Research Article

Hyperelliptic Covers of Different Degree for Elliptic Curves

Jing Fan,¹,² Xuejun Fan,² Ningning Song,² and Long Wang²

¹University of Science and Technology of China, Hefei 230026, Anhui, China
²The 6th Research Institute of China Electronics Corporation, Beijing 100083, China

Correspondence should be addressed to Xuejun Fan; fanxj@ncse.com.cn

Received 17 March 2022; Accepted 23 April 2022; Published 4 July 2022

Academic Editor: Li Haitao

Copyright © 2022 Jing Fan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In elliptic curve cryptography (ECC) and hyperelliptic curve cryptography (HECC), the size of cipher-text space defined by the cardinality of Jacobian is a significant factor to measure the security level. Counting problems on Jacobians of elliptic curves can be solved in polynomial time by Schoof–Elkies–Atkin (SEA) algorithm. However, counting problems on Jacobians of hyperelliptic curves are solved less satisfactorily than those on elliptic curves. So, we consider the construction of the cover map from the hyperelliptic curves to the elliptic curves to convert point counting problems on hyperelliptic curves to those on elliptic curves. We can also use the cover map as a kind of cover attacks. Given an elliptic curve over an extension field of degree \( n \), one might try to use the cover attack to reduce the discrete logarithm problem (DLP) in the group of rational points of the elliptic curve to DLPs in the Jacobian of a curve of genus \( g \geq n \) over the base field. An algorithm has been proposed for finding genus 3 hyperelliptic covers as a cover attack for elliptic curves with cofactor 2. Our algorithms are about the cover map from hyperelliptic curves of genus 2 to elliptic curves of prime order. As an application, an example of an elliptic curve whose order is a 256-bit prime vulnerable to our algorithms is given.

1. Introduction

The Weil restriction of scalar has significant implications in ECC. This idea was proposed by Frey and Gangl [1] as an attack on the elliptic curve discrete logarithm problem (ECDLP) and then developed further in [2, 3]. A nonconstant morphism \( \phi: C \to E \) between algebraic curve \( C \) over \( \mathbb{F}_q \) and elliptic curve \( E \) over \( \mathbb{F}_{q^n} \) is a way to achieve this attack. Based on the constructive Weil restriction, Scholten [4] constructed hyperelliptic curves whose Jacobian was isogeneous to the Weil restriction of an elliptic curve and then counted points on the hyperelliptic curve by using an algorithm to count points on the elliptic curve.

Jacobians of hyperelliptic curves \( J_H \) have been proposed for use in public key cryptography [5]. In ECC and HECC [6], the size of cipher-text space defined by the cardinality of Jacobian is significant to measure the security level. Specifically, the cardinality should be a prime time for a small so-called cofactor \( c \) to avoid the baby-step giant-step attack and Pohlig–Hellman attack [7]. For elliptic curves, there is a practical algorithm SEA to count the number of the points over finite fields [8–10]. However, for doing this on hyperelliptic curves, no subexponential general algorithm is currently known except for some small sets of examples [11], which is an impediment to their use. An algorithm proposed by Gaudry and Harley [12] to compute order for Jacobians of random hyperelliptic curves would run for about a week for a genus 2 curve defined over an 80-bit field. In 2003, Scholten [4] proposed a way of counting for hyperelliptic curves of special type \( y^2 = r x^5 + s x^4 + \sigma(s)x^2 + \sigma(r) \), where \( \sigma \) is the generator of the Galois group of a quadratic extension. Inspired by Scholten, we consider that the cover map can help to count the order of Jacobians of hyperelliptic curves and the crucial point is to find the cover map from some specific hyperelliptic curves to elliptic curves.

ECDLP is the fundamental building block for ECC and concerned by many researchers [13–17]. For many elliptic curves over finite fields, the generally fastest algorithms to solve the ECDLP are still generic algorithms, which are the conversion of attack algorithms on DLP. But there are also many families of elliptic curves, in particular those over finite nonprime fields, where the ECDLP can be solved faster.
by other methods, such as summation polynomials and cover attack. The former is proposed by Semaev [18] in order to find out whether the index calculus is suitable for ECDLP or not and then Diem [14] and Gaudry [19] independently use it to calculate the ECDLP over small degree extension fields. For cover attack [20], it aims at reducing the DLP in the group of the rational points of an elliptic curve over $\mathbb{F}_{q^2}$ to DLP in the Jacobian groups of a curve $C$ over $\mathbb{F}_q$. The main idea of cover attacks is Weil descent, which is first introduced in cryptography by Frey [1]. The major difficulty in it lies in constructing the curve $C$, which is first solved by Gaudry, Hess, and Smart (GHS) [3] over binary field and generalized by Diem [21] in odd characteristic. For DLPs in the Jacobian groups of the curve $C$, decomposed attack was proposed by Gaudry [22] for hyperelliptic curves over $\mathbb{F}_q$ and then advanced to $\mathbb{F}_{q^n}$ by Nagao [23] using Riemann–Roch spaces. To apply to all composite degree extension fields, Joux and Vitse [24] combined the Weil descent and decomposition attack. They used GHS attack for the part of Weil descent, while GHS attack can not produce a cover with small genus to make the whole attack works well when the elliptic curves have cofactor 2 over cubic extension fields. Tian et al. [25] used the results in reference [26] to fill the gap in GHS. In ECC, the elliptic curves of prime orders are of great interest, so it will be useful to focus on the elliptic curves of cofactor 1 over quadratic extension field. Inspired by reference [25], we try constructing genus 2 hyperelliptic covers for this kind of elliptic curves.

The above two applications induce us to construct genus 2 hyperelliptic covers. We can use the cover to count the order of Jacobians of hyperelliptic curves and to attack the ECDLP.

1.1. Contribution. The contribution of our work is that we construct cover maps from a hyperelliptic curve of genus 2 to an elliptic curve with prime order over quadratic extension field. The whole process is based on the results in references [4, 25, 26]. The corresponding pattern of the map $\psi: H/\mathbb{F}_q^\times \rightarrow E/\mathbb{F}_q^\times$ is that the Weierstrass points of the hyperelliptic curve lie over the 2-torsion points of the elliptic curve. Under the given restrictions, we can get a system of some equations, which can be computed easily and its solutions determine the cover maps.

We focus on genus 2 hyperelliptic curves, which seem to be less vulnerable to attacks than others. About the equations of the hyperelliptic curves $y^2 = f(x)$, we give propositions about the form of $f$, which offers more specific scope of the hyperelliptic curves suitable for our algorithm. There is also a relationship that $\# J_H(\mathbb{F}_q) = \# E(\mathbb{F}_q)$ when $H$ satisfies $J_H/\mathbb{F}_q^\times \sim E/\mathbb{F}_q^\times$, which is useful for counting applications. If we want to count the order of Jacobian of a hyperelliptic curve $H$, then the experiment can begin with the hyperelliptic curve and aim at finding the corresponding elliptic curve $E$. Then, SEA can be used to compute the cardinality of $E(\mathbb{F}_q)$ to evaluate $\# J_H(\mathbb{F}_q)$ in polynomial running time as long as the cover map $\psi: H \rightarrow E$ exists. At the end of the study, we give an example in 128-bit field to show that our algorithm is faster than previous achievements.

As a kind of a cover attacks, our map can transfer the DLP in the elliptic curve with prime order into DLPs in the Jacobians of a hyperelliptic curves, which can be later solved by decomposition attack of Nagao [23]. The main difference between GHS and our method is that the results of former are mainly nonhyperelliptic curves, while our algorithms have hyperelliptic curves as the final result. We can then construct isogeny from $\text{Jac}(H)$ to Jacobian of nonhyperelliptic curves to reduce the time complexity. So, the method in the study has same complexity $O(q)$ as GHS attack. The isogeny walk can also extend the scope of curves vulnerable to our attack. After experiments, we count the number of isomorphic classes of $E$ in the specific form over relatively small fields and find that all of these elliptic curves can be attacked by our algorithm (Table 1).

Inspired by Satoh [27], we can also use our algorithms to generate the required hyperelliptic curves, which can be viewed as a by-product of counting method. For example, if a hyperelliptic curve with prime order of the Jacobian is required, then we can randomly select an elliptic curve of prime order as the input of our algorithms. If we can construct the cover map successfully, then the required hyperelliptic curve with the order of its Jacobian can be given. Otherwise, we can select another elliptic curve. The whole process can be viewed as a probabilistic polynomial-time algorithm.

We have published a small part of our work [28] on Australasian Conference on Information Security and Privacy 2019. We only introduce the algorithm for the case when $\deg \phi = 2$ and $f$ is reducible in detail in reference [28]. In this study, we offer more concrete proof for all of the propositions and new algorithms for the case when $\deg \phi = 3$, which is more complex than before. Moreover, more experiments on these new algorithms are given in Section 4.

2. Preliminaries

In this section, we review some important conclusions on elliptic curves and hyperelliptic curves and we hope that the reader is familiar with the notions and results of algebraic curves [29].

2.1. Cover Maps. Let $\psi: H \rightarrow E$ be a map of degree $d$ from a curve of genus 2 to a curve of genus 1 and let $\iota_H$ be the hyperelliptic involution on $H$. The hyperelliptic involution $\iota_H$ can induce a rational involution $i_E$ on $E$ that satisfies $\psi \iota_H = i_E \psi$. Let $H' = H/\langle \iota_H \rangle$ and $E' = E/\langle \iota_E \rangle$ be the curves of genus 0 obtained by taking the quotient by the involution. So, the quotient map $\pi_H: H \rightarrow H/\langle \iota_H \rangle$ ramifies at 6 points $A_1, A_2, \ldots, A_6$, which are called Weierstrass ramification points of $H$. The map $\pi_E: E \rightarrow E/\langle \iota_E \rangle$ ramifies at 4 points $B_1, B_2, B_3, B_4$, which can be called ramification points of $E$ over $E'$. There is also a map $\psi': H/\langle \iota_H \rangle \rightarrow E/\langle \iota_E \rangle$. The following lemma [26] is about the relationship among the ramification points.
Lemma 1. Let \( A_j, i = 1, 2, 3, 4, 5, 6, \) be the Weierstrass ramification points of \( H \) and \( B_j, j = 1, 2, 3, 4 \), be the ramification points of \( E \) over \( E' \). The \( \alpha_i \) and \( \beta_j \) are the image of these points in \( H' \) and \( E' \) respectively, and then \( (\phi')^{-1}(\beta_j) \) contains \( \alpha_i \) with odd multiplicity and any other points of \( H' \) with even multiplicity for each \( j \).

This lemma determines the pattern of the correspondence between \( \alpha_i \) and \( \beta_j \). We give the following two kinds of maps of the even degree and odd degree, respectively. In the diagram, \( \otimes \) represents evenly ramified points, which are therefore other points of \( H' \).

\[
\begin{array}{cccccc}
\otimes & \otimes & \otimes & \alpha_4 \\
\alpha_1 & \alpha_3 & \alpha_5 & \otimes & \otimes & \otimes & \alpha_5 \\
\otimes & \alpha_2 & \alpha_4 & \otimes & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_6 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\
\end{array}
\]

even degree odd degree

More details, such as the degree of the map and the ramification index of the map at \( \alpha_i \), will be discussed in Section 3.

2.2. 2-Torsion Subgroup of the Jacobian. Let \( \mathbb{F}_q \) denote the finite field of \( q \) elements and \( \overline{\mathbb{F}}_q \) be the algebraic closure of the prime field \( \mathbb{F}_q \). Then, the unique subfield of \( \overline{\mathbb{F}}_q \) with \( q^n \) elements, \( \overline{\mathbb{F}}_{q^n} \), is an extension field of \( \mathbb{F}_q \). Consider that the Jacobian of \( H \) over \( \overline{\mathbb{F}}_q \) is isogenous to the product of \( E_1 \) and \( E_2 \), which have the same number in \( \mathbb{F}_q \). That is \( J_H/\overline{\mathbb{F}}_q \sim E_1/\overline{\mathbb{F}}_q \times E_2/\overline{\mathbb{F}}_q \sim E_1/\overline{\mathbb{F}}_q \).

A hyperelliptic curve \( H \) of genus \( g \) is determined by an equation \( y^2 = f(x) \), where \( f \in \mathbb{F}_q[x] \) is a polynomial of degree \( 2g + 1 \) or \( 2g + 2 \). The curve of degree \( 2g + 1 \) (resp. \( 2g + 2 \)) is termed an imaginary (resp. a real) hyperelliptic curve and all of the hyperelliptic curves can be written in the form of real hyperelliptic curve. Let \( H \) be a real hyperelliptic curve and there are \( 2g + 2 \) Weierstrass points, \( P_i = (\eta_i, 0), i \in \{ 1, 2, \ldots, 2g + 2 \}, \eta_i \in \mathbb{F}_q \). By the corollary in reference [30], every 2-torsion element of \( J_H \) is of the form \( e_T = \sum_{P \neq T}(P - T)/((\alpha_1) + (\alpha_2)) \), where \( T \in \{ P_1, \ldots, P_{2g+2} \} \) and \( T \) must be even. \( e_T \) satisfies the following three properties:

(i) \( 2e_T = 0; \)

(ii) \( e_{T_1} = e_{T_2} \Leftrightarrow T_1 = T_2 \) or \( T_1 = T_2 \backslash \{ \alpha_i \} \), \( \alpha_i \) refers to the complement set;

(iii) \( e_{T_1} + e_{T_2} = e_{T_1 \cap T_2} \), where \( T_1 \cap T_2 = (T_1 \cup T_2) - (T_1 - T_2) \).

If \( h \) is an \( \mathbb{F}_q \)-rational factor of \( f \) with even degree, then a divisor \( D \) can be defined by \( \text{div}(h) = 2 \) and the order of the divisor class \( [D] \) is \( 2 \) if and only if \( \text{deg}(h) \neq 0, 2g + 2 \). So, if \( f = h_1h_2h \) and the degrees of \( h_1 \) and \( h_2 \) are even, we can obtain two distinct divisor classes \([D_1]\) and \([D_2]\).

3. Our Algorithms

In this section, we give algorithms to find the cover map of different degrees from hyperelliptic curves of genus 2 to elliptic curves with prime order. First, we give two basic propositions, which are about the order of Jacobians and the form of the equations of hyperelliptic curves. Then we give the algorithms for \( \text{deg}(\phi) = 2 \), among which we find that there is a more specific form of the equations of hyperelliptic curves. Finally, we give an algorithm for \( \text{deg}(\phi) = 3 \), which is more complex than that for \( \text{deg}(\phi) = 2 \). We also give statistical analysis about the maps of different degrees based on the experimental results in small fields after each algorithm.

3.1. Theory Derivation for the Algorithms. In this subsection, we will compute the order of the Jacobian and the equations of the hyperelliptic curves. For \( C \) a smooth projective curve of genus \( g \), the polynomial \( L_q(T) \) is the numerator of the zeta function:

\[
Z\left( \frac{C}{\mathbb{F}_q}, T \right) = \exp \left( \sum_{n \geq 1} \frac{\#C(\mathbb{F}_{q^n})}{n} \right) = \frac{L_q(T)}{(1 - T)(1 - qT)}.
\]

(1)

The order of the group of \( \mathbb{F}_q \) rational points on the Jacobian of \( C \) is as follows:

\[ \#J_C(\mathbb{F}_q) = L_q(1) = \chi_q(1), \]

(2)

where \( \chi_q(1) \) is the characteristic polynomial of the Frobenius endomorphism.

Lemma 2. Let \( C/\overline{\mathbb{F}}_q \) be a genus \( g \) curve with simple Jacobian \( J_C \) and there is a nonconstant morphism \( \phi/\overline{\mathbb{F}}_q: C_{\overline{\mathbb{F}}_q} \longrightarrow E \), then \( J_C/\overline{\mathbb{F}}_q \) is isogenous to the Weil restriction of \( E \) with respect to \( \overline{\mathbb{F}}_q/\mathbb{F}_q \), denoted by \( \text{Res}(E) \). So, the characteristic polynomial of the Frobenius endomorphism of \( J_C \) is equal to that of \( \text{Res}(E) \): \( \chi_{C}(T) = T^{2g} - tr_E T^g + q^g \) with \( tr_E = q^g + 1 - #E(\overline{\mathbb{F}}_q) \).

Proposition 1. If \( H \) has simple Jacobian over \( \mathbb{F}_q \) and split Jacobian \( J_H/\overline{\mathbb{F}}_q \sim E^2/\overline{\mathbb{F}}_q \) over \( \overline{\mathbb{F}}_q \), then \( \#J_H(\mathbb{F}_q) = #E(\overline{\mathbb{F}}_q) \).

Proof. If \( H \) is regarded as a curve of genus 2 over \( \mathbb{F}_q \), from equation (2), we can obtain that

\[ \#J_H(\mathbb{F}_q) = q^2 - tr_E + 1. \]

(3)

If \( H \) is regarded as a curve of genus 2 over \( \overline{\mathbb{F}}_q \), then we can obtain

\[ L_q(T) = (q^2T^2 - tr_E T + 1)^2. \]

(4)

So

\[ \#J_H(\overline{\mathbb{F}}_q) = L_q(1) = (q^2 - tr_E + 1)^2. \]

(5)

Because of split Jacobian \( J_H/\overline{\mathbb{F}}_q \sim E^2/\overline{\mathbb{F}}_q \), we can deduce that

\[ \#J_H(\overline{\mathbb{F}}_q) = (#E(\overline{\mathbb{F}}_q))^2. \]

(6)

Combining equations (3), (5), and (6), we can get

\[ #E(\mathbb{F}_q) = #J_H(\mathbb{F}_q), \]

which is important for us to evaluate \( #J_H(\overline{\mathbb{F}}_q) \).
Proposition 2. Let $H$ be a genus 2 hyperelliptic curve and assume that $H$ is given by $y^2 = f(x)$ with $f$ a polynomial of degree 6 in $\mathbb{F}_q[x]$. If $H$ has split Jacobian $J_H/\mathbb{F}_q \cong E^2/\mathbb{F}_q$ with $\#J_H(\mathbb{F}_q)$ an odd, then $f$ is irreducible or a product of two irreducible polynomials with degree 3.

Proof. We have already known that the characteristic polynomial of the Frobenius endomorphism $\pi$ of $J_H$ is $\chi_H(T) = T^4 + \sigma T^2 + q^2$ with $\sigma = \#E(\mathbb{F}_q) - q^2 - 1$. Because $\chi_H(\mathbb{F}_q) = \chi_H(1)$ is prime, $\sigma$ is odd. Then, $T^{3q} \equiv 1 \mod ((2, \chi_H))$, where $\chi_H$ is the characteristic polynomial of Frobenius endomorphism $\pi$ of $J_H$. So, $\chi_H(\mathbb{F}_q)[2] = \{D \in J_H(\mathbb{F}_q) : 2D = 0\}$ is fixed by $\pi^6$, which means the 2-torsion points of $J_H$ are all $\mathbb{F}_{q^2}$-rational. Hence, $f$ is a product of linear factors over $\mathbb{F}_{q^2}$, which means the degrees of the $\mathbb{F}_{q^2}$-irreducible factors of $f$ must be factors of 6. So, if $f$ has more than 2 factors, there will be two cases:

(i) $f = h_1 h_2 h_3$ is a product of three $\mathbb{F}_q$-irreducible polynomials and there must be an irreducible factor of degree 2. The factor of degree 2 can be factored into $(x - x_0)(x - x_0')$ over $\mathbb{F}_q$. So, we can define a divisor $D_1$ by $D_1 = 2((x_0, 0) + (x_0', 0) - (\omega_1))$. Affected by the elements in $\text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$, $D_1$ has no change, which shows that $[D_1]$ is a $\mathbb{F}_q$-rational divisor class of order 2. That is a contradiction with our condition that $\#J_H(\mathbb{F}_q)$ is a prime. So, this case should be excluded. □

(ii) $f = h_1 h_2 \ldots h_i (i \geq 4)$ and there must be $\deg(h_1) = \deg(h_2) = 1$. We can define $D_1$ by $D_1 = 2D_1 = 0 \in \text{Pic}^0(H)$, which is similar to the first case. So, this case should be excluded.

3.2. Algorithms for $\deg(\phi) = 2$. Now we illustrate some concrete information about the cover map $\phi : H \to E$, which is in the form of $\phi(x, y) = (\phi_1(x), \phi_2(x, y))$. We start the experiment from a given elliptic curve. Under the existence of $\phi$, it is easy to deduce map $\phi_1 : \mathbb{P}^1 \to \mathbb{P}^1$, which satisfies the commutative diagram, where we represent the point $[x, 1]$ in $\mathbb{P}^1$ by $x$.

We define $E$ by $s^2 = g(t) \in \mathbb{F}_q[t]$, where $g(t)$ is an irreducible polynomial of degree 3. Otherwise, there will be a contradiction with the claim that $\#E(\mathbb{F}_{q^2})$ is prime. So, $g(t)$ can be written into the form of $g(t) = (t - \beta)(t - \beta')$ $(t - \beta'' \ldots \beta'')$, $\beta \in \mathbb{F}_{q^2}/\mathbb{F}_{q^2}$. Because the degree of $\phi$ equals 2, the expression of $\phi_1$ is as follows:

$$\phi_1(x) = \frac{a_2 x^2 + a_1 x + a_0}{(x - \omega)^2},$$

where $a_0, a_1, a_2, \epsilon \in \mathbb{F}_{q^2}$ are the values that should be determined from the given $E$. However, the number of the values that should be determined is more than the number of the equations from restrictions, so we must fix some of them. The following lemma is helpful for reducing the number of the indeterminate values.

Lemma 3. For every automorphism $\psi : H/\mathbb{F}_{q^2} \to H/\mathbb{F}_{q^2}$, there is a linear fractional transformation $\tau : \mathbb{P}^1/\mathbb{F}_{q^2} \to \mathbb{P}^1/\mathbb{F}_{q^2}$ with $\tau(x) = ax + bcx + d$ for some $a, b, c, d \in \mathbb{F}_{q^2}$ with $a \neq bc \neq 0$ such that the following diagram commutes:

$$\begin{array}{ccc}
H & \to & H \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \to & \mathbb{P}^1 \\
\psi & & \tau \\
\end{array}$$

It can be proved that this map is transitive over $\mathbb{F}_{q^2}/\mathbb{F}_{q^2}$, which means the map satisfies (i) $ax + b/cx + d \in \mathbb{F}_{q^2}/\mathbb{F}_{q^2}$ for all $x \in \mathbb{F}_{q^2}/\mathbb{F}_q$, and (ii) there exist $a, b, c, d \in \mathbb{F}_{q^2}$ such that $y = ax + bcx + d$ for all $x, y \in \mathbb{F}_{q^2}/\mathbb{F}_q$.

From the lemma, we can fix the value of $\epsilon \in \mathbb{F}_{q^2}$ in the expression of $\phi_1(x)$ because different values of $\epsilon$ induce equivalent cover map $\phi$. So, we can fix $\epsilon$ into $\omega$, a generator of $\mathbb{F}_{q^2}$, and any other value can be mapped into it by the linear map above. Then, the expression of $\phi_1$ can be fixed in

$$\phi_1(x) = \frac{a_2 x^2 + a_1 x + a_0}{(x - \omega)^2}.$$
on Lemma 1, we can deduce the corresponding maps, where the ramification of \( \phi_1 \) at \( \alpha^{q^i} \) is 1.

\[
\begin{array}{cccc|cccc|cccc|cccc}
\alpha & \alpha^{q^2} & \alpha^{q^4} & \cdots & \alpha & \alpha^{q^2} & \alpha^{q^4} & \cdots & \alpha & \alpha^{q^2} & \alpha^{q^4} & \cdots \\
\beta & \beta^{q^2} & \beta^{q^4} & \cdots & \beta & \beta^{q^2} & \beta^{q^4} & \cdots & \beta & \beta^{q^2} & \beta^{q^4} & \cdots \\
\end{array}
\]

where \( x_1, \ldots, x_12 \) are extra six unknown values. The useful information of the map is extracted, and we can obtain the following two equations:

\[
a_2 a_1^2 + a_1 a_0 + a_0 - \beta (a_0 - \omega)^2 = 0, \quad (11)
\]

\[
a_2 a_1^2 + a_1 a_0 + a_0 - \beta (a_1 - \omega)^2 = 0. \quad (12)
\]

By using these equations and the scalar restriction process, we can get a system of 12 equations of degree 3. Then, we can obtain an ideal generated by the equations and the solutions emerge because the dimension of the ideal is 0.

As the results, \( t = \phi_1(x) \) can be submitted into the equation of \( E: s^2 = (t - \beta)(t - \beta^{q^i}) \) and the procedure can be inferred as follows:

\[
s^2 = (t - \beta)(t - \beta^{q^i}) (t - \beta^{q^j})
\]

\[
= \left( a_2 x^2 + a_1 x + a_0 \right) \left( a_2 x^2 + a_1 x + a_0 \right) \left( a_2 x^2 + a_1 x + a_0 \right) \left( x - \omega \right) \left( x - \omega \right)
\]

\[
= \frac{y^2 g(a_2)}{(x - \omega)^6}
\]

So, in order to get the expression of \( \phi_2(x, y) \), \( g(a_2) \) must be a square in \( \mathbb{F}_{q^2} \).

Let us retell the whole process of our algorithms. First, we examine the existence of the hyperelliptic curves, which can be mapped into \( E/\mathbb{F}_{q^2} \) and satisfy that (i) \( f \) is simple and (ii) \( H_{E/\mathbb{F}_{q^2}} \sim E^2 \); (iii) \( \# H_{F_q} \) is a prime. Then, we get a system consisting of 12 equations through scalar restriction of equations (11) and (12), whose Groebner basis is easy to compute. The solutions of the equations are what we want and they can make us obtain the expressions of the cover maps and the corresponding hyperelliptic curves.

3.2.2. \( f \) is Reducible. In this part, we discuss that the equation of \( H \) is reducible. Then, by Proposition 2, the equation can be factored into such two \( \mathbb{F}_{q^2} \)-irreducible polynomials of degree 3 that we can factor it over \( \mathbb{F}_{q^2} \) into \( f(x) = (x - \alpha)(x - \alpha^{q^i})(x - \gamma)(x - \gamma^{q^j}) \)
\((x - y^t), \alpha, \gamma \in \mathbb{F}_q \setminus \{0\}\). So, we can get the corresponding map.

\[
\begin{array}{c|ccc}
\mathbb{P}^1 & \alpha & \alpha^g & \alpha^2 \\
\hline
\mathbb{P}^1 & \gamma & \gamma^g & \gamma^2 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
\mathbb{P}^1 & \beta & \beta^g & \beta^2 \\
\end{array}
\]

By using the scalar restriction on equations (14) and (15), we can also get a system of 12 equations on 12 variables. Something should be noticed that dimension of the ideal generated by the system is 3. For dimension reduction, we should choose fixed value for 3 variables and then the rational points can be computed on a zero-dimension scheme. To give more information about the forms of the hyperelliptic curves in this case, we propose the following proposition.

**Proposition 3.** Let H be a genus 2 hyperelliptic curve and assume that H is given by \(y^2 = f(x)\) with f a polynomial of degree 6 in \(\mathbb{F}_q[x]\). If H has split Jacobian \(J_H/\mathbb{F}_q \sim E/\mathbb{F}_{q^2}\) with \(\#J_H(\mathbb{F}_q)\) is a prime and the degree of the cover map \(\phi: H/\mathbb{F}_q \rightarrow E/\mathbb{F}_{q^2}\) is 2. Then, the corresponding cover map can be easily computed if \(f\) is of the form:

\[
f(x) = (x - \alpha)(x - \alpha^g)(x - \alpha^2)(x - \gamma)(x - \gamma^g)(x - \gamma^2),
\]

where \((\alpha + \gamma)(\omega^2 + \omega) = 2(\alpha \gamma + \omega^{g+1})\) and \(\omega \in \mathbb{F}_{q^2}/\mathbb{F}_q\) is the generator of \(\mathbb{F}_{q^2}\). \(\alpha, \gamma \in \mathbb{F}_{q^2}/\mathbb{F}_q\).

**Proof.** The corresponding x-coordinate map can be written into

\[
\phi_1(x) = \frac{a_2 x^2 + a_1 x + a_0}{(x - \omega)^2} \in \mathbb{F}_{q^2}(x),
\]

(17) So, it is clear that the ramification index of \(\phi_1\) at \(\omega\) is 2. By the Riemann–Hurwitz formula [31]

\[
= 2 - 2g_{\phi_1} = \deg(2 - 2g_{\phi_1}) - \sum (e_{\phi} - 1) - W,
\]

(18) where \(W\) is the notation for wild ramification, there must be another point \(c_0\), where the ramification index of \(\phi_1\) is 2. If \(\phi_1(c_0) = t_0\), then we can construct an equation \(a_2 x^2 + a_1 x + a_0 = t_0 (x - \omega)^2\), which has such a double root that can help us get the relationship among \(t_0\) and \(a_2, a_1, a_0\):

\[
\Delta = 0 \Rightarrow t_0 = \frac{4a_0 a_2 - a_1^2}{4a_1 \omega + 4a_0 \omega^2 + 4a_0}.
\]

(19) Substituting formula (19) into the equation \(\phi_1(c_0) = t_0\), we can get the following expression:

\[
c_0 = \frac{2a_0 + a_1 \omega}{2a_1 \omega + a_1}.
\]

(20) The linear fractional transformation \(\tau: x = a x + b/c x + d\) is considered. Because \(\phi_1\) is ramified at \(\omega\) and \(c_0\), there are two diagrams:

It can be found that \(\tau \neq \text{id}\) while \(\tau^2 = \text{id}\), where \(\text{id}\) means identity transformation. So

\[
\begin{pmatrix}
 a \\ c
 b \\ d
\end{pmatrix}
\begin{pmatrix}
 a \\ c
 b \\ d
\end{pmatrix}
\sim
\begin{pmatrix}
 a^2 + bc & b(a + d) \\ c(a + d) & d^2 + bc
\end{pmatrix}
\sim
\begin{pmatrix}
 1 & 0 \\ 0 & 1
\end{pmatrix}
\]

(21) Then, we can simplify the formula of \(\tau\) into

\[
\tau(x) = x + b/c x - 1.
\]

After adjusting the coefficients of \(\phi_1\), it is reasonable to require \(\phi_1(x) = \phi_1(\tau(x))\). Combining it with \(\tau(\omega) = \omega\), we can get
\[ a_0 = 0, \quad (22) \]
\[ c\omega^2 - 2\omega - b = 0, \quad (23) \]
\[ a_1 + (2\omega - c\omega^2)a_2 = 0. \quad (24) \]

Using the original restriction of \( \phi_1: \phi_1(a) = \phi_1(y), a \neq y \), we can derive that
\[ (a_1 + 2a_2\omega)xy + (a_0 - a_2\omega^2)(\alpha + y) - a_1\omega^2 - 2a_0\omega = 0. \quad (25) \]

From equations (22), (24), and (25), the following equation can be derived:
\[ cxy - (\alpha + y) + 2\omega - c\omega^2 = 0, \quad (26) \]
which means \( \tau(\alpha) = y \). Similarly, using \( \phi_1(a^2) = \phi_1(\gamma^3) \), \( \phi_1(\beta^2) = \phi_1(\gamma^3) \), we can get an equation system as follows:
\[ \begin{align*}
\alpha + b &= c\gamma \alpha + 1, \\
\alpha^2 + b &= c\gamma \alpha \beta + 1, \\
\alpha^3 + b &= c\gamma \alpha \beta^2 + 1.
\end{align*} \quad (27) \]

From which we can find that \( b, c \in \mathbb{F}_q \), which means the linear fractional transformation \( \tau(x) = ax + b/cx + d \) satisfies \( a, b, c, d \in \mathbb{F}_q \). Now, we can get the relationship between the two points, at which the ramification index of \( \phi_1 \) is 2:
\[ \omega = \frac{aw + b}{cw + d} \implies \omega^2 = \frac{aw^2 + b}{cw^2 + d} \quad (28) \]

Because \( c_0 \) and \( \omega \) are the only two points, which satisfy \( \tau(x) = x \), we can have \( c_0 = \omega^2 \). Combining \( c_0 = \omega^2 \) with equations (20), (25), and (28) and using \( a_i \)'s proportional coefficients, we can get the final result (\( \alpha + y \)(\( \omega^2 + \omega \)) = 2(\( \alpha y + \omega \)).

### 3.2.3. Statistical Results.

Elliptic curves are in the same isomorphism class if they have the same \( j \)-invariant. We count the number of the isomorphism classes that can be attacked by the algorithms of degree 2 in some small fields (Table 1). Let Total be the number of \( j(E) \neq 0, 1728 \) when \( E/\mathbb{F}_q \) is in the form of \( y^2 = (x - \beta)(x - \beta^2)(x - \beta^3) \), \( \beta \in \mathbb{F}_q \). Let \( \text{Attack}_1 \) (resp. \( \text{Attack}_2 \)) be the number of \( j(E) \neq 0, 1728 \) that \( E \) can be attacked by the algorithms with \( \text{deg}(\phi(x)) = 2 \) and irreducible (resp. reducible) \( f \).

From the table, we can find that all of the isomorphic classes of \( E \) in the form of \( y^2 = (x - \beta)(x - \beta^2)(x - \beta^3) \), \( \beta \in \mathbb{F}_q \) can be attacked by our algorithms with \( \text{deg}(\phi(x)) = 2 \) and reducible \( f \).

### 3.3. Algorithms for \( \text{deg}(\phi) = 3 \).

The whole progress of the experiment for \( \text{deg}(\phi) = 3 \) is similar to that for \( \text{deg}(\phi) = 2 \) with a few differences on the cover diagram and the equation system to be solved. So, for \( \text{deg}(\phi) = 3 \), we only introduce one circumstance that \( f \) can be written into the product of two irreducible polynomials of degree 3 and the map is as follows:

| Table 1: Number of isomorphism classes that can be attacked by the algorithms. |
|-----------------|-----------------|-----------------|-----------------|
| \( q \)        | 3               | 5               | 7               |
| Total          | 3               | 8               | 16              |
| \( \text{Attack}_1 \) | 1               | 4               | 4               |
| \( \text{Attack}_2 \) | 3               | 8               | 16              |

It is obvious that the expression of \( \phi_1 \) is as follows:
\[ \phi_1(x) = \frac{a_0x^3 + a_2x^2 + a_1x + a_0}{(x - \gamma)(x - \gamma^3)(x - \gamma^2)} \quad (29) \]

where \( \gamma \) is one of the roots of \( f \) over \( \mathbb{F}_q \) and \( a_i \in \mathbb{F}_q \). The expression of \( \alpha \) and \( y \) is same as that in algorithm for \( \text{deg}(\phi) = 2 \) and \( f \) is reducible, while there are a few changes in the variables because of the different expression of \( \phi_1 \) and the existence of \( \nu \in \mathbb{F}_q \):
\[ \nu = x\gamma \omega + x\gamma^2 \omega^2 + \cdots + x\gamma^6 \omega^7, \]
\[ a_i = x_{i+3} \left( \omega + \omega^2 + \omega^3 \right) + x_{i+2} \left( \omega + \omega^7 + \omega^6 \right), \text{where } i \in \{0, 1, 2, 3\}. \]

From Lemma 1, we can derive that the function \( \phi_1(x) - \beta \) has a multiple root \( \nu \), which must not be equal to \( a \) because of Riemann-Hurwitz formula:
\[ \phi_1(x) - \beta = \frac{a_3x^3 + a_2x^2 + a_1x + a_0 - \beta(x - \gamma)(x - \gamma^3)(x - \gamma^2)}{(x - \gamma)(x - \gamma^3)(x - \gamma^2)} = 0. \quad (31) \]

Because \( \phi_1(x) - \beta \) has two different roots \( \alpha \) and \( \nu \) with \( \nu \) a double root, we can get the following equation:
\[ a_3x^3 + a_2x^2 + a_1x + a_0 - \beta(x - \gamma)(x - \gamma^3)(x - \gamma^2) = (a_3 - \beta)(x - \alpha)^2 \quad (32) \]

From that, we can induce three equations, which can be transferred into a system of 18 equations with 20 variables through scalar restriction:
\[ a_0 + \beta y \gamma \gamma^3 \gamma^2 \gamma^3 = -(a_3 - \beta) \gamma^2 \alpha, \quad (33) \]
\[ a_2 + \beta y \gamma^3 \gamma^2 \gamma^3 + \beta y \gamma^3 \gamma^2 = -(a_3 - \beta) (2y + \alpha), \quad (34) \]
\[ a_3 - \beta y \gamma \gamma^2 \gamma^2 - \beta y \gamma \gamma^2 \gamma^2 - \beta y \gamma \gamma^2 \gamma^2 = (a_3 - \beta)(y^2 + 2\alpha). \quad (35) \]
We should fix the value of \(a_3 \neq 0\) and other 2 variables to compute on a zero-dimension scheme. To derive the expression of \(\Phi_2(x, y)\), the value of \(a_1\) should be classified, one is a quadratic residue and the other is a quadratic nonresidue.

3.3.1. Statistical Analysis. After analyzing the solutions of a fixed hyperelliptic curve in a relatively small field, we can find that \(\nu\) only has two different values \(\nu_1\) and \(\nu_2\) with \(\nu_2 = \nu_1^q\). Each choice of \(\nu\) corresponds to an isomorphism class of elliptic curves, which conforms to the split Jacobian of \(H\) over \(\mathbb{F}_{q^2}\). The relationship between the cover maps \(\Phi_1(x)\) and \(\Phi_1(x)\), related to \(\nu_1\) and \(\nu_2\) respectively, is \(\Phi_1(x) = \Phi_1(x)\), where the \(p\)th power over \(\Phi_1\) means \(p\)th power over each coefficient of \(\Phi_1\).

\[
\phi_1 \rightarrow E_1 \quad \text{corresponding to the preimage } \nu_1
\]
\[
\Phi_1 = \alpha \Phi_1 \rightarrow E_2 \quad \text{corresponding to the preimage } \nu_2 = \nu_1^p.
\]

It can be checked that the coefficients of the formula of \(E_2\) equal to the \(p\)th power over those of \(E_1\), so \(E_1\) and \(E_2\) are in the same isogeny class. Because of the special relationship of \(\nu\), we consider that it may be possible to express \(\nu\) by other unknown values, which will reduce 6 variables. Equations (33)–(35) can be used to preprocess these unknown data and the relationship is as follows:

\[
\nu = \frac{a_3 \alpha + a_2 - \beta \alpha + \beta (y + y^p + y^{2p})}{2(\beta - 1)}.
\]

However, the substitute of the expression for \(\nu\) will make equation (18) forever admitted. After experiments begin with elliptic curves and hyperelliptic curves respectively, we give the following suggestions:

(i) If count \#_H(\mathbb{F}_{q^2}) of a given hyperelliptic curve \(H\) is the goal, which means that the experiment is started with the hyperelliptic curve, \(\nu\) should be expressed by \(\nu = a_3 \alpha + a_2 - \beta \alpha + \beta (y + y^p + y^{2p})/2(\beta - 1)\), which can reduce 6 variables in the final equations. Because of the reduction in the number of both variables and restrictions, the dimension of the final ideal will decrease from 6 to 2, which will cut down the time complexity to a great extent.

(ii) If the cover attack on a given elliptic curve is the goal, which means that the experiment is started with the elliptic curve, \(\nu\) can be expressed by either \(\nu = x_1 \alpha + x_6 \alpha + \cdots + x_{12} \alpha^p, i \in [0, 1, \ldots, 5]\) or \(\nu = a_3 \alpha + a_2 - \beta \alpha + \beta (y + y^p + y^{2p})/2(\beta - 1)\). The dimension of the ideal generated by restrictions is always 2 under both of the two expressions.

3.3.2. Algorithm Improvement. We now try to reduce the dimension of the final ideal, which will enhance the efficiency of the algorithm. The key point is to reduce the number of the variables. The elliptic curve \(y^2 = (x - \beta(x - \beta^q))(x - \beta^q)\) may be written as \(y^2 = x(x - 1)\). Hence, we can reduce 6 variables in the final equations. Because \(\alpha_{1}^{\nu} \neq \alpha_{2} \), with the hyperelliptic curve, the goal, which means that the experiment is started with the elliptic curve, \(\nu_1\) and \(\nu_2\) respectively, the dimension of the ideal generated by restrictions is always 2 under both of the two expressions.

The expression of \(\Phi_1\) is as follows:

\[
\Phi_1 = \frac{b_0 (x - a)(x - y)^2}{(x - y)(x - y^p)}
\]

where \(a\) and \(y\) are the roots of \(f\) over \(\mathbb{F}_{q^2}\) and \(b_0, \nu \in \mathbb{F}_{q^2}\). The variables are as follows:

\[
\begin{align*}
\alpha_i &= \alpha_1^\nu = x_i \left(\alpha_1^\nu + \varepsilon \alpha_1^{i\nu}\right) + x_i \left(\alpha_1^{\nu - \varepsilon \nu} + \varepsilon \alpha_1^{i\nu}\right) \quad i \in [0, 1, 2], \\
y_i &= \alpha_1^\nu = x_i \left(\alpha_1^\nu + \varepsilon \alpha_1^{i\nu}\right) + x_i \left(\alpha_1^{\nu - \varepsilon \nu} + \varepsilon \alpha_1^{i\nu}\right) \quad i \in [0, 1, 2], \\
\beta_i &= \alpha_1^\nu = x_i \alpha_1^\nu + \cdots + x_{12} \alpha_1^\nu, \quad i \in [0, 1, \ldots, 5].
\end{align*}
\]

\[
\begin{align*}
b_0 &= x_{13} \alpha_1^\nu + x_{14} \alpha_1^\nu + \cdots + x_{16} \alpha_1^\nu.
\end{align*}
\]

The restricted equations are as follows:

\[
\begin{align*}
b_0 (a_2 - a_0)(a_2 - y_0) &= (a_2 - y_0)(a_2 - y_1)(a_2 - y_2), \\
b_0 (y_2 - a_0)(y_2 - y_0) &= (y_2 - y_0)(y_2 - y_1)(y_2 - y_2), \\
b_0 (y_4 - a_0)(y_4 - y_0) &= (y_4 - y_0)(y_4 - y_1)(y_4 - y_2), \\
b_0 (a_1 - a_0)(a_1 - y_0) &= (a_1 - y_0)(a_1 - y_1)(a_1 - y_2),
\end{align*}
\]

which can be transferred into a system of 24 equations with 18 variables through scalar restriction. The dimension of the final ideal is 1 which is reduced by a half.

If we start with hyperelliptic curves, when \(a, y\) are known, then the dimension of the final ideal in the previous algorithm is 2 so that we must try all of the possible values of the two free variables. After the improvement, we can get a system of 18 equations with 12 variables and the dimension of the final ideal is 0, which will reduce the time of traversing all values of the free variables.

4. Comparison and Experiments in Large Field

4.1. Experiment for \(\deg(f) = 2\) and \(f\) is Reducible. We give a finite field \(\mathbb{F}_{q^2}\), where \(q = 2^{128} + 51\). Defining the \(\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha^{2}]\), where \(\alpha^2 + 28167277929244298220226\).
4.2. Example for degree 3 and $f$ is reducible. Given the finite field $\mathbb{F}_q$ with $q = 2^{10} + 7$ and $\mathbb{F}_{q'} = \mathbb{F}_q[\omega]$ with $\omega = \frac{10}{3} + 7$, the elliptic curve $E$ over $\mathbb{F}_q$ with the following equation:

$$y^2 = x^3 + (1722396203232322949247395322935747591\omega + 7094719520841470544987103040980544)x^2 + (13400311736338243271469458662641534\omega + 31472243432282025055895452768326513302)x + 24655036166906225336773174912389706\omega + 164982211005580436237787851811362782805,$$

whose order over $\mathbb{F}_q$ is a 256-bit prime.


\[
\begin{align*}
\phi_1(x) &= \frac{x^2 + 29567739428955780381390627507299503045x}{(x - \omega)^2}, \\
\phi_2(x, y) &= \frac{7792966484872093801383267758033379311\omega + 241747055078217882048817891777938173676}{\text{deno}},
\end{align*}
\]

where deno $= x^3 + 340282366920938463463374 \cdot 607431768211504\omega x^2 + (17582876288546443220873432757023 \cdot 74086\omega + 8712335979187571187991945702287453310)x + (15869988704662135810832199000196489929\omega + 640075049601734131141520643438648547).$

According to Proposition 1, we can get $\#I_H(\mathbb{F}_q) = 1157920892373619542357$ and $\#E(\mathbb{F}_q)$ is not a prime.

\[
\begin{align*}
\phi_1(x) &= \frac{\omega x^3 + (589\omega + 879)x^2 + (365\omega + 41)x + 355\omega + 506}{(x - \gamma)(x - \gamma^p)(x - \gamma^{p^2})}, \\
\phi_2(x, y) &= \frac{(960\omega + 789)x^3 + (177\omega + 21)x^2 + (56\omega + 793)x + (986\omega + 449)}{x^3 + 1000x^2 + 964x^3 + 564x^2 + 90x^2 + 842x + 807}\cdot y.
\end{align*}
\]

We can also get that the order of the Jacobian of $H$ over $\mathbb{F}_q$ is 1064295, whose bit length is equal to the bit length of $\#I_{H,q}$. This example illustrates that our algorithms can also apply to the case, in which $\#E(\mathbb{F}_q) = \#I_H(\mathbb{F}_q)$ is not a prime.
4.3. Comparison. Here, we offer comparisons between our algorithms and existing cover attacks for ECDLP (resp. counting methods for Jacobians of hyperelliptic curves).

As a kind of cover attack for ECDLP, the method in the study has same complexity $O(q)$ as GHS attack, which is the most efficient algorithm for general elliptic curves.

As a counting method for Jacobians of hyperelliptic curves, our algorithms can easily compute the cover map for hyperelliptic curves $y^2 = f(x) = (x - a)(x - a^q)$, where $(a + \gamma)(a^q + \gamma) = 2(\alpha \gamma + \omega^{q+1})$, $\omega \in \mathbb{F}_{q^2}/\mathbb{F}_q$, $a, \gamma \in \mathbb{F}_{q^2}/\mathbb{F}_q$. To be noted that, there is no subexponential general algorithm for some small sets of examples [11]. The algorithm in reference [4] dealt with hyperelliptic curves of form $y^2 = rx^6 + sx^4 + \sigma(s)x^2 + \sigma(r)$, where $\sigma$ is the generator of the Galois group of a quadratic extension. For random hyperelliptic curves [12], an experiment is run for about one week for a genus 2 curve defined over an 80-bit field.

5. Conclusion

In the article, we propose a new method to compute the cover map from hyperelliptic curves of genus 2 to the elliptic curves with prime order. To conduct the experiments successfully, we put forward some important lemmas and propositions first. Then, we propose three different algorithms according to the different degrees of $\phi$ and the different forms of equations of hyperelliptic curves. As an application, we also give examples in relatively large fields. Under the existence of the cover map, we can use it to substitute the GHS attack in cover and decomposition attack in some specific cases. We can also use the algorithms to evaluate the order of the Jacobians of hyperelliptic curves in polynomial time, which can be generalized to generating required hyperelliptic curves. It should be improved that our algorithms apply to a particular part of elliptic curves and hyperelliptic curves, but the method is still very useful in the ECC and HECC.

For the further areas related to this work, we can probe the following two directions:

(i) About Finding the More Concrete Form of the Hyperelliptic Curves or Elliptic Curves. We take Proposition 3 as an example. According to the relationship between $a$ and $y$ in Proposition 3, we can reduce the number of the variates, thus enhancing the efficiency of our algorithm. So, the more concrete form of hyperelliptic or elliptic curves may improve the efficiency.

(ii) About the Fast Solution Method Nonlinear Systems. We now use scalar restriction and Groebner basis to get the solutions of the equations, thus getting the expressions of the cover maps and the corresponding hyperelliptic curves. The further research may investigate faster way to solve nonlinear systems.

Data Availability

Data can be obtained upon request to the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References
