Pairing based cryptography

Antoine Joux
DGA/SPOTI and
University de Versailles St-Quentin-en-Yvelines
France

Introduction: EC in cryptography

- Starting point: 1985 (V. Miller)
- Discrete logarithm based systems
- EC are almost “generic groups”
  - No general non-generic algorithm for DL
  - High security with short keys
- Now present in standards (ECDSA)

Choosing EC for cryptography

- According to a talk by Koblitz at IPAM
- Two possibilities
  - A pragmatic anwer
  - A paranoid answer

Pragmatic Answer (Normal security)

- Special curves
  - Counting points is easier
  - Computation speed can be optimized
  - Potential security risk
    - Example: MOV attack (Weil pairings)
  - Just avoid the known bad cases

Paranoid answer (High security)

- Avoid all special curves
- Random or pseudo-random curves
  - Large prime of the cardinal is needed
  - Preferable to prove: EC is not an hidden special case
    - Used a seeded deterministic generation
    - Publish the seed of the PRNG
    - Then users can check the generation process

A recent idea: Using pairing constructively

- Starting point: ANTS IV (2000)
- (some) EC are groups with additional properties
  - **Cons:** Subexponential algorithm for DL
  - **Pros:** New properties in Cryptosystems
- Expanding area of Cryptography

Tools

Review of mathematic tools

- Elliptic Curves
- Divisors
- Function Field
- The Weil and Tate pairings
- Computing with divisors and functions

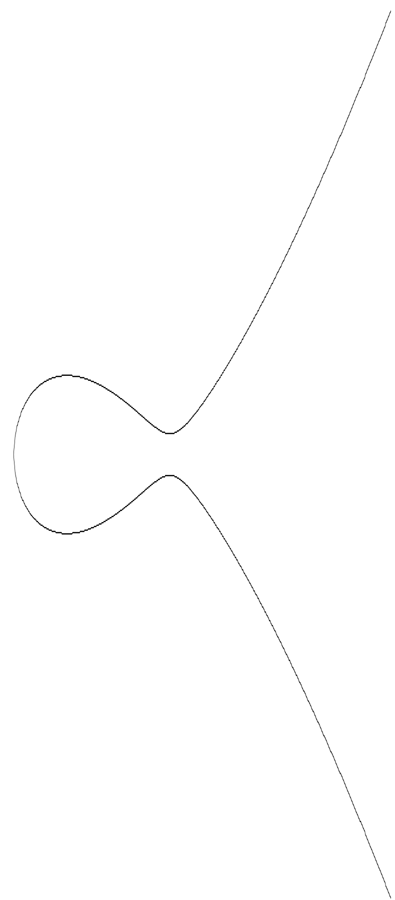
Elliptic Curves

- Curve of genus 1 over some field K
- Often represented by an equation:

$$Y^2 = X^3 + aX + b$$

- Group structure

An elliptic curve



Divisors

- Elements of the free group generated by the points of the curve.
- Formal sum of points on the curve

$$\sum c_P(P)$$

- The degree of a divisor is $\sum c_P$.

Function field

- For an elliptic curve over K given by:

$$Y^2 = X^3 + aX + b$$

- The function field is (*informal notation*):

$$K(X,Y)/(Y^2 - X^3 - aX - b).$$

- For a function f, its zeroes and poles define a divisor $div(f)$.
- A function f can be evaluated at a point or a divisor.

Principal Divisors

- A divisor of the form $div(f)$ is called principal
- Principal divisors are of degree 0
- On an elliptic curve, a divisor is principal **iff** its degree is zero and its evaluation on the curve is zero.
- Any divisor can be written as:

  $$(P) - (O) + div(f)$$

  for some point P and some function f.

From divisors to functions

- A divisor D is called q-fold when qD is principal
- If $D = (P) - (O) + div(g)$ is q-fold,
  we can compute f such that $qD = div(f)$.

Explicit computation

- Write qD_1 as $div(f_{D_1})$:
  - Start from

$$D_1 = ((aP) - (O)) - ((aQ) - (O))$$

  - Use addition formulas:
    * $D = (P) - (O) + div(f)$,
    * $D' = (P') - (O) + div(f')$
    * Then

$$\begin{aligned} D + D' &= (P + P') - (O) \\ &\quad + div(f f' g) \end{aligned}$$

    * where $g = l/v$: l line (P, P') and v line $(P + P', O)$.
- **Optional:** Evaluate it at D_2 (fundamental for performance)

The Weil Pairing

- Given P and Q two q-torsion points
- Let

$$\begin{aligned} D_P &= (P) - (O) \\ D_Q &= (Q) - (O) \end{aligned}$$

- Compute

$$e_q(P, Q) = f_{D_P}(D_Q)/f_{D_Q}(D_P)$$

- **Warning:** Write D_P as $(P + R) - (R)$
- $e_q(P, Q)$ is a q-th root of unity
- e_q is called the Weil Pairing

The Weil Pairing – Some Properties

- **Identity** $e_q(P, P) = 1$
- **Alternation** $e_q(P, Q) = e_q(Q, P)^{-1}$
- **Bilinearity**

$$e_q(P + Q, R) = e_q(P, R)e_q(Q, R)$$

$$e_q(R, P + Q) = e_q(R, P)e_q(R, Q)$$

- **Non-Degeneracy** If P is non-zero, there exist some q-torsion point Q such that $e_q(P, Q) \neq 1$.

The Tate Pairing

- Given D_1 and D_2 two q-fold divisors
- Compute $T_q(D_1, D_2) = f_{D_1}(D_2)$
- $T_q(D_1, D_2)$ is in K^*/K^{*q}
- $t_q(D_1, D_2) = T_q(P, Q)^{(p^r-1)/q}$ is a root of unity
- As before

$$\begin{aligned} D_P &= (P) - (O) \\ D_Q &= (Q + R) - (R) \end{aligned}$$

- Bilinear symmetric
- Usually faster than the Weil pairing

Elliptic curves with computable pairing

- A curve E over $\mathbb{F}_p$ and a "small" r such that:

$$N_E \mid p^r - 1.$$

- On such curves, we find:

$$\langle aP, bQ \rangle = \langle P, Q \rangle^{ab} \text{ in } \mathbb{F}_{p^r}$$

  - Constructed using pairings
  - Efficiently computable

Some examples

- Smallest r:

$$N_E = p - 1.$$

- Supersingular curves ($r = 2$):

$$N_E = p + 1 \mid p^2 - 1.$$

- Supersing. in char 3 ($r = 6$):

$$N_E = 3^n \pm 3^{\frac{n+1}{2}} + 1 \mid 3^{6n} - 1.$$

- With CM in large char. (example $r = 6$):

$$p = l^2 + 1,$$

$$N_E = l^2 - l + 1 \mid p^6 - 1.$$

An important special case

- We have a **single point** pairing when

$$\langle P, P \rangle \neq 1.$$

- However, directly works only with the first of the above examples
- In fact, always works when:
  - $N_E = p - 1$
  - P is a q–torsion point
  - and q^2 does not divides $p - 1$
- Constructing such curves is hard

Single point pairing with supersingular curves

- Nice solution found by Verheul
- With supersingular curves, only part of the q–torsion is defined over the base field
- A **distorsion** is an endomorphism Ψ such that:
  - $\Psi(P)$ is not defined over the base field when $P \neq 0$ is.
  - Thus $\Psi(P)$ is not in the subgroup generated by P

Single point pairing with supersingular curves

- As a consequence:
  - $w(P, \Psi(P)) \neq 1$
- Thus the modified pairing:

$$\langle P_0, P_1 \rangle = w(P_0, \Psi(P_1))$$

  is a single point pairing.

- It sends pairs of points (over the base field) to roots of unity (in the extension field).
- It is bilinear and symmetric

Some distorsions

Field	Curve	Distorsion	Conditions	Order	Mul
$\mathbb{F}_p$	$y^2 = x^3 + ax$	$(x, y) \mapsto (-x, iy)$ $i^2 = -1$	$p \equiv 3[4]$	$p + 1$	2
$\mathbb{F}_p$	$y^2 = x^3 + a$	$(x, y) \mapsto (\zeta x, y)$ $\zeta^3 = 1$	$p \equiv 2[3]$	$p + 1$	2
$\mathbb{F}_{p^2}$	$y^2 = x^3 + a$ $a \notin \mathbb{F}_p$	$(x, y) \mapsto (\omega \frac{x^p}{r^{(2p-1)/3}}, \frac{y^p}{r^{p-1}})$ $r^2 = a, r \in \mathbb{F}_{p^2}$ $\omega^3 = r, \omega \in \mathbb{F}_{p^6}$	$p \equiv 2[3]$	$p^2 - p + 1$	3
$\mathbb{F}_{3^n}$	$y^2 = x^3 + 2x + 1$	$(x, y) \mapsto (-x + r, uy)$ $u^2 = -1, u \in \mathbb{F}_{3^{2n}}$ $r^3 + 2r + 2 = 0, r \in \mathbb{F}_{3^{3n}}$	$n \equiv \pm 1[12]$	$3^n + 3^{\frac{n+1}{2}} + 1$	6
$\mathbb{F}_{3^n}$	$y^2 = x^3 + 2x + 1$	$(x, y) \mapsto (-x + r, uy)$ $u^2 = -1, u \in \mathbb{F}_{3^{2n}}$ $r^3 + 2r + 2 = 0, r \in \mathbb{F}_{3^{3n}}$	$n \equiv \pm 5[12]$	$3^n - 3^{\frac{n+1}{2}} + 1$	6
$\mathbb{F}_{3^n}$	$y^2 = x^3 + 2x - 1$	$(x, y) \mapsto (-x + r, uy)$ $u^2 = -1, u \in \mathbb{F}_{3^{2n}}$ $r^3 + 2r - 2 = 0, r \in \mathbb{F}_{3^{3n}}$	$n \equiv \pm 1[12]$	$3^n - 3^{\frac{n+1}{2}} + 1$	6
$\mathbb{F}_{3^n}$	$y^2 = x^3 + 2x - 1$	$(x, y) \mapsto (-x + r, uy)$ $u^2 = -1, u \in \mathbb{F}_{3^{2n}}$ $r^3 + 2r - 2 = 0, r \in \mathbb{F}_{3^{3n}}$	$n \equiv \pm 5[12]$	$3^n + 3^{\frac{n+1}{2}} + 1$	6

Abstract single point pairing

- For crypto applications, we can forget EC and view pairings as follows:
  - Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two (cyclic) groups of prime order ℓ
  - A pairing is bilinear symmetric map from $\mathbb{G}_1$ to $\mathbb{G}_2$
  - The group operation on $\mathbb{G}_1$ is written additively
  - The group operation on $\mathbb{G}_2$ is written multiplicatively
  - Some operations (such as DL) are hard on $\mathbb{G}_1$ and/or $\mathbb{G}_2$

Application

Applications of the pairing

- Cryptanalytic purpose
- Constructive side
  - Tripartite Diffie-Hellman
  - Identity based encryption
  - Short Signatures
  - Verifiable random functions

Pairing for cryptanalysis

- Called the MOV attack
- Use the pairing with R to move

$$Q = aP$$

  on the EC to

$$\langle Q, R\rangle = \langle P, R\rangle^a$$

  in the finite field
- Yields a subexponential algorithm.

Usual Diffie–Hellman

- Alice publishes g^a, Bob publishes g^b
- Both compute $(g^a)^b = (g^b)^a$

They end up with a (computational) common secret.

Can we do more ?

- Yes, Conference keying
  - All t users publish $X_i = g^{a_i}$
  - Publish $Y_i = (X_{i+1}/X_{i-1})^{a_i}$
  - Common key computed as:

$$X_{i-1}^{ta_i} \cdot Y_i^{t-1} \cdot Y_{i+1}^{t-2} \cdots Y_{i+t-3}^{2} \cdot Y_{i+t-2}^{1}$$

  In fact it is:

$$g^{a_1 a_2 + a_2 a_3 + \cdots + a_{t-1} a_t + a_t a_1}.$$

- However, non-interactivity is lost.

Our Goal: One round Tripartite Diffie–Hellman

- Alice, Bob and Charlie publish (something similar to) g^a, g^b, g^c
- They all compute g^{abc}

Tripartite Diffie–Hellman

With a single point pairing:

- P a point of order q.
- Alice, Bob and Charlie publish
  aP, bP and cP
- They all compute:

$$\langle bP, cP\rangle^a = \langle cP, aP\rangle^b = \langle aP, bP\rangle^c$$

- This value is the common secret (in $\mathbb{G}_2$)

Identity based encryption

- Concept introduced by Shamir in 1984
- **Goal:** Offer a simpler replacement of PKIs
- **Main idea:** Use name as public key
- **Problem:** Finding the private key
- Computationally heavy solution of Maurer and Yacobi (92)

Identity based encryption with pairings

Boneh Franklin – Crypto 2001

- **Parameters:** P_{pub}, $Q_{\text{pub}} = sP_{\text{pub}}$ (s is secret)
- Public key of user ID: $Q_{\text{ID}} = G(\text{ID})$
- Private key of user ID: $P_{\text{ID}} = sQ_{\text{ID}}$
- Key exchange with user ID
  - Pick a random r
  - Send rQ_{pub} to ID
  - The exchange key is derived from

$$\langle Q_{\text{ID}}, rP_{\text{pub}} \rangle = \langle P_{\text{ID}}, rQ_{\text{pub}} \rangle.$$

- Can be used in El Gamal like encryption.

Short signatures

- Recurring problematic
- Signatures are often too long
- **RSA:** Signatures have the length of the modulus
- **Diffie-Hellman:** Lengths are doubled (due to randomization)
- **Others:** Potential short signatures with multivariate crypto.

Short signatures with pairings

Boneh Shacham Lynn – Asiacrypt 2001

- Public key: P, $Q = sP$ (s is secret)
- Private key: s
- To sign M send it to a point $P_M = G(M)$ on $\mathbb{G}_1$
- The signature is σ the x-coordinate of sP_M
- To verify the signature M, σ
  - Find a point S with x-coordinate σ
  - Compute $u = \langle P, S\rangle$ and $v = \langle Q, P_M\rangle$
  - Accept if $u = v$ or $u = v^{-1}$

Verifiable random functions

- Pseudo-Random functions are very useful in cryptography
- They use a secret key
- Verifiable random functions allow verification by a third party
- Must use a private/public key pair
- First known construction by Dodis (2002) using pairings

Security

Security Issues

- The security of application relies on some hard problems related to pairing:
- In Boneh-Franklin: Weil Diffie-Hellman (WDH) problem
  - Given (P, aP, bP, cP) for random a, b, c compute $w(P, \Psi(P))^{abc}$
- Can be generalized to any pairing: TDH
- Gives security in the random oracle model

Security Issues

- Alternatively, could use the decision problem DTDH.
  - Given (P, aP, bP, cP, dP), decide whether $d = abc$ (modulo the order of P)

Other classical related problems

- DDH in $\mathbb{G}_1$: $\mathrm{DDH}_{\mathbb{G}_1}$
- DDH in $\mathbb{G}_2$: $\mathrm{DDH}_{\mathbb{G}_2}$
- CDH in $\mathbb{G}_1$: $\mathrm{CDH}_{\mathbb{G}_1}$
- CDH in $\mathbb{G}_2$: $\mathrm{CDH}_{\mathbb{G}_2}$
- DL in $\mathbb{G}_1$: $\mathrm{DL}_{\mathbb{G}_1}$
- DL in $\mathbb{G}_2$: $\mathrm{DL}_{\mathbb{G}_2}$

Some less classical problems

- GTI: general Tate inversion
  - Given g in $\mathbb{G}_2$, find P and Q such that:

$$\langle P, Q \rangle = g.$$

- FTI: fixed (operand) Tate inversion
  - P being fixed
  - Given g in $\mathbb{G}_2$, Q such that:

$$\langle P, Q \rangle = g.$$

Relations between the complexity assumptions

$$
\begin{tikzcd}
 & & \mathrm{CDH}_{\mathbb{G}_1} \arrow[rr] \arrow[dr] & & \mathrm{DL}_{\mathbb{G}_1} \arrow[d] \\
\mathrm{DTDH} \arrow[r] \arrow[dr] & \mathrm{TDH} \arrow[ur] \arrow[dr] & \mathrm{GTI} \arrow[r] & \mathrm{FTI} \arrow[r] & \mathrm{DL}_{\mathbb{G}_2} \arrow[d, leftrightarrow] \\
 & \mathrm{DDH}_{\mathbb{G}_2} \arrow[r] & \mathrm{CDH}_{\mathbb{G}_2} \arrow[ur] & & \mathrm{DL}_{\mathbb{G}_1} \text{ or } \mathrm{GTI}
\end{tikzcd}
$$

Choosing EC for pairing-based cryptography

- Many possibilities
  - Singular or supersingular
  - Embedding degree k from 1 to 24 (largest effective example)
- Possibility of "high-security" discussed by Koblitz and Menezes

Conclusion

Questions