Open Problems in Pairings

Tanja Lange

Department of Mathematics and Computer Science

Eindhoven University of Technology

tanja@hyperelliptic.org

Protocols

Security Assumptions – DL systems

All 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 $(G_1, \oplus), (G_2, \oplus)$ and $(G_T, \cdot)$ be cyclic groups of prime order ℓ and let

$$e : G_1 \times G_2 \to G_T$$

be a an efficiently computable map satisfying

- $e(P \oplus Q, R') = e(P, R')e(Q, R')$
- $e(P, R' \oplus S') = e(P, R')e(P, S')$
- The map is non-degenerate in the first argument, i.e. if $e(P, R') = 1$ for all $R' \in G_2$ for some P then P is the identity in G_1

Then e is called a bilinear map or pairing.This implies

$$e([a]P, R') = e(P, [a]R') = e(P, R')^a.$$

In protocol papers often $G_1 = G_2$ (keyword “distortion map”).

Consequences I

Pairings allow to transfer the DLP in G_1 to a DLP in G_T.

Let $P' \in G_2$ be such that $e(P, P') \neq 1$,

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

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

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

DL system G_1 is at most as secure as the system G! Same works with G_2 instead of G_1.

This is the background of the Menezes-Okamoto-Vanstone ($g = 1$) and the Frey-Rück attack (arbitrary g).

Consequences II

Assume that $G_1 = G_2$ and hence $e(P, P) \neq 1$. Then for all triples $(P_1, P_2, P_3) \in \langle P \rangle^3$, $P_i = [a_i]P$ one can decide efficiently whether

$$P_3 = [a_1 a_2]P, \text{ i.e. } \log_P(P_3) = \log_P(P_1)\log_P(P_2)$$

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

$$e(P_1, P_2) = e([a_1]P, [a_2]P) = e(P, [a_1 a_2]P) = e(P, P_3).$$

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

This was used by Joux and Nguyen to construct gap DH groups, i.e. groups in which CDHP and DLP are hard while DDHP is easy.

Pairing based protocols I

Joux, ANTS 2000, one round tripartite key exchange

Let P, P' be generators of G_1 and G_2 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

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

- Only one user needs to do both computations (with P and P').
- Obvious saving in first step if $G_1 = G_2$.

Pairing based protocols II

Sakai-Ohgishi-Kasahara, 2000, Boneh and Franklin, Crypto 2001.
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 $H : \{0,1\}^* \to G_2$ 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 $H(ID) \in G_2$.
- Secret key $S' = [s]H(ID) \in G_2$ 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. Just for this slide let $G_1 = G_2$ 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 in Real Life

Prerequisites I

We want to define pairings

$$G_1 \times G_2 \to G_T$$

preserving the group structure.

- Tate and the Weil pairing both use abelian varieties as the first argument. Assume that $\ell \big| |\mathrm{Pic}_C^0(\mathbb{F}_q)|$ and $\ell^2 \not| \, |\mathrm{Pic}_C^0(\mathbb{F}_q)|$.
- Let ℓ be a prime, let C be a (hyper)elliptic curve over $\mathbb{F}_q$.
- G_1 is the group of $\mathbb{F}_q$-rational ℓ-torsion points of Pic_C^0,
- i.e. $G_1 = E[\ell](\mathbb{F}_q)$, $\mathbb{F}_q$-rational points on elliptic curve $C = E$ of order ℓ
- or $G_1 = \mathrm{Pic}_C^0[\ell](\mathbb{F}_q)$, $\mathbb{F}_q$-rational divisor classes of order ℓ.

Prerequisites II

- The pairings we use map to the multiplicative group of a finite extension field $\mathbb{F}_{q^k}$.
- G_T has order ℓ, so by Lagrange ℓ must divide the group order of $\mathbb{F}_{q^k}^*$, this happens if $\ell \mid q^k - 1$.
- The embedding degree k is defined to be the minimal extension degree of $\mathbb{F}_q$ so that the ℓ-th roots of unity are in $\mathbb{F}_{q^k}^*$, i.e.

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

- The embedding degree is important to balance security between G_i and G_T. (Index Calculus attacks make finite fields far less secure.)
- For $k > 1$ Tate-Lichtenbaum pairing is degenerate on linear dependent points, i.e. $T_\ell(P, P) = 1$.

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

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

defines a bilinear and non-degenerate map

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

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

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

$\tilde{T}_\ell$ called modified Tate-Lichtenbaum pairing.

Tate-Lichtenbaum pairing Elliptic Curves

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.

Usual setting

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

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

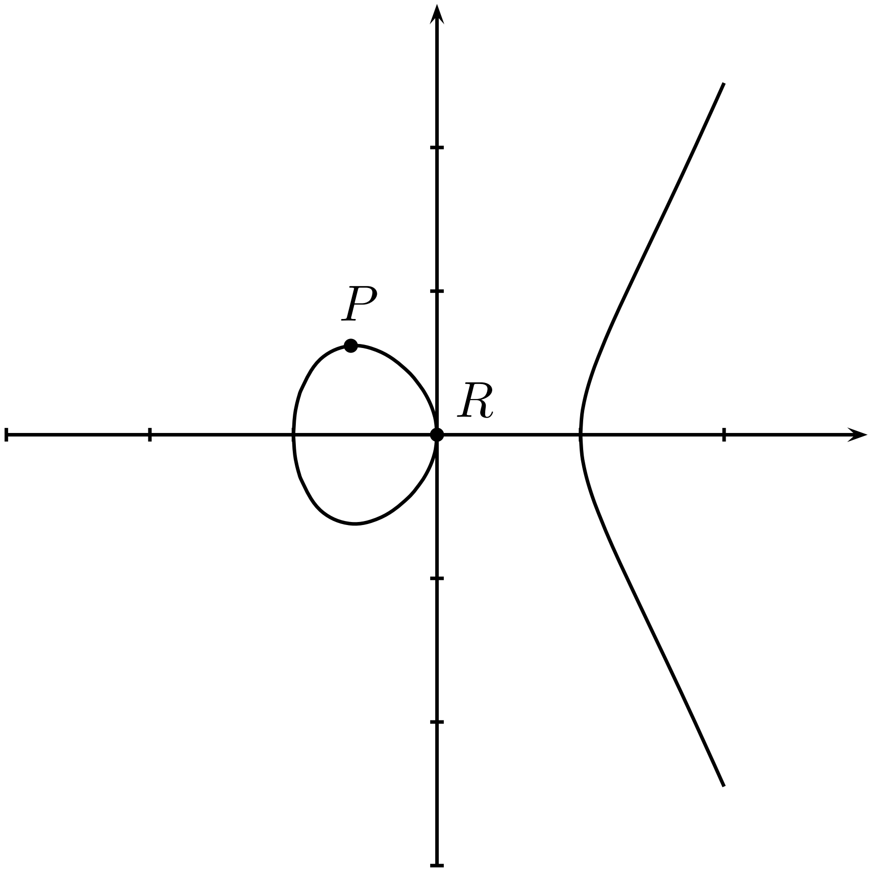
Miller's algorithm

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

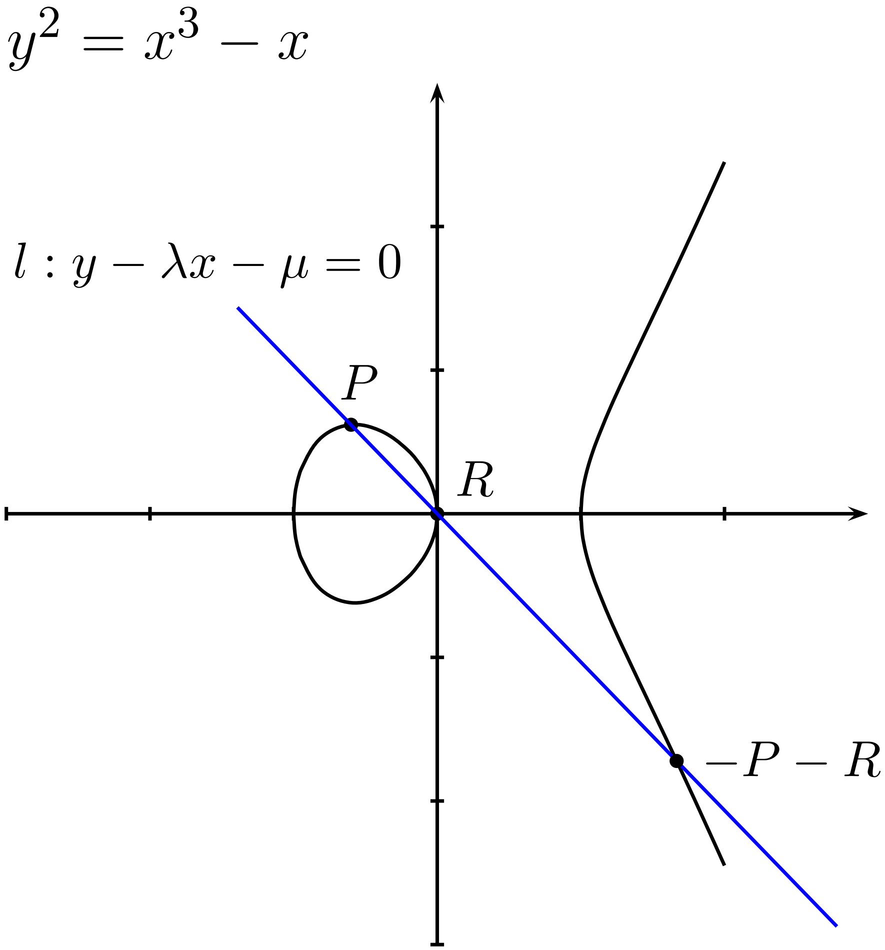
1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n - 2$ downto 0 do
   (a) Calculate lines l and v in doubling $[2]T$
   $T \leftarrow [2]T$
   $F \leftarrow F^2 \cdot l(Q \oplus R)v(R)/(l(R)v(Q \oplus R))$
   (b) if $\ell_i = 1$ then
   Calculate lines l and v in addition $T \oplus P$
   $T \leftarrow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

Group Law in $E(\mathbb{R}), h = 0$

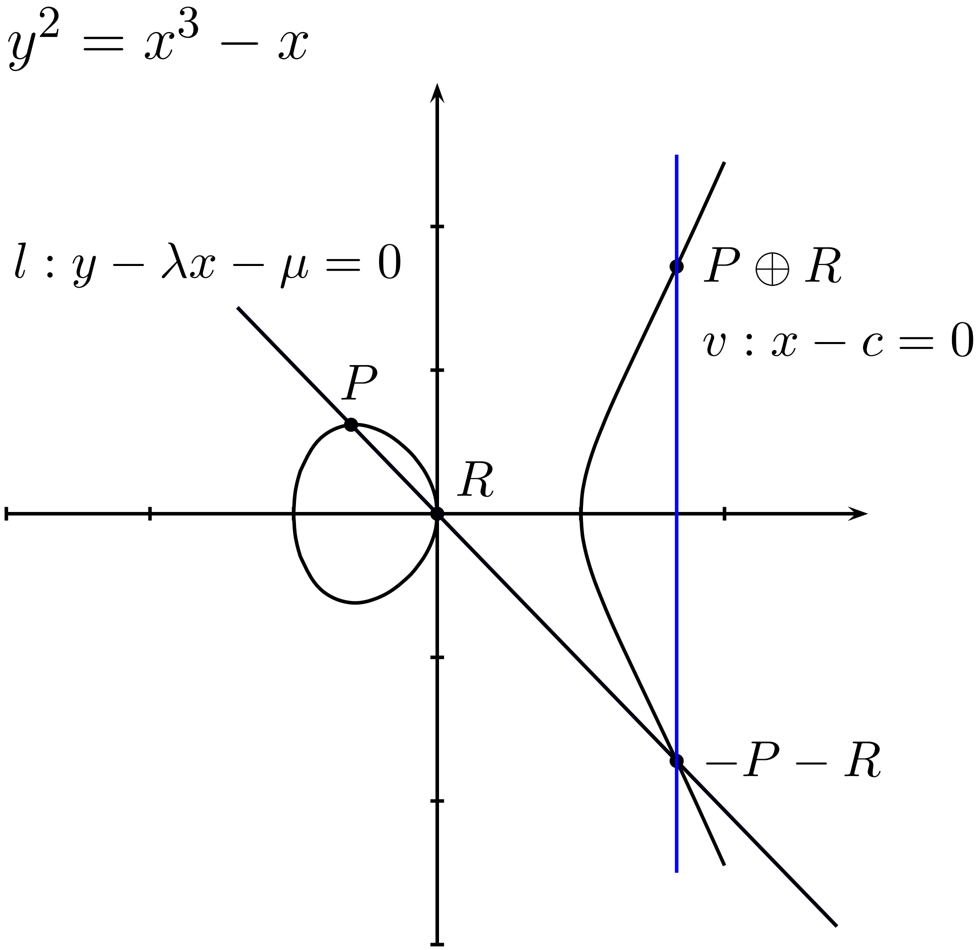
$y^2 = x^3 - x$



Group Law in $E(\mathbb{R}), h = 0$



Group Law in $E(\mathbb{R}), h = 0$



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.
End_E order in quaternion algebra means that there are maps which are linearly independent of the Frobenius endomorphism. They are called distortion maps.

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).

Distortion map I

For supersingular curves it is possible to find maps $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$ that map to a linearly independent subgroup, i.e.

$$T'_\ell(P,P) \neq 1 \text{ for } T'_\ell(P,P) = T_\ell(P,\phi(P)).$$

(This needs that there are independent endomorphisms, so no chance for ordinary curves).
Examples:

- $y^2 = x^3 + a_4 x$, for $p \equiv 3 \pmod 4$.
  Distortion map $(x,y) \mapsto (-x, iy)$ with $i^2 = -1$
- $y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
  Distortion map $(x,y) \mapsto (jx, y)$ with $j^3 = 1, j \neq 1$,

In both cases, $\#E(\mathbb{F}_p) = p + 1$, $k = 2$.

Distortion maps II

- Over $\mathbb{F}_{2^d}$ consider
$$y^2 + y = x^3 + x + a_6, \text{ with } a_6 = 0 \text{ or } 1$$
and distortion map
$$(x, y) \mapsto (x+s^2, y+sx+t),\ s, t \in \mathbb{F}_{2^{4d}},\ s^4+s = 0,\ t^2+t+s^6+s^2 = 0.$$
$$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2},\ k = 4.$$
- Over $\mathbb{F}_{3^d}$ consider
$$y^2 = x^3 + x + a_6, \quad \text{with} \quad a_6 = \pm 1$$
and distortion map
$$(x, y) \mapsto (-x + s, iy) \ \text{ with } \ s^3 + 2s + 2a_6 = 0 \ \text{ and } \ i^2 = -1.$$
$$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2},\ k = 6.$$

Application of distortion maps

- Distortion maps allow to state the protocols as using bilinear map
$$G_1 \times G_1 \to G.$$
- Scalar multiplications of input point can be performed over $\mathbb{F}_q$ and then mapped into $E(\mathbb{F}_{q^k})$, this saves computation time
$\Rightarrow$ obvious computational savings in the above protocols.
- Can be used to map on points with x-coordinate in subfield (leads to speed-up, see next section).
- Systems are easier to state.
- Really short signatures (see next slide).

Short signatures

Boneh, Lynn, and Shacham, Asiacrypt 2001
(followed by papers in the standard model)

Requires hash function $H : \{0,1\}^* \to G_1$.

User secret key s, public key $[s]P$.

Signature of message m:
Compute and send $S = [s]H(m)$.

Verification:
Check if

$$e([s]P, H(m)) = e(P, S).$$

Point compression to the x-coordinate achieves signatures given by one field element, i.e. of half the length of ECDSA.

Distortion maps for ordinary curves I

- E is an ordinary elliptic curve, then $\mathrm{End}(E)$ is order in quadratic number field.
- Every endomorphism commutes with the Frobenius endomorphism σ.
- Over algebraic closure

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

  Common choices for generators are $P \in E(\mathbb{F}_q)$, thus $\sigma(P) = P$, and Q other eigenvector of σ, $\sigma(Q) = [q]Q$.
- $\mathrm{Tr}(Q) = Q \oplus \sigma(Q) \oplus \cdots \oplus \sigma^{k-1}(Q) = [1+q+q^2+\cdots+q^{k-1}]Q$
  $= [(q^k - 1)/(q-1)]Q = P_\infty$.
  since k minimal with $\ell \big| q^k - 1$.
- Q is in trace zero subgroup.

Distortion maps for ordinary curves II

- If $G_1 = \langle P \rangle$ and $G_2 = \langle Q \rangle$ no endomorphism can map from G_1 to G_2. No distortion map in this case.
- Other cases, i.e. $G_2 = \langle [a]P \oplus [b]Q \rangle$ allows to use trace Tr to map from G_2 to G_1 :

$$\mathrm{Tr}([a]P \oplus [b]Q) = [ak]P$$

  which is linearly independent of $[a]P \oplus [b]Q$.
- Detailed analysis of distortion maps for supersingular and ordinary curves
  - E. Verheul, Eurocrypt 2001 & J. Crypto (17), 277–296, 2004.
  - Steven D. Galbraith and Victor Rotger, LMS JCM (7), 201-218.

More on this later.

Efficient computation

Minimal embedding degree

Observation:
k is minimal with $\ell \mid q^k - 1$, so final exponentiation $T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell}$ removes all terms from subfields.

- Choose $R \in E(\mathbb{F}_q)$, computation of $l(R)$ and $v(R)$ not needed.
- Choose $R = P_\infty$,

$$\tilde{T}_\ell(P, Q) = F_{P-P_\infty}(Q)^{(q^k-1)/\ell}.$$

- If protocol allows and k even, choose $Q = (x_Q, y_Q) \in \mathbb{F}_{q^k}$ with x in subfield, this avoids computation of $v(Q)$. This means no extra division!
- Same works for hyperelliptic curves.

Improvements to Miller

Observation:
Let $N = c\ell$ for some c, then

$$\tilde{T}_\ell(P,Q) = T_\ell(P,Q)^{(q^k-1)/\ell} = T_N(P,Q)^{(q^k-1)/N}.$$

- Other addition chains can be used in Miller's algorithm, e.g. NAF.
  Other bases might be good depending on characteristic of the field.
- Use multiple N with low Hamming weight (in p-adic representation).
  For supersingular curves choosing N as number of points gives fast final exponentiation.
- Same works for hyperelliptic curves.

Special curves

- Duursma-Lee and Barreto-Galbraith-ÓhEigeartaigh-Scott obtain further speed-up by choosing supersingular curves of genus $(p-1)/2$ over $\mathbb{F}_{p^r}$.

  Main ideas are to use p as basis in addition chain $\Rightarrow$ much shorter chain and take into account that each order divides p^r+1.
- Generalization and further speed up on other supersingular curves: “eta-pairing” and “eta-T-pairing”.
- ePrint 2006/110 by Hess, Smart, and Vercauteren introduces ate-pairing which does loop shortening for ordinary curves, fast for curves with CM by $\sqrt{-3}$.
- Scott (Indocrypt’05) studies endomorphisms to speed up pairing on ordinary elliptic curves (GLV approach).

Special divisors (joint work with G. Frey)

- Useful if no map $\mathrm{Pic}^0_C(\mathbb{F}_q) \mapsto \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ given.
- Katagi, Kitamura, Akishita, and Takagi suggested to use special divisor classes $\bar{D} = P - P_\infty$ as basis for DL system, also for $g > 1$
  $\Rightarrow$ additions involving special divisor much cheaper.
- For pairings on HEC already suggested in Duursma-Lee, but no justification of this choice.
- Use subset of special divisor classes in $\mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ as second argument of the pairing – or even restricted to points P with x-coordinate in subfield (if k is even).
- Evaluation of functions only in one point much faster.
- Speed-up grows with genus!
- For non-degeneracy etc. see ANTS 2006 proceedings.

Embedding degree

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.

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 (cf. following slide).

Parameter sizes

- Balance security: in G_1 only generic square-root attacks, in finite fields index calculus.
- Common requirement $|(\mathbb{F}_q)| \sim q$: 160 bits, q^k: 1024 bits.
- Optimal embedding degree would be $k = 1024/160 = 6.4$.
- Difference between sizes grows $\Rightarrow$ larger k becomes optimal; maybe revive $g = 4$ (Frey/L. 2006).
- $k = 6$ & supersingular only for small characteristic ($q = 3^r$ for $g = 1$, $q = 2^r$ for $g = 2$) $\Rightarrow$ slower field arithmetic & faster index calculus methods (function field sieve) $\Rightarrow$ asymptotically the field size must be twice as large for small characteristic.
- Page, Smart, and Vercauteren "A comparison of MNT curves and supersingular curves" (2004).

MNT curves

Find ordinary curves with small embedding degree! Thus force

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

- First proposal: Miyaji, Nakabayashi & Takano (2001).
- Other approach: Cocks and Pinch (unpublished, 2002).
- Dupont, Enge & Morain: small k by CM
- Barreto, Lynn, Scott: Curves for $k = 3, 4$ and 6.
- Generalization to co-factors, $k = 5, 10, 12$ Galbraith, McKee & Valença.
- Brezing & Weng $k \leq 60$ (in steps), often large co-factor.
- Family of curves with $k = 12$ by Barreto and Naehrig.
- Family of curves with $k = 10$ by Freeman.

Supersingular vs. ordinary

Supersingular:

- pro: known, speed ups by choosing $N = c\ell$, eta-T-pairing, distortion maps
- con: only small k, either small characteristic or far too large field size for ground field $k = 2$, small number of curves

Ordinary:

- pro: can be used over prime fields, more and larger embedding degrees possible, more (but also finite) choice, ate-pairing, speed-up for hyperelliptic curves.
- con: most cases (in practical use) no distortion maps, no reason why good multiple N should exist.

Open problems so far

- speed up the computation,
- find more MNT curves:
  - larger extension degrees (not too large, though)
  - more families
  - smaller co-factors
  - real challenge to find hyperelliptic curves
- Study exact speed-security tradeoff for genus 4 curves.
- Break system???
- Break weaker security assumptions (see following slides).

Great collection at
P. S. L. M. Barreto, “The Pairing-Based Crypto Lounge”
`http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`

Security Assumptions Revisited

Big open problem:
Update Joux'2002 and give taxonomy of pairing-related assumptions

Tried and failed to do it for this talk. Quite a volume of assumptions; more a master thesis topic

Decisional DH Problem

- If $G_1 = G_2$, i.e. if a distortion map exists from G_1 to G_2 then the DDHP is easy in G_1.
- E is supersingular, usual setting $k > 1$, $G_1 = E[\ell](\mathbb{F}_q)$ and $\ell^2 \nmid |E(\mathbb{F}_q)|$. Then we can always find distortion maps into G_2.
- E is ordinary:
  - $G_2 = \langle [a]P \oplus [b]Q \rangle, a, b \neq 0$. Tr is distortion map from G_2 to G_1. Then the modified pairing has $\mathrm{Tr}(S) \times S$ as domain.
  - No maps for $G_1 = \langle P \rangle$. (One would have to come up with consistent multiples of Q to map the DDHP in G_1 to the DDHP in $\langle [a]P \oplus [b]Q \rangle$.)
  - Similarly no hope for $G_2 = \langle Q \rangle$.

co-DH Problem

- G_1, G_2 groups of same prime order ℓ.
- $P_1 \in G_1, Q \in G_2$.
- Distinguish distributions

$$(P, [a]P, Q, [a]Q) \text{ from } (P, [a]P, Q, [c]Q).$$

- Possible to build on DDHP.
- Easy to solve if there is an explicit isomorphism between G_1 and G_2.
- In pairings setting one needs to exclude distortion maps.
- Steven D. Galbraith and Victor Rotger, LMS JCM, (7) 201-218 give exact study when co-DDH is easy.

m-strong DH-Problem

- Suggested in Boneh & Boyen, short signatures without random oracles
- The m-SDH problem in (G_1, G_2) is defined as follows: given a $(m+2)$-tuple

  $$(P_1, P_2, [a]P_2, [a^2]P_2, ..., [a^m]P_2)$$

  with $P_1 = \psi(P_2)$, ψ distortion map, output

  $$([1/(a+x)]P_1, x) \text{ for some } x.$$

- Problem phrased in gap DH groups.
- Security reduction to DLP weaker by factor $\sqrt{m}$. Cheon (Eurocrypt'06): actual security reduced in many cases.
- See also Neal Koblitz comments in following talk and his joint paper with Alfred Menezes.

Decision Linear Problem

- Suggested in Boneh, Boyen and Shacham. "Short group signatures"
- Needs bilinear map $G_1 \times G_2 \to G_t$ and distortion map $\psi : G_2 \to G_1$.
- Decision Linear Problem in G_1:
  Given $P, Q, R, [a]P, [b]Q, [c]R \in G_1$ as input, output yes if $a + b = c$ and no otherwise.
- Solving Decision Linear Problem implies solving DDH. The converse is believed to be false.
- Could be an interesting assumption in pairing friendly groups G_1.
- Open Problem:
  Find out whether Decision Linear Problem is harder than DDH or not.

External Diffie-Hellman (XDH)

- Suggested in L. Ballard, M. Green, B. de Medeiros, and F. Monrose: “Correlation-resistant storage”, 2005 and G. Ateniese, J. Camenisch, and B. de Medeiros: “Untraceable RFID tags via insubvertible encryption” ACM CCS, 2005.
- The XDH assumption is that there exists a bilinear map

  $$G_1 \times G_2 \to G_t$$

  and DDH is hard in G_1 and G_2. This is also referred to as Symmetric XDH.
- The Asymmetric XDH assumption requests only DDH hard in G_1.
- Instantiations are possible in non-supersingular curves; see discussion of Galbraith/Rotgers paper.

Generalization: Different DDH Problems

- Very nice overview in: N.P. Smart and F. Vercauteren: "On Computable Isomorphisms in Efficient Pairing Based Systems", To appear Discrete Applied Mathematics. (See also Nigel's talk at ECC 2006.)
- Study assumes bilinear map.
- Their paper discusses possible instantiations of the DDH problems in relations to ID-based signatures.
- Lays out possibilities of hardness assumptions for proofs (DDH in G_1, G_2 or G_T and combinations thereof).
- Their paper stresses importance of distortion maps in security proofs.
- Open Problem:
  Give the proofs without distortion maps.

Pairing Inversion Problem I

- Given $P \in G_1, z \in G_T$ find $Q \in G_2$ with $e(P,Q) = z$ (or given Q find P.)
- Sometimes stated with $G_1 = G_2$.
- Computability would imply DDH in G_T.
- Sometimes allowing the attacker to choose P and Q, i.e. given z find P, Q with $e(P,Q) = z$.
- Proposed by E. Verheul, defending XTR.
- Q. Chen, S. Uchiyama (CT-RSA 2002) try lifting DHP in $\mathbb{F}_q^*$ to supersingular curve and further to number field; hope to find a reduction with computable Tate Pairing. Aim: attack DHP in $\mathbb{F}_q^*$.
- Koblitz/Menezes (Math. Comp. 2004) show that existence of computable lifted curve is unlikely.

Pairing Inversion Problem II

- Evidence for hardness of this assumption (as good as it gets)
  - T. Satoh: "Some Remarks on Polynomial Interpolation Related to ECC", WCC 2005 and post-proceedings, studies complexity of pairing inversion.
  - Pairing Inversion Problem mentioned in S. Galbraith, C. ÓhEigeartaigh, C. Sheedy, ePrint 2006/169; they try to attack it via multivariate methods.
- cf. also following talk by Yvo Desmedt (IPAM 2006).
- Open Problem:
  Study hardness of Pairing Inversion Problem.