ROYAL HOLLOWAY, UNIVERSITY OF LONDON

Information Security Group

Hidden pairings and trapdoor DDH groups

Alexander W. Dent

Joint work with Steven D. Galbraith

Pairings in cryptography

- Elliptic curves have become an important tool in cryptography…
- …and pairings have become an important tool within elliptic curve cryptography, both as an attack technique and to provide extra functionality.
- The main use is to solve the DDH and DL problems in large prime-order subgroups.

Pairings in cryptography

- High security pairing-based cryptography (Granger, Page and Smart)
- Constructing pairing-friendly curves of embedding degree 10 (Freeman)
- Fast bilinear maps from the Tate-Lichtenbaum pairing on hyperelliptic curves (Frey and Lange)

Pairings in cryptography

- In this paper we will be mostly concerned with the decisional Diffie-Hellam (DDH) problem:

> Let G be a group generated by an element P.
>
> The DDH problem is to determine, given (A,B,C), where A=aP, B=bP, whether C=cP or C=abP, when a, b and (potentially) c are chosen at random.

Pairings in cryptography

- In all normal situations, when a pairing is computable, the pairing algorithm is comparatively obvious given the curve description.
- We conjecture that there exist elliptic curve groups on which a pairing can only be computed given some extra trapdoor information.
- We call these *hidden pairings*.

Pairings in cryptography

- A hidden pairing is an instantiation of a trapdoor DDH group: a group on which the DDH problem can only be efficiently solved by an algorithm with the trapdoor information.
- We also conjecture the existence of trapdoor discrete logarithm groups.

First construction

First construction

- Let p and q be large primes.
- Let E: $y^2 = x^3 + ax + b$ be an elliptic curve such that $E(F_p)$ and $E(F_q)$ both have a small embedding degree.
- Hence, there exist a public pairing algorithm for $E(F_p)$ and $E(F_q)$.
- Suppose further than $\#E(F_p)$ and $\#E(F_q)$ have large prime divisors r and s.

First construction

- Now consider the elliptic curve E over the ring Z_N where $N=pq$.
- Clearly, group operations are efficient.
- $E(Z_N)$ contains a cyclic subgroup of order rs.
- The security of elliptic curves over rings has been studied by Galbraith and McKee in "Pairings on elliptic curves over finite commutative rings".

First construction

Yes?

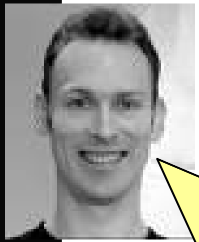
First construction

- There is no evidence to suggest that, without knowing (a multiple of) *rs*, that we can compute pairings on this subgroup.
- If *r* and *s* are large enough, then knowledge of *rs* is enough to factor *N*.
- However, knowledge of (a multiple of) *rs* is sufficient to be able to compute a pairing.

First construction

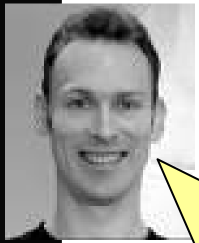
- So, if we know $\#E(F_p)$ and $\#E(F_q)$, then we can compute pairings because *rs* divides $\#E(F_p)\#E(F_q)$.
- Alternatively, we can solve the DDH problem by projecting the points of the curve $E(Z_N)$ onto $E(F_p)$ and $E(F_q)$ and solving these two problems individually.
- Hence, we can solve the DDH problem if we know *p* and *q*.

First construction



- Take p and q to be large primes congruent to 3 mod 4 for which there exists large prime divisors of r and s of $p+1$ and $q+1$.
- Take E: $y^2 = x^3 + x$.
- Then E is a supersingular curve over F_p with embedding degree 2 and $p+1$ points.
- And $\#E(F_p)$ has the large prime divisor r.

First construction



- This means that $\#E(Z_N) = (p+1)(q+1)$.
- If we know p and q then we can compute pairings because rs divides into $(p+1)(q+1)$.
- Hence we have a hidden pairing.
- We can also solve the DDH problem on $E(Z_N)$ by solving two DDH problems on $E(F_p)$ and $E(F_q)$.

First construction

- What about the practicalities of cryptography:
  - We can hash into the group by using the techniques of Demytko, i.e. we use the x-coordinate only and use a standard hash algorithm to map an arbitrary string to an element of Z_N.
  - We can use similar techniques to randomly sample elements from the group.
  - The DDH problem has to be generalised in this case, but it's not difficult.
  - Points will be of size $\log N \approx 1024$-bits.

First construction

- Our example also a cute property:
- We can delegate the ability to compute a pairing to a third party by releasing *rs* without giving away the factorisation of *N*.
- Obviously, in this case we want *r* and *s* to be large enough so that we can't break the system, but not so large that knowledge of *rs* implies knowledge of *p* and *q*.

Second construction

Second construction

- This time we consider an elliptic curve E over a finite field F_q of characteristic 2.
- In particular, we want q to be equal to 2^{mn}.
- We also want there to exist an efficiently computable pairing on the elliptic curve.
- We will represent points on E using projective coordinates $(x{:}y{:}z)$.
- And we will ~~steal~~ adapt an idea of Frey's.

Second construction

- We may think F_q as a vector space of dimension n over the field $F_{q'}$ where $q'=2^m$.
- Hence, we may think of points as $3m$-tuples:

$$(x_0,x_1,\ldots,x_{m-1},y_0,y_1,..y_{m-1},z_0,z_1,\ldots,z_{m-1})$$

- We may think of the doubling formula as a series of $3m$ formulae (fx_i,fy_i,fz_i) in $3m$ variables such that if $(x':y':z')=[2](x:y:z)$ then

$$x'_i = fx_i(x_0,x_1,\ldots,x_{m-1},y_0,y_1,..y_{m-1},z_0,z_1,\ldots,z_{m-1})$$

Second construction

- Each of these formulae are homogeneous polynomials of degree at most six.

- We can do the same thing to the addition formula to get 3*m* formulae in 6*m* variables, (gx_i,gy_i,gz_i).

Second construction

- Now we apply Frey’s idea of disguising an elliptic curve.
- Let *U* be an invertible linear transformation on 3*m*-variables.
- We apply U to the point of $E(F_q)$.
- Note that we can express the addition and doubling formulae in this new system as

$$fx'_i = U\, fx_i\, U^{-1} \qquad \text{and} \qquad gx'_i = U\, gx_i\, U^{-1}$$

Second construction

- Public group description:
  - Blinded doubling and addition formulae
  - Blinded generator $U(P)$
  - The order r of the point P
- Trapdoor information:
  - The inverse transformation U^{-1}
- Difficult to hash onto the group, sample group elements at random or even test for equality.

Second construction

- Wow, this all seems very dodgy!
- It is easy to break for finite fields and the algebraic torus T_2.
- "Disguising tori and elliptic curves" (http://eprint.iacr.org/2006/248)
- It's also related to the isomorphism of polynomials problem.
- Faugère and Perret's result from Eurocrypt 2006 suggests parameter sizes have to be so large as to be infeasible in practice.

Applications

Applications to cryptography

- Not as many as one would like.
- If trapdoor to be used by an individual, that individual must compute the group description.
- We give a few simple examples in the paper.
- Perhaps useful for a situation with a central authority that generates a group description on behalf of a set of users.
- Group signatures?

Applications to cryptography

- Applications to the Gap-DH problem?
- Most people assume that the Gap-DH problem is hard on any group for which the CDH problem is hard.
- Not proven when the DDH problem is hard.
- Our results *do not* necessarily give new gap groups.
- However, most proofs can be easily adapted.

Questions?

First construction

Wow, that's a great question.

First construction

I’m not sure what the answer is right now,
But why don’t you pop it in an e-mail and
I’ll think about and get back to you.

You might want to CC Alex on the e-mail too.

First construction

Oh that’s an easy question.
The answer’s ‘yes’.
Or, in certain circumstances, ‘no’.
Hmmm. Maybe it’s not as easy as I thought.

Why don’t you e-mail it to me?