Attacks on the curve-based discrete logarithm problem

Vanessa VITSE

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Summer School – ECC 2011

Section 1

Introduction

The Discrete Logarithm Problem

Definition

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

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

The Diffie-Hellman problem

Computational Diffie-Hellman problem

CDHP: given $g, g^a, g^b \in G$, compute g^{ab}

Closely related to the DLP:

- CDHP $\prec$ DLP
- converse not known but strong hints of equivalence [Maurer-Wolf]

Many cryptographic protocols actually rely on the assumption that CDHP is hard, especially elliptic curve cryptography.

Relevance in cryptography

The canonical example: Diffie-Hellman key exchange

Alice $[secret = a]$ Bob $[secret = b]$

$$\xrightarrow{\quad g^a \quad}$$

$$\xleftarrow{\quad g^b \quad}$$

$K_{ab} = (g^b)^a$ shared key $K_{ab} = (g^a)^b$

Other classical protocols based on CDHP:

- ElGamal encryption
- (EC)DSA signature scheme
- pairing-based cryptosystems (bilinear CDHP)
- ...

Goals of these lectures

Survey of existing attacks on the **curve-based** DLP:

1. generic attacks
2. index calculus for
   - hyperelliptic curves of genus > 2
   - curves defined over extension fields
   - small degree plane curves
3. transfer methods using
   - pairings
   - lift to characteristic zero fields
   - isogenies
   - Weil descent (GHS)

Generic attacks on the DLP

Let G a finite abelian group of known order n.

Definition

An algorithm is **generic** when the only authorized operations are:

- addition of two elements
- opposite of an element
- equality test of two elements

$\rightsquigarrow$ representation of the group as a black box.

Generic attacks can be applied indifferently to any group.

Generic attacks on the DLP

Let G a finite abelian group of known order n.

Definition

An algorithm is **generic** when the only authorized operations are:

- addition of two elements
- opposite of an element
- equality test of two elements

$\rightsquigarrow$ representation of the group as a black box.

Generic attacks can be applied indifferently to any group.

First example: brute force search!

For all $x \in \{0; \ldots; n-1\}$, test if $g^x = h$.
Exponential complexity in the size of the group...

Pohlig-Hellman reduction

Let $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ be the prime factorization of $\#G$.

G cyclic $\rightsquigarrow$ $G \simeq \prod_i G_i$ where $G_i \simeq \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$

1. work with the subgroup G_i to find the DL mod $p_i^{\alpha_i}$ and use Chinese remaindering to deduce the DL in G
2. further simplification: to obtain the DL mod $p_i^{\alpha_i}$, compute iteratively its expression in base p_i by solving α_i DLPs in the subgroup of order p_i of G_i.

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2

Pohlig-Hellman reduction: example

Let $E \; : \; y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0)$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$[x_0 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) \quad = \quad (12, 47)$$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rcl} [x_0 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\ \Rightarrow \quad [x_0]([3^3](135, 51)) & = & [3^3](12, 47) \end{array}$$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rcl} & [x_0 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [x_0](57, 41) & = & (57, 41) \end{array}$$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{rcl}
 & [x_0 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\
\Rightarrow & [x_0](57, 41) & = & (57, 41) \\
\Rightarrow & x_0 & = & 1
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$[1 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) \quad = \quad (12, 47)$$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rrcl} & [1 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) - (135, 51) \end{array}$$

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{rccc}
 & [1 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\
\Rightarrow & [3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) - (135, 51) \\
\Rightarrow & [x_1]([3^3](135, 51)) & = & [3^2]((12, 47) - (135, 51))
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rrcl} & [1 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) - (135, 51) \\ \Rightarrow & [x_1](57, 41) & = & \mathcal{O} \end{array}$$

Pohlig-Hellman reduction: example

Let $E \; : \; y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{rccc}
 & [1 + 3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) \\
\Rightarrow & [3x_1 + 3^2x_2 + 3^3x_3](135, 51) & = & (12, 47) - (135, 51) \\
\Rightarrow & [x_1](57, 41) & = & \mathcal{O} \\
\Rightarrow & x_1 & = & 0
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$[1 + 3 \cdot 0 + 3^2 x_2 + 3^3 x_3](135, 51) \quad = \quad (12, 47)$$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{rrcl}
 & [1 + 3 \cdot 0 + 3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) \\
\Rightarrow & [3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) - (135, 51)
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E \ : \ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{rcl}
[1 + 3 \cdot 0 + 3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) \\
\Rightarrow \quad [3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) - (135, 51) \\
\Rightarrow \quad [x_2]([3^3](135, 51)) & = & [3]((12, 47) - (135, 51))
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E \;:\; y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$
\begin{array}{ccc}
 & [1 + 3 \cdot 0 + 3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) \\
\Rightarrow & [3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) - (135, 51) \\
\Rightarrow & [x_2](57, 41) & = & (57, 116)
\end{array}
$$

Pohlig-Hellman reduction: example

Let $E \; : \; y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rccl} & [1 + 3 \cdot 0 + 3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [3^2 x_2 + 3^3 x_3](135, 51) & = & (12, 47) - (135, 51) \\ \Rightarrow & [x_2](57, 41) & = & (57, 116) \\ \Rightarrow & x_2 & = & 2 \end{array}$$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$[1 + 3 \cdot 0 + 3^2 \cdot 2 + 3^3 x_3](135, 51) \quad = \quad (12, 47)$$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{lrcl} & [1 + 3 \cdot 0 + 3^2 \cdot 2 + 3^3 x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [x_3]([3^3](135, 51)) & = & (12, 47) - [19](135, 51) \end{array}$$

Pohlig-Hellman reduction: example

Let $E \;:\; y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rccl} & [1 + 3 \cdot 0 + 3^2 \cdot 2 + 3^3 x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [x_3](57, 41) & = & (57, 116) \\ \Rightarrow & x_3 & = & 2 \end{array}$$

Pohlig-Hellman reduction: example

Let $E : y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
$[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$

2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
$2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

$$\begin{array}{rccc} & [1 + 3 \cdot 0 + 3^2 \cdot 2 + 3^3 x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [x_3](57, 41) & = & (57, 116) \\ \Rightarrow & x_3 & = & 2 \end{array}$$

$\Rightarrow x = 73 \bmod 81$

Pohlig-Hellman reduction: example

Let $E\ :\ y^2 = x^3 + 77x + 28$ elliptic curve defined over $\mathbb{F}_{157}$,
solve $[x]P = Q$ where $P = (9, 115)$ and $Q = (2, 70)$
The order of P is $162 = 2 \cdot 3^4$

1. Mod 2: solve $[x]([3^4]P) = [3^4]Q$ where $[3^4]P = (24, 0)$ has order 2
   $[3^4]Q = (24, 0) \quad \Rightarrow x = 1 \bmod 2$
2. Mod 3^4: solve $[x]([2]P) = [2]Q$ where $[2]P = (135, 51)$ has order 3^4
   $2[Q] = (12, 47)$, $x = x_0 + 3x_1 + 3^2x_2 + 3^3x_3$

   $$\begin{array}{rcl} & [1 + 3 \cdot 0 + 3^2 \cdot 2 + 3^3 x_3](135, 51) & = & (12, 47) \\ \Rightarrow & [x_3](57, 41) & = & (57, 116) \\ \Rightarrow & x_3 & = & 2 \end{array}$$

   $\Rightarrow x = 73 \bmod 81$
3. Chinese remainders: $x = 73 \bmod 162$

Pohlig-Hellman reduction

Let $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ be the prime factorization of $\#G$.

G cyclic $\rightsquigarrow$ $G \simeq \prod_i G_i$ where $G_i \simeq \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$

1. work with the subgroup G_i to find the DL mod $p_i^{\alpha_i}$ and use Chinese remaindering to deduce the DL in G
2. further simplification: to obtain the DL mod $p_i^{\alpha_i}$, compute iteratively its expression in base p_i by solving α_i DLPs in the subgroup of order p_i of G_i.

Consequence

Solving the DLP in a group of size n is approximately as hard as solving it in a group of size the largest prime factor of n.

Baby-step giant-step [Shanks]

Idea

Use birthday paradox and space-time trade-off to speed up the exhaustive search

Let $d = \lceil\sqrt{\#G}\rceil$

1. Compute and store (g^j, j) for $0 \leq j \leq d$
2. For $0 \leq k \leq \#G/d$, compute $h.(g^{-d})^k$ and check if it appears in the stored list
3. Collision $h.(g^{-d})^k = g^j \Rightarrow$ DL of h is $(j + kd)$

Using a hash table, cost of membership test in step 2 is in $O(1)$
$\rightsquigarrow$ overall complexity is $O(\sqrt{\#G})$ in both time and memory

Complexity bounds

Other generic algorithm: Pollard-Rho

- based on the iteration of a pseudo-random function
- same time complexity in $O(\sqrt{\#G})$
- but $O(1)$ memory requirement

Complexity bounds

Other generic algorithm: Pollard-Rho

- based on the iteration of a pseudo-random function
- same time complexity in $O(\sqrt{\#G})$
- but $O(1)$ memory requirement

Best possible complexity of generic attacks!

Theorem [Shoup]

The complexity of a generic attack of the DLP on a group G is in $\Omega(\sqrt{p})$ where p is the largest prime factor of $\#G$.

To improve over this complexity, one has to use additional information on the given group G.

Hardness of the DLP

Depends on the choice of the group G. Some classical examples:

1. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm
2. $G \subset (\mathbb{Z}/p\mathbb{Z}^*, \times)$: subexponential complexity in $L_p(1/3)$ (NFS)
3. $G \subset (\mathbb{F}_q^*, \times)$: subexponential complexity in $L_q(1/3)$ (FFS/NFS)

Hardness of the DLP

Depends on the choice of the group G. Some classical examples:

1. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm
2. $G \subset (\mathbb{Z}/p\mathbb{Z}^*, \times)$: subexponential complexity in $L_p(1/3)$ (NFS)
3. $G \subset (\mathbb{F}_q^*, \times)$: subexponential complexity in $L_q(1/3)$ (FFS/NFS)

Key points on the complexity function L

$$L_n(\alpha, c) = \exp\left(c(\log n)^\alpha (\log\log n)^{1-\alpha}\right)$$

- $L_n(\alpha)$ shorthand for $L_n(\alpha, c + o(1))$ for a constant c.
- $L(\alpha_2, c_2) = o(L(\alpha_1, c_1))$ if $\alpha_2 < \alpha_1$ or $\alpha_2 = \alpha_1$ and $c_2 < c_1$
- $L(\alpha_1, c_1)L(\alpha_2, c_2) = L(\alpha_1, c_1 + o(1))$ if $\alpha_1 > \alpha_2$
- $L(\alpha, c_1)L(\alpha, c_2) = L(\alpha, c_1 + c_2)$

Hardness of the DLP

Depends on the choice of the group G. Some classical examples:

1. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm
2. $G \subset (\mathbb{Z}/p\mathbb{Z}^*, \times)$: subexponential complexity in $L_p(1/3)$ (NFS)
3. $G \subset (\mathbb{F}_q^*, \times)$: subexponential complexity in $L_q(1/3)$ (FFS/NFS)

Key points on the complexity function L

$$L_n(\alpha, c) = \exp\left(c(\log n)^\alpha (\log\log n)^{1-\alpha}\right)$$

4. $G \subset (\mathrm{Jac}_\mathcal{C}(\mathbb{F}_q), +)$: if the genus of $\mathcal{C}$ is s.t. $g > 2$, existence of algorithms asymptotically faster than generic attacks

Target groups

In these lectures, we focus on curve-based DLP, i.e. on the following groups:

- $G \subset E(\mathbb{F}_q)$, the group of $\mathbb{F}_q$-rational points of an elliptic curve
- $G \subset \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$ the divisor class group of an algebraic curve $\mathcal{C}$, with an emphasis on the hyperelliptic case
- when q is a prime power, Weil restrictions of the above varieties

Note that all these targets are examples of abelian varieties.

Section 2

The index calculus method

Introduction to index calculus

Originally developed for the factorization of large integers, improving on the square congruence method of Fermat.

Index calculus based Number/Function Field Sieve hold records for both integer factorization and finite field DLP.

Idea

- Find group relations between a "small" number of generators (or *factor base* elements)
- With sufficiently many relations and linear algebra, deduce the group structure and the DL of elements

Basic outline

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

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$

Basic outline

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

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g + [b_i]h$ (a_i, b_i random) into $\mathcal{F}$

$$[a_i]g + [b_i]h = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

Basic outline

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

1. Choice of a factor base: $\mathcal{F} = \{g_1, \dots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g + [b_i]h$ (a_i, b_i random) into $\mathcal{F}$

$$[a_i]g + [b_i]h = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

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 $v = (v_1, \dots, v_k) \in \ker({}^t M)$ such that $vA \neq \begin{pmatrix} 0 & 0 \end{pmatrix} \bmod r$
   - compute the solution of DLP: $x = -\left(\sum_i a_i v_i\right) / \left(\sum_i b_i v_i\right) \bmod r$

Basic outline (variant)

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g$ (a_i random) into $\mathcal{F}$

$$[a_i]g = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

Basic outline (variant)

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g$ (a_i random) into $\mathcal{F}$

$$[a_i]g = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the vector $A = \left(a_i\right)_{1 \leq i \leq k}$ and the matrix $M = \left(c_{ij}\right)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $X = (x_j)$ unique solution to $MX = A \bmod r$

Basic outline (variant)

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g$ (a_i random) into $\mathcal{F}$

$$[a_i]g = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the vector $A = \left(a_i\right)_{1 \leq i \leq k}$ and the matrix $M = \left(c_{ij}\right)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $X = (x_j)$ unique solution to $MX = A \bmod r$
4. Descent phase: find a relation involving h

$$[a]g + [b]h = \sum_{j=1}^{N} [c_j]g_j, \text{ where } b \wedge r = 1$$

and deduce the solution of DLP $\left(\sum_{j=1}^{N} c_j x_j - a\right) b^{-1} \bmod r$.

Second outline

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: find relations between elements of $\mathcal{F}$

$$\sum_{j=1}^{N} [c_{ij}] g_j = 0, \quad \text{where } c_{ij} \in \mathbb{Z}$$

Second outline

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: find relations between elements of $\mathcal{F}$

$$\sum_{j=1}^{N} [c_{ij}] g_j = 0, \quad \text{where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the matrix $M = (c_{ij})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $X = (x_j)$ s.t. $\ker M = \mathrm{span}(X) \bmod r$

Second outline

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: find relations between elements of $\mathcal{F}$

$$\sum_{j=1}^{N} [c_{ij}] g_j = 0, \quad \text{where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the matrix $M = (c_{ij})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $X = (x_j)$ s.t. $\ker M = \mathrm{span}(X) \bmod r$
4. Descent phase: find relations involving g and h

$$[a]g = \sum_{j=1}^{N} [c_j] g_j, \quad [b]h = \sum_{j=1}^{N} [c'_j] g_j, \quad \text{where } a, b \wedge r = 1$$

and deduce DLP solution $(\sum_j c_j x_j)(\sum_j c'_j x_j)(ab)^{-1} \bmod r$.

General remarks

1. Relation search very specific to the group (several examples in this lecture) and can be the main obstacle (elliptic curves)

2. On the other hand, linear algebra almost the same for all groups

3. Balance to find between the two phases:

   - if $\#\mathcal{F}$ small, few relations needed and fast linear algebra but small probability of decomposition $\rightsquigarrow$ many trials before finding a relation

   - if $\#\mathcal{F}$ large, easy to find relations but many of them needed and slow linear algebra

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\begin{aligned}
g^1 &= 31, \text{ not smooth} \\
g^2 &= -2 = -1 \times 2 \\
g^3 &= 45 = 3^2 \times 5 \\
g^4 &= 4 = 2^2 \\
g^5 &= 17, \text{ not smooth}
\end{aligned}$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$
\begin{aligned}
g^1 &= 31, \text{ not smooth} \\
g^2 &= -2 = -1 \times 2 \\
g^3 &= 45 = 3^2 \times 5 \\
g^4 &= 4 = 2^2 \\
g^5 &= 17, \text{ not smooth} \\
&\ldots
\end{aligned}
$$

$$
\begin{aligned}
&\ldots \\
g^{13} &= -49 = -1 \times 7^2 \\
g^{14} &= -21 = -1 \times 3 \times 7 \\
g^{15} &= -9 = -1 \times 3^2 \\
g^{16} &= 42 = 2 \times 3 \times 7 \\
g^{21} &= -35 = -1 \times 5 \times 7
\end{aligned}
$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\begin{pmatrix} 2 \\ 3 \\ 4 \\ 13 \\ 14 \\ 15 \\ 16 \\ 21 \end{pmatrix} = \begin{array}{c} \begin{array}{ccccc} -1 & 2 & 3 & 5 & 7 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array} X \mod 106 \quad \Rightarrow \quad X = \begin{pmatrix} 53 \\ 55 \\ 34 \\ 41 \\ 33 \end{pmatrix}$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\log(-1) = 53 \quad \log(2) = 55 \quad \log(3) = 34 \quad \log(5) = 41 \quad \log(7) = 33$$

$$gh = 54 = 2 \times 3^3 = (g^{55})(g^{34})^3 = g^{51} \Rightarrow h = g^{50}$$

Complexity in the prime field case

Optimal choice of B?

Theorem [Bruijn,Canfield-Erdös-Pomerance]

A random integer smaller than x is $L_x(\alpha, c)$-smooth with probability

$$1/L_x(1-\alpha, (1-\alpha)/c) \text{ as } x \to \infty.$$

Complexity in the prime field case

Optimal choice of B?

Theorem [Bruijn,Canfield-Erdös-Pomerance]

A random integer smaller than x is $L_x(\alpha, c)$-smooth with probability

$$1/L_x(1-\alpha, (1-\alpha)/c) \text{ as } x \to \infty.$$

- Let $B = L_p(\alpha, c)$
- Relation step complexity in $L_p(\alpha, c)L_p(1-\alpha, (1-\alpha)/c)$
  $\rightsquigarrow$ best choice is $B \simeq L_p(1/2, 1/\sqrt{2})$
- Overall complexity of this index calculus in $L_p(1/2, \sqrt{2})$ (assuming quadratic complexity of linear algebra step)

The linear algebra step

The matrix of relations

- very large for real-world applications: typical size is several millions rows/columns.
- extremely **sparse**: only a few non-zero coefficients per row

$\Rightarrow$ use sparse linear algebra techniques instead of standard resolution tools

The linear algebra step

The matrix of relations

- very large for real-world applications: typical size is several millions rows/columns.
- extremely **sparse**: only a few non-zero coefficients per row

$\Rightarrow$ use sparse linear algebra techniques instead of standard resolution tools

Main ideas:

- Keep the matrix sparse (~~Gauss~~)
- Use matrix-vector products: cost only proportional to the number of non-zero entries

Two principal algorithms: Lanczos and Wiedemann

Wiedemann's algorithm (Coppersmith)

Goal: given M square $n \times n$ matrix, A vector, find X s.t. $MX = A$
Idea: compute the minimal polynomial P s.t. $P(M)v = 0$ for a given vector v

Wiedemann's algorithm (Coppersmith)

Goal: given M square $n \times n$ matrix, A vector, find X s.t. $MX = A$
Idea: compute the minimal polynomial P s.t. $P(M)v = 0$ for a given vector v

1. Berlekamp-Massey: compute minimal polynomial $P = \sum_{k=1}^{d} p_k x^k$ of the sequence $a_i = u \cdot M^i v$ where u random vector
2. If $P(M)v \neq 0$, start again with a new u and take lcm
3. To deduce X
   - if $A = 0$: take $v = Mw$, w random, then $X = P(M)w$
   - otherwise: take $v = A$, then $X = -(p_0)^{-1} \sum_{k=1}^{d} p_k M^{k-1} A$

Wiedemann's algorithm (Coppersmith)

Goal: given M square $n \times n$ matrix, A vector, find X s.t. $MX = A$
Idea: compute the minimal polynomial P s.t. $P(M)v = 0$ for a given vector v

1. Berlekamp-Massey: compute minimal polynomial $P = \sum_{k=1}^{d} p_k x^k$ of the sequence $a_i = u \cdot M^i v$ where u random vector
2. If $P(M)v \neq 0$, start again with a new u and take lcm
3. To deduce X
   - if $A = 0$: take $v = Mw$, w random, then $X = P(M)w$
   - otherwise: take $v = A$, then $X = -(p_0)^{-1} \sum_{k=1}^{d} p_k M^{k-1} A$

Complexity

$O(n)$ dot products and $O(n)$ matrix-vector multiplications
$\Rightarrow$ if M has c non-zero entries per row, total cost in $O(n^2 c)$

Improving the linear algebra step

Remark

- Relation search always straightforward to distribute
- Not so true for the linear algebra

Often advantageous to compute many more relations than needed and use extra information to simplify the relation matrix

Two methods:

1. **Structured Gaussian elimination:**
   Particularly well-suited when elements of the factor base have different frequencies (e.g on finite fields)

2. **Large prime variations**

Structured Gaussian elimination [LaMacchia-Odlyzko]

Goal: reduce the size of the matrix while keeping it sparse.
Distinction between the matrix columns (i.e. the factor base elements):

- dense columns correspond to "small primes"
- other columns correspond to "large primes"

Structured Gaussian elimination [LaMacchia-Odlyzko]

Goal: reduce the size of the matrix while keeping it sparse.
Distinction between the matrix columns (i.e. the factor base elements):

- dense columns correspond to "small primes"
- other columns correspond to "large primes"

1. If a column contains only one non-zero entry, remove it and the corresponding row.
   Also, remove columns/rows containing only zeroes.
2. Mark some new columns as dense
3. Find rows with only one ± 1 coefficient in the non-dense part
   - Use this coefficient as a pivot to clear its column
   - Remove corresponding row and column
4. Remove rows that have become too dense and go back to step 1

Section 3

Applications of index calculus

Subsection 1

The hyperelliptic case

Hyperelliptic curves

Reminders

An (imaginary) hyperelliptic curve $\mathcal{H}$ of genus g defined over $\mathbb{F}_q$ is given by an equation

$$y^2 + h_0(x)y = h_1(x), \quad h_0, h_1 \in \mathbb{F}_q[x], \ \deg h_0 \leq g, \ \deg h_1 = 2g + 1$$

- possesses a unique point at infinity $\mathcal{O}_\mathcal{H}$
- hyperelliptic involution ι:
  maps $P = (x_P, y_P)$ to $\iota(P) = (x_P, -y_P - h_0(x_P))$

Jacobian variety $\mathrm{Jac}_\mathcal{H}(\mathbb{F}_q)$ (or divisor class group): set of linear equivalence class of degree zero divisors (defined over $\mathbb{F}_q$)

- $\#\mathcal{H}(\mathbb{F}_q) \simeq q$
- $\#\mathrm{Jac}_\mathcal{H}(\mathbb{F}_q) \simeq q^g$

Representations of elements of $\mathrm{Jac}_{\mathcal{H}}$

Reduced representation

An element $[D] \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ has a unique reduced representation

$$D \sim (P_1) + \cdots + (P_r) - r(\mathcal{O}_{\mathcal{H}}), \quad r \leq g,\ P_i \neq \iota(P_j) \text{ for } i \neq j$$

Note: the points P_i's are usually not $\mathbb{F}_q$-rational

Mumford representation

One-to-one correspondence between elements of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ and couples of polynomials $(u, v) \in \mathbb{F}_q[x]^2$ s.t.

- u monic, $\deg u \leq g$
- $\deg v < \deg u$
- u divides $v^2 + vh_0 - h_1$

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Allows to apply index calculus [Enge-Gaudry]

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) : u \text{ irreducible, } \deg u \leq B\}$ ("small prime divisors")
- Element $[a_i]D_0 + [b_i]D_1$ yields a relation if corresponding u polynomial is B-smooth

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Allows to apply index calculus [Enge-Gaudry]

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) : u \text{ irreducible}, \ \deg u \leq B\}$ ("small prime divisors")
- Element $[a_i]D_0 + [b_i]D_1$ yields a relation if corresponding u polynomial is B-smooth

Possible to divide size of $\mathcal{F}$ by 2 using the hyperelliptic involution

Analysis in the large genus case

Very similar to the prime field case:

Theorem [Enge-Gaudry-Stein]

Let $B = \lceil \log_q(L_{q^g}(1/2, c)) \rceil$. The probability that a random element of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ is B-smooth is bounded from below by

$$1/L_{q^g}(1/2, 1/2c + o(1)).$$

Analysis in the large genus case

Very similar to the prime field case:

Theorem [Enge-Gaudry-Stein]

Let $B = \left\lceil \log_q(L_{q^g}(1/2, c)) \right\rceil$. The probability that a random element of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ is B-smooth is bounded from below by

$$1/L_{q^g}(1/2, 1/2c + o(1)).$$

As $q \to \infty$ and $g/\log q \to \infty$,

- optimal choice of B is in $\log_q(L_{q^g}(1/2, 1/\sqrt{2}))$
- total complexity is in $L_{q^g}(1/2, \sqrt{2} + o(1))$

The small genus case

Problem

When g small i.e. $g = o(\log q)$, former analysis suggests $B < 1$...

The small genus case

Problem

When g small i.e. $g = o(\log q)$, former analysis suggests $B < 1$...

Gaudry's algorithm for small genus curves

Choose $B = 1$

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) \ : \ \deg u = 1\}$ of size $\simeq q$
- $D = (u, v)$ decomposable $\Leftrightarrow$ u splits over $\mathbb{F}_q$
- Probability of decomposition $\simeq 1/g!$

$\Rightarrow O(g!q)$ tests (relation search) $+$ $O(gq^2)$ field operations (linear alg.)

Total cost: $O((g^2 \log^3 q)g!q + (g^2 \log q)q^2)$

The small genus case

Problem

When g small i.e. $g = o(\log q)$, former analysis suggests $B < 1$...

Gaudry's algorithm for small genus curves

Choose $B = 1$

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) \ : \ \deg u = 1\}$ of size $\simeq q$
- $D = (u, v)$ decomposable $\Leftrightarrow$ u splits over $\mathbb{F}_q$
- Probability of decomposition $\simeq 1/g!$

$\Rightarrow$ $O(g!q)$ tests (relation search) + $O(gq^2)$ field operations (linear alg.)

Total cost: $O((g^2 \log^3 q)g!q + (g^2 \log q)q^2)$

For fixed g, resolution of the DLP in $\tilde{O}(q^2)$

$\Rightarrow$ better than generic attacks as soon as $g > 4$

Reducing the factor base

For fixed genus g, relation search in $\tilde{O}(q)$ **vs** linear algebra in $\tilde{O}(q^2)$
$\rightsquigarrow$ need to rebalance the two phases

Reducing the factor base

For fixed genus g, relation search in $\tilde{O}(q)$ **vs** linear algebra in $\tilde{O}(q^2)$
$\rightsquigarrow$ need to rebalance the two phases

First idea: reduce the factor base [Harley]

- Define new factor base $\mathcal{F}' \subset \mathcal{F}$ ("small primes") with $\#\mathcal{F}' = q^\alpha$
  $\rightsquigarrow$ linear algebra in $\tilde{O}(q^{2\alpha})$
- Keep relations involving only small primes, discard others
  $\rightsquigarrow$ proba. of decomposition drops by factor $\left(\frac{\#\mathcal{F}'}{\#\mathcal{F}}\right)^g = \left(\frac{q^\alpha}{q}\right)^g$
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)g}\, q^\alpha)$
- Asymptotically optimal choice $\alpha = 1 - 1/(g+1)$
  Total complexity in $\tilde{O}(q^{2-2/(g+1)})$

One large prime variation [Thériault]

Main ideas

- Same new “small prime” factor base $\mathcal{F}' \subset \mathcal{F}$ with $\#\mathcal{F}' = q^\alpha$
  “large primes”: $\mathcal{F} \setminus \mathcal{F}'$
- Keep “partial” relations involving at most one large prime
- Combine partial relations with same large prime to get “full” relations (involving only small primes)

One large prime variation [Thériault]

Main ideas

- Same new "small prime" factor base $\mathcal{F}' \subset \mathcal{F}$ with $\#\mathcal{F}' = q^\alpha$
  "large primes": $\mathcal{F} \setminus \mathcal{F}'$
- Keep "partial" relations involving at most one large prime
- Combine partial relations with same large prime to get "full" relations (involving only small primes)

Improvement of Harley's method:

- Probability of decomposition drops by factor $\left(\frac{q^\alpha}{q}\right)^{g-1}$

One large prime variation [Thériault]

Main ideas

- Same new "small prime" factor base $\mathcal{F}' \subset \mathcal{F}$ with $\#\mathcal{F}' = q^{\alpha}$
  "large primes": $\mathcal{F} \setminus \mathcal{F}'$
- Keep "partial" relations involving at most one large prime
- Combine partial relations with same large prime to get "full" relations (involving only small primes)

Improvement of Harley's method:

- Probability of decomposition drops by factor $\left(\frac{q^{\alpha}}{q}\right)^{g-1}$
- Birthday paradox: $\simeq \sqrt{q\, q^{\alpha}}$ partial relations needed to obtain $\simeq q^{\alpha}$ full relations
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)(g-1)} q^{(1+\alpha)/2})$

One large prime variation [Thériault]

Main ideas

- Same new "small prime" factor base $\mathcal{F}' \subset \mathcal{F}$ with $\#\mathcal{F}' = q^\alpha$
  "large primes": $\mathcal{F} \setminus \mathcal{F}'$
- Keep "partial" relations involving at most one large prime
- Combine partial relations with same large prime to get "full" relations (involving only small primes)

Improvement of Harley's method:

- Probability of decomposition drops by factor $\left(\frac{q^\alpha}{q}\right)^{g-1}$
- Birthday paradox: $\simeq \sqrt{q\, q^\alpha}$ partial relations needed to obtain $\simeq q^\alpha$ full relations
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)(g-1)} q^{(1+\alpha)/2})$
- Asymptotically optimal choice $\alpha = 1 - 1/(g + 1/2)$

Total complexity in $\tilde{O}(q^{2-2/(g+1/2)})$

Double large prime variation

Further improvement [Gaudry-Thomé-Thériault-Diem]:

- Keep relations involving at most two large primes
  $\rightsquigarrow$ proba. of decomposition drops by factor $q^{(\alpha-1)(g-2)}$

Double large prime variation

Further improvement [Gaudry-Thomé-Thériault-Diem]:

- Keep relations involving at most two large primes
  $\rightsquigarrow$ proba. of decomposition drops by factor $q^{(\alpha-1)(g-2)}$

- After $\simeq q$ relations are found, possible to eliminate the large primes and obtain $\simeq q^{\alpha}$ relations involving only small primes
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)(g-2)}\, q)$

Double large prime variation

Further improvement [Gaudry-Thomé-Thériault-Diem]:

- Keep relations involving at most two large primes
  $\rightsquigarrow$ proba. of decomposition drops by factor $q^{(\alpha-1)(g-2)}$
- After $\simeq q$ relations are found, possible to eliminate the large primes and obtain $\simeq q^{\alpha}$ relations involving only small primes
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)(g-2)}\, q)$
- Asymptotically optimal choice $\alpha = 1 - 1/g$

Double large prime variation

Further improvement [Gaudry-Thomé-Thériault-Diem]:

- Keep relations involving at most two large primes
  $\rightsquigarrow$ proba. of decomposition drops by factor $q^{(\alpha-1)(g-2)}$
- After $\simeq q$ relations are found, possible to eliminate the large primes and obtain $\simeq q^{\alpha}$ relations involving only small primes
  $\rightsquigarrow$ relation search in $\tilde{O}(q^{(1-\alpha)(g-2)}\, q)$
- Asymptotically optimal choice $\alpha = 1 - 1/g$

Total complexity in $\tilde{O}(q^{2-2/g})$
$\rightsquigarrow$ better than generic attacks as soon as $g \geq 3$

Double large prime variation

How to deduce "full" relations from 2LP relations?

Construct a graph of relations

- vertices: large primes + special vertex "1"
- relation involving 2 LP $\rightsquigarrow$ edge between corresponding vertices
- relation involving 1 LP $\rightsquigarrow$ edge between corresponding vertex and 1

Double large prime variation

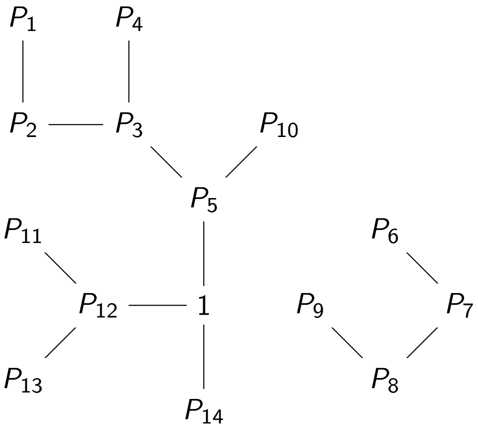
How to deduce "full" relations from 2LP relations?

Construct a graph of relations

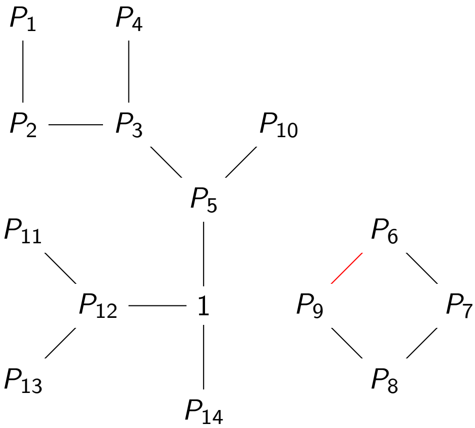
- vertices: large primes + special vertex "1"
- relation involving 2 LP $\rightsquigarrow$ edge between corresponding vertices
- relation involving 1 LP $\rightsquigarrow$ edge between corresponding vertex and 1

Idea: cycles of relations allow to eliminate LP

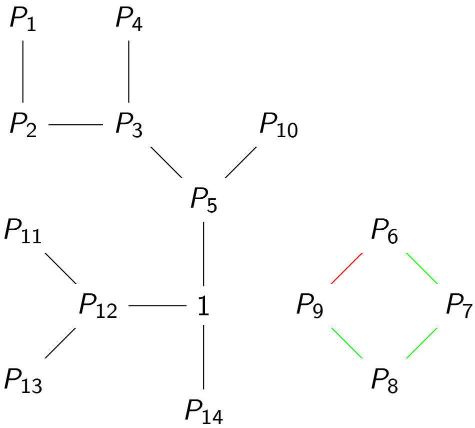
Elimination of large primes



Elimination of large primes

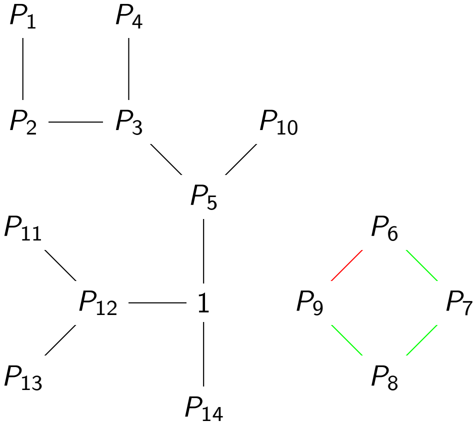


Elimination of large primes



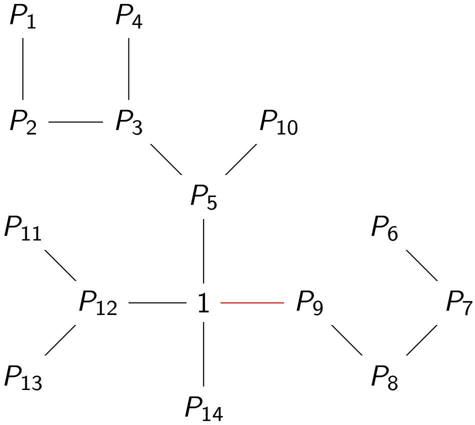
$$\begin{array}{cccc} P_6 & P_7 & P_8 & P_9 \\ \end{array}$$
$$\begin{pmatrix} * & * & 0 & 0 \\ 0 & * & * & 0 \\ 0 & 0 & * & * \\ * & 0 & 0 & * \end{pmatrix}$$

Elimination of large primes



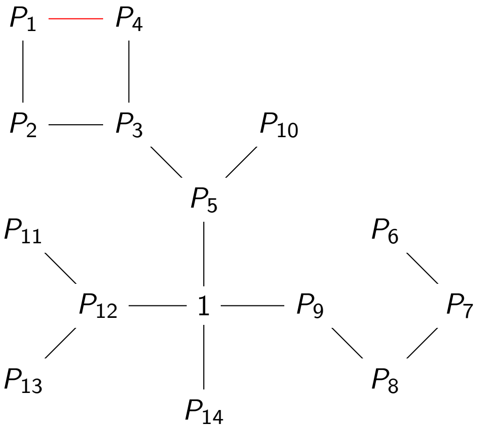
$$\begin{array}{c}
\begin{array}{cccc} P_6 & P_7 & P_8 & P_9 \end{array} \\
\begin{pmatrix} * & * & 0 & 0 \\ 0 & * & * & 0 \\ 0 & 0 & * & * \\ \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{?} \end{pmatrix}
\end{array}$$

Elimination of large primes

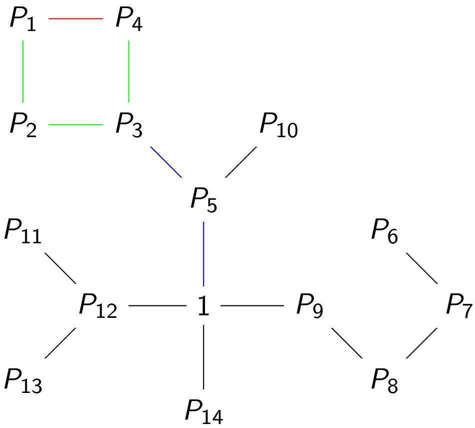


$$
\begin{array}{cccc}
P_6 & P_7 & P_8 & P_9 \\
\end{array}
$$
$$
\begin{pmatrix}
* & * & 0 & 0 \\
0 & * & * & 0 \\
0 & 0 & * & * \\
\color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{2}
\end{pmatrix}
$$

Elimination of large primes

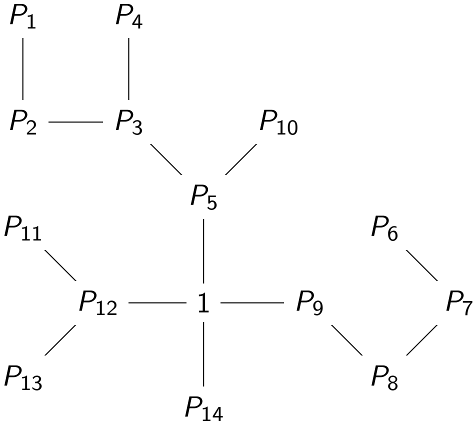


Elimination of large primes



$$\begin{array}{c} \begin{array}{ccccc} P_1 & P_2 & P_3 & P_4 & P_5 \end{array} \\ \begin{pmatrix} * & * & 0 & 0 & 0 \\ 0 & * & * & 0 & 0 \\ 0 & 0 & * & * & 0 \\ * & 0 & 0 & * & 0 \\ 0 & 0 & * & 0 & * \\ 0 & 0 & 0 & 0 & * \end{pmatrix} \end{array}$$

Elimination of large primes



$$\begin{array}{ccccc} P_1 & P_2 & P_3 & P_4 & P_5 \end{array}$$
$$\begin{pmatrix} * & * & 0 & 0 & 0 \\ 0 & * & * & 0 & 0 \\ 0 & 0 & * & * & 0 \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{0} \end{pmatrix}$$

Double large prime variation

How to deduce “full” relations from 2LP relations?

Construct a graph of relations

- vertices: large primes + special vertex “1”
- relation involving 2 LP $\rightsquigarrow$ edge between corresponding vertices
- relation involving 1 LP $\rightsquigarrow$ edge between corresponding vertex and 1

Idea: cycles of relations allow to eliminate LP

Random graph heuristics:

- $\#\{\text{edges}\} \ll \#\{\text{vertices}\} \rightsquigarrow$ no cycle expected
- $\#\{\text{edges}\} \simeq \#\{\text{vertices}\} \rightsquigarrow$ giant connected component of diameter in $O(\log \#\{\text{vertices}\})$
- $\#\{\text{edges}\} > \#\{\text{vertices}\} \rightsquigarrow$ most new edges give new cycles

Summary

Asymptotic comparison on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$

Genus	2	3	4	5
Generic methods	q	$q^{3/2}$	q^2	$q^{5/2}$
Classical index calculus	q^2	q^2	q^2	q^2
Harley	$q^{4/3}$	$q^{3/2}$	$q^{8/5}$	$q^{5/3}$
1LP	$q^{6/5}$	$q^{10/7}$	$q^{14/9}$	$q^{18/11}$
2LP	q	$q^{4/3}$	$q^{3/2}$	$q^{8/5}$

Summary

Asymptotic comparison on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$

Genus	2	3	4	5
Generic methods	q	$q^{1.5}$	q^2	$q^{2.5}$
Classical index calculus	q^2	q^2	q^2	q^2
Harley	$q^{1.33}$	$q^{1.5}$	$q^{1.6}$	$q^{1.67}$
1LP	$q^{1.2}$	$q^{1.43}$	$q^{1.56}$	$q^{1.64}$
2LP	q	$q^{1.33}$	$q^{1.5}$	$q^{1.6}$

Subsection 2

Elliptic curves defined over extension fields

Index calculus over elliptic curves

How to define smooth elements on an elliptic curve ?

- no known equivalent on $E(\mathbb{F}_p)$, p prime
- breakthrough on $E(\mathbb{F}_{p^n})$ by Gaudry in 2004, using ideas of Semaev

Index calculus over elliptic curves

How to define smooth elements on an elliptic curve ?

- no known equivalent on $E(\mathbb{F}_p)$, p prime
- breakthrough on $E(\mathbb{F}_{p^n})$ by Gaudry in 2004, using ideas of Semaev

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

Main idea [Semaev '04]:

- consider decompositions in a fixed number of points of $\mathcal{F}$

$$R = [a]P + [b]Q = P_1 + \ldots + P_n$$

- convert this into a polynomial system by using the $(n+1)$-th summation polynomial:

$$f_{n+1}(x_R, x_{P_1}, \ldots, x_{P_n}) = 0$$
$$\Leftrightarrow \exists \epsilon_1, \ldots, \epsilon_n \in \{1, -1\}, R = \epsilon_1 P_1 + \cdots + \epsilon_n P_n$$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $$f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$
- for $m \geq 4$, determine f_m by induction

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$
- for $m \geq 4$, determine f_m by induction

$$\begin{aligned} & P_1 \pm P_2 \pm \ldots \pm P_m = \mathcal{O} \\ \Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \exists R \in E(\overline{K}), \begin{cases} P_1 \pm \ldots \pm P_j + R = \mathcal{O} \\ R \mp P_{j+1} \mp \ldots \mp P_m = \mathcal{O} \end{cases} \end{aligned}$$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$
- for $m \geq 4$, determine f_m by induction

$$\begin{aligned}
& P_1 \pm P_2 \pm \ldots \pm P_m = \mathcal{O} \\
\Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \exists R \in E(\overline{K}), \begin{cases} P_1 \pm \ldots \pm P_j + R = \mathcal{O} \\ R \mp P_{j+1} \mp \ldots \mp P_m = \mathcal{O} \end{cases} \\
\Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \quad f_{j+1}(x_{P_1}, \ldots, x_{P_j}, X) \\
& \text{and } f_{m-j+1}(X, x_{P_{j+1}}, \ldots, x_{P_m}) \text{ have a common root}
\end{aligned}$$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$
- for $m \geq 4$, determine f_m by induction

$$
\begin{aligned}
& P_1 \pm P_2 \pm \ldots \pm P_m = \mathcal{O} \\
\Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \exists R \in E(\overline{K}), \begin{cases} P_1 \pm \ldots \pm P_j + R = \mathcal{O} \\ R \mp P_{j+1} \mp \ldots \mp P_m = \mathcal{O} \end{cases} \\
\Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \quad f_{j+1}(x_{P_1}, \ldots, x_{P_j}, X) \\
& \text{ and } f_{m-j+1}(X, x_{P_{j+1}}, \ldots, x_{P_m}) \text{ have a common root} \\
\Leftrightarrow \quad & \forall j \in [\![1; m-3]\!], \quad \mathrm{Res}_X \left(f_{j+1}(x_{P_1}, \ldots, x_{P_j}, X)\,,\right. \\
& \qquad \left. f_{m-j+1}(X, x_{P_{j+1}}, \ldots, x_{P_m})\right) = 0
\end{aligned}
$$

Computation of Semaev's summation polynomials

Let $E : y^2 = x^3 + ax + b$

- $f_2(X_1, X_2) = X_1 - X_2$
- $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 + (X_1X_2 - a)^2 - 4b(X_1 + X_2)$
- for $m \geq 4$, determine f_m by induction

$$f_m(X_1, X_2, \ldots, X_m) = \mathrm{Res}_X\left(f_{m-j}(X_1, X_2, \ldots, X_{m-j-1}, X), f_{j+2}(X_{m-j}, \ldots, X_m, X)\right)$$

$\deg_{X_i} f_m = 2^{m-2} \Rightarrow$ only computable for small values of m

Digression: Weil restriction of scalars

L/K field extension, $[L:K] = d < \infty$

V n-dimensional algebraic variety defined over L

Assume for simplicity V affine, given by equations

$$f_1(x_1,\dots,x_r) = \cdots = f_s(x_1,\dots,x_r) = 0$$

Digression: Weil restriction of scalars

L/K field extension, $[L:K] = d < \infty$

V n-dimensional algebraic variety defined over L

Assume for simplicity V affine, given by equations

$$f_1(x_1,\ldots,x_r) = \cdots = f_s(x_1,\ldots,x_r) = 0$$

Weil restriction

$$W_{L/K}(V) = \mathbb{V}(f_{11},\ldots,f_{sd}) \quad nd\text{-dim. variety over } K$$

- $\{u_1,\ldots,u_d\}$ K-linear basis of L and $x_i = \sum_j x_{ij}u_j$
- $f_k(x_1,\ldots,x_r) = \sum_j f_{kj}(x_{11},\ldots,x_{rd})u_j$, $f_{kj} \in K[x_{11},\ldots,x_{rd}]$

Digression: Weil restriction of scalars

L/K field extension, $[L:K] = d < \infty$

V n-dimensional algebraic variety defined over L

Assume for simplicity V affine, given by equations

$$f_1(x_1, \ldots, x_r) = \cdots = f_s(x_1, \ldots, x_r) = 0$$

Weil restriction

$$W_{L/K}(V) = \mathbb{V}(f_{11}, \ldots, f_{sd}) \quad nd\text{-dim. variety over } K$$

- $\{u_1, \ldots, u_d\}$ K-linear basis of L and $x_i = \sum_j x_{ij} u_j$
- $f_k(x_1, \ldots, x_r) = \sum_j f_{kj}(x_{11}, \ldots, x_{rd}) u_j$, $f_{kj} \in K[x_{11}, \ldots, x_{rd}]$

Examples:

- $W_{\mathbb{C}/\mathbb{R}}(\mathbb{C}) = \mathbb{R}^2$
- $W_{\mathbb{C}/\mathbb{R}}(\mathbb{P}^1(\mathbb{C})) = \mathbb{S}^2$

Properties of Weil restriction

Let $\mathcal{W} = W_{L/K}(V)$

- As sets, $V(L) = \mathcal{W}(K)$. But topology is finer on the latter
- V abelian variety $\Rightarrow \mathcal{W}$ abelian variety
- If L/K Galois, $\mathcal{W}(L) \simeq \prod_{\tau \in \mathrm{Gal}(L/K)} V^{\tau}(L)$
  $\rightsquigarrow \exists$ L-morphism $pr : \mathcal{W}(L) \to V(L)$
- Universal property:
  V' variety over K, $\varphi : V'(L) \to V(L)$ L-morphism

$$\begin{tikzcd} V'_{|K} \arrow[r, "\varphi"] \arrow[dr, dashed, "\psi"'] & V_{|L} \\ & \mathcal{W}_{|K} \arrow[u, "pr"'] \end{tikzcd}$$

Index calculus over elliptic curves

Convenient factor base on $E(\mathbb{F}_{q^n})$ [Gaudry 04]

- Natural factor base: $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$, $\#\mathcal{F} \simeq q$
- Scalar restriction: decompose along a $\mathbb{F}_q$-linear basis of $\mathbb{F}_{q^n}$

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

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

Index calculus over elliptic curves

Convenient factor base on $E(\mathbb{F}_{q^n})$ [Gaudry 04]

- Natural factor base: $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$, $\#\mathcal{F} \simeq q$
- Scalar restriction: 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 $\mathbb{F}_q$

$\rightsquigarrow$ requires efficient techniques to solve multivariate polynomial system over finite fields (e.g. Gröbner basis)

Example over $E(\mathbb{F}_{101^3})$

- $\mathbb{F}_{101^3} \simeq \mathbb{F}_{101}[t]/(t^3 + t + 1)$
  $E : y^2 = x^3 + (44 + 52t + 60t^2)x + (58 + 87t + 74t^2)$, $\#E = 1029583$,

  base point: $P \left| \begin{array}{l} 25+58t+23t^2 \\ 96+69t+37t^2 \end{array} \right.$ challenge point: $Q \left| \begin{array}{l} 89+78t+52t^2 \\ 14+79t+71t^2 \end{array} \right.$

Example over $E(\mathbb{F}_{101^3})$

- $\mathbb{F}_{101^3} \simeq \mathbb{F}_{101}[t]/(t^3+t+1)$
  $E : y^2 = x^3 + (44+52t+60t^2)x + (58+87t+74t^2)$, $\#E = 1029583$,

  base point: $P \left| \begin{array}{l} 25+58t+23t^2 \\ 96+69t+37t^2 \end{array} \right.$ challenge point: $Q \left| \begin{array}{l} 89+78t+52t^2 \\ 14+79t+71t^2 \end{array} \right.$

- random combination of P and Q:

$$R = [658403]P + [919894]Q = \left| \begin{array}{l} 44+57t+55t^2 \\ 8+11t+73t^2 \end{array} \right.$$

Example over $E(\mathbb{F}_{101^3})$

- $\mathbb{F}_{101^3} \simeq \mathbb{F}_{101}[t]/(t^3+t+1)$
  $E : y^2 = x^3 + (44+52t+60t^2)x + (58+87t+74t^2)$, $\#E = 1029583$,

  base point: $P \left| \begin{array}{l} 25+58t+23t^2 \\ 96+69t+37t^2 \end{array} \right.$ challenge point: $Q \left| \begin{array}{l} 89+78t+52t^2 \\ 14+79t+71t^2 \end{array} \right.$

- random combination of P and Q:
  $$R = [658403]P + [919894]Q = \left| \begin{array}{l} 44+57t+55t^2 \\ 8+11t+73t^2 \end{array} \right.$$

- compute 4-th summation polynomial with resultant:
  $f_4(X_1, X_2, X_3, X_4) = Res_X\big(f_3(X_1, X_2, X), f_3(X_3, X_4, X)\big)$

Example over $E(\mathbb{F}_{101^3})$

- $\mathbb{F}_{101^3} \simeq \mathbb{F}_{101}[t]/(t^3+t+1)$
  $E : y^2 = x^3 + (44+52t+60t^2)x + (58+87t+74t^2)$, $\#E = 1029583$,

  base point: $P \left| \begin{array}{l} 25+58t+23t^2 \\ 96+69t+37t^2 \end{array} \right.$ challenge point: $Q \left| \begin{array}{l} 89+78t+52t^2 \\ 14+79t+71t^2 \end{array} \right.$

- random combination of P and Q:

$$R = [658403]P + [919894]Q = \left| \begin{array}{l} 44+57t+55t^2 \\ 8+11t+73t^2 \end{array} \right.$$

- compute 4-th summation polynomial with resultant:
  $f_4(X_1, X_2, X_3, X_4) = Res_X\big(f_3(X_1, X_2, X), f_3(X_3, X_4, X)\big)$

- after partial symmetrization, solve in $s_1, s_2, s_3 \in \mathbb{F}_{101}$

$$\begin{array}{l} f_4(s_1,s_2,s_3,x_R) = x_R^4 s_2^4 + 93 x_R^4 s_1 s_2^2 s_3 \\ \quad +16 x_R^4 s_1^2 s_3^2 + \cdots + 94 b^3 s_3 = 0 \end{array} \Leftrightarrow \begin{cases} 28s_1^4 + 94s_1^3 s_2 + \cdots + 4s_3 + 69 = 0 \\ 49s_1^4 + 72s_1^3 s_2 + \cdots + 14s_3 + 100 = 0 \\ 32s_1^4 + 97s_1^3 s_2 + \cdots + 50s_3 + 8 = 0 \end{cases}$$

Example over $E(\mathbb{F}_{101^3})$

$$\mathrm{I}(\mathcal{S}_R) = \langle 28s_1^4 + 94s_1^3s_2 + \cdots + 4s_3 + 69, 49s_1^4 + 72s_1^3s_2 + \cdots + 14s_3 + 100, \\ 32s_1^4 + 97s_1^3s_2 + \cdots + 50s_3 + 8\rangle$$

- Gröbner basis of $\mathrm{I}(\mathcal{S}_R)$ for $lex_{s_1>s_2>s_3}$:

$$G = \{s_1 + 33s_3^{63} + 23s_3^{62} + \cdots + 95, s_2 + 80s_3^{63} + 79s_3^{62} + \cdots + 45, \\ s_3^{64} + 36s_3^{63} + 80s_3^{62} + \cdots + 56\}$$

Example over $E(\mathbb{F}_{101^3})$

$$\mathrm{I}(\mathcal{S}_R) = \langle 28s_1^4 + 94s_1^3s_2 + \cdots + 4s_3 + 69, 49s_1^4 + 72s_1^3s_2 + \cdots + 14s_3 + 100, \\ 32s_1^4 + 97s_1^3s_2 + \cdots + 50s_3 + 8\rangle$$

- Gröbner basis of $\mathrm{I}(\mathcal{S}_R)$ for $lex_{s_1>s_2>s_3}$:

$$G = \{s_1 + 33s_3^{63} + 23s_3^{62} + \cdots + 95, s_2 + 80s_3^{63} + 79s_3^{62} + \cdots + 45, \\ s_3^{64} + 36s_3^{63} + 80s_3^{62} + \cdots + 56\}$$

- $V\big(\mathrm{I}(\mathcal{S}_R)\big)_{/\mathbb{F}_{101}} = \{(30, 3, 53), (75, 25, 75)\}$
  Roots of $X^3 - s_1X^2 + s_2X - s_3 = 0$ over $\mathbb{F}_{101}$?

Example over $E(\mathbb{F}_{101^3})$

$$\mathrm{I}(\mathcal{S}_R) = \langle 28s_1^4 + 94s_1^3s_2 + \cdots + 4s_3 + 69, 49s_1^4 + 72s_1^3s_2 + \cdots + 14s_3 + 100, 32s_1^4 + 97s_1^3s_2 + \cdots + 50s_3 + 8\rangle$$

- Gröbner basis of $\mathrm{I}(\mathcal{S}_R)$ for $lex_{s_1>s_2>s_3}$:

$$G = \{s_1 + 33s_3^{63} + 23s_3^{62} + \cdots + 95, s_2 + 80s_3^{63} + 79s_3^{62} + \cdots + 45, s_3^{64} + 36s_3^{63} + 80s_3^{62} + \cdots + 56\}$$

- $V\big(\mathrm{I}(\mathcal{S}_R)\big)_{/\mathbb{F}_{101}} = \{(30, 3, 53), (75, 25, 75)\}$
  Roots of $X^3 - s_1X^2 + s_2X - s_3 = 0$ over $\mathbb{F}_{101}$?
  - $X^3 - 30X^2 + 3X - 53$ irreducible over $\mathbb{F}_{101}[X]$

Example over $E(\mathbb{F}_{101^3})$

$$\mathrm{I}(\mathcal{S}_R) = \langle 28s_1^4 + 94s_1^3s_2 + \cdots + 4s_3 + 69, 49s_1^4 + 72s_1^3s_2 + \cdots + 14s_3 + 100, \\ 32s_1^4 + 97s_1^3s_2 + \cdots + 50s_3 + 8\rangle$$

- Gröbner basis of $\mathrm{I}(\mathcal{S}_R)$ for $lex_{s_1>s_2>s_3}$:

$$G = \{s_1 + 33s_3^{63} + 23s_3^{62} + \cdots + 95, s_2 + 80s_3^{63} + 79s_3^{62} + \cdots + 45, \\ s_3^{64} + 36s_3^{63} + 80s_3^{62} + \cdots + 56\}$$

- $V\big(\mathrm{I}(\mathcal{S}_R)\big)_{/\mathbb{F}_{101}} = \{(30, 3, 53), (75, 25, 75)\}$
  Roots of $X^3 - s_1X^2 + s_2X - s_3 = 0$ over $\mathbb{F}_{101}$?
  * $X^3 - 30X^2 + 3X - 53$ irreducible over $\mathbb{F}_{101}[X]$
  * $X^3 - 75X^2 + 25X - 75 = (X - 4)(X - 7)(X - 64)$

  $\Rightarrow P_1 \left| \begin{array}{l} 4 \\ {\scriptstyle 27+34t+91t^2} \end{array} \right. P_2 \left| \begin{array}{l} 7 \\ {\scriptstyle 58+95t+91t^2} \end{array} \right. P_3 \left| \begin{array}{l} 64 \\ {\scriptstyle 76+54t+18t^2} \end{array} \right.$ and $P_1 - P_2 + P_3 = R$

Example over $E(\mathbb{F}_{101^3})$

$$\mathrm{I}(\mathcal{S}_R) = \langle 28s_1^4 + 94s_1^3s_2 + \cdots + 4s_3 + 69, 49s_1^4 + 72s_1^3s_2 + \cdots + 14s_3 + 100, \\ 32s_1^4 + 97s_1^3s_2 + \cdots + 50s_3 + 8\rangle$$

- Gröbner basis of $\mathrm{I}(\mathcal{S}_R)$ for $lex_{s_1>s_2>s_3}$:

$$G = \{s_1 + 33s_3^{63} + 23s_3^{62} + \cdots + 95, s_2 + 80s_3^{63} + 79s_3^{62} + \cdots + 45, \\ s_3^{64} + 36s_3^{63} + 80s_3^{62} + \cdots + 56\}$$

- $V\big(\mathrm{I}(\mathcal{S}_R)\big)_{/\mathbb{F}_{101}} = \{(30,3,53),(75,25,75)\}$
  Roots of $X^3 - s_1X^2 + s_2X - s_3 = 0$ over $\mathbb{F}_{101}$?
  - $*$ $X^3 - 30X^2 + 3X - 53$ irreducible over $\mathbb{F}_{101}[X]$
  - $*$ $X^3 - 75X^2 + 25X - 75 = (X-4)(X-7)(X-64)$

  $\Rightarrow P_1 \left| \begin{matrix} 4 \\ 27+34t+91t^2 \end{matrix} \right. \quad P_2 \left| \begin{matrix} 7 \\ 58+95t+91t^2 \end{matrix} \right. \quad P_3 \left| \begin{matrix} 64 \\ 76+54t+18t^2 \end{matrix} \right.$ and $P_1 - P_2 + P_3 = R$

- Number of relations needed: $\#\mathcal{F}_{/\sim} = 54 \Rightarrow 55$

- Linear algebra $\rightarrow x = 771080$

Complexity analysis

- size of factor base $\#\mathcal{F} \simeq q$
  $\rightsquigarrow$ linear algebra in $\tilde{O}(nq^2)$
- proba. of decomposition $\simeq \dfrac{\#(\mathcal{F}^n/\mathfrak{S}_n)}{\#E(\mathbb{F}_{q^n})} \simeq \dfrac{1}{n!}$
  $\rightsquigarrow$ need $O(n!q)$ decomposition tests
- for **fixed** n and $q \to \infty$, decomposition cost is in $\tilde{O}(1)$

Complexity analysis

- size of factor base $\#\mathcal{F} \simeq q$
  $\rightsquigarrow$ linear algebra in $\tilde{O}(nq^2)$
- proba. of decomposition $\simeq \dfrac{\#(\mathcal{F}^n/\mathfrak{S}_n)}{\#E(\mathbb{F}_{q^n})} \simeq \dfrac{1}{n!}$
  $\rightsquigarrow$ need $O(n!q)$ decomposition tests
- for **fixed** n and $q \to \infty$, decomposition cost is in $\tilde{O}(1)$

$\Rightarrow$ Total cost in $\tilde{O}(q^2)$ (from linear algebra)

Complexity analysis

- size of factor base $\#\mathcal{F} \simeq q$
  $\rightsquigarrow$ linear algebra in $\tilde{O}(nq^2)$
- proba. of decomposition $\simeq \dfrac{\#(\mathcal{F}^n/\mathfrak{S}_n)}{\#E(\mathbb{F}_{q^n})} \simeq \dfrac{1}{n!}$
  $\rightsquigarrow$ need $O(n!q)$ decomposition tests
- for **fixed** n and $q \to \infty$, decomposition cost is in $\tilde{O}(1)$

$\Rightarrow$ Total cost in $\tilde{O}(q^2)$ (from linear algebra)

Rebalance the two steps with 2LP

Asymptotic complexity becomes $\tilde{O}(q^{2-2/n})$

$\rightsquigarrow$ better than generic attacks as soon as $n \geq 3$

In practice...

Decomposition cost

Solving multivariate polynomial systems is **very** expensive
Rough cost estimate is $2^{O(n^2)}$ $\rightsquigarrow$ only feasible for n small

In practice...

Decomposition cost

Solving multivariate polynomial systems is **very** expensive
Rough cost estimate is $2^{O(n^2)} \rightsquigarrow$ only feasible for n small

1. Experimentally:
   - decomposition too hard for $n > 4$
   - generic attacks always faster for "reasonable" group sizes

In practice...

Decomposition cost

Solving multivariate polynomial systems is **very** expensive
Rough cost estimate is $2^{O(n^2)} \rightsquigarrow$ only feasible for n small

1. Experimentally:
    - decomposition too hard for $n > 4$
    - generic attacks always faster for “reasonable” group sizes
2. Theoretically:
   gives a subexponential algorithm when $n = \Theta(\sqrt{\log q})$ [Diem]

Subsection 3

Other applications

Index calculus on small dimension abelian varieties [Gaudry]

- Last algorithm uses that $E(\mathbb{F}_{q^n}) = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)(\mathbb{F}_q)$, n-dimensional abelian variety over $\mathbb{F}_q$
- Specific case of a more general index calculus algorithm for abelian varieties of small dimension

Index calculus on small dimension abelian varieties [Gaudry]

- Last algorithm uses that $E(\mathbb{F}_{q^n}) = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)(\mathbb{F}_q)$, n-dimensional abelian variety over $\mathbb{F}_q$
- Specific case of a more general index calculus algorithm for abelian varieties of small dimension

Let $\mathcal{A}$ dimension d abelian variety defined over $\mathbb{F}_q$

- For fixed d, asymptotic cost of index calculus on $\mathcal{A}(\mathbb{F}_q)$ in $\tilde{O}(q^{2-2/d})$
- Main practical obstacle: using algebraic expression of group law, decomposition tests $\leftrightarrow$ resolution of polynomial systems

Index calculus on small dimension abelian varieties [Gaudry]

- Last algorithm uses that $E(\mathbb{F}_{q^n}) = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)(\mathbb{F}_q)$, n-dimensional abelian variety over $\mathbb{F}_q$
- Specific case of a more general index calculus algorithm for abelian varieties of small dimension

Let $\mathcal{A}$ dimension d abelian variety defined over $\mathbb{F}_q$

- For fixed d, asymptotic cost of index calculus on $\mathcal{A}(\mathbb{F}_q)$ in $\tilde{O}(q^{2-2/d})$
- Main practical obstacle: using algebraic expression of group law, decomposition tests $\leftrightarrow$ resolution of polynomial systems

The hyperelliptic case

Weil restriction of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$: abelian variety of dimension ng.
Nice formulation of the polynomial systems [Nagao]
$\Rightarrow$ feasible for $n = 2$, $g \leq 4$, and $n = 3$, $g = 2$.

Index calculus on small degree plane curves [Diem]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

Index calculus on small degree plane curves [Diem]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

For $\mathcal{C}_{|\mathbb{F}_q}$ of fixed degree d, complexity in $\tilde{O}(q^{2-2/(d-2)})$

- most genus g curves admit a plane model of degree $g+1$
  $\rightsquigarrow$ complexity in $\tilde{O}(q^{2-2/(g-1)})$
- not true for hyperelliptic curves

Index calculus on small degree plane curves [Diem]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

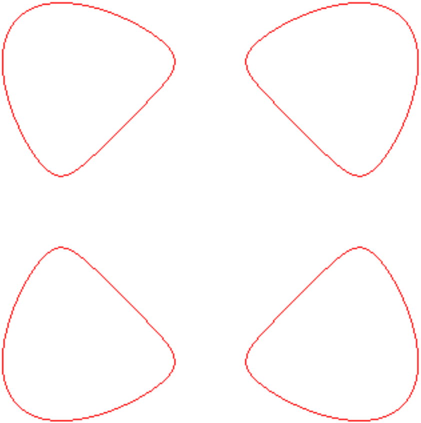
For $\mathcal{C}_{|\mathbb{F}_q}$ of fixed degree d, complexity in $\tilde{O}(q^{2-2/(d-2)})$

- most genus g curves admit a plane model of degree $g+1$
  $\rightsquigarrow$ complexity in $\tilde{O}(q^{2-2/(g-1)})$
- not true for hyperelliptic curves

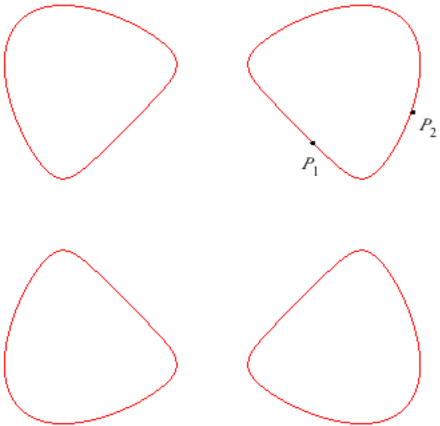
Consequence

Jacobians of non-hyperelliptic curves usually weaker than those of hyperelliptic curves (especially true for $g = 3$).

Idea of index calculus on small degree plane curves

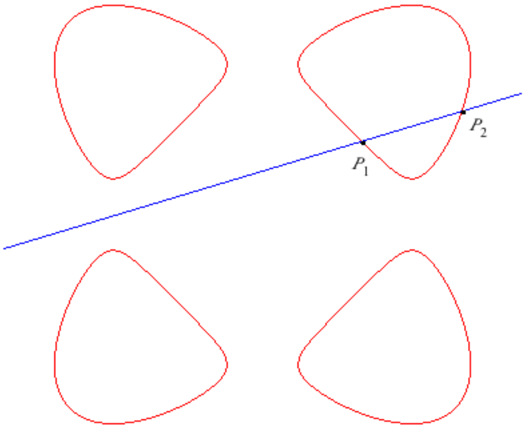


Idea of index calculus on small degree plane curves



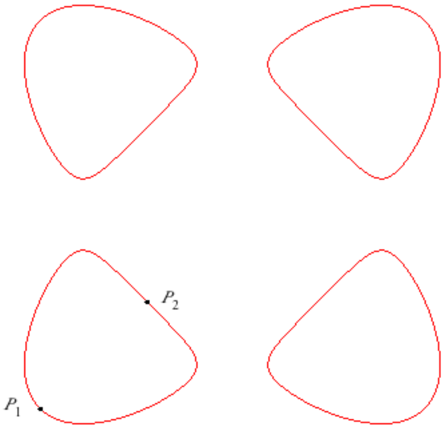
- Take P_1, P_2 small primes

Idea of index calculus on small degree plane curves



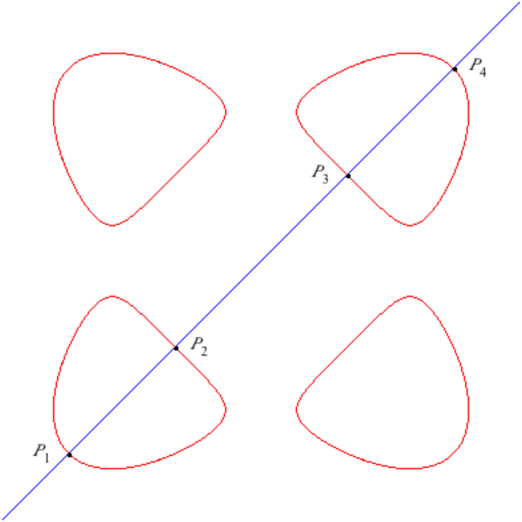
- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Idea of index calculus on small degree plane curves



- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Idea of index calculus on small degree plane curves



- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Section 4

Transfer attacks

Principle of transfer

Transfer maps

G_2: group where DLP is weak
If there exists $\varphi \in \mathrm{Hom}(G_1, G_2)$ one-to-one and **computable**, then DLP is also weak on G_1.

Let $\varphi \in \mathrm{Hom}(G_1, G_2)$, $g, h \in G_1$. If $\mathrm{ord}(\varphi(g)) = \mathrm{ord}(g)$, then

$$h = [x]g \Leftrightarrow \varphi(h) = [x]\varphi(g).$$

Principle of transfer

Transfer maps

G_2: group where DLP is weak
If there exists $\varphi \in \mathrm{Hom}(G_1, G_2)$ one-to-one and **computable**, then DLP is also weak on G_1.

Let $\varphi \in \mathrm{Hom}(G_1, G_2)$, $g, h \in G_1$. If $\mathrm{ord}(\varphi(g)) = \mathrm{ord}(g)$, then

$$h = [x]g \Leftrightarrow \varphi(h) = [x]\varphi(g).$$

Main target groups for $G_1 = E(\mathbb{F}_q)$

Groups with faster algorithms than square-root algorithms:

- $\mathbb{F}_{q^k}^*$
- $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q'})$, q power of q'

Transfer via pairings

Let G_1, G_2 two additive groups of exponent n and G_3 a multiplicative cyclic group of order n.

Definition

A pairing is a map $e : G_1 \times G_2 \to G_3$ which is:

- bilinear: $e([a]g_1, [b]g_2) = e(g_1, g_2)^{ab}$
- non degenerate: $\forall g_1 \in G_1 \setminus \{0\}, \exists g_2 \in G_2, e(g_1, g_2) \neq 1$

Allows to transfer DLP given by $(g, h = [x]g)$ from G_1 to G_3:

- non-degeneracy $\Rightarrow \exists g_2 \in G_2, \mathrm{ord}(g) = \mathrm{ord}(e(g, g_2))$
- transfer map $\varphi = e(., g_2)$ from G_1 to G_3

Pairings on elliptic curves

The Weil pairing

- E elliptic curve defined over $\mathbb{F}_q$
- n integer co-prime to char$(\mathbb{F}_q)$
- $k = k(n, q)$ embedding degree, i.e. smallest integer s.t. $n | (q^k - 1)$

Weil pairing: $w_n : E[n] \times E[n] \to \mu_n \subset \mathbb{F}_{q^k}^*$
computable in $O(\log n)$ operations in $\mathbb{F}_{q^k}$ [Miller]

Pairings on elliptic curves

The Weil pairing

- E elliptic curve defined over $\mathbb{F}_q$
- n integer co-prime to $\mathrm{char}(\mathbb{F}_q)$
- $k = k(n,q)$ embedding degree, i.e. smallest integer s.t. $n|(q^k - 1)$

Weil pairing: $w_n : E[n] \times E[n] \to \mu_n \subset \mathbb{F}_{q^k}^*$
computable in $O(\log n)$ operations in $\mathbb{F}_{q^k}$ [Miller]

Menezes-Okamoto-Vanstone's attack

Transfer + index calculus on $\mathbb{F}_{q^k}^*$ efficient when k small:

- $k \leq 6$ for supersingular curves $\rightsquigarrow$ always vulnerable
- but $k \simeq q$ for random curves $\rightsquigarrow$ most elliptic curves remain safe

Pairings on elliptic curves

The Weil pairing

- E elliptic curve defined over $\mathbb{F}_q$
- n integer co-prime to $\mathrm{char}(\mathbb{F}_q)$
- $k = k(n, q)$ embedding degree, i.e. smallest integer s.t. $n | (q^k - 1)$

Weil pairing: $w_n : E[n] \times E[n] \to \mu_n \subset \mathbb{F}_{q^k}^*$
computable in $O(\log n)$ operations in $\mathbb{F}_{q^k}$ [Miller]

Menezes-Okamoto-Vanstone's attack

Transfer + index calculus on $\mathbb{F}_{q^k}^*$ efficient when k small:

- $k \leq 6$ for supersingular curves $\rightsquigarrow$ always vulnerable
- but $k \simeq q$ for random curves $\rightsquigarrow$ most elliptic curves remain safe

Other pairings available [Frey-Rück], but same condition on the embedding degree...

Anomalous curves

Elliptic curves over q-adic fields

$\mathcal{E}$ elliptic curve defined over $\mathbb{Q}_q$, $q = p^n$. Reduction mod p map

$$\psi : \mathcal{E}(\mathbb{Q}_q) \to E(\mathbb{F}_q)$$

where E (possibly singular) elliptic curve defined over $\mathbb{F}_q$.

Fact: DLP on $\mathcal{E}_1(\mathbb{Q}_q) = \ker \psi$ is easy

Anomalous curves

Elliptic curves over q-adic fields

$\mathcal{E}$ elliptic curve defined over $\mathbb{Q}_q$, $q = p^n$. Reduction mod p map

$$\psi : \mathcal{E}(\mathbb{Q}_q) \to E(\mathbb{F}_q)$$

where E (possibly singular) elliptic curve defined over $\mathbb{F}_q$.

Fact: DLP on $\mathcal{E}_1(\mathbb{Q}_q) = \ker \psi$ is easy

Several attempts to transfer the DLP from $E(\mathbb{F}_q)$ to $\mathcal{E}_1(\mathbb{Q}_q)$
Only success so far: when DLP defined on an order p subgroup of E
$\rightsquigarrow$ resolution in polynomial complexity

Anomalous curves

Elliptic curves over q-adic fields

$\mathcal{E}$ elliptic curve defined over $\mathbb{Q}_q$, $q = p^n$. Reduction mod p map

$$\psi : \mathcal{E}(\mathbb{Q}_q) \to E(\mathbb{F}_q)$$

where E (possibly singular) elliptic curve defined over $\mathbb{F}_q$.

Fact: DLP on $\mathcal{E}_1(\mathbb{Q}_q) = \ker \psi$ is easy

Several attempts to transfer the DLP from $E(\mathbb{F}_q)$ to $\mathcal{E}_1(\mathbb{Q}_q)$
Only success so far: when DLP defined on an order p subgroup of E
$\rightsquigarrow$ resolution in polynomial complexity

Vulnerable curves satisfy $p | \#E(\mathbb{F}_q)$ (anomalous curves)
$\rightsquigarrow$ very few of them, can be easily avoided

Weil descent: geometric approach [Frey]

$\mathcal{A}_{|\mathbb{F}_q}$: abelian variety, e.g. Weil restriction of $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$.
Possible DLP pull-back from $\mathcal{A}$ to $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$ for any curve $\mathcal{C}' \subset \mathcal{A}$

$$\mathcal{C}' \hookrightarrow \mathcal{A}$$

Weil descent: geometric approach [Frey]

$\mathcal{A}_{|\mathbb{F}_q}$: abelian variety, e.g. Weil restriction of $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$.
Possible DLP pull-back from $\mathcal{A}$ to $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$ for any curve $\mathcal{C}' \subset \mathcal{A}$

$$\begin{tikzcd}
\mathrm{Jac}_{\mathcal{C}'} \arrow[d] \arrow[dr, dotted] & \\
\mathcal{C}'^{(g)} \arrow[r] & \mathcal{A} \\
(P_1, \ldots, P_g) \arrow[r, mapsto] & P_1 + \cdots + P_g
\end{tikzcd}$$

Weil descent: geometric approach [Frey]

$\mathcal{A}_{|\mathbb{F}_q}$: abelian variety, e.g. Weil restriction of $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$.
Possible DLP pull-back from $\mathcal{A}$ to $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$ for any curve $\mathcal{C}' \subset \mathcal{A}$

$$\begin{tikzcd} \mathrm{Jac}_{\mathcal{C}'} \arrow[d] \arrow[dr, dotted] & \\ \mathcal{C}'^{(g)} \arrow[r] & \mathcal{A} \end{tikzcd}$$

$$(P_1, \ldots, P_g) \longmapsto P_1 + \cdots + P_g$$

Difficulties

- find convenient $\mathcal{C}'$ with small genus
- computation of preimages $\leftrightarrow$ decompositions into sum of points of $\mathcal{C}'$ $\leftrightarrow$ resolutions of multivariate polynomial systems

Weil descent: Cover attacks

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Existence of a **cover map** $\pi : \mathcal{C}' \to \mathcal{C}$, where $\mathcal{C}'$ defined over $\mathbb{F}_q$

$\Rightarrow$ "conorm-norm" homomorphism between $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ and $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$

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

Weil descent: Cover attacks

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Existence of a **cover map** $\pi : \mathcal{C}' \to \mathcal{C}$, where $\mathcal{C}'$ defined over $\mathbb{F}_q$

$\Rightarrow$ "conorm-norm" homomorphism between $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ and $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$

$$
\begin{array}{ccccc}
\mathcal{C}' & \quad & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q^n}) & \xrightarrow{\mathrm{tr}} & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q) \\
\downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \pi^*} & \nearrow & \\
\mathcal{C} & & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) & &
\end{array}
$$

- conorm-norm map efficiently computable if $\deg \pi$ not too large
- transfer the DLP from $G \subset \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$
  $\rightsquigarrow$ need $\mathcal{C}'$ with small genus
- want $\ker(\mathrm{tr} \circ \pi^*) \cap G = \{\mathcal{O}_{\mathcal{C}}\}$ ($\Rightarrow g_{\mathcal{C}'} \geq n g_{\mathcal{C}}$)

Weil descent: Cover attacks

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Existence of a **cover map** $\pi : \mathcal{C}' \to \mathcal{C}$, where $\mathcal{C}'$ defined over $\mathbb{F}_q$

$\Rightarrow$ "conorm-norm" homomorphism between $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ and $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$

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

- conorm-norm map efficiently computable if $\deg \pi$ not too large
- transfer the DLP from $G \subset \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q)$
  $\rightsquigarrow$ need $\mathcal{C}'$ with small genus
- want $\ker(\mathrm{tr} \circ \pi^*) \cap G = \{\mathcal{O}_{\mathcal{C}}\}$ $(\Rightarrow g_{\mathcal{C}'} \geq n g_{\mathcal{C}})$

Difficulty: how to find such a curve $\mathcal{C}'$?

Transfer via isogenies

Reminders

Non constant rational map $\phi : E_1 \to E_2$ **isogeny** if $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$

- an isogeny is a group morphism
- existence of a dual isogeny $\hat{\phi} : E_2 \to E_1$
  $\rightsquigarrow$ "being isogenous" is an equivalence relation
- E_1 and E_2 are isogenous iff $\#E_1 = \#E_2$

Hasse bound: $\Theta(\sqrt{q})$ isogeny classes
$\rightsquigarrow$ on average, $O(\sqrt{q})$ curves in each isogeny class

Transfer via isogenies

Reminders

Non constant rational map $\phi : E_1 \to E_2$ **isogeny** if $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$

- an isogeny is a group morphism
- existence of a dual isogeny $\hat{\phi} : E_2 \to E_1$
  $\rightsquigarrow$ "being isogenous" is an equivalence relation
- E_1 and E_2 are isogenous iff $\#E_1 = \#E_2$

Hasse bound: $\Theta(\sqrt{q})$ isogeny classes
$\rightsquigarrow$ on average, $O(\sqrt{q})$ curves in each isogeny class

Motivation

E_1, E_2 isogenous and DLP weak on $E_2 \Rightarrow$ DLP weak on E_1
$\rightsquigarrow$ not useful for anomalous or small embedding degree curves, but may be interesting to reach curves vulnerable to Weil descent attacks

Isogeny walk [Galbraith-Hess-Smart]

Strategy 1: random walk of small degree isogenies starting from E_1, until a weak curve E_2 is found

- best approach when cardinality of weak curves is large
- polynomial complexity for each step in most cases

Strategy 2: search all weak curves until one with $\#E_1 = \#E_2$ is found, then compute isogeny from E_1 to E_2

- need to compute cardinality of weak curves (polynomial complexity)
- cost of finding the isogeny in $\tilde{O}(q^{1/4})$ in most cases

More isogenies

Isogeny of abelian varieties

More generally, rational map $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ isogeny if ϕ surjective with finite fibers and $\phi(\mathcal{O}_1) = \mathcal{O}_2$
$\to$ still a group morphism

More isogenies

Isogeny of abelian varieties

More generally, rational map $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ isogeny if ϕ surjective with finite fibers and $\phi(\mathcal{O}_1) = \mathcal{O}_2$
$\to$ still a group morphism

Index calculus usually more efficient for Jacobians in the non-hyperelliptic case than in the hyperelliptic case (for fixed genus)

Idea [Smith]

Use isogenies to transfer DLP from $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$
Main application: genus 3 case $\rightsquigarrow$ complexity from $\tilde{O}(q^{4/3})$ down to $\tilde{O}(q)$ if successful.

Section 5

Gaudry-Hess-Smart technique

Geometric background

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Goal of cover attack

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\pi : \mathcal{C}' \to \mathcal{C}$ morphism defined over $\mathbb{F}_{q^n}$

$$\Updownarrow$$

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\psi : \mathcal{C}' \to \mathcal{W}$ morphism defined over $\mathbb{F}_q$, where $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$ is the Weil restriction of $\mathcal{C}$

Geometric background

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Goal of cover attack

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\pi : \mathcal{C}' \to \mathcal{C}$ morphism defined over $\mathbb{F}_{q^n}$

$$\Updownarrow$$

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\psi : \mathcal{C}' \to \mathcal{W}$ morphism defined over $\mathbb{F}_q$, where $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$ is the Weil restriction of $\mathcal{C}$

Idea: to have $\mathcal{C}'$ of small genus, try an equation of small degree
$\rightsquigarrow$ intersect $\mathcal{W}$ by hyperplanes

Geometric background

$\mathcal{C}$ algebraic curve defined over $\mathbb{F}_{q^n}$

Goal of cover attack

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\pi : \mathcal{C}' \to \mathcal{C}$ morphism defined over $\mathbb{F}_{q^n}$

$$\Updownarrow$$

Find $\mathcal{C}'$ defined over $\mathbb{F}_q$ and $\psi : \mathcal{C}' \to \mathcal{W}$ morphism defined over $\mathbb{F}_q$, where $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$ is the Weil restriction of $\mathcal{C}$

Idea: to have $\mathcal{C}'$ of small genus, try an equation of small degree
$\rightsquigarrow$ intersect $\mathcal{W}$ by hyperplanes

Conceptually nicer formulation in terms of function fields [GHS]

Function fields

Reminders

- Function field over $F/\mathbb{F}_q$: extension of transcendence degree 1
- Field of constants of F is $F \cap \overline{\mathbb{F}_q}$
- Category equivalence between curves and function fields

$$\left\{ \begin{array}{c} \text{Objects:} \\ \text{smooth curves defined over } \mathbb{F}_q \\ \text{Maps:} \\ \text{non constant morphisms} \\ \text{defined over } \mathbb{F}_q \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{Objects:} \\ \text{function fields } F/\mathbb{F}_q \\ \text{with constant field } \mathbb{F}_q \\ \text{Maps:} \\ \text{field injections fixing } \mathbb{F}_q \end{array} \right\}$$

$$\begin{array}{rcl} \mathcal{C}_{|\mathbb{F}_q} & \longmapsto & \mathbb{F}_q(\mathcal{C}) \\ \phi : \mathcal{C}_1 \to \mathcal{C}_2 & \longmapsto & \phi^* : \mathbb{F}_q(\mathcal{C}_2) \to \mathbb{F}_q(\mathcal{C}_1) \end{array}$$

The GHS technique

$\mathcal{H}$ hyperelliptic curve. Goal: find fields F and F' s.t.

$$\begin{tikzcd}
 & & F' = \mathbb{F}_{q^n} \cdot F = \mathbb{F}_{q^n}(\mathcal{C}') \arrow[d, dash] \\
 & \mathbb{F}_{q^n}(\mathcal{H}) \arrow[ur, dash] & F = \mathbb{F}_q(\mathcal{C}') \\
\mathbb{F}_{q^n} \arrow[ur, dash] \arrow[d, dash] & & \\
\mathbb{F}_q \arrow[uurr, dash] & &
\end{tikzcd}$$

The GHS technique

$\mathcal{H}$ hyperelliptic curve. Goal: find fields F and F' s.t.

$$\begin{tikzcd}
 & & F' = \mathbb{F}_{q^n} \cdot F = \mathbb{F}_{q^n}(\mathcal{C}') \arrow[loop above, "\sigma"] \arrow[dl, dash] \arrow[d, dash] \\
 & \mathbb{F}_{q^n}(\mathcal{H}) \arrow[dl, dash] & F = F'^{\sigma} \arrow[ddll, dash] \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[d, dash] & & \\
\mathbb{F}_q & &
\end{tikzcd}$$

Lift of Frobenius σ must exist on F', with fixed subfield F

The GHS technique

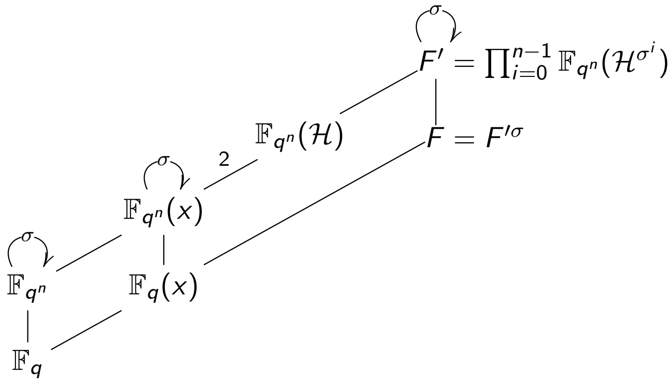
$\mathcal{H}$ hyperelliptic curve. Goal: find fields F and F' s.t.

$$\begin{tikzcd}[arrows=-]
 & & & F' \arrow[loop above, "\sigma"] \arrow[d] \\
 & & \mathbb{F}_{q^n}(\mathcal{H}) \arrow[ur] & F = F'^{\sigma} \\
 & \mathbb{F}_{q^n}(x) \arrow[loop above, "\sigma"] \arrow[ur, "2"] \arrow[d] & & \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[ur] & \mathbb{F}_q(x) \arrow[uurr] & & \\
\mathbb{F}_q \arrow[u] \arrow[ur] & & &
\end{tikzcd}$$

No lift of Frobenius on $\mathbb{F}_{q^n}(\mathcal{H})$, but on index 2 subfield $\mathbb{F}_{q^n}(x)$

The GHS technique

$\mathcal{H}$ hyperelliptic curve. Goal: find fields F and F' s.t.



Choose for F' compositum of function fields $\mathbb{F}_{q^n}(\mathcal{H}^{\sigma^i})$.

The GHS technique

$\mathcal{H}$ hyperelliptic curve. Goal: find fields F and F' s.t.

$$\begin{tikzcd}
 & & & F' = \prod_{i=0}^{n-1} \mathbb{F}_{q^n}(\mathcal{H}^{\sigma^i}) \arrow[loop above, "\sigma"] \arrow[d, dash] \\
 & & \mathbb{F}_{q^n}(\mathcal{H}) \arrow[ur, dash] & F = F'^{\sigma} \\
 & \mathbb{F}_{q^n}(x) \arrow[loop above, "\sigma"] \arrow[ur, dash, "2"] & & \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[ur, dash] & \mathbb{F}_q(x) \arrow[u, dash] \arrow[uurr, dash] & & \\
\mathbb{F}_q \arrow[u, dash] \arrow[ur, dash] & & &
\end{tikzcd}$$

Choose for F' compositum of function fields $\mathbb{F}_{q^n}(\mathcal{H}^{\sigma^i})$.

Construction depends of the choice of x, i.e. of the equation for $\mathcal{H}$

From the geometric to the function field approach

Hyperelliptic curve $\mathcal{H}$: $Y^2 + Y\,h_0(X) = h_1(X), \quad h_0, h_1 \in \mathbb{F}_{q^n}[X]$

Weil restriction

Choose $(\theta^{\sigma^i})_i$ normal basis of $\mathbb{F}_{q^n}$ with $\sum \theta^{\sigma^i} = 1$.
Let $X = \sum_i x_i\,\theta^{\sigma^i}, Y = \sum_i z_i\,\theta^{\sigma^i}$. Equation of $\mathcal{W}$ given (component-wise) by

$$\Big(\sum_i z_i\,\theta^{\sigma^i}\Big)^2 + \Big(\sum_i z_i\,\theta^{\sigma^i}\Big) h_0\Big(\sum_i x_i\,\theta^{\sigma^i}\Big) = h_1\Big(\sum_i x_i\,\theta^{\sigma^i}\Big)$$

From the geometric to the function field approach

Hyperelliptic curve $\mathcal{H}$: $Y^2 + Y\, h_0(X) = h_1(X), \quad h_0, h_1 \in \mathbb{F}_{q^n}[X]$

Weil restriction

Choose $(\theta^{\sigma^i})_i$ normal basis of $\mathbb{F}_{q^n}$ with $\sum \theta^{\sigma^i} = 1$.
Let $X = \sum_i x_i\, \theta^{\sigma^i}, Y = \sum_i z_i\, \theta^{\sigma^i}$. Equation of $\mathcal{W}$ given (component-wise) by

$$\Big(\sum_i z_i\, \theta^{\sigma^i}\Big)^2 + \Big(\sum_i z_i\, \theta^{\sigma^i}\Big) h_0\Big(\sum_i x_i\, \theta^{\sigma^i}\Big) = h_1\Big(\sum_i x_i\, \theta^{\sigma^i}\Big)$$

Hyperplane sections: put $x_0 = x_1 = \ldots = x_{n-1} = x$.
Then equation of the intersection is given (component-wise) by

$$\Big(\sum_i z_i\, \theta^{\sigma^i}\Big)^2 + \Big(\sum_i z_i\, \theta^{\sigma^i}\Big) h_0(x) = h_1(x)$$

From the geometric to the function field approach

Equation of the hyperplane section is
$(\sum_i z_i \theta^{\sigma^i})^2 + (\sum_i z_i \theta^{\sigma^i}) h_0(x) = h_1(x)$

From the geometric to the function field approach

Equation of the hyperplane section is
$(\sum_i z_i\,\theta^{\sigma^i})^2 + (\sum_i z_i\,\theta^{\sigma^i})h_0(x) = h_1(x)$

Change of coordinates over $\mathbb{F}_{q^n}$: $\begin{pmatrix} y_0 & \cdots & y_{n-1} \end{pmatrix} = \begin{pmatrix} z_0 & \ldots & z_{n-1} \end{pmatrix} M$
where $M = (\theta^{\sigma^{i+j-2}})_{i,j}$.
New equation defined over $\mathbb{F}_{q^n}$ of the hyperplane section is

$$(*) \qquad \begin{cases} y_0^2 + y_0\,h_0(x) = h_1(x) \\ \vdots \\ y_{n-1}^2 + y_{n-1}\,h_0^{\sigma^{n-1}}(x) = h_1^{\sigma^{n-1}}(x) \end{cases}$$

From the geometric to the function field approach

Equation of the hyperplane section is
$(\sum_i z_i\,\theta^{\sigma^i})^2 + (\sum_i z_i\,\theta^{\sigma^i})h_0(x) = h_1(x)$

Change of coordinates over $\mathbb{F}_{q^n}$: $\begin{pmatrix} y_0 & \cdots & y_{n-1} \end{pmatrix} = \begin{pmatrix} z_0 & \dots & z_{n-1} \end{pmatrix} M$
where $M = (\theta^{\sigma^{i+j-2}})_{i,j}$.
New equation defined over $\mathbb{F}_{q^n}$ of the hyperplane section is

$$(*) \qquad \begin{cases} y_0^2 + y_0\,h_0(x) = h_1(x) \\ \vdots \\ y_{n-1}^2 + y_{n-1}\,h_0^{\sigma^{n-1}}(x) = h_1^{\sigma^{n-1}}(x) \end{cases}$$

Let $\mathcal{C}' =$ an irreducible component of the intersection.
Then $\mathbb{F}_{q^n}(\mathcal{C}') = \mathbb{F}_{q^n}(x, y_0, \dots, y_{n-1})$ where the y_i's satisfy $(*)$.

From the geometric to the function field approach

Equation of the hyperplane section is
$(\sum_i z_i\,\theta^{\sigma^i})^2 + (\sum_i z_i\,\theta^{\sigma^i})h_0(x) = h_1(x)$

Change of coordinates over $\mathbb{F}_{q^n}$: $\begin{pmatrix} y_0 & \cdots & y_{n-1} \end{pmatrix} = \begin{pmatrix} z_0 & \dots & z_{n-1} \end{pmatrix} M$
where $M = (\theta^{\sigma^{i+j-2}})_{i,j}$.
New equation defined over $\mathbb{F}_{q^n}$ of the hyperplane section is

$$(*) \qquad \begin{cases} y_0^2 + y_0\,h_0(x) = h_1(x) \\ \vdots \\ y_{n-1}^2 + y_{n-1}\,h_0^{\sigma^{n-1}}(x) = h_1^{\sigma^{n-1}}(x) \end{cases}$$

Let $\mathcal{C}'$ = an irreducible component of the intersection.
Then $\mathbb{F}_{q^n}(\mathcal{C}') = \mathbb{F}_{q^n}(x, y_0, \dots, y_{n-1})$ where the y_i's satisfy $(*)$.

This is exactly the compositum $F' = \prod_i \mathbb{F}_{q^n}(\mathcal{H}^{\sigma^i})$.

Magic number

$$
\begin{tikzcd}
 & & F' \arrow[dll, no head] \arrow[dl, no head] \arrow[dr, no head] \arrow[dd, bend left=80, no head, "2^m"] & \\
\mathbb{F}_{q^n}(\mathcal{H}) \arrow[drr, no head, "2"'] & \mathbb{F}_{q^n}(\mathcal{H}^{\sigma}) \arrow[dr, no head, "2"] & \cdots & \mathbb{F}_{q^n}(\mathcal{H}^{\sigma^{n-1}}) \arrow[dl, no head, "2"] \\
 & & \mathbb{F}_{q^n}(x) &
\end{tikzcd}
$$

- m "magic number": the genus g of F' depends essentially of $[F' : \mathbb{F}_{q^n}(x)] = 2^m$
- For most curves $\mathcal{H}$, $m \simeq n$ $\rightarrow g(\mathcal{C}') \text{ is of order } 2^n g(\mathcal{H})$
  $\rightsquigarrow$ few curves are directly vulnerable

Possible issues

Recall:

$$\begin{aligned} F' &= \prod_i \mathbb{F}_{q^n}(\mathcal{H}^{\sigma^i}) \\ &= \mathbb{F}_{q^n}(x, y_0, \ldots, y_{n-1}) \\ &= \mathbb{F}_{q^n}(x, y_0, \ldots, y_{m-1}) \end{aligned}$$

where $y_i^2 + y_i\, h_0^{\sigma^i}(x) = h_1^{\sigma^i}(x)$

- Field of constants of F' must be $\mathbb{F}_{q^n}$
- Frobenius σ defined on $\mathbb{F}_{q^n}(x)$ (with $\sigma(x) = x$) must have an order n extension to F'
  $\rightsquigarrow$ always the case if n odd or $m = n$

Possible issues

- Kernel of conorm-norm map must preserve a large prime order subgroup

Possible issues

- Kernel of conorm-norm map must preserve a large prime order subgroup
  - fails if equation of $\mathcal{H}$ defined over proper subfield:

$$\begin{tikzcd}
\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q^n}) \arrow[r, "\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}"] & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q^d}) \arrow[r, "\mathrm{tr}_{\mathbb{F}_{q^d}/\mathbb{F}_{q}}"] & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q}) \\
\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[r, "\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}"] & \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^d}) \arrow[u, "\pi^*"] &
\end{tikzcd}$$

Transfer map vanishes on (large) kernel of bottom-row map.

Possible issues

- Kernel of conorm-norm map must preserve a large prime order subgroup
  - fails if equation of $\mathcal{H}$ defined over proper subfield:

$$\begin{array}{ccccc}
\mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q^n}) & \xrightarrow{\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}} & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_{q^d}) & \xrightarrow{\mathrm{tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}} & \mathrm{Jac}_{\mathcal{C}'}(\mathbb{F}_q) \\
\pi^* \uparrow & & \pi^* \uparrow & & \\
\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}) & \xrightarrow{\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}} & \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^d}) & &
\end{array}$$

    Transfer map vanishes on (large) kernel of bottom-row map.

  - ok otherwise: kernel of conorm-norm map $\subset \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})[2^{m-1}]$ [Diem,Hess]

GHS in characteristic 2

$\mathcal{H} : y^2 + y\, h_0(x) = h_1(x)$. Change of variable $y \leftrightarrow y/h_0(x)$:
$\rightsquigarrow$ new equation in Artin-Schreier form $y^2 + y = h_1(x)/h_0(x)^2 = f(x)$.

Artin-Schreier operator

On any char. 2 field K, define $\mathcal{P} : K \to K, \quad z \mapsto z^2 + z$

$\mathbb{F}_2[t]$-action

For any $P = \sum_i a_i t^i$ in $\mathbb{F}_2[t]$, any $g \in \mathbb{F}_{q^n}(x)$, let

$$P \cdot g = \sum_i a_i g^{\sigma^i}$$

$\rightsquigarrow$ turns $\mathbb{F}_{q^n}(x)$ and $\mathbb{F}_{q^n}(x)/\mathcal{P}(\mathbb{F}_{q^n}(x))$ into $\mathbb{F}_2[t]$-modules

GHS in characteristic 2

$\mathcal{H} : y^2 + y = f(x)$

Main result

Let $\mathcal{I}_f = \{P \in \mathbb{F}_2[t] \ : \ P \cdot f \in \mathcal{P}(\mathbb{F}_{q^n}(x))\} = \langle M_f \rangle$. Then $m = \deg M_f$.
Furthermore $M_f | t^n + 1$.

GHS in characteristic 2

$\mathcal{H} : y^2 + y = f(x)$

Main result

Let $\mathcal{I}_f = \{P \in \mathbb{F}_2[t] \; : \; P \cdot f \in \mathcal{P}(\mathbb{F}_{q^n}(x))\} = \langle M_f \rangle$. Then $m = \deg M_f$.
Furthermore $M_f | t^n + 1$.

Consequence

Magic number m cannot take all values between 1 and n

In particular if n prime, then $t^n + 1 = (t+1)\Phi_n(t) = (t+1)\prod_i \Phi_{n,i}(t)$
where $\deg \Phi_{n,i} = \phi_2(n) =$ order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$
$\rightsquigarrow m = k\phi_2(n)$ or $k\phi_2(n) + 1$ for some integer k

GHS in characteristic 2

$\mathcal{H} : y^2 + y = f(x)$

Main result

Let $\mathcal{I}_f = \{P \in \mathbb{F}_2[t] \ : \ P \cdot f \in \mathcal{P}(\mathbb{F}_{q^n}(x))\} = \langle M_f \rangle$. Then $m = \deg M_f$. Furthermore $M_f | t^n + 1$.

Consequence

Magic number m cannot take all values between 1 and n

In particular if n prime, then $t^n + 1 = (t+1)\Phi_n(t) = (t+1)\prod_i \Phi_{n,i}(t)$ where $\deg \Phi_{n,i} = \phi_2(n) =$ order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$
$\rightsquigarrow m = k\phi_2(n)$ or $k\phi_2(n) + 1$ for some integer k

Problem: $\phi_2(n)$ small only for few primes n (Mersenne or Fermat primes), so GHS cannot work for all field extensions.

The elliptic curve case

Let $E \ : \ y^2 + xy = x^3 + ax^2 + b$. After simple change of variables, new equation in Artin-Schreier form:

$$E \ : \ y^2 + y = \beta x + \alpha + \gamma / x$$

Let $M_\beta \in \mathbb{F}_2[t]$ minimal polynomial s.t. $M_\beta \cdot \beta = 0$; same for γ

Theorem

Assume $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\alpha) = 0$ or $(t+1) | lcm(M_\beta, M_\gamma)$. Then

- $M_f = lcm(M_\beta, M_\gamma)$ and constant field of F' is $\mathbb{F}_{q^n}$
- genus of F' is

$$g(F') = 2^m - 2^{m - \deg M_\beta} - 2^{m - \deg M_\gamma} + 1$$

- if β or γ is in $\mathbb{F}_q$, then F' is hyperelliptic

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

$n = 7$: factorization of $t^7 + 1$ is $(t+1)(t^3+t^2+1)(t^3+t+1)$
$\rightarrow$ possible values of m are $3, 4, 6$ or 7 (or 1).

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve E : $y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variable $y \leftrightarrow yx + \sqrt{\theta^2 + 1} \rightsquigarrow$ new equation

$$y^2 + y = x + (\theta + 1)/x$$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \; : \; y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variable $y \leftrightarrow yx + \sqrt{\theta^2 + 1} \rightsquigarrow$ new equation

$$y^2 + y = x + (\theta + 1)/x$$

- $\beta = 1 \rightsquigarrow M_\beta = t + 1$, $\gamma = \theta + 1 \rightsquigarrow M_\gamma = \sum_{i=0}^{6} t^i$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \; : \; y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variable $y \leftrightarrow yx + \sqrt{\theta^2 + 1} \rightsquigarrow$ new equation

$$y^2 + y = x + (\theta + 1)/x$$

- $\beta = 1 \rightsquigarrow M_\beta = t + 1$, $\gamma = \theta + 1 \rightsquigarrow M_\gamma = \sum_{i=0}^{6} t^i$
- $M_h = lcm(M_\beta, M_\gamma) = t^7 + 1$
  $\Rightarrow m = 7$ and genus of cover is $g = 2^7 - 2^6 - 2^1 + 1 = 63.$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variable $y \leftrightarrow yx + \sqrt{\theta^2 + 1} \rightsquigarrow$ new equation

$$y^2 + y = x + (\theta + 1)/x$$

- $\beta = 1 \rightsquigarrow M_\beta = t + 1$, $\gamma = \theta + 1 \rightsquigarrow M_\gamma = \sum_{i=0}^{6} t^i$
- $M_h = lcm(M_\beta, M_\gamma) = t^7 + 1$
  $\Rightarrow m = 7$ and genus of cover is $g = 2^7 - 2^6 - 2^1 + 1 = 63$.
- $\beta \in \mathbb{F}_q$, so cover is hyperelliptic, equation (obtained with a computer algebra system):

$$y^2 + (\sum_{i=0}^{6} x^{2^i})y = \sum_{i=0}^{6} x^{2^i}$$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \; : \; y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variables $y \leftrightarrow yx + \sqrt{\theta^2 + 1}$, $x \leftrightarrow (\theta^5 + \theta^4)x \rightsquigarrow$ new equation

$$y^2 + y = (\theta^5 + \theta^4)x + (\theta^3 + \theta^2)/x$$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variables $y \leftrightarrow yx + \sqrt{\theta^2 + 1}$, $x \leftrightarrow (\theta^5 + \theta^4)x \rightsquigarrow$ new equation

$$y^2 + y = (\theta^5 + \theta^4)x + (\theta^3 + \theta^2)/x$$

- $\beta = \theta^5 + \theta^4$, $\gamma = \theta^3 + \theta^2 \rightsquigarrow M_\beta = M_\gamma = t^3 + t + 1$

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variables $y \leftrightarrow yx + \sqrt{\theta^2 + 1}$, $x \leftrightarrow (\theta^5 + \theta^4)x \rightsquigarrow$ new equation

$$y^2 + y = (\theta^5 + \theta^4)x + (\theta^3 + \theta^2)/x$$

- $\beta = \theta^5 + \theta^4$, $\gamma = \theta^3 + \theta^2 \rightsquigarrow M_\beta = M_\gamma = t^3 + t + 1$
- $M_h = lcm(M_\beta, M_\gamma) = t^3 + t + 1$
  $\Rightarrow m = 3$ and genus of cover is $g = 2^3 - 2^0 - 2^0 + 1 = 7$.

A toy example

On $\mathbb{F}_{2^7} \simeq \mathbb{F}_2(\theta)$ where $\theta^7 + \theta^6 + 1 = 0$

Elliptic curve $E \ : \ y^2 + xy = x^3 + (\theta^2 + 1)$

Change of variables $y \leftrightarrow yx + \sqrt{\theta^2 + 1}$, $x \leftrightarrow (\theta^5 + \theta^4)x \rightsquigarrow$ new equation

$$y^2 + y = (\theta^5 + \theta^4)x + (\theta^3 + \theta^2)/x$$

- $\beta = \theta^5 + \theta^4$, $\gamma = \theta^3 + \theta^2 \rightsquigarrow M_\beta = M_\gamma = t^3 + t + 1$
- $M_h = lcm(M_\beta, M_\gamma) = t^3 + t + 1$
  $\Rightarrow m = 3$ and genus of cover is $g = 2^3 - 2^0 - 2^0 + 1 = 7$.
- equation of cover (obtained with a computer algebra system):

$$x^2(y^8 + y^4 + y) = x^6 + 1 \quad \text{(not hyperelliptic)}$$

GHS in odd characteristic

$\mathcal{H} : y^2 + y\,h_0(x) = h_1(x)$. Change of variable $y \leftrightarrow y + h_0(x)/2$:
$\rightsquigarrow$ new equation in Kummer form $y^2 = f(x)$.

$\mathbb{F}_2[t]$-action

For any $P = \sum_i a_i t^i$ in $\mathbb{F}_2[t]$, any $g \in \mathbb{F}_{q^n}(x)^*/(\mathbb{F}_{q^n}(x)^*)^2$, let

$$P \cdot g = \prod_i (g^{\sigma^i})^{a_i}$$

$\rightsquigarrow$ turns $\mathbb{F}_{q^n}(x)^*/(\mathbb{F}_{q^n}(x)^*)^2$ into a $\mathbb{F}_2[t]$-module

GHS in odd characteristic

$$\mathcal{H} : y^2 = f(x)$$

Main result (as in binary case)

Let $\mathcal{I}_f = \{P \in \mathbb{F}_2[t] \ : \ P \cdot f = 0 \text{ in } \mathbb{F}_{q^n}(x)^* / (\mathbb{F}_{q^n}(x)^*)^2\} = \langle M_f \rangle$.
Then $m = \deg M_f$.
Furthermore $M_f | t^n + 1$.

GHS in odd characteristic

$\mathcal{H} : y^2 = f(x)$

Main result (as in binary case)

Let $\mathcal{I}_f = \{P \in \mathbb{F}_2[t] \ : \ P \cdot f = 0 \text{ in } \mathbb{F}_{q^n}(x)^*/(\mathbb{F}_{q^n}(x)^*)^2\} = \langle M_f \rangle$.
Then $m = \deg M_f$.
Furthermore $M_f | t^n + 1$.

Same consequence as in char. 2: possible values of magic number m depend of factorization of $t^n + 1$
$\rightsquigarrow$ GHS cannot work for all field extensions.

Genus of cover

$\mathcal{H} : y^2 = f(x)$.

Let $f(x, z)$ homogenization of f with $\deg f = 2g(\mathcal{H}) + 2$, and

$$R_0 = \left\{[x : z] \in \mathbb{P}^1(\overline{\mathbb{F}_{q^n}}) \;:\; f(x, z) = 0\right\}, \quad R = \bigcup_i \sigma^i(R_0)$$

($\leftrightarrow$ ramification points of $\overline{\mathbb{F}_{q^n}}F'/\overline{\mathbb{F}_{q^n}}(x)$)

Theorem [Diem]

Assume constant field of F' is $\mathbb{F}_{q^n}$. Then

$$g(F') = 2^{m-2}(\#R - 4) + 1 \qquad (\Leftarrow \text{Hurwitz formula})$$

Genus of cover

$\mathcal{H} : y^2 = f(x)$.

Let $f(x,z)$ homogenization of f with $\deg f = 2g(\mathcal{H}) + 2$, and

$$R_0 = \left\{[x : z] \in \mathbb{P}^1(\overline{\mathbb{F}_{q^n}}) \ : \ f(x,z) = 0\right\}, \quad R = \bigcup_i \sigma^i(R_0)$$

($\leftrightarrow$ ramification points of $\overline{\mathbb{F}_{q^n}}F'/\overline{\mathbb{F}_{q^n}}(x)$)

Theorem [Diem]

Assume constant field of F' is $\mathbb{F}_{q^n}$. Then

$$g(F') = 2^{m-2}(\#R - 4) + 1 \qquad (\Leftarrow \text{Hurwitz formula})$$

Note: contrarily to the char. 2 case, F' (almost) never hyperelliptic when $m \geq 4$

Examples for $n = 5$

$$E : y^2 = f(x)$$

- f "random" degree 3 polynomial: $m = 5$, $\#R = 3 \times 5 + 1$
  $\rightsquigarrow g = 2^{5-2}(16 - 4) + 1 = 97$, too large for DLP

Examples for $n = 5$

$$E : y^2 = f(x)$$

- optimal genus obtained for
  $f = (x - a)(x - \sigma(a))(x - \sigma^2(a))(x - \sigma^3(a)), \quad a \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$

Examples for $n = 5$

$$E : y^2 = f(x)$$

- optimal genus obtained for
  $f = (x-a)(x-\sigma(a))(x-\sigma^2(a))(x-\sigma^3(a)), \quad a \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$

$$\begin{array}{cc} & \begin{array}{ccccc} a & \sigma(a) & \sigma^2(a) & \sigma^3(a) & \sigma^4(a) \end{array} \\ \begin{array}{c} f \\ f^{\sigma} \\ f^{\sigma^2} \\ f^{\sigma^3} \\ f^{\sigma^4} \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Examples for $n = 5$

$$E : y^2 = f(x)$$

- optimal genus obtained for
  $f = (x - a)(x - \sigma(a))(x - \sigma^2(a))(x - \sigma^3(a)), \quad a \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$

$$\begin{array}{c} \\ f \\ f^{\sigma} \\ f^{\sigma^2} \\ f^{\sigma^3} \\ f^{\sigma^4} \end{array}
\begin{array}{c} \begin{array}{ccccc} a & \sigma(a) & \sigma^2(a) & \sigma^3(a) & \sigma^4(a) \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}
\quad \rightsquigarrow \quad \begin{array}{l} m = \text{rank} = 4 \\ \#R = 5 \end{array}$$

Examples for $n = 5$

$$E : y^2 = f(x)$$

- optimal genus obtained for
  $f = (x-a)(x-\sigma(a))(x-\sigma^2(a))(x-\sigma^3(a)), \quad a \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$

$$\begin{array}{c} \\ f \\ f^{\sigma} \\ f^{\sigma^2} \\ f^{\sigma^3} \\ f^{\sigma^4} \end{array} \begin{array}{c} \begin{array}{ccccc} a & \sigma(a) & \sigma^2(a) & \sigma^3(a) & \sigma^4(a) \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array} \rightsquigarrow \begin{array}{l} m = \text{rank} = 4 \\ \#R = 5 \end{array}$$

$$\Rightarrow g(F') = 2^{4-2}(5-4) + 1 = 5$$

Scope of the GHS attack

- On some finite fields of composite extension degree, DLP "weak" on most elliptic curves
- Some finite fields are immune to the GHS attack:
  - prime fields
  - $\mathbb{F}_{p^2}$ for elliptic curves
  - $\mathbb{F}_{p^n}$, p prime, for most large primes n
- Complete overview of the speed-up provided by GHS attack too ambitious for this lecture
  Keep in mind that:
  - GHS usually gives only minor security reductions over generic attacks
  - but can be very efficient for some very specific curves

Comparison between GHS and direct index calculus on $E(\mathbb{F}_{q^n})$

- Both use a one-dimensional subvariety ($\mathcal{C}'$ or $\mathcal{F}$) of Weil restriction $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$
- Take place in different abelian varieties: $\mathrm{Jac}_{\mathcal{C}'}$ for GHS, $\mathcal{W}$ for direct index calculus
- Crucial parameter is $g(\mathcal{C}')$ for GHS, n for direct index calculus
  - GHS much more efficient on some curves than others
  - direct index calculus equally efficient on all curves
- GHS better for the minority of curves s.t. $g(\mathcal{C}')$ close to n, otherwise direct index calculus better

Conclusion

Consequence on DLP security

For maximal security, one should avoid:

- small embedding degrees
- subgroups of order divisible by the characteristic
- curves of genus $g \geq 3$
- curves defined over small degree extension fields

Consequence on DLP security

For maximal security, one should avoid:

- small embedding degrees
- subgroups of order divisible by the characteristic
- curves of genus $g \geq 3$
- curves defined over small degree extension fields

No known algorithm better than generic attacks on random curves with genus ≤ 2 defined over prime fields (or large prime degree extension fields)
$\rightsquigarrow$ **best candidates for DLP-based cryptography**