2-1}(P)$ are also in $\mathcal{F}$ and we construct an equivalence class $\{P, \pi_{m_1}(P), \pi_{m_1}^2(P), \cdots, \pi_{m_1}^{m_2-1}(P)\}$. By putting only one representant of each equivalence class in the factor base, we reduce its size by a factor m_2.

This reduction applies for all elliptic curve defined over $\mathbb{F}_{q^n}$, with full 2-torsion defined over $\mathbb{F}_{q^{m_1}}$, and consequently to all isogeny classes containing such curves. Indeed, when the full 2-torsion is not defined over $\mathbb{F}_{q^{m_1}}$, the elliptic curve will be 2-isogenous to a curve having the full 2-torsion defined over $\mathbb{F}_{q^{m_1}}$. Using a heuristic assumption, there are only 2^{m_1} isogeny classes out of the $2^{n/2}$ isogeny classes of elliptic curves defined over $\mathbb{F}_{q^n}$ which are concerned by this reduction.

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{F}_{q^{m_1}}$. The complexity of the relation collection step in the index calculus algorithm in the group $E(\mathbb{F}_{q^n})$ with $n = m_1 m_2$ is*

$$\mathcal{O}\left((\frac{m_1!}{m_2} 2^{m_1(m_1-1)+m_2} e^{m_1} m_1^{-1/2})^{\omega} + m_1 2^{m_2} \right). \tag{8}$$

Proof. Here, we need to find $\frac{2^{m_2}}{m_2}$ relations. Recall that whenever a relation $Q = P_1 + P_2 + \ldots + P_{m_1}$ is computed, one searches first the representatives of the equivalence classes to which these points belong to. Since we need to do a look up in an equivalence class with m_2 elements for each point involved in a relation, the cost of search in an equivalence class is $m_1 m_2$. The probability of finding a decomposition of a random point $R \in E(\mathbb{F}_{2^n})$ in the factor basis is approximately

$$\frac{\#\mathcal{F}^{m_1}/\#S_{m_1}}{\#E(\mathbb{F}_{2^n})} \simeq \frac{(2^{m_2})^{m_1}/m_1!}{2^{m_2 m_1}} = \frac{1}{m_1!}.$$

So, the total cost of the relations search step in the index calculus algorithm is

$$\mathcal{O}(\frac{2^{m_2}}{m_2} m_1! + 2^{m_2} m_1),$$

where A is the complexity of solving a polynomial system S of m_2 equations and m_2 unknowns. Under the assumption that this system is regular, we use Equation (5) and bound A by $\tilde{\mathcal{O}}\left(\left(2^{m_1(m_1-1)} e^{m_1} m_1^{-1/2}\right)^{\omega}\right)$. This yields the complexity in Equation (8). □

3.2 GLV curves.

The scalar multiplication of a point on a small dimension abelian variety is one of the most important operations used in curve-based cryptography. In 2001, Gallant, Lambert and Vanstone [16] introduced a method which uses efficiently computable endomorphisms on the elliptic curve to decompose the scalar multiplication in a 2-dimensional multi-multiplication. They considered a curve E with complex multiplication by $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}]$, with D small. We quickly review the examples of curves in [16] in the case where these are defined over an extension field $\mathbb{F}_{q^n}$, and show how to choose a factor basis invariant under the action of an endomorphism such that the value of k is small.

Example 2. Consider the elliptic curve $E_1 : y^2 = x^3 + ax$ defined over $\mathbb{F}_{q^n}$ with $a \in \mathbb{F}_{q^n}$. Let $\alpha \in \mathbb{F}_{q^n}$ an element of order 4. The map $\phi : E_1 \to E_1$ defined by $(x, y) \mapsto (-x, \alpha y)$ and $\mathcal{O} \mapsto \mathcal{O}$ is an endomorphism of the curve defined over $\mathbb{F}_{q^n}$. The characteristic equation of this endomorphism is $X^2+1 = 0$. To perform the index calculus on this curve we consider the factor basis $\mathcal{F}_{E_1,x}$. We realize that $x(\phi(Q)) \in \mathbb{F}_q$ whenever $x(Q) \in \mathbb{F}_q$ for all $Q \in E_1(\mathbb{F}_{q^n})$. Thus, if $Q \in \mathcal{F}_{E_1,x}$, then $\phi(Q) \in \mathcal{F}_{E_1,x}$. Considering the equivalence class $\{Q, \phi(Q)\}$, we can reduce the size of the factor basis by a factor 2 as compared to the classical algorithm considering the equivalence class $\{Q, -Q\}$.

Example 3. Consider the elliptic curve $E_2 : y^2 = x^3 + b$ defined over $\mathbb{F}_{q^n}$. Let $\beta \in \mathbb{F}_{q^n}$ be the cubic root of 1 in $\mathbb{F}_q$. Then, the map $\phi : E_2 \to E_2$ defined by $(x, y) \mapsto (\beta x, y)$ and $\mathcal{O} \mapsto \mathcal{O}$ is an endomorphism defined over $\mathbb{F}_{q^n}$. If $Q \in E_2(\mathbb{F}_{q^n})$ is a point of prime order r, then $\phi(Q) = \lambda Q$, where λ is an integer satisfying the equation $X^2 + X \equiv -1 \pmod{r}$. We define our factor basis as $\mathcal{F}_{E_2,x}$.

3.3 GLS curves.

In 2009, Galbraith, Lin and Scott [30] improved scalar multiplication on an elliptic curve by using the endomorphisms of a curve isogenous to it. We focus on the case where the isogenous curve is the twist of the given elliptic curve.

Theorem 2. *[30, Theorem 2] Let $q > 3$ be a prime number and E be an elliptic curve over $\mathbb{F}_q$. Let E' over $\mathbb{F}_{q^n}$ be the quadratic twist of $E(\mathbb{F}_{q^n})$, $n \geq 2$. Let $\phi : E \to E'$ be the twisting isomorphism defined over $\mathbb{F}_{q^{2n}}$, $r | \#E'(\mathbb{F}_{q^n})$ be a prime such that $r > 2q$. Let $\psi = \phi \circ \pi \circ \hat{\phi}$, π is the q-power Frobenius map on E. For $P = (x, y) \in E'(\mathbb{F}_{q^n})[r]$ we have $\psi(x, y) = (u^{(1-q)}x^q, u^{3(1-q)/2}y^q)$ and $\psi^n(P) + P = \mathcal{O}_E$.*

In this section, we consider $\mu = \mathrm{Tr}_\psi(x)$. A straightforward computation shows that this morphism is given by

$$\begin{aligned} &\mu : E' \to \mathbb{P}^1 \\ &\quad Q \mapsto x(Q) + u^k x(Q)^q + u^{k(1+q)} x(Q)^{q^2} + \cdots + u^{k(1+q+\cdots+q^{n-2})} x(Q)^{q^{n-1}}, \end{aligned}$$

where $k = 1 - q$.

Lemma 2. *We use the notation in Theorem 2. The morphism μ has degree q^{n-1}.*

Proof. For all $Q \in E'$, the index of ramification of μ in Q, $e_\mu(Q) = 1$. Indeed, the formal derivative $\mu' = 1 \neq 0$ for all $P \in E'$. We have $deg(\mu) = \#\mu^{-1}(Q) = q^{n-1}$.

In the light of Lemma 1, by choosing $\mathcal{F}_{E,\mu}$ as a factorization basis for index calculus, we may reduce the factor basis size by a factor n, as compared to the classical algorithm. However, to perform index calculus, we would need to use the summation polynomial $S_{\mu,n}$ whose degree is $q^{(n-1)^2}$ by Lemma 2. Consequently, it is hard to give an explicit formula of the polynomial $S_{\mu,n}$, not to mention solving it. To work around this problem, we work with $S_{x,n}$ and perform the Weil descent in the decomposition step with respect to a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem 3. *We use the notation of Theorem 2. The relation collection in the index calculus algorithm on E' with the factor basis $\mathcal{F}_{E',\mu}$ has complexity*

$$\tilde{\mathcal{O}}\left((n-1)!\left(2^{n(n-2)}e^n n^{-1/2}\right)^\omega q\right).$$

Proof. We pick $\mathcal{N} = \{\omega, \omega^q, \ldots, \omega^{q^{n-1}}\}$ a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We denote by $S_{x,n+1} \in \mathbb{F}_{q^n}[X_1, \ldots, X_{n+1}]$ the $n+1$-th Semaev polynomial of E' and by $S'_{x,n+1} \in \mathbb{F}_{q^n}[X_{11}, X_{12}, \ldots, X_{1n}, \ldots, X_{n1}, \ldots, X_{nn}, X_{n+1}]$ the polynomial obtained by substituting in $S_{x,n+1}$ the variables X_i by $X_{i1}\omega + X_{i2}\omega^q + \ldots + X_{in}\omega^{q^{n-1}}$, $1 \leq i \leq n$. During the decomposition step of the index calculus attack, we evaluate $S'_{x,n+1}$ at X_{n+1} by the x-coordinate of a random point R and then perform a Weil restriction on the polynomial obtained in this way. This yields a system of n equations and n^2 variables, that we denote by $\mathcal{S}$. Now, let us write the conditions that the points in the decomposition are in the factor basis. For the point of whose x-coordinate is X_i we have that

$$\mu_i = X_i + u^k X_i^q + u^{k(1+q)} X_i^{q^2} + \cdots + u^{k(1+q+\cdots+q^{n-2})} X_i^{q^{n-1}}.$$

In this equation, we substitute again formally X_i by $X_{i1}\omega + X_{i2}\omega^q + \ldots + X_{in}\omega^{q^{n-1}}$ and obtain

$$\mu_i = A_{i0}\omega + A_{i1}\omega^q + A_{i2}\omega^{q^2} + \cdots + A_{in-1}\omega^{q^{n-1}},$$

where A_{ij} are linear polynomials in $\mathbb{F}_q[X_{i1}, X_{i2}, \cdots, X_{in}]$. The condition that $\mu_i^q = \mu_i$ writes as

$$A_{i0}\omega^q + A_{i1}\omega^{q^2} + \cdots + A_{in-1}\omega = A_{i0}\omega + A_{i1}\omega^q + \cdots + A_{in-1}\omega^{q^{n-1}}.$$

After performing a Weil descent, we deduce the equations

$$\begin{aligned} A_{in-1} - A_{i0} &= 0 \\ A_{i0} - A_{i1} &= 0 \\ &\vdots \\ A_{in-2} - A_{in-1} &= 0. \end{aligned}$$

Since the first equation is linearly dependent on the $n-1$ others, we obtain a system of $n-1$ linear equations in the variables $X_{i1}, \ldots, X_{in}$, for $1 \leq i \leq n$. We solve this system and get $X_{i2}, \ldots, X_{in}$ in terms of X_{i1}. After substituting their expressions in $\mathcal{S}$, we are left with a system of n equations in the variables $X_{11}, \ldots X_{n1}$, whose degrees in each variables are 2^{n-2} that we solve using Gröbner basis algorithms.

Finally, the complexity of Gröbner basis computation is in

$$\tilde{\mathcal{O}}\left(\left(2^{n(n-2)} e^n n^{-1/2}\right)^{\omega}\right).$$

The probability of finding a decomposition of a point $R \in E'(\mathbb{F}_{q^n})$ in the factorization basis is approximately

$$\frac{\#\mathcal{F}^n_{E',\mu}/S_n}{\#E(\mathbb{F}_{q^n})} \simeq \frac{q^n/n\,!}{q^n} = \frac{1}{n\,!}$$

and the cardinality of the factorization basis is approximately $\frac{q}{n}$. We conclude that the relation collection step of the index calculus algorithm on E' with the factor basis $\mathcal{F}_{E',\mu}$ has complexity

$$\tilde{\mathcal{O}}\left((n-1)\,!\left(2^{n(n-2)} e^n n^{-1/2}\right)^{\omega} q\right).$$

□

3.4 GLV-GLS curves.

Longa and Sica [25] generalized the GLS method to all GLV curves by exploiting both the endomorphisms arising from the GLV and the GLS approach to decompose the scalar multiplication in a 4-dimensional multi-multiplication. We conclude this section with an example where two endomorphisms may be used to reduce the factor basis.

Example 4. [25, Section 8] Consider the curve in Weierstrass form $E_3'(\mathbb{F}_{q^2})$: $y^2 = x^3 + 9u$, where $q = 2^{127} - 58309$ and $\#E_3'(\mathbb{F}_{q^2}) = r$, r a 254-bit prime. We take $\mathbb{F}_{q^2} = \mathbb{F}_q[i]/(i^2+1)$ and $u = 1 + i \in \mathbb{F}_{q^2}$ and $\phi(x, y) = (\beta x, y)$ with $\beta^3 \equiv 1 \pmod q$ and $\psi(x, y) = (u^{\frac{1-q}{3}} x^q, u^{\frac{1-q}{2}} y^q)$. We have that $\phi^2 + \phi + 1 = 0$ and $\psi^2 + 1 = 0$.

As before, we consider the factor basis $\mathcal{F}_{E_3',\mu}$ where $\mu = \mathrm{Tr}_\psi(x)$. Recall that we have

$$\begin{aligned} \mu(Q) &= x(Q) + x(\psi(Q)) \\ &= x(Q) + u^{\frac{1-q}{3}} x(Q)^q. \end{aligned}$$

Using the fact that $\beta, \mu(Q) \in \mathbb{F}_q$ we compute:

$$\begin{aligned} \mu(\phi(Q)) &= \mu((\beta x(Q), y(Q))) \\ &= \beta x(Q) + u^{\frac{1-q}{3}} (\beta x(Q))^q \\ &= \beta x(Q) + u^{\frac{1-q}{3}} \beta x(Q)^q \\ &= \beta(x(Q) + u^{\frac{1-q}{3}} x(Q)^q) \\ &= \beta\mu(Q) \in \mathbb{F}_q. \end{aligned}$$

Therefore, Q, $\phi(Q)$ and $\phi^2(Q)$ are simultaneously in $\mathcal{F}_{E_3',\mu}$. Since $\mathcal{F}_{E_3',\mu}$ is also closed with respect to ψ, we extend the equivalence class to

$$\{Q, \phi(Q), \phi^2(Q), \psi(Q), \psi(\phi(Q)), \psi(\phi^2(Q))\}.$$

This allows us to gain a factor 6 speed up in the relation search step of the index calculus algorithm. □

Note that we cannot always extend the equivalence classes on the factor basis using both endomorphisms for the simple reason that usually the GLV endomorphism ϕ has characteristic equation of the type $\phi^2 + a\phi + b = 0$, where $a \neq 0$ and $b \neq \pm 1$. For such an endomorphism, the eigenvalues do not have small order modulo $\#E(\mathbb{F}_{q^n})$ and this would result into large equivalence classes, which we not know how to handle.

3.5 Elliptic curves with a rational small torsion point

In [11], Huot *et al.* proposed a method to reduce the factorization basis whenever the elliptic curve has a rational two torsion point. Huot et al. worked out the attack on Edwards curves and on Jacobi intersection curves. We explain the main idea of this method on a simple example of an elliptic curve in Weierstrass form.

Example 5. We revisit the example of the elliptic curve E_1 defined in Example 2. We further assume that $a \in \mathbb{F}_q$. We notice that $(0,0)$ is a 2-torsion point on E_1. For a given point $P = (x,y) \in E_1(\mathbb{F}_{q^n})$ we see that

$$x(P+T_2) = \frac{x^3+ax}{x^2} - x$$

is in $\mathbb{F}_q$ whenever $x \in \mathbb{F}_q$. Therefore, for a given point Q, the points Q and $Q+T_2$ are simultaneously in the factor basis $\mathcal{F}_{E_1,x}$. Considering the equivalence class $Q, Q+T_2, -Q, -Q+T_2$ in the factor basis, we can reduce its size by a factor 4 compared to the classical algorithm using the equivalence class $\{Q, -Q\}$.

In Example 5, the 2-torsion point T_2 verifies $x(P+T_2) \in \mathbb{F}_q$ whenever $x(P) \in \mathbb{F}_q$. But this condition is not always satisfied. To work around this problem, in [12] the authors consider a factor basis defined with respect to a morphism φ invariant under the 2-torsion point of the curve.

Proposition 1. *[12, Proposition 8] Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$. If char$(\mathbb{F}_{q^n}) \neq 2$, then there exists $T \in E(\mathbb{F}_{q^n})[2]$ and $\varphi : E \to \mathbb{P}^1$ a degree 2 morphism such that $\varphi(P+T) = -\varphi(P)$ and $\varphi(-P) = -\varphi(P)$ if and only if there exists $T' \in E[4]$ such that $x(T') \in \mathbb{F}_{q^n}$. In this case $T = [2]T'$ and the curve E has an equation of the form $y^2 = x^3 + ax^2 + bx$ where $T = (0,0)$ and b a square in $\mathbb{F}_{q^n}$; moreover, φ is of the form*

$$\lambda \tfrac{x(P)+\sqrt{b}}{x(P)-\sqrt{b}},$$

for a choice of the square root of b and $\lambda \in \mathbb{F}_{q^n}$.

We will show that whenever an efficient endomorphism exists on the curve and a 2-torsion point is defined over $\mathbb{F}_{q^n}$ it is possible in most cases to reduce the factorization basis with respect to both the torsion point of the curve and the endomorphism. To this purpose, we reformulate a result given by Charles [5] and give its proof for completeness.

Lemma 3. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_{q^n}$ and let ψ be an endomorphism different from multiplication by a scalar. Assume that $E(\mathbb{F}_{q^n})[2]$ is non-trivial.*

1. *If $E(\mathbb{F}_{q^n})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ then $\psi(T) = \gamma T$, with $\gamma \in \{0,1\}$ for all T in $E(\mathbb{F}_{q^n})[2]$.*
2. *Assume that $E(\mathbb{F}_{q^n})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and that $\mathbb{Z}[\psi] \simeq \mathcal{O}$, where $\mathcal{O}$ is the ring of integers of a quadratic imaginary field. Then if 2 is split or ramified in $\mathcal{O}$, then there is a 2-torsion point T defined over $\mathbb{F}_{q^n}$ such that $\psi(T) = \gamma T$, with $\gamma \in \{0,1\}$. If 2 is inert, there is no such T.*

Proof. 1) This is straightforward. Indeed, let us denote by π_n the Frobenius endomorphism of E. Using the commutativity of the endomorphism ring of E, we have that:

$$\pi_n(\psi(T)) = \psi(\pi_n(T)) = \psi(T).$$

Hence $\psi(T) = \gamma T$, with $\gamma \in \{0, 1\}$. 2) Under the isomorphism $\mathbb{Z}[\psi] \simeq \mathcal{O}$, ψ acts on $E[2]$ as a matrix whose characteristic polynomial is the minimal polynomial of $\alpha \in \mathcal{O}$ modulo 2. If 2 is inert in $\mathcal{O}$, then no 2-torsion group is stabilized by α. If 2 is split or ramified, then the matrix of α on $E[2]$ is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, respectively. In these cases, it is obvious that there is at least one 2-torsion point T which is an eigenvector for ψ. □

Theorem 4. *We use the notation and assumptions in Proposition 1. We consider that there exists an endomorphism $\psi : E \to E$ and k a small integer such that $\psi^k(Q) = \pm Q$ for all $Q \in E$ and T is not in Ker ψ. Consider $\mu_1 = \mathrm{Tr}_\psi(\varphi) : E \to \mathbb{P}_1$ and $\mu_2 = N_\psi(\varphi) : E \to \mathbb{P}_1$. The factorization basis $\mathcal{F}_{E,\mu_1}$ and $\mathcal{F}_{E,\mu_2}$ are invariant under T and ψ. Morever, the summation polynomials $S_{\mu_1,n}$ and $S_{\mu_2,n}$ are invariant under the action of the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_n$.*

Proof. The invariance of $\mathcal{F}_{E,\mu_1}$ and $\mathcal{F}_{E,\mu_2}$ with respect to ψ follows from Lemma 1 and the invariance with respect to T comes from Lemma 3. Indeed, we have that:

$$\begin{aligned}
\mu_1(P+T) &= \varphi(P+T) + \varphi(\psi(P+T)) + \cdots + \varphi(\psi^{k-1}(P+T)) \\
&= -\varphi(P) + \varphi(\psi(P)+T) + \cdots + \varphi(\psi^{k-1}(P)+T)) \\
&= -\varphi(P) + \varphi(\psi(P)+T) + \cdots + \varphi(\psi^{k-1}(P)+T)) \\
&= -\varphi(P) - \varphi(\psi(P)) - \cdots - \varphi(\psi^{k-1}(P)) \\
&= -\mu_1(P) \in \mathbb{F}_q.
\end{aligned}$$

A similar computation will show that $\mu_2(P+T) = \pm\mu_2(P)$. As shown in [12, Prop. 7], the polynomial $P_{\varphi,n}$ is invariant under the action of $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_n$. This implies that $P_{\mu_1,n}$ and $P_{\mu_2,n}$ are also invariant under the action of this group.

Remark 1. Heuristically, and the degrees of $\mathrm{Tr}_\psi(\varphi)$ and $N_\psi(\varphi)$ are both equal to $d = \sum_{i=0}^{k-1} \deg(\varphi)(\deg(\psi))^i$. This means that in general the degree of the polynomials $S_{\mu_1,n}$ and $S_{\mu_2,n}$ will be augmented by a factor d^{n-1} in each variable as compared to the degree of $S_{\varphi,n}$. This results into slower Gröbner basis computation, which suggests that both k and $\deg\psi$ have to be very small in general.

The invariance in Theorem 4 allows us to reduce the size of the factor basis by a factor of $2k$ as compared to the original algorithm.

Example 6. We consider the example of the elliptic curve E_2 defined in Example 3 such that b is a cubic root in $\mathbb{F}_{q^n}$, and let $d = 3\sqrt[3]{b}^2$. The curve E_2 admits an endomorphism ψ of order 3 and a 4-torsion point T', then, a 2-torsion point $T = 2T'$. By Proposition 1, there exists a degree 2 morphism φ such that $\varphi(P+T) = -\varphi(P)$ and $\varphi(-P) = -\varphi(P)$ of the form

$$\varphi(P) = \tfrac{x(P)+\sqrt{d}}{x(P)-\sqrt{d}}.$$

We consider the morphism

$$\mu : P \mapsto \varphi(P) \cdot \varphi(\psi(P)) \cdot \varphi(\psi^2(P)).$$

We have:

$$\begin{aligned}\mu &= \frac{x+\sqrt{d}}{x-\sqrt{d}} \cdot \frac{\beta x+\sqrt{d}}{\beta x-\sqrt{d}} \cdot \frac{\beta^2 x+\sqrt{d}}{\beta^2 x-\sqrt{d}} \\ &= \frac{x^3+d\sqrt{d}}{x^3-d\sqrt{d}} \quad \mathit{since} \quad \beta^2+\beta+1=0.\end{aligned}$$

Using the observation in Remark 1 we obtain a polynomial with degree $3 \cdot 2^{n-1}$ in each variable.

To perform the index calculus on $E_2(\mathbb{F}_{q^n})$, we use the factorization basis $\mathcal{F}_{\mu,E_2}$. By Theorem 4, the size of $\mathcal{F}_{\mu,E_2}$ is reduced by a factor 3, as compared to the factor basis proposed in [12]. Moreover, since μ is invariant under the action of $\mathbb{Z}/3\mathbb{Z}$, we can further symmetrize the polynomial $S_{\mu,n}$ and reduce its degree by a factor 3 in each variable, so the cost of the Gröbner basis computation is unchanged.

4 Index calculus attack over the Jacobian of a hyperelliptic curve of genus $g \geq 2$.

Throughout this section, the group G denotes a subgroup of order r of the Jacobian $J(H)$ of a hyperelliptic curve H of genus g defined over a finite field $\mathbb{F}_{q^n}$ by the equation

$$y^2 + h_1(x)y = h_0(x), \tag{9}$$

where $deg(h_1) \leq g$, h_0 a monic polynomial of degree $2g+1$ and r the greatest prime divisor of the order of $J(H)$. We denote by P_0 the point at infinity of H. Whenever we use the Mumford representation of a representative $D = (x^2 + u_1 x + u_0, v_1 x + v_0) \in J(H)$ we will simply write $D = (u_1, u_0, v_1, v_0)$.

The factor basis for the index calculus algorithm is defined by:

$$\mathcal{F} = \{D = (P) - (P_0) \in J(H) : x(P) \in \mathbb{F}_q\}. \tag{10}$$

This approach yields attacks faster than generic methods for genus $g \geq 3$ (see [19]).

Similar considerations as those in Section 3 apply to an ordinary hyperelliptic curve of genus > 1 defined over $\mathbb{F}_{q^n}$, most notably by the use of the Frobenius morphism.

4.1 Binary hyperelliptic curves defined over a prime degree extension field

Lange [23, 24] showed that hyperelliptic curves defined over $\mathbb{F}_{2^n}$ given by Equation (9) with $h_0, h_1 \in \mathbb{F}_2[x]$ and n prime are suitable for cryptographic applications because they allow fast arithmetic. These curves are called hyperelliptic Koblitz curves in the literature.

Recall that for the Jacobian of these hyperelliptic curves the factor base is defined by

$$\mathcal{F} = \{D = (P) - (P_0) \in J(\mathbb{F}_{2^n}) : x(P) \in \mathbb{F}_{2^n}\}. \tag{11}$$

We notice that if $D \in \mathcal{F}$, then $\pi(D), \pi^2(D), \cdots, \pi^{n-1}(D)$ are also in $\mathcal{F}$. Hence we can construct the equivalence class $\{D, \pi(D), \pi^2(D), \cdots, \pi^{n-1}(D)\}$ in the factor base and reduce its size by a factor n.

The characteristic polynomial of the Frobenius map is

$$\chi_H(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 q^{m_1(g-1)} T + q^{m_1 g}, \tag{12}$$

where $a_i \in \mathbb{Z}$ and $1 \leq i \leq g$ can be precomputed by solving a point counting problem.

We improve the complexity by a logarithmic factor as compared to the initial algorithm in [19]. Indeed, the analysis in [19] can be rewritten in terms of the size of the factor base, by keeping track that only $\#\mathcal{F}^r$ elements in $\mathcal{F}$ will be kept for the linear algebra step. We do not detail the analysis here since this would be a mere reproduction of the computation in [19], but by taking into account logarithmic factors, the complexity of the double large prime variation algorithm is $\mathcal{O}(\#\mathcal{F}^{2-2/g} log(\#\mathcal{F}))$.

In our case, given the fact that we do a look up in an equivalence relation of size n, this yields $\mathcal{O}(n^2(\frac{2^n}{n})^{2-2/g}) = \mathcal{O}(n^{2/g}(2^n)^{2-2/g})$ for $g \geq 3$. This is to be compared against $\mathcal{O}(n(2^n)^{2-2/g})$, which is the complexity of the algorithm in [19] for Koblitz curves.

4.2 Buhler-Koblitz curves.

Buhler-Koblitz (BK) curves [4] are genus 2 hyperelliptic curves of the form

$$H_b : y^2 = x^5 + b$$

defined over the finite field $\mathbb{F}_q$ where q is a prime such that $q \equiv 1 \pmod{10}$. We take $\epsilon \neq 1$ a primitive fifth root of the unity in $\mathbb{F}_q$. If the point $(x, y) \in H_b$, then $(\epsilon x, y) \in H_b$. This implies that the Jacobian of H_b admits an endomorphism

$$\varphi : (u_1, u_0, v_1, v_0) \mapsto (\epsilon u_1, \epsilon^2 u_0, \epsilon^4 v_1, v_0)$$

of order 5 which satisfies the minimal polynomial $T^4 + T^3 + T^2 + T + 1$. To perform the index calculus algorithm on the Jacobian of H_b, we define the factorization basis by

$$\mathcal{F} = \{D = (P) - (P_0) \in J(H_b(\mathbb{F}_q)) : x(P) \in \mathbb{F}_q\}.$$

This factor basis is invariant with respect to φ and we can reduce its size by a factor 5. As shown in [2, Section 8.1], if the BK curve is defined over $\mathbb{F}_{q^2}$ and index calculus is performed in $J(\mathbb{F}_{q^2})$, then we can reduce the size of the factor basis up to a factor 10 by considering a GLS endomorphism construction.

4.3 Furukawa-Kawazoe-Takahashi curves.

The Furukawa-Kawazoe-Takahashi (FKT) curves [14] are genus 2 hyperelliptic curves of the form

$$H_a : y^2 = x^5 + ax$$

defined over the finite field such that $q \equiv 1 \pmod 8$. Let $\alpha \neq 1$ be a primitive eighth root of the unity in $\mathbb{F}_q$. We observe that if $(x, y) \in H_a$, then $(\alpha^2 x, \alpha y) \in H_a$. This induces an endomorphism of the Jacobian

$$\psi : (u_1, u_0, v_1, v_0) \mapsto (\alpha^2 u_1, \alpha^4 u_0, \alpha^7 v_1, \alpha v_0)$$

of order 8, which satisfies the minimal polynomial $T^4 + 1$. To perform the index calculus algorithm on the Jacobian of H_a, we use the same factorization basis $\mathcal{F}$ than those of the BK curves. This factor basis is invariant with respect to ψ and this invariance allows us to reduce its size by a factor 4 as compared to the classical algorithm considering the equivalence class $\{D, -D\}$.

4.4 Guillevic-Ionica curves.

Guillevic and Ionica [20] considered two families of elliptic curves defined over $\mathbb{F}_{q^2}$ and having efficiently computable endomorphisms for which the 4-dimensional multi-multiplication algorithm can be applied.

The first family is given by curves with equation

$$E_{1,c}(\mathbb{F}_{q^2}) : y^2 = x^3 + 27(10 - 3c)x + 14 - 9c,$$

with $c \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, $c^2 \in \mathbb{F}_q$. The construction of the endomorphisms in [20] is based on the existence of an isogeny from the Jacobian of the genus 2 hyperelliptic curve with equation

$$H_1 : Y^2 = X^5 + aX^3 + bX, \text{ with } a, b \neq 0 \in \mathbb{F}_q \text{ such that } c = a/\sqrt{b}.$$

to the product $E_{1,c} \times E_{1,-c}$. This isogeny is defined over $\mathbb{F}_{q^2}$. The second family is given by curves with equation

$$E_{2,c}(\mathbb{F}_{q^2}) : y^2 = x^3 + 3(2c - 5)x + c^2 - 14c + 22,$$

with $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $c^2 \in \mathbb{F}_q$. Again, $E_{2,c} \times E_{2,-c}$ is isogenous over $\mathbb{F}_{q^2}$ to the Jacobian of a genus 2 hyperelliptic curve given by the following equation.

$$H_2 : Y^2 = X^6 + aX^3 + b, \text{ with } a, b \neq 0 \in \mathbb{F}_q \text{ such that } c = a/\sqrt{b}.$$

The two endomorphisms used in [20] do not have small order and hence it does not seem possible to identify a factor basis on $E_{i,c}$ with small orbits under the action of these endomorphisms. However, due to the existence of isogenies to $J(H_i)$, solving the discrete logarithm problem on the elliptic curves is equivalent to solving the problem on the genus 2 Jacobian. These curves were also proposed by Smith in [29].

As explained in Section 2, on the Jacobian we define the factor basis by

$$\mathcal{F} = \{D = (P) - (P_0) \in J(H_i(\mathbb{F}_{q^2})) : x(P) \in \mathbb{F}_q\}.$$

The divisors $D = (P) - (P_0)$ and $\pi_q(D) = (\pi_q(P)) - (P_0)$ are simultaneously in $\mathcal{F}$. So, we construct the equivalence class $\{D, \pi_q(D)\}$ in $\mathcal{F}$ and reduce the size of the factor basis by a factor 2.

5 Complexity analysis and benchmarks

We have implemented in MAGMA [3] the relation search step of the index calculus attack for the discrete logarithm problem on elliptic curves given in Sections 3.1 and 3.3. The polynomial system issued from the decomposition step is solved using MAGMA's implementation of the F_4 algorithm. Since the decomposition step for hyperelliptic curves is different from the elliptic curve case, we have also experimented with genus 2 Koblitz curves. All tests were performed on a 2.40GHz Intel Xeon E5-2680 processor.

Each equivalence class is of the form $\{Q, \phi(Q), \cdots, \phi^{k-1}(Q)\}$; where k is such that $\phi^k = \pm 1$. We pick an element of this class which will be the representative of it, and put it in the reduced basis. To implement this reduced basis, we used the **AssociativeArray** data structure in MAGMA [3] which allows an efficient look up in the equivalence classes. Thus, to be able to write a line in the relation matrix comes with an extra cost because whenever we obtain a new decomposition, for each point in the relation we search the representative of its equivalence class in the reduced factor basis. However, the cost of this search remains negligible with respect to the cost of computation of Gröbner basis.

In Table 1, we compare the theoretical complexities of the index calculus algorithm with reduced basis, with full basis and Pollard's rho method [8]. In Table 2 and Table 3, we compare the runtime of the relation collection for the full basis and for the reduced basis with respect to the equivalence classes for elliptic curves defined over composite degree extension and for $GLV - GLS$ curves defined over $\mathbb{F}_{q^2}$ respectively. In Table 4, for $n \in \{7, 11, 13, 17\}$, we compare the runtime of the relation collection algorithm for the full basis and for the reduced basis with respect to our equivalence classes for hyperelliptic curves defined in Section 4.1. In this table, for a given curve, only the values of n for which the factor basis has large enough size were considered. Our running times for the Pollard rho algorithm on these curves shown in the last column of this Table suggest that Pollard rho remains faster for these genus 2 curves. The timings presented in Table 2, 3 and 4 are an average of 10 runs for each parameter choice and we can see that our reduced basis yields a decomposition phase which is faster by a factor greater than the size of the equivalence class in each case.

Table 1: Complexity Analysis.

	Reduced basis	Full basis	Pollard rho
Elliptic curve over $\mathbb{F}_{2^{m_1 m_2}}$	$(\frac{m_1!}{m_2}2^{m_1(m_1-1)+m_2}e^{m_1}m_1^{-1/2})^{\omega}$	$(m_1!2^{m_1(m_1-1)+m_2}e^{m_1}m_1^{-1/2})^{\omega}+m_1 2^{m_2}$	$\sqrt{\frac{\pi 2^{m_1 m_2 - 1}}{m_2}}$
Hyperelliptic curve over $\mathbb{F}_{2^n}$	$\frac{(2^n)^{2-2/g}}{n^{-2/g}}$	$n(2^n)^{2-2/g}$	$\sqrt{\frac{\pi 2^{gn}}{2n}}$
GLV-GLS	$(n-1)!\left(2^{n(n-2)}e^n n^{-1/2}\right)^{\omega} q$	$n!\left(2^{n(n-2)}e^n n^{-1/2}\right)^{\omega} q$	$\frac{\sqrt{\pi q^n}}{2}$

Table 2: Experiments on elliptic curves defined over composite extension field.

m_1	m_2	Time reduced basis	Time full basis	Reduction ratio
2	7	0.229 sec.	1.63 sec.	7.1
3	11	1039.4 sec.	11442.4 sec.	11
2	17	154755.566 sec.	2727802.448 sec.	17.6

Table 3: Experiments on GLV-GLS curve defined over $\mathbb{F}_{p^2}$.

p	Time reduced basis	Time full basis	Reduction ratio
43	0.046 sec.	0.282 sec.	6.13
739	1.083 sec.	6.155 sec.	5.68
1051	2.538 sec.	15.92 sec.	6.27
2731	6.662 sec.	50.836 sec.	7.63
3163	8.211 sec.	68.881 sec.	8.38

Table 4: Experiments on hyperelliptic curves defined over prime extension field.

Curves	n	Time reduced basis	Time full basis	Reduction ratio	Time Pollard-Rho
$y^2+(x^2+x+1)y=x^5+1$	7	0.011 sec.	0.059 sec.	5.36	0.01 sec.
$y^2+(x^2+x+1)y=x^5+x$	11	0.252 sec.	2.441 sec.	9.69	0.054 sec.
	13	0.559 sec.	7.740 sec.	13.84	0.212 sec.
	17	17.432 sec.	613.6 sec.	38.2	5.178 sec.
$y^2+y=x^5+x^3$	11	0.117 sec.	0.997 sec.	8.52	0.045 sec.
	17	15.498 sec.	716.78 sec.	46.25	4.075 sec.
$y^2+y=x^5+x^3+1$	7	0.026 sec.	0.082 sec.	3.15	0.006 sec.
	11	0.604 sec.	6.855 sec.	11.35	0.11 sec.
$y^2+xy=x^5+x^2+1$	7	0.016 sec.	0.114 sec.	7.12	0.01 sec.
	17	10.386 sec.	118.761 sec.	11.43	0.89 sec.
$y^2+(x^2+x)y=x^5+1$	7	0.02 sec.	0.089 sec.	4.45	0.01 sec
	17	53.158 sec.	1621.319 sec.	30.5	6.03 sec.

6 Conclusion

We have revisited the relation search step of the index calculus algorithm for several families of small genus hyperelliptic curves considered for elliptic curve cryptography. We have shown that the endomorphism of a Jacobian allows us to construct equivalence classes on the factor base and decreases its size by a factor equal to the order of the endomorphism of the Jacobian. This results into a smaller number of relations to collect and also reduces the cost of the linear algebra phase, and thus improves the complexity of the index calculus algorithm on several families of curves suited for cryptography.

References

1. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: P. Gianni, editor, *The Effective Methods in Algebraic Geometry Conference, Mega 2005*, Mai 2005.
2. Bos, J.-W., Costello, C., Hisil, H., and Lauter, K.: High-performance scalar multiplication using 8-dimensional GLV/GLS decomposition. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 331–348. Springer, Heidelberg (2013)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language, Journal of Symbolic Computation, **24**, 235–265 (1997), http://magma.maths.usyd.edu.au/magma/
4. Buhler, J.-P., Koblitz, N.: Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, Bulletin of the Australian Mathematical Society 58 (1), 147-154.
5. Charles, D. On the existence of distortion maps on ordinary elliptic curves, https://eprint.iacr.org/2006/128, 2006
6. Cohen, H., Gerhard, F., editors.: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Mathematics and its Applications, Chapman and Hall/CRC (2006)
7. Diem, C.: On the discrete logarithm problem in elliptic curves.Compos. Math.,147(1):75–104, 2011.
8. Duursma, I., Gaudry, P., Morain, F.: Speeding up the discrete log computation on curves with automorphisms. ASIACRYPT 1999, Singapore. pp.103-121.
9. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F_4). Journal of Pure Applied Algebra **139**(1-3),99–110 (1999) 61-88
10. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero ($F5$). In Mora,T. (Ed.), ISSAC 2002. ACM Press, pp. 75–83, proceedings of the 2002 International Symposium on Symbolic andAlgebraic Computation, July 07–10, 2002, Université de Lille, France.
11. Faugère, J.-C., Gaudry, P., Huot, L., Renault, L.: Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm. Journal of Cryptology, Springer Verlag, 2013, pp.1-40.
12. Faugère, J.-C., Huot, L., Joux, A., Renault, G., Vitse, V.: Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus. Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014.

13. Faugère, J.-C., Perret, L., Petit, C., Renault, G.: Improving the complexity of index calculus algorithms in elliptic curves over binary fields. EUROCRYPT 2012, 31st Annual International Conference on the Theory and Applications of Cryptographic techniques, Proceeding, pages 27–44.
14. Furukawa, E., Kawazoe, M., and Takahashi, T.: Counting points for hyperelliptic curves of type y2= x5+ax over finite prime fields. In M. Matsui and R. J. Zuccherato, editors,Selected Areas in Cryptography,volume 3006 ofLecture Notes in Computer Science, pages 26–41. Springer, 2003
15. Galbraith, S D., Gebregiyorgis, S W.: Summation polynomial algorithms for elliptic curves in characteristic two. Journal of Cryptology (2014) 806
16. Gallant, R., Lambert, R., Vanstone, S.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) CRYPTO. LNCS, vol. 2139, pp. 190-200. Springer(2001).
17. Gaudry, P.: An algorithm for solving the discrete log problem on hyperelliptic curves. In Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, pages 19–34, 2000.
18. Gaudry, P.: Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. J. Symb. Comput **44**(12), 1960-1702 (2009)
19. Gaudry, P., Thomé, E., Thériault, N., Diem, C. A double large prime variation for small genus hyperelliptic index calculus, Mathematics of Computation, **76**, 475-492 (2007)
20. Guillevic, A., Ionica, S.: Four-Dimensional GLV via the Weil Restriction. Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Satya Lokam, Dec 2013, Bengalore, India. pp.79-96
21. Huang, Y.-J., Petit, C., Shinohara, N., Takagi, T.,: Improvement of Faugère et al.'s method to solve ECDLP. In: Advances in Information and Computer Security - 8th International Workshop on Security, IWSEC 2013 on Proceedings, pp. 115–132. Okinawa, Japan, November 18-20, 2013
22. Joux, A., Vitse, V.: Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields Application to the Static Diffie-Hellman Problem on $E(\mathbb{F}_{q^5})$, Journal of Cryptology. 26(1): 119-143 (2013)
23. Lange, T.: Hyperelliptic curves allowing fast arithmetic webpage, 2001. https://www.hyperelliptic.org/tanja/KoblitzC.html
24. Lange, T.: Efficient Arithmetic on Hyperelliptic Koblitz Curves, 2001 https://www.hyperelliptic.org/tanja/preprints/preprint.pdf
25. Longa, P., Sica, F.: Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication. Journal of Cryptology **27**, (2014) 248-283
26. Nagao, K.-I.: Decomposition Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field. In: Algorithmic Number Theory on Proceedings, pp. 285–300. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
27. Petit, C., Quisquater, J.-J: On polynomial systems arising from a Weil descent. ASIACRYPT 2012, International Conference on the Theory and Applications of Cryptology and information security, Proceeding, pages 451–466.
28. Semaev, I.: Summation polynomial and the discrete logarithm algorithm problem on elliptic curve. Preprint available at: http:// eprint.iacr.org/2004/031 (2004)
29. Smith, B.: Families of fast elliptic curves from Q-curves. In: Sako, K., Sarkar, P. (eds.) Asiacrypt. LNCS, vol. To appear. Springer (2013), http://eprint.iacr.org/2013/312

30. Steven D, G., Xibin, L., Michael S,.: Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves . Journal of Cryptology **24**(3), 446-469 (2011)