DISCRETE LOGARITHMS
IN QUASI-POLYNOMIAL TIME
IN FINITE FIELDS OF SMALL CHARACTERISTIC

Benjamin Wesolowski

ECC 2019: 23rd Workshop on
Elliptic Curve Cryptography
December 2019
Bochum, Germany

Based on a joint work with
Thorsten Kleinjung
RIGOROUS OR HEURISTIC

If it seems to work, is it good enough?
RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with $p$ fixed and $n \to \infty$... think $\mathbb{F}_{2^n}$):

- Given a generator $g$ of $\mathbb{F}_{p^n}^\times$ and an arbitrary element $h$, find an integer $m$ such that $h = g^m$
- Pomerance (1987) proved complexity $L_{p^n}(1/2)$
- We prove it can be done in quasi-polynomial time

$$L_{p^n}(\alpha) = e^{O((\log p^n)^\alpha (\log \log p^n)^{1-\alpha})}$$

quasi-poly($\log p^n$) $= e^{O(1)}$

For constant $p$:

$= e^{n^{O(1)}}$

$= e^{\log(n)^{O(1)}}$
RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with $p$ fixed and $n \to \infty$... think $\mathbb{F}_{2^n}$):

- Given a generator $g$ of $\mathbb{F}_{p^n}^{\times}$ and an arbitrary element $h$, find an integer $m$ such that $h = g^m$

  ➞ Pomerance (1987) proved complexity $L_{p^n}(1/2)$

  ➞ We prove it can be done in quasi-polynomial time

**Theorem:** Given any prime number $p$ and any positive integer $n$, the discrete logarithm problem in the group $\mathbb{F}_{p^n}^{\times}$ can be solved in expected time $(pn)^{2\log_2(n) + O(1)}$
TIMELINE

1922  |  KRAITCHIK  |  NO COMPLEXITY
1968  |  MILLER, WESTERN  |  NO COMPLEXITY
1976  |  DIFFIE, HELLMAN  |  BEST KNOWN O(Q^{1/2})
1979  |  ADLEMAN  |  L(1/2) IN LARGE CHAR.
1982  |  HELLMAN, REYNERI  |  L(1/2)
1984  |  COPPERSMITH  |  L(1/3)
1987  |  POMERANCE  |  L(1/2)
...  |  ...  |  ...
2013  |  JOUX  |  L(1/4)
2013  |  BARBULESCU, GAUDRY, JOUX, THOME  |  QUASI-POLY
2014  |  GRANGER, KLEINJUNG, ZUMBRAGEL  |  QUASI-POLY
2019  |  THIS WORK (KLEINJUNG, W.)  |  QUASI-POLY
A RIGOROUS ALGORITHM

Finely crafted and analysed by Pomerance in 1987
AN INDEX CALCULUS ALGORITHM

- $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(J)$, generator $g \in \mathbb{F}_{p^n}^\times$

- Factor base $\mathcal{G} = \{ f \in \mathbb{F}_p[x] \mid \text{deg}(f) \leq B, \text{monic, irreducible} \} \cup \{g\}$

- Index calculus:

  ➡ Relation collection: collect relations of the form
  $$\sum_{f \in \mathcal{G}} e_f \log_g f = r \pmod{p^n - 1}$$

  ➡ Linear algebra: the relations form a linear system with unknowns $\log_g f$. Solve it, recover the values $\log_g f$

  ➡ Individual logarithm: given $h \in \mathbb{F}_{p^n}$, compute $\log_g h$
INDEX CALCULUS FROM DESCENT

- **Descent**: given \( h \in \mathbb{F}_{p^n}^\times \) find integers \( e_f \), for \( f \) in \( \mathcal{S} \), such that

\[
h = \prod_{f \in \mathcal{S}} f^{e_f}
\]

- **Relation collection**: generate random \( r \in [1, p^n - 1] \),

\[
r = \log_g(\text{descent}(g^r)) = \sum_{f \in \mathcal{S}} e_f \log_g f
\]

- **Individual logarithm**: given \( h \),

\[
\log_g h = \log_g(\text{descent}(h)) = \sum_{f \in \mathcal{S}} e_f \log_g f
\]
SUMMARY

Efficient Descent Algorithm

Pomerance: there is a descent of complexity $L(1/2)$

Efficient Algorithm for Computing Logarithms

So one can solve DLP in time $L(1/2)$
A ZIGZAG DESCENT
Descending one step at a time
A HEURISTIC QUASI-POLYNOMIAL ALGORITHM

Theorem (Granger, Kleinjung, Zumbrägel): the DLP in fixed characteristic can be solved in expected quasi-poly. time in fields that admit a suitable representation

- Suitable representation? Field $\mathbb{F}_{q^4}[x]/(J)$ where $J$ is an irreducible polynomial in $\mathbb{F}_{q^4}[x]$ such that

\[ x^q = h_0/h_1 \mod J \]

with $h_0$ and $h_1$ polynomials in $\mathbb{F}_{q^4}[x]$ of degree at most 2

- Expected time $q^{\log_2(\deg(J))}$
A DESCENT IS SUFFICIENT

A descent algorithm is sufficient

- Fix the factor base $\mathcal{F} = \{ \text{linear polynomials in } \mathbb{F}_{q^4}[x] \}$

- **Descent:** Given any polynomial $Q$ in $\mathbb{F}_{q^4}[x]$ find integers $e_f$, for $f$ in $\mathcal{F}$, such that

$$Q \equiv \prod_{f \in \mathcal{F}} f^{e_f} \pmod{J}.$$ 

- Main ingredient of the descent, **degree 2 to 1 elimination:** given a degree 2 polynomial over an extension $k$ of $\mathbb{F}_{q^4}$, rewrite it as a product of degree 1 polynomials over $k$
ZIGZAG DESCENT

The zigzag descent: transform the degree 2 to 1 elimination into a full descent algorithm

\[ \mathbb{F}_{q^4 \cdot 2^{e-1}} \]
\[ \mathbb{F}_{q^4 \cdot 2^{e-2}} \]
\[ \mathbb{F}_{q^8} \]
\[ \mathbb{F}_{q^4} \]
ZIGZAG DESCENT

The zigzag descent: transform the degree 2 to 1 elimination into a full descent algorithm

Degree 2 to 1 elimination

\[ \mathbb{F}_{q^{4 \cdot 2^{e-1}}} \]
\[ \mathbb{F}_{q^{4 \cdot 2^{e-2}}} \]
\[ \mathbb{F}_{q^8} \]
\[ \mathbb{F}_{q^4} \]

\[ \mathbb{F}_{q^{4 \cdot 2^{e-1}}} \]
\[ \mathbb{F}_{q^{4 \cdot 2^{e-2}}} \]

\[ \text{Rewrite as irreducible of degree } 2^e \]

\[ Q \text{ in } \mathbb{F}_q[x] \text{ of degree } D \]

\[ \text{Factorisation into quadratics over } \mathbb{F}_{q^{4 \cdot 2^{e-1}}} \]
SUMMARY

DEGREE 2 TO 1 ELIMINATION

DESCENT ALGORITHM

EFFICIENT ALGORITHM FOR COMPUTING LOGARITHMS
GKZ'S DEGREE 2 TO 1 ELIMINATION

A building block
POLYNOMIALS WITH HIGHER SPLITTING PROBABILITY

Fix an extension $k$ of $\mathbb{F}_{q^4}$, and let $Q$ an irreducible quadratic in $k[x]$

- Key idea (from [GGMZ13]): polynomials of the form

$$\alpha x^q + 1 + \beta x^q + \gamma x + \delta \quad \text{in} \quad k[x]$$

have a high probability to split over $k$ (around $q^{-3}$)

- Let $V$ be the vector space of dimension 4 of these polynomials, i.e., $V = \text{span}(x^q + 1, x^q, x, 1) \subset k[x]$

SMOOTH RELATIONS

- \( V = \text{span}(x^q + 1, x^q, x, 1) \subset k[x] \)

- We have \( x^q \equiv h_0/h_1 \mod J \), so

\[
\alpha x^q + 1 + \beta x^q + \gamma x + \delta \equiv \frac{\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1}{h_1} \mod J
\]

Splits with high probability numerators of degree 3

- Consider the vector subspace \( V_Q \) of dimension 2 in \( V \), where \( Q \) divides the right-hand side:

\[
V_Q = \{ \alpha x^q + 1 + \beta x^q + \gamma x + \delta \mid \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \equiv 0 \mod Q \}\]
THE DEGREE 2 TO 1 ELIMINATION

- For any $f = \alpha x^q + 1 + \beta x^q + \gamma x + \delta$ in $V_Q$,
  
  $$h_1 f = \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \mod J$$

- The quotient $L_0 = (\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1)/Q$ is linear
  
  $$h_1 f = L_0 Q \mod J$$

- If $f$ splits into linears $L_1, \ldots, L_{q+1}$ in $k[x]$, then
  
  $$Q = h_1 L_0^{-1} L_1 \ldots L_{q+1} \mod J$$

- **Algorithm**: choose random $f \in V_Q$ until it splits over $k$
SUMMARY

DEGREE 2 TO 1 ELIMINATION

DONE, ASSUMING WE HAVE A SUITABLE MODEL FOR THE FIELD!

DESCENT ALGORITHM

ALGORITHM FOR COMPUTING DISCRETE LOGARITHMS
ELLIPITIC CURVE MODEL

A convenient model for the finite field
HEURISTIC MODEL

- Model $\mathbb{F}_q[x]/(J)$ used in heuristic algorithms

- **Good:** the relation $x^q = h_0/h_1$, i.e., the Frobenius is congruent to a small degree rational map

- **Bad:** we cannot prove this model always exists

- *For our new rigorous algorithm:* other model that always exists and has a ‘small degree’ Frobenius?
FINITE FIELDS FROM ELLIPTIC CURVES

- Construct a model for $\mathbb{F}_{q^n}$ where the $q$-Frobenius is congruent to a small degree rational map...

- Use elliptic curves!
FINITE FIELDS FROM ELLIPTIC CURVES

- Construct a model for $\mathbb{F}_{q^n}$ where the $q$-Frobenius is congruent to a small degree rational map...

- Let $E/\mathbb{F}_q$ be an elliptic curve such that $E(\mathbb{F}_q)$ has a point $Q$ of order $n$

- Let $S \in E$ such that $S^{(q)} = S + Q$. Then

  \[ S^{(q^i)} = S^{(q^{i-1})} + Q = S^{(q^{i-2})} + 2Q = \ldots = S + iQ \]

- $Q$ of order $n$ implies $(q^n)$ is the first Frobenius fixing $S$

- $\mathbb{F}_{q^n} = \text{residue field of } S \text{ over } \mathbb{F}_q$ ?
FINITE FIELDS FROM ELLIPTIC CURVES

- $\mathbb{F}_q^n = \text{residue field of } S \text{ over } \mathbb{F}_q$

- ‘Coordinate ring of $E = \mathbb{F}_q[E] = \mathbb{F}_q[x,y] / (y^2 - x^3 - ax - b)$

- ‘Residue field of $S' = \mathbb{F}_q[E]/\sim \text{ where}

  \[ f \sim g \iff f(S) = g(S) \]
FROBENIUS AS A SMALL DEGREE MAP

- Let $\varphi_q : E \to E : P \mapsto P^{(q)}$ be the $q$-Frobenius.
- For $R \in E$ let $\tau_R : E \to E : P \mapsto P + R$ be the translation by $R$.
- For any $f \in \mathbb{F}_q[E]/\sim = \mathbb{F}_q^n$, we have

$$f \circ \varphi_q \sim f \circ \tau_Q$$

"Frobenius = translation by $Q$"

is the new "$x^q \equiv h_0/h_1 \mod J$"

$$f \circ \varphi_q(S) = f(S^{(q)}) = f(S+Q) = f \circ \tau_Q(S)$$
PROVABLE MODEL

- We want to solve DLP in $\mathbb{F}_q^n$: find $E/\mathbb{F}_q$ with a point of order $n$

- **Theorem (Waterhouse, 1969):** For any integer $t$ coprime to $q$ such that $|t| \leq 2q^{1/2}$, there is an ordinary elliptic curve $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = q + 1 - t$.

- If $n^2 \leq 2q^{1/2}$, there exists $E/\mathbb{F}_q$ that contains a point of order $n$

- To solve DLP in $\mathbb{F}_{p^n}$, solve it in a small extension $\mathbb{F}_{q^n}$ such that $n^2 \leq 2q^{1/2}$
NEW ELIMINATIONS

Eliminations in the elliptic curve model
DEGREES

Fix an extension $k$ of $\mathbb{F}_q$

- $k(E) = k(x,y) / (y^2 - x^3 - ax - b)$
- ‘Degree of $f \in k(E)$’ = number of solutions of $f(P) = 0$, $P \in E$
- $x \in k(E)$ has degree 2
SPLITTING POLYNOMIALS

Fix an extension $k$ of $\mathbb{F}_q$

- $V = \text{span}(x^q + 1, x^q, x, 1) \subset k(E)$

- Random $f \in V$ splits with high probability into ‘linear factors’ $L_1, \ldots, L_{q+1}$ defined over $k$

- Each $L_i$ is of the form $x - a$, they are of degree 2...

- No ‘degree 2 to 1’ elimination… Can we do ‘3 to 2’?

- Let $D$ in $k(E)$ of degree 3
A FIRST ATTEMPT…

- Let

\[ Y = \{ \alpha x^{q+1} + \beta x^q + \gamma x + \delta \mid \alpha(x \circ \tau_Q)x + \beta(x \circ \tau_Q) + \gamma x + \delta \equiv 0 \mod D \} \subset \mathbb{P}(V) \]

- For any \( f \in Y(k) \),

\[ g = (\alpha(x \circ \tau_Q)x + \beta(x \circ \tau_Q) + \gamma x + \delta)/D \]

has degree \( 4 - 3 = 1 \)

- Suppose \( f = L_1 \ldots L_{q+1} \) where each \( L_i \) is linear in \( k[x] \) (so \( L_i \) has degree 2 in \( k(E) \))

\[ D = L_1 \ldots L_{q+1} g^{-1} \]

- **Algorithm:** choose random \( f \in Y(k) \) until \( f \) splits over \( k \)

Warning: hand-wavy

Degree 3 to degree 2 elimination??

degrees 1 and 2
A FIRST ATTEMPT...

\[ Y = \{\alpha x^{q+1} + \beta x^q + \gamma x + \delta \mid \alpha(x \circ \tau_Q) + \beta(x \circ \tau_Q) + \gamma x + \delta \equiv 0 \mod D\} \subset \mathbb{P}(V) \]

- \[ Y = \mathbb{P}(\ker(V \to \langle k(E)/D' \rangle)) \]
- \[ V \text{ has dimension } 4, \text{ } \langle k(E)/D' \rangle \text{ has dimension } \deg(D) = 3, \text{ the kernel is expected to have dimension } 1: Y \text{ is a single point} \]
- **Bad:** \[ Y \text{ is too small, we need a curve...} \]
AN EXTRA DEGREE OF FREEDOM

Fix an extension $k$ of $\mathbb{F}_q$, and let $D$ in $k(E)$ of degree 3

- $V = \text{span}(x^q + 1, x, x, 1) \subset k(E)$
- For any $P \in E$ let

\[
\psi_P : V \rightarrow k(E) : \begin{cases} 
  1 & \mapsto 1 \\
  x & \mapsto x \circ \tau_P \\
  x^q & \mapsto x \circ \tau_{Q + P(q)} \\
  x^q + 1 & \mapsto (x \circ \tau_P)(x \circ \tau_{Q + P(q)})
\end{cases}
\]

- For any $f \in V$, $f \circ \tau_P \equiv \psi_P(f)$

Splits with high probability into degree 2's

Degree 4
For any \((f, P) \in X(k)\), \(g = \psi_P(f)/D\) has degree \(4 - 3 = 1\)

Suppose \(f = L_1 \ldots L_{q+1}\) where each \(L_i\) is linear in \(k[x]\)

\[
D = \psi_P(f) \ g^{-1} = (L_1 \circ \tau_P) \ldots (L_{q+1} \circ \tau_P) \ g^{-1}
\]

Algorithm: choose random \((f, P) \in X(k)\) until \(f\) splits over \(k\)
Algorithm for computing discrete logarithms

Descent algorithm

Zig-zag descent

Degree 2 to 1 elimination

Heuristic
DEGREE 3 TO 2 ELIMINATION

DECENT ALGORITHM

ALGORITHM FOR COMPUTING DISCRETE LOGARITHMS
RIGOROUS DEGREE 4 TO 3 ELIMINATION + DEGREE 3 TO 2 ELIMINATION

DEGREE 4 TO 2 ELIMINATION

ZIG-ZAG DESCENT

DESCENT ALGORITHM

ALGORITHM FOR COMPUTING DISCRETE LOGARITHMS RIGOROUS!
PROOF

STRATEGY

Irreducible covers
WHAT REMAINS TO BE PROVED?

- **Algorithm**: choose random \((f, P) \in X(k)\) until \(f\) splits over \(k\)

- For how many \((f, P) \in X(k)\) does \(f\) split over \(k\)?
IRREDUCIBLE CURVES

A curve is **irreducible** if it is not a union of two sub-curves.

\[ C_1 \text{ and } C_2 \text{ are both irreducible} \]
IRREDUCIBLE CURVES

A curve is **irreducible** if it is not a union of two sub-curves

\[ C_1 \cup C_2 \]

\( C_1 \) and \( C_2 \) are both irreducible

\( C_1 \cup C_2 \) is not irreducible
IRREDUCIBLE CURVES

A CURVE IS IRREDUCIBLE IF IT IS NOT A UNION OF TWO SUB-CURVES

A CURVE IS ABSOLUTELY IRREDUCIBLE IF IT IS IRREDUCIBLE OVER THE ALGEBRAIC CLOSURE OF THE FIELD OF DEFINITION
A morphism of curves is a map $C \rightarrow D$ described by polynomials in the coordinates.

A morphism between absolutely irreducible curves is either constant or surjective over the algebraic closure.
PROOF STRATEGY

For how many \((f,P) \in X(k)\) does \(f\) split over \(k\)?

- Construct a curve \(C\) defined over \(k\), and a surjective morphism \(\theta : C \to X\) such that
  
  - For any point \(z\) in \(C(k)\), the polynomial in \(\theta(z)\) splits over \(k\)
  
  - \(C\) is absolutely irreducible

OPEN QUESTIONS
A DETERMINISTIC ALGORITHM?
A POLYNOMIAL TIME ALGORITHM?
IS SMALL-CHAR-CHAR-DLP IN P?
MEDIUM AND LARGE CHARACTERISTIC?
DISCRETE LOGARITHMS
IN QUASI-POLYNOMIAL TIME
IN FINITE FIELDS OF SMALL CHARACTERISTIC

Benjamin Wesolowski

ECC 2019: 23rd Workshop on Elliptic Curve Cryptography
December 2019
Bochum, Germany

Based on a joint work with Thorsten Kleinjung