Trace zero varieties and the ECDLP over extension fields

Elisa Gorla
based on `eprint.iacr.org/2014/318`
joint work with M. Massierer

Université de Neuchâtel

ECC, October 9, 2014

Hardness of the ECDLP

Definition

Elliptic Curve Discrete Logarithm Problem (ECDLP): given $P, Q \in E(\mathbb{F}_q)$, find ℓ s.t. $Q = \ell P$.

Hardness of the ECDLP

Definition

Elliptic Curve Discrete Logarithm Problem (ECDLP): given $P, Q \in E(\mathbb{F}_q)$, find ℓ s.t. $Q = \ell P$.

Generic attack: Pohlig-Hellman + Pollard ρ requires $\tilde{O}(\sqrt{q})$ opns and negligible memory.

Hardness of the ECDLP

Definition

Elliptic Curve Discrete Logarithm Problem (ECDLP): given $P, Q \in E(\mathbb{F}_q)$, find ℓ s.t. $Q = \ell P$.

Generic attack: Pohlig-Hellman + Pollard ρ requires $\tilde{\mathcal{O}}(\sqrt{q})$ opns and negligible memory.

Attacks on specific curves:

- transfer to a DLP in $\mathbb{F}_q^k$ via a pairing, if the embedding degree k is small (e.g., supersingular curves),
- index calculus on $E(\mathbb{F}_{p^n})$, if $q = p^n$,
- transfer to a DLP in $\mathrm{Jac}_C(\mathbb{F}_p)$ for a suitable C of genus $g \geq n$, if $q = p^n$ (cover attack),
- transfer to a DLP in T_n, if $q = p^n$ and E is defined over $\mathbb{F}_p$.

The trace zero variety

Let $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, n odd prime, E an elliptic curve over $\mathbb{F}_p$.

Definition

The Frobenius endomorphism is

$$\begin{array}{rcl} \sigma : E(\mathbb{F}_{p^n}) & \longrightarrow & E(\mathbb{F}_{p^n}) \\ (x, y) & \longmapsto & (x^p, y^p). \end{array}$$

The trace map is

$$\begin{array}{rcl} \mathrm{Tr} : E(\mathbb{F}_{p^n}) & \longrightarrow & E(\mathbb{F}_p) \\ P & \longmapsto & P + \sigma(P) + \ldots + \sigma^{n-1}(P). \end{array}$$

The trace zero subgroup is

$$T_n = \ker \mathrm{Tr} \subset E(\mathbb{F}_{p^n}).$$

T_n is the group of $\mathbb{F}_p$-rational points of the trace zero variety, an abelian variety of dimension $n-1$.

Geometric construction of the trace zero variety

E of equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$,
$\mathbb{F}_{p^n} = \mathbb{F}_p[\zeta]$ with $\mathbb{F}_p$-basis $1, \zeta, \ldots, \zeta^{n-1}$.

1. Construct a variety $\mathcal{E}$ of dimension n over $\mathbb{F}_p$ s.t. $\mathcal{E}(\mathbb{F}_p) = E(\mathbb{F}_{p^n})$ by Weil restriction from $\mathbb{F}_{p^n}$ down to $\mathbb{F}_p$. In practice, set:

$$x := \sum_{i=0}^{n-1} x_i \zeta^i, \quad y := \sum_{i=0}^{n-1} y_i \zeta^i,$$

plug into the equation of E and sort according to powers of ζ to obtain n equations in the $2n$ variables $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}$.

2. The trace condition yields one more equation, hence a subvariety $\mathcal{T} \subset \mathcal{E}$ of dimension $n-1$ s.t. $\mathcal{T}(\mathbb{F}_p) = T_n$.

Example ($n = 3$)

Assume $3 \mid (p-1)$ and let $1, \zeta, \zeta^2$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$.

$$y^2 = \quad x^3 + Ax \quad + B$$

Example ($n = 3$)

Assume $3 \mid (p-1)$ and let $1, \zeta, \zeta^2$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$.

$$(y_0 + y_1\zeta + y_2\zeta^2)^2 = (x_0 + x_1\zeta + x_2\zeta^2)^3 + A(x_0 + x_1\zeta + x_2\zeta^2) + B$$

Example ($n = 3$)

Assume $3 \mid (p-1)$ and let $1, \zeta, \zeta^2$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$.

$$
\begin{aligned}
&(y_0 + y_1\zeta + y_2\zeta^2)^2 - (x_0 + x_1\zeta + x_2\zeta^2)^3 - A(x_0 + x_1\zeta + x_2\zeta^2) - B \\
&= \quad (y_0^2 + 2\mu y_1 y_2 - x_0^3 - \mu x_1^3 - \mu^2 x_2^3 - 6\mu x_0 x_1 x_2 - A x_0 - B) \\
&\quad + (2y_0 y_1 + \mu y_2^2 - 3\mu x_1^2 x_2 - 3x_0^2 x_1 - 3\mu x_0 x_2^2 - A x_1)\zeta \\
&\quad + (2y_0 y_2 + y_1^2 - 3\mu x_1 x_2^2 - 3x_0^2 x_2 - 3x_0 x_1^2 - A x_2)\zeta^2 \\
&= \quad 0
\end{aligned}
$$

Example ($n = 3$)

Assume $3 \mid (p-1)$ and let $1, \zeta, \zeta^2$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$.

$$
\begin{aligned}
0 &= y_0^2 + 2\mu y_1 y_2 - x_0^3 - \mu x_1^3 - \mu^2 x_2^3 - 6\mu x_0 x_1 x_2 - A x_0 - B \\
0 &= 2 y_0 y_1 + \mu y_2^2 - 3\mu x_1^2 x_2 - 3 x_0^2 x_1 - 3\mu x_0 x_2^2 - A x_1 \\
0 &= 2 y_0 y_2 + y_1^2 - 3\mu x_1 x_2^2 - 3 x_0^2 x_2 - 3 x_0 x_1^2 - A x_2
\end{aligned}
$$

Example ($n = 3$)

Assume $3 \mid (p-1)$ and let $1, \zeta, \zeta^2$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$.

$$
\begin{aligned}
0 &= y_0^2 + 2\mu y_1 y_2 - x_0^3 - \mu x_1^3 - \mu^2 x_2^3 - 6\mu x_0 x_1 x_2 - A x_0 - B \\
0 &= 2y_0 y_1 + \mu y_2^2 - 3\mu x_1^2 x_2 - 3x_0^2 x_1 - 3\mu x_0 x_2^2 - A x_1 \\
0 &= 2y_0 y_2 + y_1^2 - 3\mu x_1 x_2^2 - 3x_0^2 x_2 - 3x_0 x_1^2 - A x_2 \\
0 &= x_1 y_2 - x_2 y_1
\end{aligned}
$$

Remark

For $n = 3$ the trace condition is $P + \sigma(P) + \sigma^2(P) = \mathcal{O}$, i.e., $P, \sigma(P), \sigma^2(P)$ collinear. In general it is not obvious how to express the trace condition.

Trace zero varieties and the ECDLP

$$E(\mathbb{F}_{p^n}) \overset{\mathrm{Tr}}{\twoheadrightarrow} E(\mathbb{F}_p)$$

Trace zero varieties and the ECDLP

$$T_n \hookrightarrow E(\mathbb{F}_{p^n}) \overset{\mathrm{Tr}}{\twoheadrightarrow} E(\mathbb{F}_p)$$

$$P = \ell Q \text{ in } E(\mathbb{F}_{p^n}) \;\leftrightsquigarrow\; \begin{cases} \mathrm{Tr}(P) = \ell\,\mathrm{Tr}(Q) & \text{in } E(\mathbb{F}_p) \\ P - \sigma(P) = \ell(Q - \sigma(Q)) & \text{in } T_n \end{cases}$$

Trace zero varieties and the ECDLP

$$T_n \hookrightarrow E(\mathbb{F}_{p^n}) \overset{\mathrm{Tr}}{\twoheadrightarrow} E(\mathbb{F}_p)$$

$$P = \ell Q \text{ in } E(\mathbb{F}_{p^n}) \;\leftrightsquigarrow\; \begin{cases} \mathrm{Tr}(P) = \ell\,\mathrm{Tr}(Q) & \text{in } E(\mathbb{F}_p) \\ P - \sigma(P) = \ell(Q - \sigma(Q)) & \text{in } T_n \end{cases}$$

Since $\#E(\mathbb{F}_p) \sim p$, $\#E(\mathbb{F}_{p^n}) \sim p^n$, and $\#T_n \sim p^{n-1}$

Theorem

The DLP in $E(\mathbb{F}_{p^n})$ and T_n has the same complexity.

Trace zero varieties and the ECDLP

$$T_n \hookrightarrow E(\mathbb{F}_{p^n}) \stackrel{\mathrm{Tr}}{\twoheadrightarrow} E(\mathbb{F}_p)$$

$$P = \ell Q \text{ in } E(\mathbb{F}_{p^n}) \;\leftrightsquigarrow\; \begin{cases} \mathrm{Tr}(P) = \ell\,\mathrm{Tr}(Q) & \text{in } E(\mathbb{F}_p) \\ P - \sigma(P) = \ell(Q - \sigma(Q)) & \text{in } T_n \end{cases}$$

Since $\#E(\mathbb{F}_p) \sim p$, $\#E(\mathbb{F}_{p^n}) \sim p^n$, and $\#T_n \sim p^{n-1}$

Theorem

The DLP in $E(\mathbb{F}_{p^n})$ and T_n has the same complexity.

To solve a DLP in T_n or $E(\mathbb{F}_{p^n})$ we have:

- square root attacks in T_n,
- index calculus attacks in $E(\mathbb{F}_{p^n})$,
- index calculus attacks in T_n.

Other reasons for our interest in T_n

1. The elements of T_n can be represented using $n-1$ coordinates in $\mathbb{F}_p$ (Naumann, Lange, Rubin-Silverberg, G.-Massierer).

2. Groups of points of supersingular abelian varieties of dim > 1, such as T_n, provide higher security per bit in pairing-based cryptography (Rubin-Silverberg).

3. Using the Frobenius endomorphism speeds up scalar multiplication, which can be computed with as many additions, but $1/n-1$ as many doublings for $n = 3, 5$ (Lange; Avanzi, Cesena).

4. Computing the order of T_n (of order $\sim p^{n-1}$) has the same complexity as computing the order of $E(\mathbb{F}_p)$.

Summarizing

- The DLP in T_n and $E(\mathbb{F}_{p^n})$ has the same complexity.
- Computing the cardinality of $E(\mathbb{F}_p)$, $E(\mathbb{F}_{p^n})$, and T_n has the same complexity.
- Computation of the group operation in T_n is more efficient than in $E(\mathbb{F}_{p^n})$.
- The elements of T_n can be represented with $n-1$ coordinates in $\mathbb{F}_p$, those of $E(\mathbb{F}_{p^n})$ with n.

Summarizing

- The DLP in T_n and $E(\mathbb{F}_{p^n})$ has the same complexity.
- Computing the cardinality of $E(\mathbb{F}_p)$, $E(\mathbb{F}_{p^n})$, and T_n has the same complexity.
- Computation of the group operation in T_n is more efficient than in $E(\mathbb{F}_{p^n})$.
- The elements of T_n can be represented with $n-1$ coordinates in $\mathbb{F}_p$, those of $E(\mathbb{F}_{p^n})$ with n.

Question

Study the hardness of the DLP in T_n for $n=3,5$.

Index calculus

Goal: solving the DLP $Q = \ell P$ in T_n.

Relation search: choose a factor base $\mathcal{F} = \{P_1, \ldots, P_b\} \subseteq T_n$.
Find $k \geq b$ relations of the form

$$\alpha_i P + \beta_i Q = m_{i1} P_1 + \ldots + m_{ib} P_b$$

Linear algebra: solve the system

$$\begin{pmatrix} m_{11} & \ldots & m_{1b} \\ \vdots & & \vdots \\ m_{k1} & \ldots & m_{kb} \end{pmatrix} \begin{pmatrix} \ell_1 \\ \vdots \\ \ell_b \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Solution: output $\ell = -(\alpha_1 \ell_1 + \ldots + \alpha_b \ell_b)(\beta_1 \ell_1 + \ldots + \beta_k \ell_k)^{-1}$.

Semaev's summation polynomials

E of equation $y^2 = x^3 + Ax + B$.

The n^{th} Semaev's summation polynomial f_n satisfies

$$f_n(t_1, \ldots, t_n) = 0 \Longleftrightarrow \sum_{i=1}^{n} (t_i, u_i) = \mathcal{O}$$

for some $u_1, \ldots, u_n \in \overline{\mathbb{F}_p}$ s.t. $(t_i, u_i) \in E$.

Semaev's summation polynomials

E of equation $y^2 = x^3 + Ax + B$.

The n^{th} Semaev's summation polynomial f_n satisfies

$$f_n(t_1, \dots, t_n) = 0 \iff \sum_{i=1}^{n} (t_i, u_i) = \mathcal{O}$$

for some $u_1, \dots, u_n \in \overline{\mathbb{F}_p}$ s.t. $(t_i, u_i) \in E$.

For small n, f_n can be computed recursively via:

$$\begin{aligned} f_2(t_1, t_2) &= t_1 - t_2 \\ f_3(t_1, t_2, t_3) &= (t_1 - t_2)^2 t_3^2 - 2((t_1 + t_2)(t_1 t_2 + A) + 2B)t_3 \\ &\quad +(t_1 t_2 - A)^2 - 4B(t_1 + t_2) \\ f_n(t_1, \dots, t_n) &= \operatorname{Res}_t(f_{n-1}(t_1, \dots, t_{n-2}, t), f_3(t_{n-1}, t_n, t)) \\ &\quad \text{for } n \geq 4. \end{aligned}$$

It has degree $(n-1)2^{n-2}$.

Gaudry's relation search

$\mathcal{A}$ abelian variety of dimension $d > 2$.

Factor base: $\mathcal{F} = \{(x_0, \ldots, x_{n-1}) \in \mathcal{A} \mid x_{n-d+1} = \ldots = x_{n-1} = 0\}$ the $\mathbb{F}_p$-rational points of a one-dimensional subvariety of $\mathcal{A}$, $\#\mathcal{F} \sim p$.

Relations: for random α, β compute $R = \alpha P + \beta Q = (a, b)$, then solve $f_{d+1}(x_{P_1}, \ldots, x_{P_d}, a) = 0$ to find d points $P_1, \ldots, P_d \in \mathcal{F}$ s.t.

$$P_1 + \ldots + P_d = \alpha P + \beta Q.$$

Using Weil restriction one rewrites $f_{d+1}(x_{P_1}, \ldots, x_{P_d}, a) = 0$ as a system of $\geq n + d(n-d)$ equations in $d(n-d+1)$ variables.

Example

Gaudry's original application to the DLP in $E(\mathbb{F}_{p^3})$ has $d = n = 3$, hence 3 equations in 3 variables.

Assuming that the systems have finitely many solutions over $\overline{\mathbb{F}_p}$, in order to solve them it suffices to compute a lexicographic Gröbner basis.

Remarks

1. One system of multivariate polynomials $\leftrightarrow$ one possible relation.
2. About one in $d!$ systems produces a relation.
3. The complexity of computing a Gröbner basis depends exponentially on d.

Complexity: $\tilde{\mathcal{O}}(p^{2-\frac{2}{d}})$ using the double large prime variation. There is a hidden exponential dependency on d, due to the use of Gröbner bases.

Remark

Straightforward application of this to T_n yields a system with n^2+2n-1 equations, n of which of degree $(n-1)2^{n-2}$, in n^2+n-2 variables.

Applying Gaudry's index calculus algorithm to T_n

Goal

Study the hardness of the DLP in T_n for $n = 3, 5$.

Recall: E elliptic curve, n prime,

$$T_n = \{P \in E(\mathbb{F}_{p^n}) \mid P + \sigma(P) + \ldots + \sigma^{n-1}(P) = \mathcal{O}\} \subset E(\mathbb{F}_{p^n}).$$

T_n is the group of $\mathbb{F}_p$-rational points of an abelian variety of dim $n - 1$.

Our contribution:

1. A simple equation for the points of T_n, which only involves x-coordinates. This halves the number of variables in the system.
2. Complexity analysis in n, p.
3. Implementation in Magma and experimental results.

A simple equation for T_n

$$T_n = \{P \in E(\mathbb{F}_{p^n}) \mid P + \sigma(P) + \ldots + \sigma^{n-1}(P) = \mathcal{O}\} \subset E(\mathbb{F}_{p^n}) \Rightarrow$$
$$T_n \subseteq \{(x,y) \in E(\mathbb{F}_{p^n}) \mid f_n(x, x^p, \ldots, x^{p^{n-1}}) = 0\} \cup \{\mathcal{O}\}$$

where f_n is the n^{th} summation polynomial.

A simple equation for T_n

$$T_n = \{P \in E(\mathbb{F}_{p^n}) \mid P + \sigma(P) + \ldots + \sigma^{n-1}(P) = \mathcal{O}\} \subset E(\mathbb{F}_{p^n}) \Rightarrow$$
$$T_n \subseteq \{(x,y) \in E(\mathbb{F}_{p^n}) \mid f_n(x, x^p, \ldots, x^{p^{n-1}}) = 0\} \cup \{\mathcal{O}\}$$

where f_n is the n^{th} summation polynomial.

Proposition

Weil restriction on $f_n(x, x^p, \ldots, x^{p^{n-1}})$ produces exactly one equation $\tilde{f}_n(x_0, \ldots, x_{n-1})$ of degree $\leq (n-1)2^{n-2}$.

A simple equation for T_n

$$T_n = \{P \in E(\mathbb{F}_{p^n}) \mid P + \sigma(P) + \ldots + \sigma^{n-1}(P) = \mathcal{O}\} \subset E(\mathbb{F}_{p^n}) \Rightarrow$$
$$T_n \subseteq \{(x,y) \in E(\mathbb{F}_{p^n}) \mid f_n(x, x^p, \ldots, x^{p^{n-1}}) = 0\} \cup \{\mathcal{O}\}$$

where f_n is the n^{th} summation polynomial.

Proposition

Weil restriction on $f_n(x, x^p, \ldots, x^{p^{n-1}})$ produces exactly one equation $\tilde{f}_n(x_0, \ldots, x_{n-1})$ of degree $\leq (n-1)2^{n-2}$.

Remarks:

- This is only an equation for T_n and not for the whole trace zero variety.
- The standard equations for the trace zero varieties are $n+1$ in $2n$ variables.
- The containment above is strict for $n > 3$. E.g., if $(a,b) \in E[3]$, $a \in \mathbb{F}_p$, then $\tilde{f}_5(a,a,a,a,a) = 0$ since $P + P + P + P - P = \mathcal{O}$.
- Assume $n \mid (p-1)$, and $\mathbb{F}_{p^n} = \mathbb{F}_p[\zeta]/(\zeta^n = \mu)$. If $x = \sum_{i=0}^{n-1} x_i \zeta^i$, then $x^p = \sum_{i=0}^{n-1} x_i \mu^{\frac{i(p-1)}{n}} \zeta^i$.

Example ($n = 3$)

Let $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$ and choose the basis $1, \zeta, \zeta^2$.
The elements of T_3 are the zeroes over $\mathbb{F}_p$ of

$$f_3(x, x^p, x^{p^2}) = x^{2p^2+2} - 2x^{2p^2+p+1} + x^{2p(p+1)} - 2x^{p^2+p+2} - 2Ax^{p^2+1} +$$
$$-2x^{(p+1)^2} - 2Ax^{p(1+p)} - 4Bx^{p^2} + x^{2p+2} - 2Ax^{p+1} + A^2 - 4Bx - 4Bx^p$$

Example ($n = 3$)

Let $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$ and choose the basis $1, \zeta, \zeta^2$.
The elements of T_3 are the zeroes over $\mathbb{F}_p$ of

$$f_3(x, x^p, x^{p^2}) = x^{2p^2+2} - 2x^{2p^2+p+1} + x^{2p(p+1)} - 2x^{p^2+p+2} - 2Ax^{p^2+1} + \\ -2x^{(p+1)^2} - 2Ax^{p(1+p)} - 4Bx^{p^2} + x^{2p+2} - 2Ax^{p+1} + A^2 - 4Bx - 4Bx^p$$

which, after Weil restriction, becomes

$$\tilde{f}_3(x_0, x_1, x_2) = -3x_0^4 - 12\mu^2 x_0 x_2^3 - 12\mu x_0 x_1^3 + 18\mu x_0^2 x_1 x_2 + 9\mu^2 x_1^2 x_2^2 - 6Ax_0^2 \\ +6A\mu x_1 x_2 - 12Bx_0 + A^2.$$

Example ($n = 3$)

Let $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$ and choose the basis $1, \zeta, \zeta^2$.
The elements of T_3 are the zeroes over $\mathbb{F}_p$ of

$$f_3(x, x^p, x^{p^2}) = x^{2p^2+2} - 2x^{2p^2+p+1} + x^{2p(p+1)} - 2x^{p^2+p+2} - 2Ax^{p^2+1} + \\ -2x^{(p+1)^2} - 2Ax^{p(1+p)} - 4Bx^{p^2} + x^{2p+2} - 2Ax^{p+1} + A^2 - 4Bx - 4Bx^p$$

which, after Weil restriction, becomes

$$\tilde{f}_3(x_0, x_1, x_2) = -3x_0^4 - 12\mu^2 x_0 x_2^3 - 12\mu x_0 x_1^3 + 18\mu x_0^2 x_1 x_2 + 9\mu^2 x_1^2 x_2^2 - 6Ax_0^2 \\ +6A\mu x_1 x_2 - 12Bx_0 + A^2.$$

Compare with

$$\begin{aligned} y_0^2 + 2\mu y_1 y_2 - x_0^3 - \mu x_1^3 - \mu^2 x_2^3 - 6\mu x_0 x_1 x_2 - Ax_0 - B &= 0 \\ 2y_0 y_1 + \mu y_2^2 - 3\mu x_1^2 x_2 - 3x_0^2 x_1 - 3\mu x_0 x_2^2 - Ax_1 &= 0 \\ 2y_0 y_2 + y_1^2 - 3\mu x_1 x_2^2 - 3x_0^2 x_2 - 3x_0 x_1^2 - Ax_2 &= 0 \\ x_1 y_2 - x_2 y_1 &= 0 \end{aligned}$$

Choice of the factor base

We choose the factor base

$$\mathcal{F} = \{(x_0, \ldots, x_{n-1}) \in T_n \mid x_0 = \ldots = x_{n-3} = 0\}$$
$$= \{(x_0, \ldots, x_{n-1}) \in \mathbb{F}_p^n \mid \tilde{f}_n(0, \ldots, 0, x_{n-2}, x_{n-1}) = 0\}.$$

$\#\mathcal{F} \sim p$ heuristically, experimentally confirmed.

Choice of the factor base

We choose the factor base

$$\mathcal{F} = \{(x_0, \ldots, x_{n-1}) \in T_n \mid x_0 = \ldots = x_{n-3} = 0\}$$
$$= \{(x_0, \ldots, x_{n-1}) \in \mathbb{F}_p^n \mid \tilde{f}_n(0, \ldots, 0, x_{n-2}, x_{n-1}) = 0\}.$$

$\#\mathcal{F} \sim p$ heuristically, experimentally confirmed.

Example ($n = 3$)

Let $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$ and choose the basis $1, \zeta, \zeta^2$. Since

$$\tilde{f}_3(x_0, x_1, x_2) = -3x_0^4 - 12\mu^2 x_0 x_2^3 - 12\mu x_0 x_1^3 + 18\mu x_0^2 x_1 x_2 - 6A x_0^2 + \\ +9\mu^2 x_1^2 x_2^2 + 6A\mu x_1 x_2 - 12B x_0 + A^2$$

we choose the factor base

$$\mathcal{F} = \{(0, x_1, x_2) \mid x_1, x_2 \in \mathbb{F}_p,\ (3\mu x_1 x_2 + A)^2 = 0\}$$

Choice of the factor base

We choose the factor base

$$\mathcal{F} = \{(x_0, \dots, x_{n-1}) \in T_n \mid x_0 = \dots = x_{n-3} = 0\}$$
$$= \{(x_0, \dots, x_{n-1}) \in \mathbb{F}_p^n \mid \tilde{f}_n(0, \dots, 0, x_{n-2}, x_{n-1}) = 0\}.$$

$\#\mathcal{F} \sim p$ heuristically, experimentally confirmed.

Example ($n = 3$)

Let $\mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - \mu)$ and choose the basis $1, \zeta, \zeta^2$. Since

$$\tilde{f}_3(x_0, x_1, x_2) = -3x_0^4 - 12\mu^2 x_0 x_2^3 - 12\mu x_0 x_1^3 + 18\mu x_0^2 x_1 x_2 - 6A x_0^2 + \\ +9\mu^2 x_1^2 x_2^2 + 6A\mu x_1 x_2 - 12B x_0 + A^2$$

we choose the factor base

$$\mathcal{F} = \{(0, x_1, x_2) \mid x_1, x_2 \in \mathbb{F}_p,\ (3\mu x_1 x_2 + A)^2 = 0\}$$
$$= \{(0, x_1, -A(3\mu x_1)^{-1}) \mid x_1 \in \mathbb{F}_p^*\} \quad \text{if } A \neq 0$$
$$= \{(0, x_1, 0) \mid x_1 \in \mathbb{F}_p^*\} \cup \{(0, 0, x_2) \mid x_2 \in \mathbb{F}_p^*\} \quad \text{if } A = 0.$$

Relation search

Decompose a given $R = \alpha P + \beta Q = (a, b) \in T_n$ into a sum

$$R = P_1 + \ldots + P_{n-1}, \qquad P_i \in \mathcal{F}.$$

Translate the decomposition condition into the equation

$$f_n(x_{P_1}, \ldots, x_{P_{n-1}}, a) = 0.$$

Relation search

Decompose a given $R = \alpha P + \beta Q = (a, b) \in T_n$ into a sum

$$R = P_1 + \ldots + P_{n-1}, \qquad P_i \in \mathcal{F}.$$

Translate the decomposition condition into the equation

$$f_n(x_{P_1}, \ldots, x_{P_{n-1}}, a) = 0.$$

Doing Weil restriction with $x_{P_i} = x_{i,n-2}\zeta^{n-2} + x_{i,n-1}\zeta^{n-1}$ one obtains a system of $2n-1$ equations of degree $\leq (n-1)2^{n-2}$ in $2n-2$ variables

$$F_0(0, \ldots, 0, x_{0,n-2}, x_{0,n-1}, \ldots, 0, \ldots, 0, x_{n-1,n-2}, x_{n-1,n-1}, a_0, \ldots, a_{n-1}) = 0$$

$$\vdots$$

$$F_{n-1}(0, \ldots, 0, x_{1,n-2}, x_{1,n-1}, \ldots, 0, \ldots, 0, x_{n-1,n-2}, x_{n-1,n-1}, a_0, \ldots, a_{n-1}) = 0$$

$$\tilde{f}_n(0, \ldots, 0, x_{1,n-2}, x_{1,n-1}) = 0$$

$$\vdots$$

$$\tilde{f}_n(0, \ldots, 0, x_{n-1,n-2}, x_{n-1,n-1}) = 0$$

The system

1. The system consists $2n-1$ equations of degree $\leq (n-1)2^{n-2}$ in $2n-2$ variables.
2. It has two parts, each with a different symmetry in the variables, hence it is hard to symmetrize.
3. It needs to be solved about $p(n-1)!$ times to find about p relations.
4. Each time, one computes a degree reverse lexicographic Gröbner basis, then converts it to a lexicographic one.

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)
- enumerating $\mathcal{F}$ takes $\tilde{\mathcal{O}}(p(n-1)2^{n-2})$

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)
- enumerating $\mathcal{F}$ takes $\tilde{\mathcal{O}}(p(n-1)2^{n-2})$
- computing a degree reverse lexicographic Gröbner basis of the system takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}\right)$ using F5 and assuming that the system is semi-regular (Bardet-Faugere-Salvy-Yang)

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)
- enumerating $\mathcal{F}$ takes $\tilde{\mathcal{O}}(p(n-1)2^{n-2})$
- computing a degree reverse lexicographic Gröbner basis of the system takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}\right)$ using F5 and assuming that the system is semi-regular (Bardet-Faugere-Salvy-Yang)
- converting it to a lexicographic Gröbner basis takes $O((2n-2)\cdot D^3)$ with FGLM, where D is the number of solutions counted with multiplicity in $\overline{\mathbb{F}_p}$, hence $D \leq ((n-1)2^{n-2})^{2n-2}$

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)
- enumerating $\mathcal{F}$ takes $\tilde{\mathcal{O}}(p(n-1)2^{n-2})$
- computing a degree reverse lexicographic Gröbner basis of the system takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}\right)$ using F5 and assuming that the system is semi-regular (Bardet-Faugere-Salvy-Yang)
- converting it to a lexicographic Gröbner basis takes $O((2n-2)\cdot D^3)$ with FGLM, where D is the number of solutions counted with multiplicity in $\overline{\mathbb{F}_p}$, hence $D \leq ((n-1)2^{n-2})^{2n-2}$
- hence relation collection takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}(n-1)!p\right)$ if we solve about $p(n-1)!$ systems

Complexity estimates

- computing the n^{th} summation polynomial and its Weil restriction is polynomial in $\tilde{\mathcal{O}}(e^{n^2})$ (Diem)
- enumerating $\mathcal{F}$ takes $\tilde{\mathcal{O}}(p(n-1)2^{n-2})$
- computing a degree reverse lexicographic Gröbner basis of the system takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}\right)$ using F5 and assuming that the system is semi-regular (Bardet-Faugere-Salvy-Yang)
- converting it to a lexicographic Gröbner basis takes $O((2n-2)\cdot D^3)$ with FGLM, where D is the number of solutions counted with multiplicity in $\overline{\mathbb{F}_p}$, hence $D \leq ((n-1)2^{n-2})^{2n-2}$
- hence relation collection takes $\mathcal{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}(n-1)!p\right)$ if we solve about $p(n-1)!$ systems
- the linear algebra step takes $\mathcal{O}((n-1)p^2)$ with Lanczos' or Wiedermann's algorithm.

Total complexity

The total complexity is then

$$\tilde{\mathcal{O}}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}(n-1)!p+(n-1)p^2\right).$$

Using the double-large prime variation, one collects $p^{2-2/(n-1)}$ and solves a linear system of size $p^{1-1/(n-1)} \times p^{1-1/(n-1)}$.

Theorem

The complexity of solving a DLP in T_n, hence in $E(\mathbb{F}_{p^n})$ for E defined over $\mathbb{F}_p$, is

$$\tilde{O}\left(\binom{(2n-2)(n-1)2^{n-2}+1}{2n-2}^{\omega}(n-1)!p^{2-2/(n-1)}\right).$$

The case of T_3 and T_5

If $n = 3$ we chose the factor base

$$\begin{aligned}\mathcal{F} &= \{(0, x_1, x_2) \mid x_1, x_2 \in \mathbb{F}_p,\ (3\mu x_1 x_2 + A)^2 = 0\} \\ &= \{(0, x_1, -A(3\mu x_1)^{-1}) \mid x_1 \in \mathbb{F}_p^*\} \text{ if } A \neq 0 \\ &= \{(0, x_1, 0) \mid x_1 \in \mathbb{F}_p^*\} \cup \{(0, 0, x_2) \mid x_2 \in \mathbb{F}_p^*\} \text{ if } A = 0.\end{aligned}$$

This allow us to eliminate half the variables.
So we obtain a system of 3 equations in 2 variables of degrees $7, 8, 7$, instead than 5 equations in 4 variables of degrees $4, 4, 4, 2, 2$.
A generic system has regularity 14 in our experiments.

The case of T_3 and T_5

If $n = 3$ we chose the factor base

$$\begin{aligned} \mathcal{F} &= \{(0, x_1, x_2) \mid x_1, x_2 \in \mathbb{F}_p,\ (3\mu x_1 x_2 + A)^2 = 0\} \\ &= \{(0, x_1, -A(3\mu x_1)^{-1}) \mid x_1 \in \mathbb{F}_p^*\} \text{ if } A \neq 0 \\ &= \{(0, x_1, 0) \mid x_1 \in \mathbb{F}_p^*\} \cup \{(0, 0, x_2) \mid x_2 \in \mathbb{F}_p^*\} \text{ if } A = 0. \end{aligned}$$

This allow us to eliminate half the variables.
So we obtain a system of 3 equations in 2 variables of degrees $7, 8, 7$, instead than 5 equations in 4 variables of degrees $4, 4, 4, 2, 2$.
A generic system has regularity 14 in our experiments.

If $n = 5$ we obtain a system of 9 equations in 8 variables of degrees 32.

An example of the system for $n = 3$

Let $p = 2^{12} - 3, \mathbb{F}_{p^3} = \mathbb{F}_p[\zeta]/(\zeta^3 - 2)$, and $E : y^2 = x^3 + x + 21$.

If $R = P_1 + P_2 = (a, b)$, where $x_{P_1} = x_{11}\zeta + x_{12}\zeta^2$, $x_{P_2} = x_{21}\zeta + x_{22}\zeta^2$,
$a = 2960 + 1129\zeta + 1917\zeta^2$, one gets the system

$$\begin{aligned} 439x_{21}^4x_{11}^3 + 1215x_{21}^4x_{11}^2 + 2556x_{21}^4x_{11} + 2274x_{21}^4 + 439x_{21}^3x_{11}^4 + 1663x_{21}^3x_{11}^3 + \\ +1537x_{21}^3x_{11}^2 + 3403x_{21}^3x_{11} + 2023x_{21}^3 + 1215x_{21}^2x_{11}^4 + 1537x_{21}^2x_{11}^3 + 1961x_{21}^2x_{11}^2 + \\ +2070x_{21}^2x_{11} + 2326x_{21}^2 + 2556x_{21}x_{11}^4 + 3403x_{21}x_{11}^3 + 2070x_{21}x_{11}^2 + 3534x_{21}x_{11} + \\ +716x_{21} + 2274x_{11}^4 + 2023x_{11}^3 + 2326x_{11}^2 + 716x_{11} = 0 \\ 2x_{21}^4x_{11}^4 + 3670x_{21}^4x_{11}^3 + 938x_{21}^4x_{11}^2 + 609x_{21}^4x_{11} + 3670x_{21}^3x_{11}^4 + 2217x_{21}^3x_{11}^3 + \ldots = 0 \\ 518x_{21}^4x_{11}^3 + 1692x_{21}^4x_{11}^2 + 2117x_{21}^4x_{11} + 518x_{21}^3x_{11}^4 + 2070x_{21}^3x_{11}^3 + \ldots = 0 \end{aligned}$$

of 3 equations in 2 variables, of degrees $7, 8, 7$. The regularity of the system is 14.

Solving it, one gets $X_{01} = 1770, X_{11} = 1515$, from which $X_{02} = 338, X_{12} = 3029$,

Timings for $n = 3$

$\log_2 \lvert T_3 \rvert$	20	24	28	32	36	40
p	$2^{10} - 3$	$2^{12} - 3$	$2^{14} - 3$	$2^{16} - 15$	$2^{18} - 93$	$2^{20} - 3$
μ	5	2	2	2	2	2
A	2	1	1	1	1	1
B	0	21	11	5	10	25
$\lvert\mathcal{F}\rvert$	900	4002	16380	65388	261822	1045962
number of R's tried	2208	8263	32828	130533	522935	2091965
time for GB	0.00102	0.00169	0.00167	0.00124	0.00146	0.00135
time to solve system	0.00115	0.00180	0.00173	0.00134	0.00159	0.00136
time to collect relations	3.52	13.53	49.71	197.17	803.95	2845.01
time linear algebra	0.01	0.30	5.22	108.29	129.69	–
total time	3.60	14.25	56.08	310.70	957.23	–
$\log_2 \lvert T_3 \rvert$	60	80	100	120	140	160
p	$2^{30} - 105$	$2^{40} - 87$	$2^{50} - 51$	$2^{60} - 93$	$2^{70} - 267$	$2^{79} - 67$
μ	2	2	2	2	5	3
A	1	1	1	1	1	1
B	24	49	40	193	15	368
$\lvert\mathcal{F}\rvert$	$\mathbf{2^{30}}$	$\mathbf{2^{40}}$	$\mathbf{2^{50}}$	$\mathbf{2^{60}}$	$\mathbf{2^{70}}$	$\mathbf{2^{79}}$
number of R's tried	$\mathbf{2^{31}}$	$\mathbf{2^{41}}$	$\mathbf{2^{51}}$	$\mathbf{2^{61}}$	$\mathbf{2^{71}}$	$\mathbf{2^{80}}$
time for GB	0.00146	0.00231	0.00244	0.00249	0.00304	0.00262
time to solve system	0.00171	0.00291	0.00342	0.00351	0.00467	0.00442
time to collect relations	$\mathbf{2^{21.8}}$	$\mathbf{2^{32.5}}$	$\mathbf{2^{42.8}}$	$\mathbf{2^{52.8}}$	$\mathbf{2^{63.2}}$	$\mathbf{2^{72.1}}$

More on the system for $n = 5$

Let $5 \mid (p-1)$ and use $1, \zeta, \dots, \zeta^4$ as $\mathbb{F}_p$-basis of $\mathbb{F}_{p^5} = \mathbb{F}_p[\zeta]/(\zeta^5 - \mu)$.

Let $\mathcal{F} = \{(0,0,0,x_3,x_4) \mid \tilde{f}_5(0,0,0,x_3,x_4) = 0\}$.

More on the system for $n = 5$

Let $5 \mid (p-1)$ and use $1, \zeta, \ldots, \zeta^4$ as $\mathbb{F}_p$-basis of $\mathbb{F}_{p^5} = \mathbb{F}_p[\zeta]/(\zeta^5 - \mu)$.

Let $\mathcal{F} = \{(0,0,0,x_3,x_4) \mid \tilde{f}_5(0,0,0,x_3,x_4) = 0\}$.

Look for relations $R = P_1 + P_2 + P_3$ (Joux-Vitse).

Remark

1. Decreases the probability of finding a relation by a factor p.
2. The system consists of 9 equations in 8 variables, 5 of degree 12 and 4 of degree 32. See `http://www.loria.fr/~mmassier/phdthesis/equations.txt`
3. Use a hybrid approach to solve the system, fixing one variable.

Increase the size of $\mathcal{F}$ to increase the probability of a decomposition, hence reduce the number of systems to be solved.

More on the system for $n = 5$

Let $5 \mid (p-1)$ and use $1, \zeta, \dots, \zeta^4$ as $\mathbb{F}_p$-basis of $\mathbb{F}_{p^5} = \mathbb{F}_p[\zeta]/(\zeta^5 - \mu)$.

Let $\mathcal{F} = \{(0,0,0,x_3,x_4) \mid \tilde{f}_5(0,0,0,x_3,x_4) = 0\}$.

Look for relations $R = P_1 + P_2 + P_3$ (Joux-Vitse).

Remark

1. Decreases the probability of finding a relation by a factor p.
2. The system consists of 9 equations in 8 variables, 5 of degree 12 and 4 of degree 32. See `http://www.loria.fr/~mmassier/phdthesis/equations.txt`
3. Use a hybrid approach to solve the system, fixing one variable.

Increase the size of $\mathcal{F}$ to increase the probability of a decomposition, hence reduce the number of systems to be solved.

This methods needs improvements to become a feasible attack for a T_5 of cryptographic size.

Timings for $n = 5$

$\log_2 \lvert T_5 \rvert$	20	22	27	32	36	40
p	$2^5 - 1$	$2^6 - 23$	$2^7 - 27$	$2^8 - 15$	$2^9 - 21$	$2^{10} - 3$
μ	2	2	2	3	2	2
A	1	1	1	1	1	1
B	16	3	3	13	18	1
$\lvert\mathcal{F}\rvert$	40	70	110	230	520	970
number of R's tried	886	884	2424	**5784**	**11784**	**24528**
number of systems solved	17719	30934	244824	**1393944**	**5785944**	**25043088**
time for GB	1.30	1.31	1.28	1.21	1.22	1.32
time to enumerate $\mathcal{F}$	0.02	0.04	0.07	0.18	0.43	0.89
time to collect relations	25004	38219	171085	**821328**	**3818016**	**15084720**
time linear algebra	0.01	0.01	0.01	0.01	0.01	0.01
total time	25164	43618	171085	**821328**	**3818016**	**15084720**

$\log_2 \lvert T_5 \rvert$	60	80	100	120	140	160
p	$2^{15} - 157$	$2^{20} - 5$	$2^{25} - 61$	$2^{30} - 173$	$2^{35} - 547$	$2^{40} - 195$
μ	3	2	2	2	5	2
A	1	1	1	1	1	1
B	7	10	17	5	3	12
$\lvert\mathcal{F}\rvert$	32600	1051440	$\mathbf{2^{25}}$	$\mathbf{2^{30}}$	$\mathbf{2^{35}}$	$\mathbf{2^{40}}$
number of R's tried	$\mathbf{2^{20}}$	$\mathbf{2^{25}}$	$\mathbf{2^{30}}$	$\mathbf{2^{35}}$	$\mathbf{2^{40}}$	$\mathbf{2^{45}}$
number of systems solved	$\mathbf{2^{35}}$	$\mathbf{2^{45}}$	$\mathbf{2^{55}}$	$\mathbf{2^{65}}$	$\mathbf{2^{75}}$	$\mathbf{2^{85}}$
time for GB of one system	1.34	1.33	7.09	6.93	146.16	147.89
time to enumerate $\mathcal{F}$	38.80	1530.91	$\mathbf{2^{17.1}}$	$\mathbf{2^{22.9}}$	$\mathbf{2^{28.7}}$	$\mathbf{2^{34.0}}$
time to collect relations	$\mathbf{2^{34.3}}$	$\mathbf{2^{45.4}}$	$\mathbf{2^{57.8}}$	$\mathbf{2^{67.7}}$	$\mathbf{2^{82.2}}$	$\mathbf{2^{92.2}}$
time linear algebra	89.12	–	–	–	–	–
total time	$\mathbf{2^{34.3}}$	$\mathbf{2^{45.4}}$	$\mathbf{2^{57.8}}$	$\mathbf{2^{67.7}}$	$\mathbf{2^{82.2}}$	$\mathbf{2^{92.2}}$

Comparison with other attacks

- Pollard ρ on T_n has complexity $\mathcal{O}(p^{\frac{n-1}{2}})$, index calculus on $E(\mathbb{F}_{p^n})$ has complexity $\mathcal{O}(p^{2-\frac{2}{n}})$, while this attack on T_n has complexity $\mathcal{O}(p^{2-\frac{2}{n-1}})$. The latter is lower for $n \geq 5$.

Comparison with other attacks

- Pollard ρ on T_n has complexity $\mathcal{O}(p^{\frac{n-1}{2}})$, index calculus on $E(\mathbb{F}_{p^n})$ has complexity $\mathcal{O}(p^{2-\frac{2}{n}})$, while this attack on T_n has complexity $\mathcal{O}(p^{2-\frac{2}{n-1}})$. The latter is lower for $n \geq 5$.
- Advantage of Pollard ρ on T_n: the constant has the smallest dependency n.

Comparison with other attacks

- Pollard ρ on T_n has complexity $\mathcal{O}(p^{\frac{n-1}{2}})$, index calculus on $E(\mathbb{F}_{p^n})$ has complexity $\mathcal{O}(p^{2-\frac{2}{n}})$, while this attack on T_n has complexity $\mathcal{O}(p^{2-\frac{2}{n-1}})$. The latter is lower for $n \geq 5$.
- Advantage of Pollard ρ on T_n: the constant has the smallest dependency n.
- Advantages of index calculus on $E(\mathbb{F}_{p^n})$: fewer variables, smaller systems to solve.

Comparison with other attacks

- Pollard ρ on T_n has complexity $\mathcal{O}(p^{\frac{n-1}{2}})$, index calculus on $E(\mathbb{F}_{p^n})$ has complexity $\mathcal{O}(p^{2-\frac{2}{n}})$, while this attack on T_n has complexity $\mathcal{O}(p^{2-\frac{2}{n-1}})$. The latter is lower for $n \geq 5$.
- Advantage of Pollard ρ on T_n: the constant has the smallest dependency n.
- Advantages of index calculus on $E(\mathbb{F}_{p^n})$: fewer variables, smaller systems to solve.
- The bottleneck of this attack are (summation polynomials and) Gröbner bases computations. At the moment, the attack is unfeasible for $n > 5$.

Comparison with other attacks

- Pollard ρ on T_n has complexity $\mathcal{O}(p^{\frac{n-1}{2}})$, index calculus on $E(\mathbb{F}_{p^n})$ has complexity $\mathcal{O}(p^{2-\frac{2}{n}})$, while this attack on T_n has complexity $\mathcal{O}(p^{2-\frac{2}{n-1}})$. The latter is lower for $n \geq 5$.
- Advantage of Pollard ρ on T_n: the constant has the smallest dependency n.
- Advantages of index calculus on $E(\mathbb{F}_{p^n})$: fewer variables, smaller systems to solve.
- The bottleneck of this attack are (summation polynomials and) Gröbner bases computations. At the moment, the attack is unfeasible for $n > 5$.
- We welcome ideas on how to simplify our system for $n \geq 5$!

Thank you for your attention!