Cover Attacks on Trace-Zero groups

Jasper Scholten

COSIC,

Katholieke Universiteit Leuven

Joint work with Claus Diem

Introduction

Let C be a smooth projective curve of genus $g = g(C)$ defined over a finite field $K = \mathbb{F}_{q^n}$.
Let $\mathsf{Cl}^0(C)$ be the degree-0-divisor class group of C, i.e.:

$$\mathsf{Cl}^0(C) = \frac{\{K\text{-rational divisors of degree } 0\}}{\{\text{principal divisors}\}}$$

Facts:

- $\mathsf{Cl}^0(C) \cong \mathrm{Jac}(C)(K)$
- $\#\mathsf{Cl}^0(C) \approx q^{ng}$

The Discrete Logarithm Problem

Assume that $\mathsf{Cl}^0(C)$ can not be embedded in the additive group or multiplicative group of a relatively small finite field using pairings. (This is a condition on $\#\mathsf{Cl}^0(C)$.)

Let ℓ be the largest prime divisor of $\#\mathsf{Cl}^0(C)$.

Methods for solving the DLP in $\mathsf{Cl}^0(C)$:

- Pollard-ρ: Takes $\mathcal{O}(\sqrt{\ell})$ group operations. Best for genera ≤ 3.

The Discrete Logarithm Problem

Assume that $\mathsf{Cl}^0(C)$ can not be embedded in the additive group or multiplicative group of a relatively small finite field using pairings. (This is a condition on $\#\mathsf{Cl}^0(C)$.)

Let ℓ be the largest prime divisor of $\#\mathsf{Cl}^0(C)$.

Methods for solving the DLP in $\mathsf{Cl}^0(C)$:

- Pollard-ρ: Takes $\mathcal{O}(\sqrt{\ell})$ group operations. Best for genera ≤ 3.
- Low-genus Index Calculus (Gaudry, Thériault): $\mathcal{O}\left(g^5 q^{2-\frac{4}{2g+1}+\epsilon}\right)$.

The Discrete Logarithm Problem

Assume that $\mathsf{Cl}^0(C)$ can not be embedded in the additive group or multiplicative group of a relatively small finite field using pairings. (This is a condition on $\#\mathsf{Cl}^0(C)$.)

Let ℓ be the largest prime divisor of $\#\mathsf{Cl}^0(C)$.

Methods for solving the DLP in $\mathsf{Cl}^0(C)$:

- Pollard-ρ: Takes $\mathcal{O}(\sqrt{\ell})$ group operations. Best for genera ≤ 3.
- Low-genus Index Calculus (Gaudry, Thériault): $\mathcal{O}\left(g^5 q^{2-\frac{4}{2g+1}+\epsilon}\right)$.
- High-genus Index Calculus (Adleman, DeMarrais, Huang; Gaudry, Enge): subexponential with $\alpha = \frac{1}{2}$.

Cover Attacks

(aka Weil descent attacks, or Weil restriction attacks).

Dates back to Frey's talk at ECC 1998.

Recall that C is defined over $K = \mathbb{F}_{q^n}$.

Let $k = \mathbb{F}_q$.

Let X be a curve defined over k.

Let $X_K = X \otimes_k K$ be the curve X considered over the field K.

Cover Attacks

A map

$$c : X_K \to C$$

induces a map

$$\phi : \mathsf{Cl}^0(C) \xrightarrow{c^*} \mathsf{Cl}^0(X_K) \xrightarrow{\text{norm}} \mathsf{Cl}^0(X)$$

Cover Attacks

A map

$$c : X_K \to C$$

induces a map

$$\phi : \mathsf{Cl}^0(C) \xrightarrow{c^*} \mathsf{Cl}^0(X_K) \xrightarrow{\text{norm}} \mathsf{Cl}^0(X)$$

Maybe a DLP on $\mathsf{Cl}^0(C)$ can be computed more efficiently by mapping it to $\mathsf{Cl}^0(X)$ and using index calculus.

Cover Attacks

A map

$$c : X_K \to C$$

induces a map

$$\phi : \mathsf{Cl}^0(C) \xrightarrow{c^*} \mathsf{Cl}^0(X_K) \xrightarrow{\text{norm}} \mathsf{Cl}^0(X)$$

Maybe a DLP on $\mathsf{Cl}^0(C)$ can be computed more efficiently by mapping it to $\mathsf{Cl}^0(X)$ and using index calculus.
Two conditions:

- The order-ℓ subgroup of $\mathsf{Cl}^0(C)$ is not in $\ker \phi$.
- $g(X) \approx ng(C)$.

Cover Attacks

How to construct such curves X?

Examples

- Gaudry, Hess, Smart et al. (2000): Construction in characteristic 2, based on Artin-Schreier theory.

Cover Attacks

How to construct such curves X?

Examples

- Gaudry, Hess, Smart et al. (2000): Construction in characteristic 2, based on Artin-Schreier theory.
- Some odd-characteristic cases using Artin-Schreier and Kummer theory (Hess, Thériault, Diem).

Cover Attacks

How to construct such curves X?

Examples

- Gaudry, Hess, Smart et al. (2000): Construction in characteristic 2, based on Artin-Schreier theory.
- Some odd-characteristic cases using Artin-Schreier and Kummer theory (Hess, Thériault, Diem).
- This talk: Constructions for trace-zero groups, based on Galois theory of curves.

Trace-zero groups

Suppose C can already be defined over the small field k:

$$C = C_K = C_k \otimes_k K$$

for some C_k defined over k.

Let

$$T := \ker\left(\mathsf{Cl}^0(C_K) \to \mathsf{Cl}^0(C_k)\right)$$

be the trace-zero group.

$$\#T \approx \frac{(\#K)^g}{(\#k)^g} = q^{(n-1)g}.$$

Trace-zero groups

Advantages of using trace-zero groups for cryptography:

- Easy pointcounting
- Efficient Arithmetic

Trace-zero groups

Advantages of using trace-zero groups for cryptography:

- Easy pointcounting
- Efficient Arithmetic

Examples

- Koblitz curves (n is large).
- Lange, Avanzi: efficient arithmetic for $g(C) = 2$ and $n = 3$.

We concentrate on the case that n is small.

First Approach

Suppose

$$c : X_k \longrightarrow C_k.$$

Consider the “base-extension”

$$c : X_K \longrightarrow C_K.$$

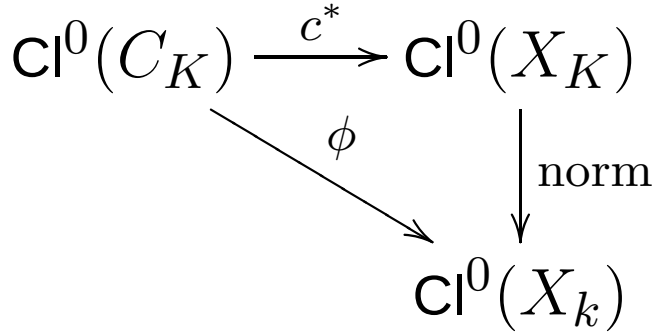
First Approach

Suppose

$$c : X_k \longrightarrow C_k.$$

Consider the "base-extension"

$$c : X_K \longrightarrow C_K.$$



First Approach

Suppose

$$c : X_k \longrightarrow C_k.$$

Consider the "base-extension"

$$c : X_K \longrightarrow C_K.$$

$$\begin{array}{ccc} \mathsf{Cl}^0(C_K) & \xrightarrow{c^*} & \mathsf{Cl}^0(X_K) \\ \downarrow & \overset{\phi}{\searrow} & \downarrow \text{norm} \\ \mathsf{Cl}^0(C_k) & \longrightarrow & \mathsf{Cl}^0(X_k) \end{array}$$

So

$$T \subset \ker \phi.$$

Not what we want. . .

Twists

Modify this construction as follows:
Suppose

$$\tau : X_k \longrightarrow X_k$$

is an automorphism of order n.
One can twist X_k by τ over K/k. Call this twist X_k^τ. This is a curve defined over k, and there is a canonical isomorphism between the base-changed curves $\psi : X_K^\tau \to X_K$.

The set of k-rational points $X_k^\tau(k)$ can be identified with

$$\{P \in X_k(K) \mid \tau^{-1}(P) = \mathrm{Frob}_q(P)\}.$$

Consider the modified cover

$$c' : X_K^{\tau} \xrightarrow{\psi} X_K \xrightarrow{c} C_K.$$

Consider the modified cover

$$c' : X_K^\tau \xrightarrow{\psi} X_K \xrightarrow{c} C_K.$$

We have the induced map $\phi' : \mathsf{Cl}^0(C_K) \longrightarrow \mathsf{Cl}^0(X_k^\tau)$.
The corresponding Trace-zero subgroup T should not be mapped to 0. A necessary condition for this is that

$$c \circ \tau \neq c$$

How to construct such X?

With Galois theory!
Assume n is prime. Let $k(C_k)$ be the function field of C_k.
Let $f \in k(C_k)$ be a function of degree n.
Consider the extension of fields

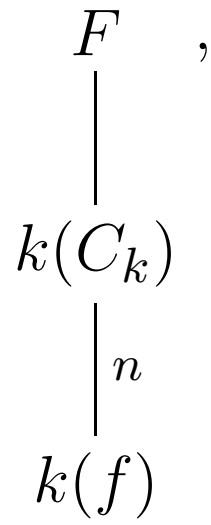
How to construct such X?

With Galois theory!
Assume n is prime. Let $k(C_k)$ be the function field of C_k.
Let $f \in k(C_k)$ be a function of degree n.
Consider the extension of fields

$$\begin{array}{c} k(C_k) \\ \Big| n \\ k(f) \end{array}$$

How to construct such X?

With Galois theory!
Assume n is prime. Let $k(C_k)$ be the function field of C_k.
Let $f \in k(C_k)$ be a function of degree n.
Consider the extension of fields



where F is the Galois closure. So $F/k(f)$ is a Galois extension whose Galois group G containes an element τ of order n.

Curves instead of fields

Assume that k is the exact constant field in F. F is then the function field of some curve X defined over k with an automorphism τ of order n.

$g(C)$ and $g(X)$ are determined in terms of the ramification indices by the Hurwitz formula:

$$2g(C) - 2 = -2n + \sum_{P \in C_k(\bar{k})} (e_P - 1).$$

Galois theory of curves

Assume for now that we work over $\mathbb{C}$. Let $P_1, \ldots, P_r \in \mathbb{P}^1(\mathbb{C})$ denote r distinct points.
Let $\pi = \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{P_1, \ldots, P_r\})$ denote the fundamental group. One knows that

$$\pi \cong \langle s_1, \ldots, s_r \mid s_1 \cdot s_2 \cdot \ldots \cdot s_r = 1 \rangle.$$

There is a one to one correspondence between the following sets:

$$\{\text{covers } f : C \to \mathbb{P}^1 \text{ unramified outside } \{P_1, \ldots, P_r\}\}/\sim$$

and

$$\{\text{finite sets with transitive } \pi\text{-action}\}/\sim$$

Galois theory of curves

Let $S = \{1, \ldots, n\}$ be a finite set with transitive π-action.
Denote the action of s_i by σ_i.
The corresponding cover $f : C \to \mathbb{P}^1$ satisfies:

- $\deg(f) = n$.
- The ramification indices above P_i are exactly the cycle lenghts of σ_i.

Hence the genus $g(C)$ is determined by the group-theoretic data.

Galois theory of curves

Let

$$X \longrightarrow C \longrightarrow \mathbb{P}^1$$

be the Galois closure. Then

- The Galois group G of $X \to \mathbb{P}^1$ is $\langle \sigma_1, \ldots, \sigma_r \rangle \subset S_n$.
- The unique ramification index above P_i is $\mathrm{ord}(\sigma_i)$.

So the genus $g(X)$ is also determined by this data.

Remarks on this construction

The Galois theory of curves over $\overline{\mathbb{F}}_q$ is the same as over $\mathbb{C}$ as long as the characteristic does not divide the group order $\#G$.

Remarks on this construction

The Galois theory of curves over $\overline{\mathbb{F}}_q$ is the same as over $\mathbb{C}$ as long as the characteristic does not divide the group order $\#G$.

Theorem If G is the group of affine linear transformations $x \mapsto ax + b$ of $\mathbb{Z}/n\mathbb{Z}$, then $\ker \phi'$ is annihilated by n.

So for big ℓ, the order-ℓ subgroup of $\mathsf{Cl}^0(C)$ is not mapped to zero.

Summary of examples

Examples for this theorem.

- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 6$: Can be done for every curve C.

Summary of examples

Examples for this theorem.

- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 6$: Can be done for every curve C.
- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 5$: Can be done for $\frac{1}{3}$-rd of the curves C. These are excluded from the Lange's paper.

Summary of examples

Examples for this theorem.

- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 6$: Can be done for every curve C.
- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 5$: Can be done for $\frac{1}{3}$-rd of the curves C. These are excluded from the Lange's paper.
- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 4$: We have an explicit family of such curves C.

Summary of examples

Examples for this theorem.

- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 6$: Can be done for every curve C.
- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 5$: Can be done for $\frac{1}{3}$-rd of the curves C. These are excluded from the Lange's paper.
- $n = 3$, $G = S_3$, $g(C) = 2$, $g(X) = 4$: We have an explicit family of such curves C.
- $n = 7$, G is the group of affine linear transformations of $\mathbb{Z}/7\mathbb{Z}$. $g(C) = 1$, $g(X) = 8$: We have explicit 1-parameter families.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 6$.
Take $\sigma_1 = (1\ 2\ 3), \sigma_2 = (3\ 2)$, $\sigma_3 = \ldots = \sigma_7 = (1\ 2)$.
Given C_k, one can construct the function f as follows:
Take a point $P \in C_k(k)$, and take f from the Riemann-Roch space $\mathcal{L}(3P) \setminus \mathcal{L}(2P)$. Then $f : C_k \to \mathbb{P}^1_k$ has ramification index 3 above ∞, and in general there will be 6 other ramification points, all with index 2.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 6$.
Take $\sigma_1 = (1\ 2\ 3), \sigma_2 = (3\ 2)$, $\sigma_3 = \ldots = \sigma_7 = (1\ 2)$.
Given C_k, one can construct the function f as follows:
Take a point $P \in C_k(k)$, and take f from the Riemann-Roch space $\mathcal{L}(3P) \setminus \mathcal{L}(2P)$. Then $f : C_k \to \mathbb{P}^1_k$ has ramification index 3 above ∞, and in general there will be 6 other ramification points, all with index 2.

Security comparison:
Pollard-ρ: $(\log q)^2 q^2$
Index calculus: $6^5 q^{22/13+\epsilon}$.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 6$.
Take $\sigma_1 = (1\ 2\ 3), \sigma_2 = (3\ 2)$, $\sigma_3 = \ldots = \sigma_7 = (1\ 2)$.
Given C_k, one can construct the function f as follows:
Take a point $P \in C_k(k)$, and take f from the Riemann-Roch space $\mathcal{L}(3P) \setminus \mathcal{L}(2P)$. Then $f : C_k \to \mathbb{P}^1_k$ has ramification index 3 above ∞, and in general there will be 6 other ramification points, all with index 2.

Security comparison:
Pollard-ρ: $(\log q)^2 q^2$
Index calculus: $6^5 q^{22/13+\epsilon}$.

Index calculus is faster for large key sizes

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 5$.

Take $\sigma_1 = \sigma_4 = (1\ 2\ 3),\ \sigma_2 = \sigma_5 = (3\ 2)$ and $\sigma_3 = \sigma_6 = (2\ 1)$.

Explicit construction of f:

Let $\iota : C \to C$ denote the hyperelliptic involution.

Suppose $\mathsf{Cl}^0(C_k)$ has a 3-torsion divisor class that is represented by a divisor class of the form $P_1 + P_2 - O - \iota(O)$ then $3P_1 - 3\iota(P_2)$ is the divisor of a function f. Generically, this f has the required ramification.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 5$.
Take $\sigma_1 = \sigma_4 = (1\ 2\ 3),\ \sigma_2 = \sigma_5 = (3\ 2)$ and $\sigma_3 = \sigma_6 = (2\ 1)$.
Explicit construction of f:
Let $\iota : C \to C$ denote the hyperelliptic involution.
Suppose $\mathrm{Cl}^0(C_k)$ has a 3-torsion divisor class that is represented by a divisor class of the form $P_1 + P_2 - O - \iota(O)$ then $3P_1 - 3\iota(P_2)$ is the divisor of a function f. Generically, this f has the required ramification.

If the class group of a quadratic twist of C_k has 3-torsion of the above form, then this construction can be applied aswell.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 5$.
Take $\sigma_1 = \sigma_4 = (1\ 2\ 3),\ \sigma_2 = \sigma_5 = (3\ 2)$ and $\sigma_3 = \sigma_6 = (2\ 1)$.
Explicit construction of f:
Let $\iota : C \to C$ denote the hyperelliptic involution.
Suppose $\mathsf{Cl}^0(C_k)$ has a 3-torsion divisor class that is represented by a divisor class of the form $P_1 + P_2 - O - \iota(O)$ then $3P_1 - 3\iota(P_2)$ is the divisor of a function f. Generically, this f has the required ramification.

If the class group of a quadratic twist of C_k has 3-torsion of the above form, then this construction can be applied aswell.

One can construct an explicit family such that the curve X is hyperelliptic.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 4$.

Take $\sigma_1 = (1\ 2\ 3\ 4\ 5)$, $\sigma_2 = (1\ 2\ 3\ 5\ 4)$ and $\sigma_3 = (1\ 3)(2\ 4)$.

Explicit families can be constructed using Kummer theory.

Examples

Example for $g(C) = 2,\ n = 3,\ g(X) = 4$.
Take $\sigma_1 = (1\ 2\ 3\ 4\ 5)$, $\sigma_2 = (1\ 2\ 3\ 5\ 4)$ and $\sigma_3 = (1\ 3)(2\ 4)$.
Explicit families can be constructed using Kummer theory.

Example for $g(C) = 1$, $n = 7$, $g(X) = 8$.
Take $\sigma_1 = (1\ 6)(2\ 5)(3\ 4)$, $\sigma_2 = (1\ 7)(2\ 6)(3\ 5)$,
$\sigma_3 = (1\ 2\ 4)(3\ 6\ 5)$ and $\sigma_4 = (2\ 5\ 3)(4\ 6\ 7)$.
Explicit families can be constructed using Kummer theory.

Are there other examples?

- $n = 5$, $G = A_5$, $g(C) = 1$, $g(X) = 4$: There is one such curve: $y^2 = x^3 + 3165x - 31070$.

Are there other examples?

- $n = 5$, $G = A_5$, $g(C) = 1$, $g(X) = 4$: There is one such curve: $y^2 = x^3 + 3165x - 31070$.
- There are other isolated examples in Diem's thesis.

Are there other examples?

- $n = 5$, $G = A_5$, $g(C) = 1$, $g(X) = 4$: There is one such curve: $y^2 = x^3 + 3165x - 31070$.
- There are other isolated examples in Diem's thesis.
- A complete classification is work in progress, joint work with Avanzi.