

Cover and Decomposition Attacks on Elliptic Curves

Vanessa VITSE

Joint work with Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Séminaire de cryptologie, codage et infrastructures sécurisées

Section 1

Background

Hardness of ECDLP

ECDLP

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

Attacks on special curves

- Curves defined over prime fields
 - ▶ small embedding degree (transfer via pairings)
 - ▶ anomalous curves (p -adic lifts)
- Curves defined over extension fields
 - ▶ Weil descent [Frey]:
transfer from $E(\mathbb{F}_{p^n})$ to $\text{Jac}_{\mathcal{C}}(\mathbb{F}_p)$ where \mathcal{C} is a genus $g \geq n$ curve
 - ▶ Decomposition index calculus on $E(\mathbb{F}_{p^n})$

Hardness of ECDLP

ECDLP

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

Attacks on special curves

- Curves defined over prime fields
 - ▶ small embedding degree (transfer via pairings)
 - ▶ anomalous curves (p -adic lifts)
- Curves defined over extension fields
 - ▶ Weil descent [Frey]:
transfer from $E(\mathbb{F}_{p^n})$ to $\text{Jac}_{\mathcal{C}}(\mathbb{F}_p)$ where \mathcal{C} is a genus $g \geq n$ curve
 - ▶ Decomposition index calculus on $E(\mathbb{F}_{p^n})$

Objective of this talk

Present a combined attack for curves over extension fields

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** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \rightarrow E(\mathbb{F}_{q^n})$.

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** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \rightarrow E(\mathbb{F}_{q^n})$.

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

$$\begin{array}{ccc}
 \mathcal{C}(\mathbb{F}_{q^n}) & \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \xrightarrow{Tr} \text{Jac}_{\mathcal{C}}(\mathbb{F}_q) & \\
 \downarrow \pi & \uparrow \pi^* & \nearrow \\
 E(\mathbb{F}_{q^n}) & \text{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) &
 \end{array}$$

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** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \rightarrow E(\mathbb{F}_{q^n})$.

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

$$\begin{array}{ccc}
 \mathcal{C}(\mathbb{F}_{q^n}) & \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \xrightarrow{Tr} & \text{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\
 \downarrow \pi & \uparrow \pi^* & \nearrow \\
 E(\mathbb{F}_{q^n}) & \text{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) &
 \end{array}$$

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

- ② use index calculus on $\text{Jac}_{\mathcal{C}}(\mathbb{F}_q)$:
 → efficient if \mathcal{C} is hyperelliptic with small genus g [Gaudry] or has a small degree plane model [Diem]

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** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \rightarrow E(\mathbb{F}_{q^n})$.

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

$$\begin{array}{ccc}
 \mathcal{C}(\mathbb{F}_{q^n}) & \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \xrightarrow{\text{Tr}} \text{Jac}_{\mathcal{C}}(\mathbb{F}_q) & \\
 \downarrow \pi & \uparrow \pi^* & \nearrow \\
 E(\mathbb{F}_{q^n}) & \text{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) &
 \end{array}$$

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

- use index calculus on $\text{Jac}_{\mathcal{C}}(\mathbb{F}_q)$:
 → efficient if \mathcal{C} is hyperelliptic with small genus g [Gaudry] or has a small degree plane model [Diem]

The Gaudry-Heß-Smart technique

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

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** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \rightarrow E(\mathbb{F}_{q^n})$.

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

$$\begin{array}{ccc}
 \mathcal{C}(\mathbb{F}_{q^n}) & \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \xrightarrow{\text{Tr}} & \text{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\
 \downarrow \pi & \uparrow \pi^* & \nearrow \\
 E(\mathbb{F}_{q^n}) & \text{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) &
 \end{array}$$

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

- ② use index calculus on $\text{Jac}_{\mathcal{C}}(\mathbb{F}_q)$:
 → efficient if \mathcal{C} is hyperelliptic with small genus g [Gaudry] or has a small degree plane model [Diem]

The Gaudry-Heß-Smart technique

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

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{\mathbb{F}_q}$, n -dimensional abelian variety

Gaudry's method

- 1 Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \dots, x_n, y_1, \dots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \dots, x_n)$
- 2 Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \dots = x_n(P) = 0\}$
- 3 Decompose enough points of \mathcal{A} as sum of n points of \mathcal{F} using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
- 4 Extract the logarithms with sparse linear algebra

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n -dimensional abelian variety

Gaudry's method

- 1 Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \dots, x_n, y_1, \dots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \dots, x_n)$
- 2 Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \dots = x_n(P) = 0\}$
- 3 Decompose enough points of \mathcal{A} as sum of n points of \mathcal{F} using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
- 4 Extract the logarithms with sparse linear algebra

\mathcal{F} should have $\simeq q$ points

→ need $O(q)$ relations

→ linear algebra in $\tilde{O}(nq^2)$

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n -dimensional abelian variety

Gaudry's method

- 1 Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \dots, x_n, y_1, \dots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \dots, x_n)$
- 2 Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \dots = x_n(P) = 0\}$
- 3 Decompose enough points of \mathcal{A} as sum of n points of \mathcal{F} using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
- 4 Extract the logarithms with sparse linear algebra

For fixed n , one relation costs $\tilde{O}(1)$

\Rightarrow relation search in $\tilde{O}(q)$ vs linear algebra in $\tilde{O}(q^2)$

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{\mathbb{F}_q}$, n -dimensional abelian variety

Gaudry's method

- 1 Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \dots, x_n, y_1, \dots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \dots, x_n)$
- 2 Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \dots = x_n(P) = 0\}$
- 3 Decompose enough points of \mathcal{A} as sum of n points of \mathcal{F} using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
- 4 Extract the logarithms with sparse linear algebra

Rebalance with double large prime variation:

(heuristic) asymptotic complexity in $\tilde{O}(q^{2-2/n})$ as $q \rightarrow \infty$, n fixed

Index calculus on small dimension abelian varieties

- Generalizes the classical index calculus on $\mathcal{A} = \text{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ where \mathcal{H} is hyperelliptic with small genus g
- Main application so far: $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ where E elliptic curve defined over \mathbb{F}_{q^n} [Gaudry-Diem]

Index calculus on small dimension abelian varieties

- Generalizes the classical index calculus on $\mathcal{A} = \text{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ where \mathcal{H} is hyperelliptic with small genus g
- Main application so far: $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ where E elliptic curve defined over \mathbb{F}_{q^n} [Gaudry-Diem]

Practical difficulty

In general, polynomial systems arising from decompositions are huge
 \rightsquigarrow find nice representations of \mathcal{A} and clever reformulation of the decompositions

- For elliptic curves, use Semaev's summation polynomials
- For $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}))$: no equivalent of Semaev's polynomials, use reformulation by Nagao instead

Section 2

Decomposition attack on hyperelliptic curves defined over extension fields

Decomposition for Jacobians over extension fields

\mathcal{C} curve defined over \mathbb{F}_{q^n} of genus g with a unique point \mathcal{O} at infinity
 $\rightarrow \mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}))$ has dimension ng

Framework

- Factor base:

$$\mathcal{F} = \{D_Q \in \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) : D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$$

▶ about q elements in \mathcal{F}

- Decomposition of an arbitrary divisor $D \in \text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ into ng divisors of the factor base: $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}))$
- Sparse linear algebra + double large prime variation

The Riemann-Roch based approach of Nagao

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = \text{div}(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}(ng(\mathcal{O}) - D)$, \mathbb{F}_{q^n} -vector space of dim. $(n-1)g + 1$

The Riemann-Roch based approach of Nagao

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = \text{div}(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}(ng(\mathcal{O}) - D)$, \mathbb{F}_{q^n} -vector space of dim. $(n-1)g + 1$

- Set of decomp. of D parametrized by $\mathbb{P}(\mathcal{L}_D) \simeq \mathbb{P}^\ell$, $\ell = (n-1)g$
- $(\lambda_1, \dots, \lambda_\ell)$ affine chart of $\mathbb{P}(\mathcal{L}_D)$ s.t. $Q_i \neq \mathcal{O}$ for all $i = 1, \dots, ng$

The Riemann-Roch based approach of Nagao

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = \text{div}(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}(ng(\mathcal{O}) - D)$, \mathbb{F}_q -vector space of dim. $(n-1)g + 1$

- Set of decomp. of D parametrized by $\mathbb{P}(\mathcal{L}_D) \simeq \mathbb{P}^\ell$, $\ell = (n-1)g$
- $(\lambda_1, \dots, \lambda_\ell)$ affine chart of $\mathbb{P}(\mathcal{L}_D)$ s.t. $Q_i \neq \mathcal{O}$ for all $i = 1, \dots, ng$

Goal: determine $\lambda_1, \dots, \lambda_\ell$ such that $x(Q_i) \in \mathbb{F}_q$

Nagao's approach for hyperelliptic curves

Given the Mumford representation of $D = (u, v) \in \text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- $\mathcal{L}(ng(\mathcal{O}_{\mathcal{H}}) - D) = \langle u, xu, \dots, x^{m_1}u, y - v, x(y - v), \dots, x^{m_2}(y - v) \rangle$

$$f_{\lambda_1, \dots, \lambda_{\ell+1}}(x, y) = u \sum_{i=0}^{m_1} \lambda_{2i+1} x^i + (y - v) \sum_{i=0}^{m_2} \lambda_{2i+2} x^i$$

Affine chart of $\mathbb{P}(\mathcal{L}_D) \leftrightarrow \lambda_{\ell+1} = 1$

Nagao's approach for hyperelliptic curves

Given the Mumford representation of $D = (u, v) \in \text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- $\mathcal{L}(ng(\mathcal{O}_{\mathcal{H}}) - D) = \langle u, xu, \dots, x^{m_1}u, y - v, x(y - v), \dots, x^{m_2}(y - v) \rangle$

$$f_{\lambda_1, \dots, \lambda_{\ell+1}}(x, y) = u \sum_{i=0}^{m_1} \lambda_{2i+1} x^i + (y - v) \sum_{i=0}^{m_2} \lambda_{2i+2} x^i$$

Affine chart of $\mathbb{P}(\mathcal{L}_D) \leftrightarrow \lambda_{\ell+1} = 1$

- Using equation of \mathcal{H} , compute $f_{\lambda_1, \dots, \lambda_{\ell}, 1}(x, y) \cdot f_{\lambda_1, \dots, \lambda_{\ell}, 1}(x, -y)/u$ to get a new polynomial with roots $x(Q_1), \dots, x(Q_{ng})$:

$$F_{\lambda_1, \dots, \lambda_{\ell}}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \dots, \lambda_{\ell}) x^i$$

Nagao's approach for hyperelliptic curves

Given the Mumford representation of $D = (u, v) \in \text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- $\mathcal{L}(ng(\mathcal{O}_{\mathcal{H}}) - D) = \langle u, xu, \dots, x^{m_1}u, y - v, x(y - v), \dots, x^{m_2}(y - v) \rangle$

$$f_{\lambda_1, \dots, \lambda_{\ell+1}}(x, y) = u \sum_{i=0}^{m_1} \lambda_{2i+1} x^i + (y - v) \sum_{i=0}^{m_2} \lambda_{2i+2} x^i$$

Affine chart of $\mathbb{P}(\mathcal{L}_D) \leftrightarrow \lambda_{\ell+1} = 1$

- Using equation of \mathcal{H} , compute $f_{\lambda_1, \dots, \lambda_{\ell}, 1}(x, y) \cdot f_{\lambda_1, \dots, \lambda_{\ell}, 1}(x, -y)/u$ to get a new polynomial with roots $x(Q_1), \dots, x(Q_{ng})$:

$$F_{\lambda_1, \dots, \lambda_{\ell}}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \dots, \lambda_{\ell}) x^i$$

→ coefficient c_i of x^i is quadratic in the $\lambda_j \in \mathbb{F}_{q^n}$

Nagao's approach for hyperelliptic curves

$$F_{\lambda_1, \dots, \lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \dots, \lambda_\ell) x^i \text{ with roots } x(Q_1), \dots, x(Q_{ng})$$

→ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \dots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1, \dots, \lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0}, \dots, \lambda_{\ell,n-1})t^j \end{cases}$$

Nagao's approach for hyperelliptic curves

$$F_{\lambda_1, \dots, \lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \dots, \lambda_\ell) x^i \text{ with roots } x(Q_1), \dots, x(Q_{ng})$$

→ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \dots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1, \dots, \lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0}, \dots, \lambda_{\ell,n-1})t^j \end{cases}$$

Then

$$F_{\lambda_1, \dots, \lambda_\ell} \in \mathbb{F}_q[x] \Leftrightarrow \forall i \in \{0, \dots, ng-1\}, \forall j \in \{1, \dots, n-1\}, c_{i,j} = 0$$

Nagao's approach for hyperelliptic curves

$F_{\lambda_1, \dots, \lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \dots, \lambda_\ell) x^i$ with roots $x(Q_1), \dots, x(Q_{ng})$

→ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \dots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1, \dots, \lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0}, \dots, \lambda_{\ell,n-1})t^j \end{cases}$$

Then

$F_{\lambda_1, \dots, \lambda_\ell} \in \mathbb{F}_q[x] \Leftrightarrow \forall i \in \{0, \dots, ng-1\}, \forall j \in \{1, \dots, n-1\}, c_{i,j} = 0$

Decomposition of D

- solve a quadratic polynomial system of $(n-1)ng$ eq./var.
- test if $F_{\lambda_1, \dots, \lambda_\ell}$ is split in $\mathbb{F}_q[x]$
- recover decomposition from roots of $F_{\lambda_1, \dots, \lambda_\ell}$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2 - 2)$

$$\mathcal{H} : y^2 = x^5 + (50t + 66)x^4 + (40t + 22)x^3 + (65t + 23)x^2 + (61t + 3)x + 43t + 6$$

Decomposition of

$$D = [x^2 + (52t + 3)x + 21t + 2, (22t + 41)x + 25t + 42] \in \text{Jac}_{\mathcal{H}}(\mathbb{F}_{67^2})$$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2 - 2)$

$$\mathcal{H} : y^2 = x^5 + (50t + 66)x^4 + (40t + 22)x^3 + (65t + 23)x^2 + (61t + 3)x + 43t + 6$$

Decomposition of

$$D = [x^2 + (52t + 3)x + 21t + 2, (22t + 41)x + 25t + 42] \in \text{Jac}_{\mathcal{H}}(\mathbb{F}_{67^2})$$

- consider $\mathcal{L}(4(\mathcal{O}_{\mathcal{H}}) - D) = \langle u(x), y - v(x), x u(x) \rangle$
- from $f_{\lambda_1, \lambda_2, 1}(x, y) = x u(x) + \lambda_1(y - v(x)) + \lambda_2 u(x)$ and $h(x)$
 $\rightarrow F_{\lambda_1, \lambda_2}(x) = x^4 + (-\lambda_1^2 + 2\lambda_2 + 52t + 3)x^3 + \dots \in \mathbb{F}_{67}[x]$ with roots $x(Q_i)$
- find $\lambda_1, \lambda_2 \in \mathbb{F}_{67^2}$ s.t. F_{λ_1, λ_2} is in $\mathbb{F}_{67}[x]$
 $\Rightarrow \lambda_1, \lambda_2$ such that
$$\begin{cases} -\lambda_1^2 + 2\lambda_2 + 52t + 3 \in \mathbb{F}_{67} \\ \vdots \end{cases}$$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2 - 2)$

Weil restriction: let $\lambda_1 = \lambda_{1,0} + t\lambda_{1,1}$ and $\lambda_2 = \lambda_{2,0} + t\lambda_{2,1}$

$$F_{\lambda_1, \lambda_2}(x) \in \mathbb{F}_{67}[x] \Rightarrow \begin{cases} -2\lambda_{1,0}\lambda_{1,1} + 2\lambda_{2,1} + 52 = 0 \\ \vdots \end{cases} \quad \text{with 2 solutions:}$$

- $\lambda_1 = 7 + 40t$, $\lambda_2 = 8 + 53t$: $F_{\lambda_1, \lambda_2}(x) = x^4 + 53x^3 + 26x^2 + 44x + 12$
- $\lambda_1 = 55 + 37t$, $\lambda_2 = 52 - t$: $F_{\lambda_1, \lambda_2}(x) = (x - 23)(x - 34)(x - 51)(x - 54)$

From $f_{\lambda_1, \lambda_2, 1}(x, y) = x u(x) + \lambda_1(y - v(x)) + \lambda_2 u(x) = 0$ recover $y(Q_i)$

$\rightsquigarrow D = (Q_1) + (Q_2) + (Q_3) + (Q_4) - 4(O_{\mathcal{H}})$ where

$$Q_1 = \begin{vmatrix} 23 \\ 23t+12 \end{vmatrix}, Q_2 = \begin{vmatrix} 34 \\ 10t+43 \end{vmatrix}, Q_3 = \begin{vmatrix} 51 \\ 17t+3 \end{vmatrix}, Q_4 = \begin{vmatrix} 54 \\ 23t+15 \end{vmatrix}$$

Complexity on hyperelliptic curves

Double large prime variation

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

Complexity on hyperelliptic curves

Double large prime variation

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

What about hidden constants?

1 decomp. test \leftrightarrow solve a quadratic system of $(n-1)ng$ eq/var

- Zero-dimensional ideal of degree $d = 2^{(n-1)ng}$
- Resolution with a lexicographic Gröbner basis computation
Tools: grevlex basis with **F4Remake** + ordering change with **FGLM**
- Complexity: at least polynomial in d
 \rightarrow relevant only for n and g small enough

Complexity on hyperelliptic curves

Double large prime variation

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

What about hidden constants?

1 decomp. test \leftrightarrow solve a quadratic system of $(n-1)ng$ eq/var

- Zero-dimensional ideal of degree $d = 2^{(n-1)ng}$
- Resolution with a lexicographic Gröbner basis computation
Tools: grevlex basis with **F4Remake** + ordering change with **FGLM**
- Complexity: at least polynomial in d
 \rightarrow relevant only for n and g small enough

Huge cost of decompositions \rightarrow need for rebalance not so clear in practice

Remark on the non-hyperelliptic case

\mathcal{C} non-hyperelliptic curve defined over \mathbb{F}_{q^n} of genus g , with a unique point $\mathcal{O} \in \mathcal{C}(\mathbb{F}_{q^n})$ at infinity

- Compute a basis of $\mathcal{L}(ng(\mathcal{O}) - D)$ [Heß] and express $f_{\lambda_1, \dots, \lambda_{\ell+1}}$ wrt this basis
- Use (multi-)resultant to compute $F_{\lambda_1, \dots, \lambda_{\ell}}(x)$ from $f_{\lambda_1, \dots, \lambda_{\ell}, 1}$ and equations of \mathcal{C}

Remark on the non-hyperelliptic case

\mathcal{C} non-hyperelliptic curve defined over \mathbb{F}_{q^n} of genus g , with a unique point $\mathcal{O} \in \mathcal{C}(\mathbb{F}_{q^n})$ at infinity

- Compute a basis of $\mathcal{L}(ng(\mathcal{O}) - D)$ [Heß] and express $f_{\lambda_1, \dots, \lambda_{\ell+1}}$ wrt this basis
- Use (multi-)resultant to compute $F_{\lambda_1, \dots, \lambda_{\ell}}(x)$ from $f_{\lambda_1, \dots, \lambda_{\ell}, 1}$ and equations of \mathcal{C}

Decomposition of D

Need to solve a polynomial system of $(n-1)ng$ equations and variables **with degree** > 2

\Rightarrow Resolution of the polynomial system (much) more complicated than in the hyperelliptic case

Remark on the elliptic curve case

Gaudry and Diem's original approach

Decomposition of a random point into sum of n points $Q_1, \dots, Q_n \in \mathcal{F}$ using Semaev summation's polynomials

Nagao versus Semaev for decomposition:

- $n(n-1)$ var/eq of deg. 2 \longleftrightarrow n var/eq of deg. 2^{n-1}
Nagao's decomposition is actually slower than Semaev's approach
- Alternative method to compute symmetrized summation polynomials:
 - 1 Compute $F_{\lambda_1, \dots, \lambda_\ell}(x)$, identify its coefficients with elementary symmetric polynomials of $x(Q_1), \dots, x(Q_n)$
 - 2 Eliminate the variables $\lambda_1, \dots, \lambda_\ell$

Modification of the relation search [Joux-V.]

\mathcal{H} hyperelliptic curve of genus g with a unique point $\mathcal{O}_{\mathcal{H}}$ at infinity

In practice, decompositions as $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_{\mathcal{H}}))$ are too slow to compute

Another type of relations

Compute relations involving only elements of \mathcal{F} :

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

Heuristically, expected number of such relations is $\simeq q^{m-ng} / m!$

→ as $\simeq q$ relations are needed, consider $m = ng + 2$

Modification of the relation search [Joux-V.]

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

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

- Riemann-Roch based approach:
work in $\mathcal{L}((ng+2)(\mathcal{O}_{\mathcal{H}})) = \langle 1, x, x^2, \dots, x^{m_1}, y, yx, \dots, yx^{m_2} \rangle$ of dimension $\ell + 1 = (n-1)g + 3$
- Derive $F_{\lambda_1, \dots, \lambda_\ell}(x)$ whose roots are $x(Q_1), \dots, x(Q_{ng+2})$
- $F_{\lambda_1, \dots, \lambda_\ell}(x) \in \mathbb{F}_q[x] \Rightarrow$ **under-determined** quadratic polynomial system of $n(n-1)g + 2n - 2$ equations in $n(n-1)g + 2n$ variables.
- After initial lex Gröbner basis precomputation, each specialization of the last two variables yields an easy to solve system.

Modified index calculus algorithm

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

Precomputation on $\text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- Find enough relations between factor base elements
- Do linear algebra to get logs of factor base elements (up to a multiplicative constant)

Modified index calculus algorithm

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

Precomputation on $\text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- Find enough relations between factor base elements
- Do linear algebra to get logs of factor base elements (up to a multiplicative constant)

Individual logarithms on $\text{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

How to find x such that $D_2 = [x]D_1$?

- Use some Nagao's style decompositions into ng divisors to obtain a representation of a multiple $[r]D_1$ as sum of factor base elements
- Recover discrete logarithms in base D_1 of all factor base elements
- Decompose a multiple of D_2 and deduce its logarithm

A special case: quadratic extensions

\mathcal{H} hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g + 1$.

- Riemann-Roch: $f(x, y) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0, \dots, \lambda_g, \mu}(x) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0)^2 - \mu^2 h(x)$$

A special case: quadratic extensions

\mathcal{H} hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g + 1$.

- Riemann-Roch: $f(x, y) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0, \dots, \lambda_g, \mu}(x) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0)^2 - \mu^2 h(x)$$

- $\mu = 0 \rightsquigarrow$ trivial relations of the form

$$(P_1) + (\iota(P_1)) + \dots + (P_{g+1}) + (\iota(P_{g+1})) - (2g + 2)\mathcal{O}_{\mathcal{H}} \sim 0$$

A special case: quadratic extensions

\mathcal{H} hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g + 1$.

- Riemann-Roch: $f(x, y) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0, \dots, \lambda_g, \mu}(x) = (x^{g+1} + \lambda_g x^g + \dots + \lambda_0)^2 - \mu^2 h(x)$$

- $\mu = 0 \rightsquigarrow$ trivial relations of the form
 $(P_1) + (\iota(P_1)) + \dots + (P_{g+1}) + (\iota(P_{g+1})) - (2g + 2)\mathcal{O}_{\mathcal{H}} \sim 0$

- Weil restriction: $\lambda_i = \lambda_{i,0} + t\lambda_{i,1}$ and $\mu^2 = \mu_0 + t\mu_1$

$$F_{\lambda_0, \dots, \lambda_g, \mu}(x) \in \mathbb{F}_q[x] \text{ and } \mu \neq 0$$

$$\Leftrightarrow (\lambda_{0,0}, \dots, \lambda_{g,0}, \lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1) \in \mathbb{V}_{\mathbb{F}_q}(\mathbf{I}: (\mu_0, \mu_1)^\infty)$$

where \mathbf{I} is the ideal corresponding to the quadratic polynomial system of $2g + 2$ equations in $2g + 4$ variables.

A special case: quadratic extensions

Key point

Define \mathbb{F}_{q^2} as $\mathbb{F}_q(t)/(t^2 - \omega) \rightsquigarrow$ additional structure on the equations

$$F_{\lambda_0, \dots, \lambda_g, \mu}(x) = (1 \cdot x^{g+1} + \lambda_g x^g + \dots + \lambda_0)^2 - \mu^2 h(x) \in \mathbb{F}_q[x] \Leftrightarrow$$

$$2(1 \cdot x^{g+1} + \lambda_{g,0} x^g + \dots + \lambda_{0,0})(\lambda_{g,1} x^g + \dots + \lambda_{0,1}) - \mu_0 h_1(x) - \mu_1 h_0(x) = 0$$

A special case: quadratic extensions

Key point

Define \mathbb{F}_{q^2} as $\mathbb{F}_q(t)/(t^2 - \omega) \rightsquigarrow$ additional structure on the equations

$$F_{\lambda_0, \dots, \lambda_g, \mu}(x) = (1 \cdot x^{g+1} + \lambda_g x^g + \dots + \lambda_0)^2 - \mu^2 h(x) \in \mathbb{F}_q[x] \Leftrightarrow$$

$$2(1 \cdot x^{g+1} + \lambda_{g,0} x^g + \dots + \lambda_{0,0})(\lambda_{g,1} x^g + \dots + \lambda_{0,1}) - \mu_0 h_1(x) - \mu_1 h_0(x) = 0$$

The polynomials generating I are **multi-homogeneous** of deg (1, 1) in $(1, \lambda_{0,0}, \dots, \lambda_{g,0}), (\lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1)$

→ speeds up the computation of the lex Gröbner basis:

genus	2	3	4
nb eq./var.	6/8	8/10	10/12
approx. timing	<1 sec	2 sec	1 h

$$(g \log_2 q \simeq 70)$$

A special case: quadratic extensions

The polynomials generating I are **multi-homogeneous** of deg $(1, 1)$ in $(1, \lambda_{0,0}, \dots, \lambda_{g,0}), (\lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1)$

$\rightarrow \pi_1(\mathbb{V}(I: (\mu_0, \mu_1)^\infty)) = \pi_1(\mathbb{V}(I: (\lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1)^\infty))$ has dim. 1
where $\pi_1 : (\lambda_{0,0}, \dots, \lambda_{g,0}, \lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1) \mapsto (\lambda_{0,0}, \dots, \lambda_{g,0})$

A special case: quadratic extensions

The polynomials generating I are **multi-homogeneous** of deg $(1, 1)$ in $(1, \lambda_{0,0}, \dots, \lambda_{g,0}), (\lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1)$

$\rightarrow \pi_1(\mathbb{V}(I: (\mu_0, \mu_1)^\infty)) = \pi_1(\mathbb{V}(I: (\lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1)^\infty))$ has dim. 1
 where $\pi_1 : (\lambda_{0,0}, \dots, \lambda_{g,0}, \lambda_{0,1}, \dots, \lambda_{g,1}, \mu_0, \mu_1) \mapsto (\lambda_{0,0}, \dots, \lambda_{g,0})$

Decomposition method

1 Outer loop:

- ▶ “specialization”: instead of evaluating e.g. $\lambda_{0,0}$, choose of a point $(\lambda_{0,0}, \dots, \lambda_{g,0}) \in \pi_1(\mathbb{V}(I: (\mu_0, \mu_1)^\infty))$
- ▶ remaining variables lie in a one-dimensional vector space

2 Inner loop:

- ▶ specialization of a second variable $\lambda_{0,1} \rightsquigarrow$ easy to solve system
- ▶ factorization of $F_{\lambda_0, \dots, \lambda_g, \mu}(x) \in \mathbb{F}_q[x] \rightsquigarrow$ potential relation

A second improvement: sieving

Idea: combine the modified relation search with a sieving technique
→ **avoid the factorization** of $F_{\lambda_0, \dots, \lambda_g, \mu}$ in $\mathbb{F}_q[x]$

A second improvement: sieving

Idea: combine the modified relation search with a sieving technique
 → **avoid the factorization** of $F_{\lambda_0, \dots, \lambda_g, \mu}$ in $\mathbb{F}_q[x]$

Sieving method

- ① Specialize $\lambda_{0,0}, \dots, \lambda_{g,0}$ and express all remaining var. in terms of $\lambda_{0,1}$
 → F becomes a polynomial in $\mathbb{F}_q[x, \lambda_{0,1}]$ of degree 2 in $\lambda_{0,1}$
- ② Enumeration in $x \in \mathbb{F}_q$ instead of $\lambda_{0,1}$
 → corresponding values of $\lambda_{0,1}$ are easier to compute
- ③ Possible to recover the values of $\lambda_{0,1}$ for which there were $\deg_x F$ associated values of x

Time-memory trade-off:

$\lambda_{0,1}$	0	1	2	...	i	...	$p-1$
$\#x$	x_0	x_1	x_2	...	x_i	...	x_{p-1}

Complexity with the modified relation search

On the asymptotic side...

Decomposition in $ng + 2$ instead of ng points seems worse:

- Double large prime variation less efficient:
→ $O(q^{2-2/(ng+2)})$ instead of $O(q^{2-2/ng})$ with Gaudry/Nagao
- Speed-up by sieving only on x -coordinates of “small primes”
→ $O(q^{2-2/(ng+1)})$

Complexity with the modified relation search

On the asymptotic side...

Decomposition in $ng + 2$ instead of ng points seems worse:

- Double large prime variation less efficient:
→ $O(q^{2-2/(ng+2)})$ instead of $O(q^{2-2/ng})$ with Gaudry/Nagao
- Speed-up by sieving only on x -coordinates of “small primes”
→ $O(q^{2-2/(ng+1)})$

But in practice...

- much faster to compute decompositions with our variant
→ about 960 times faster for $(n, g) = (2, 3)$ on a 150-bit curve
- better actual complexity for all accessible values of q

Section 3

Cover and decomposition attacks

A combined attack

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

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

A combined attack

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

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

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 $\text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
- 2 then use decomposition attack on $\text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field \mathbb{F}_q to solve the DLP

A combined attack

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

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

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 $\text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
- 2 then use decomposition attack on $\text{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field \mathbb{F}_q to solve the DLP

→ 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 $g = 9$: $\tilde{O}(p^{7/4})$, ≈ 1500 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

- Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years
- 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 $g = 9$: $\tilde{O}(p^{7/4})$, ≈ 1500 years

- Cover and decomposition:
 - $\tilde{O}(p^{5/3})$ cost using a hyperelliptic genus 3 cover defined over \mathbb{F}_{p^2}
 - 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⁾
→ 960× faster than Nagao

Linear algebra

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

(Descent phase done in ~ 14 s for one point)

⁽¹⁾ Magma on 2.6 GHz Intel Core 2 Duo

⁽²⁾ 2.93 GHz quadri-core Intel Xeon 5550

Scaling data for our implementation

Size of p	$\log_2 p \approx 23$	$\log_2 p \approx 24$	$\log_2 p \approx 25$
Sieving (CPU.hours)	3 600	15 400	63 500
Sieving (real time)	3.5 hours	15 hours	62 hours
Group size	136 bits	142 bits	148 bits
Matrix column nb (SGE reduction)	990 193 (4.2)	1 736 712 (4.8)	3 092 914 (5.4)
Lanczos (CPU.hours)	4 900	16 000	43 800
Lanczos (real time)	77 hours	250 hours	28.5 days

→ approximately 200 CPU.years to break DLP over a 160-bit curve group

Cover and Decomposition Attacks on Elliptic Curves

Vanessa VITSE

Joint work with Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Séminaire de cryptologie, codage et infrastructures sécurisées