Attaques algébriques du problème du logarithme discret sur courbes elliptiques

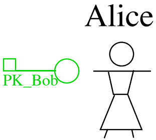
Vanessa VITSE

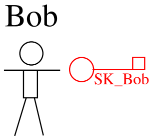
Université de Versailles Saint-Quentin, Laboratoire PRiSM

Soutenance de thèse

Asymmetric cryptography

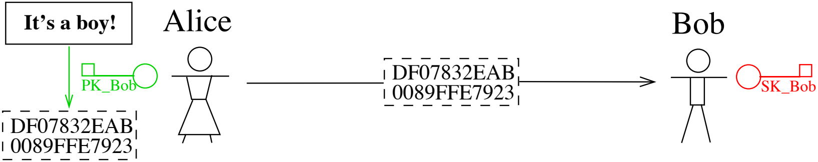
Asymmetric cryptography



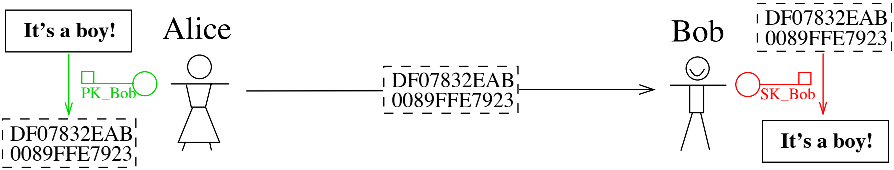


Asymmetric cryptography

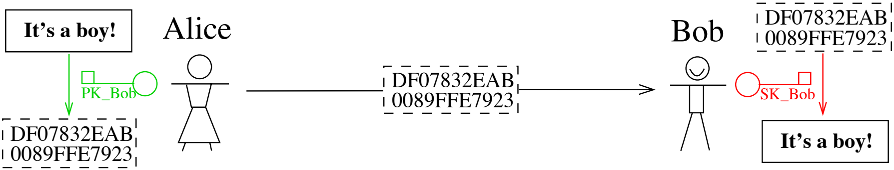
Asymmetric cryptography



Asymmetric cryptography

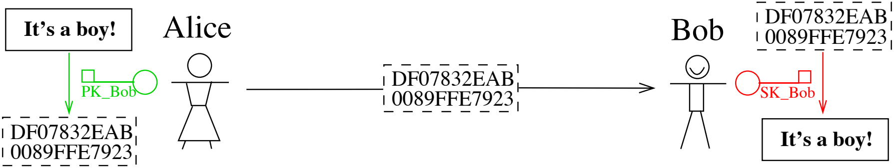


Asymmetric cryptography



PK is computed from SK, but SK *must not* be easily deducible from PK
$\Rightarrow$ asymmetric cryptography relies on **one-way functions**

Asymmetric cryptography



PK is computed from SK, but SK *must not* be easily deducible from PK
$\Rightarrow$ asymmetric cryptography relies on **one-way functions**

Main one-way functions currently in use:

- multiplication of two primes (RSA)
- exponentiation in finite groups (Diffie-Hellman, ElGamal)
- evaluation of multivariate polynomial systems (HFE,UOV)

...

The Discrete Logarithm Problem

Let G be a group, $g \in G$ an element of finite order n.
The discrete logarithm of $h \in \langle g \rangle$ is the integer $x \in \mathbb{Z}/n\mathbb{Z}$ such that

$$h = g^x.$$

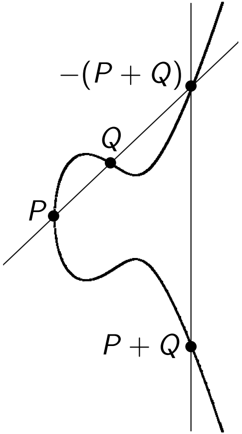
This is a one-way function:

- given g and x, easy to compute $h = g^x$, assuming an efficiently computable group law (*always the case here*)
- computing discrete log much harder in general: best *generic* algorithms in $\tilde{O}(\sqrt{r})$, r largest prime factor of n

DLP: given $g, h \in G$, find x – if it exists – such that $h = g^x$

Elliptic curve DLP

Good candidates for DLP-based cryptosystems:
elliptic curves defined over finite fields



ECDLP: Given $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$
find x such that $Q = [x]P$

- On $\mathbb{F}_p$ (p prime): in general, no known attack better than generic algorithms
  $\rightarrow$ good security
- On $\mathbb{F}_{p^n}$ (for faster hardware arithmetic): possible to apply *index calculus*
  $\rightarrow$ security reduction in some cases

Part I

Resolution of multivariate polynomial systems

"Solving" polynomial systems

Consider multivariate polynomials $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad\quad\vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \quad \Leftrightarrow \quad (x_1, \ldots, x_n) \in \mathbb{V}(\langle f_1, \ldots, f_m \rangle)$$

- If $\mathbb{V}(I)$ zero-dimensional, complete resolution makes sense
- Otherwise, goal is to obtain "good" descriptions of $\mathbb{V}(I)$, i.e. special sets of generators of I $\rightarrow$ provided by Gröbner bases

Hard problem in the general case

Main tool: Gröbner bases

$\mathbb{K}[\underline{X}] = \mathbb{K}[X_1, \ldots, X_n]$ polynomial ring, $\mathcal{T}$: set of all monomials

Monomial ordering

$\prec$ is an admissible monomial order if it is a well-founded strict total order on $\mathcal{T}$ such that $m' \prec m'' \Rightarrow m \cdot m' \prec m \cdot m''$

- main orders:
  - lexicographic order (*lex*)
  - graded reverse lexicographic order (*grevlex*)
- allows to define the leading monomial $LM(f)$ of a polynomial f

Main tool: Gröbner bases

$\mathbb{K}[\underline{X}] = \mathbb{K}[X_1, \ldots, X_n]$ polynomial ring, $\mathcal{T}$: set of all monomials

Monomial ordering

$\prec$ is an admissible monomial order if it is a well-founded strict total order on $\mathcal{T}$ such that $m' \prec m'' \Rightarrow m \cdot m' \prec m \cdot m''$

- main orders:
  - lexicographic order (*lex*)
  - graded reverse lexicographic order (*grevlex*)
- allows to define the leading monomial $LM(f)$ of a polynomial f

Gröbner basis

$(g_1, \ldots, g_s)$ Gröbner basis of I (wrt $\prec$) if

$$I = \langle g_1, \ldots, g_s \rangle \text{ and } \forall f \in I,\ \exists i \text{ s.t. } LM(g_i) | LM(f)$$

Gröbner bases always exist and can be algorithmically computed

Elimination theory and shape lemma

I ideal of $\mathbb{K}[X_1, \ldots, X_n]$, $\quad I_k = I \cap \mathbb{K}[X_k, \ldots, X_n]$ k-th **elimination ideal**

If G is a lex GB of I, then $G \cap \mathbb{K}[X_k, \ldots, X_n]$ is a GB of I_k
$\rightsquigarrow$ lex GB provide "triangular systems"

Shape lemma

Up to a generic linear change of coordinates, the (reduced) lex GB of a 0-dim radical ideal is of the form

$$\big(X_1 - g_1(X_n), \quad \ldots, \quad X_{n-1} - g_{n-1}(X_n), \quad g_n(X_n)\big),$$

where $g_1, \ldots, g_n$ are univariate.

Algorithms for computing Gröbner basis

1. Buchberger (1965): uses critical pairs $(lcm, u_1, f_1, u_2, f_2)$ where $lcm = LM(f_1) \vee LM(f_2)$, $u_i = \frac{lcm}{LT(f_i)}$ to construct new elements of the GB
   - reduction of $u_1 f_1 - u_2 f_2$ modulo current basis very expensive
   - many useless critical pairs

Algorithms for computing Gröbner basis

1. Buchberger (1965): uses critical pairs $(lcm, u_1, f_1, u_2, f_2)$ where $lcm = LM(f_1) \vee LM(f_2)$, $u_i = \frac{lcm}{LT(f_i)}$ to construct new elements of the GB
   - reduction of $u_1 f_1 - u_2 f_2$ modulo current basis very expensive
   - many useless critical pairs
2. Lazard (1983): uses Macaulay matrices containing multiples of initial generators, replaces reductions by linear algebra
   - complexity can be bounded
   - many useless rows

$$
\begin{array}{cc}
 & \begin{array}{c}\text{monomial } m \\ \downarrow\end{array} \\
P = m \cdot f \longrightarrow & \begin{pmatrix} & \vdots & \\ \cdots\cdots & \mathrm{coeff}(P, m) & \cdots \\ & \vdots & \end{pmatrix}
\end{array}
$$

Algorithms for computing Gröbner basis

1. Buchberger (1965): uses critical pairs $(lcm, u_1, f_1, u_2, f_2)$ where $lcm = LM(f_1) \vee LM(f_2)$, $u_i = \frac{lcm}{LT(f_i)}$ to construct new elements of the GB
   - reduction of $u_1 f_1 - u_2 f_2$ modulo current basis very expensive
   - many useless critical pairs
2. Lazard (1983): uses Macaulay matrices containing multiples of initial generators, replaces reductions by linear algebra
   - complexity can be bounded
   - many useless rows

$$\begin{array}{cc} & \begin{array}{ccc} & \text{monomial } m & \\ & \downarrow & \end{array} \\ P = m \cdot f \rightarrow & \begin{pmatrix} & \vdots & \\ \cdots\cdots & \text{coeff}(P, m) & \cdots\cdots \\ & \vdots & \end{pmatrix} \end{array}$$

3. Faugère: two algorithms F4 (1999) and F5 (2002) considered as the best ones currently available

Algorithms for computing Gröbner basis

1. Buchberger (1965): uses critical pairs $(lcm, u_1, f_1, u_2, f_2)$ where $lcm = LM(f_1) \vee LM(f_2)$, $u_i = \frac{lcm}{LT(f_i)}$ to construct new elements of the GB
   - reduction of $u_1 f_1 - u_2 f_2$ modulo current basis very expensive
   - many useless critical pairs
2. Lazard (1983): uses Macaulay matrices containing multiples of initial generators, replaces reductions by linear algebra
   - complexity can be bounded
   - many useless rows

$$\begin{array}{cc} & \begin{array}{c}\text{monomial } m\\ \downarrow\end{array} \\ P = m \cdot f \longrightarrow & \left(\begin{array}{ccc} & \vdots & \\ \cdots\cdots & \mathrm{coeff}(P, m) & \cdots \\ & \vdots & \end{array}\right)\end{array}$$

3. Faugère: two algorithms F4 (1999) and F5 (2002) considered as the best ones currently available
4. FGLM (1993): change of order in the 0-dimensional case

Main algorithms

1. F4 algorithm: efficient combination of Buchberger and Lazard
   - fast and simultaneous reductions of several critical pairs: Macaulay-style matrix of polynomials from selected pairs and preprocessing + memorization of previous reductions
   - drawback: many reductions to zero

Main algorithms

1. F4 algorithm: efficient combination of Buchberger and Lazard
   - fast and simultaneous reductions of several critical pairs: Macaulay-style matrix of polynomials from selected pairs and preprocessing + memorization of previous reductions
   - drawback: many reductions to zero
2. F5 algorithm
   - elaborate criterion: skip unnecessary reductions
   - drawback: incomplete polynomial reductions
   - rough complexity estimate: $\tilde{O}\left(\binom{n+d_{max}}{n}^{\omega}\right)$ (based on Lazard)

     ω constant s.t. complexity of multiplication of matrices of size n is in $O(n^{\omega})$ op.

Main algorithms

1. F4 algorithm: efficient combination of Buchberger and Lazard
   - fast and simultaneous reductions of several critical pairs: Macaulay-style matrix of polynomials from selected pairs and preprocessing + memorization of previous reductions
   - drawback: many reductions to zero
2. F5 algorithm
   - elaborate criterion: skip unnecessary reductions
   - drawback: incomplete polynomial reductions
   - rough complexity estimate: $\tilde{O}\left(\binom{n+d_{max}}{n}^{\omega}\right)$ (based on Lazard)

     ω constant s.t. complexity of multiplication of matrices of size n is in $O(n^{\omega})$ op.

- multipurpose algorithms
- what about polynomial systems arising from algebraic cryptanalysis?

A relevant case for cryptanalysis

Several examples from cryptanalysis/index calculus where systems can be considered as "similar":

$V \subset \mathbb{K}^\ell$ algebraic variety

- Parametric family of systems: $F_1, \ldots, F_r \in \mathbb{K}(V)[\underline{X}]$
- Random instance:
  $\{f_1, \ldots, f_r\} = \{F_1(y), \ldots, F_r(y)\} \subset \mathbb{K}[\underline{X}]$ for $y \in V$ random

$\rightarrow$ systems are *similar* if instances of a same parametric family

A relevant case for cryptanalysis

Several examples from cryptanalysis/index calculus where systems can be considered as "similar":

$V \subset \mathbb{K}^\ell$ algebraic variety

- Parametric family of systems: $F_1, \dots, F_r \in \mathbb{K}(V)[\underline{X}]$
- Random instance:
  $\{f_1, \dots, f_r\} = \{F_1(y), \dots, F_r(y)\} \subset \mathbb{K}[\underline{X}]$ for $y \in V$ random

$\rightarrow$ systems are *similar* if instances of a same parametric family

Goal: find a technique to solve efficiently many similar systems

A GB algorithm for similar systems

Contribution: the F4Remake algorithm

1. detect the useful critical pairs from F4 computation of a first instance
2. deduce GB of subsequent instances without any useless computations

A GB algorithm for similar systems

Contribution: the F4Remake algorithm

1. detect the useful critical pairs from F4 computation of a first instance
2. deduce GB of subsequent instances without any useless computations

When to use F4Remake?

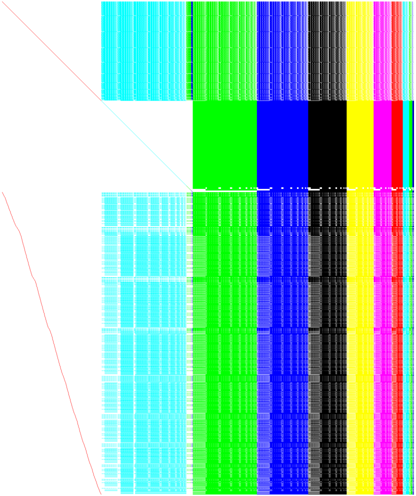
- need to solve many similar systems
- GB computation of one instance is feasible
- computation of "comprehensive Gröbner basis" intractable

Previous works

- GB computations over $\mathbb{Q}[\underline{X}]$ using CRT
- Traverso ('88): "GB traces" for Buchberger's algorithm in the rational case

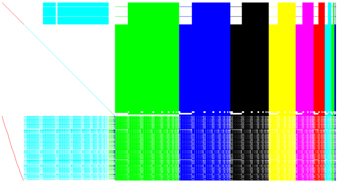
Performances of F4Remake

Example of a matrix of size $1\,539 \times 1\,285$ obtained with F4



Performances of F4Remake

Same matrix with F4Remake is of size $553 \times 1\,043$ (≈ 3.5 times smaller)



Performances of F4Remake

Advantages over F4/F5

- always faster than F4
- same rough complexity upper bound as F5, but computes much less polynomials in practice

F4Remake is a probabilistic algorithm

- heuristic probability of success greater than

$$\left(\prod_{i=1}^{\infty}(1-q^{-i})\right)^{n_{step}} \geq (1-2/q)^{n_{step}}$$

  $\rightarrow$ good probability over large fields
- can also perform well over small fields

Part II

The discrete logarithm problem for curves over extension fields

1. Decomposition index calculus

The index calculus method – basic outline

$(G, +) = \langle P \rangle$ finite abelian group of prime order r, $Q \in G$

1. Choice of a factor base: $\mathcal{F} = \{P_1, \ldots, P_N\} \subset G$
2. Relation search: decompose $[a_i]P + [b_i]Q$ (a_i, b_i random) into $\mathcal{F}$

$$[a_i]P + [b_i]Q = \sum_{j=1}^{N} [c_{ij}]P_j, \text{ where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the matrices $A = \begin{pmatrix} a_i & b_i \end{pmatrix}_{1 \leq i \leq k}$ and $M = (c_{ij})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $v = (v_1, \ldots, v_k) \in \ker({}^t M)$ such that $vA \neq \begin{pmatrix} 0 & 0 \end{pmatrix} \bmod r$
   - compute the solution of DLP: $x = -\left(\sum_i a_i v_i\right) / \left(\sum_i b_i v_i\right) \bmod r$

Application to elliptic curves

No canonical choice of factor base nor natural way of finding decompositions

Application to elliptic curves

No canonical choice of factor base nor natural way of finding decompositions

What kind of "decomposition" over $E(K)$?

Main idea [Semaev '04]:

- consider decompositions in a fixed number of points of $\mathcal{F}$
$$R = [a]P + [b]Q = P_1 + \cdots + P_m$$
- convert this algebraically by using the $(m+1)$-*th summation polynomial*:
$$f_{m+1}(x_R, x_{P_1}, \ldots, x_{P_m}) = 0$$
$$\Leftrightarrow \exists \epsilon_1, \ldots, \epsilon_m \in \{1, -1\}, R = \epsilon_1 P_1 + \cdots + \epsilon_m P_m$$

Gaudry and Diem (2004)

"Decomposition attack": index calculus on $E(\mathbb{F}_{q^n})$

- Natural factor base: $\mathcal{F} = \{(x,y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$
  $\mathcal{F}$ curve in *Weil restriction* $\mathcal{W}$ of $E \rightsquigarrow \#\mathcal{F} \simeq q$
- Relations involve $n = \dim \mathcal{W}$ points: $R = P_1 + \cdots + P_n$
- Restriction of scalars: decompose along a $\mathbb{F}_q$-linear basis of $\mathbb{F}_{q^n}$

$$f_{n+1}(x_R, x_{P_1}, \ldots, x_{P_n}) = 0 \Leftrightarrow \begin{cases} \varphi_1(x_{P_1}, \ldots, x_{P_n}) = 0 \\ \vdots \\ \varphi_n(x_{P_1}, \ldots, x_{P_n}) = 0 \end{cases} \qquad (\mathcal{S}_R)$$

One decomposition trial $\leftrightarrow$ resolution of $\mathcal{S}_R$ over $\mathbb{F}_q$

Gaudry and Diem (2004)

"Decomposition attack": index calculus on $E(\mathbb{F}_{q^n})$

- Natural factor base: $\mathcal{F} = \{(x,y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$
  $\mathcal{F}$ curve in *Weil restriction* $\mathcal{W}$ of $E \rightsquigarrow \#\mathcal{F} \simeq q$
- Relations involve $n = \dim \mathcal{W}$ points: $R = P_1 + \cdots + P_n$
- Restriction of scalars: decompose along a $\mathbb{F}_q$-linear basis of $\mathbb{F}_{q^n}$

$$f_{n+1}(x_R, x_{P_1}, \ldots, x_{P_n}) = 0 \Leftrightarrow \begin{cases} \varphi_1(x_{P_1}, \ldots, x_{P_n}) = 0 \\ \vdots \\ \varphi_n(x_{P_1}, \ldots, x_{P_n}) = 0 \end{cases} \qquad (\mathcal{S}_R)$$

One decomposition trial $\leftrightarrow$ resolution of $\mathcal{S}_R$ over $\mathbb{F}_q$

- With "double large prime" variation, overall complexity in
  $\tilde{O}\left(n! 2^{3n(n-1)} q^{2-2/n}\right)$
- Bottleneck: $\deg I(\mathcal{S}_R) = 2^{n(n-1)}$. But most solutions not in $\mathbb{F}_q$

Variant "$n-1$" [Joux-V. '10]

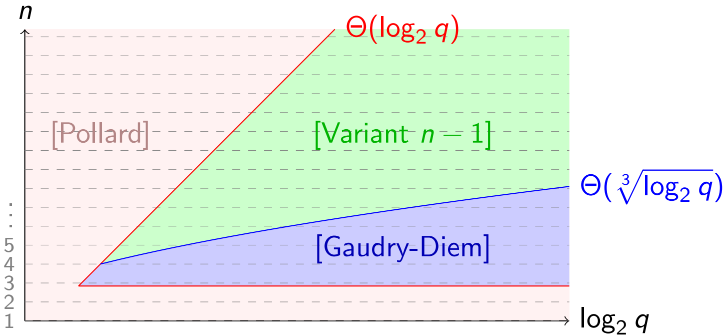
Decompositions into $m = n-1$ points

- compute the n-th summation polynomial (instead of $n+1$-th) with partially symmetrized resultant
- solve $\mathcal{S}_R$ with $n-1$ var, n eq and total degree 2^{n-2}
- $(n-1)!q$ expected numbers of trials to get one relation

Computation speed-up

1. $\mathcal{S}_R$ is overdetermined and $I(\mathcal{S}_R)$ has very low degree (0 or 1 excep.)
   - resolution with a *grevlex* Gröbner basis
   - no need to change order (FGLM)
2. Speed up computations with F4Remake

Comparaison of the three attacks of ECDLP over $\mathbb{F}_{q^n}$



Under some heuristic assumptions, complexity of variant $n-1$ in

$$\tilde{O}\left((n-1)!\left(2^{(n-1)(n-2)}e^n n^{-1/2}\right)^{\omega} q^2\right)$$

Example of application to $E(\mathbb{F}_{p^5})$

Standard 'Well Known Group' 3 Oakley curve

E elliptic curve defined over $\mathbb{F}_{2^{155}}$,
$\#E(\mathbb{F}_{2^{155}}) = 12 \cdot 3805993847215893016155463826195386266397436443$

- $\mathcal{F} = \{P \in E(\mathbb{F}_{2^{155}}) : x(P) \in \mathbb{F}_{2^{31}}\}$
- Decomposition test with variant $n-1$ takes 22.95 ms using F4Remake (on 2.93 GHz Intel Xeon)

Example of application to $E(\mathbb{F}_{p^5})$

Standard 'Well Known Group' 3 Oakley curve

E elliptic curve defined over $\mathbb{F}_{2^{155}}$,
$\#E(\mathbb{F}_{2^{155}}) = 12 \cdot 3805993847215893016155463826195386266397436443$

- $\mathcal{F} = \{P \in E(\mathbb{F}_{2^{155}}) : x(P) \in \mathbb{F}_{2^{31}}\}$
- Decomposition test with variant $n-1$ takes 22.95 ms using F4Remake (on 2.93 GHz Intel Xeon)

- too slow for complete DLP resolution
- but efficient threat for Oracle-assisted Static Diffie-Hellman Problem (only one relation needed)

Decomposition for Jacobians

$\mathcal{C}$ curve defined over $\mathbb{F}_{q^n}$ of genus g with a unique point $\mathcal{O}$ at infinity

Gaudry's framework

Work with $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}))$ of dim. ng

- Factor base containing about q elements
  $\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition search: try to write arbitrary divisor $D \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ as sum of ng divisors of $\mathcal{F}$

Asymptotic complexity for n, g fixed in $\tilde{O}(q^{2-2/ng})$

Decomposition for Jacobians

$\mathcal{C}$ curve defined over $\mathbb{F}_{q^n}$ of genus g with a unique point $\mathcal{O}$ at infinity

Gaudry's framework

Work with $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}))$ of dim. ng

- Factor base containing about q elements
  $\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition search: try to write arbitrary divisor $D \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ as sum of ng divisors of $\mathcal{F}$

Asymptotic complexity for n, g fixed in $\tilde{O}(q^{2-2/ng})$

How to check if D can be decomposed?

- Semaev's summation polynomials are no longer available
- use Riemann-Roch based reformulation of Nagao instead

Decomposition for hyperelliptic Jacobians over $\mathbb{F}_{q^n}$

Main difficulty in Nagao's decompositions

Solve a 0-dim quadratic polynomial system of $(n-1)ng$ eq./var. for each divisor $D(=[a_i]D_0 + [b_i]D_1) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$.

- complexity at least polynomial in $d = 2^{(n-1)ng}$ [F4Remake + FGLM]
- relevant only for n and g small enough

Decomposition for hyperelliptic Jacobians over $\mathbb{F}_{q^n}$

Main difficulty in Nagao's decompositions

Solve a 0-dim quadratic polynomial system of $(n-1)ng$ eq./var. for each divisor $D(=[a_i]D_0+[b_i]D_1)\in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$.

- complexity at least polynomial in $d=2^{(n-1)ng}$ [F4Remake + FGLM]
- relevant only for n and g small enough

In practice:

- Decompositions as $D\sim\sum_{i=1}^{ng}((Q_i)-(\mathcal{O}_{\mathcal{H}}))$ are too slow to compute
- Faster alternative [Joux-V.]: compute relations involving only elements of $\mathcal{F}$

$$\sum_{i=1}^{ng+2}((Q_i)-(\mathcal{O}_{\mathcal{H}}))\sim 0$$

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_{\mathcal{H}})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2}((Q_i) - (\mathcal{O}_\mathcal{H})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

- With Nagao: about $(ng)!\,q$ quadratic polynomial systems of $n(n-1)g$ eq./var. to solve
- With variant: only 1 under-determined quadratic system of $n(n-1)g + 2n - 2$ eq. and $n(n-1)g + 2n$ var.

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2}((Q_i) - (\mathcal{O}_\mathcal{H})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

- With Nagao: about $(ng)!\,q$ quadratic polynomial systems of $n(n-1)g$ eq./var. to solve
- With variant: only 1 under-determined quadratic system of $n(n-1)g + 2n - 2$ eq. and $n(n-1)g + 2n$ var.

Fast resolution

Goal: find a new set of generators of the ideal s.t. each specialization of two variables yields an easy to solve system $\rightarrow$ lex Gröbner basis

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2 - \omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1, 1)$

$\rightarrow$ variables of the 1st block belong to a one-dimensional variety

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2 - \omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1, 1)$
$\rightarrow$ variables of the 1st block belong to a one-dimensional variety

Decomposition method:

1. "specialization": choose a value for the first variables
2. remaining variables lie in a one-dimensional vector space $\rightsquigarrow$ easy to solve system

Further improvement possible by using a sieving technique

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2 - \omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1, 1)$

$\rightarrow$ variables of the 1st block belong to a one-dimensional variety

Decomposition method:

1. "specialization": choose a value for the first variables
2. remaining variables lie in a one-dimensional vector space $\rightsquigarrow$ easy to solve system

Further improvement possible by using a sieving technique

Much faster to compute decompositions with our variant

$\rightarrow$ about 960 times faster for $(n, g) = (2, 3)$ on a 150-bit curve

Part II

The discrete logarithm problem for curves over extension fields

2. Cover and decomposition

Transfer of the ECDLP via cover maps

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the Weil restriction of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

Transfer of the ECDLP via cover maps

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the Weil restriction of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $\langle P \rangle \subset E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd}
\mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[r, "Tr"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\
E(\mathbb{F}_{q^n}) & \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[ur, dotted] &
\end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

Transfer of the ECDLP via cover maps

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the Weil restriction of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $\langle P \rangle \subset E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd}
\mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] & & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[r, "Tr"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\
E(\mathbb{F}_{q^n}) & \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq & E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"'] \arrow[ur, dotted] &
\end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
   - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
   - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

Transfer of the ECDLP via cover maps

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the Weil restriction of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $\langle P \rangle \subset E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd} \mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] \\ E(\mathbb{F}_{q^n}) \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[rr, "Tr"] & & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[urr, dotted] & & \end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
    - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
    - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

The Gaudry-Heß-Smart technique

Construct $\mathcal{C}_{|\mathbb{F}_q}$ and $\pi : \mathcal{C} \to E$ from $E_{|\mathbb{F}_{q^n}}$ and a degree 2 map $E \to \mathbb{P}^1$

Transfer of the ECDLP via cover maps

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the Weil restriction of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $\langle P \rangle \subset E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd} \mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] \\ E(\mathbb{F}_{q^n}) \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[r, "Tr"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[ur, dotted] & \end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
   - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
   - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

The Gaudry-Heß-Smart technique

Problem: for most elliptic curves, $g(\mathcal{C})$ is of the order of 2^n

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

Cover and decomposition attack [Joux-V.]

If n composite, combine both approaches:

1. use GHS on the subextension $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ to transfer the DL to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. then use decomposition attack on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

Cover and decomposition attack [Joux-V.]

If n composite, combine both approaches:

1. use GHS on the subextension $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ to transfer the DL to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. then use decomposition attack on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

$\longrightarrow$ well adapted for curves defined over some Optimal Extension Fields

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years
2. Former index calculus methods:

	Decomposition	GHS
$\mathbb{F}_{p^6}/\mathbb{F}_{p^2}$	$\tilde{O}(p^2)$ memory bottleneck	
$\mathbb{F}_{p^6}/\mathbb{F}_{p}$	intractable	efficient for $\leq 1/p^3$ curves $g = 9$: $\tilde{O}(p^{7/4})$, $\approx 1\,500$ years

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years
2. Former index calculus methods:

	Decomposition	GHS
$\mathbb{F}_{p^6}/\mathbb{F}_{p^2}$	$\tilde{O}(p^2)$ memory bottleneck	
$\mathbb{F}_{p^6}/\mathbb{F}_{p}$	intractable	efficient for $\leq 1/p^3$ curves $g = 9$: $\tilde{O}(p^{7/4})$, $\approx 1\,500$ years

3. Cover and decomposition:
   $\tilde{O}(p^{5/3})$ cost using a hyperelliptic genus 3 cover defined over $\mathbb{F}_{p^2}$
   $\rightarrow$ occurs directly for $1/p^2$ curves and most curves after isogeny walk
   - Nagao-style decomposition: ≈ 750 years
   - Modified relation search: ≈ 300 years

A concrete attack on a 150-bit curve

$E: \; y^2 = x(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{25}+35$, such that $\#E = 4 \cdot 356814156285346166966901450449051336101786213$

- Previously unreachable curve: GHS gives cover over $\mathbb{F}_p$ of genus 33...

A concrete attack on a 150-bit curve

$E: \; y^2 = x(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{25}+35$, such that $\#E = 4 \cdot 356814156285346166966901450449051336101786213$

- Previously unreachable curve: GHS gives cover over $\mathbb{F}_p$ of genus 33...
- Complete resolution of DLP in about 1 month
  with cover and decomposition, using genus 3 hyperelliptic cover $\mathcal{H}_{|\mathbb{F}_{p^2}}$

Relation search

- lex GB: 2.7 sec with one core(1)
- sieving: $p^2/(2\cdot 8!) \simeq 1.4\times 10^{10}$ relations in 62 h on 1 024 cores(2)
  $\to$ 960$\times$ faster than Nagao

Linear algebra

- SGE: 25.5 h on 32 cores(2)
  $\to$ fivefold reduction
- Lanczos: 28.5 days on 64 cores(2)
  (200 MB of data broadcast/round)

(Descent phase done in $\sim$ 14 s for one point)

(1) Magma on 2.6 GHz Intel Core 2 Duo

(2) 2.93 GHz quadri-core Intel Xeon 5550

Attaques algébriques du problème du logarithme discret sur courbes elliptiques

Vanessa VITSE

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Soutenance de thèse