Hardness of Supersingular Isogeny Graph-based Cryptography

WAM: Uhlenbeck Lecture #2

Kristin Lauter

Microsoft Research

Course Goals

- Goal: Convey context and status of

  Post-Quantum Cryptography (PQC)

  - What is PQC?
  - Current Proposals for PQC
  - Familiarity with algorithms and running times
  - Introduce Supersingular Isogeny Graphs (SIG)
  - Introduce Ring-Learning With Errors (RLWE)

Course Outline

- Day 1: Supersingular Isogeny Graphs—definitions and applications
- Day 2: Hard Problems—number theory attacks
- Day 3: RLWE—motivation and definition of schemes
- Day 4: Attacks on Ring-LWE for special rings.

Yesterday

- Cryptography intro
- Motivation for PQC and NIST competition
- Cryptographic Hash functions
- Defined Supersingular Isogeny Graphs
  - Graphs
  - Elliptic Curves
  - J-invariants (labels)
  - Isogenies (maps between curves = edges)
- Review session:
  - Computed a 2-isogeny from a 2-torsion point

Graph of supersingular elliptic curves modulo p with isogeny edges (Pizer graphs)

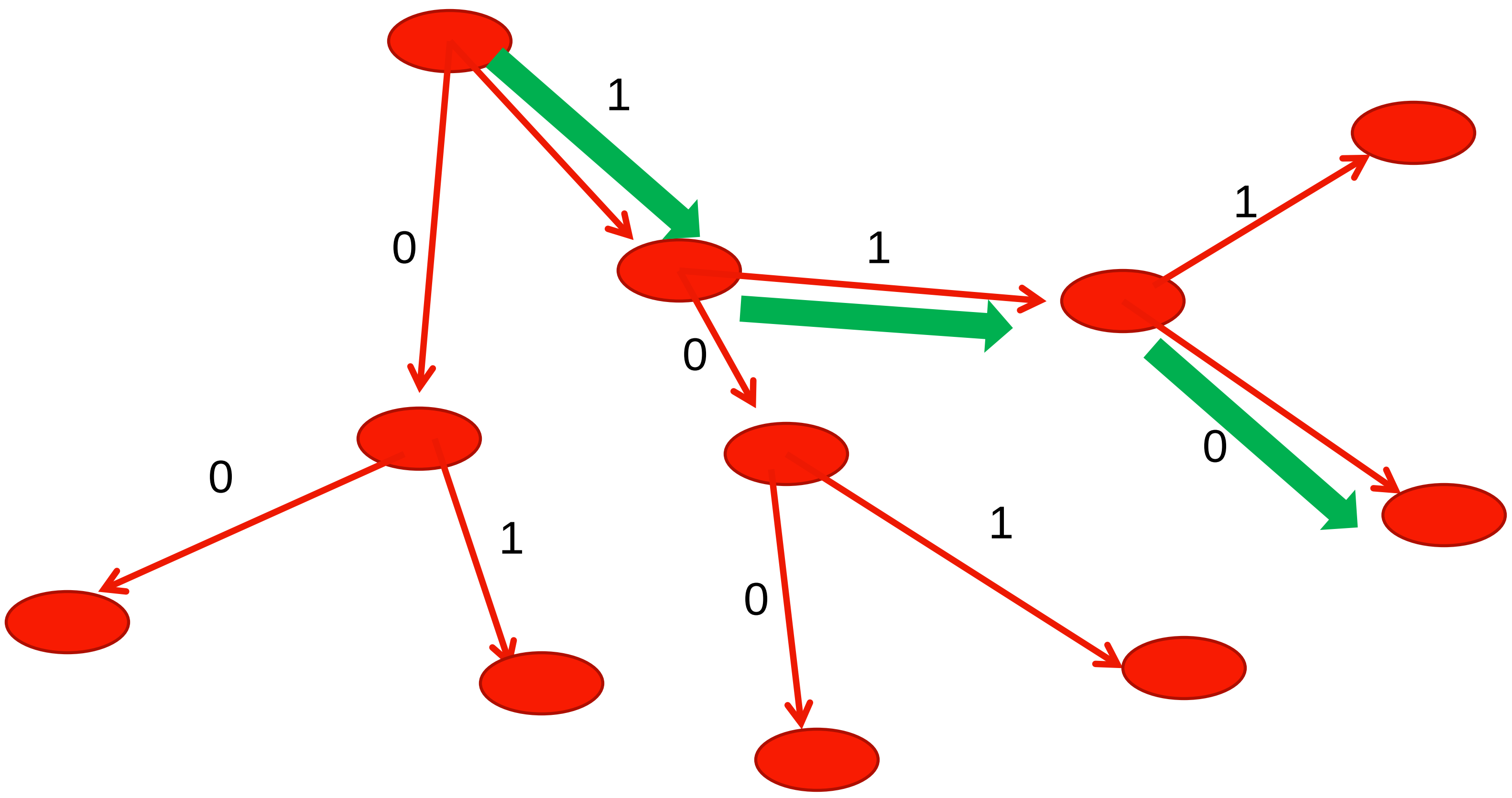
- Vertices: supersingular elliptic curves mod p
  - Curves are defined over $GF(p^2)$ (or $GF(p)$)
- Labeled by j-invariants
  - $E_1 : y^2 = x^3 + ax + b$
  - $j(E_1)= 1728*4a^3/(4a^3+27b^2)$
- Edges: ℓ-Isogenies between elliptic curves
  - ℓ = degree, ℓ = size of the kernel

Collision resistance

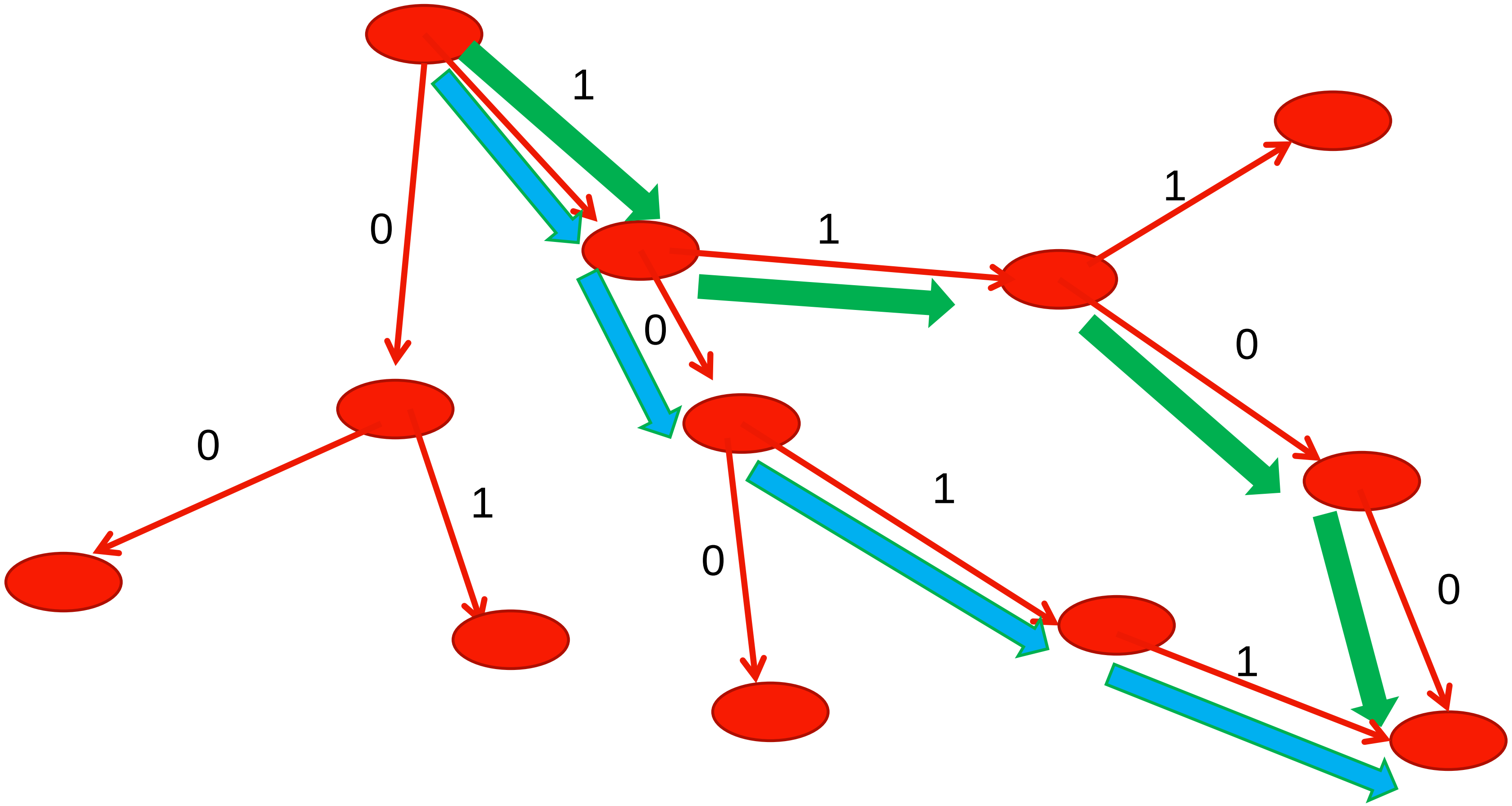
Finding collisions reduces to finding isogenies between elliptic curves:

- Finding a collision→ finding 2 distinct paths between any 2 vertices (or a cycle)
- Finding a pre-image→finding any path between 2 *given* vertices
- $O(\sqrt{p})$ birthday attack to find a collision

Walk on a graph: 110



Colliding walks: 1100 and 1011



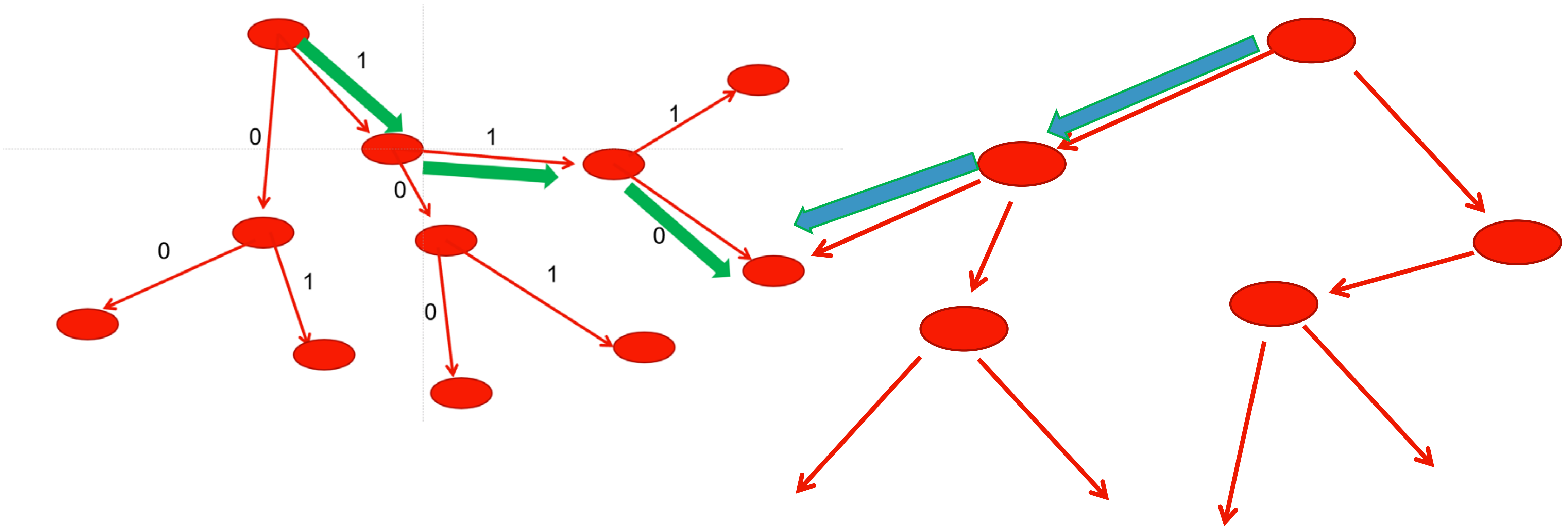
Hard Problems ?

- **Problem 1**. Produce a pair of supersingular elliptic curves, E_1 and E_2, and two distinct isogenies of degree ℓ^n between them.
- **Problem 2**. Given E, a supersingular elliptic curve, find an endomorphism $f : E \rightarrow E$ of degree ℓ^{2n} , not the multiplication by ℓ^n map.
- **Problem 3**. Given two supersingular elliptic curves, find an isogeny of degree ℓ^n between them.

Hardness

- Generic square root attacks are best known classical attacks
- Ensure large girth by putting conditions on the splitting behavior of p in various imaginary quadratic extensions

Generic Square Root Attack



Supersingular

- End(E)={φ: E→E}
- An elliptic curve is supersingular modulo p if its endomorphism ring is a maximal order in a quaternion algebra, we say that E is supersingular.
- Example:
  - If $p = 3 \bmod 4$, $E_0: y^2 = x^3 + x$ is supersingular
  - j-invariant $j = 1728$.
  - End(E) = maximal order $O_0 = Z\{1, i, (1+k)/2, (i+j)/2\}$

Quaternion Algebras

- Definite quaternion algebra ramified at p & infinity: $B_{p,\infty}$
- basis $<1,i,j,ij>$ for $B_{p,\infty}$
- $i^2 = a$, $j^2 = b$, $ij = -ji$

- If $p = 3 \pmod 4$ then $(a,b) = (-p,-1)$
- Maximal order: $O = <1, j, (j+k)/2, (1+i)/2>$

- Norm map:
- $N(c + dj + fi + gij) = c^2 + d^2 + p(f^2 + g^2)$

Deuring's correspondence

- Deuring:
- supersingular elliptic curves over F_p (up to isomorphism)

$$\longleftrightarrow$$

- maximal orders of $B_{p,\infty}$ (up to conjugation)

- Deuring's correspondence associates to a supersingular invariant j a maximal order O such that O = End(E).
- Any left ideal I of O corresponds to an isogeny
- $\varphi_I : E \to E_I$ with kernel $\ker\varphi_I = \{P \in E \mid \alpha(P) = 0, \forall\alpha \in I\}$.
- 1-1 correspondence if degree of φ_I is coprime to p.
- the right order of I, $O_R(I)$ = endomorphism ring of E_I.

Deuring's correspondence

Deuring's correspondence:

- isomorphism of quaternion algebras
- $\theta : B_{p,\infty} \to \mathrm{End}(E_0) \otimes \mathbb{Q}$ sending $(1,i,j,k)$ to $(1,\varphi,\pi,\pi\varphi)$
  - $\pi : (x,y) \to (x^p,y^p)$ is the Frobenius endomorphism
  - $\varphi : (x,y) \to (-x,\iota y)$ with $\iota^2 = -1$.
- Norm map on quaternions corresponds to degree map on endomorphisms!

Number theoretic algorithms to attack

- $p \sim 2^{256}$
- Given E_1, E_2, supersingular elliptic curves over $F_p{}^2$
- Compute endomorphism rings as maximal orders in $B_{p,\infty}$
- Use path-finding algorithm on maximal orders in the quaternion algebra [Kohel-Lauter-Petit-Tignol]

- But! Computing endomorphism rings is hard!
- Can compute representation numbers for number of elements of norm n
- Compare with # of isogenies of various degrees

Applications of SIG

- Proposed as basis for other cryptosystems:
  - Key exchange: Jao-De Feo 2011

    (adds transmitting torsion images)
  - Encryption: De Feo-Jao-Plut, 2014
  - Signatures: Galbraith-Petit-Silva 2016

Key Exchange

$$
\begin{tikzcd}
 & E_A \arrow[dr, "\phi'_A"] & \\
E \arrow[ur, "\phi_A"'] \arrow[dr, "\phi_B"] & & E_{AB} \\
 & E_B \arrow[ur, "\phi'_B"'] &
\end{tikzcd}
$$

E: supersingular elliptic curve over GF(p^2)

$p = \ell_A^m \ \ell_B^n + 1$

ℓ_A and ℓ_B prime ($\ell_A = 2$ and $\ell_B = 3$)

A and B want to exchange a key.

Public parameters:

A picks P_A, Q_A such that $< P_A, Q_A > = E[\ell_A^m]$

B picks P_B, Q_B such that $< P_B, Q_B > = E[\ell_B^n]$

Secret parameters:

A picks two random integers m_A, n_A

A uses Velu's formulas to compute the isogeny

$$\varphi_A : E \longrightarrow E_A := E/ < m_A P_A + n_A Q_A >$$

B picks two random integers m_B, n_B

B uses Velu's formulas to compute the isogeny

$$\varphi_B : E \longrightarrow E_B := E/ < m_B P_B + n_B Q_B >$$

A and B have constructed the following diagram.

$$\begin{tikzcd} & E_A \\ E \arrow[ur, "\phi_A"'] \arrow[dr, "\phi_B"] & \\ & E_B \end{tikzcd}$$

To complete the diamond, A and B exchange information:

A computes the points $\varphi_A(P_B)$ and $\varphi_A(Q_B)$ and sends $\{\varphi_A(P_B), \varphi_A(Q_B), E_A\}$ to B

B computes the points $\varphi_B(P_A)$ and $\varphi_B(Q_A)$ and sends $\{\varphi_B(P_A), \varphi_B(Q_A), E_B\}$ to A

$$
\begin{tikzcd}
 & E_A \arrow[dr, "\phi'_A"] & \\
E \arrow[ur, "\phi_A"'] \arrow[dr, "\phi_B"] & & E_{AB} \\
 & E_B \arrow[ur, "\phi'_B"'] &
\end{tikzcd}
$$

To obtain E_{AB}, quotient EA by
The j-invariant of the curve E_{AB} is the shared secret.

Security of Key Exchange relies on CGL path-finding problem

- If you can find the path between E and E_A, then you can break the Key Exchange.

Reduction result from WIN4 project 2017: Costache-Feigon-Lauter-Massierer-Puskas:

Problem 1. *(Supersingular Computational Diffie–Hellman (SSCDH)): Let* E, E_A, E_B, E_{AB}, P_A, Q_A, P_B, Q_B *be as above.*

Let ϕ_A *be an isogeny from* E *to* E_A *whose kernel is equal to* $\langle [m_A]P_A + [n_A]Q_A \rangle$, *and let* ϕ_B *be an isogeny from* E *to* E_B *whose kernel is equal to* $\langle [m_B]P_B + [n_B]Q_B \rangle$, *where* m_A,n_A *(respectively* m_B,n_B*) are integers chosen at random between* 0 *and* ℓ_A^m *(respectively* ℓ_B^n*), and not both divisible by* ℓ_A *(resp.* ℓ_B*).*

Given the curves E_A, E_B *and the points* $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$, *find the* j*-invariant of*

$$E_{AB} \cong E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle;$$

see diagram (2).

Problem 2. *(Path-finding [CGL06]) Let* p *and* ℓ *be distinct prime numbers, and* E_0 *and* E_1 *two supersingular elliptic curves over* $\mathbb{F}_{p^2}$. *Find* $k \in \mathbb{N}$ *and a path of length* k *in the* ℓ*-isogeny graph corresponding to a composition of* k ℓ*-isogenies which lead from* E_0 *to* E_1.

Theorem 3.2. *Problem 1 is no harder than Problem 2.*

Take-away:

- Uncertain timing for building quantum computers at scale
- Need to try to break proposals for new cryptosystems using ***both classical and quantum algorithms***
- ***We need more mathematicians working on mathematical problems in cryptography and applications!***

Back-up slides

Classical security for RSA and ECC

RSA cryptosystems (~1975)

Security based on hardness of factoring n=p*q

(n) = (p) (q) = (p 1)(q 1) = n - (p + q -1)

Choose an integer e such that gcd(e, (n)) = 1

Determine d as d e^{1} (mod (n));

Public key (n, *e)*

Private key (n,d)

p, q, and (n) secret
(because they can be used to calculate d)

Encryption

$$c \equiv m^e \pmod{n}$$

Decryption

$$m \equiv c^d \pmod{n}$$

Diffie-Hellman Key Exchange

Given a cyclic group G generated by g

Alice picks random a

Bob picks random b

Alice sends g^a $\longrightarrow$

$\longleftarrow$ Bob sends g^b

Secret :

$g^{ab} = (g^b)^a = (g^a)^b$

Elliptic Curve Cryptography

- Elliptic Curve Cryptography (ECC) is an alternative to RSA and Diffie-Hellman, primarily signatures and key exchange
- Proposed in 1985 (vs. 1975 for RSA) by Koblitz and Miller
- Security is based on a hard mathematical problem different than factoring ECDLP
- ECC 25^{th} anniversary conference October 2010 hosted at MSR Redmond
- *Pairing-based cryptography* currently entirely on pairings on elliptic curves

Elliptic CURVE Groups

- Group of points (x, y) on an elliptic curve,

$$y^2 = x^3 + a x + b,$$

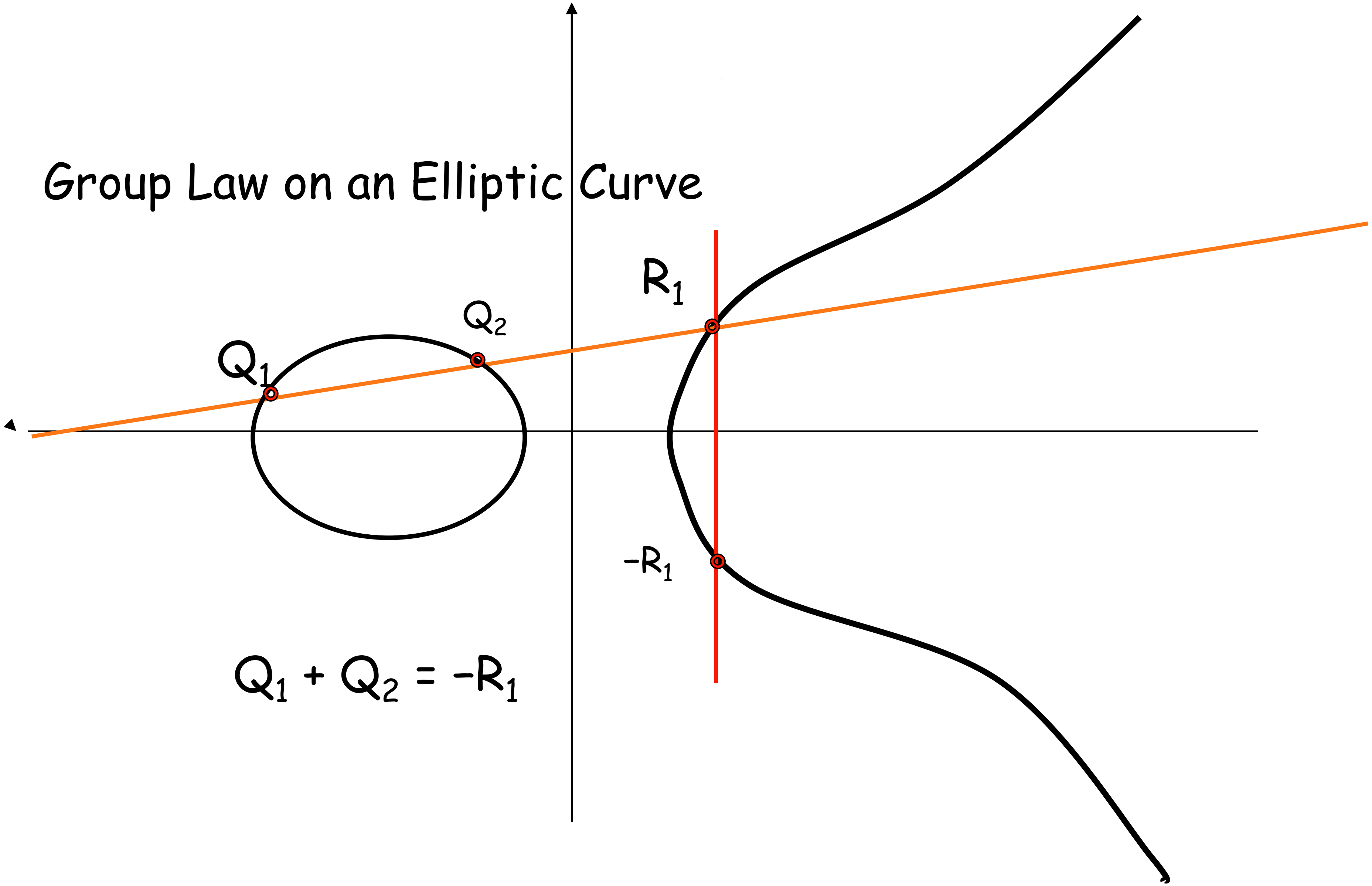
Over a field of minimum size: 256-bits

(short Weierstrass form, characteristic not 2 or 3)

Identity in the group is the "point at infinity"

Group law computed via "chord and tangent method"

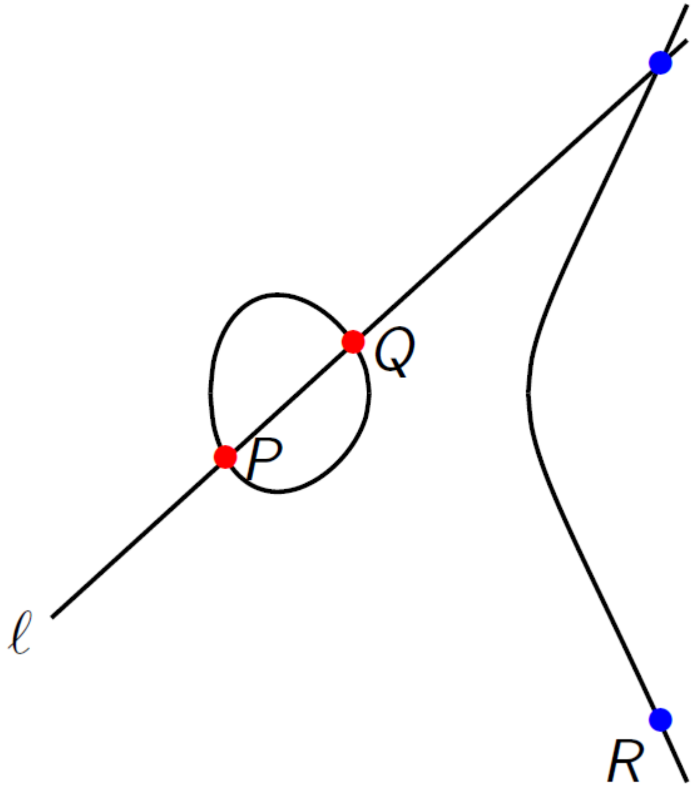
Group Law on an Elliptic Curve



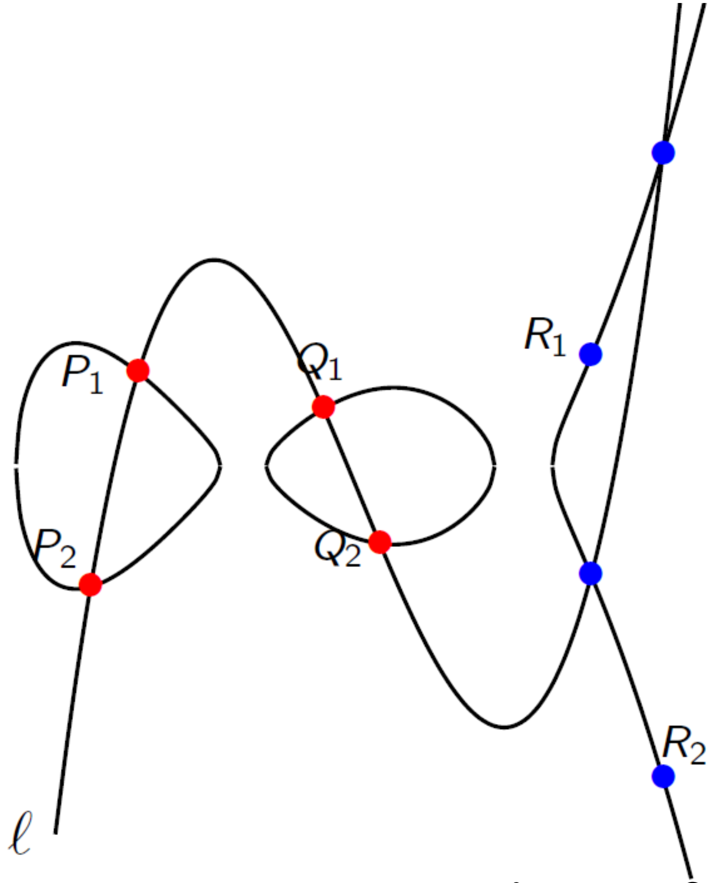
$$Q_1 + Q_2 = -R_1$$

Genus 2 Jacobians

$y^2 = x^3 + a_2x^2 + a_1x + a_0$



$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$



How to add pairs of points?

$\#E(\mathbf{F}_p) \approx p$

$\#\mathrm{Jac}_C(\mathbf{F}_p) \approx p^2$

RSA Security

- Security based on hardness of factoring n=p*q
  - p and q have equal size
- Otherwise: Elliptic curve factoring method finds factors in time proportional to the size of the factor (H. Lenstra, `85)
- Quadratic Sieve (Fermat, Kraitchik, Lehmer-Powers, Pomerance)
- Number field sieve (NFS) runs in subexponential time

$$O(e^{c\,(\log n)^{1/3}\,(\log \log n)^{2/3}})$$

c=1.526… Special NFS;

c=1.92… General NFS

Pollard `88, Lenstra-Lenstra-Manasse `90, Coppersmith `93,

Discrete logarithm problem in (Z/pZ)*

- Square-root algorithms:
  - Baby-Step-Giant-Step (Shanks `71)
  - Pollard rho (Pollard, `78)
  - Pohlig-Hellman, `78
- Subexponential:
  - Index calculus (Adleman, `79)
- Recent significant breakthroughs, improving the exponent in subexponential algorithms for DLP to ¼ for small characteristic:
  - Function Field Sieve (Joux 2013)

Elliptic Curve Cryptography

- Menezes–Okamoto–Vanstone (MOV) attack `93:
  - supersingular elliptic curves
- Semaev, Satoh, Smart `98-`99 (Trace 1)
- Generic square-root algorithms:
  - Baby-Step Giant-Step, Pollard's rho
- No generic, classical sub-exponential algorithm known