Index calculus attacks on hyperelliptic Jacobians with efficient endomorphisms

Sulamithe Tsakou, Sorina Ionica

Laboratoire MIS, Université Picardie Jules Verne 33 rue Saint Leu Amiens 80000, France

Received: August 6, 2021 | Revised: August 6, 2021 | Accepted: August 6, 2021

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 operations on the factor base, 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 original attack.*

Keywords: Discrete Logarithm Problem, Index Calculus, Endomorphism

2010 Mathematics Subject Classification: 14G50,11G15

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 [7] 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 base 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 base, the linear algebra step and the descent phase in which the discrete logarithm of h is deduced. The choice of the factor base depends on the curve and its field of definition. The complexity of the algorithm crucially depends on the size of the factor base, since this determines the probability for a point to be decomposed over the base and also the cost of the linear algebra step.

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$. In [6, 18], the authors suggest, if q is a large prime and n small, to take the factor base as :

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

which has approximately q elements. Defining the factor base as Gaudry did, 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 base and thus reduce its size by a factor 2. Going further in this direction, the authors of [10, 11, 13] exploited small torsion points to reduce the size of the factor base. More recently, Galbraith *et al.* [16] used the action of the Frobenius endomorphism on certain factor bases to improve the index calculus attack on subfield elliptic curves (i.e. curves defined over smaller extension fields). Recently, Chi-Dominguez *et al.* [5] proposed the use of the Galbraith-Lin-Scott (GLS) endomorphism to speed up the index calculus algorithm on the Jacobian of a hyperelliptic curve constructed in the GHS Weil descent attack on generalized GLS curves defined over $\mathbb{F}_{2^{ln}}$, with $l \geq 2$ and $\gcd(l, n) = 1$.

We generalize the reduction of the factor base based on the use of the automorphism $[-] : P \mapsto -P$ and the Frobenius endomorphism and show that any efficient computable endomorphism ϕ of the Jacobian may be used to speed up index calculus. To this purpose, we redefine the factor base so that it would be invariant under the action of the endomorphism (i.e. $\phi(P) \in \mathcal{F}$ for all $P \in \mathcal{F}$). This allows us to consider equivalence classes of larger size

*Corresponding Author: sorina.ionica@u-picardie.fr

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, GLV-GLS families of elliptic curves and on Buhler-Koblitz and Furukawa-Kawazoe-Takahashi elliptic curves over finite fields with characteristic greater than 2. 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 base is compatible to the one in [11], resulting into an improved algorithm for some of these curves as well. We implemented this decomposition algorithm using the computer algebra system MAGMA [2] 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 base 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 base $\mathcal{F} = \{g_1, g_2, \cdots, g_N\}$ consisting of N elements in G.
2. The relation collection: Choose random integers α_i modulo r and try to decompose $[\alpha_i]g$ into the factor base, 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 independent 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 base 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 base, 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 $h = ((\sum_{j=1}^{N} \lambda_j x_j) - \alpha)\beta^{-1} g$.

2.0.1 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 base, we follow the approach in [11] which is useful for our purposes. Let $\mathbb{P}_1$ be the projective space. Suppose that we have a morphism $\mu : E \to \mathbb{P}_1$ defined over $\mathbb{F}_{q^n}$.

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

$$\mathcal{F}_{E,\mu} = \{P \in E(\mathbb{F}_{q^n}) : \mu(P) \in \mathbb{P}_1(\mathbb{F}_q)\}.$$

To find a relation of the form

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

we use the summation polynomial associated to the morphism μ, introduced in [11, Proposition 2].

Denote by O the point at infinity on E. The m^{th}-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

$$P_1 + P_2 + \cdots + P_m = O \iff S_{m,\mu}(\mu(P_1), \mu(P_2), \cdots, \mu(P_m)) = 0. \tag{2}$$

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

$$\begin{array}{rccc} x: & E & \to & \mathbb{P}_1 \\ & P & \mapsto & (x(P), 1) \end{array}$$

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

$$S_{n+1,\mu}(\mu(P_1), \mu(P_2), \cdots, \mu(P_n), \mu(R)) = 0, \tag{3}$$

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 base 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 [8, 9]. For a random morphism μ, the expected degree of $S_{n+1,\mu}$ 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

$$\left(\begin{array}{c} d+n \\ n \end{array} \right) = \left(\begin{array}{c} n(\deg \mu)^{n-1} + 1 \\ n \end{array} \right) \simeq \left(\begin{array}{c} n(\deg \mu)^{n-1} \\ n \end{array} \right).$$

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

$$\tilde{O}\left(\left(\begin{array}{c} n(\deg \mu)^{n-1} \\ n \end{array} \right)^{\omega} \right),$$

where $\omega < 3$ is the complexity exponent of matrix multiplication. Using Stirling's formula, we get:

$$\left(\begin{array}{c} n(\deg \mu)^{n-1} \\ n \end{array} \right) \sim \frac{(n(\deg \mu)^{n-1})^n}{n!} \sim (\deg \mu)^{n(n-1)} e^n (2\pi n)^{-1/2}.$$

Finally, the complexity of Gröbner basis computation is

$$\tilde{O}\left(\left((\deg \mu)^{n(n-1)} e^n n^{-1/2} \right)^{\omega} \right). \tag{4}$$

Consequently, to be able to solve the system resulting from Equation (3), 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 $\phi(P) = \beta P$.

First, we exhibit some simple examples of curves and endomorphisms ϕ with the property that the factor base $\mathcal{F}_{x,E}$ is invariant under ϕ, i.e. for every $P \in \mathcal{F}_{E,x}$, then $\phi(P) \in \mathcal{F}_{E,x}$. Whenever this property is not verified, we adjust the base in function of the endomorphism.

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 :*

$$\begin{array}{rcl} \mathrm{Tr}_\phi(\mu) : E & \to & \mathbb{P}_1 \\ Q & \mapsto & (\mu(Q) + \mu(\phi(Q)) + \cdots + \mu(\phi^{k-1}(Q)), 1), \end{array}$$

and

$$\begin{array}{rcl} N_\phi(\mu) : E & \to & \mathbb{P}_1 \\ Q & \mapsto & (\mu(Q) \bullet \mu(\phi(Q)) \bullet \cdots \bullet \mu(\phi^{k-1}(Q)), 1). \end{array}$$

The following lemma shows that given a morphism μ, the basis introduced in Definition 2 are indeed invariant under the endomorphism ϕ.

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 $\phi : E \to E$ an endomorphism of E such that $\phi^k = \pm 1$. The factor bases $\mathcal{F}_{E,\mathrm{Tr}_\phi(\mu)}$ and $\mathcal{F}_{E,N_\phi(\mu)}$ are invariant with respect to the endomorphism ϕ.*

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. □

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 representative 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 $O(\log r)$.

3.1 GLV AND GLS 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 [17] introduced a method which uses efficiently computable endomorphisms on the elliptic curve to decompose the scalar multiplication in a 2-dimensional multi-multiplication. Their approach was extended to more families of curves by Galbraith, Lyn and Scott [15]. Elliptic curves allowing two efficient endomorphisms were also studied in [26, 21] since scalar multiplication on these curves reduces to 4-dimensional multi-multiplication. This section focuses on GLV and GLS curves defined over finite field with characteristic greater than 2.

GLV CURVES

Gallant, Lambert and Vanstone considered curves with complex multiplication by $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}]$, with D small. We quickly review the examples of curves in [17] in the case where these are defined over an extension field $\mathbb{F}_{q^n}$, char$q > 2$, and show how to choose a factor base invariant under the action of an endomorphism such that the value of k is small.

Example 2. *Let $q \equiv 1 \pmod 4$ be a prime number. 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 $O \mapsto O$ 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 base $\mathcal{F}_{E_1,x}$. 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 base by a factor 2 as compared to the classical algorithm considering the equivalence class $\{Q, -Q\}$.*

Example 3. *Let $q \equiv 1 \pmod 3$ be a prime number. 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 $O \mapsto O$ 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 base as $\mathcal{F}_{E_2,x}$.*

GLS CURVES

In 2009, Galbraith, Lin and Scott [15] 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 1. *[15, 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 $\mathbb{F}_{q^{2n}}$ and $\hat{\phi}$ its dual, $r|\#E'(\mathbb{F}_{q^n})$ be a prime such that $r > 2q$. Let $\psi = \phi \circ \pi \circ \hat{\phi}$, π is the q-power Frobenius map on E. Let $u \in \mathbb{F}_{q^n}$ a non square in $\mathbb{F}_{q^n}$. 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 $\psi^n(P) + P = O_{E'}$.*

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

$$\begin{aligned} \mu : E' &\to \mathbb{P}_1 \\ Q &\mapsto (x(Q) + u^k x(Q)^q + u^{k(1+q)} x(Q)^{q^2} + \cdots + u^{k(1+q+\cdots+q^{n-2})} x(Q)^{q^{n-1}}, 1), \end{aligned}$$

where $k = 1 - q$.

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

Theorem 2. *We use the notation of Theorem 1. The relation collection in the index calculus algorithm on E' with the factor base $\mathcal{F}_{E',\mu}$ 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 base of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We denote by $S_{n+1,x} \in \mathbb{F}_{q^n}[X_1, \ldots, X_{n+1}]$ the $n+1$-th Semaev polynomial of E' and by $S'_{n+1,x} \in \mathbb{F}_{q^n}[X_{11}, X_{12}, \ldots, X_{1n}, \ldots, X_{n1}, \ldots, X_{nn}, X_{n+1}]$ the polynomial obtained by substituting in $S_{n+1,x}$ 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 $S'_{n+1,x}$ 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 base. For the point 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

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

The probability of finding a decomposition of a point $R \in E'(\mathbb{F}_{q^n})$ in the factorization base 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 base is approximately $\frac{q}{n}$. We conclude that the relation collection step of the index calculus algorithm on E' with the factor base $\mathcal{F}_{E',\mu}$ has complexity

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

□

GLV-GLS CURVES

Longa and Sica [26] 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 base.

Example 4. *[26, 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 base $\mathcal{F}_{E'_3,\mu}$ 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 base 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.

3.2 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 $\mathbb{F}_{q^n}$ and assume that $\#E(\mathbb{F}_{q^n}) = hr$, with h small and r a prime number. These curves are subject to the index calculus attack but also to the gGHS attack [19, 14, 23]. While an improved gGHS attack on the particular case of binary GLS curves by using endomorphisms is analyzed in [5], we focus here on the index calculus attack in the group $E(\mathbb{F}_{q^n})$.

ELLIPTIC CURVES DEFINED OVER SUBFIELDS

Assume that E admits a model over $\mathbb{F}_{q^{m_1}}$. Note that the curve E admits a Frobenius endomorphism π_{m_1} defined by

$$\pi_{m_1} : P = (x, y) \mapsto \pi_{m_1}(P) = (x^{q^{m_1}}, y^{q^{m_1}}). \tag{5}$$

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:

$$\chi_E(T) = T^2 - tT + q^{m_1}, \tag{6}$$

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 $\pi_{m_1}(P), \pi^2_{m_1}(P), \cdots, \pi^{m_2-1}_{m_1}(P)$ are also in $\mathcal{F}$ and we construct an equivalence class $\{P, \pi_{m_1}(P), \pi^2_{m_1}(P), \cdots, \pi^{m_2-1}_{m_1}(P)\}$. 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 3. *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*

$$\tilde{O}(\frac{q^{m_2}}{m_2}\left(2^{m_1(m_1-1)} e^{m_1} m_1^{-1/2}\right)^{\omega} m_1 ! + q^{m_2} m_1), \tag{7}$$

Proof. Here, we need to find $\frac{q^{m_2}}{m_2}$ relations. Recall that whenever a relation $Q = P_1 + P_2 + \ldots + P_{m_1}$ is computed, in order to write in the matrix of relations we compute first the discrete logs of these points with respect to the representatives of their equivalence classes. 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 $R \in E(\mathbb{F}_{q^n})$ in the factor basis is approximately

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

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

$$O(\frac{q^{m_2}}{m_2} A m_1 ! + q^{m_2} m_1),$$

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 (4) and bound A by $\tilde{O}\left(\left(2^{m_1(m_1-1)} e^{m_1} m_1^{-1/2}\right)^{\omega}\right)$. This yields the complexity in Equation (7). □

GLS BINARY CURVES

Binary GLS curves over extension field $\mathbb{F}_{2^{2m}}$ were studied in [22] and yield fast implementations of scalar multiplication. Let E be the elliptic curve defined over $\mathbb{F}_{2^{2m}}$ with equation

$$y^2 + xy = x^3 + ax + b,$$

with $a, b \in F_{2^m}$ and consider the curve E'

$$y^2 + xy = x^3 + a'x + b,$$

with $a' \in \mathbb{F}_{2^{2m}}$. Then E' is a quadratic twist of E and the isomorphism $\phi : E \to E'$ is given by $(x, y) \to (x, y + sx)$ with $s \in \mathbb{F}_{2^{4m}}$ such that $s^2 + s = a + a'$. Then the GLS endomorphism $\psi : E' \to E'$ is given by $(x, y) \to (x^q, y^q + s^q x^q + s x^q)$. One can easily see that the factor base $\mathcal{F}_{E',x}$ is invariant under ψ. This yields a factor 2 speed up in the relation collection step of the index calculus algorithm.

3.3 ELLIPTIC CURVES WITH A RATIONAL SMALL TORSION POINT

In [10], Faugère *et al.* proposed a method to reduce the factorization base 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 $T_2 = (0,0)$ is a 2-torsion point on E_1. Then, if $P_1 + \ldots + \ldots P_n + R = 0$ with $P_i \in \mathcal{F}_{E_1,x}$ yields a relation, we also have that $(P_1 + k_1T_2) + \ldots (P_n + k_nT_n) + R = 0$ with $\sum_{i=1}^{n} k_i = 0$ is a relation, provided that $P_i + k_iT_2 \in \mathcal{F}_{E_1,x}$. 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 base $\mathcal{F}_{E_1,x}$. Considering the equivalence class $Q, Q + T_2, -Q, -Q + T_2$ in the factor base, we can reduce its size by a factor 2 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 satisfied on any curve. To work around this problem, in [11] the authors consider a factor base defined with respect to a morphism φ invariant under the 2-torsion point of the curve.

Proposition 1. *[11, 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*

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

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 base with respect to both the torsion point of the curve and the endomorphism. To this purpose, we reformulate a result given by Charles [4] 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. 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 bases $\mathcal{F}_{E,\mu_1}$ 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:

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

A similar computation will show that $\mu_2(P+T) = \pm\mu_2(P)$. As shown in [11, Prop. 7], the polynomial $P_{n,\varphi}$ is invariant under the action of $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_n$. This implies that P_{n,μ_1} and P_{n,μ_2} are also invariant under the action of this group. □

Remark 1. *Heuristically, 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_{n,μ_1} *and* S_{n,μ_2} *will be augmented by a factor* d^{n-1} *in each variable as compared to the degree of* $S_{n,\varphi}$. *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 base 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:

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

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 base* $\mathcal{F}_{E_2,\mu}$. *By Theorem 4, the size of* $\mathcal{F}_{E_2,\mu}$ *is reduced by a factor* 6, *as compared to the factor base proposed in [11].*

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

$$y^2 + h_1(x)y = h_0(x), \tag{8}$$

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_∞ the point at infinity of H. Whenever we use the Mumford representation of a representative $D = (x^2 + u_0x + u_1, v_0x + v_1) \in J(H)$ we will simply write $D = (u_0, u_1, v_0, v_1)$.

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

$$\mathcal{F} = \{D = (P) - (P_\infty) \in J(H) : x(P) \in \mathbb{F}_{q^n}\}. \tag{9}$$

This approach yields attacks faster than generic methods for genus $g \geq 3$ (see [20]).

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 [25, 24] showed that hyperelliptic curves defined over $\mathbb{F}_{2^n}$ given by Equation (8) 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

$$\mathcal{F} = \{D = (P) - (P_\infty) \in J(\mathbb{F}_{2^n}) : x(P) \in \mathbb{F}_{2^n}\}. \tag{10}$$

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

$$\chi_H(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 2^{n(g-1)} T + 2^{ng}, \tag{11}$$

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 [20]. Indeed, the analysis in [20] 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 [20], but by taking into account logarithmic factors, the complexity of the double large prime variation algorithm is $O(\#\mathcal{F}^{2-2/g} log(\#\mathcal{F}))$.

In our case, given the fact that we do a look up in an equivalence relation of size n, this yields $O(n^2(\frac{2^n}{n})^{2-2/g}) = O(n^{2/g}(2^n)^{2-2/g})$ for $g \geq 3$. This is to be compared against $O(n(2^n)^{2-2/g})$, which is the complexity of the algorithm in [20] for Koblitz curves.

4.2 BUHLER-KOBLITZ CURVES.

Buhler-Koblitz (BK) curves [3] 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

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

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 use the factor base defined by Equation 9. This factor base is invariant with respect to φ and we can reduce its size by a factor 5. As shown in [1, 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 base up to a factor 10 by considering a GLS endomorphism construction.

4.3 FURUKAWA-KAWAZOE-TAKAHASHI CURVES.

The Furukawa-Kawazoe-Takahashi (FKT) curves [12] 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

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

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 factor base $\mathcal{F}$ in Equation 9. This factor base 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 [21] 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 $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $c^2 \in \mathbb{F}_q$. The construction of the endomorphisms in [21] 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 [21] do not have small order and hence it does not seem possible to identify a factor base 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 [27].

Since the curves H_1 and H_2 are defined over $\mathbb{F}_q$, the qth-power Frobenius morphism π_q is an endomorphism of the Jacobian. We note that the factor base $\mathcal{F}$ in Equation 9 is invariant under π_q. So, we construct the equivalence class $\{D, \pi_q(D)\}$ in $\mathcal{F}$ and reduce the size of the factor base $\mathcal{F}$ by a factor 2.

5 COMPLEXITY ANALYSIS AND BENCHMARKS

We have implemented in MAGMA [2] the relation search step of the index calculus attack for the discrete logarithm problem on elliptic curves given in Sections 3.2 and 3.1. 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. .

Recall that 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 each class which will be the representative of it, and put it in the reduced base. 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 base. To implement the reduced base, we used the **AssociativeArray** data structure in MAGMA [2] which allows efficient look up when checking for the equivalence classes. However, the cost of this search remains negligible with respect to the cost of computation of Gröbner bases.

In Table 1, we compare the theoretical complexities of the index calculus algorithm with reduced base, with full base and Pollard's rho method [7]. In Table 2 and Table 3, we compare the runtime of the relation collection for the full base and for the reduced base 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. The expected ratio that we obtain for $GLV - GLS$ curves is 6 as shown in Section 3.1. In Table 4, for $n \in \{7, 11, 13, 17\}$, we compare the runtime of the relation collection algorithm for the full base and for the reduced base 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 base 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 100 runs for each parameter choice and we can see that our reduced base yields a decomposition phase which is faster by a factor greater than the size of the equivalence class in each case.

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

Table 1: Complexity Analysis.

	Reduced base	Full base	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: Relation collection stage on elliptic curves defined over composite extension field.

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

Table 3: Relation collection stage on GLV-GLS curve defined over $\mathbb{F}_{q^2}$.

q	Time reduced base	Time full base	Reduction ratio
739	1.412 sec.	5.722 sec.	4.052
1051	3.475 sec.	14.909 sec.	4.290
2731	9.001 sec.	42.628 sec.	4.73
3163	11.037 sec.	58.304 sec.	5.28

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] J. W. Bos et al. "High-Performance Scalar Multiplication Using 8-Dimensional GLV/GLS Decomposition". In: *Cryptographic Hardware and Embedded Systems - CHES 2013*. Ed. by G. Bertoni and J.-S. Coron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 331–348.

[2] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language*. 1997. URL: `http://magma.maths.usyd.edu.au/magma/`.

[3] J.-P. Buhler and N. Koblitz. "Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems". In: *Bulletin of the Australian Mathematical Society* 58.1 (1998), pp. 147–154.

[4] D. Charles. *On the existence of distortion maps on ordinary elliptic curves*. 2006. URL: `https://eprint.iacr.org/2006/128`.

[5] J.-J. Chi-Domínguez, F. Rodríguez-Henríquez, and B. Smith. "Extending the GLS endomorphism to speed up GHS Weil descent using Magma". In: *Finite Fields and Their Applications* in press (2021).

[6] C. Diem. "On the discrete logarithm problem in elliptic curves". In: *Compos. Math.* 147.(1) (2011), pp. 75–104.

[7] I. M. Duursma, P. Gaudry, and F. Morain. "Speeding up the Discrete Log Computation on Curves with Automorphisms". In: *Advances in Cryptology - ASIACRYPT '99, International Conference on the Theory and Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, Proceedings*. Ed. by K.-Y. Lam, E. Okamoto, and C. Xing. Vol. 1716. Lecture Notes in Computer Science. Springer, 1999, pp. 103–121.

[8] J.-C. Faugère. "A new efficient algorithm for computing Gröbner bases (F_4)". In: *Journal of Pure Applied Algebra* 139.1-3 (1999), pp. 99–110.

[9] J.-C. Faugère. "A new efficient algorithm for computing Gröbner bases without reduction to zero ($F5$)". In: *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*. Ed. by T. Mora. 2002.

[10] J.-C. Faugère et al. "Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm". In: *Journal of Cryptology* (2013), pp. 1–40.

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

Curves	n	Time reduced base	Time full base	Reduction ratio	Time Pollard-Rho
$y^2 + (x^2 + x + 1)y = x^5 + 1$	7	0.011 sec.	0.066 sec.	6.07	0.004 sec.
$y^2 + (x^2 + x + 1)y = x^5 + x$	11	0.340 sec.	2.969 sec.	8.73	0.056 sec.
	13	0.994 sec.	8.566 sec.	8.60	0.274 sec.
	17	17.891 sec.	176.936 sec.	9.88	4.994 sec.
$y^2 + y = x^5 + x^3$	11	0.119 sec.	1.235 sec.	10.37	0.061 sec.
	17	11.597 sec.	189.918 sec.	16.37	5.386 sec.
$y^2 + y = x^5 + x^3 + 1$	7	0.013 sec.	0.081 sec.	6.23	0.009 sec.
	11	0.337 sec.	1.996 sec.	5.92	0.11 sec.
$y^2 + xy = x^5 + x^2 + 1$	7	0.021 sec.	0.131 sec.	6.23	0.01 sec.
	17	6.920 sec.	109.265 sec.	15.78	0.204 sec.
$y^2 + (x^2 + x)y = x^5 + 1$	7	0.015 sec.	0.122 sec.	8.13	0.010 sec
	17	15.279 sec.	205.313 sec.	13.43	0.011 sec.

[11] J.-C. Faugère et al. “Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus”. In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark*. Springer Verlag, 2014.

[12] E. Furukawa, M. Kawazoe, and T. Takahashi. “Counting Points for Hyperelliptic Curves of Type $y^2 = x^5 + ax$ over Finite Prime Fields”. In: *Selected Areas in Cryptography*. Ed. by M. Matsui and Robert J. Zuccherato. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 26–41.

[13] S. D. Galbraith and S. W. Gebregiyorgis. “Summation Polynomial Algorithms for Elliptic Curves in Characteristic Two”. In: *Selected Areas in Cryptography SAC 2020*. Ed. by W. Meier and D. Mukhopadhyay. Vol. 8885. Lecture Notes in Computer Science. Springer, 2020, pp. 409–427.

[14] S. D. Galbraith, F. Hess, and N. P. Smart. “Extending the GHS Weil descent attack”. In: (2002), pp. 29–44.

[15] S. D. Galbraith, X. Lin, and M. Scott. “Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves”. In: *Journal of Cryptology* 24.3 (2011), pp. 446–469.

[16] S. D. Galbraith et al. “On Index Calculus Algorithms for Subfield Curves”. In: *Selected Areas in Cryptography - SAC 2020 - 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers*. Ed. by O. Dunkelman, M. J. Jacobson Jr., and C. O’Flynn. Vol. 12804. Lecture Notes in Computer Science. Springer, 2020, pp. 115–138.

[17] R. P. Gallant, R. J. Lambert, and S. A. Vanstone. “Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms”. In: *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*. Ed. by J. Kilian. Vol. 2139. Lecture Notes in Computer Science. Springer, 2001, pp. 190–200.

[18] P. Gaudry. “Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem”. In: *J. Symb. Comput* 44.12 (2009), pp. 1960–1702.

[19] P. Gaudry, F. Hess, and N. P. Smart. “Constructive and Destructive Facets of Weil Descent on Elliptic Curves”. In: *Journal of Cryptology* 15 (2000), p. 2002.

[20] P. Gaudry et al. “A double large prime variation for small genus hyperelliptic index calculus”. In: *Math. Comput.* 76.257 (2007), pp. 475–492.

[21] A. Guillevic and S. Ionica. “Four-Dimensional GLV via the Weil Restriction”. In: *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*. Ed. by K. Sako and P. Sarkar. Vol. 8269. Lecture Notes in Computer Science. Springer, 2013, pp. 79–96.

[22] D. Hankerson, K. Karabina, and A. Menezes. “Analyzing the Galbraith-Lin-Scott Point Multiplication Method for Elliptic Curves over Binary Fields”. In: *IEEE Trans. Computers* 58.10 (2009), pp. 1411–1420.

[23] F. Hess. “The GHS Attack Revisited”. In: *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*. Ed. by Eli Biham. Vol. 2656. Lecture Notes in Computer Science. Springer, 2003, pp. 374–387.

[24] T. Lange. *Efficient Arithmetic on Hyperelliptic Koblitz Curves*. 2001. URL: https://www.hyperelliptic.org/tanja/preprints/preprint.pdf.

[25] T. Lange. *Hyperelliptic curves allowing fast arithmetic webpage*. 2001. URL: https://www.hyperelliptic.org/tanja/KoblitzC.html.

[26] P. Longa and F. Sica. "Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication". In: *Journal of Cryptology* 27 (2014), pp. 248–283.

[27] Benjamin Smith. "The $\mathbb{Q}$-curve Construction for Endomorphism-Accelerated Elliptic Curves". In: *J. Cryptol.* 29.4 (2016), pp. 806–832.