Weak Fields for Elliptic Curve Cryptography

ECC 2003, August 13

Edlyn Teske[1]

Alfred J. Menezes[1] and Annegret Weng[2]

[1] C&O/CACR, University of Waterloo

[2] IEM, Universität Essen-Duisburg

E = **elliptic curve** over finite field $\mathbb{F}_q$.

Elliptic Curve Discrete Logarithm Problem (ECDLP):

Given E, $P \in E(\mathbb{F}_q)$,
$r = \mathrm{ord}(P)$ a large prime
and $Q \in \langle P \rangle$,
find $s \in [0, r-1]$ such that

$$Q = sP \ .$$

Definition: A finite field $\mathbb{F}_q$ is *weak* for ECC if

- For some elliptic curves E over $\mathbb{F}_q$, solving the ECDLP in $E(\mathbb{F}_q)$ using Pollard's rho method is intractable using existing computer technology.

- Algorithms are known for which any ECDLP instance for any elliptic curve over $\mathbb{F}_q$ can be solved in **significantly less** time than it takes Pollard's rho method to solve the hardest ECDLP instances over $\mathbb{F}_q$.

We will show that all fields $\mathbb{F}_{2^N}$ with $N \in [185, 600]$ and $N \equiv 0 \pmod 5$ are weak.
$\mathbb{F}_{2^{210}}$ is particularly weak.

Motivation:

- Advantage of ECC: Over each finite field, there are an enormous number of curves to choose from.
- Each user can select their own elliptic curve parameters.
- Parameters can be changed if some curves are found to be weak (e.g. supersingular curves, or prime-field anomalous curves).
- Standards bodies recommend a small selection of finite fields.
- Special hardware is built to support elliptic curves over these fields.
- Wide deployment of special hardware makes it difficult to change fields in the future.
- Thus, the fields selected must not be weak.

Outline

- Introduction
- Exact analysis of Pollard's rho method
- Gaudry-Hess-Smart Weil Descent attack
- Weakness of $\mathbb{F}_{2^{5l}}$
  - Exact analysis of Enge-Gaudry Index Calculus
  - Comparison EG-IC and Pollard rho
- Particular weakness of $\mathbb{F}_{2^{210}}$
- Conclusion

Exact analysis of Pollard's rho method

Consider only fields $\mathbb{F}_{2^N}$.
Assume no Weil or Tate pairing attacks apply.
Then ECDLP for curve E over $\mathbb{F}_{2^N}$ is hardest when

$$\#E(\mathbb{F}_{2^N}) = 2r \ , \quad r \text{ prime} \ .$$

Then $r \approx 2^{N-1}$, and Pollard rho takes

$$\frac{\pi r}{2} \approx 2^{(N-1)/2}$$

random walk steps in $E(\mathbb{F}_{2^N})$.
Cost:

$$R_\rho \approx c_E 2^{(N-1)/2} \approx c_N 2^{3+(N-1)/2}$$

where
$c_E =$ cost for 1 addition in $E(\mathbb{F}_{2^N})$,
$c_N =$ cost for 1 multiplication in $\mathbb{F}_{2^N}$.
(Use mixed affine-projective coordinates.)

Weil Descent Methodology

- First proposed by G. Frey in 1998.
- Idea: Reduce the ECDLP in $\mathbb{F}_{q^n}$ to a DLP in an abelian variety over a proper subfield $\mathbb{F}_q$.

The GHS Weil Descent Attack for $\mathbb{F}_{2^N}$

- P. **G**audry & F. **H**ess & N. **S**mart (2000f.)
- $N = n \cdot l$, $q = 2^l$. Then $\mathbb{F}_{2^N} = \mathbb{F}_{q^n}$.
- Explicit construction
  that reduces instance of ECDLP in $\mathbb{F}_{q^n}$
  to instance of DLP in the Jacobian $J_C(\mathbb{F}_q)$
  of a hyperelliptic curve over $\mathbb{F}_q$.
  $\longrightarrow$ HCDLP, the **hyperelliptic curve discrete logarithm problem**.

Facts on the GHS attack

- Running times of algorithms for HCDLP depend on $\#J_C(\mathbb{F}_q)$, and on g.
  - For HCDLP in curves of **high genus** g we know **subexponential** (in $\#J_C(\mathbb{F}_q)$) algorithms.
  - Also for $4 \leq g < 10$ we know faster algorithms than Pollard rho method.

- **Thus:** Depending on the genus of the resulting hyperelliptic curve, the GHS Weil Descent may or may not yield an attack that is better than Pollard's rho method.

- Genus g of the resulting hyperelliptic curve over $\mathbb{F}_q$ is determined by $E(\mathbb{F}_{q^n})$:
  Let
  $$E : y^2 + xy = x^3 + ax^2 + b \ ,$$
  then $g = g(b) = 2^{m-1}(-1)$
  with $m = m(b) =$ "magic number",
  easily computable.

- In fact, which m-values are possible is prescribed by the factorization of $x^n - 1$ in $\mathbb{F}_2[x]$: Classification by Menezes & Qu (2002), along with exact count on how many isomorphism classes of curves over $\mathbb{F}_{q^n}$ with given m exist.

Analysis of the GHS Weil Descent Attack

A. Menezes & M. Qu (2001):
If $\mathbb{F}_{q^n} = \mathbb{F}_{2^N}$ with N **prime**, then
GHS attack fails for $127 < N \leq 600$.

M. Maurer & A. Menezes & E. Teske (2002):
For each **composite** integer $N \in [100, 600]$,
$N = nl$:

Among all possible ways to perform the GHS Weil descent attack on any given ECDLP over $\mathbb{F}_{2^N}$,

- determine those descent parameters n, l,
- classify (and count) those curve parameters a, b of E over $\mathbb{F}_{2^N}$

such that the resulting HCDLP in the Jacobian $J(\mathbb{F}_{2^l})$ is most efficiently solvable.

Result: GHS attack is **successful** in many specific cases. Such as for certain elliptic curves over $\mathbb{F}_{2^N}$ where $N = 161, 180, 186, 217, 248, 300$.

Weak Fields

A. Menezes & E. Teske & A. Weng (2003):

Find GHS attack parameters for elliptic curves over $\mathbb{F}_{2^N}$ (N composite)
such that ECDLP in $\mathbb{F}_{2^N}$ can be solved

- not necessarily most efficiently,
  but significantly faster than in $2^{(N-1)/2}$ elliptic curve operations

- for all curves over $\mathbb{F}_{2^N}$.

Result:
$\mathbb{F}_{2^{5l}}$ is weak, where $185 \leq 5l \leq 600$.

$\mathbb{F}_{2^{210}}$ is particularly weak.

Weakness of $\mathbb{F}_{2^N}$ with $N = 5l$

$\mathbb{F}_{2^N} = \mathbb{F}_{q^5}$ with $q = 2^l$.
$n = 5$, $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.
Two possible magic numbers occur in GHS Weil descent:

- $m = 1$ iff E is isomorphic to curve defined over $\mathbb{F}_q$.
  Then $\#E(\mathbb{F}_q)$ divides $\#E(\mathbb{F}_{q^5})$, and Pohlig-Hellman applies.

- Otherwise, $m = 5$ and $g = 15$ or $g = 16$.
  Then apply GHS Weil descent attack:
  - Perform GHS reduction: < 1 minute.
  - Solve the resulting HCDLP:

    Enge-Gaudry Index-Calculus Algorithm:
    1. Creation of factor base
    2. Relation generation stage
    3. Linear algebra stage.

Exact analysis of Enge–Gaudry IC:
Given $J_C(\mathbb{F}_q)$, where C of genus g.

1. Smoothness bound: $t = 1$.
   Factor base: $\approx 2^{l-1}$ degree-one divisors.
   Fast.

2. # of 1-smooth divisors: $\approx 2^{lg}/g!$.
   # of random walk steps for one relation: $\approx g!$.
   Need $w \approx 2^{l-1}$ relations.
   Thus, for $g = 16$: $\approx 2^{l-1}g! \approx 2^{l+43}$ steps.
   Total cost:

   $$R_1 \approx (c_J + c_S)\, 2^{l+43} = (128l - 288)\, c_l\, 2^{l+43} \ ,$$

   where
   $c_J =$ cost for 1 addition in $J_C(\mathbb{F}_q)$,
   $c_S =$ cost for 1 smoothness test,
   $c_l =$ cost for 1 multiplication in $\mathbb{F}_{2^l} = \mathbb{F}_q$.
   (Use NUCOMP for Jacobian arithmetic.)

   Effectively parallelizable.

3. Linear system:
   # of relations (= dimension): $w \approx 2^{l-1}$.
   # of non-zero coefficients per relation: $\approx g$.
   Solution with Lanczos' algorithm:

   $$\approx gw^2 \approx 2^{2l+2} \text{ arithm. operations mod } r \ .$$

   Total cost:

   $$R_2 \approx c_r 2^{2l+2} \ ,$$

   where
   c_r = cost for one multiplication mod r.

   Effective parallelization not known so far.

Notes on the linear algebra stage:
Large storage requirements may represent bottleneck.
Thus, results are most meaningful when $R_2 \ll R_1$.

However, note:

1. Consider *full cost* (= running time $\times$ #of processors):
   Bernstein (2001), Wiener(2002):
   To solve D-dimensional system of sparse linear equations over $\mathbb{F}_2$:
   Full cost is $D^{7/3+o(1)}$
   (reduced from $D^{3+o(1)}$).

N	l	R_1/c_l	R_2/c_r	R_ρ/c_N	c_r	c_N
160	32	2^{87}	2^{66}	$2^{82.5}$	5.8	7.7
185	37	2^{92}	2^{76}	2^{95}	5.8	7.9
210	42	2^{97}	2^{86}	$2^{107.5}$	8.0	10.3
255	51	2^{107}	2^{104}	2^{130}	7.7	11.0
385	77	2^{133}	2^{156}	2^{195}	9.4	15.0
515	103	2^{160}	2^{208}	2^{260}	11.1	15.3
600	120	2^{177}	2^{242}	$2^{302.5}$	12.5	17.7

($c_l = 1.0$. Relative timings on PII 400 MHz.)

N	l	R_1	R_2	R_ρ	δ	N_{equiv}
160	32	2^{87}	2^{69}	$2^{85.5}$	–	–
185	37	2^{92}	2^{79}	2^{98}	2^{6}	173
210	42	2^{97}	2^{89}	$2^{110.5}$	2^{13}	183
255	51	2^{107}	2^{107}	2^{133}	2^{26}	202
385	77	2^{133}	2^{160}	2^{199}	2^{39}	309
515	103	2^{160}	2^{212}	2^{264}	2^{52}	412
600	120	2^{177}	2^{246}	$2^{306.5}$	2^{60}	479

Notes on the linear algebra stage: (continued)

2. If $R_2 \gg R_1$:
   Opt for trade-off between matrix stage and relation generation stage:
   Reduce factor base size by a factor of 2^d
   (by selecting only a proportion of degree-one divisors)
   $\Longrightarrow$ R_2 decreases by factor 2^{2d},
   R_1 increases by factor $2^{d(g-1)}$.

N	d	R_1	R_2	R_ρ	δ	N_{equiv}
385	1.5	$2^{155.5}$	2^{157}	2^{199}	2^{42}	302
515	3	2^{205}	2^{206}	2^{264}	2^{58}	401
600	4	2^{237}	2^{238}	$2^{306.5}$	$2^{68.5}$	463

Particular weakness of $\mathbb{F}_{2^{210}}$:

$210 \equiv 0 \pmod 6$.
$\mathbb{F}_{2^{210}} = \mathbb{F}_{q^6}$ with $q = 2^{35}$.

For the vast majority of elliptic curves, we have $m = 6$ and $g = 31$ or $g = 32$.
But for $\approx 2^{175}$ isomorphism classes:
$m = 5$, and then $g = 15$ or $g = 16$.

Then

$$\begin{aligned} R_1 &\approx c_l 2^{90} = 2^{90} \\ R_2 &\approx c_r 2^{75} \\ R_\rho &\approx c_N 2^{107.5} \approx 2^{110.5} \end{aligned}$$

so GHS Weil descent is $\delta \approx 2^{20}$ times faster than Pollard rho for hardest instances in $E(\mathbb{F}_{2^{210}})$.

Aim: Extend attack beyond those 2^{175} isomorphism classes.

Note:

1.) This GHS attack only works if

$$\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = 0 \ .$$

2.) $m = 5$ with respect to $n = 6$ implies

$$(\sigma^4 + \sigma^2 + Id)(b) = 0 \ ,$$

where $\sigma(b) = b^q$, $q = 2^{35}$.

Consequently,

$$\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(b) = 0 \ .$$

Which, given $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = 0$, is equivalent to

$$\#E(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8 \ .$$

Extension to all $E/\mathbb{F}_{2^{210}}$ with $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8$

Endomorphism class of E:

$$\mathcal{C}(E) \ := \ \{\text{isogenous, non-isomorphic curves } E' \text{ with } \mathrm{End}E = \mathrm{End}(E')\} \ .$$

We may assume (using an algorithm of Kohel) that E has maximal endomorphism ring, $\mathcal{O}$.

One-to-one correspondence

$$\mathcal{C}(E) \leftrightarrow \mathrm{Cl} \ ,$$

where Cl = ideal class group of the maximal order $\mathcal{O}$ of $\mathbb{Q}(\sqrt{\Delta})$,
where $\Delta = \mathrm{trace}(E)^2 - 4 \cdot 2^N$ (< 0).

This 1-1 correspondence will be used to find, for a given curve with $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \bmod 8$, an isogenous curve E' with magic number $m = 5$ with respect to $n = 6$.

Observe:

$\approx 2^{209}$ isomorphism classes of $E/\mathbb{F}_{2^{210}}$ with $8 \mid \#E(\mathbb{F}_{2^{210}})$.

$2^{175} - 2^{105}$ isomorphism classes of $E/\mathbb{F}_{2^{210}}$ with $(n,m) = (6,5)$.

Thus: reasonable to expect that

$$\text{Prob}\{E/\mathbb{F}_{2^{210}} \text{ has } (n,m) = (6,5) \mid \#E(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8\} = 2^{-34} .$$

Assume:

Also true for E' randomly chosen from a fixed endomorphism class $\mathcal{C}(E)$.

(Confirmed experimentally for $E/\mathbb{F}_{2^N}$, $36 \le N \le 84$.)

Now adapt Galbraith & Hess & Smart (2002):

1. Simulate pseudo-random walk in $\mathcal{C}(E)$.
2. Find curve E' isogenous to E with $(n, m) = (6, 5)$.
3. Use 1-1 correspondence Cl $\leftrightarrow \mathcal{C}(E)$ to compute a chain of low-degree isogenies from E to E'.
4. Use index-calculus techniques and Vélu's formulae to compute explicit isogeny between E and E'.

Then ECDLP in $E(\mathbf{F}_{2^{210}})$ can be mapped to ECDLP in $E'(\mathbf{F}_{2^{210}})$, where ECDLP can be solved 2^{20} times faster than hardest instances over $\mathbf{F}_{2^{210}}$ with Pollard rho.

Cost of this extension:

Expected # of random walk steps in $\mathcal{C}(E)$:

$$2^{34}.$$

Cost of each step:

$$\approx 2^{26} \text{ operations in } \mathbb{F}_{2^{210}}.$$

Thus, cost to find E':

$$\approx 2^{60} \text{ operations in} \mathbb{F}_{2^{210}} .$$

Cost to compute explicit isogeny $E \to E'$:

$$const \cdot 2^{53} \text{ bit operations} .$$

These costs are negligible compared to

$$R_1 \approx c_l 2^{90} \text{ and } R_2 \approx c_r 2^{75} .$$

Summary: Weakness of $\mathbb{F}_{2^{210}}$:

$N = 210 = nl$

n	l	R_1/c_l	R_2/c_r	R_ρ/c_N
5	42	2^{97}	2^{86}	$2^{107.5}$
6	35	2^{90}	2^{72}	$2^{107.5}$

n	l	R_1	R_2	R_ρ	δ	N_{equiv}
5	42	2^{97}	2^{89}	$2^{110.5}$	$2^{13.5}$	183
6	35	2^{90}	2^{75}	$2^{110.5}$	$2^{20.5}$	169

Recall:

$n = 6$ data only apply to $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \bmod 8$,

$\approx 1/4$ of all $E/\mathbb{F}_{2^{210}}$.

Remark 1:

For almost* all $E/\mathbb{F}_{2^{210}}$,
the ECDLP in $E(\mathbb{F}_{2^{210}})$ can be reduced to a DLP in the Jacobian variety of a curve of genus ≤ 14.

Subexponential algorithms for solving this DLP apply.

(Consequence of F. Hess:
The GHS attack revisited, Eurocrypt 2003).

Remark 2:

Results analogous to the above apply to all finite fields $\mathbb{F}_{2^N}$ with $N = 6l$.

* Exceptional set: those 2^{106} isomorphism classes of curves over $\mathbb{F}_{2^{210}}$ with $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_{2^{105}}}(b) = 0$.

The fields $\mathbb{F}_{2^N}$ wih $N = 4l$
Four possible magic numbers: $m = 1, 2, 3, 4$.

- $m = 1$: E is isomorphic to subfield curve: $\#E(\mathbb{F}_{2^l})$ divides $\#E(\mathbb{F}_{2^{4l}})$.
- $m = 2$. Dito. $\#E(\mathbb{F}_{2^{2l}})$ divides $\#E(\mathbb{F}_{2^{4l}})$.
- $m = 3$. Then GHS attack reduces ECDLP to HCDLP, with genus 4 curve.
  ($g = 3$ not possible, see F. Hess (2003).)
- $m = 4$. True for almost all isomorphism classes.
  Then $g = 7$ or $g = 8$.
  Analyse as for $N = 5l \Longrightarrow$
  Running times for Pollard rho and matrix stage are very close.

Improve Enge-Gaudry algorithm:
Reduce factor base by factor 2^d to decrease cost for matrix stage:

N	l	d	R_1/c_l	R_2/c_r	R_ρ/c_N	δ
160	40	2	2^{78}	2^{77}	$2^{82.5}$	$2^{4.5}$
192	48	3	2^{94}	2^{91}	$2^{98.5}$	$2^{4.5}$
224	56	4	2^{109}	2^{104}	$2^{114.5}$	$2^{5.5}$
256	64	5	2^{124}	2^{119}	$2^{130.5}$	$2^{6.5}$
384	96	8	2^{178}	2^{177}	$2^{194.5}$	$2^{16.5}$
512	128	12	2^{238}	2^{233}	$2^{258.5}$	$2^{20.5}$
600	150	14	2^{274}	2^{273}	$2^{302.5}$	$2^{28.5}$

Conclusions

- The fields $\mathbb{F}_{2^N}$, where $N \in [185, 600]$ is divisible by 5, are weak for ECC.
- $\mathbb{F}_{2^{210}}$ is even weaker, because $6 \mid 210$.
- Fields $\mathbb{F}_{2^{4l}}$ exhibit some signs of being weak.
- Are there **bad fields** for ECC? That is, weak fields for which algorithms are known which can feasibly solve any ECDLP instance for any elliptic curve over $\mathbb{F}_q$ (using current computer technology).
- Are there algorithms for solving the HCDLP faster than the Enge-Gaudry algorithm?
- Exact analysis for index calculus in arbitrary Jacobians?
- Are there any weak fields for genus two hyperelliptic curve cryptography?

Preprint: CACR Technical Report 2003-15, Cryptology ePrint Archive Report 2003/128.