Easy decisions: Applications of pairings in cryptography

Steven Galbraith
Royal Holloway University of London
http://www.isg.rhul.ac.uk/~sdg/

This is a survey of work on applications of pairings in cryptography. I will present the work of various researchers, including some joint work with J. McKee, V. Rotger and P. Valença.

1 Contents

- DDH problems
- Pairings
- Curves with small embedding degree
- Applications of pairings
- Distortion maps
- Constructing distortion maps

2 The elliptic curve decision Diffie-Hellman problem (ECDDHP)

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let l be a large prime such that $l | \#E(\mathbb{F}_q)$. As usual we define

$$E[l] = \{P \in E(\overline{\mathbb{F}}_q) : [l]P = 0_E\}.$$

Let $P = (x, y) \in E[l]$ and let $P_1 = [a]P$, $P_2 = [b]P$ and $P_3 = [c]P$ be given points on E. The **ECDDH** is to decide whether

$$c \equiv ab \pmod{l}.$$

Let $P_1 = [a]P$, Q, $Q_1 = [c]Q \in E[l]$. The **co-ECDDH** is to decide whether

$$c \equiv a \pmod{l}.$$

3 The Weil pairing

With notation as above (i.e., $l | \# E(\mathbb{F}_q)$) define k to be the smallest positive integer such that $l | (q^k - 1)$. Note that k depends on q and l. The number k is sometimes called the **embedding degree** (or MOV degree or security multiplier).

Define $\mu_l = \{\zeta \in \mathbb{F}_{q^k}^* : \zeta^l = 1\}$. The **Weil pairing** is a function

$$e_l : E[l] \times E[l] \to \mu_l \subset \mathbb{F}_{q^k}^*$$

which satisfies the following properties:

- (Bilinear) $e_l(P_1 + P_2, Q) = e_l(P_1, Q) e_l(P_2, Q)$ and $e_l(P, Q_1 + Q_2) = e_l(P, Q_1) e_l(P, Q_2)$.
- (Non-degenerate) $e_l(P, Q) = 1$ for all $Q \in E[l]$ implies $P = 0_E$.
- (Alternating) $e_l(P, P) = 1$ for all $P \in E[l]$.

4 The Tate-Lichtenbaum pairing (special case)

Let $K = \mathbb{F}_{q^k}$. The **Tate-Lichtenbaum pairing** is a function

$$E(K)[l] \times (E(K)/lE(K)) \longrightarrow K^*/(K^*)^l.$$

For $P \in E(K)[l]$ and $Q \in E(K)$ we write this equivalence class representative as

$$\langle P, Q \rangle \in K^*/(K^*)^l.$$

Note that:

- $(K^* : (K^*)^l) = l$.
- Denote by $\equiv$ equivalence in $K^*/(K^*)^l$.
- $E(K)/lE(K)$ is a group of exponent l.

The Tate-Lichtenbaum pairing satisfies the following properties:

- (Bilinear) $\langle P_1 + P_2, Q \rangle \equiv \langle P_1, Q \rangle \langle P_2, Q \rangle$ and $\langle P, Q_1 + Q_2 \rangle \equiv \langle P, Q_1 \rangle \langle P, Q_2 \rangle$. Hence $\langle [n]P, Q \rangle \equiv \langle P, [n]Q \rangle \equiv \langle P, Q \rangle^n$.
- (Non-degenerate) If $\langle P, Q \rangle \equiv 1$ for all $Q \in E(K)$ then $P = 0_E$.
- Not necessarily alternating.
  But one can show that if $P \in E(\mathbb{F}_q)$ and $l \not| (q-1)$ (i.e., if $k > 1$) then
  $$\langle P, P \rangle \equiv 1.$$
- A unique value of the Tate-Lichtenbaum pairing can be obtained by raising to the power
  $$(q^k - 1)/l.$$

5 MOV/Frey-Rück attack

To solve an elliptic curve discrete logarithm problem $Q = [\lambda]P$ where P has order l in $E(\mathbb{F}_q)$ do the following:

- Construct the field $K = \mathbb{F}_{q^k}$ such that $l|(q^k - 1)$.
- Find an auxiliary point $S \in E(K)$ such that $\langle P, S\rangle \not\equiv 1$.
- Compute $\zeta_1 = \langle P, S\rangle$ and $\zeta_2 = \langle Q, S\rangle$.
- Solve the discrete logarithm problem in K^* (or a subfield) using an index calculus method (performing linear algebra modulo l).

This strategy is effective when $K = \mathbb{F}_{q^k}$ is not too large an extension of $\mathbb{F}_q$.

6 Supersingular curves

An elliptic curve E over $\mathbb{F}_{p^n}$ is **supersingular** if and only if $\#E(\mathbb{F}_{p^n}) \equiv 1 \pmod{p}$.

Theorem (Menezes-Okamoto-Vanstone): If E is supersingular then $k \leq 6$.

Theorem (Galbraith): If A is a supersingular abelian variety of dimension 2 then $k \leq 12$.

7 Other curves with small k

Miyaji-Nakabayashi-Takano gave families of ordinary elliptic curve group orders with $k = 3, 4, 6$.
Example: Family with $k = 6$. Let $q = 4l^2 + 1$, $t = 1 \pm 2l$. Then can check that

$$(q + 1 - t) \mid (q^2 - q + 1) = \Phi_6(q)$$

where $\Phi_k(q)$ is the k-th cyclotomic polynomial.

These ideas have been extended to the case of cofactors by Galbraith, McKee and Valença (also by Scott and Barreto). Listed below are some families with $(q + 1 - t) = hr$ where h is a small cofactor and

$$r \mid (q^2 - q + 1).$$

h	q	t
2	$8l^2+6l+3$	$2+2l$
2	$8l^2+10l+5$	$-2l$
2	$24l^2+6l+1$	$-6l$
2	$24l^2+24l+19$	$6+6l$
3	$12l^2+4l+3$	$1-2l$
3	$12l^2+20l+11$	$3+2l$
3	$84l^2+16l+1$	$-1-14l$
3	...	...

Families for genus 2

Probabilistic arguments show the existence of genus 2 curves with moderate embedding degree (suitable candidates are $k = 5, 8, 10, 12$). Experiments suggest that parameterised families do not exist in general. The only ordinary family we have found is for $k = 10$. The family has

$$q = 11l^2 + 10l + 3$$

and

$$n = q^2 + a_1 q + a_2 + a_1 + 1$$

where $a_1 = l$ and $a_2 = 2l + 1$. One can check that

$$n(l) = 11m(l) \text{ where } m(l) \mid (q(l)^4 - q(l)^3 + q(l)^2 - q(l) + 1).$$

Since, in general, $\gcd(a_1, q) = 1$ the curves are not supersingular.

In any case, we have seen that there are a number of ways to obtain curves over finite fields with small embedding degree k. Hence:

$$\boxed{\textbf{from now on suppose } k \textbf{ is small.}}$$

8 Pairings solve subgroup membership (Miller)

Lemma: $P, Q \in E[l]$ then $Q \in \langle P \rangle$ if and only if $e_l(P, Q) = 1$.
Proof: Choose $S \in E[l]$ such that $\{P, S\}$ forms an $\mathbb{F}_l$-basis for $E[l]$. If $e_l(P, S) = 1$ then

$$e_l(P, [a]P + [b]S) = 1$$

for all a, b. But this contradicts non-degeneracy. Hence $e_l(P, S) = \zeta_l \neq 1$. Now write $Q = [a]P + [b]S$. Then $e_l(P, Q) = \zeta_l^b$ and the result follows. □

Note: The Tate-Lichtenbaum pairing is not necessarily alternating, so the lemma may not be true for Tate-Lichtenbaum pairing.

9 Pairings solve co-ECDDH

Suppose that $K = \mathbb{F}_{q^k}$ is not too big an extension of $\mathbb{F}_q$ and suppose that

$$\langle P, Q \rangle \not\equiv 1.$$

Then $c \equiv a \pmod{l}$ if and only if

$$\langle P, [c]Q \rangle \equiv \langle [a]P, Q \rangle.$$

Hence, all genuine co-ECDDH problems (i.e., where the points P and Q are independent) are easy when k is small.

10 Some applications of pairings

- Identity-based encryption (Sakai-Ohgishi-Kasahara, Boneh-Franklin)
- Identity-based key exchange (Sakai-Ohgishi-Kasahara, Smart)
- Short signatures (Boneh-Lynn-Shacham)
- Many more . . .

11 Short signatures (Boneh-Lynn-Shacham)

The following public key signature protocol can be applied whenever the decision Diffie-Hellman problem is easy.

Public key: $Q = [a]P$.
Sign m**:** $S = [a]H(m)$ where $e(P, H(m)) \neq 1$.
Transmit: x-coordinate of S.
Verify: Recover $\pm S$ and test whether

$$e(H(m), Q) \stackrel{?}{=} e(\pm S, P).$$

Note: Group order is odd so cannot handle ± by computing the square of the ratio of the pairing values.

Security of short signatures

Security against forgery in the passive case depends on ECDH (sometimes called Gap-DH in this context).

Security against adaptive adversaries can be proved in the random oracle model. But adaptive security requires a computable homomorphism (i.e., a distortion map) φ from the subgroup containing public keys to the subgroup containing the hash values. This requirement is essential, as the following example shows.

Example (BLS)

Let $G_1 = (\mathbb{Z}_l, +)$ and $G_2 = (\langle g \rangle, \cdot)$ of order l. Consider the pairing $G_1 \times G_2 \to G_2$ given by

$$e(x, y) = y^x.$$

The co-ECDH problem in $G_2 \times G_1$ is: Given $(g, h = g^x, a)$ compute xa.
Public key: $h = g^x$.
Sign: $s = xH(m) \in \mathbb{Z}_l$.
Verify: $e(H(m), h) \overset{?}{=} e(s, g)$.

Problem: A single message-signature pair (m, s) reveals the private key.
Note: In this case the map $\varphi : G_2 \to G_1$ is the discrete logarithm map.

12 What about ECDDH problems?

We have seen how pairings solve co-ECDDH. The Weil pairing is alternating so $e_l(P, P) = 1$. Hence we can't use the Weil pairing directly to solve ECDDH problems. For the Tate-Lichtenbaum pairing, in general $\exists P$ such that $\langle P, P \rangle \equiv 1$.

13 Non-rational endomorphisms (Verheul)

Let P and Q be points such that $\langle P, Q \rangle \equiv 1$. An endomorphism φ of E such that

$$\langle P, \varphi(Q) \rangle \not\equiv 1.$$

is called a **distortion map**. Note that φ depends on P and Q. For cryptographic applications, we often use the modified pairing

$$e(P, Q) = \langle P, \varphi(Q) \rangle^{(q^k - 1)/l}.$$

As we have seen, these are important in cryptography both as a tool for constructing non-degenerate pairings, and as a tool in security proofs.

14 Examples

(I) Consider the elliptic curve

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

which is supersingular over $\mathbb{F}_p$ when $p \equiv 3 \pmod 4$. The distortion map is

$$\varphi(x, y) = (-x, iy)$$

where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. In this case $\#E(\mathbb{F}_p) = p+1$ and the embedding degree is $k = 2$.

(II) The elliptic curves

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

over $\mathbb{F}_2$ (where $a = 0, 1$) have $k = 4$. Non-rational endomorphism

$$\varphi(x, y) = (\zeta_3 x + s^2, y + \zeta_3 s x + s)$$

where $\zeta_3^3 = 1$ and $s^2 + \zeta_3 s + 1 = 0$. We can work over $\mathbb{F}_{2^m}$ for certain values of m.

(III) The elliptic curves

$$E : y^2 = x^3 - x \pm 1$$

over $\mathbb{F}_3$, have $k = 6$. Non-$\mathbb{F}_3$-rational endomorphism

$$\varphi(x, y) = (\alpha - x, iy)$$

where $i^2 = -1$ and $\alpha^3 - \alpha \mp 1 = 0$. We can work over $\mathbb{F}_{3^m}$ for certain values of m.

(IV) The elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

has complex multiplication of discriminant -7. Deuring reduction theory implies that E is supersingular over $\mathbb{F}_p$ when $(\frac{-7}{p}) = -1$. The order $\mathbb{Z}[(1+\sqrt{-7})/2]$ does not have non-trivial units, hence unlike the previous examples we cannot have a distortion map which is an automorphism of the curve.

Using Vélu's formulae we can find a 2-isogeny $\phi : E \to E$ defined over $\mathbb{F}_{p^2}$. The x-coordinate of $\phi(x, y)$ is

$$\frac{-3+\sqrt{-7}}{8} x + \frac{(-63 - 35\sqrt{-7})/16}{8x + 5 + \sqrt{-7}} + \frac{11 - \sqrt{-7}}{32}.$$

Note that this example will show that our algorithm is not optimal (since it would construct the 7-isogeny coming from $\sqrt{-7}$ in this case).

15 Trace map

Denote by π the q-power Frobenius map. Let $P \in E(\mathbb{F}_{q^k})$ where $k > 1$. Define the **trace** (where the $\sum$ represents addition on the elliptic curve E)

$$\mathrm{Tr}(P) = \sum_{i=1}^{k} \pi^i(P) \in E(\mathbb{F}_q).$$

The trace map is a group homomorphism.

Lemma: (Boneh) Let $P \in E(\mathbb{F}_{q^k})[l]$ such that $P \neq 0_E$. Then $e_l(P, \mathrm{Tr}(P)) = 1$ if and only if P is an eigenpoint for π.

Note: It is enough to just use π, and this is more efficient to compute than $\mathrm{Tr}(P)$.

16 Which ECDDH problems are easy?

For elliptic curves with small k, all co-ECDDH problems are easy due to the Weil pairing. Similarly, the trace map means all ECDDH problems are easy except for the two π-eigenspaces.

For ordinary (non-supersingular) curves it seems the two Frobenius eigenspaces give hard ECDDH problems.

Theorem: (Verheul/Schoof) Let E be supersingular and let $P \in E(\mathbb{F}_{q^k})[l]$. Then there is a distortion map ψ which makes the ECDDH problem in $\langle P \rangle$ easy.

Proof: (sketch) Let $K = \mathbb{F}_{q^k}$. If E is supersingular then $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a 4-dimensional $\mathbb{Z}_l$-module which is isomorphic to the $\mathbb{Z}_l$-module $\mathrm{Hom}_K(T_l(E))$ of homomorphisms which commute with q^k-power Frobenius.

Since E is supersingular the Frobenius over K is an integer and it follows that

$$\mathrm{Hom}_K(T_l(E)) \cong M_2(\mathbb{Z}_l).$$

Hence $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong M_2(\mathbb{Z}_l)$ and, by restriction, we have

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}/l\mathbb{Z} \cong M_2(\mathbb{Z}/l\mathbb{Z}).$$

For any $P \in E[l]$ there is some $\Psi \in M_2(\mathbb{Z}_l)$ which maps P outside $\langle P \rangle$, so the preimage of Ψ under this map suffices. $\square$

17 Constructing distortion maps (1)

Theorem: (Galbraith-Rotger) Let E/F be an elliptic curve with CM of discriminant D in characteristic zero which has supersingular reduction modulo p to $\tilde{E}/\mathbb{F}_{p^m}$. Let π be the p^m-power Frobenius. Suppose $\mathbb{Q}(\sqrt{D}) \not\subset F$. Let $d \in \mathbb{N}$ and $\Psi \in \mathrm{End}(E)$ such that $\Psi^2 = -d$. Then $\psi = \Psi \pmod{p}$ is a suitable distortion map for any π-eigenpoint $P \in \tilde{E}(\overline{\mathbb{F}}_p)$ of order coprime to $4pd$.

Proof: (sketch) Let $H = F(\sqrt{D})$, let σ be the non-trivial element of $\mathrm{Gal}(H/F)$ and reduce everything modulo p. Then $\psi^\sigma = -\psi$.

We have $\mathrm{End}(\tilde{E}) = B$ a quaternion algebra. We are in the case $k = 2$ so $\pi^2 = -p^m$ and so $\overline{\pi} = -\pi$ and $\overline{\psi} = -\psi$.

By the Skolem-Noether theorem, the action of σ on the quaternion algebra $B = \mathrm{End}(\tilde{E}) \otimes \mathbb{Q}$ is conjugation by some $\gamma \in B$. Clearly, $\pi\gamma = \gamma\pi$ and so $\gamma \in \mathbb{Q}(\pi)$. Also, $\psi\gamma = -\gamma\psi$. Hence,

$$\mathrm{Tr}(\pi\psi) = -\mathrm{Tr}(\gamma)\psi.$$

and so $\mathrm{Tr}(\gamma) = 0$. Hence $\gamma = u\pi$ for some $u \in \mathbb{Q}^*$. Thus $\psi\pi - \pi\psi = 2\psi\pi$ has degree $4p^m d$.

Suppose P is an eigenpoint with $\pi(P) = [m]P$ of order coprime to $4pd$. Then $\pi\psi(P) \neq \psi\pi(P)$ and in fact $\pi(\psi(P)) = -\psi(\pi(P)) = [-m]\psi(P)$. Hence, ψ maps P outside $\langle P \rangle$. □

18 Constructing distortion maps (2)

The following algorithm (due to Galbraith and Rotger) constructs a distortion map for a known CM curve with supersingular reduction. We imagine the algorithm being used by a builder of a cryptosystem in the case where the known examples of CM curves (and distortion maps) are not suitable.

Input: $\tilde{E}/\mathbb{F}_q$ with known $\mathcal{O} \subseteq \mathrm{End}(\tilde{E})$.

1. Compute an integer d such that $\sqrt{-d} \in \mathcal{O}$.
2. Factor $d = \prod_{i=1}^{n} l_i$ (not necessarily distinct primes).
3. Starting from $j(\tilde{E})$ construct graph of j-invariants by taking l_i-isogenies (factoring l_i-th modular polynomial) for $i = 1, \ldots, n$.
4. Find a cycle in the graph corresponding to the d-isogeny ψ from $\tilde{E})$ to itself. Hence construct ψ using methods of Elkies and Vélu.

The complexity is roughly $O(h^6)$ where h is the class number of the the order $\mathcal{O}$.

The only known efficient way to construct supersingular curves is using reduction of CM curves in characteristic zero. Since these algorithms are of exponential complexity, we can only construct CM curves whose class number is bounded by a polynomial function. Hence, when the input is restricted to these curves then our algorithm has polynomial complexity.

Performance

But the complexity $O(h^6)$ is very poor. For example, it is feasible to generate curves using the CM method with $h \approx 2^{20}$. Whereas 2^{120} operations is slower than Pollard methods to solve the discrete logarithm problem for a 160-bit elliptic curve.

The algorithm given above usually does not construct a distortion map of minimal degree (e.g., the example with $D = -7$ above gave a 2-isogeny whereas the algorithm would give a 7-isogeny). Ad-hoc methods can usually be used to compute a distortion map of lower degree and in much faster time.

Comments on the case of genus two

Let C be a genus 2 curve over $\mathbb{F}_q$. Consider the DDH problem in the divisor class group of C. Suppose the embedding degree k is small. In general, the torsion is 4-dimensional and so it does not follow that all co-DDH problems are easy. Similarly, the trace map is no longer sufficient for divisors which do not lie in an eigenspace.

The proof of Verheul/Schoof easily generalises. The algorithm for constructing distortion maps does not generalise.