Sub-exponential algorithms for ECDLP?

Michiel Kosters (UCI)

based on work with Ming-Deh A. Huang (USC), Yun Yang (NTU), Sze Ling Yeo (I2R)

28th September, ECC 2015

Articles

Most content of this talk comes from:

- *Notes on summation polynomials* (Michiel Kosters, Sze Ling Yeo);
- *Last fall degree, HFE, and Weil descent attacks on ECDLP* (Ming-Deh A. Huang, Michiel Kosters, Sze Ling Yeo);
- *On the last fall degree of zero-dimensional Weil descent systems* (Ming-Deh A. Huang, Michiel Kosters, Yun Yang, Sze Ling Yeo).

Contents

1: Prerequisites

ECDLP

Let k be a finite field. Consider an **elliptic curve** over k defined by

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

The set

$$E(k) = \{(x, y) \in k^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}$$

has a natural addition law $+$ which makes $E(k)$ into a *finite abelian group* with identity element ∞.

ECDLP

Let k be a finite field. Consider an **elliptic curve** over k defined by

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

The set

$$E(k) = \{(x, y) \in k^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}$$

has a natural addition law $+$ which makes $E(k)$ into a *finite abelian group* with identity element ∞.

The group $E(k)$ is used in *elliptic curve cryptography* (for example elliptic curve Diffie-Hellman) – ECC 2015 is devoted to this completely! One of the main assumptions is that it is hard to solve the following problem.

Elliptic curve discrete logarithm problem (**ECDLP**): Let $P \in E(k)$ and $Q \in \langle P \rangle$. Find an integer c with $Q = cP$.

Methods for solving ECDLP

Set $N = |\langle P \rangle|$.

Different methods:

- *Generic algorithms*: exhaustive search ($O(N)$), baby-step giant-step ($O(\sqrt{N})$), Pollard's rho ($O(\sqrt{N})$), ...;
- *Special cases*: supersingular curves using pairings (MOV 1993, reduce to discrete logarithm finite field), anomalous curves using p-adic methods (Semaev 1998, ..., poly in $\log(N)$);
- *Weil descent*: index calculus using **Weil descent** for $k = \mathbf{F}_{q^n}$ and summation polynomials (Semaev 2004, Gaudry 2008, Diem 2010, 2012, ...).

In this talk, we will focus on the last approach.

2: Weil descent attacks

Main questions

Can the above method involving Weil descent be used to solve ECDLP in sub-exponential time when $k = \mathbf{F}_{q^n}$

- where q^n goes to infinity, q not necessarily fixed?
- with fixed q, where n goes to infinity?

Answer to the first question

Heuristically using Gröbner basis (Gaudry 2008): the case $k = \mathbf{F}_{q^n}$ where $q \to \infty$ and n fixed can be done in time $\tilde{O}((q^n)^{2/n-2/n^2})$.

Answer to the first question

Heuristically using Gröbner basis (Gaudry 2008): the case $k = \mathbf{F}_{q^n}$ where $q \to \infty$ and n fixed can be done in time $\tilde{O}((q^n)^{2/n-2/n^2})$.

Theorem (Diem 2012)**.**
Let $(q_i)_{i\in\mathbf{Z}_{\geq 0}}$, $(n_i)_{i\in\mathbf{Z}_{\geq 0}}$ be sequences such that $q_i \to \infty$, $n_i \to \infty$ and $n_i/\log(q_i)^2 \to 0$ as $i \to \infty$. Then one can solve ECDLP over $\mathbf{F}_{q_i^{n_i}}$ in expected time $(q_i^{n_i})^{o(1)}$.

The result of Diem uses an algorithm of Rojas in the area of toric varieties to solve the 'decomposition of points'. The hardest part of the paper is to show that the decompositions behave as they are expected to behave.

Answer to the second question

Case $\mathbf{F}_{q^n}$ where q is fixed and $n \to \infty$.

Answer to the second question

Case $\mathbf{F}_{q^n}$ where q is fixed and $n \to \infty$.

Petit–Quisquater 2012, Semaev 2015, Karabina 2015:
sub-exponential algorithms under certain heuristical assumptions.
Results based on some computational evidence.

Answer to the second question

Case $\mathbf{F}_{q^n}$ where q is fixed and $n \to \infty$.

Petit–Quisquater 2012, Semaev 2015, Karabina 2015: sub-exponential algorithms under certain heuristical assumptions. Results based on some computational evidence.

K.–Yeo 2015: raise doubt to correctness of heuristics, by computation and theory.

Answer to the second question

Case $\mathbf{F}_{q^n}$ where q is fixed and $n \to \infty$.

Petit–Quisquater 2012, Semaev 2015, Karabina 2015: sub-exponential algorithms under certain heuristical assumptions. Results based on some computational evidence.

K.–Yeo 2015: raise doubt to correctness of heuristics, by computation and theory.

Current status: complexity of such an approach is still *unknown*. More research is needed.

Solving ECDLP (simplified index calculus)

Given E/k elliptic curve, $P \in E(k)$ and $Q \in \langle P \rangle$.

Main steps for solving ECDLP (*index calculus*). First fix $m \in \mathbf{Z}_{\geq 2}$.

1. *Factor base*: Construct a factor base $\mathcal{B} \subseteq E(k)$;
2. *Relation search* (repeat about $|\mathcal{B}|$ times): pick $a, b \in \mathbf{Z}$ random and write $aP + bQ = b_1 + \ldots + b_m$ with $b_i \in \mathcal{B}$;
3. *Linear algebra*: Use linear algebra on relations from 2 to find c with $Q = cP$.

Solving ECDLP (simplified index calculus)

Given E/k elliptic curve, $P \in E(k)$ and $Q \in \langle P \rangle$.

Main steps for solving ECDLP (*index calculus*). First fix $m \in \mathbf{Z}_{\geq 2}$.

1. *Factor base*: Construct a factor base $\mathcal{B} \subseteq E(k)$;
2. *Relation search* (repeat about $|\mathcal{B}|$ times): pick $a, b \in \mathbf{Z}$ random and write $aP + bQ = b_1 + \ldots + b_m$ with $b_i \in \mathcal{B}$;
3. *Linear algebra*: Use linear algebra on relations from 2 to find c with $Q = cP$.

We must pick m, $\mathcal{B}$. For example, the larger $\mathcal{B}$, the harder the linear algebra and the more relations we need, but it might be easier to find relations.

One chooses these parameters based on the complexity of the relation search. Hence it is important to study this step.

Factor base

From now on: $k = \mathbf{F}_{q^n}$.

Let $V \subseteq k$ be an $\mathbf{F}_q$-subspace of dimension n'. Set

$$\mathcal{B} = \{P' \in E(k) : x(P') \in V\}.$$

Summation polynomials 1

Theorem (Semaev 2004)**.**
Given $r \in \mathbf{Z}_{\geq 2}$*, there exists* $S_r \in k[X_1, \ldots, X_r]$ *with the following property. For* $b_1, \ldots, b_r \in \overline{k}$ *one has* $S_r(b_1, \ldots, b_r) = 0$ *if and only if there exist* $P_1, \ldots, P_r \in E(\overline{k})$ *with* $x(P_i) = b_i$ *such that* $P_1 + \ldots + P_r = \infty$.

Summation polynomials 2

Set

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1 a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 + 4a_2 a_6 - a_4^2. \end{aligned}$$

Then one can put

$$\begin{aligned} S_3 = &(X_1^2 X_2^2 + X_1^2 X_3^2 + X_2^2 X_3^2) - 2(X_1^2 X_2 X_3 + X_1 X_2^2 X_3 + X_1 X_2 X_3^2) \\ &- b_2(X_1 X_2 X_3) - b_4(X_1 X_2 + X_1 X_3 + X_2 X_3) - b_6(X_1 + X_2 + X_3) - b_8, \end{aligned}$$

and for $r \geq 4$ one sets

$$S_r = \mathrm{Res}_X \left(S_{r-1}(X_1, \ldots, X_{r-2}, X), S_3(X_{r-1}, X_r, X) \right).$$

Relation search

Suppose we want to decompose $aP + bQ = b_1 + \ldots + b_m$.

Set $f = \prod_{v \in V}(X - v) \in k[X]$.

Consider the following system in $k[X_1, \ldots, X_m]$:

$$\mathcal{F} = \{S_{m+1}(X_1, \ldots, X_m, x(aP + bQ)), f(X_1), \ldots, f(X_m)\}.$$

Solving this system allows one to obtain relations: if the system has a solution, then one can try all corresponding points and obtain a possible decomposition (often one finds decompositions over bigger fields).

Relation search

Suppose we want to decompose $aP + bQ = b_1 + \ldots + b_m$.

Set $f = \prod_{v \in V}(X - v) \in k[X]$.

Consider the following system in $k[X_1, \ldots, X_m]$:

$$\mathcal{F} = \{S_{m+1}(X_1, \ldots, X_m, x(aP + bQ)), f(X_1), \ldots, f(X_m)\}.$$

Solving this system allows one to obtain relations: if the system has a solution, then one can try all corresponding points and obtain a possible decomposition (often one finds decompositions over bigger fields).

Problems when using generic Gröbner basis algorithm:

1. $f(X_i)$ has high degree;
2. S_{m+1} has high degree and is hard to compute.

Weil descent

We have $\mathcal{F} \subset k[X_1, \ldots, X_m]$. Using **Weil descent** we can construct a system

$$\mathcal{F}' \subseteq \mathbf{F}_q[X_{ij} : i = 1, \ldots, m, j = 1, \ldots, n] = S.$$

such that solutions of $\mathcal{F}'$ over $\mathbf{F}_q$ correspond to solutions of $\mathcal{F}$ over k.

After Weil descent, the $f(X_i)$ become *linear polynomials*.

Weil descent

We have $\mathcal{F} \subset k[X_1, \ldots, X_m]$. Using **Weil descent** we can construct a system

$$\mathcal{F}' \subseteq \mathbf{F}_q[X_{ij} : i = 1, \ldots, m, j = 1, \ldots, n] = S.$$

such that solutions of $\mathcal{F}'$ over $\mathbf{F}_q$ correspond to solutions of $\mathcal{F}$ over k.

After Weil descent, the $f(X_i)$ become *linear polynomials*.

Construction of Weil descent of one polynomial $g \in k[X_1, \ldots, X_m]$:

- Fix basis $\alpha_1, \ldots, \alpha_n$ of $k/\mathbf{F}_q$ and substitute $X_i = \sum_{j=1}^{n} \alpha_j X_{ij}$
- Write

$$g(X_1, \ldots, X_m) = \sum_{i=1}^{n} [g]_i \alpha_i$$

where $[g]_i \in S$ (and we reduce modulo $X_{ij}^q - X_{ij}$).

The set $\{[g]_1, \ldots, [g]_n\}$ is the Weil descent of $\{g\}$.

Example of Weil descent

Consider $S = S_3(X, Y, x(P))$ for some specific curve $\mathbf{F}_{2^4}$. One specific Weil descent looks like:

$$
\begin{aligned}
[S]_1 &= X_2X_4 + X_2 + X_3 + 1, \\
[S]_2 &= X_2X_4 + X_1 + X_3 + 1, \\
[S]_3 &= X_2X_3 + X_1X_4 + X_2X_4 + X_1 + X_2 + X_3 + X_4 + 1, \\
[S]_4 &= X_1X_3 + X_2X_3 + X_1X_4 + X_1 + X_2 + X_3 + X_4.
\end{aligned}
$$

Splitting trick

2015 (Semaev, Karabina, Huang–Petit–Shinohara–Takagi, Yeo): Instead of considering the system $\mathcal{F}$ which involves S_{m+1}, one can introduce a system with more variables which only involve (many) S_3 polynomials and the $f(X_i)$ - one essentially removes the Res in making S_r.

Splitting trick

2015 (Semaev, Karabina, Huang–Petit–Shinohara–Takagi, Yeo): Instead of considering the system $\mathcal{F}$ which involves S_{m+1}, one can introduce a system with more variables which only involve (many) S_3 polynomials and the $f(X_i)$ - one essentially removes the Res in making S_r.

Idea: $P_1 + P_2 + P_3 + P_4 = \infty$ is almost the same as:

$$P_1 + P_2 + Q_1 = \infty$$
$$-Q_1 + P_3 + P_4 = \infty.$$

So instead of $\{S_4(X_1, X_2, X_3, X_4)\}$ one can consider $\{S_3(X_1, X_2, Y_1), S_3(Y_1, X_3, X_4)\}$, where Y_1 is unrestricted (no subspace constraints). One can easily generalize this for $r > 4$.

Weil descent and splitting trick

If one combines Weil descent and the splitting trick, one obtains a system $\mathcal{F}''$ of low degree, but with a lot of variables.

One can easily write down this system and give it to a computer to solve the system!

3: First fall degree assumption

A very very brief introduction to Gröbner basis

Let $\mathcal{G} = \{g_1, \ldots, g_t\} \subset k[X_1, \ldots, X_s] = R$ and let I be the ideal generated by $\mathcal{G}$. Put a monomial order $\leq$ on R.

A Gröbner basis for $\mathcal{G}$ with respect to $\leq$ is a finite subset of I such that the leading term ideal generated by this set is the same as the one of I.

Facts:

- a Gröbner basis can be computed using Buchberger's algorithm (or $F4, F5$);
- Gröbner bases have many practical applications (solving polynomial systems, ideal membership, ...);

The complexity of solving a system using Gröbner basis algorithms depends on the so-called *degree of regularity* of the system (maximal degree seen in computation using the degrevlex order).

First fall degree assumption

From now on: $k = \mathbf{F}_{2^n}$.

Definition.
Let $\mathcal{G} = \{g_1, \ldots, g_t\} \subset k[X_1, \ldots, X_s] = R$. The *first fall degree* d_{ff} of $\mathcal{G}$ is the smallest d such that there exist $h_1, \ldots, h_t \in R$ with $\max_i(\deg(h_i g_i)) = d$ and $0 \leq \deg(\sum_i h_i g_i) < d$.

First fall degree assumption

From now on: $k = \mathbf{F}_{2^n}$.

Definition.
Let $\mathcal{G} = \{g_1, \ldots, g_t\} \subset k[X_1, \ldots, X_s] = R$. The *first fall degree* d_{ff} of $\mathcal{G}$ is the smallest d such that there exist $h_1, \ldots, h_t \in R$ with $\max_i(\deg(h_i g_i)) = d$ and $0 \leq \deg(\sum_i h_i g_i) < d$.

Conjecture (Petit–Quisquater 2012, Semaev 2015, Karabina 2015,...).
The degree of regularity of $\mathcal{F}'$ (respectively $\mathcal{F}''$) is 'close' to the first fall degree of $\mathcal{F}'$ (respectively $\mathcal{F}''$).

This conjecture leads to **sub-exponential** algorithms for ECDLP since the first fall degree can be bounded!

Problems with first fall degree conjecture 0

- The notion of first fall degree does not behave very well under certain operations and the definition feels a bit artificial.
- It is unclear in which generality the first fall degree conjecture should hold and it unclear what close would really mean. Why only for $\mathbf{F}_{2^n}$?
- Artificial problem: Gröbner basis algorithms in Magma are not open source, and it is hard to read off the first fall degree! Hence, not enough experiments have been done.

Problems with first fall degree conjecture 1

Let l be a finite field. Set $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, 0, 0)$ (this gives a singular curve).
For the corresponding summation polynomial one has: for $x_1, \ldots, x_r \in l^*$ one has $S_r(1/x_1^2, \ldots, 1/x_r^2) = 0$ iff there is a solution to $\pm x_1 \pm \ldots \pm x_r = 0$.
Assume $\mathrm{char}(l) \neq 2$. The latter is equivalent to checking if there is a subset of $\{x_1, \ldots, x_r\}$ summing to $\frac{x_1 + \ldots + x_r}{2}$.

Problems with first fall degree conjecture 1

Let l be a finite field. Set $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, 0, 0)$ (this gives a singular curve).
For the corresponding summation polynomial one has: for $x_1, \ldots, x_r \in l^*$ one has $S_r(1/x_1^2, \ldots, 1/x_r^2) = 0$ iff there is a solution to $\pm x_1 \pm \ldots \pm x_r = 0$.
Assume $\mathrm{char}(l) \neq 2$. The latter is equivalent to checking if there is a subset of $\{x_1, \ldots, x_r\}$ summing to $\frac{x_1 + \ldots + x_r}{2}$.

Theorem.
Fix a prime $p \geq 3$. Given a subset S of $G = (\mathbf{Z}/p\mathbf{Z})^n$ and $t \in G$, it is NP-complete to determine if there is a subset of S summing to t.

Problems with first fall degree conjecture 1

Let l be a finite field. Set $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, 0, 0)$ (this gives a singular curve).
For the corresponding summation polynomial one has: for $x_1, \ldots, x_r \in l^*$ one has $S_r(1/x_1^2, \ldots, 1/x_r^2) = 0$ iff there is a solution to $\pm x_1 \pm \ldots \pm x_r = 0$.
Assume $\mathrm{char}(l) \neq 2$. The latter is equivalent to checking if there is a subset of $\{x_1, \ldots, x_r\}$ summing to $\frac{x_1 + \ldots + x_r}{2}$.

Theorem.
Fix a prime $p \geq 3$. Given a subset S of $G = (\mathbf{Z}/p\mathbf{Z})^n$ and $t \in G$, it is NP-complete to determine if there is a subset of S summing to t.

It is NP-complete to check if $S_r(1/x_1^2, \ldots, 1/x_r^2)$ is 0 or not, and one can do this if one can solve systems similar to $\mathcal{F}'$ and $\mathcal{F}''$. For the system $\mathcal{F}''$ with certain first fall degree conjectures, this would lead to P = NP.

Problems with first fall degree conjecture 2

Consider the system $\mathcal{F}'$ (or $\mathcal{F}''$) when $m = 2$: this is the Weil descent of $S_3(X_1, X_2, x)$ together with subspace constraints ($n' = n/2$).
Previously:

n	First fall degree	Degree of regularity	Random
12	≤ 4	3	4
16	≤ 4	3	5
18	≤ 4	4	5
20	≤ 4	4	5
24	≤ 4	4	6
30	≤ 4	4	–
40	≤ 4	**conjecture** : 4	–

Problems with first fall degree conjecture 2

Consider the system $\mathcal{F}'$ (or $\mathcal{F}''$) when $m = 2$: this is the Weil descent of $S_3(X_1, X_2, x)$ together with subspace constraints ($n' = n/2$).
Now:

n	First fall degree	Degree of regularity	Random
12	2	3	4
16	2	3	5
18	2	4	5
20	2	4	5
24	2	4	6
30	2	4	–
40	2	≥ 5	–

The gap between the degree of regularity and the first fall degree seems to increase: **doubt** on sub-exponential estimates.

Example of fall degree

Consider $S = S_3(X, Y, x(P))$ for some specific curve $\mathbf{F}_{2^4}$. Under some basis one has:

$$
\begin{aligned}
[S]_1 &= X_2X_4 + X_2 + X_3 + 1, \\
[S]_2 &= X_2X_4 + X_1 + X_3 + 1, \\
[S]_3 &= X_2X_3 + X_1X_4 + X_2X_4 + X_1 + X_2 + X_3 + X_4 + 1, \\
[S]_4 &= X_1X_3 + X_2X_3 + X_1X_4 + X_1 + X_2 + X_3 + X_4.
\end{aligned}
$$

Example of fall degree

Consider $S = S_3(X, Y, x(P))$ for some specific curve $\mathbf{F}_{2^4}$. Under some basis one has:

$$\begin{aligned}
[S]_1 =& X_2X_4 + X_2 + X_3 + 1,\\
[S]_2 =& X_2X_4 + X_1 + X_3 + 1,\\
[S]_3 =& X_2X_3 + X_1X_4 + X_2X_4 + X_1 + X_2 + X_3 + X_4 + 1,\\
[S]_4 =& X_1X_3 + X_2X_3 + X_1X_4 + X_1 + X_2 + X_3 + X_4.
\end{aligned}$$

One has:

$$[S]_1 + [S]_2 = X_1 + X_2.$$

First fall degree is 2.

Explaining first fall degree 1

Lenstra and K. discovered the following in 2013 using CFT:

Theorem.
Let E/k be an elliptic curve given by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. Assume that E is ordinary ($a_1 \neq 0$). Then we have a surjective group morphism

$$\begin{aligned} E(k) &\to \mathbb{F}_2 \\ \infty &\mapsto 0 \\ P &\mapsto \mathrm{Tr}_{k/\mathbb{F}_2}\left(\frac{x(P)+a_2}{a_1^2}\right) \end{aligned}$$

with kernel $2E(k)$.

Explaining first fall degree 1

Lenstra and K. discovered the following in 2013 using CFT:

Theorem.
Let E/k be an elliptic curve given by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. Assume that E is ordinary ($a_1 \neq 0$). Then we have a surjective group morphism

$$\begin{aligned} E(k) &\to \mathbb{F}_2 \\ \infty &\mapsto 0 \\ P &\mapsto \mathrm{Tr}_{k/\mathbb{F}_2}\left(\frac{x(P)+a_2}{a_1^2}\right) \end{aligned}$$

with kernel $2E(k)$.

It is a morphism: if $P_1 + P_2 + P_3 = \infty$, then we get $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda + a_2$ and this gives

$$\frac{x_1+a_2}{a_1^2} + \frac{x_2+a_2}{a_1^2} + \frac{x_3+a_2}{a_1^2} = \left(\frac{\lambda}{a_1}\right)^2 + \frac{\lambda}{a_1}.$$

Explaining first fall degree 2

Corollary.
Assume that E is ordinary. Let $P \in E(k) \setminus E(k)[2]$ and set $T = S_3(X_1, X_2, x(P)) \in k[X_1, X_2]$. Set $b = a_1(a_1 x(P) + a_3) \in k^*$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of k over $\mathbf{F}_2$. Then one has

$$\sum_j \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{\alpha_j}{b^2}\right)[T]_j = \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{x(P)+a_2}{a_1^2}\right) + \sum_{j=1}^{n} \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{\alpha_j}{a_1^2}\right)\cdot(X_{1j}+X_{2j})\,.$$

The $[T]_j$ have usually degree 2, whereas the right hand side is usually of degree 1: *degree fall.*

Explaining first fall degree 2

Corollary.
Assume that E is ordinary. Let $P \in E(k) \setminus E(k)[2]$ and set $T = S_3(X_1, X_2, x(P)) \in k[X_1, X_2]$. Set $b = a_1(a_1 x(P) + a_3) \in k^*$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of k over $\mathbf{F}_2$. Then one has

$$\sum_j \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{\alpha_j}{b^2}\right)[T]_j = \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{x(P)+a_2}{a_1^2}\right) + \sum_{j=1}^{n} \mathrm{Tr}_{k/\mathbf{F}_2}\left(\frac{\alpha_j}{a_1^2}\right)\cdot(X_{1j}+X_{2j})\,.$$

The $[T]_j$ have usually degree 2, whereas the right hand side is usually of degree 1: *degree fall*.

Question: it is easy to see that there is a polynomial expression in the $[T]_j$ giving the right hand side, but why is it linear?

Big question

How does the degree of regularity grow as a function of the various parameters for the systems $\mathcal{F}'$ and $\mathcal{F}''$? It seems to grow slower than random similar systems. If slow enough, this approach gives good algorithms for ECDLP.

Big question

How does the degree of regularity grow as a function of the various parameters for the systems $\mathcal{F}'$ and $\mathcal{F}''$? It seems to grow slower than random similar systems. If slow enough, this approach gives good algorithms for ECDLP.

Currently, we do not understand the situation. Estimating the complexity of a Gröbner basis algorithm in general is very hard. It also seems to be too hard to do experiments at the moment. New ideas are needed!

4: Attempt to study complexity

Where does the first fall degree conjecture come from?

There is a polynomial system coming from the cryptographic protocol **HFE** which looks very similar. In that case, the first fall degree conjecture seems to hold.

Where does the first fall degree conjecture come from?

There is a polynomial system coming from the cryptographic protocol **HFE** which looks very similar. In that case, the first fall degree conjecture seems to hold.

Questions:

- What is the difference between the ECDLP and the HFE systems?
- Can we prove (=no heuristics) results regarding complexity of solving the HFE system?

HFE system

Set $k = \mathbf{F}_{q^n}$. Let $f \in k[X]$. Let $\mathcal{F}'$ be a Weil descent system of $\{f\}$ in $\mathbf{F}_q[X_1, \ldots, X_n]$. Perturb $\mathcal{F}'$ using transformations to obtain a system $\mathcal{G}$.

Hidden field equations (**HFE**, Patarin 1996): easy to find zeros of f in k, but hard to find zeros of $\mathcal{G}$ in $\mathbf{F}_q$ without knowing transformations.

HFE system

Set $k = \mathbf{F}_{q^n}$. Let $f \in k[X]$. Let $\mathcal{F}'$ be a Weil descent system of $\{f\}$ in $\mathbf{F}_q[X_1, \ldots, X_n]$. Perturb $\mathcal{F}'$ using transformations to obtain a system $\mathcal{G}$.

Hidden field equations (**HFE**, Patarin 1996): easy to find zeros of f in k, but hard to find zeros of $\mathcal{G}$ in $\mathbf{F}_q$ without knowing transformations.

Experiments (Faugère 2002, ...): degree of regularity of $\mathcal{G}$ depends on q, $\deg(f)$, but not on n and is quite low, and hence one can solve the system relatively easily. Furthermore, looks like degree of regularity is close to first fall degree.

Proofs: "Our conclusions rely on no heuristic assumptions beyond the standard assumption that the Gröbner basis algorithms terminate at or shortly after the degree of regularity." (Ding–Hodges 2011, ...); proof? (Petit 2013).

Last fall degree 1

Let k be a field. Let $\mathcal{F} \subset R = k[X_1, \ldots, X_m]$ be a finite set generating an ideal I.

Definition.

For $i \in \mathbf{Z}_{\geq 0}$, we let V_i be the smallest k-vector space such that

1. $\{f \in \mathcal{F} : \deg(f) \leq i\} \subseteq V_i$;
2. if $g \in V_i$ and if $h \in R$ with $\deg(hg) \leq i$, then $hg \in V_i$.

We set $V_\infty = I$. Note: $V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots \subseteq V_\infty = I$ and $V_i \subseteq R_{\leq i}$.

Last fall degree 1

Let k be a field. Let $\mathcal{F} \subset R = k[X_1, \ldots, X_m]$ be a finite set generating an ideal I.

Definition.

For $i \in \mathbf{Z}_{\geq 0}$, we let V_i be the smallest k-vector space such that

1. $\{f \in \mathcal{F} : \deg(f) \leq i\} \subseteq V_i$;
2. if $g \in V_i$ and if $h \in R$ with $\deg(hg) \leq i$, then $hg \in V_i$.

We set $V_\infty = I$. Note: $V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots \subseteq V_\infty = I$ and $V_i \subseteq R_{\leq i}$.

Definition.

The minimal $d \in \mathbf{Z}_{\geq 0} \sqcup \{\infty\}$ such that for all $h \in I$ we have $h \in V_{\max(d, \deg(h))}$, is called the **last fall degree** of $\mathcal{F}$, and is denoted by $d_{\mathcal{F}}$.

Last fall degree 2

An *equivalent* definition: $d_{\mathcal{F}}$ is the **largest** integer d such that

$$V_d \cap R_{\leq d-1} \neq V_{d-1}$$

Last fall degree 2

An *equivalent* definition: $d_{\mathcal{F}}$ is the **largest** integer d such that

$$V_d \cap R_{\leq d-1} \neq V_{d-1}$$

This is very similar to a more natural notion of the first fall degree: the first fall degree *should* be the **smallest** integer d with

$$V_d \cap R_{\leq d-1} \neq V_{d-1}.$$

Last fall degree 3

Properties of the last fall degree:

- $d_{\mathcal{F}} \in \mathbf{Z}_{\geq 0}$.
- $d_{\mathcal{F}}$ does not depend on any monomial order, behaves well under linear change of variables and of linear change of polynomials.
- "$d_{\mathcal{F}}$ is at most the degree of regularity" (if V_d contains a Gröbner basis for some order, then one has $d_{\mathcal{F}} \leq d$).
- If the system $\mathcal{F}$ has e solutions over the algebraic closure and is radical, then one can solve the system by computing $V_{\max(d_{\mathcal{F}},e)}$ and monovariate factoring algorithms (use projection polynomials; looks a lot like mutant XL).

Last fall degree 3

Properties of the last fall degree:

- $d_{\mathcal{F}} \in \mathbf{Z}_{\geq 0}$.
- $d_{\mathcal{F}}$ does not depend on any monomial order, behaves well under linear change of variables and of linear change of polynomials.
- "$d_{\mathcal{F}}$ is at most the degree of regularity" (if V_d contains a Gröbner basis for some order, then one has $d_{\mathcal{F}} \leq d$).
- If the system $\mathcal{F}$ has e solutions over the algebraic closure and is radical, then one can solve the system by computing $V_{\max(d_{\mathcal{F}},e)}$ and monovariate factoring algorithms (use projection polynomials; looks a lot like mutant XL).

The third and the fourth point explain why it is sometimes faster to solve a system than to find a Gröbner basis when the number of solutions is small (XL vs Gröbner).

Solving HFE

Let $k = \mathbf{F}_{q^n}$ and let $f \in k[X]$ nonzero with HFE system $\mathcal{G}$.

Theorem.
Assume that f has $\leq e$ different solutions in k. Set

$$d = \max(\lfloor 2(q-1)\left(\log_q\left(\deg(f)\right)+1\right)\rfloor, q, e).$$

One can deterministically find all solutions to $\mathcal{G}$ in time polynomial in $(n+d)^d$.

Note that d does *not* depend on n.

Idea of proof: upper bound last fall degree using some sparse GCD algorithm.

ECDLP versus HFE

Differences:

- HFE system is 0-**dimensional** (=finitely many solutions) and one can generalize our results to multivariate 0-dimensional systems $\mathcal{F}$. We can relate last fall degree after Weil descent with the last fall degree before Weil descent for 0-dimensional systems.
- ECDLP system (without subspace constraints) is **not** 0-**dimensional**.

Conclusion

We raise **doubt** to the **first fall degree assumption** for systems which are not zero-dimensional.
In particular, we **doubt** the recent **subexponential time** complexity estimates for solving ECDLP using summation polynomials and Gröbner basis algorithms over $\mathbf{F}_{2^n}$ with n prime. More research is needed to understand the complexity of this approach.

I believe ECDLP over $\mathbf{F}_{2^n}$ with n prime is still **safe** when using the current generation of computers.

Thank you for your attention!