A Simple Method for Obtaining Relations Among Factor Basis Elements for Special Hyperelliptic Curves

Palash Sarkar and Shashank Singh

Applied Statistics Unit
Indian Statistical Institute
palash@isical.ac.in, sha2nk.singh@gmail.com

Abstract. Nagao had proposed a decomposition method for divisors of hyperelliptic curves defined over a field $\mathbb{F}_{q^n}$ with $n \geq 2$. Joux and Vitse had later proposed a variant which provided relations among the factor basis elements. Both Nagao's and the Joux-Vitse methods require solving a multi-variate system of non-linear equations. In this work, we revisit Nagao's approach with the idea of avoiding the requirement of solving a multi-variate system. While this cannot be done in general, we are able to identify special cases for which this is indeed possible. Our main result is for curves $C : y^2 = f(x)$ of genus g defined over $\mathbb{F}_{q^2}$ having characteristic greater than two. If $f(x)$ has at most g consecutive coefficients which are in $\mathbb{F}_{q^2}$ while the rest are in $\mathbb{F}_q$, then we show that it is possible to obtain a single relation in about $(2g+3)!$ trials. The method combines well with a sieving method proposed by Joux and Vitse. Our implementation of the resulting algorithm provides examples of factor basis relations for $g = 5$ and $g = 6$. We believe that none of the other methods known in the literature can provide such relations faster than our method. Other than obtaining such decompositions, we also explore the applicability of our approach for $n > 2$ and also for binary characteristic fields.
Keywords: hyperelliptic curves, index calculus algorithm, Nagao's decomposition, Joux-Vitse sieving.

1 Introduction

For a finite cyclic group $\langle g \rangle$ of order q, the discrete log problem (DLP) is the following: Given g and $h \in \langle g \rangle$, find an i in $\{0, 1 \ldots, q-1\}$ such that $h = g^i$. For certain groups, the discrete log problem is known to be computationally hard. Such groups find applications in designing cryptographic protocols such as the Diffie-Hellman key agreement protocol [2] which was originally proposed over a suitable subgroup of the multiplicative group of an appropriately chosen finite field.

Cryptographic use of groups obtained from elliptic curves over finite fields was introduced independently by Miller [13] and Koblitz [10]. A few years later, the use of groups obtained from hyperelliptic curves (HEC) was proposed by Koblitz [11]. In the present state-of-the-art, there are known choices for both elliptic curves and genus two hyperelliptic curves which lead to the realisation of secure cryptographic schemes.

From the cryptanalytic viewpoint, there have been attempts to find algorithms for solving DLP in cryptographic groups. Presently, the main approach to solving the DLP is the so-called index calculus algorithm which consists of three steps. The first step is to identify a factor basis which is a subset of G. Elements of the factor basis are in some sense "simpler" than a general element of G. The next step is to obtain a method whereby relations can be obtained between the elements of the factor basis. These relations are converted into linear relations between the discrete logs of the elements of the factor basis. Typically the relations which arise are extremely sparse and the resulting system of linear equations can be solved using either the Lanczos or the block Wiedemann algorithm. This yields the discrete logs of the elements of

the factor basis. The final step is to obtain a decomposition of the target element over the factor basis. Since the discrete log of the factor basis elements have already been computed, the discrete log of the target element can now be determined. For certain variants of the index calculus algorithm, the relation collection step itself ensures that relations are obtained between the target element and the elements of the factor basis. In such cases, the discrete log of the target element is obtained immediately after the linear algebra step.

We briefly mention some of the earlier works on index calculus algorithms for hyperelliptic curves which are relevant to our work. Adleman, DeMarrais and Huang Decomposition [1] provided an index calculus algorithm for function fields which provided a sub-exponential time algorithm for higher genus hyperelliptic curves. Later work along this line have been reported in [5, 3, 4, 18].

For small genus curves, the algorithm is no longer a sub-exponential time algorithm. It can still, however, be faster than the generic Pollard rho algorithm. This was described by Gaudry [6] which led to an algorithm that was used to solve certain HEC-DLP challenges. Variants of Gaudry's algorithm called the large prime variant [17] and the double large prime variant [8] were proposed later. A more recent work [15] shows an alternative to Gaudry's decomposition method.

The above mentioned algorithms work for hyperelliptic curves defined over a finite field $\mathbb{F}_q$ for any prime power q. When the field is $\mathbb{F}_{q^n}$, for $n \geq 2$, Nagao [14] presented a new decomposition method. In his method, the factor basis consists of divisors represented by single points whose x-coordinates are in the base field $\mathbb{F}_q$. Nagao showed that testing about $(ng)!$ random divisors results in obtaining one divisor which is smooth over the factor basis. Testing each divisor requires solving a system of $ng(n-1)$ non-linear equations in $ng(n-1)$ variables.

A variant of this method was proposed by Joux and Vitse [9] who showed how to obtain relations among the elements of the factor basis. To obtain relations, the Joux-Vitse method consists of initially solving a system of $ng(n-1) + 2(n-1)$ equations in $ng(n-1) + 2n$ variables. Any such solution provides two free variables which are then varied to generate triangular systems of equations. Solving about $(ng+2)!$ of these simpler systems provides a single relation. Joux and Vitse use their method as an intermediate step in solving DLP for certain elliptic curves.

Nagao had reported [14] solutions for the systems of non-linear equations arising in his method for (n, g) equal to $(2, 2), (2, 3)$ and $(3, 2)$. It was mentioned that for other values of the pair (n, g) it becomes difficult to solve the resulting system of non-linear equations. This issue was also briefly reiterated by Joux and Vitse [9] though in their application to elliptic curves they only required (n, g) to be $(2, 3)$ and $(3, 2)$.

Our Contributions: We follow the approach of Nagao and Joux-Vitse and consider the problem of obtaining relations among the elements of the factor basis proposed by Nagao. Our goal is to obtain a method which avoids solving a system of non-linear equations. Though this cannot be done in general, for certain special kinds of curves we show how this can be done.

Our main result is for curves defined over quadratic extension fields of characteristic greater than two. Suppose $C : y^2 = f(x)$ is such a curve of genus $g \geq 1$. If there are no restrictions on the coefficients of $f(x)$, we show that one relation can be obtained in about $(4g+4)!$ trials. This quickly becomes impractical. For a sub-class of curves we provide a better result. Suppose C is such that at most g consecutive coefficients of $f(x)$ are in $\mathbb{F}_{q^2}$ while the rest of the coefficients of $f(x)$ are in the base field $\mathbb{F}_q$. For such curves we show that one relation can be obtained

in $(2g+3)!$ trials. This is combined with a sieving method introduced by Joux and Vitse [9]. The resulting method has been implemented and we report examples of relations among factor basis elements for $g = 5$ and $g = 6$. This is to be contrasted with the previous methods of Nagao and Joux-Vitse which only reported examples for $g = 2$ and $g = 3$.

For the special type of curves considered here, the new technique suggests a faster method for carrying out discrete log computations for $g = 4$ and $g = 5$. For generating relations among the factor basis elements, the new method is faster than Nagao's and the Joux-Vitse methods. So, the relations are to be generated using the method proposed here. On the other hand, the new method (as well as the Joux-Vitse method) does not provide a decomposition of a divisor over the factor basis. So, Nagao's technique has to be used for this step. This, however, is a one-time decomposition. The speed-up in the discrete log computation arises from replacing Nagao's technique by the new method for the relation collection step.

We describe other results that can be obtained using our techniques. Suppose C is a curve defined over $\mathbb{F}_{q^n}$ with no restriction on n (i.e., $n \geq 1$) such that only the constant term of $f(x)$ is a general element of $\mathbb{F}_{q^n}$ while all other elements are in $\mathbb{F}_q$. For such curves we show that it is possible to easily obtain $q/(2(2g+1)!\,)$ relations. When $g = 1$, i.e., for elliptic curves, this gives a method for obtaining $q/12$ relations. The obtained relations are of a special type and can be used to reduce the size of the factor basis. Curves defined over characteristic two fields are also briefly considered and we describe methods for obtaining factor basis relations for certain sub-classes of such curves.

2 Background on Hyperelliptic Curves

We start with a brief description of hyperelliptic curves based on the discussion given in [12]. Let K be a field and $\overline{K}$ be its algebraic closure. A hyperelliptic curve C of genus $g \geq 1$ over K is given by an equation of the following form.

$$C : y^2 + h(x)y = f(x) \tag{1}$$

where $f(x) \in K[x]$ is a polynomial of degree $2g+1$ and $h(x) \in K[x]$ is a polynomial of degree at most g. A point $(x, y) \in \overline{K} \times \overline{K}$ is said to be singular if it simultaneously satisfies the curve equation C and also the partial derivatives $2y + h(x) = 0$ and $h'(x)y = f'(x)$. If $\mathrm{char}(K) \neq 2$, a change of variables $x \to x$, $y \to (y - h(x)/2)$ transforms the curve to the form $y^2 = f(x)$ where $\deg(f) = 2g + 1$. Further, if $h(x) = 0$, then C has no singular points if and only if $f(x)$ has no repeated roots in $\overline{K}$. If C does not have any singular point, then it is said to be non-singular. Only non-singular curves are considered for cryptographic applications. When $g = 1$, the corresponding curves are called elliptic curves.

Let L be an extension of K. The set of all L-rational points of C, denoted $C(L)$ consists of all points $(x, y) \in L \times L$ which lie on C (i.e., satisfy C) along with a special point at infinity denoted ∞. The set $C(\overline{K})$ will simply be denoted as C. The points in C other than ∞ are called finite points. Let $P(x, y)$ be a finite point on C. The notation $x(P)$ and $y(P)$ denote the x-coordinate and y-coordinate of P. The opposite of P, denoted as $\widetilde{P}$, is defined to be $\widetilde{P} = (x, -y - h(x))$. The opposite of ∞ is itself, i.e., $\widetilde{\infty} = \infty$. A finite point P such that $\widetilde{P} = P$ is said to be special; otherwise P is said to be ordinary.

The coordinate ring of C over K is defined to be $K[x, y]/(y^2 + h(x)y - f(x))$ and is denoted as $K[C]$. Any element of $K[C]$ can be written as $a(x) - yb(x)$ for some polynomials $a(x), b(x) \in K[x]$. A non-zero polynomial $G(x, y) = a(x) - yb(x)$ in $K[C]$ is assigned degree

$\deg(G) = \max(2\deg_x(a), 2g+1+2deg_x(b))$. Similarly, one defines the coordinate ring $\overline{K}[C]$ of C over $\overline{K}$. An element of $\overline{K}[C]$ is called a polynomial function and it represents a polynomial map from C to $\overline{K}$. The norm of $G(x,y) = a(x) - yb(x)$ is defined to be $N(G) = a^2(x) - f(x)b^2(x)$. The norm $N(G)$ of G is a polynomial in the single variable x and the degree of $N(G)$ in x is equal to the degree of $G(x,y)$.

Since C is non-singular, the polynomial $y^2 + h(x)y - f(x)$ is necessarily irreducible over $\overline{K}$ and hence $\overline{K}[C]$ is an integral domain. The function field $K(C)$ of C over K is the field of fractions of $K[C]$. Similarly, the function field $\overline{K}(C)$ is the field of fractions of $\overline{K}(C)$. The elements of $\overline{K}(C)$ are called rational functions on C.

Let $G(x,y) = a(x) - y(b)$ be a non-zero polynomial function, i.e., a non-zero element of $\overline{K}[C]$ and let P be a point in C. The order of G at P, denoted as $\mathrm{ord}_P(G)$, is defined in the following manner.

1. If $P = (\alpha, \beta)$ is a finite point, then let r be the highest power of $(x-\alpha)$ which divides both $a(x)$ and $b(x)$ and write $G(x,y) = (x-\alpha)^r(a_0(x) - yb_0(x))$. If $a_0(\alpha) - \beta b_0(\alpha) \neq 0$, then let $s = 0$; otherwise, let s be the highest power of $(x-\alpha)$ which divides $N(a_0(x) - yb_0(x)) = a_0^2(x) - a_0(x)b_0(x)h(x) - b_0^2(x)f(x)$. If P is an ordinary point, then define $\mathrm{ord}_P(G) = r + s$; if P is a special point, then define $\mathrm{ord}_P(G) = 2r + s$.
2. If $P = \infty$, then $\mathrm{ord}_P(G) = -\max(2\mathrm{deg}_x(a), 2g + 1 + 2\mathrm{deg}_x(b))$.

The order of a rational function $R = G/H$ at a point P is defined to be $\mathrm{ord}_P(R) = \mathrm{ord}_P(G) - \mathrm{ord}_P(H)$.

A divisor D is a formal sum $D = \sum_{P \in C} m_P(P)$ of points in C, where m_P's are integers and only finitely many of the m_P's are zero. The degree of D is the sum $\sum_{P \in C} m_P$ and the order of D at P is m_P. Let $D_1 = \sum m_P(P)$ and $D_2 = \sum n_P(P)$ be two divisors. Their gcd is defined to be $\gcd(D_1, D_2) = \sum \min(m_P, n_P)(P) - (\sum \min(m_P, n_P))(\infty)$.

The set $\mathbf{D}$ of all divisors forms an abelian group and the set $\mathbf{D}^0$ of all degree 0 divisors form a subgroup of this group. Let R be a rational function in $\overline{K}(C)$. The divisor of R is defined to be $\mathrm{div}(R) = \sum_{P \in C} \mathrm{ord}_P(R)(P)$, where $\mathrm{ord}_P(R)$ is the order of R at the point P. It can be shown that $\mathrm{div}(R)$ is a zero divisor. A divisor is said to be principal if it is the divisor of a rational function. The set $\mathbf{P}$ of all principal divisors forms a subgroup of $\mathbf{D}^0$. The quotient group

$$J_C \triangleq \mathbf{D}^0/\mathbf{P} \tag{2}$$

is called the Jacobian of the curve C.

Two zero divisors D_1 and D_2 are said to be equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is the divisor of a rational function and so $D_1 - D_2 \in \mathbf{P}$. For a divisor D, its support $\mathrm{supp}(D)$ is defined to be the set $\{P \in C : m_P \neq 0\}$.

A divisor of the form $D = \sum m_i(P_i) - (\sum m_i)(\infty)$ is said to be semi-reduced if the following conditions hold: (i) $m_i \geq 0$, (ii) P_i's are finite points, (iii) if $P_i \in \mathrm{supp}(D)$, then $\widetilde{P_i} \notin \mathrm{supp}(D)$ unless $P_i = \widetilde{P_i}$ in which case $m_i = 1$. For a semi-reduced divisor D, if $\sum m_i \leq g$, then D is said to be a reduced divisor. It can be shown that for each divisor D in $\mathbf{D}^0$, there is a unique reduced divisor D_1 such that $D_1 \sim D$.

Let σ be an automorphism of $\overline{K}$ over K. Then for a point $P = (x,y)$ on C, the point $P^\sigma \triangleq (x^\sigma, y^\sigma)$ is also a point on C. A divisor $D = \sum m_P(P)$ is said to be defined over K if $D^\sigma \triangleq \sum m_P(P^\sigma)$ is equal to D for all automorphisms σ of $\overline{K}$ over K. A principal divisor is defined over K if and only if it is the divisor of a rational function that has coefficients in K.

The set $J_C(K)$ of all divisor classes in J_C that have a representative that is defined over K is a subgroup of J_C.

For cryptographic applications, it is required to choose K and C such that the order of $J_C(K)$ has a large prime factor and cryptographic schemes are implemented over the corresponding prime order subgroup of $J_C(K)$. Determining K and C such that $J_C(K)$ is suitable for doing cryptography is a non-trivial problem. A requirement for doing cryptography is to be able to add elements of $J_C(K)$, i.e., to be able to add divisors.

In terms of computation, it is convenient to view reduced divisors via their Mumford representations. A divisor in this representation is given by a pair of polynomials $(u(x), v(x))$ with $u(x), v(x) \in K[x]$ such that $u(x)$ is monic, $\deg(v) < \deg(u) \leq g$ and u divides $v^2 + vh - f$. Such a pair of polynomials represents the divisor $\gcd(\mathrm{div}(u(x)), \mathrm{div}(v(x) - y))$ and this divisor is simply denoted as $\mathrm{div}(u, v)$. If $\deg(u) < g$, then the divisor is said to be degenerate, otherwise it is called non-degenerate. When elements of $J_C(K)$ are given by their Mumford representation their addition in $J_C(K)$ is made possible by Cantor's algorithm.

3 Nagao Type Decompositions

Let $K = \mathbb{F}_{q^n}$ be a field of characteristic greater than 2. Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus g so that $f(x)$ is a monic polynomial of degree $2g + 1$. The assumption on the characteristic is not essential and the method can be modified to work over characteristic two fields.

Define the factor basis to be the following.

$$\mathcal{FB} = \{D \in J_C(K) : D = (P) - (\infty), P \in C(K), x(P) \in \mathbb{F}_q\}. \tag{3}$$

In other words, the factor basis consists of all divisors of the form $(P) - (\infty)$ where P is an $\mathbb{F}_{q^n}$-rational point on C and the x-coordinate of P is in $\mathbb{F}_q$. There is no restriction on the y-coordinate of P, i.e., it is a general element of $\mathbb{F}_{q^n}$.

We discuss how a divisor $D = \mathrm{div}(u(x), v(x))$ in $J_C(K)$ can be decomposed over the factor basis. Given D, consider a bi-variate polynomial

$$G(x, y) = u(x)\lambda(x) + (y - v(x))\mu(x) \tag{4}$$

where $\lambda(x)$ and $\mu(x)$ are in $\mathbb{F}_{q^n}[x]$ and are of degrees m_1 and m_2 respectively. The choices of the degrees m_1 and m_2 are to be made appropriately as we discuss later. If α is a root of $u(x)$ and $\beta = v(\alpha)$, then (α, β) is a zero of $G(x, y)$. This shows that all points of D are zeros of $G(x, y)$. The choices of $\lambda(x)$ and $\mu(x)$ lead to additional zeros of $G(x, y)$ through which a decomposition is obtained.

Eliminating y between $y^2 = f(x)$ and $G(x, y) = 0$ gives the polynomial

$$S(x) = (-u(x)\lambda(x) + v(x)\mu(x))^2 - \mu^2(x)f(x) \tag{5}$$

By the property of Mumford representation, $u(x)$ divides $v^2(x) - f(x)$ and so $u(x)|S(x)$. So,

$$H(x) = \frac{S(x)}{u(x)} = \frac{(-u(x)\lambda(x) + v(x)\mu(x))^2 - \mu^2(x)f(x)}{u(x)} \tag{6}$$

is a polynomial. Let γ be such that $H(\gamma) = 0$ and $u(\gamma) \neq 0$. Further, let $\delta = v(\gamma) - (u(\gamma)\lambda(\gamma))/\mu(\gamma)$. Then (γ, δ) is a zero of $G(x, y)$ which is not a point of D.

Suppose $H(x)$ is in $\mathbb{F}_q[x]$ and is smooth over $\mathbb{F}_q$. Then all roots of $H(x)$ are in $\mathbb{F}_q$. Let these roots be $\gamma_1, \ldots, \gamma_h$, where $h = \deg_x(H(x))$. Define $\delta_i = v(\gamma_i) - (u(\gamma_i)\lambda(\gamma_i))/\mu(\gamma_i)$. Then we have

$$\mathrm{div}(G) = D + \sum_{i=1}^{h}((\gamma_i, \delta_i) - (\infty)).$$

Since G is a rational function, we obtain the following relation:

$$-D \sim \sum_{i=1}^{h}((\gamma_i, \delta_i) - (\infty)). \tag{7}$$

The divisors $(\gamma_i, \delta_i) - (\infty)$ are in the factor basis and so the above relation provides a decomposition of D over the factor basis.

Nagao describes the above decomposition with the only difference that he refers to the Riemann-Roch theorem to define the polynomial $G(x, y)$. That does not appear to be necessary. One can simply start with a bi-variate polynomial of the form in (4) to see how a decomposition is obtained.

The number of points in the decomposition is determined by the degree of $H(x)$. The degrees of $S(x)$ and $H(x)$ are separately determined in two cases as follows:

$\mathbf{D} = \mathbf{div}(\mathbf{u}(\mathbf{x}), \mathbf{v}(\mathbf{x}))$ with $v(x) \neq 0$: In this case, we have

$$\left.\begin{aligned} \deg_x(S) &= \max(2\deg_x(u) + 2\deg_x(\lambda), 2\deg_x(v) + 2\deg_x(\mu), 2g + 1 + 2\deg_x(\mu)); \\ \deg_x(H) &= \max(\deg_x(u) + 2\deg_x(\lambda), 2\deg_x(v) + 2\deg_x(\mu) - \deg_x(u), \\ &\qquad 2g + 1 + 2\deg_x(\mu) - \deg_x(u)); \end{aligned}\right\} \tag{8}$$

When $\deg_x(u) = g$, the degrees of $S(x)$ and $H(x)$ are respectively $\max(2g+2m_1, 2g+1+2m_2)$ and $\max(g + 2m_1, g + 1 + 2m_2)$.

$\mathbf{D} = \mathbf{div}(\mathbf{1}, \mathbf{0})$: In this case, D is the Mumford representation of 0 and (7) provides a relation among the elements of the factor basis. Since $u(x) = 1$ and $v(x) = 0$, the degrees of $S(x)$ and $H(x)$ are $\deg_x(S) = \max(2\deg_x(\lambda), 2g + 1 + 2\deg_x(\mu))$ and $\deg_x(H) = \max(2\deg_x(\lambda), 2g + 1 + 2\deg_x(\mu)$.

In the above description, there is no restriction on the extension degree n, i.e., $n \geq 1$. Both Nagao and Joux-Vitse, on the other hand, consider $n \geq 2$. In the rest of this work, we will also consider $n \geq 2$. The case for $n = 1$ has been worked out in details in [15].

For $n \geq 2$, we briefly mention how a nonlinear system of equations arises and the conditions on the number of variables and equations for the system to have a solution. Consider the decomposition of a divisor $D = \mathrm{div}(u(x), v(x))$ and suppose the degree of $H(x)$ given by (6) is h.

The control variables in the expression for $H(x)$ in (6) are the coefficients of $\lambda(x)$ and $\mu(x)$ which are $\lambda_0, \ldots, \lambda_{m_1}$ and $\mu_0, \ldots, \mu_{m_2}$. Either λ_{m_1} or μ_{m_2} will be 1 to ensure that $H(x)$ is monic. So, there are a total of $m_1 + m_2 + 1$ variables and each of these are elements of $\mathbb{F}_{q^n}$. Expressing these using a polynomial basis over $\mathbb{F}_q$ gives a total of $n(m_1 + m_2 + 1)$ variables over $\mathbb{F}_q$.

For $H(x)$, apart from the leading coefficient (which is one), the other h coefficients can be expressed in terms of the $n(m_1 + m_2 + 1)$ variables over $\mathbb{F}_q$ obtained from $\lambda(x)$ and $\mu(x)$. Requiring the coefficients of $H(x)$ to be elements of $\mathbb{F}_q$ leads to a total of $h(n-1)$ multivariate

non-linear equations over $\mathbb{F}_q$ in $n(m_1 + m_2 + 1)$ variables over $\mathbb{F}_q$. If the number of variables is less than the number of equations, then the system is under-defined and it is not possible to solve such a system. So, we require the following condition.

$$n(m_1 + m_2 + 1) \geq h(n-1). \tag{9}$$

The choices of m_1 and m_2 made by Nagao and Joux-Vitse are the following.

1. For a divisor $D = \mathrm{div}(u(x), v(x))$ with $\deg_x(u) = g$, Nagao chooses $m_1 = \lfloor (n-1)g/2 \rfloor$ and $m_2 = \lfloor ((n-1)g - 1)/2 \rfloor$ so that $m_1 + m_2 + 1 = ng - g$ and the degree h of $H(x)$ is ng. As a result, both sides of (9) equal $ng(n-1)$ and the relation holds with equality. Solving a system of $ng(n-1)$ equations in $ng(n-1)$ variables provides an $H(x)$ which is in $\mathbb{F}_q[x]$. Such an $H(x)$ is not necessarily smooth. Trying about $(ng)!$ random divisors results in a smooth $H(x)$ and hence a decomposition of the corresponding divisor. In the context of discrete log, the random divisors are generated using a random walk technique as in [6].
2. Joux and Vitse consider obtaining a relation among the elements of the factor basis and so $v(x) = 0$. They choose $m_1 = \lfloor m/2 \rfloor$ and $m_2 = \lfloor (m-1)/2 \rfloor - g$. In this case, the degree h of $H(x)$ is $\max(2m_1, g + 1 + 2m_2) = m$ and $m_1 + m_2 + 1 = m - g$. So, the left side of (9) is $n(m-g)$ and the right side is $m(n-1)$. Joux and Vitse set m to be equal to $ng+2$ whence the number of equations is $m(n-1) = ng(n-1) + 2(n-1)$ and the number of variables is $n(m-g) = ng(n-1) + 2n$. So, there are two extra variables which play the role of control variables. Solution of the system of equations results in a triangular system in the two control variables. Varying the control variables generates solutions of the triangular system. Since the degree of $H(x)$ is $ng+2$ after about $(ng+2)!$ trials it is possible to find a relation.

4 Obtaining Relations Between Factor Basis Elements

For $n \geq 2$, the decomposition technique proposed by Nagao [14] and the one by Joux and Vitse [9] both require solving a system of non-linear equations using Gröbner basis techniques. We consider whether it is possible to avoid this step of the decomposition. In general this is not possible, but, there are special cases where this is indeed possible.

The setting is that of Section 3. Let $\mathbb{F}_q$ be a field of characteristic greater than two and for an integer $n > 1$, we are interested in the Jacobian $J_C(\mathbb{F}_{q^n})$ of the curve $C : y^2 = f(x)$. The factor basis is as defined in (3). Following Joux and Vitse, we are interested in obtaining relations between elements of the factor basis. In other words, we wish to obtain relations of the form $D_1 + \cdots + D_m = 0$ where $D_1, \ldots, D_m \in \mathcal{FB}$. We will call such a decomposition to be an m-point decomposition.

The crux of the decomposition method is to obtain polynomials $\lambda(x), \mu(x) \in \mathbb{F}_{q^n}[x]$ such that $H(x) = \lambda^2(x) - \mu^2(x)f(x)$ defined in (6) (with $u(x) = 1$ and $v(x) = 0$) is in $\mathbb{F}_q[x]$. Our idea is that given $f(x)$, we try to select $\lambda(x)$ and $\mu(x)$ appropriately such that $H(x)$ is guaranteed to be over $\mathbb{F}_q$. The choices of $\lambda(x)$ and $\mu(x)$ depend upon the form of $f(x)$ and the attempt is to adjust for the coefficients of $f(x)$ which are in $\mathbb{F}_{q^n}$. Smoothness of the resulting $H(x)$ is not guaranteed and has to be ensured iteratively. For iteration to be possible, we have to ensure that there are some control variables which can be varied to obtain different possible $H(x)$'s.

4.1 Subfield Curves

If all coefficients of $f(x)$ are in $\mathbb{F}_q$, then C is called a subfield curve. Let C be a subfield curve and consider the extension degree n to be even.

Choose $\mu(x)$ to be a constant, i.e., $\mu(x) = \mu_0 \in \mathbb{F}_{q^n}$ such that $b = \mu_0^2$ is in $\mathbb{F}_q$. A necessary condition for μ_0^2 to be in $\mathbb{F}_q$ is that n should be even. So, we are assuming that $b \in \mathbb{F}_q$ is a quadratic residue in $\mathbb{F}_{q^n}$. On the other hand, we do not want b to be a quadratic residue in $\mathbb{F}_q$ the reason for which we will explain shortly.

For any non-zero $\lambda(x) \in \mathbb{F}_q[x]$ consider the polynomial $H(x)/b = b\lambda^2(x) - f(x)$. This polynomial is in $\mathbb{F}_q[x]$ and is of degree $\max(2m_1, 2g+1)$. If this polynomial is smooth, then so is $H(x)$ and we obtain an m-point decomposition where $m = \max(2m_1, 2g+1)$. The number of control variables are the coefficients of $\lambda(x)$. Taking $\lambda(x)$ to be monic, the number of control variables is m_1. Since $\lambda(x) \in \mathbb{F}_q$, each control variable ranges over $\mathbb{F}_q$ and so the total number of options that can be tried with m_1 control variables is q^{m_1}.

Suppose $\alpha \in \mathbb{F}_q$ is a root of $H(x)/b$. So, $f(\alpha) = b\lambda^2(\alpha) = (\mu_0\lambda(\alpha))^2$ and setting $\beta = \mu_0\lambda(\alpha)$ gives the points $(\alpha, \pm\beta)$ on the curve C. If b is a quadratic residue in $\mathbb{F}_q$, then μ_0 is also in $\mathbb{F}_q$ and hence so is β. In this case, we only obtain decompositions in $J_C(\mathbb{F}_q)$ and not in $J_C(\mathbb{F}_{q^n})$. For this reason, we need b to be a quadratic non-residue in $\mathbb{F}_q$.

In the above, we have chosen $\mu(x)$ to be a constant polynomial. Instead one can choose $\lambda(x)$ to be a constant polynomial $\lambda(x) = \lambda_0 \in \mathbb{F}_{q^n}$ such that $c = \lambda_0^2 \in \mathbb{F}_q$ and c is not a quadratic residue in $\mathbb{F}_q$. Once more considering the smoothness of $H(x) = \lambda_0^2 - f(x)\mu^2(x) = c - f(x)\mu^2(x) \in \mathbb{F}_q$ we will obtain m-point decompositions where m is now equal to $2g+1+2m_2$. The m in this case is larger than in the previous case.

4.2 Partial Sub-Field Curve

Suppose $C : y^2 = f(x)$ is such that only the constant term of $f(x)$ is in $\mathbb{F}_{q^n}$ while all other coefficients of $f(x)$ are in $\mathbb{F}_q$. Such a curve is not a sub-field curve and may be called a partial sub-field curve.

In this case it is possible to obtain a number of relations between the elements of the factor basis. The following simple result provides the basis for doing this.

Proposition 1. *Suppose $C : y^2 = f(x)$ and $f(x) = x\phi(x) + A_0$ where $\phi(x) \in \mathbb{F}_q[x]$ and $A_0 \in \mathbb{F}_{q^n}$. Suppose t is an element of $\mathbb{F}_q$ such that $A_0 + t$ is a quadratic residue in $\mathbb{F}_{q^n}$ and let $\lambda_0^2 = A_0 + t$. Then setting $\lambda(x) = \lambda_0$ and $\mu(x) = 1$ gives $H(x)$ in $\mathbb{F}_q[x]$.*

Proof. Recall that $H(x) = \lambda^2(x) - f(x)\mu^2(x)$. With the given values of $\lambda(x)$ and $\mu(x)$, we obtain $H(x) = \lambda_0^2 - f(x)$. Using $\lambda_0^2 = A_0 + t$ and $f(x) = x\phi(x) + A_0$, we get $H(x) = A_0 + t - x\phi(x) - A_0 = x\phi(x) + t$ which is in $\mathbb{F}_q[x]$. □

When $H(x) = \lambda_0^2 - f(x)$ is smooth over $\mathbb{F}_q$, we obtain a $(2g+1)$-point decomposition. If α is a root of $H(x)$, then $f(\alpha) = \lambda_0^2$ and so $(\alpha, \pm\lambda_0)$ are points on C. Note that for two distinct roots α_1 and α_2 of $H(x)$, the corresponding points on C are $(\alpha_1, \pm\lambda_0)$ and $(\alpha_2, \pm\lambda_0)$, i.e., the y-coordinates are the same. This corresponds to the line $y = \lambda_0$ which is parallel to the x-axis cutting the curve at $(2g+1)$-points. Since all the corresponding x-coordinates are in $\mathbb{F}_q$, the obtained decomposition is not trivial. For example, in the case of elliptic curves, if we apply the line-and-chord rule to two points whose x-coordinates are in $\mathbb{F}_q$, it is not guaranteed that the x-coordinate of the sum will also be in $\mathbb{F}_q$.

Suppose $t_0 \neq t_1$ are such that $A_0 + t_0$ and $A_0 + t_1$ are both squares in $\mathbb{F}_{q^n}$ and the corresponding H-polynomials $A_0+t_0-f(x)$ and $A_0+t_1-f(x)$ are both smooth over $\mathbb{F}_q$. Let a_0 and a_1 be such that $a_0^2 = A_0+t_0$ and $a_1^2 = A_0+t_1$. The divisors in the decomposition corresponding to t_0 are defined from points all of whose y-coordinates are equal to $\pm a_0$. Similarly, the divisors in the decomposition corresponding to t_1 are defined from points all of whose y-coordinates are equal to $\pm a_1$. As a result, the two sets of divisors in the two decompositions are disjoint. More generally, decompositions obtained using Proposition 1 have the property that no two relations have a divisor in common.

An important point to note is that the possibility of obtaining a relation does not depend on the extension degree n. We obtain a $(2g + 1)$-point relation whatever be the extension degree.

In Proposition 1, the only control variable we have is t. Out of the q possible values of t, about $q/2$ will result in $A_0 + t$ being a square in $\mathbb{F}_{q^n}$. So, the number of trials will be about $q/2$. The degree of $H(x)$ is $2g + 1$ and so in about $(2g + 1)!$ trials we will obtain a smooth $H(x)$. As a result, the number of relations that will be obtained by this technique will be about $q/(2(2g + 1)!)$. Sieving can be used to speed up this computation.

The number of relations that are obtained is not sufficient to be able to perform the complete linear algebra step. The obtained relations can be used to reduce the size of the factor basis. This is a consequence of the fact that the sets of divisors in the relations are disjoint.

For example, when $g = 1$, i.e., in the case of elliptic curves, we will obtain about $q/12$ 3-point relations. No two of these relations will have a common divisor. As a result, we can remove about $q/12$ elements from the factor basis by choosing one divisor from each of the $q/12$ relations. Whenever one of these removed divisors occur in a relation obtained using other methods, it can be replaced by the negation of the sum of two other divisors in the factor basis. Such a reduction in the size of the factor basis will reduce the time for the linear algebra step. This reduction of the factor basis can be useful when combined with Semaev's [16] summation formula based discrete log alogrithm for elliptic curves proposed by Gaudry [7].

Example 1. Let $q = 16781747$ be a prime and let $n = 7$ with $\mathbb{F}_{q^7}$ realised as $\mathbb{F}_q[x]/\langle w^7 + w + 8\rangle$. Consider the elliptic curves $E : y^2 = x^3 + 10805452x + (10262628w^6 + 8483277w^5 + 6794783w^4 + 10836145w^3 + 4047688w^2 + 5008212w + 10168056)$, defined over $\mathbb{F}_{q^7}$. Then $\#E = 2\times p_1$, where $p_1 = 187426152609583203245776700781399275920191867781567$ is a prime. Using Proposition 1, we will get relations of following types.

$$(7986974, \beta_1) + (6100752, \beta_1) + (2694021, \beta_1) \sim 0; \tag{10}$$

$$(14109678, \beta_2) + (12931646, \beta_2) + (6522170, \beta_3) \sim 0 \tag{11}$$

where, $\beta_1 = 6096369w^6 + 15638567w^5 + 12407480w^4 + 5727199w^3 + 14632270w^2 + 11070711w + 6011652$ and $\beta_2 = 1121656w^6 + 13545884w^5 + 1208363w^4 + 8743129w^3 + 12948727w^2 + 4403294w + 16123844$. It is possible to efficiently generate all such relations. We can see that the the y coordinate of the points in the above relations are same and the relations are distinct. So they can be used to reduce the size of factor basis.

5 Curves over Quadratic Extension Fields

Let $\mathbb{F}_q$ be a finite field of characterisitic greater than 2 and $n \geq 2$ be a positive integer. Let $C : y^2 = f(x) = x^{2g+1} + \sum_{i=0}^{2g} A_i x^i$ be a hyperelliptic curve with $A_i \in \mathbb{F}_{q^n}$. Suppose

that there are non-negative integers k and e with $k+e \leq 2g+1$ such that A_i is in $\mathbb{F}_q$ for all $i \in \{0,\ldots,2g\} \setminus \{k,\ldots,k+e-1\}$. In other words, all coefficients of $f(x)$ other than $A_k,\ldots,A_{k+e-1}$ are in the base field $\mathbb{F}_q$. We will call such a curve C to be a (k,e)-curve. If $k=0$ and $e=2g+1$, then there is no restriction on $f(x)$; on the other hand, if $k=e=0$, then all coefficients of $f(x)$ are in $\mathbb{F}_q$ and C is a sub-field curve. Partial sub-field curves arise with intermediate values of k and e. For example, with $k=0$ and $e=g$, only the coefficients $A_0,\ldots,A_{g-1}$ may be in $\mathbb{F}_{q^n}$ while the coefficients $A_g,\ldots,A_{2g}$ are necessarily in $\mathbb{F}_q$.

Note that in a (k,e)-curve, the coefficients $A_0,\ldots,A_{k-1},A_{k+e},\ldots,A_{2g}$ are necessarily restricted to be in the base field $\mathbb{F}_q$. On the other hand, there are no restrictions on $A_k,\ldots,A_{k+e-1}$. It is possible that some of these coefficients are also in the base field. More particularly, a (k,e)-curve has *at most* e coefficients (which are consecutive and start from k) to be in $\mathbb{F}_{q^n}$.

The next result provides a method for obtaining factor basis relations for partial sub-field curves defined over quadratic extension fields.

Theorem 1. *Let $\mathbb{F}_{q^2}$ be realised as $\mathbb{F}_q/(w^2-c)$ where w^2-c is an irreducible polynomial over $\mathbb{F}_q$. Let $C: y^2=f(x)=x^{2g+1}+\sum_{i=0}^{2g}A_ix^i$ be a (k,e)-curve with $e \geq g$. Given any positive integer m_2 and a monic polynomial $\mu(x)=x^{m_2}+\mu_{m_2-1}x^{m_2-1}+\cdots+\mu_1x+\mu_0$ of degree m_2 in $\mathbb{F}_q[x]$, it is possible to choose $\lambda(x)=\sum_{i=0}^{m_1}\lambda_ix^i$ of degree $m_1=e+2m_2-1$ such that the polynomial $H(x)=\lambda^2(x)-f(x)\mu^2(x)$ is in $\mathbb{F}_q[x]$. Further, $\lambda_k \in \mathbb{F}_{q^2}$ while $\lambda_i \in \mathbb{F}_q$ for $i \neq k$ and the degree of $H(x)$ is $\max(2e+4m_2-2, 2m_2+2g+1)$.*

1. Notation: For $\alpha \in \mathbb{F}_{q^2}$, write $\alpha=\alpha_1w+\alpha_0$. The part α_1w will be said to be the complex part of α. If $\alpha_1=0$, then α is in $\mathbb{F}_q$ and we call such an α to be simple.
2. The theorem statement has the condition that $e \geq g$. This, however, does not mean that the result does not cover curves with $f(x)$ having less than g complex coefficients. Note that by the definition of (k,e)-curve, there are at most e complex coefficients. So, if $f(x)$ has less than g complex coefficients, then one needs to choose k and e such that the complex coefficients of $f(x)$ are among $A_k,\ldots,A_{k+e-1}$.

Proof. For a (k,e)-curve, $k+e \leq 2g+1$. Since we have the condition $e \geq g$, it follows that $k \leq g+1$. Since $m_1=e+2m_2-1$ and $m_2 \geq 1$, it follows that $m_1 \geq e+1 \geq g+1$. So, $k \leq m_1$ and $\lambda(x)$ indeed has the coefficient λ_k.

From the definition of a (k,e)-curve, only the coefficients $A_k,\ldots,A_{k+e-1}$ are in $\mathbb{F}_{q^2}$ while all the other A's are in $\mathbb{F}_q$. If it turns out that $A_k,\ldots,A_{k+e-1}$ are also in $\mathbb{F}_q$ (i.e., the curve in question is a subfield curve), then we choose λ_k to be any element of $\mathbb{F}_q$ and the result holds. So, for the rest of the proof, we will assume that at least one of the coefficients $A_k,\ldots,A_{k+e-1}$ is in $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. In such a situation, λ_k will also chosen to be in $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Writing $\lambda_k=\lambda_{k,0}+\lambda_{k,1}w$ we will assume that $\lambda_{k,1} \neq 0$. For notational uniformity, we will write $\lambda_i=w\lambda_{i,1}+\lambda_{i,0}$ where $\lambda_{i,1}=0$ for $i \neq k$ and $\lambda_{k,1} \neq 0$. Also, we write $A_i=wA_{i,1}+A_{i,0}$ where $A_{i,1}=0$ for i not in $\{k,k+1,\ldots,k+e-1\}$.

Note that $\mu(x)$ is given. Our aim is to show that it is possible to determine $\lambda(x)$ such that $H(x)$ is in $\mathbb{F}_q[x]$. More particularly, we will show the elements $\lambda_0,\ldots,\lambda_{k-1},\lambda_{k,0},\lambda_{k+1},\ldots,\lambda_{m_1}$ are determined from $\lambda_{k,1},\mu_0,\ldots,\mu_{m_2-1}$.

Let

$$\begin{aligned}\mu^2(x)f(x) &= (x^{m_2}+\mu_{m_2-1}x^{m_2-1}+\cdots+\mu_1x+\mu_0)^2(x^{2g+1}+A_{2g}x^{2g}+\cdots+A_1x+A_0)\\ &= x^{2m_2+2g+1}+\sum_{i=0}^{2g+2m_2}B_ix^i \qquad (12)\end{aligned}$$

We write $B_i = B_{i,0} + B_{i,1}w$. For convenience of notation, we set $B_{2m_2+2g+1} = 1$. Since C is a (k, e)-curve, other than the coefficients $A_k, \ldots, A_{k+e-1}$ all other coefficients A_i's of $f(x)$ are simple. As a result, B_i is complex only for $i = k, k+1, \ldots, k+e+2m_2-1$ and all other B_j's are necessarily simple. In other words, $B_{i,1} = 0$ if i is not one of $k, k+1, \ldots, k+e+2m_2-1$. Note that $m_1 = e + 2m_2 - 1$. So, we can write

$$\begin{aligned}\mu^2(x)f(x) &= \sum_{i=0}^{2g+2m_2+1} B_{i,0}x^i + w \times \sum_{i=0}^{e+2m_2-1} B_{i+k,1}x^{i+k} \\ &= \sum_{i=0}^{2g+2m_2+1} B_{i,0}x^i + w \times \sum_{i=0}^{m_1} B_{i+k,1}x^{i+k}. \end{aligned} \tag{13}$$

We now consider $\lambda^2(x)$. Apart from λ_k, all other coefficients of $\lambda(x)$ are simple. The complex coefficients of $\lambda^2(x)$ arise only from λ_k. So, in $\lambda^2(x) = (\lambda_0 + \lambda_1 x + \cdots + \lambda_{m_1}x^{m_1})^2$ only the coefficients of $x^k, x^{k+1}, \ldots, x^{k+m_1}$ are complex while all other coefficients are simple.

The way λ_k affects the coefficients of $\lambda^2(x)$ is as follows: The term λ_k^2 appears in the coefficient of x^{2k} and for $i \neq k$, the term $2\lambda_i\lambda_k$ appears in the coefficient of x^{i+k}. Note that

$$\lambda_k^2 = (\lambda_{k,0} + w\lambda_{k,1})^2 = \lambda_{k,0}^2 + 2w\lambda_{k,0}\lambda_{k,1} + w^2\lambda_{k,1}^2 = \lambda_{k,0}^2 + c\lambda_{k,1}^2 + w(2\lambda_{k,0}\lambda_{k,1}).$$

So, the complex part of λ_k^2 is $2w\lambda_{k,0}\lambda_{k,1}$. For $i \neq k$, λ_i is simple and equal to $\lambda_{i,0}$ and so the complex part of $2\lambda_i\lambda_k$ is $2w\lambda_{i,0}\lambda_{k,1}$.

We now show that the λ_i's can be computed so as to ensure $H(x) \in \mathbb{F}_q[x]$. It is easy to see that the numbers of complex coefficients in the two expressions $\lambda^2(x)$ and $\mu^2(x)f(x)$ are same and these coefficients correspond to the same powers of x. Given $\mu(x)$, the values of B_i's are fixed.

Recall that $H(x) = \lambda^2(x) - \mu^2(x)f(x)$. Equating the complex part of the coefficient of x^{i+k}, $(i = 0, 1, \ldots, m_1)$ in $H(x)$ equal to 0, we obtain

$$2\lambda_{k,1}\lambda_{i,0} - B_{i+k,1} = 0.$$

From this it follows that for $i = 0, 1, \ldots, m_1$

$$\lambda_{i,0} = \frac{B_{k+i,1}}{2\lambda_{k,1}}. \tag{14}$$

The above values of the λ_i's ensure that the complex parts of the coefficients of $H(x)$ are 0 and hence $H(x) \in \mathbb{F}_q[x]$. □

The exact expression for $H(x)$ given by Theorem 1 is mentioned in the following corollary.

Corollary 1.

$$H(x) = cx^{2k}\lambda_{k,1}^2 + \frac{1}{4\lambda_{k,1}^2} \times \left(\mu^2(x) \sum_{i=k}^{k+e-1} A_{i,1}x^{i-k}\right)^2 - \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right). \tag{15}$$

Proof. Write $f(x)$ as $f(x) = x^{2g+1} + w\left(\sum_{i=0}^{2g} A_{i,1}x^i\right) + \left(\sum_{i=0}^{2g} A_{i,0}x^i\right)$ and then writing $\mu^2(x)f(x)$ once more we have:

$$\mu^2(x)f(x) = \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i + w\sum_{i=1}^{2g} A_{i,1}x^i\right)$$

$$= \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right) + w\mu^2(x)\left(\sum_{i=1}^{2g} A_{i,1}x^i\right)$$
$$= \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right) + w\mu^2(x)\left(\sum_{i=k}^{k+e-1} A_{i,1}x^i\right). \quad (16)$$

Comparing (13) and (16) we get

$$\sum_{i=0}^{m_1} B_{i+k,1}x^{i+k} = \mu^2(x)\left(\sum_{i=k}^{k+e-1} A_{i,1}x^i\right).$$

Dividing both sides by x^k gives the following relation.

$$\sum_{i=0}^{m_1} B_{i+k,1}x^{i} = \mu^2(x)\left(\sum_{i=k}^{k+e-1} A_{i,1}x^{i-k}\right). \quad (17)$$

Note that $\lambda(x) = wx^k\lambda_{k,1} + \sum_{i=0}^{m_1}\lambda_{i,0}x^i$.

$$\begin{aligned}
H(x) &= \lambda^2(x) - \mu^2(x)f(x)\\
&= \left(wx^k\lambda_{k,1} + \sum_{i=0}^{m_1}\lambda_{i,0}x^i\right)^2 - \mu^2(x)\left(x^{2g+1} + w\left(\sum_{i=0}^{2g} A_{i,1}x^i\right) + \sum_{i=0}^{2g} A_{i,0}x^i\right)\\
&= cx^{2k}\lambda_{k,1}^2 + \left(\sum_{i=0}^{m_1}\lambda_{i,0}x^i\right)^2 - \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right)\\
&\quad + w\left(2\lambda_{k,1}\left(\sum_{i=0}^{m_1}\lambda_{i,0}x^i\right)x^k - \mu^2(x)\left(\sum_{i=0}^{2g} A_{i,1}x^i\right)\right)\\
&= cx^{2k}\lambda_{k,1}^2 + \frac{1}{4\lambda_{k,1}^2} \times \left(\sum_{i=0}^{m_1} B_{i+k,1}x^i\right)^2 - \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right)\\
&= cx^{2k}\lambda_{k,1}^2 + \frac{1}{4\lambda_{k,1}^2} \times \left(\mu^2(x)\sum_{i=k}^{k+e-1} A_{i,1}x^{i-k}\right)^2 - \mu^2(x)\left(x^{2g+1} + \sum_{i=0}^{2g} A_{i,0}x^i\right).
\end{aligned}$$

The complex terms in the expression for $H(x)$ cancel out by the choice of $\lambda_{i,0}$'s and recall that we use the polynomial $w^2 - c$ to represent $\mathbb{F}_{q^2}$. Further, (17) has been used. □

Given $B_{k,1}, \ldots, B_{k+m_1,1}$ and a non-zero value for $\lambda_{k,1}$ the values of λ_i for $i = 0, \ldots, m_1$ are completely determined by the relation (14) in the proof of Theorem 1. Further, the values of $B_{i,1}$'s are determined completely by $\mu_0, \ldots, \mu_{m_2-1}$ and the curve coefficients $A_0, \ldots, A_{2g}$. As a result, for any choice of $\mu_0, \ldots, \mu_{m_2-1}$ and $\lambda_{k,1}$ the values of $\lambda_{i,0}$ for $i = 0, \ldots, m_1$ are completely determined.

The quantities $\mu_0, \ldots, \mu_{m_2-1}$ can vary over $\mathbb{F}_q$ and $\lambda_{k,1}$ varies over $\mathbb{F}_q^*$. So, by varying $\mu_0, \ldots, \mu_{m_2-1}$ and $\lambda_{k,1}$ over all possible choices, about q^{m_2+1} different $H(x)$'s can be generated. Note that the term $\lambda_{k,1}$ occurs in $H(x)$ only as $\lambda_{k,1}^2$ and so $\lambda_{k,1}$ and $-\lambda_{k,1}$ give rise to the same $H(x)$. So, effectively there are about $q/2$ choices of $\lambda_{k,1}$.

Let h be the degree of $H(x)$ and so $h = \max(2e + 4m_2 - 2, 2m_2 + 2g + 1)$. By varying $\lambda_{k,1}, \mu_0, \ldots, \mu_{m_2-1}$ we obtain different possible choices for $H(x)$. In about $h!$ trials we will obtain an $H(x)$ which is smooth. This gives a relation among the factor basis elements. Since the factor basis contains q elements, we will need about q relations to carry out the linear algebra step. The condition for obtaining q relations is the following:

$$\frac{q^{m_2+1}}{2} \geq h! \times q = (\max(2e + 4m_2 - 2, 2m_2 + 2g + 1))\,! \times q. \tag{18}$$

We note the following points.

1. The complexity of obtaining a smooth $H(x)$ is independent of k and depends only on e.
2. To improve the speed of obtaining smooth $H(x)$, the value of h should be as small as possible. This is achieved by setting $m_2 = 1$. In this case, the degree of $H(x)$ is $h = \max(2e + 2, 2g + 3)$.
3. The minimum possible degree of $H(x)$ is $2g + 3$ and this is attained when $e \leq g$. For Theorem 1 we have the condition $e \geq g$ which combined with $e \leq g$ shows $e = g$. So, if C is a (k, g)-curve, then a single relation can be obtained in about $(2g + 3)!$ trials.
4. The most general case is when $k = 0$ and $e = 2g + 1$. In this case, the degree of $H(x)$ is $h = \max(4g+4m_2, 2m_2+2g+1)$. For $m_2 = 1$, $h = 4g+4$ and so a smooth $H(x)$ is obtained in about $(4g + 4)!$ trials. While this gives a concrete complexity estimate for obtaining a relation (unlike that of Nagao's and Joux-Vitse methods which require solving a system of non-linear equations), the number of trials is too high for the method to be practical for $g \geq 4$.

5.1 Sieving

The expression for $H(x)$ given in Corollary 1 is determined by $\mu(x)$ and $\lambda_{k,1}$. As mentioned earlier, for different choices of $\mu(x)$ and $\lambda_{k,1}$ we can construct different choices of $H(x)$ and test these for smoothness. Smoothness testing, however, is quite time consuming. Sieving can be used to avoid such testing. We explain how this is done based on the sieving technique used by Joux and Vitse in [9].

For simplicity of notation, let $t_1 = \lambda_{k,1}$. Note that the expression for $H(x)$ involves only t_1^2 and we let $t_2 = t_1^2$. Also, by $\overline{\mu}$ denote $(\mu_0, \ldots, \mu_{m_2-1})$. For a fixed value of $\overline{\mu}$, denote by $H_{\overline{\mu}}(x, t_2)$ the expression for $H(x)$ in (15) where we explicitly show the dependence of $H(x)$ on t_2. Note that for a fixed $\alpha \in \mathbb{F}_q$, the numerator of the expression for $H_{\overline{\mu}}(\alpha, t_2)$ is a quadratic in t_2.

Let ctr be an array of size q whose entries are initialised to 0. Choose a random $\overline{\mu}$. For each $\alpha \in \mathbb{F}_q$, perform the following steps: construct the quadratic in t_2 corresponding to the numerator for $H_{\overline{\mu}}(\alpha, t_2)$; if this quadratic is reducible over $\mathbb{F}_q$, then determine its roots δ_0 and δ_1; if δ_i is a square, then increment $\mathsf{ctr}[\delta_i]$ for $i = 0, 1$. After the loop over $\mathbb{F}_q$ has been completed, step through the array ctr looking for a δ such that $\mathsf{ctr}[\delta] = 2g + 3$. Note that such a δ is necessarily a square. Choose $\lambda_{k,1}$ to be a square root of this δ. For this $\lambda_{k,1}$ and the chosen value of $\overline{\mu}$, the corresponding $H(x)$ given by (15) is necessarily smooth. This $H(x)$ can be factored to obtain the roots and hence a relation among the factor base elements.

It may turn out that for the particular $\overline{\mu}$ there is no entry in ctr which provides a smooth $H(x)$. In such a situation, we choose another $\overline{\mu}$ and repeat the sieving process. Note that at no point is smoothness testing required. In practice, this leads to significantly improved efficiency.

Additional speed-up can be obtained by using a pre-computed table of square-roots of the elements of $\mathbb{F}_q$. There are two places where this will be used. The first use is in the solution of the quadratic $H_{\overline{\mu}}(\alpha, t_2)$. The discriminant is computed and the square root extracted using the pre-computed table. The second use is in testing whether δ_i is a square. This is done by a simple table look-up.

Example 2. ($g = 5$, $k = 0$, $e = 5$): Let $q = 536870923$ which is a prime. The polynomial $w^2 + 487791668$ is irreducible over $\mathbb{F}_q$ and let $\mathbb{F}_{q^2}$ be represented as $\mathbb{F}[w]/\langle w^2 + 487791668\rangle$. Consider the curve C over $\mathbb{F}_{q^2}$ given by the following equation.

$$\begin{aligned} y^2 = {} & x^{11} + 72867692x^{10} + 266240208x^9 + 189702338x^8 + 403941598x^7 + 243294425x^6 \\ & + 161364907x^5 + (481611065w + 113938517)x^4 + (302739899w + 218608566)x^3 \\ & + (277004398w + 100790511)x^2 + (32516642w + 523324966)x + (148834277w + 444734696). \end{aligned} \tag{19}$$

We have collected 24 relations among the factor basis elements. The average time per relation was 15 hours. For illustrative purpose we provide one such relation below.

$$\sum_{i=1}^{13} \Big((P_i) - (\infty) \Big) \sim 0$$

where P_i are the following points on the curve C.

$$\begin{aligned} P_1 &= (461653145, 227963090w + 69237873) \\ P_2 &= (416967427, 404086065w + 524185991) \\ P_3 &= (395947819, 169482988w + 531757234) \\ P_4 &= (374926825, 302252595w + 497356260) \\ P_5 &= (366109950, 158087663w + 153008186) \\ P_6 &= (267888952, 210317996w + 472116172) \\ P_7 &= (241362678, 154484158w + 57775439) \\ P_8 &= (209173699, 332896640w + 209227835) \\ P_9 &= (132224988, 514472422w + 449592808) \\ P_{10} &= (130531868, 390327959w + 74840939) \\ P_{11} &= (30575684, 531315607w + 153861896) \\ P_{12} &= (14940740, 216381479w + 216507315) \\ P_{13} &= (14586917, 146027799w + 360620670) \end{aligned}$$

Example 3. ($g = 5$, $k = 5$, $e = 5$): As in the previous example, let $q = 536870923$. Let $\mathbb{F}_{q^2}$ be represented as $\mathbb{F}_q[x]/\langle w^2 + 315734631\rangle$. Consider the curve C over $\mathbb{F}_{q^2}$ given by the following equation.

$$\begin{aligned} y^2 = {} & x^{11} + 536070224x^{10} + (372000917w + 121411583)x^9 \\ & + (327360521w + 173943725)x^8 + (58415006w + 484515562)x^7 \\ & + (202132854w + 174537446)x^6 + (36125993w + 280775023)x^5 \\ & + 480682978x^4 + 245423911x^3 + 144246068x^2 + 176472615x + 485640527. \end{aligned} \tag{20}$$

Note that in this example the complex coefficients in $f(x)$ are not the first g terms. In this case also, the average time per relation was about 15 hours. For illustrative purpose we provide one relation below.

$$\sum_{i=1}^{13} \Big((P_i) - (\infty)\Big) \sim 0$$

where P_i are the following points on the curve C.

$$\begin{aligned}
P_1 &= (488169155, 127507425w + 11619026)\\
P_2 &= (414967071, 411968940w + 526402989)\\
P_3 &= (367542253, 271345312w + 71563790)\\
P_4 &= (360417276, 146775404w + 529629782)\\
P_5 &= (327156809, 148898586w + 313658158)\\
P_6 &= (321069144, 401672122w + 516009885)\\
P_7 &= (297696598, 332164999w + 71083788)\\
P_8 &= (282773404, 165994134w + 128263175)\\
P_9 &= (153245666, 299447617w + 31791782)\\
P_{10} &= (148847735, 131086868w + 526494330)\\
P_{11} &= (122238345, 501760005w + 500393269)\\
P_{12} &= (46402515, 207894339w + 345845407)\\
P_{13} &= (3075334, 414551777w + 407607294)
\end{aligned}$$

Example 4. ($g = 6$, $k = 7$, $e = 6$): The prime $q = 536870923$ as before. The field $\mathbb{F}_q^2 = \mathbb{F}_q[x]/\langle w^2 + 391407656\rangle$. The curve C is given by the following equation.

$$\begin{aligned}
y^2 = {} & x^{13} + (26724425w + 521111574)x^{12} + (108641052w + 409984592)x^{11}\\
& + (24302877w + 201680702)x^{10} + (340698236w + 334614899)x^9\\
& + (90984934w + 92561831)x^8 + (279332373w + 378470239)x^7 + 171216922x^6\\
& + 303496296x^5 + 144977430x^4 + 252906250x^3 + 276374600x^2 + 508777162x + 206709783
\end{aligned} \tag{21}$$

It took us 8 days to get a single relation by running on 15 parallel cores. The relation is the following.

$$\sum_{i=1}^{15} \Big((P_i) - (\infty)\Big) \sim 0$$

where P_i are the following points on the curve C.

$$\begin{aligned}
P_1 &= (529627927, 324604233w + 328370059)\\
P_2 &= (457161741, 324649665w + 308701675)\\
P_3 &= (318999554, 451438865w + 383125220)\\
P_4 &= (282246842, 41996416w + 31292053)\\
P_5 &= (280379434, 403412458w + 426683854)\\
P_6 &= (263884452, 32875161w + 244297866)
\end{aligned}$$

$$P_7 = (259928285, 260498525w + 90308916)$$
$$P_8 = (222312520, 408316107w + 330320218)$$
$$P_9 = (200790649, 38478293w + 527202107)$$
$$P_{10} = (179779688, 352410950w + 516715413)$$
$$P_{11} = (119409638, 334594398w + 28958127)$$
$$P_{12} = (79561862, 510759460w + 518110662)$$
$$P_{13} = (62284590, 333545883w + 331763559)$$
$$P_{14} = (31745814, 453648987w + 25464942)$$
$$P_{15} = (29265458, 294026161w + 533582133)$$

5.2 Comparison with Nagao's and Joux-Vitse Methods

In Nagao's method, a relation is obtained by solving a system of $ng(n-1)$ nonlinear equations in as many variables. In the present case, $n = 2$ and so the system consists of $2g$ equations and variables.

1. For $g = 4$, this leads to a system of 8 equations in 8 variables. Solving one such system using Magma requires about a second. The solution only ensures that $H(x)$ is in $\mathbb{F}_q[x]$. The degree of $H(x)$ is $2g = 8$. To obtain an $H(x)$ which is smooth over $\mathbb{F}_q[x]$, it is required to consider about $8! \approx 2^{15.3}$ divisors and so correspondingly solve about 8! systems of 8 non-linear equations in 8 variables. Practically we get a single decomposition in about 7 hours. In comparison, the new method provides a single relation in about 8 to 10 minutes.
2. For $g = 5$, Nagao's method requires solving a system of 10 equations in 10 variables. We were able to solve one such system using Magma in about one minute. As above, such a solution only ensures that $H(x)$ is in $\mathbb{F}_q[x]$. In this case, the degree of $H(x)$ is 10 and so to obtain an $H(x)$ which is smooth over $\mathbb{F}_q[x]$ we need to consider about $(2g)! = 10!$ divisors. This requires solving about $10! \approx 2^{22}$ systems of 10 non-linear equations in 10 variables. As a result, the time for obtaining a single relation will be about 10! minutes (which is about 60000 hours). In comparison, the new method requires about 9 hours to find a single relation.
3. For $g = 6$, Nagao's method involves repeatedly solving systems consisting of 12 equations in 12 variables. We were able to solve one such system in about 6000 seconds (which is about 1.6 hours). Obtaining a single decomposition will require solving about $12! \approx 2^{28.8}$ such systems which is infeasible. In comparison, the new method yielded a relation in about 8 days.

The method proposed in this paper raises the possibility of actually carrying out DLP computations for $g = 4$ and $g = 5$. Relations between the elements of the factor basis are to be generated using the new method. The linear algebra step is to be carried out as usual. Suppose D_1 is the generator of an appropriate subgroup of the Jacobian and D_2 is a target divisor and the requirement is to compute $\log_{D_1} D_2$. Using the random walk technique from [6] divisors $D = a_1 D_1 + a_2 D_2$ are to be generated. Nagao's method is to be used to obtain the decomposition of one such D over the factor basis. Such a decomposition in conjunction with the discrete log of the factor basis elements will provide the desired discrete log of the target element.

Note that Nagao's method could also be used for generating relations. The speed improvement arises from replacing Nagao's method by the new method for the relation collection step.

Availability of multiple cores will speed up the computation of both relation collection by the new method and the single decomposition to be obtained using Nagao's method. Even though we suggest that DLP computations for $g = 4$ and $g = 5$ are feasible, at the present time we do not have sufficient computational resources to actually carry out one such computation.

The initial phase of the Joux-Vitse method involves solving a system of $ng(n-1)+2(n-1)$ equations in $ng(n-1)+2n$ variables. Again, here $n = 2$ leading to a system of $2g+2$ equations in $2g+4$ variables. For $g = 4$, this leads to a system of 10 equations in 12 variables; for $g = 5$, this leads to a system of 12 equations in 14 variables; and for $g = 6$, this leads to a system of 14 equations in 16 variables. We were unable to solve even one such system using Magma on our computers. That Magma could not solve the system arising for $g = 4$ is a bit surprising. A system arising out of Nagao's method for $g = 6$ consists of 12 equations in 12 variables and Magma was able to solve one such system. So, one would expect that Magma should be able to solve a system of 10 equations in 12 variables. That, however, did not happen.

The major bottleneck in the Joux-Vitse method is the requirement of solving the initial non-linear system of equations. For the same g, the system is more complex than the system generated by Nagao's method. On the other hand, once the initial system is solved, the successive iterations are much faster and a single relation is obtained in about $(2g + 2)!$ trials. In comparison, obtaining one relation by the new method requires about $(2g + 3)!$ trials. Both the Joux-Vitse method and the new method use sieving to obtain practical efficiency gains. So, if the initial non-linear system in the Joux-Vitse method can be solved, then the rest of the compuation will be faster than the new method. However, as mentioned above, for $g \geq 4$, on our computers, Magma was unable to solve the initial system arising in the Joux-Vitse method.

In conclusion, for the special types of curves considered in this work, the new method provides relations faster than either Nagao's or the Joux-Vitse methods. We note the following points.

1. The new method (as well as the Joux-Vitse method) only provides relations among factor basis elements. Decomposition of a target element (using the random walk technique from [6]) over the factor basis still has to be done by Nagao's method.
2. The new method works only for a sub-class of curves while Nagao's and the Joux-Vitse methods work for all curves.

6 Curves Over Characteristic Two Fields

We briefly consider how our techniques apply to characteristic two field. In this case, the form of a hyperelliptic curve is $y^2+xy = f(x)$. Let q be a power of 2 and for $n \geq 2$, we consider $\mathbb{F}_{q^n}$-rational points of C. As before, we consider polynomial maps of the form $G(x, y) = \lambda(x)+y\mu(x)$ where $\lambda(x)$ and $\mu(x)$ are polynomials of degrees m_1 and m_2 respectively in $\mathbb{F}_{q^n}[x]$.

We are interested in the zeros of the polynomial $\lambda(x) + y\mu(x)$ on the curve C. For any such point (α, β), $\beta = \lambda(\alpha)/\mu(\alpha)$ and (α, β) also satisfies the equation of the curve, i.e., $\beta^2 + \beta\alpha = f(\alpha)$. Eliminating β between these two equations yields $\lambda^2(\alpha) + \alpha\lambda(\alpha)\mu(\alpha) = \mu^2(\alpha)f(\alpha)$. So, in this case, the form of the polynomial $H(x)$ is the following.

$$H(x) = \lambda^2(x) + x\lambda(x)\mu(x) + \mu^2(x)f(x). \tag{22}$$

Proposition 2. *Let q be a power of 2 and $n \geq 2$ be a positive integer. Consider the curve $C : y^2+xy = f(x) = x^3\phi(x)+A_2x^2+A_1x+A_0$ where $\phi(x) \in \mathbb{F}_q[x]$, $A_1, A_0 \in \mathbb{F}_q$ and $A_2 \in \mathbb{F}_{q^n}$.*

If for some $t \in \mathbb{F}_q$, the polnomial $z^2 + z + A_2 + t$ is reducible over $\mathbb{F}_{q^n}$, then for $\mu(x) = 1$, it is possible to choose the polynomial $\lambda(x)$ such that $H(x) = \lambda^2(x) + x\lambda(x)\mu(x) + \mu^2(x)f(x)$ is in $\mathbb{F}_q[x]$.

Proof. Let $\lambda(x) = \lambda_{m_1}x^{m_1} + \cdots + \lambda_2 x^2 + \lambda_1 x + \lambda_0$, where λ_1 is a root of the polynomial $z^2 + z + A_2 + t$ and $\lambda_0, \lambda_2, \ldots, \lambda_{m_1}$ are in $\mathbb{F}_q$. Then

$$\begin{aligned} H(x) &= \lambda^2(x) + x\lambda(x) + f(x) \\ &= \lambda^2(x) + x\lambda(x) + x^3\phi(x) + A_2x^2 + A_1x + A_0 \\ &= (\lambda_{m_1}^2 x^{2m_1} + \cdots + \lambda_2^2 x^4 + \lambda_1^2 x^2 + \lambda_0^2) \\ &\quad +(\lambda_{m_1}x^{m_1+1} + \cdots + \lambda_2 x^3 + \lambda_1 x^2 + \lambda_0 x) \\ &\quad +x^3\phi(x) + A_2x^2 + A_1x + A_0 \\ &= x^2(\lambda_1^2 + \lambda_1 + A_2) + \psi(x) \\ &= tx^2 + \psi(x). \end{aligned}$$

Here $\psi(x)$ is in $\mathbb{F}_q[x]$, i.e., all its coefficients are in $\mathbb{F}_q$. Also, t is in $\mathbb{F}_q$ and so $H(x)$ is in $\mathbb{F}_q[x]$. □

The degree of $H(x)$ is $h = \max(2m_1, 3)$ and we obtain an h-point decomposition. In the choice of $\lambda(x)$, the constant term λ_0 is a control variable and can be varied freely over $\mathbb{F}_q$. For $m_1 = 1$, the quantity t is the only other control variable which has the constraint that it has to be varied so that the polynomial $z^2 + z + A_2 + t$ is reducible over $\mathbb{F}_{q^n}$. For $m_1 \geq 2$, the coefficients $\lambda_2, \ldots, \lambda_{m_1}$ are $m_1 - 2$ additional independent control variables over $\mathbb{F}_q$.

Choosing $m_1 = 2$, gives two independent control variables and possibly a partial control variable t. In this case, there are more than q^2 choices for $H(x)$. The degree of $H(x)$ is $2m_1 = 4$ and in about 4! trials we will obtain an $H(x)$ which is smooth over $\mathbb{F}_q$. Each such $H(x)$ gives rise to a 4-point decomposition and we obtain a total of more than $q^2/4!$ such relations. If $q^2/4! > q$, i.e., $q > 4!$, then we will obtain sufficiently many relations to carry out the linear algebra step.

There is a condition in the statement of Proposition 2. For some $t \in \mathbb{F}_q$, the polynomial $z^2 + z + A_2 + t$ has to be reducible over $\mathbb{F}_{q^n}$. Consider the case of elliptic curves. In this case, we can take $A_1 = 0$ and the form of the curve is $y^2 + xy = x^3 + A_2x^2 + A_0$. For elliptic curves, when n is odd, then we have experimentally found that for the values of n we tested, it is always possible to find a t such that the reducibility condition holds. On the other hand, if n is even, then there are cases when $z^2 + z + A_2$ is irreducible over $\mathbb{F}_{q^n}$ and for even n, this implies that for every $t \in \mathbb{F}_q$, the polynomial $z^2 + z + A_2 + t$ is also irreducible over $\mathbb{F}_{q^n}$. (This can be proved using elementary arguments involving the trace function.) So, for even n, there are situations where the condition of Proposition 2 does not hold and hence, the stated decompositions cannot be obtained.

Super-singular HEC: In this case, the equation of the curve is of the form $y^2 + y = f(x)$. The above decomposition method works with a different condition on $f(x)$.

Proposition 3. *Let q be a power of 2 and $n \geq 2$ be a positive integer. Consider the curve $C : y^2 + y = f(x) = x\phi(x) + A_0$ where $\phi(x) \in \mathbb{F}_q[x]$ and $A_0 \in \mathbb{F}_{q^n}$. If for some $t \in \mathbb{F}_q$, the polnomial $z^2 + z + A_0 + t$ is reducible over $\mathbb{F}_{q^n}$, then for $\mu(x) = 1$, it is possible to choose the polynomial $\lambda(x)$ such that $H(x) = \lambda^2(x) + x\lambda(x)\mu(x) + \mu^2(x)f(x)$ is in $\mathbb{F}_q[x]$.*

Proof. Let $\lambda(x) = \lambda_{m_1} x^{m_1} + \cdots + \lambda_2 x^2 + \lambda_1 x + \lambda_0$, where λ_0 is a root of the polynomial $z^2 + z + A_0 + t$ and $\lambda_1, \lambda_2, \ldots, \lambda_{m_1}$ are in $\mathbb{F}_q$. Then

$$\begin{aligned} H(x) &= \lambda^2(x) + \lambda(x) + f(x) \\ &= \lambda^2(x) + \lambda(x) + x\phi(x) + A_0 \\ &= (\lambda_{m_1}^2 x^{2m_1} + \cdots + \lambda_2^2 x^4 + \lambda_1^2 x^2 + \lambda_0^2) \\ &\quad + (\lambda_{m_1} x^{m_1} + \cdots + \lambda_2 x^2 + \lambda_1 x + \lambda_0) + x\phi(x) + A_0 \\ &= (\lambda_0^2 + \lambda_0 + A_0) + \psi(x) \\ &= t + \psi(x). \end{aligned}$$

Here $\psi(x)$ is in $\mathbb{F}_q[x]$, i.e., all its coefficients are in $\mathbb{F}_q$. Also, t is in $\mathbb{F}_q$ and so $H(x)$ is in $\mathbb{F}_q[x]$. □

7 Conclusion

Nagao had proposed a decomposition method for the Jacobian of a hyperelliptic curve defined over $\mathbb{F}_{q^n}$. This involved solving a system of multi-variate non-linear equations. Later work by Joux and Vitse had considered the problem of obtaining relations between elements of the factor basis again by solving a system of non-linear equations.

In this work, we considered whether such relations can be obtained without requiring the solution of non-linear system of equations. For special cases, we show that this can indeed be done. For quadratic extension fields, i.e., for $n = 2$, for certain special curves we describe a method for obtaining relations. This yields an algorithm which can be implemented in practice and we are able to report the computation of a relation for genus six curves.

We also explore the applicability of our technique for fields with $n > 2$. In this case, the curves that can be tackled are more restrictive and also we can obtain only one degree of freedom. As a result, it is not possible to obtain sufficiently many relations for the linear algebra step to go through.

For fields with characteristic two, it is possible to tackle $n \geq 2$, but, the curves that are tackled are also quite special. In this case, though, it is possible to obtain sufficiently many relations so as to be able to complete the linear algebra step.

An interesting question that arises is whether the technique of Section 5 can be applied to a subset of curves defined over $\mathbb{F}_{q^n}$ for other small values of n such as 3 and 4. Our initial efforts for doing this were not successful. The problem is that it becomes difficult to explicitly write down the relations which ensure that the complex terms of $H(x)$ cancel out. It remains to be seen whether there is some way of managing the complexity of the equations.

References

1. Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh A. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In Leonard M. Adleman and Ming-Deh A. Huang, editors, *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings*, volume 877 of *Lecture Notes in Computer Science*, pages 28–40. Springer, 1994.
2. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
3. Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Math. Comput.*, 71(238):729–742, 2002.

4. Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 102:83–103, 2002.
5. Ralf Flassenberg and Sachar Paulus. Sieving in function fields. *Experimental Mathematics*, 8(4):339–349, 1999.
6. Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2000.
7. Pierrick Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symb. Comput.*, 44(12):1690–1702, 2009.
8. Pierrick Gaudry, Emmanuel Thomé, Nicolas Thériault, and Claus Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comput.*, 76(257):475–492, 2007.
9. Antoine Joux and Vanessa Vitse. Cover and decomposition index calculus on elliptic curves made practical - application to a previously unreachable curve over F_{p^6}. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 9–26. Springer, 2012.
10. Neal Koblitz. Elliptic curve cryptosystesm. *Math. Comp.*, 48(177):203–209, 1987.
11. Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.
12. Alfred Menezes, Yi-Hong Wu, and R. Zuccherato. An elementary introduction to hyperelliptic curves. Appendix in 'Algebraic Aspects of Cryptography' by Neal Koblitz, 1998.
13. Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985.
14. Koh-ichi Nagao. Decomposition attack for the Jacobian of a hyperelliptic curve over an extension field. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 285–300. Springer, Berlin, 2010.
15. Palash Sarkar and Shashank Singh. A new method for decomposition in the jacobian of small genus hyperelliptic curves. Cryptology ePrint Archive, Report 2014/815, 2014. `http://eprint.iacr.org/`.
16. Igor Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2004/031, 2004. http://eprint.iacr.org/.
17. Nicolas Thériault. Index calculus attack for hyperelliptic curves of small genus. In Chi-Sung Laih, editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2003.
18. M. D. Velichka, Michael J. Jacobson Jr., and Andreas Stein. Computing discrete logarithms in the Jacobian of high-genus hyperelliptic curves over even characteristic finite fields. *Math. Comput.*, 83(286), 2014.