Elliptic Curve Cryptography

Patrick Maedgen

Texas A&M University

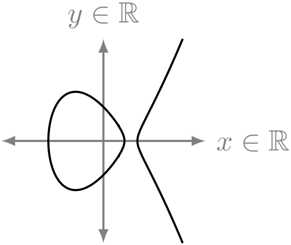
November 2019

Outline

- What is an elliptic curve?
- Group law for elliptic curves
- The ECDLP
- Using the collision algorithm to solve the ECDLP
- Advantages of using elliptic curves
- Example using Diffie-Hellman

What is an Elliptic Curve?

- $y^2 = x^3 + ax + b$
  - Where the determinant $4a^3 + 27b^2 \neq 0$
  - This is known as the *Weierstrass normal form*



$y^2 = x^3 - 2x + 1$ over $\mathbb{R}$

What is an Elliptic Curve?

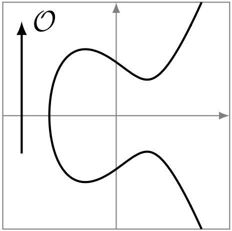
- We also need a "point at infinity" denoted as $\mathcal{O}$
- So our definition becomes $\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{\mathcal{O}\}$
- To be able to use these curves we need to define the Group Law for them

Group Law

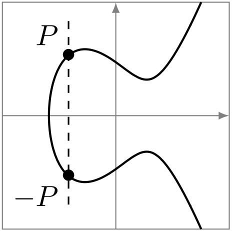
- A group is a type of set with a defined binary operation, in this case addition
- There are 5 parameters that our addition operator must satisfy for a set G to be a group
  - **Closure:** $a, b \in G \longrightarrow a + b \in G$
  - **Associativity:** $(a + b) + c = a + (b + c)$
  - **An Identity Element:** $a + 0 = a$
  - **Every Element has an Inverse:** $a + b = 0,\ a = -b$
  - **Commutativity:** $a + b = b + a$
- This fifth requirement, Commutativity, makes an abelian group

Group Law for Elliptic Curves

- We can define a group over elliptic curves which would allow us to use the $+$ operator on points
- the identity element is the point at infinity, $\mathcal{O}$
- The inverse of a point is that point reflected across the x-axis
  - If $P = (x, y)$ is a point on the curve then the inverse of P is $-P = (x, -y)$



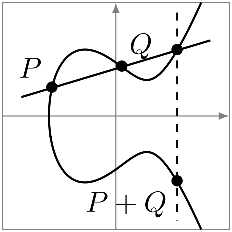
Neutral element $\mathcal{O}$



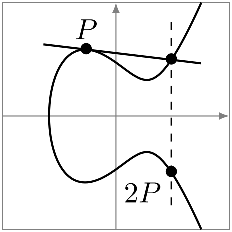
Inverse element $-P$

Point Addition

- Addition of points is defined as $P + Q = -R$ where P, Q, R are all aligned points on the curve
- Algebraic addition:
  - if $P \neq Q, \ -Q$: $\lambda = \frac{y_P - y_Q}{x_P - x_Q}$
  - if $P = Q$: $\lambda = \frac{3x_P^2 + a}{2y_P}$
  - $x_R = \lambda^2 - x_P - x_Q$
  - $y_R = y_P + \lambda(x_R - x_P) = y_Q + \lambda(x_R - x_Q)$



Addition $P + Q$



Doubling $P + P$

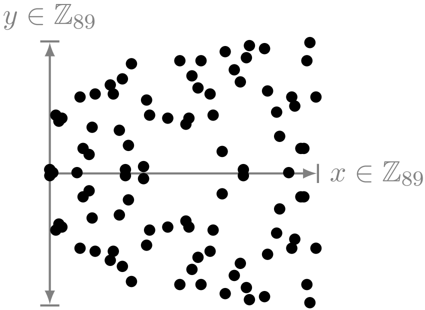
Scalar Multiplication

- Now that we know how to add points together, what if we wanted to do repeated addition of the same point?
- $nP = Q$
- Q must be a point on the curve because of group closure
- If we know Q and n, can we find P? If we know Q and P, can we find n?

Curves Over Finite Fields

- Need to restrict the curves over a finite field $\mathbb{F}_p$ for some prime p
- The definition of the curve becomes: $\{(x, y) \in (\mathbb{F}_p)^2 \mid y^2 \equiv x^3 + ax + b \ (mod\ p),$ $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)\} \cup \{\mathcal{O}\}$
- Adding points is similar to before but now the points must be connected by some line mod p

Curves Over Finite Fields



$y^2 = x^3 - 2x + 1$ over $\mathbb{Z}_{89}$

Elliptic Curve Discrete Logarithm Problem

- Core of Elliptic Curve Cryptography
- Based on the discrete logarithm problem from other cryptosystems
- $nP = Q$ is analogous to, but harder to solve than $g^x \equiv h\ (mod\ p)$

Solving the ECDLP with the Collision Algorithm

- Given an elliptic curve over a finite field $E(\mathbb{F}_p)$, we want to solve $Q = nP$, given P and Q
- Choose two sets of random integers between 1 and p
  - $j_1,\ j_2, \ldots,\ j_r$ and $k_1,\ k_2, \ldots,\ k_r$
- Create two lists of points
  - List 1: $j_1P,\ j_2P, \ldots,\ j_rP$
  - List 2: $k_1P + Q,\ k_2P + Q, \ldots,\ k_rP + Q$

Collision Algorithm

- As soon as one match is found between the two lists we are done
- If $j_u P = k_v P + Q$, then $Q = (j_u - k_v)P$
- So, $n = j_u - k_v$

Advantages of Elliptic Curves

- The ECDLP is more secure than the DLP
- Can acheive the same level of security with a smaller key

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA[21]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Elliptic Diffie-Hellman Key Exchange

- Alice wants to send Bob a secret value, but doesn't want Eve to intercept it
- Alice and Bob will choose a particular curve $E(\mathbb{F}_p)$ and a point $P \in E(\mathbb{F}_p)$
- They will each choose an integer and compute Q
  - Alice: $Q_A = n_A P$
  - Bob: $Q_B = n_B P$

Elliptic Diffie-Hellman Key Exchange

- Alice and Bob exchange their respective Qs
- They multiply that by their own secret integer, now they share a secret value
- $n_A Q_B = n_A n_B P = n_B n_A P = n_B Q_A$

Thanks To

- Changningphaabi Namoijam (Texas A&M University)
- Kari Eifler, Taylor Brysiewicz, and Anne Shiu (Texas A&M University)

References

- Corbellini, Andrea. "Elliptic Curve Cryptography: a Introduction." Andrea Corbellini, 17 May 2015, andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/.
- Eichlseder, Maria. "Elliptic Curve Group Operations." TikZ for Cryptographers, June 2016, www.iacr.org/authors/tikz/.
- Eichlseder, Maria. "Elliptic Curves over R and Fp." TikZ for Cryptographers, June 2016, www.iacr.org/authors/tikz/.
- "Elliptic Curves and Cryptography." An Introduction to Mathematical Cryptography, by Jeffrey Hoffstein et al., Springer, 2010, pp. 299–360.