Elliptic Curve Cryptography and Applications

Kristin Lauter
Microsoft Research, Redmond
SIAM Annual Meeting
July 9, 2012

Public Key Cryptography

- 1. Key exchange: two parties agree on a common secret using only publicly exchanged information
- 2. Signature schemes: allows parties to authenticate themselves
- 3. Encryption: preserve confidentiality of data

- Examples of public key cryptosystems:
  RSA, Diffie-Hellman, ECDH, DSA, ECDSA

Applications:

- Secure browser sessions (https: SSL/TLS)
- Signed, encrypted email (S/MIME)
- Virtual private networking (IPSec)
- Authentication (X.509 certificates)
- …

Diffie-Hellman Key Exchange

Given a cyclic group G generated by g

Alice picks random a

Bob picks random b

Alice sends g^a →

← Bob sends g^b

Secret :

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

Problem:

- Public key operations are computationally expensive compared to symmetric key (block ciphers, stream ciphers, AES)
- Public keys can be long: currently in use 2048-bit RSA up to 16,000-bit keys
- Issues of power, bandwidth, and time

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)
- Security is based on a hard mathematical problem different than factoring ECDLP
- ECC 25th 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,

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

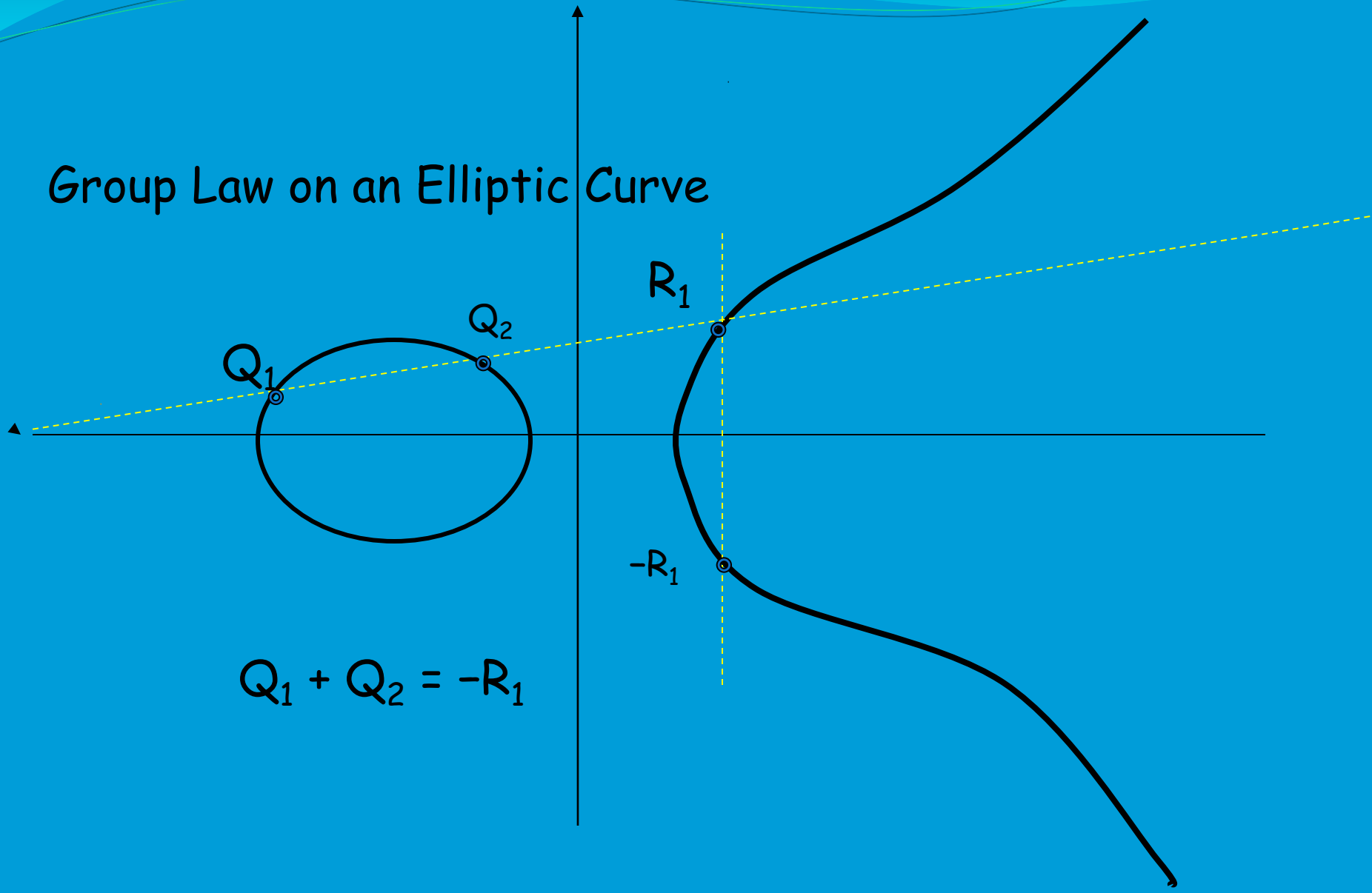
Over a field of minimum size: 256-bits

(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



$$Q_1 + Q_2 = -R_1$$

Another group for DLP

Jacobians of hyperelliptic curves

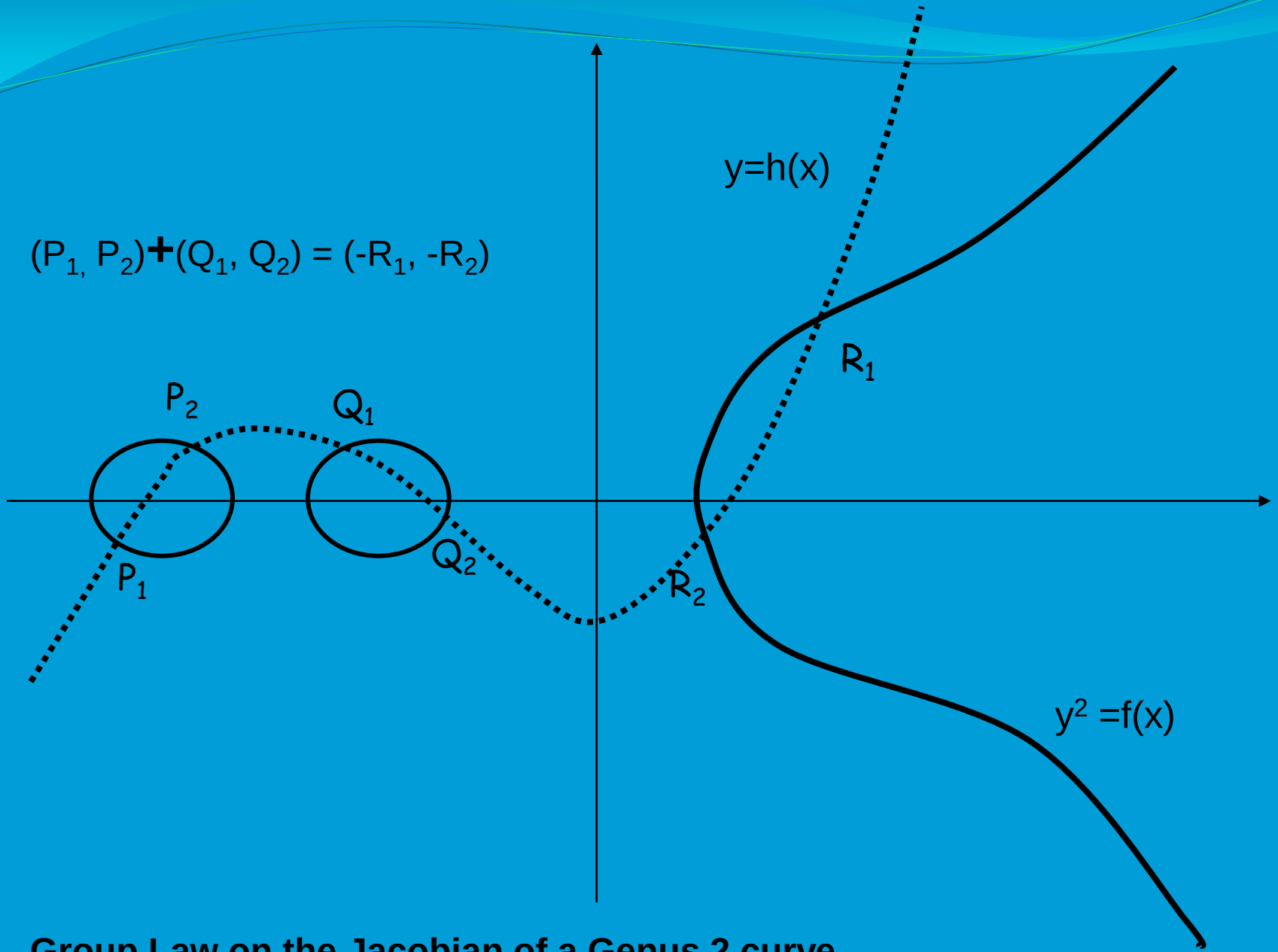
- For genus 2, affine model of curve

C: $y^2 = f(x)$, degree $f = 5$ or 6

- Elements of the Jacobian J(C)

represented by pairs of points on C

- Mumford representation for elements
- Efficient group law: Cantor's algorithm



Group Law on the Jacobian of a Genus 2 curve

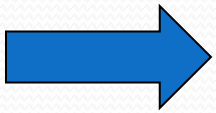
NIST Recommendations
Key length equivalences

symmetric	ECC	RSA/DH
80	160	1024
128	256	3072
192	384	7680
256	512	15360

equal difficulty against currently known attacks

Advantages over RSA/DH

- Shorter key lengths



1) Fewer bits to store and send
2) Less computational power
3) Faster

- Sample timing comparison on Intel Pentium IV 1700Mhz :

- RSA1024/ECC163

7:1

- RSA3072/ECC283

60:1

U.S. Standards governing ECC

- ietf standards for ECC for
  1) TLS, successor to SSL (secure browser)
  2) S/MIME, CMS (secure email)
  3) IPSec, X509 certificates, …
- FIPS, Digital Signature Standard (NIST)
- ANSI X9.62, X9.63 (Financial Services)
- IEEE P1363

NIST Curves

(National Institute of Standards and Technology)

- Standard curves for P-256, B-256, K-256,…. up to 512-bit field size
  - P- prime fields
  - B- binary fields
  - K- Koblitz curves (defined over F_2)
- Prime fields use special primes:

Generalized Mersenne Primes with very fast modular reduction

Affine vs. Projective coordinates

- (weighted) Projective coordinates allow group law computation on E without field inversions, at the cost of more multiplies
- Roughly 16 field multiplies to compute 2P
- Better than affine if field inversions are very expensive
- e.g. for NIST prime curves, some estimate 1 inversion ~ 80 multiplies.
- MSR implementation general curves, much lower ratio

Pairings in Cryptography

- MOV attack on ECDLP

Menezes-Okamoto-Vanstone

- In 2001, Boneh-Franklin introduced IBE

Identity-Based Encryption

- Joux, Tri-partite Diffie-Hellman

Many other applications…

- ABE (attribute-based encryption)
- PEKS (Public Key Encryption with Keyword Search)
- Predicate Encryption …
- Homomorphic encryption

BLS Short signatures: Boneh, Lynn, Shacham

Given a bilinear pairing (map):

$$e: G_1 \times G_1 \rightarrow G_2,$$

With a secret, s, a group element, P, in G_1

Create a public key pair (P, Q=sP)

Need a cryptographic hash function h to hash messages onto points on the curve.

BLS Signatures

Sign messages M → (M, S(M)),

$$S(M) = s\,h(M)$$

Verification is: $e(Q,h(M)) = e(P,S(M))$ **?**

bilinearity → $e(sP,h(M)) = e(P,sh(M))$

Implemented using Weil or Tate pairing, when G_1 is an elliptic curve and G_2 is the multiplicative group of a finite field

Pairings

- Weil pairing on elliptic curves
- Tate pairing on elliptic curves
- Squared Weil and Tate pairings
- Optimal Ate pairing
- Eta pairing and generalized forms

All these for Jacobians hyperelliptic curves:

[Duursma-Lee 03], [ELM 04], [Lee et al]

Application: Signatures for Network Coding

Denis Charles, Kamal Jain, Kristin Lauter,

Signatures for Network Coding,

In 40th Annual Conference on Information Sciences and Systems (CISS 06) (2006).

Network Coding for Content Distribution

- A directed graph of users G
- A server (single source) distributes content
- Content is divided into packets and represented as vectors in a vector space
- Each node receives linear combinations of packets from other nodes
- At each node, new linear combinations of received packets are formed and sent out along new edges
- Extra bits keep track of which linear combination at each step, allows recovery of the content

Pollution attacks

- A malicious node can inject garbage into the distribution network
- If undetected, the garbage will pollute the whole network, as meaningless packets are combined with others and redistributed
- *Signatures* on received packets can be used to check for garbage

Assumptions

- Public key digital signatures
- Only the server possesses the secret key for signing
- Any node can verify signatures using public information
- So how can nodes re-sign linear combinations of received packets?

Homomorphic signature scheme

- Our solution is based on:
  - Elliptic curves
  - Bilinear pairing (Weil pairing)
  - Homomorphic hashing of content onto points on the elliptic curve
  - BLS-type signatures (Boneh-Lynn-Schacham)
- Security reduction to ECDLP

  (Elliptic curve discrete logarithm problem)

Security

- Theorem: Finding a collision of the hash function h is polynomial-time equivalent to computing the discrete log on the elliptic curve.
- Fact: Forging signatures is as hard as the computational Diffie-Hellman problem on the curve E.
- Our scheme establishes authentication in addition to detecting pollution.

Generating Curves with CM Method

p = 263300183685717422065746325660655084022315089991 53.

$q = p^2 + 187515030262203983526300351743447020023129023021773 0^2$

=351688192729081689963486221568344816704455675519621991572654792860046102641340797974735424442696107030 9

- The complex multiplication method tells us that the elliptic curve

$$E : y^2 = x^3 + x$$

is a suitable elliptic curve. MAGMA tells us that #E(Fq) = 351688192729081689963486221568344816704455675519621986306651119766132641428476163374399639430720 04

== 0 mod p.

Subsequent work

Signing a Linear Subspace: Signature Schemes for Network Coding, Dan Boneh, David Freeman, Jonathan Katz, Brent Waters, Public Key Cryptography (PKC), 2009.

Secure Network Coding Over the Integers

Rosario Gennaro, Jonathan Katz, Hugo Krawczyk, Tal Rabin, Public Key Cryptography – PKC 2010

On Homomorphic Signatures for Network Coding

Yun, JH Cheon, Kim, IEEE Transactions on Computers 2010

Preventing pollution attacks in multi-source network coding.
by S. Agrawal, D. Boneh, X. Boyen, and D. Freeman In proceedings of PKC 2010.

Application: Anonymous Healthcare System

An Anonymous Health Care System,

Melissa Chase, Kristin Lauter,

HealthSec 2010, Workshop at Usenix Security

An Anonymous Healthcare System

Policy token

Buy insurance policy

Doctor / Clinic

Policy token

Insurance Co.

Anonymized token for procedure

Procedure info

Learns only that some patient covered by the policy received the prescription

An Anonymous Healthcare System

Policy token

Buy insurance policy

Insurance Co.

Pick up prescription

Prescription token

Doctor / Clinic

Policy token

Anonymized token for prescription

pharmacy

Anonymized token for prescription

Prescription info

Learns only that some patient covered by the policy received the prescription