Trapdooring with Isogenies

Edlyn Teske

C&O, University of Waterloo/

CWI Amsterdam

Paris, 18.7.2006

Key Escrow with Elliptic Curves.

- Key escrow: BIG BROTHER (BB) wants to listen.

- So, users have to submit information about their secret keys to an escrow agency.

- Often, this simply means submitting the decrypt information. Then **BB can decrypt everyone's encrypted messages in polynomial time**.

- **Proposal:** an elliptic curve based key escrow where BB can derive a user's secret key, but **only with considerable computational effort.**

- For example, this makes widespread wiretapping impossible.

Key escrow with elliptic curves - The big picture

- Alice constructs a pair of elliptic curves $(E_{\text{sec}}, E_{\text{pub}})$ over $\mathbb{F}_{2^{161}}$ such that
  - E_{pub} is isogenous to E_{sec} (over $\mathbb{F}_{2^{161}}$).
  - Best attack on the ECDLP in $E_{\text{pub}}(\mathbb{F}_{2^{161}})$ is the parallelized Pollard rho method.
  - ECDLP in $E_{\text{sec}}(\mathbb{F}_{2^{161}})$ is computationally feasible, but by far non-trivial.

- Use E_{pub} just as usual in ECC.

- Submit E_{sec} to trusted authority.

Magic numbers

- Let N be composite, write $N = nf$. Let $q = 2^f$.

- For $b \in \mathbb{F}_{2^N}$, $b \neq 0$ let
  $m = m_n(b) =$ "magic number" $=$

  $$\dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), \ldots, (1, b_{n-1}^{1/2})\})$$

  where $b_i = b^{q^i}$.

- Now consider $N = 161 = 7 \cdot 23, n = 7$.

- For $b \in \mathbb{F}^*_{2^{161}}$ we have $m_7(b) \in \{1, 4, 7\}$.

- There are

  $$\approx 2^{93}$$

  $b \in \mathbb{F}^*_{2^{161}}$ for which

  $$m_7(b) = 4 \ .$$

  There are $\approx 2^{23}$ values of b with $m_7 = 1$.
  The overwhelming majority has $m_7 = 7$.

Magic numbers and elliptic curves

- Let

  $$E : y^2 + xy = x^3 + ax^2 + b \ ,$$

  $a, b \in \mathbb{F}_{2^N}, b \neq 0$ be an elliptic curve.
  Then the magic number of E with respect to n is $m = m_n(b)$.

- Properties of m:
  - m is invariant under isomorphisms.
  - m is invariant under the power-2-Frobenius map.
  - m is invariant under the 2-isogeny stemming from $\Phi_2(X, Y)$.
  - m is invariant under the multiplication-by-l map.
  - In general, m *changes* under isogenies.

Weil descent attack

Input:

- A cryptographically interesting curve $E/\mathbb{F}_{2^N}$, with N composite.

  $E : y^2 + xy = x^3 + ax^2 + b$, $a, b \in \mathbb{F}_{2^N}, b \neq 0$.

- P = a point on E of large prime order.

Write $N = nf$. Then $\mathbb{F}_{2^N} = \mathbb{F}_{(2^f)^n}$.

Gaudry-Hess-Smart (GHS) Weil descent attack and its implementation (in KASH) gives **explicit group homomorphism**

$$\Phi : \langle P \rangle \longrightarrow J_C(\mathbb{F}_{2^f})$$

into the Jacobian of a hyperelliptic curve C. C is of genus

$$g = 2^{m-1} \text{ or } g = 2^{m-1} - 1 ,$$

where $m = m_n(b)$ = magic number.

Thus:

Instead of solving the **ECDLP**

$$Q = sP$$

in $E(\mathbb{F}_{2^N})$
for some unknown $s \in [0, \operatorname{ord} P)$,

solve **HCDLP**

$$\Phi(Q) = s\Phi(P)$$

in the Jacobian $J_C(\mathbb{F}_{2^f})$.

HCDLP solver: Enge-Gaudry index calculus algorithm.

This **may** be faster than Pollard rho for corresponding ECDLP if the genus of C has the "right" size.

Now consider $N = 161 = 7 \cdot 23$.

$$\begin{array}{c} \mathbb{F}_{2^{161}} \\ | \\ | \quad\quad n = 7 \\ | \\ \mathbb{F}_{2^{23}} \end{array}$$

$$m = m_7(b) \in \{1, 4, 7\}$$

If $m_7(b) = 4$, the ECDLP maps to HCDLP in Jacobian $J_C(\mathbb{F}_{2^{23}})$ of curve C of genus 7 or 8.

The vast majority of curves over $\mathbb{F}_{2^{161}}$ has $m_7(b) = 7$ and yields genus 64 or 63 hyperelliptic curves. In which case the resulting HCDLP is even harder than the ECDLP in $E(\mathbb{F}_{2^{161}})$.

Solving the HCDLP

Enge-Gaudry index calculus: $g(C) = 7(8)$: expected 2^{34} (2^{37}) hyperelliptic curve operations,
factor base of 2^{22} prime divisors of degree 1.
25.000 (200.000) days on 1GHz PIII workstation.

To compare:
DES break using exhaustive search:
110.000 days on a 450MHz PII.
Pollard rho for 108-bit ECDLP:
200.000 days on 450MHz PII.
Pollard rho for E161: 2^{80} additions on E161.
10^{14} days on 500MHz Alpha workstation.

Constructing the secret trapdoor curve

Let

$$I_4 = \left\{ \begin{array}{c} \text{isomorphism classes of} \\ E/\mathbb{F}_{2^{161}} \text{ with } m_7(b_E) = 4 \end{array} \right\}.$$

That is, $I_4 = \{E_{0,b}, E_{1,b} \ : \ b \in S\}$

where $S = \{b \in \mathbb{F}_{2^{161}} \ : \ m_7(b) = 4\}$.

Note: $S = (W_0 \oplus (W_1 \setminus \{0\})) \cup (W_0 \oplus (W_2 \setminus \{0\}))$, where the W_i are subspaces of $\mathbb{F}_{2^{161}}$. Bases of the W_i can be efficiently computed. (Menezes & Qu, CT-RSA 2001).

Algorithm to construct the secret curve

1. Choose $b \in_R S$ until
   $\#E_{1,b}(\mathbb{F}_{2^{161}}) = 2{\cdot}\text{prime}$, or
   $\#E_{0,b}(\mathbb{F}_{2^{161}}) = 4{\cdot}\text{prime}$.
   Denote the resulting curve by E.

2. Let $\Delta = t^2 - 4 \cdot 2^{161}$ be the discriminant of E.
   (where $t = 2^N + 1 - \#E(\mathbb{F}_{2^{161}})$, the trace).
   If

   (a) Δ is squarefree,

   (b) $|\Delta| > 2^{157}$,

   (c) $2^{76} \leq \#\text{Cl}_\Delta < 2^{83}$
   (where Cl_Δ = class group of $\mathcal{O}_\Delta$ of $\mathbb{Q}(\sqrt{\Delta})$),

   (d) the odd, cyclic part of Cl_Δ has cardinality $\geq 2^{68}$.

   then output $E =: E_{\text{sec}}$, **else** go back to (1).

Notes:

- Step (1) = the major barrier. We expect 0.8% of curves to pass.
(Experimentally, 1% pass.)

- $90 - 95\%$ of all $E/\mathbb{F}_{2^{161}}$ have squarefree discriminant. (Experimentally).

- A curve passing Step (2a) most likely passes the remaining steps.
Confirmed experimentally.

- Estimate: There exist $\approx 2^{87}$ suitable secret curves.

Constructing the public curve

Use pseudo-random walk in the isogeny class of E_{sec}.

Theorem: Let $E/\mathbb{F}_{2^N}$ be an elliptic curve with endomorphism ring $\mathrm{End}(E) \cong \mathcal{O}_{\Delta}$.
Let Cl_{Δ} denote the class group of $\mathcal{O}_{\Delta}$ of $\mathbb{Q}(\sqrt{\Delta})$.
Let $\mathrm{Ell}(\mathcal{O}_{\Delta})$ denote the set of isomorphism classes of curves isogenous to E with endomorphism ring isomorphic to $\mathcal{O}_{\Delta}$.
Then there is a one-to-one correspondence

$$\mathrm{Cl}_{\Delta} \longleftrightarrow \mathrm{Ell}(\mathcal{O}_{\Delta}) \ .$$

Note:
In our case, Δ squarefree, so $\mathrm{End}(E_{\mathsf{sec}}) \cong \mathcal{O}_{\Delta}$, and $\mathrm{End}(E) \cong \mathcal{O}_{\Delta}$ for any $E \sim E_{\mathsf{sec}}$.

Ideal classes and isogenous curves.

Cl_Δ		$\mathsf{Ell}(\mathcal{O}_\Delta)$
$\mathbf{a}$		$E_{a,b}$ $b = j^{-1}$ (j-invariant)
	prime l $\left(\frac{\Delta}{l}\right) = 1$	
2 prime ideals lying over l: $\mathbf{l_1}, \mathbf{l_2}$		$\Phi_l(j, X)$, 2 roots in $\mathbb{F}_{2^N}$: j_1, j_2
$\mathbf{a} \mapsto \mathbf{a_1} = \mathbf{a} * \mathbf{l_1}$ $\mathbf{a} \mapsto \mathbf{a_2} = \mathbf{a} * \mathbf{l_2}$		$E_{a,b} \mapsto E_{a,{j_1}^{-1}}$ $E_{a,b} \mapsto E_{a,{j_2}^{-1}}$ l-isogenies, "horizontal"

A random walk in the isogeny class

Let $\mathcal{L} = \{l_1, \ldots, l_M\}$, the smallest M primes ≥ 3 such that

- $\left(\frac{\Delta}{l_i}\right) = 1$ and
- the pairs $(\mathrm{Red}(\mathbf{l_i}), \mathrm{Red}(\mathbf{l_i}'))$ of the reduced representatives of the prime ideals $\mathbf{l_i}, \mathbf{l_i}'$ lying over l are pairwise distinct.

$$E_{a,j^{-1}} \quad \xrightarrow[\substack{\Phi_l(j,j_1)=\Phi_l(j,j_2)=0 \\ j' \in \{j_1, j_2\},}]{l \in_R \mathcal{L}} \quad E_{a,j'^{-1}}$$

$$\xrightarrow[\substack{\Phi_l(j',j_1)=\Phi_l(j',j_2)=0 \\ j'' \in \{j_1, j_2\}}]{l \in_R \mathcal{L}} \quad E_{a,j''^{-1}}$$

etc.etc.

Algorithm to construct public curve from secret curve

Let $\mathcal{L} = \{l\ :\ l \text{ prime}, 3 \le l \le 300, \left(\frac{\Delta}{l}\right) = 1,$
$(\text{Red}(\mathbf{l}), \text{Red}(\mathbf{l}'))$ pairwise distinct$\}$.
$=: \{l_1, \ldots, l_M\}$.

1. Let $E = E_{\text{sec}}$.

2. For $i = 1, \ldots, M$ do
   (a) Let $n_i \in_R \{0, 1, \ldots, 11\}$.
   (b) Construct a chain of length n_i of l_i-isogenous curves, starting from E.
   (c) Denote the resulting curve by E.

3. Output $E =: E_{\text{pub}}$.

Solving the ECDLP in $E_{\text{pub}}(\mathbb{F}_{2^{161}})$ using E_{sec}.

Key escrow scenario 1:
Alice submits to the trusted authority (TA) both E_{sec} and the sequence of j-invariants encountered while computing the public curve.

Then TA easily computes the explicit chain of isogenies using Vélu's formulae.

Key escrow scenario 2:
Alice submits only E_{sec}.

Then starting from E_{pub} and E_{sec}, TA computes two (deterministic) pseudo-random walks.
TA keeps track of all l-values and j-invariants used.
Uses distinguished point method to detect collision between these two walks.
Collision is expected to occur after $\sqrt{\pi h_\Delta}$ steps (that is, roughly 2^{41} steps for $E/\mathbb{F}_{2^{161}}$).
Efficiently parallelizable.
(Galbraith-Hess-Smart, Eurocrypt 2002).

Security Analysis

Assumption:

(A) The isomorphism classes of curves over $\mathbb{F}_{2^{161}}$ with $m_7(b) = 4$ are distributed uniformly at random over all isogeny classes over $\mathbb{F}_{2^{161}}$.

What does this mean?

- There are 2^{162} isomorphism classes.
- There are 2^{94} isomorphism classes with $m_7(b) = 4$.
- Assumption (A) $\Rightarrow$ a random curve from a fixed isogeny class has $m_7(b) = 4$ with

$$\text{probability } 2^{94}/2^{162} = 2^{-68} .$$

- Assumption (A) $\Rightarrow$ in any isogeny class with square-free Δ we expect

$$h_\Delta/2^{68}$$

isomorphism classes of curves with $m_7 = 4$.

Security Analysis, continued

To break the system, an attacker must solve the ECDLP in $E_{\text{pub}}(\mathbb{F}_{2^{161}})$.

Parallelized Pollard Rho: 2^{80} EC operations.

Or, the attacker solves **Problem**

(P)

Given E_{pub},
find E,
isogenous to E_{pub},
and in I_4, that is, with $m_7(b_E) = 4$.

Strategies to solve (P):

1. Reconstruct E_{sec} from E_{pub}.

2. Search isogeny class of E_{pub} for a curve in I_4.

3. Search I_4 for a curve isogenous to E_{pub}.

For analysis:

Cost to move around in the isogeny class:

Assume: one step along an l-isogeny costs $16l^2$ elliptic curve operations.

(cost to compute root of $\Phi_l(j, X)$ is $O(l^2 \cdot 161)$ operations in $\mathbb{F}_{2^{161}}$,
cost for one elliptic curve operation is 10 operations in $\mathbb{F}_{2^{161}}$.)

ad (1): Reconstruct E_{sec} from E_{pub}.

- Odd cyclic part of Cl_Δ is $\geq 2^{68}$.
  $\Rightarrow$ Most of the l_i used to construct E_{pub} correspond to ideal classes with order $\geq 2^{68}$.

- To construct E_{pub} from E_{sec}, Alice used M subchains of distinct l_i-isogenies, with chainlengths $\in_R \{0, \ldots, 11\}$.
  $\Rightarrow$ there are approx. $\max\{12^M, 2^{68}\}$ possibilities for E_{pub}.

- $3 \leq l_i \leq 300 \Longrightarrow M \geq 19$,
  and on average $M = 30$ (experimentally).
  $12^{19} > 2^{68}$.

- Attacker has to try $\approx 2^{68}/2$ curves to retrieve E_{sec}.

- Each such try costs at least $16l^2$ EC operations, where $l = \max\{l_i : n_i \neq 0\}$.
  If $l \geq 23$, then $16l^2 > 2^{13}$. Fair to assume.

- $\Rightarrow$ Total cost $2^{67} \cdot 2^{13} = 2^{80}$ EC ops.

ad (2): Search through the isogeny class of E_{pub} for a curve in I_4.

- Perform a pseudo-random walk in the isogeny class of E_{pub}.

- Under Assumption (A), expected 2^{68} curves have to be considered until one with $m_7 = 4$ is found.

- Cost of considering one curve: $16l^2$ EC operations.
  ($l=$ degree of isogeny used for this step).

- Even with only 8 different prime ideals, attacker needs to work with l-values up to 80.

- Assume an average l-value of 16,
  $\Rightarrow$ considering one curve costs $> 16 \cdot 16^2 = 2^{12}$ EC operations.

- $\Rightarrow$ Total cost $> 2^{68} \cdot 2^{12} = 2^{80}$ EC ops.

ad (3): Search through the set I_4 for a curve isogenous to E_{pub}.

- Only method known to date is exhaustive search through I_4.

- Recall: $E_{a,b} \in I_4 \Leftrightarrow m_7(b) = 4$, and the set S of all those b can be efficiently represented.

- Under Assumption (A), there are $h_\Delta/2^{68}$ curves in I_4 that are isogenous to E_{pub}.

- S has 2^{93} b-values, so we expect to have to consider
$$2^{93}/\frac{h_\Delta}{2^{68}} = 2^{161}/h_\Delta$$
b-values.

- $h_\Delta < 2^{83} \Rightarrow$ consider $> 2^{78}$ b-values.

- Cost of point counting, or scalar multiplication by $\#E_{\text{pub}}(\mathbb{F}_{2^{161}})$: > 4 EC operations.

- $\Rightarrow$ Total cost $> 2^{78} \cdot 2^2 = 2^{80}$ EC ops.

Final words

1. The proposed system can also be used over the fields $\mathbb{F}_{2^N}$ with $N = 154, 182, 189, 196$.
   - Large set I of elliptic curves for which GHS Weil descent attack is feasible.
     $\longrightarrow$ To avoid exhaustive search attack for $E_{\text{sec}} \in I$.
   - I must not be too large.
     $\longrightarrow$ otherwise a random walk in the isogeny class of E_{pub} will succeed too fast.

2. Are there any ways to approach Problem P?

   If Problem P can be solved efficiently, $\mathbb{F}_{2^{161}}$ is **bad**,
   in the sense that any ECDLP instance for **any** elliptic curve over $\mathbb{F}_{2^{161}}$ can be solved using existing computer technology.