Recent Work on Weil Descent

Various bits and bobs from work of

- G. Frey
- S. Galbraith
- F. Hess
- P. Gaudry
- G. Seroussi
- N. Smart

Story so far...

ECC is being deployed.

People want ECC to be fast.

But we also require interoperability.

People choose special fields to make stuff run faster.

$$\mathbb{F}_p, \mathbb{F}_{2^p} \text{ or } \mathbb{F}_{q^n}.$$

$\mathbb{F}_{q^n}$ is very efficient.

But standards bodies have gone for $\mathbb{F}_p$ and $\mathbb{F}_{2^p}$, after advice from NSA.

There is a **business need** to get rid of $\mathbb{F}_{q^n}$ once and for all.

But people keep proposing such fields....

G. Frey at talk in Waterloo mentioned **Weil descent**.

Uses this to hide an elliptic curve.

Mentions could produce some weak curves.

This is not enough for engineers to change their minds.

More evidence needed, and in a low brow format.

Weil Descent

Let $q = 2^l$, $K = \mathbb{F}_{q^n}$, $k = \mathbb{F}_q$.

$$E : Y^2 + XY = X^3 + \alpha X^2 + \beta$$

with $\alpha, \beta \in K$.

K has k-basis

$$\{\psi_0, \psi_1, \dots, \psi_{n-1}\}$$

We set

$$\begin{aligned} \alpha &= a_0\psi_0 + a_1\psi_1 + \ldots + a_{n-1}\psi_{n-1}, \\ \beta &= b_0\psi_0 + b_1\psi_1 + \ldots + b_{n-1}\psi_{n-1}, \\ X &= x_0\psi_0 + x_1\psi_1 + \ldots + x_{n-1}\psi_{n-1}, \\ Y &= y_0\psi_0 + y_1\psi_1 + \ldots + y_{n-1}\psi_{n-1}, \end{aligned}$$

Expand and equate coefficients of ψ_i.

Obtain an abelian variety A defined over k, this is the **Weil restriction**.

Suppose $\#E(K) = ph$ with p the interesting bit.

There is a subvariety $B \subset A$ with p dividing $\#B$.

In practice this means $\dim B = n - 1$ or n.
Suppose we found a curve C in A such that $Jac(C)$ contains a subgroup isogenous to B.

Then $g = dimJac(C) \geq dimB = n - 1$ or n.
We want $g \approx n$, but such a curve is unlikely to exist.

But if it did, could get group homomorphism:

$$\phi : E(\mathbb{F}_{q^n}) \to Jac_{\mathbb{F}_q}(C)$$

Galbraith and Smart

Suppose $\alpha = 0$ and $\psi = \theta^{2^i}$ with

$$\theta + \theta^2 + \theta^4 + \cdots + \theta^{2^{n-1}} = 1$$

"Obvious" way to produce C is to use the hyperplanes

$$x_0 = x_1 = \cdots = x_{n-1} = x.$$

Obtain a curve

$$\mathfrak{C} : \begin{cases} y_{n-1}^2 + xy_0 + x^3 + b_0 = 0, \\ y_0^2 + xy_1 + x^3 + b_1 = 0, \\ \quad\vdots \\ y_{n-2}^2 + xy_{n-1} + x^3 + b_{n-1} = 0. \end{cases}$$

Eliminate variables and set $y = y_0$ to obtain

$$C : y^{2^n} + x^{2^n-1}y + \sum_{i=0}^{n-1} x^{2^n+2^i} + g(x)$$

with

$$g(x) = \sum_{i=1}^{n} b_i^{2^{n-i}} x^{2^n-2^{n-i+1}}.$$

When $n = 4$ we obtain

$$\begin{aligned} C : y^{16} \ &+\ x^{15}y + x^{24} + x^{20} + x^{18} + x^{17} \\ &+\ b_0 x^{14} + b_3^2 x^{12} + b_2^4 x^8 + b_1^8. \end{aligned}$$

When $b_3 = b_0 + b_1 + b_2$, C is reducible and obtain a component.

$$\begin{aligned} C' : y^8 \ &+\ x^4y^4 + x^6y^2 + x^7y + x^{12} + x^9 \\ &+\ b_0x^6 + (b_2^2 + b_1^2)x^4 + b_1^4. \end{aligned}$$

When **irreducible** C appears to always have genus 8.

When **reducible** C' appears to always have genus 4.

This last point is very worrying for cryptography.

Hence need to do some more work on these curves. Require special computer algebra systems, eg KANT.

Enter **F. Hess**

Go back to the general case

$$E : Y^2 + XY = X^3 + \alpha X^2 + \beta$$

Expand coordinates wrt any basis of K over k.

Intersect with subvariety of values of X which lie in k.

This gives a curve $\mathfrak{C}$, (as above), over k.

We shall now work over K again...

$\mathfrak{C}$ is birationally equivalent over K to $\mathfrak{D}$...

$$\mathfrak{D} : \begin{cases} w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0 = 0, \\ \qquad \vdots \\ w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1}x^2 + \beta_{n-1} = 0. \end{cases}$$

where

$$\begin{aligned} \alpha_i &= \sigma^i(\alpha), \\ \beta_i &= \sigma^i(\beta), \end{aligned}$$

with σ the Frobenius automorphism of K over k.

Let F_i be the splitting field of the i-th equation of $\mathfrak{D}$ over $K(x)$.

We can form the compositum $F = F_0 \cdots F_{n-1}$ over $K(x)$ without ambiguity.

Then $[F : K(x)] = 2^m$.

m is the **magic number**.

After (a complicated) change of variable find that $\mathfrak{D}$ is birationally equivalent to

$$t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad i = 1, \ldots, m-1$$

These equations define extensions L_i of $K(z)$ such that

$$F = F_0 L$$

with $L = L_1 \cdots L_{m-1}$.

Lemma 1. *L satsifies:*

- $[L : K(z)] = 2^{m-1}$.
- *L is a rational function field.*

F is then hyperelliptic over K.
Can show genus $F = 2^{m-1}$ or $2^{m-1} - 1$ over K.

Let F' denote the fixed field of F under σ (Frob. auto.).

Theorem 2. *We obtain*

- *F' is a hyperelliptic function field.*
- *Genus $F' = 2^{m-1}$ or $2^{m-1} - 1$ over k.*
- *$\mathfrak{C}$ has an irreducible reduced component over k having F' as its function field.*

Let H denote the hyperelliptic curve.

We can explicitly construct H (code on my WWWEB site).

Using field theoretic arguments (basically the conorm) can construct group homomorphism

$$\phi : Cl(K(E)) \to Cl(F'),$$

which we can then restrict to degree zero divisors.

So given a ECDLP on $E(K)$ we can

1. Find the magic number m.

2. Determine a hyperelliptic curve H of genus
$$g = 2^{m-1} \text{ or } 2^{m-1} - 1.$$
3. Map the ECDLP over to $Jac_k(H)$ using ϕ.
4. Solve the HCDLP.

This will work as long as g is not too big.

But g cannot be too small either.

Theoretically can solve HCDLP in

$$L_{q^g}(1/2, c)$$

if g is large (Adleman-DeMarrais-Huang).

Other work...

1. **Hafner-McCurley**:
   - Muller, Stein, Thiel.
   - Flassenberg, Paulus.

2. **Function-Field-Sieve**:
   - Galbraith,Paulus,Smart.

Enter **P. Gaudry** (EuroCrypt 2000 paper)

Theorem 3 (Gaudry)**.** *One can solve the HCDLP with*

- *A factorbase of size $O(q)$.*

- *Time*
  $$O\left(g^3 g! q \log^\gamma q\right) + O\left(g^3 q^2 \log^\gamma q\right)$$
  for some fixed integer γ.

One can "optimize" this result to obtain a time estimate of

$$O(q^{2g/(g+1)+\epsilon}) \text{ as } q \to \infty.$$

for fixed g.

So we obtain $O(q^2)$ when $g \geq 4$.

For Weil descent...

n	g	ρ on $E(K)$	Gaudry
2	2	q	$q^{4/3}$
3	3	$q^{3/2}$	$q^{3/2}$
3	4	$q^{3/2}$	$q^{8/5}$
4	8	q^2	$q^{16/9}$
4	7	q^2	$q^{7/4}$
4	4	q^2	$q^{8/5}$

But the method only really works for "small" g.

For very large g need to use the method of ADH.

Unclear where the cross over points are.

But for $g = 4$ we seem to obtain a better attack.

Gaudry's Method

Combines ideas of Pollard and Hafner Mc-Curley.

Want to solve $D_2 = [\lambda]D_1$.

Define multipliers

$$M_i = [r_i]D_1 + [s_i]D_2$$

for $i = 1, \ldots, 20$.

Put $R_1 = M_1$

Compute the random walk

$$R_{i+1} = R_i + M_{h(R_i)}$$

for some hash function h.

We have

$$R_i = [a_i]D_1 + [b_i]D_2.$$

Try to factor R_i over a factorbase of degree one divisors

$$R_i = \sum_{\mathfrak{p}} [t_{\mathfrak{p}}]\mathfrak{p}.$$

Use matrix technique such as Lanczos to find dependence

$$\sum [x_i] R_i = [p] D_3$$

Then put

$$\begin{aligned} A &= \sum a_i x_i \pmod{p}, \\ B &= \sum b_i x_i \pmod{p}. \end{aligned}$$

Then

$$\begin{aligned} \sum [x_i]([a_i]D_1 + [b_i]D_2) &= [A]D_1 + [B][\lambda]D_1 \\ &= [p]D_4 \end{aligned}$$

So $\lambda = -A/B \pmod{p}$.

The Magic Number

Method only bad for curves where

$$g \approx 2^{m-1} \approx n$$

<u>Koblitz Curves</u>

We obtain $m = 1$ so Koblitz curves are safe.

<u>$\mathbb{F}_{2^p}$</u>

At least fifty percent of all such curves have $m = p$.

Easy to compute m in any given example.

<u>$\mathbb{F}_p$</u>

Method does not apply at all.

Lesson

Follow what the standards say.

Constructing Hyperelliptic Cryptosystems

There is no good way to produce HC curves for crypto.

1. **Koblitz Type**:
   Produces curves with automorphisms, Gaudry's method works better.

2. **CM Method**:
   This is dodgy in the EC case, so why use it here.

3. **Schoof**:
   Hard to implement (maybe impossible for curves of interest).

In addition for ECC use curves generated **verifiably at random**.

HC Security Requirements

Want curve H of genus g and order

$$\#Jac_{\mathbb{F}_q}(H) = ph$$

where h is a small cofactor.

- $p > 2^{160}$. (Pollard-rho and BSGS).
- $g < 4$. (Gaudry).
- $q = 2^r$, where r is prime. (Weil descent).
- The smallest $s \geq 1$ such that $q^s \equiv 1 \pmod{p}$ should be greater than 2000. (Frey-Rueck).

Genus Two

Put $K = \mathbb{F}_{q^2}$ with $q = 2^l$, l prime.

Use SEA/Satoh to generate curve

$$E : Y^2 + XY = X^3 + \alpha X^2 + \beta$$

verifiably at random, with group order $2p$.

Apply Weil descent to produce H.

Always (?) $g(H) = 2$.

If $g(H) = 2$ then expect

$$\#Jac_{\mathbb{F}_q}(H) = 2p.$$

Genus Three

Put $K = \mathbb{F}_{q^3}$ with $q = 2^l$, l prime.

Generate $\gamma \in K$ verifiably at random.

Put $\beta = \gamma + \gamma^q$.

Hence $Tr_{K/k}(\beta) = 0$.

Use SEA/Satoh to compute group order of

$$E : Y^2 + XY = X^3 + X^2 + \beta$$

Repeat until group order is $2p$.

Apply Weil descent to produce H.

By choice of β...

Always (?) $g(H) = 3$.

If $g(H) = 3$ then expect

$$\#Jac_{\mathbb{F}_q}(H) = 2p.$$

Conclusions

- Use elliptic curves over $\mathbb{F}_{2^p}$ or $\mathbb{F}_p$.
- Can produce 'secure' hyperelliptic curves in genera 2 and 3.

Future Work ?

- Investigate more in characteristic two.
- Where are exact cross over points.
- Fields of form $\mathbb{F}_{p^n}$.
- Higher genus.
- What if our method fails?