Pairing Based Cryptography

Tanja Lange

Department of Mathematics

Technical University of Denmark

tanja@hyperelliptic.org

16.08.2006

Overview

- Protocols
- Weil and Tate pairing on elliptic curves
- Efficient computation of pairings
- Supersingular and ordinary elliptic curves
- Embedding degree
- MNT curves
- Outlook

Protocols

Diffie-Hellman Key exchange

Alice

1. secretly generates $a < |\langle P \rangle|$
2. computes $Q_1 = [a]P$
3. transmits Q_1

Bob

1. secretly generates $b < |\langle P \rangle|$
2. computes $Q_2 = [b]P$
3. transmits Q_2

4. computes (Alice) $[a]Q_2$

4. computes (Bob) $[b] \cdot Q_1$

$$[a]Q_2 = [ab]P = [b] \cdot Q_1$$

Common Key: the group element $k = [(ab)]P \in G$ can be used in symmetric encryption.

ElGamal Encryption

Public parameters:
Group G, generator P, ord$(P) = l$, some invertible embedding function $H : m \rightarrow G$.
Receiver has secret key s_A and public key $P_A = [s_A]P$.

- Encrypt message m
  - choose random integer k
  - compute $R = [k]P$ and $c = H(m) + [k]P_A$
- Decrypt ciphertext (R, c)
  - compute $S = [s_A]R$
  - obtain $m = H^{-1}(c - S)$

  (This gives m as $S = [s_A]R = [ks_A]P = [k]P_A$).

DL systems

These systems assume that the Discrete Logarithm Problem (DLP) is hard to solve, i.e.

- given P and $P_A = [s_A]P$
- it is hard to find s_A.

The Computational Diffie-Hellman Problem (CDHP) is the problem

- given P, $P_A = [s_A]P$, and $P_B = [s_B]P$
- compute $[s_A s_B]P$.

The Decisional Diffie-Hellman Problem (DDHP) is the problem

- given P, $P_A = [s_A]P$, $P_B = [s_B]P$ and $R = [r]P$
- decide whether $R = [s_A s_B]P$.

Pairings

Let $(G_1, +), (G'_1, +)$ and $(G, \cdot)$ be cyclic groups of prime order ℓ and let

$$e : G_1 \times G'_1 \rightarrow G$$

be a an efficiently computable map satisfying

- $e(P + Q, R') = e(P, R')e(Q, R')$
- $e(P, R' + S') = e(P, R')e(P, S')$
- The map is non-degenerate in the first argument, i.e. if $e(P, R') = 1$ for all $R' \in G'_1$ for some P then P is the identity in G_1

Then e is called a bilinear map or pairing.

In protocol papers often $G_1 = G'_1$ (keyword “distortion map”).

Consequences I

Assume that $G_1 = G_1'$ and hence

$$e(P,P) \neq 1.$$

Then for all triples $(P_1, P_2, P_3) \in \langle P \rangle^3$ one can decide efficiently whether

$$\log_P(P_3) = \log_P(P_1)\log_P(P_2)$$

by comparing

$$e(P_1, P_2) \stackrel{?}{=} e(P, P_3).$$

Thus the DDHP is easy!
CDHP can still be hard!

Consequences II

Even for $G_1 \neq G_1'$ can transfer the DLP in G_1 to a DLP in G.

Let $P' \in G_1'$ be such that

$$e(P, P') \neq 1.$$

Given DLP $P, P_A = [s_A]P$ compute

$g = e(P, P')$ and $h = e(P_A, P') = e([s_A]P, P') = e(P, P')^{s_A} = g^{s_A}$.

This gives DLP in G with $g, h = g^{s_A}$ related by the same scalar s_A as original system.

DL system G_1 is at most as secure as the system G!

Pairing based protocols I

Joux, ANTS 2000, one round tripartite key exchange

Let P, P' be generators of G_1 and G_1' respectively.
Users A, B and C compute joint secret from their secret contributions a, b, c as follows (A's perspective)

- Compute and send $[a]P, [a]P'$.
- Upon receipt of $[b]P$ and $[c]P'$ put $k = (e([b]P, [c]P'))^a$

The resulting element k is the same for each participant as

$$k = (e([b]P, [c]P'))^a = (e(P, P'))^{abc} = (e([a]P, [c]P'))^b = (e([a]P, [b]P'))^c.$$

- Obvious saving in first step if $G_1 = G_1'$.
- Only one user needs to do both computations.

Pairing based protocols II

- Sakai-Ohgishi-Kasahara, 2000 ID-based key exchange
- Boneh and Franklin, Crypto 2001, ID-based cryptography

Idea: user's identity defines his public key.

Consequences

- Advantage in ID-based crypto if recipient is not in system or sender wants to force use of a fresh key (other applications possible).
- No need for PKI, can avoid need for authentication.
- Set-up requires a trusted authority (TA) which can compute the secret key for a given public key.

ID-based cryptography II

- Let $H : \{0,1\}^* \rightarrow G_1'$ be hash function.
- Master secret key of TA is s, public key is $P_{pub} = [s]P$.
- Public key of ID represented by string ID is $H(ID) \in G_1'$.
- Secret key $S' = [s]H(ID) \in G_1'$ computable only by TA.
- Idea is that from

  $$P_{pub}, H(ID) \text{ and } k$$

  or from

  $$[k]P, \text{ and } [s]H(ID)$$

  both parties can compute

  $$e([k]P, [s]H(ID)) = (e(P, H(ID)))^{ks} = (e([s]P, H(ID)))^k.$$

Security assumptions

(Just a few from the huge zoo.)

- Clearly these systems require that the DLP is hard in the groups.
- Additionally we define the following computational and decisional problems. To ease notation let $G_1 = G_1'$ and $g = e(P, P)$.
  - Computational Bilinear Diffie-Hellman Problem (CBDHP):
    Compute $g^{s_A s_B s_C}$ given $[s_A]P, [s_B]P, [s_C]P$, and P
  - Decisional Bilinear Diffie-Hellman Problem (DBDHP):
    Given $P, [s_A]P, [s_B]P, [s_C]P$ and g^r decide whether $g^r = g^{s_A s_B s_C}$.

Pairings

Prerequisites

We want to define pairings

$$G_1 \times G_1' \to G$$

preserving the group structure.

The pairings we use map to the multiplicative group of a finite extension field $\mathbb{F}_{q^k}$. To embed the points of order ℓ the embedding degree k has to be chosen large enough so that the ℓ-th roots of unity are in $\mathbb{F}_{q^k}^*$.

So choose

$$k \text{ minimal with } \ell \mid q^k - 1.$$

Tate-Lichtenbaum pairing I

$\mathrm{Pic}^0_C(\mathbb{F}_{q^k})[\ell]$: divisor classes on C of order ℓ defined over $\mathbb{F}_{q^k}$.

$\bar{D}_1 \in \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[\ell] \Rightarrow \exists F_{D_1}$ such that $\ell D_1 \sim \mathrm{div}(F_{D_1})$, where D_1 represents the class $\bar{D}_1$.

Let $\bar{D}_2 \in \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ be represented by D_2 with

$$\mathrm{support}(D_2) \cap \mathrm{support}(D_1) = \emptyset.$$

Tate-Lichtenbaum pairing

$$T_\ell(\bar{D}_1, \bar{D}_2) = F_{D_1}(D_2) = \frac{\prod_{i=1}^n F_{D_1}(P_i)}{\prod_{j=1}^n F_{D_1}(Q_j)}$$

for $D_2 = \sum_{i=1}^n P_i - \sum_{j=1}^n Q_j$.

Tate-Lichtenbaum pairing II

This

$$T_\ell(\bar{D}_1, \bar{D}_2) = F_{D_1}(D_2)$$

defines a bilinear and non-degenerate map

$$T_\ell : \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[\ell] \times \mathrm{Pic}^0_C(\mathbb{F}_{q^k})/\ell\mathrm{Pic}^0_C(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/\mathbb{F}^{*\ell}_{q^k}$$

as ℓ-folds are in the kernel of T_ℓ.
Namely, if $\bar{D}_2 = [\ell]\bar{D}_3$ then

$$F_{D_1}(D_2) = F_{D_1}(D_3)^\ell = 1.$$

To achieve unique value in $\mathbb{F}_{q^k}$ rather than class do final exponentiation

$$\tilde{T}_\ell = T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell}.$$

Tate-Lichtenbaum pairing III

For elliptic curves use isomorphism

$$\mathrm{Pic}^0_E(\mathbb{F}_{q^k}) \cong E(\mathbb{F}_{q^k})$$

to define pairing on points $T_\ell(P,Q)$, with

$$D_1 = P - P_\infty, D_2 = (Q \oplus R) - R$$

for some R.

Build F iteratively by Miller's algorithm (double-and-add).

Often

$$T_\ell : E(\mathbb{F}_{q})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/\mathbb{F}^{*\ell}_{q^k}.$$

Miller's algorithm

In: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q \oplus R, R$
Out: $T_\ell(P, Q)$

1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n - 2$ downto 0 do
   (a) Calculate lines l and v in doubling $[2]T$
   $T \leftarrow [2]T$
   $F \leftarrow F^2 \cdot l(Q \oplus R)v(R)/(l(R)v(Q \oplus R))$
   (b) if $\ell_i = 1$ then
   Calculate lines l and v in addition $T \oplus P$
   $T \leftarrow T \oplus P$
   $F \leftarrow F \cdot l(Q \oplus R)v(R)/(l(R)v(Q \oplus R))$
3. return F

Weil pairing

For an elliptic curve E define

$$\begin{array}{rcl} W_\ell : E(\overline{\mathbb{F}}_q)[\ell] \times E(\overline{\mathbb{F}}_q)[\ell] & \rightarrow & \mu_\ell \\ (P,Q) & \mapsto & \dfrac{F_{P-P_\infty}(D_Q)}{F_{Q-P_\infty}(D_P)} \end{array}$$

where μ_ℓ is the multiplicative groups of the ℓ-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.
Obviously, $W_\ell(P,P) = 1$.

Weil pairings can be seen as two-fold application of the Tate-Lichtenbaum pairing, note $Q \in E(\mathbb{F}_{q^k})$.

Needs full group of order ℓ in $E(\mathbb{F}_{q^k})$, if $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

Supersingular and ordinary

Definition

Let E be an elliptic curve defined over $\mathbb{F}_q, q = p^r$.
E is supersingular if

- $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$.
- $|E(\mathbb{F}_q)| = q - t + 1$ with $t \equiv 0 \bmod p$.
- End_E is order in quaternion algebra.

Otherwise it is ordinary and one has $E[p^s](\overline{\mathbb{F}}_q) = \mathbb{Z}/p^s\mathbb{Z}$.

These statements hold for all s if they hold for one.

Example

Consider

$$y^2 + y = x^3 + a_4 x + a_6 \text{ over } \mathbb{F}_{2^r},$$

so $q = 2^r$.

Negative of $P = (a, b)$ is $-P = (a, b + 1)$,
$\Rightarrow$ no affine point with $P = -P$ since $b \neq b + 1$,
$\Rightarrow$ even number of affine points, one point P_∞,

$\Rightarrow |E(\mathbb{F}_q)| = q - t + 1 = 2^r - t + 1$ is odd, so t is even.

This curve is supersingular (using the second criterion).

Embedding degrees I

Let E be supersingular and $q = p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states $|t| \leq 2\sqrt{p}$ and E supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and

$$|E(\mathbb{F}_p)| = p + 1.$$

Obviously

$$(p+1) \mid p^2 - 1 = (p+1)(p-1)$$

so $k \leq 2$ for supersingular curves over prime fields.

Parameter sizes

For DLP in groups one has square-root attacks, for finite fields index calculus methods are more efficient. A common requirement is

- $\#E(\mathbb{F}_q) \sim q$: 160 bits
- q^k: 1024 bits
- optimal embedding degree would be

$$k = 1024/160 = 6.4$$

However, 6 is only attained for small characteristic and there Coppersmith methods require larger fields, cf. Page, Smart, and Vercauteren.
Difference between sizes grows $\Rightarrow$ larger k becomes optimal.

Embedding degrees II

Let E be supersingular.
Menezes, Okamoto, and Vanstone show:

- in characteristic 2 we have $k \leq 4$,
- in characteristic 3 we have $k \leq 6$,
- over prime fields $\mathbb{F}_p$ with $p \geq 5$ we have $k \leq 2$,

and these bounds are attained.

Now or soon, larger k become necessary, no chance with supersingular elliptic curves, little hope for larger genus hyperelliptic.

MNT curves

Find ordinary curves with small embedding degree! Thus force

$$q + 1 - t \equiv 0 \pmod{\ell} \text{ and } q^k - 1 \equiv 0 \pmod{\ell}.$$

- Original proposal by Miyaji, Nakabayashi, and Takano.
- Dupont, Enge, Morain: small k by CM
- Barreto, Lynn, Scott; Brezing, Weng;
  Curves for $k = 3, 4$ and 6.
- Generalization to co-factors, $k = 5, 10, 12$
  Galbraith, McKee, Valença.
- Family of curves with $k = 12$ by Barreto and Naehrig.
- Family of curves with $k = 10$ by D. Freeman.

Outlook

Pairings are a very active area of research, e.g. on the following tasks

- find more protocols / solve posed problems,
- speed up the computation,
- find more MNT curves,
- consider other curves, e.g. hyperelliptic curves.

Great collection at

P. S. L. M. Barreto, “The Pairing-Based Crypto Lounge”

`http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`

- Break system???

Literature

- P. S. Barreto, S. Galbraith, C. O hEigeartaigh, M. Scott
  "Efficient Pairing Computation on Supersingular Abelian Varieties"
- R. Dutta, R. Barua, and P. Sakar
  "Pairing-based cryptography: A survey"
- D. Hankerson and A. J. Menezes and S. A. Vanstone
  "Guide to elliptic curve cryptography"
- Chapter in
  "Advances in Elliptic Curve Cryptography",
  by I. F. Blake, G. Seroussi, and N. P. Smart (Editors)
- Chapters in
  "Handbook of Elliptic and Hyperelliptic Curve Cryptography", by H. Cohen and G. Frey (Editors)