CSIDH WITH LEVEL STRUCTURE

STEVEN D. GALBRAITH, DEREK PERRIN, AND JOSÉ FELIPE VOLOCH

Abstract

We construct a new post-quantum cryptosystem which consists of enhancing CSIDH and similar cryptosystems by adding a full level N structure. We discuss the size of the isogeny graph in this new cryptosystem which consists of components which are acted on by the ray class group for the modulus N. We conclude by showing that, if we can efficiently find rational isogenies between elliptic curves, then we can efficiently find rational isogenies that preserve the level structure. We show that one can reduce the group action problem for the ray class group to the group action problem for the ideal class group. This reduces the security of this new cryptosystem to that of the original one.

1. Introduction

Group actions are a promising direction in post-quantum cryptography. In 1997, Couveignes proposed the first isogeny-based group action cryptosystem [4] which used ordinary elliptic curves over a finite field $\mathbb{F}_q$ and whose difficulty relied on the isogeny problem. This cryptosystem was later independently rediscovered by Rostovtsev and Stolbunov [7]. In 2018, the CSIDH [2] cryptosystem was proposed. It was based on the Couveignes-Rostovtsev-Stolbunov (CRS) key exchange but constructed using supersingular curves over $\mathbb{F}_p$ instead of ordinary curves over $\mathbb{F}_q$. The authors chose supersingular curves for various efficiency reasons which are explained in detail in [2]. When CSIDH was initially proposed, the authors claimed the key exchange was over 2000 times faster than the state-of-the-art CRS implementation at the time. However, even with this speedup, a drawback of CSIDH is that it is still considered to be inefficient when compared to other post-quantum algorithms.

In 2011, De Feo, Jao, and Plût proposed an alternative isogeny-based scheme, supersingular isogeny Diffie-Hellman (SIDH), which was based on the path finding problem in the full isogeny graph of supersingular curves[5]. The scheme involved publishing images of torsion points to create a Diffie-Hellman type protocol to overcome the non-commutativity of the endomorphism rings. These image points turned out to be problematic and this scheme was later shown to be insecure[1]. Our proposal also uses torsion points, but in a different way from SIDH.

In this paper, we will construct a modification of CSIDH which involves adding a level N structure. The hope is to gain additional security by choosing appropriate N which in turn would allow us to reduce the size of prime field we work over and thus speed up computations. We will then show if we can solve the isogeny problem presented in CRS and CSIDH that we can solve this new problem efficiently and give an algorithm for doing so.

1.1. Preliminaries.

We begin by briefly recalling the CSIDH cryptographic primitive and refer the reader to [2] for the full details.

For a supersingular elliptic curve $E/\mathbb{F}_p$, we will let $\mathrm{End}_p(E) \subseteq \mathrm{End}(E)$ denote the subring of $\mathrm{End}(E)$ that consists of $\mathbb{F}_p$-rational endomorphisms of E. Although $\mathrm{End}(E)$ is an order in a quaternion algebra, this subring is in fact isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field K.

Department of Mathematics, The University of Auckland, Auckland, New Zealand
School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
E-mail addresses: s.galbraith@auckland.ac.nz, derek.perrin@pg.canterbury.ac.nz, felipe.voloch@canterbury.ac.nz.
The authors acknowledge support from MBIE.

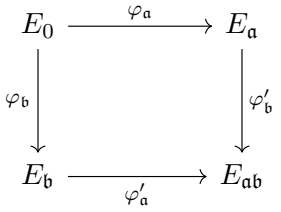

FIGURE 1. A commutative diagram of CRS-like key exchange protocols.

For an ordinary elliptic curve $E/\mathbb{F}_q$, where $q = p^k$ for some $k \in \mathbb{Z}$, the whole endomorphism ring $\mathrm{End}(E)$ is an order $\mathcal{O}$ in an imaginary quadratic field K.

For a given order $\mathcal{O}$, we are interested in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ the set of supersingular elliptic curves whose $\mathbb{F}_p$-rational endomorphism rings are $\mathcal{O}$.

It is a well-known fact that the class group $Cl(\mathcal{O})$ acts simply transitively on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$[9, Corollary II.1.2]. The CSIDH key exchange is similar to the CRS cryptosystem [4, 7]: Alice samples an element $[\mathfrak{a}] \in Cl(\mathcal{O})$, computes $[\mathfrak{a}] * E_0 = E_{\mathfrak{a}}$, for some starting curve E_0 and sends $E_{\mathfrak{a}}$ to Bob. Bob does the same but with an element $[\mathfrak{b}] \in Cl(\mathcal{O})$ and their shared secret is $[\mathfrak{a}][\mathfrak{b}]E_0 = E_{\mathfrak{ab}} = E_{\mathfrak{ba}} = [\mathfrak{b}][\mathfrak{a}]E_0$. This key exchange works due to the commutativity of the action of $Cl(\mathcal{O})$ as shown in Figure 1.

2. CSIDH with Level Structure

In this section, we will discuss modifying CSIDH by adding a level structure. Our motivation is to obtain a larger group action than standard CSIDH which would allow us to with a smaller prime. Recall the security of CSIDH is dependent on $\#Cl(\mathcal{O})$ which is asymptotically known to be $\#Cl(\mathcal{O}) \approx \sqrt{|\Delta|}$ [8] where $\Delta = t^2 - 4p$ and $t \in \mathbb{Z}$ is the trace of Frobenius. Since we are working with supersingular curves over $\mathbb{F}_p$, $t = 0$ and so the size of the class group is determined by our choice of p.

Definition 2.1. Consider an elliptic curve E and a prime N with $(p, N) = 1$. Then a $\Gamma(N)$-*structure* on E is a pair of points (P, Q) that is a basis for $E[N]$.

When considering the isogeny graph of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, we can add level structure to the graph as follows:

Definition 2.2. Let N be a prime with $(p, N) = 1$ and

$$\mathbb{V} = \{(E, P, Q) \mid E \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p), P, Q \text{ a basis for } E[N]\} / \sim$$

be a set of vertices modulo the equivalence relation $(E, P, Q) \sim (E', P', Q')$ if there exists an isomorphism $f : E \to E'$ with $f(P) = P'$ and $f(Q) = Q'$. There is an edge between vertices $(E, P, Q), (E', P', Q')$ if there is an isogeny $\varphi : E \to E'$ with $\varphi(P) = P'$ and $\varphi(Q) = Q'$. We say this graph has $\Gamma(N)$-*structure* or *full level* N *structure.*

If we consider the isogeny graph G with vertex set $\mathbb{V} = \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, we can add a $\Gamma(N)$ structure to it to obtain a new graph $G(N)$. It is clear that $\#G(N) > \#G$. In fact, it can be shown

$$\#G(N) = \#G\frac{(N^2 - N)(N^2 - 1)}{2}. \tag{1}$$

As such, we have a group larger than the usual class group acting on this set. We can observe this by considering the multiplication-by-m map where $(m, N) = 1$. For a curve E on G, we have $[m] : E \mapsto E$ while for the triple (E, P, Q) on $G(N)$ we have $[m] : (E, P, Q) \mapsto (E, mP, mQ)$.

Definition 2.3. Let K be an imaginary quadratic field, $\mathcal{O} \subseteq K$ an order, and $\mathfrak{m} \subseteq \mathcal{O}$ a modulus. We let $\mathcal{I}_{\mathfrak{m}}$ denote the group of fractional ideals which are coprime to $\mathfrak{m}$, and $\mathcal{P}_{\mathfrak{m},1} \subseteq \mathcal{I}_{\mathfrak{m}}$ denote the subgroup generated by principal ideals (α) where $\alpha \equiv 1 \mod \mathfrak{m}$. The *ray class group* for the modulus $\mathfrak{m}$ is the quotient

$$Cl_{\mathfrak{m}}(\mathcal{O}) = \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m},1}.$$

There exists an algorithm [3] to compute $Cl_{\mathfrak{m}}(\mathcal{O})$ and its size $h_{\mathfrak{m}}$.

Proposition 2.4. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and $\mathfrak{m}$ a modulus for K. The class number $h_{\mathfrak{m}} := \#Cl_{\mathfrak{m}}(\mathcal{O})$ is finite and given by*

$$h_{\mathfrak{m}}(\mathcal{O}) = \frac{\#(\mathcal{O}/\mathfrak{m})^{\times} h(\mathcal{O})}{[\mathcal{O}^{\times} : \mathcal{O}^{\times}_{\mathfrak{m}}]}$$

where $h(\mathcal{O}) = \#Cl(\mathcal{O})$ and $\mathcal{O}^{\times}_{\mathfrak{m}}$ is the group of units $\mathcal{O}^{\times}$ congruent to 1 modulo $\mathfrak{m}$.

Proof. See [3, Corollary 3.2.4]. □

Setting $\mathfrak{m} = (N)$, the group action we have on $G(N)$ comes from $Cl_{\mathfrak{m}}(\mathcal{O})$. The cardinality $h_{\mathfrak{m}}$ of $Cl_{\mathfrak{m}}(\mathcal{O})$ is at most $(N^2-1)h(\mathcal{O})$ while equation (1) gives $\#G(N) = \frac{(N^2-1)(N^2-N)h(\mathcal{O})}{2}$, and so $G(N)$ is disconnected.

We will now consider a slight modification of the CSIDH key exchange whereby we add a level structure to $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. We choose a prime N with $(p, N) = 1$, along with a basis P_0, Q_0 of $E_0[N]$. As in the original scheme, sample an element $[\mathfrak{a}] \in Cl_{\mathfrak{m}}(\mathcal{O})$ with $(N(\mathfrak{a}), N) = 1$ and compute the isogeny $\varphi_{\mathfrak{a}}$ induced by $[\mathfrak{a}]$. This time, however, in addition to sending $E_{\mathfrak{a}}$ to Bob, she also sends a basis $P_{\mathfrak{a}}, Q_{\mathfrak{a}}$ of $E_{\mathfrak{a}}[N]$ where $\varphi_{\mathfrak{a}}(P_0) = P_{\mathfrak{a}}, \varphi_{\mathfrak{a}}(Q_0) = Q_{\mathfrak{a}}$, and similarly for Bob. The shared secret is then $(E_{\mathfrak{ab}}, P_{\mathfrak{ab}}, Q_{\mathfrak{ab}})$ where $P_{\mathfrak{ab}} = P_{\mathfrak{ba}}$ by the commutativity of Figure 1.

In terms of security of such a scheme, consider the following. Suppose there is a secret isogeny $\varphi : E_0 \to E_1$ with $\varphi(P_0) = P_1$ and $\varphi(Q_0) = Q_1$ where (P_i, Q_i) is a basis for $E_i[N]$, and we can find an isogeny $\psi : E_0 \to E_1$ but with $\psi(P_0) = P, \psi(Q_0) = Q$ for (P, Q) a basis for $E_1[N]$. Any additional security of this scheme would come from the fact that the isogeny graph is disconnected and the ability to solve standard CSIDH (i.e. given E_0, E_1, find $\varphi : E_0 \to E_1$) may not imply we could find an isogeny mapping the N-torsion points correctly. This leads to the natural question: does there exist an endomorphism $\alpha = a + b\pi$ such that the following system

$$\alpha(P) = aP + b\pi P = P_1,$$
$$\alpha(Q) = aQ + b\pi Q = Q_1$$

is consistent? Recall we are interested in endomorphisms of the form $\alpha = a + b\pi$ since we are working with curves whose $\mathbb{F}_p$ endomorphism rings are of the form $\mathcal{O} = \mathbb{Z}[\pi]$ and the action of the class group corresponds to $\mathbb{F}_p$-rational isogenies.

If we consider adding a $\Gamma(N)$-structure to the isogeny graph, then the vertices (E_0, P_0, Q_0), (E_1, P_1, Q_1), and (E_1, P, Q) are certainly all on the same component. Further, we notice not all principal ideals act trivially on these vertices.

Proposition 2.5. *Let $G(N)$ be an isogeny graph with $\Gamma(N)$-structure and vertex set $\mathbb{V}$ as in Definition 2.2. Then the subgroup of $\mathcal{I}_{(N)}$ that acts trivially on $\mathbb{V}$ is given by*

$$\mathcal{P}_{N,\pm 1} = \{(\alpha) = \alpha\mathcal{O} | (\alpha) \equiv \pm 1 \mod (N)\}.$$

Proof. Consider linearly independent $P, Q \in E[N]$. Suppose $(\alpha) \equiv 1 \mod (N)$. Then $(\alpha) = 1 + \beta N$ for some $\beta \in \mathcal{O}$. It follows that $\alpha P = P$ and $\alpha Q = Q$ since $[N]P = [N]Q = O_E$. Now suppose $\alpha \in \mathcal{O}$ such that $\alpha \mid_{E[N]} = 1$. For $\alpha \neq 1$, there exist $P \in E$ such that $\alpha P \neq P$. Then $\alpha - 1$ is an isogeny. We have that $E[N] \subseteq \ker(\alpha - 1)$, and so there exists an isogeny φ such that $\alpha - 1 = \varphi \circ [N] \implies \alpha \equiv 1 \mod (N)$. Similarly for $\alpha \equiv -1 \mod (N)$ by the equivalence relation in Definition 2.2, $(E, P, Q) \sim (E, -P, -Q)$ with isomorphism $[-1]$. □

We now give the main result of this paper. We will restrict ourselves to the CSIDH problem with elliptic curves E_0, E_1 with $\mathbb{F}_p$-rational endomorphism rings $\mathcal{O} = \mathbb{Z}[\pi]$.

Theorem 2.6. *Let N be prime with $N \mid p+1$ and $\{P_0, Q_0\}, \{P_1, Q_1\}$ be bases of $E_0[N], E_1[N]$ respectively along with an isogeny $\varphi : E_0 \to E_1$ such that $\varphi(P_0) = P_1, \varphi(Q_0) = Q_1$. Suppose we can find an isogeny $\psi : E_0 \to E_1$ with $\deg \psi = m$ coprime to N and $\psi(P_0) = P, \psi(Q_0) = Q$. Then there exists an endomorphism $\alpha : E_1 \to E_1$ of the form $\alpha = a + b\pi$ such that $\alpha(P) = P_1, \alpha(Q) = Q_1$.*

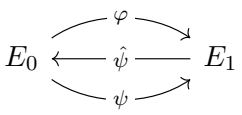

FIGURE 2. Vertices connected by an edge on an isogeny graph with no level structure.

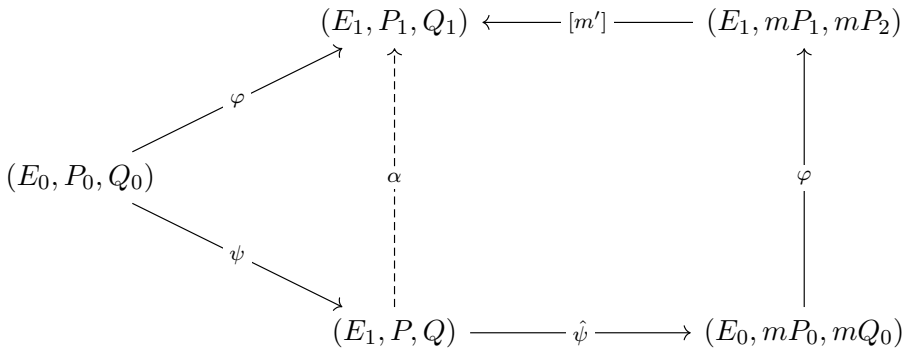

FIGURE 3. A subgraph of a $\Gamma(N)$ graph with $\deg \psi = m$.

Proof. Consider the map $\varphi \circ \hat{\psi}$ where $\hat{\psi}$ is the dual isogeny of ψ. This is certainly an endomorphism of E_1. In the isogeny graph with level structure, this map corresponds to the walk $E_1 \to E_0 \to E_1$ as seen in Figure 2. However, this is not the case when level structure is added as can be seen in Figure 3. We then have

$$\begin{aligned}\varphi \circ \hat{\psi}(P) &= \varphi \circ \hat{\psi} \circ \psi(P_0) \\ &= \varphi \circ [m](P_0) \\ &= [m]\varphi(P_0) \\ &= [m](P_1)\end{aligned}$$

where $[m]$ is the multiplication-by-m map. Since $(N, m) = 1$, there exists an m' such that $mm' \equiv 1 \pmod{N}$. Then we have $\alpha = [m'] \circ \varphi \circ \hat{\psi}$ and $\alpha(P) = P_1, \alpha(Q) = Q_1$. To see α is of the form $a + b\pi$ with $a, b \in \mathbb{Z}$, we observe that $[m'], \varphi$, and $\hat{\psi}$ are all rational and so α must also be rational. □

Remark 2.7. When working with ordinary curves as in [4, 7], the endomorphism α will not necessarily be of the form $\alpha = a + b\pi$ since we may not have $\mathcal{O} = \mathbb{Z}[\pi]$.

We emphasise the above only shows the existence of such an endomorphism and does not say anything about the difficulty in computing such an endomorphism. The problem of computing α is similar to the discrete log problem, but where the coefficient ring is $\mathcal{O}/(N)$ instead of the usual $\mathbb{Z}/N\mathbb{Z}$.

Definition 2.8. Let E/K be an elliptic curve with $\mathrm{char}(K) = p$ and N a positive integer with $(N, p) = 1$. The *Weil pairing* is a bilinear form

$$e_N : E[N] \times E[N] \to \mu_N$$

where μ_N denotes the multiplicative group of Nth roots of unity in $\overline{K}$.

Proposition 2.9. *The Weil pairing e_N satisfies the following properties.*

1. *Bilinear: For $P, Q, R \in E[N], e_N(P + Q, R) = e_N(P, R)e_N(Q, R)$ and $e_N(P, Q + R) = e_N(P, Q)e_N(P, R)$.*
2. *Alternating: For $P, Q \in E[N], e_N(P, Q) = e_N(Q, P)^{-1}$ and $e_N(P, P) = 1$.*
3. *Non-degenerate: For $P \in E[N]$, if $e_N(P, Q) = 1$ for all $Q \in E[N]$, then $P = O$.*

(4) *Galois-invariant: If E is defined over K, then for all $\sigma \in \mathrm{Gal}\,\overline{K}/K, e_N(\sigma(P), \sigma(Q)) = \sigma(e_N(P,Q))$.*
(5) *Compatible: If $P \in E[NN']$ and $Q \in E[N]$, then $e_{NN'}(P,Q) = e_N([N']P, Q)$.*

Proof. See [10, Proposition III.8.1]. □

An application of the Weil pairing is the MOV attack [6] which reduces the discrete log problem (DLP) on an elliptic curve E to the DLP in a multiplicative group in the field which E is defined over. The following algorithm is from [6] and E is defined over $\mathbb{F}_q$. Observe that

Algorithm 1 ([6, Algorithm 2])

Input: An element $P \in E[N]$ and $R \in \langle P \rangle$.

Output: An integer r such that $R = rP$.

Find $k \in \mathbb{Z}$ such that $E[N] \subseteq E(\mathbb{F}_{q^k})$.

Find $Q \in E[N]$ such that $e_N(P,Q)$ is a primitive Nth root of unity.

Compute $s = e_N(R,Q)$.

Compute the discrete log of s to the base $e_N(P,Q)$ in $\mathbb{F}_{q^k}$.

$s = e_N(R,Q) = e_N(rP,Q) = e_N(P,Q)^r$. The authors of [6] remark that Algorithm 1 does not provide a method for finding Q as required. As we will see below, this does not apply to our situation since N is prime and no extra points need to be computed. The idea is to pre-compute $e_N(P, \pi P)$ then apply Algorithm 1 once with input $P_1, \pi P$ and again with P_1, P to recover a, b respectively.

For a given basis P, Q of $E_1[N]$, we will assume P is not an eigenvector of π. If it is, we swap P and Q. This ensures that the Weil pairing $e_N(P, \pi P)$ will be an Nth root of unity. We know there exists an α as above by Theorem 2.6, and so we can find α by solving the DLP

$$\begin{aligned} e_N(P_1, \pi P) &= e_N(aP + b\pi P, \pi P) \\ &= e_N(P, \pi P)^a \end{aligned}$$

for the integer a. Similarly, we can solve

$$\begin{aligned} e_N(P, P_1) &= e_N(P, aP + b\pi P) \\ &= e_N(P, \pi P)^b \end{aligned}$$

for b and set $\alpha = a + b\pi$.

It is possible for both basis points to be eigenvectors of π. Since we have chosen N such that $N \mid p + 1$, we see the characteristic polynomial $p(X)$ of π modulo N is given by

$$p(X) = X^2 - 1 \pmod{N}$$

and so there exist eigenvectors of π in $E[N]$ with eigenvalues ± 1. Assume P, Q are such eigenvectors with $\pi P = P$ and $\pi Q = -Q$. We want to find a, b in the system

$$\begin{aligned} P_1 &= aP + bP = (a+b)P \\ Q_1 &= aP - bP = (a-b)P. \end{aligned}$$

If we let $c = a + b$, we can apply use the MOV algorithm on $P_1 = cP$ to solve for c. We use the same method to find $d = a - b$ where $Q_1 = dQ$ and use linear algebra to find a, b.

We will conclude by giving an algorithm of the above attack.

Algorithm 2 Solving CSIDH with $\Gamma(N)$ structure.

Input: $N \in \mathbb{Z}$ and $\Gamma(N)$ structures $(E_0, P_0, Q_0), (E_1, P_1, Q_1)$

Output: Ideal $\mathfrak{a}$ such that $[\mathfrak{a}] * (E_0, P_0, Q_0) = (E_1, P_1, Q_1)$.

Find an ideal $\mathfrak{b}$ such that $\varphi_{\mathfrak{b}} : E_0 \to E_1$.

Set $P \leftarrow \phi_{\mathfrak{b}}(P_0), Q \leftarrow \varphi_{\mathfrak{b}}(Q_0)$.

Solve for b in $e_N(P, P_1) = e_N(P, \pi P)^b$ where e_N is the Weil pairing.

Solve for a in $e_N(P_1, \pi P) = e_N(P, \pi P)^a$.

Set $\mathfrak{a} \leftarrow (a + b\pi)\mathfrak{b}$

return $\mathfrak{a}$

References

[1] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975.

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: an efficient post-quantum commutative group action. In *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*, pages 395–427. Springer, 2018.

[3] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[4] Jean-Marc Couveignes. Hard homogeneous spaces. *Cryptology ePrint Archive*, 2006.

[5] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4*, pages 19–34. Springer, 2011.

[6] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, 1991.

[7] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive*, 2006.

[8] Carl Siegel. Über die classenzahl quadratischer zahlkörper. *Acta Arithmetica*, 1(1):83–86, 1935.

[9] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[10] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.