Elliptic Curve Security

Zach Kellner

2024 Dec 9

Abstract

In the last few decades, mathematicians have become increasingly interested in elliptic curves, and cryptographers have become increasingly interested in digital signatures. As theoretical objects, both elliptic curves and digital signatures have numerous and wide-ranging applications in their own rights. Elliptic curves feature in the frontiers of number theory like Wiles-Fermat and of theoretical physics like String Theory. Digital signatures are keys necessary to privately identify ourselves in open channels for things like sensitive communications and financial transactions. In this paper, I explore their synthesis: the use of elliptic curves *for* digital signatures. I assume the reader has an undergraduate-level knowledge of mathematics, but minimal knowledge of cryptography. Cryptography, in brief, deals with methods of generating codes that are prohibitively difficult to decode without a certain bit of knowledge, a key. A very long key, just as with passwords, is in general more secure, but keys are used so often that they cannot be arbitrary large, due to excessive power consumption, limits in silicon area, minimal speed of communication, and so on. In this paper, I will first review the relevant basics of elliptic curves and their finite groups, and then I will demonstrate their utility for efficiently generating highly secure keys. My texts for reference were Blake (1999), Hellegouarch (2001), Menezes (1996), and Silverman (2009, 2015).

Definition 1. Define the *elliptic curve group* as $(\mathrm{E}(\mathbb{F}_q),\oplus)$, the group of rational points on a nonsingular E: $y^2 = x^3 + ax + b$ defined over $\mathbb{F}_q$ with the usual operation of taking two points to the negative (the mirror about the x-axis) of Bezout's guaranteed (possibly infinite, the identity) third collinear term.

Definitions 2. Define for shorthand *elliptic point multiplication* as

$$[m]P = \begin{cases} \infty, & m = 0 \\ [m-1]P \oplus P, & m > 0. \end{cases}$$

and analogously *elliptic point subtraction* as $Q - P := Q + (-P)$.

Definition 3. Define the *discrete logarithm*:

$$\log_g(h) := \min\{x \text{ such that } g^x = h, g, h \in G \text{ finite and abelian}\}.$$

Definition 4. Define the *Frobenius trace at q* as

$$t := q + 1 - |E(\mathbb{F}_q)|$$

for some prime power q.

Definition 5. Define the q^{th} *power frobenius map* on E defined over $\mathbb{F}_q$ as the group endomorphism

$$\varphi : \begin{cases} E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q) \\ (x, y) \mapsto (x^q, y^q), \\ \infty \mapsto \infty. \end{cases}$$

Proposition 6. $\varphi^2 - [t]\varphi + [q] = [0]$

Proof. This is equivalent to having $\forall P = (x, y)$ that

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \infty,$$

which is easily verified with Fermat's Little Theorem and Definition 4. □

Proposition 7. If A is an abelian group and $d : A \to \mathbb{Z}$ is a positive definite quadratic form then $\forall \psi, \phi \in A$ one has the relation

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}.$$

Proof. This is just a form of Cauchy–Schwarz. Let

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

be the bilinear form associated with d. Since d is positive definite, we have $\forall m, n \in \mathbb{Z}$ that

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi).$$

So when $m = -L(\psi, \phi)$ and $n = 2d(\psi)$,

$$0 \leq d(\psi)\big(4d(\phi)d(\psi) - L(\psi, \phi)^2\big).$$

□

Theorem 8 (Hasse, 1933)**.**

$$t \leq 2\sqrt{q}.$$

Proof. Note $P \in E(\mathbb{F}_q) \Leftrightarrow \varphi(P) = P$. Futhermore, the separability of $1 - \varphi$ gives that $|E(\mathbb{F}_q)| = |\ker(1 - \varphi)| = \deg(1 - \varphi)$. So using Proposition 7 and the fact $\deg(\varphi) = q$, one has the bound $||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$. □

Definitions 9 (Cryptographic terminology)**.** A *key* is a string k of symbols known privately but not publicly. *Plaintext* is a string of symbols intended to be communicated. *Encryption* is a key-dependent function mapping a plaintext to a string of symbols called the *ciphertext*. An *encryption scheme* $\mathcal{E}$ is an encryption in terms of an arbitrary key. *Decryption* is the inverse map of encryption. One's *adversary* is a hypothetical person who knows one's encryption scheme and ciphertext but not one's key or plaintext. An adversary *breaks* an encryption scheme by finding the decryption. *Security* is the estimated length of time it would take an encryption scheme to be broken. The *Discrete Logarithm Problem* (DLP) is the fact that no algorithm has been discovered which calculates $\log_g(h)$ in time which is polynomial in the number of digits of $|G|$.

Definition 10. The *ECDLP* (elliptic curve discrete logarithm problem) is the problem of finding the integer m such that, given some $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$, $Q = [m]P$.

Definitions 11. A *baby step* is $R_b := Q - [b]P$ for some nonnegative integer $b \leq \sqrt{n}$. Likewise a *giant step* is $S_a := [a]\Big([\lceil \sqrt{n} \rceil]P\Big)$ for some $a \leq \sqrt{n}$.

Definition 12. *BSGS* (baby-step giant-step) is the following algorithm applicable to any $E(\mathbb{F}_q)$ of size n: tabulate all baby steps, then compute giant steps until reaching a' such that $S_{a'} = R_{b'}$ for some $(b', R_{b'})$ in the table.

Proposition 13. BSGS solves the ECDLP.

Proof. The a', b', n solve for m by the Euclidean algorithm:

$$\begin{aligned} & S_{a'} = R_{b'} \\ \Leftrightarrow\ & Q - [b']P = [a']\Big([\lceil \sqrt{n} \rceil]P\Big) \\ \Leftrightarrow\ & Q = [b']P + [a']\Big([\lceil \sqrt{n} \rceil]P\Big) \\ \Leftrightarrow\ & m = \lceil \sqrt{n} \rceil a' + b'. \end{aligned}$$

□

Corollary 14. BSGS has a complexity of $\mathcal{O}(\sqrt{n})$.

Definition 15. Define the *sub-exponential function* as

$$L_p(v, c) := \exp(c(\ln p)^v (\ln \ln p)^{1-v})$$

for $0 < v < 1$.

Proposition 16. If breaking an $\mathcal{E}$ reduces to solving the DLP in $\mathrm{E}(\mathbb{F}_q)$, then $\mathcal{E}$ is significantly more secure than a scheme which is broken by solving the DLP in $\mathbb{F}_p^*$ for $p \approx |\mathrm{E}(\mathbb{F}_q)|$.

Proof. The BSGS method, by Corollary 14, is of complexity $\mathcal{O}(n) = e^n$ for $n = \lceil \log_2(q) \rceil$. It suffices to show that the DLP in $\mathbb{F}_p^*$ can be solved in sub-exponential time. A quick search of modern classical algorithms gives the general number field sieve an L-complexity of $v = \frac{1}{3}, c = (\frac{8}{3})^{2/3}$ (see: Carl Pomerance's 1996 paper "A Tale of Two Sieves" for more). Using $N = \lceil \log_2(p) \rceil$, equating key complexity gives

$$n = \frac{2cN^{1/3}(\ln(N \ln(2))^{2/3}}{(\ln 2)^{2/3}}.$$

Note, e.g., plugging in conventional values of $N = 2^{11}$ and 2^{12} give $n = 173$ and 313, respectively. This is a key reduction of an entire order of magnitude! □

Remark 17 (present-day cryptography)**.** The BSGS is the fastest known algorithm for a general $E(\mathbb{F}_q)$. There are minor adjustments that reduce computer memory requirements (see: Pollard's "rho" and "lambda" attacks), but the speed/complexity remains exponential. I will now review all three of the known special cases of $E(\mathbb{F}_q)$ which are uniquely susceptible to subexponential attacks and how to choose $E(\mathbb{F}_q)$ such that the attacks do not apply. (The matter of picking a "strong" $E(\mathbb{F}_q)$ is analogous to classical DLP matter of the so-called strength or safety of primes used in RSA.)

Definition 18 (Attack 1)**.** Define the *Pohlig-Hellman (PH) attack* as solving the DLP on a finite abelian group by breaking the group into subgroups of prime order, solving those by brute force, then applying the Chinese Remainder Theorem (CRT). That is, if p divides $|G|$, and $Q = [m]P$, then the DLP restricts to solving

$$Q' = [n']Q = [m_0]([n']P) = [m_0]P',$$

where $n' = |G|/p^c$ and p^c is the p-adic valuation of $|G|$. Once $m \equiv m_i \pmod{p^i}$ are known $\forall i$, then since $m = m_i + \lambda p^i$ for some integer $\lambda \in \mathbb{Z}$, $\exists R, S$ such that

$$R = (Q - [m_i]P) = [\lambda]([p^i]P) = [\lambda]S,$$

$|S| = |G|/p^i$. Let $s' = s/p^{c-i-1}$. Then, $\lambda \pmod{p}$ is obtained by solving

$$R' = [s']R = [\lambda_0]([s']S) = [\lambda_0]S',$$

where S' is a point of order p. Iterating this determines $m \pmod{p^c}$ for all prime divisors p of n, so then CRT applies.

Definition 19. Define the *Weil pairing* as a map

$$e : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of the mth roots of unity.

Definition 20 (Attack 2)**.** Define the *MOV attack* as the following reduction of the ECDLP to the DLP: if Q is linearly independent of P (so $e(P, Q) \neq 1$) then $e(P, Q)$ and $e(xP, Q) = e(P, Q)^x$ can be computed; both are elements of a finite field and are m-th roots of unity.

Definition 21. Define an elliptic curve as *anomalous* if it has a Frobenius trace of 1.

Definitions 22. If E takes values over the p-adics $\mathbb{Q}_p$, define $E_1(\mathbb{Q}_p)$ as the group of points of $E(\mathbb{Q}_p)$ which reduce to zero modulo p, and define $E_0(\mathbb{Q}_p)$ as the set of points in $E(\mathbb{Q}_p)$ which reduce modulo p to an element of $E(\mathbb{F}_p)$.

Proposition 23 (Attack 3)**.** If E is anomalous then the ECDLP can be solved in linear time.

Proof. Note

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to E(\mathbb{F}_p) \to 0.$$

So if $x \in E_0(\mathbb{Q}_p)$ and y is a multiple of $|E(\mathbb{F}_p)|$, then $xy \in E_1(\mathbb{Q}_p)$. Furthermore, if $|E(\mathbb{F}_p)| = |\mathbb{F}_p^+|$, then

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{F}_p^+.$$

So

$$Q - [m]P = R \in E_1(\mathbb{Q}_p).$$

Note that

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong E(\mathbb{F}_p) \quad \text{and} \quad E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{F}_p^+.$$

But $|E(\mathbb{F}_p)| = |\mathbb{F}_p^+| = p$, so

$$[p]Q - [m]([p]P) = [p]R \in E_2(\mathbb{Q}_p).$$

Since it takes $\mathcal{O}(n) = \log p$ time to compute $[p]P$ and $[p]Q$, it takes $\mathcal{O}(n) = p$ time to find m.

□

Corollary 24. By taking the negation of the necessary conditions for all three known attacks upon $E(\mathbb{F}_p)$, according to all known present technological and mathematical capabilities, the ECDLP is unbreakable (i.e. breakable, but at the speed of BSGS, which can easily be made to require a timescale beyond estimates of the heat death of the universe). More precisely, we only need three (easy to check) conditions:

1. $E(\mathbb{F}_p)$ has a large subgroup
2. E is not anomalous
3. q is of large order

Remark 25. The "large" of Corollary 24 is relative to one's desired complexity, but by Proposition 16, the use of elliptic curves reduces the length needed for a given complexity by an order of magnitude. This makes them the superior choice for group generation, and supports their increasing use in digital signature key generation.

References

[1] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone (1996), *Handbook of Applied Cryptography*, CRC Press.

[2] I.F. Blake, G. Seroussi, and N.P. Smart (1999) *Elliptic Curves in Cryptography*, Cambridge University Press.

[3] Joseph H. Silverman (2009) *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd ed.

[4] Joseph H. Silverman and John T. Tate (2015), *Rational Points on Elliptic Curves*, Springer.

[5] Yves Hellegouarch (2001), *Invitation to the Mathematics of Fermat-Wiles* Academic Press.