Computational challenges arising in torus-based cryptography

Elisa Gorla

Institut für Mathematik
Universität Zürich

Outline:

1. “Historical” introduction
2. The primitive subgroup of a finite field
3. Representation of the elements and arithmetic
4. The Discrete Logarithm Problem
5. Closing remarks

“Historical” introduction

LUC (Smith, Skinner - 1995):

- works in $G_{2,q} = \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{q+1} = 1\} \subseteq \mathbb{F}_{q^2}^*$
- represent an element $\alpha \in G_{2,q}$ via its trace

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q \in \mathbb{F}_q.$$

"Historical" introduction

LUC (Smith, Skinner - 1995):

- works in $G_{2,q} = \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{q+1} = 1\} \subseteq \mathbb{F}_{q^2}^*$
- represent an element $\alpha \in G_{2,q}$ via its trace

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q \in \mathbb{F}_q.$$

XTR (Brouwer, Lenstra, Pellikaan, Verheul - 1999):

- works in $G_{6,q} = \{\alpha \in \mathbb{F}_{q^6}^* \mid \alpha^{q^2-q+1} = 1\} \subseteq \mathbb{F}_{q^6}^*$
- represents an element $\alpha \in G_{6,q}$ via its trace

$$\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha) = \alpha^{q^4} + \alpha^{q^2} + \alpha \in \mathbb{F}_{q^2}.$$

“Historical” introduction

LUC (Smith, Skinner - 1995):

- works in $G_{2,q} = \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{q+1} = 1\} \subseteq \mathbb{F}_{q^2}^*$
- represent an element $\alpha \in G_{2,q}$ via its trace

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q \in \mathbb{F}_q.$$

XTR (Brouwer, Lenstra, Pellikaan, Verheul - 1999):

- works in $G_{6,q} = \{\alpha \in \mathbb{F}_{q^6}^* \mid \alpha^{q^2-q+1} = 1\} \subseteq \mathbb{F}_{q^6}^*$
- represents an element $\alpha \in G_{6,q}$ via its trace

$$\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha) = \alpha^{q^4} + \alpha^{q^2} + \alpha \in \mathbb{F}_{q^2}.$$

Recurrence sequences to compute $\mathrm{Tr}(\alpha^{ab})$ from $\mathrm{Tr}(\alpha^a)$ and b.

“Historical” introduction

- the complexity of the DLP in the subgroups $G_{2,q} \subseteq \mathbb{F}_{q^2}^*$, $G_{6,q} \subseteq \mathbb{F}_{q^6}^*$ is the same as the complexity of the DLP in the whole field

“Historical” introduction

- the complexity of the DLP in the subgroups $G_{2,q} \subseteq \mathbb{F}^*_{q^2}$, $G_{6,q} \subseteq \mathbb{F}^*_{q^6}$ is the same as the complexity of the DLP in the whole field

- an element of $G_{2,q}$ is represented via one $\mathbb{F}_q$-coordinate (instead of two)

“Historical” introduction

- the complexity of the DLP in the subgroups $G_{2,q} \subseteq \mathbb{F}_{q^2}^*$, $G_{6,q} \subseteq \mathbb{F}_{q^6}^*$ is the same as the complexity of the DLP in the whole field
- an element of $G_{2,q}$ is represented via one $\mathbb{F}_q$-coordinate (instead of two)
- an element of $G_{6,q}$ is represented via two $\mathbb{F}_q$-coordinates (instead of six)

“Historical” introduction

- the complexity of the DLP in the subgroups $G_{2,q} \subseteq \mathbb{F}_{q^2}^*$, $G_{6,q} \subseteq \mathbb{F}_{q^6}^*$ is the same as the complexity of the DLP in the whole field
- an element of $G_{2,q}$ is represented via one $\mathbb{F}_q$-coordinate (instead of two)
- an element of $G_{6,q}$ is represented via two $\mathbb{F}_q$-coordinates (instead of six)
- neither representation is 1-1

“Historical” introduction

- the complexity of the DLP in the subgroups $G_{2,q} \subseteq \mathbb{F}_{q^2}^*$, $G_{6,q} \subseteq \mathbb{F}_{q^6}^*$ is the same as the complexity of the DLP in the whole field
- an element of $G_{2,q}$ is represented via one $\mathbb{F}_q$-coordinate (instead of two)
- an element of $G_{6,q}$ is represented via two $\mathbb{F}_q$-coordinates (instead of six)
- neither representation is 1-1
- arithmetic in both subgroups is efficient

Main ideas behind torus-based cryptography:

- work in the primitive subgroup $G_{n,q} \subseteq \mathbb{F}_{q^n}^*$

Main ideas behind torus-based cryptography:

- work in the primitive subgroup $G_{n,q} \subseteq \mathbb{F}_{q^n}^*$
- the complexity of the DLP in $G_{n,q}$ is the same as in $\mathbb{F}_{q^n}^*$

Main ideas behind torus-based cryptography:

- work in the primitive subgroup $G_{n,q} \subseteq \mathbb{F}_{q^n}^*$
- the complexity of the DLP in $G_{n,q}$ is the same as in $\mathbb{F}_{q^n}^*$
- represent elements of $G_{n,q}$ via $\varphi(n)$ coordinates in $\mathbb{F}_q$ (instead of n)

Main ideas behind torus-based cryptography:

- work in the primitive subgroup $G_{n,q} \subseteq \mathbb{F}_{q^n}^*$
- the complexity of the DLP in $G_{n,q}$ is the same as in $\mathbb{F}_{q^n}^*$
- represent elements of $G_{n,q}$ via $\varphi(n)$ coordinates in $\mathbb{F}_q$ (instead of n)
- the means are arithmetic and geometric constructions

1. The primitive subgroup

$\mathbb{F}_{q^n}$ finite field, $(\mathbb{F}_{q^n}^*, \cdot)$ multiplicative group.

The **primitive subgroup** is

$$G_{n,q} = \{g \in \mathbb{F}_{q^n}^* \mid g^{\phi_n(q)} = 1\}$$

where $\phi_n(x)$ is the n-th cyclotomic polynomial.

Discrete Logarithm Problem (DLP): given $\alpha \in G$ and $\beta \in <\alpha>$, find $m \in \mathbb{Z}$ such that $\beta = \alpha^m$.

Consider the DLP in $G = \mathbb{F}_{q^n}^*$ or $G = G_{n,q}$.

The primitive subgroup

- $G_{n,q} \subseteq \mathbb{F}^*_{q^n}, \quad |G_{n,q}| = \phi_n(q) \sim q^{\varphi(n)}, \;\; |\mathbb{F}^*_{q^n}| = q^n - 1$

The primitive subgroup

- $G_{n,q} \subseteq \mathbb{F}^*_{q^n}, \quad |G_{n,q}| = \phi_n(q) \sim q^{\varphi(n)}, \ |\mathbb{F}^*_{q^n}| = q^n - 1$
- $G_{n,q} \not\subseteq \mathbb{F}^*_{q^l}$ for $l|n$, $l \neq n$ (unless $p|\phi_n(q)$ prime $\Rightarrow$ $p|n$)

The primitive subgroup

- $G_{n,q} \subseteq \mathbb{F}^*_{q^n}, \quad |G_{n,q}| = \phi_n(q) \sim q^{\varphi(n)}, \; |\mathbb{F}^*_{q^n}| = q^n - 1$
- $G_{n,q} \not\subseteq \mathbb{F}^*_{q^l}$ for $l|n$, $l \neq n$ (unless $p|\phi_n(q)$ prime $\Rightarrow$ $p|n$)
- complexity of solving the DLP in $G_{n,q}$ or $F^*_{q^n}$ is the same

The primitive subgroup

- $G_{n,q} \subseteq \mathbb{F}_{q^n}^*, \quad |G_{n,q}| = \phi_n(q) \sim q^{\varphi(n)}, \ |\mathbb{F}_{q^n}^*| = q^n - 1$
- $G_{n,q} \not\subseteq \mathbb{F}_{q^l}^*$ for $l|n$, $l \neq n$ (unless $p|\phi_n(q)$ prime $\Rightarrow p|n$)
- complexity of solving the DLP in $G_{n,q}$ or $F_{q^n}^*$ is the same

Working in $G_{n,q}$ is practical if we can represent its elements via $\varphi(n)$ elements of $\mathbb{F}_q$, as opposed to the n elements of $\mathbb{F}_q$ that we need for representing elements of $\mathbb{F}_{q^n}^*$.

Main cases of interest

For which values of n do we have the most compact representation?

- Representing an element in the primitive subgroup would require $\varphi(n)/n$ times as many bits as a general element of $\mathbb{F}_{q^n}^*$.

Main cases of interest

For which values of n do we have the most compact representation?

- Representing an element in the primitive subgroup would require $\varphi(n)/n$ times as many bits as a general element of $\mathbb{F}_{q^n}^*$.
- $\varphi(n)/n$ is the same for $n = p_1 \cdots p_t$ and $n = p_1^{e_1} \cdots p_t^{e_t}$, therefore we prefer n squarefree

Main cases of interest

For which values of n do we have the most compact representation?

- Representing an element in the primitive subgroup would require $\varphi(n)/n$ times as many bits as a general element of $\mathbb{F}_{q^n}^*$.
- $\varphi(n)/n$ is the same for $n = p_1 \cdots p_t$ and $n = p_1^{e_1} \cdots p_t^{e_t}$, therefore we prefer n squarefree
- $\varphi(p)/p$ is an increasing function of p.

Main cases of interest

For which values of n do we have the most compact representation?

- Representing an element in the primitive subgroup would require $\varphi(n)/n$ times as many bits as a general element of $\mathbb{F}_{q^n}^*$.
- $\varphi(n)/n$ is the same for $n = p_1 \cdots p_t$ and $n = p_1^{e_1} \cdots p_t^{e_t}$, therefore we prefer n squarefree
- $\varphi(p)/p$ is an increasing function of p.

So we are mainly interested in the cases $n = 2, 6, 30, 210$.

2. Representation of the elements

Roadmap:

1. Construct a variety T_n defined over $\mathbb{F}_q$ s.t. $T_n(\mathbb{F}_q) = G_{n,q}$.
2. Exploit the arithmetic-geometric structure of T_n.

2. Representation of the elements

Roadmap:

1. Construct a variety T_n defined over $\mathbb{F}_q$ s.t. $T_n(\mathbb{F}_q) = G_{n,q}$.
2. Exploit the arithmetic-geometric structure of T_n.

The **norm map** relative to $\mathbb{F}_{q^n} \supseteq \mathbb{F}_{q^l}$ is

$$\begin{array}{rcl} N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}} : \mathbb{F}_{q^n}^* & \longrightarrow & \mathbb{F}_{q^l}^* \\ \alpha & \longmapsto & \alpha \cdot \alpha^{q^l} \cdots \alpha^{q^{n-l}} = \alpha^{1+q^l+\ldots+q^{n-l}}. \end{array}$$

2. Representation of the elements

Roadmap:

1. Construct a variety T_n defined over $\mathbb{F}_q$ s.t. $T_n(\mathbb{F}_q) = G_{n,q}$.
2. Exploit the arithmetic-geometric structure of T_n.

The **norm map** relative to $\mathbb{F}_{q^n} \supseteq \mathbb{F}_{q^l}$ is

$$\begin{array}{rcl} N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}} : \mathbb{F}_{q^n}^* & \longrightarrow & \mathbb{F}_{q^l}^* \\ \alpha & \longmapsto & \alpha \cdot \alpha^{q^l} \cdots \alpha^{q^{n-l}} = \alpha^{1+q^l+\ldots+q^{n-l}}. \end{array}$$

Lemma:(Rubin, Silverberg - 2003)

$$G_{n,q} = \{\alpha \in \mathbb{F}_{q^n}^* \mid N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}}(\alpha) = 1 \text{ for all } l|n, l \neq n\}.$$

Representation of the elements

Example: $G_{6,q} = \{\alpha \in \mathbb{F}_{q^6}^* \mid \alpha^{q^2-q+1} = 1\}$

$$= \ker \left[\begin{array}{ccc} \mathbb{F}_{q^6}^* & \longrightarrow & \mathbb{F}_q^* \bigoplus \mathbb{F}_{q^2}^* \bigoplus \mathbb{F}_{q^3}^* \\ \alpha & \longmapsto & (\alpha^{1+q+q^2+q^3+q^4+q^5}, \alpha^{1+q^2+q^4}, \alpha^{1+q^3}) \end{array} \right]$$

Representation of the elements

Example: $G_{6,q} = \{\alpha \in \mathbb{F}_{q^6}^* \mid \alpha^{q^2-q+1} = 1\}$

$$= \ker \left[\begin{array}{ccc} \mathbb{F}_{q^6}^* & \longrightarrow & \mathbb{F}_q^* \oplus \mathbb{F}_{q^2}^* \oplus \mathbb{F}_{q^3}^* \\ \alpha & \longmapsto & (\alpha^{1+q+q^2+q^3+q^4+q^5}, \alpha^{1+q^2+q^4}, \alpha^{1+q^3}) \end{array} \right]$$

Define

$$T_n = \ker \left[\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m \xrightarrow{\oplus \mathcal{N}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^l}}} \bigoplus_{l|n, l \neq n} \mathrm{Res}_{\mathbb{F}_{q^l}/\mathbb{F}_q} \mathbb{G}_m \right]$$

$\mathbb{G}_m(\mathbb{F}) \cong \mathbb{F}^*$, so $\mathrm{Res}_{\mathbb{F}_{q^l}/\mathbb{F}_q} \mathbb{G}_m(\mathbb{F}_q) = \mathbb{G}_m(\mathbb{F}_{q^l}) = \mathbb{F}_{q^l}^*$.

Representation of the elements

Example: $G_{6,q} = \{\alpha \in \mathbb{F}_{q^6}^* \mid \alpha^{q^2-q+1} = 1\}$

$$= \ker \left[\begin{array}{ccc} \mathbb{F}_{q^6}^* & \longrightarrow & \mathbb{F}_q^* \oplus \mathbb{F}_{q^2}^* \oplus \mathbb{F}_{q^3}^* \\ \alpha & \longmapsto & (\alpha^{1+q+q^2+q^3+q^4+q^5}, \alpha^{1+q^2+q^4}, \alpha^{1+q^3}) \end{array} \right]$$

Define

$$T_n = \ker \left[\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m \xrightarrow{\oplus \mathcal{N}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^l}}} \bigoplus_{l|n, l \neq n} \mathrm{Res}_{\mathbb{F}_{q^l}/\mathbb{F}_q} \mathbb{G}_m \right]$$

$\mathbb{G}_m(\mathbb{F}) \cong \mathbb{F}^*$, so $\mathrm{Res}_{\mathbb{F}_{q^l}/\mathbb{F}_q} \mathbb{G}_m(\mathbb{F}_q) = \mathbb{G}_m(\mathbb{F}_{q^l}) = \mathbb{F}_{q^l}^*$.

$$T_n(\mathbb{F}_q) = \{\alpha \in \mathbb{F}_{q^n}^* \mid N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}}(\alpha) = 1 \text{ for all } l|n, l \neq n\} = G_{n,q}$$

Representation of the elements

Goal: showing that T_n is rational, i.e. construct birational maps (defined for almost all points)

$$T_n \leftrightarrows \mathbb{A}^{\varphi(n)}$$

so that taking $\mathbb{F}_q$-rational points we have an almost-bijection

$$G_{n,q} = T_n(\mathbb{F}_q) \leftrightarrows \mathbb{F}_q^{\varphi(n)}$$

Representation of the elements

Goal: showing that T_n is rational, i.e. construct birational maps (defined for almost all points)

$$T_n \leftrightarrows \mathbb{A}^{\varphi(n)}$$

so that taking $\mathbb{F}_q$-rational points we have an almost-bijection

$$G_{n,q} = T_n(\mathbb{F}_q) \leftrightarrows \mathbb{F}_q^{\varphi(n)}$$

We know that these maps exist for $n = p$ or $n = p_1 p_2$. We know that they exist for all n if we add extra copies of $\mathbb{F}_q$:

$$T_n \times \mathbb{A}^k \cong \mathbb{A}^{\varphi(n)+k} \quad \text{i.e.} \quad G_{n,q} \times \mathbb{F}_q^k \leftrightarrows \mathbb{F}_q^{\varphi(n)+k}$$

Some natural questions:

- Can we write explicit maps for the cases $n = 2, 6, 30, 210$? Yes for $n = 2, 6$ (Rubin, Silverberg - 2003).

- Can we write maps

  $$G_{n,q} \times \mathbb{F}_q^k \leftrightarrows \mathbb{F}_q^{\varphi(n)+k}$$

  for small values of k ? Yes for $(n, k) = (30, 2), (210, 22)$ (van Dijk, Granger, Page, Rubin, Silverberg, Stam, Woodruff - 2005).

- Can we find similar maps for $n = 30, 210$ with a smaller k ?

Representation for $G_{6,q}$ (Rubin, Silverberg)

$G_{6,q} \subseteq \mathbb{F}_{q^6}^*$. Choose $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, so that $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$; choose an $\mathbb{F}_q$-basis $\alpha_1, \alpha_2, \alpha_3$ of $\mathbb{F}_{q^3}$.

Then $\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^6}$.

Representation for $G_{6,q}$ (Rubin, Silverberg)

$G_{6,q} \subseteq \mathbb{F}_{q^6}^*$. Choose $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, so that $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$; choose an $\mathbb{F}_q$-basis $\alpha_1, \alpha_2, \alpha_3$ of $\mathbb{F}_{q^3}$.

Then $\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^6}$.

Define $\psi_0 : \mathbb{F}_q^3 \hookrightarrow \mathbb{F}_{q^6}^*$

$$\psi_0(u_1, u_2, u_3) = \frac{u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 + x}{u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 + x^{q^3}}.$$

Representation for $G_{6,q}$ (Rubin, Silverberg)

$G_{6,q} \subseteq \mathbb{F}_{q^6}^*$. Choose $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, so that $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$; choose an $\mathbb{F}_q$-basis $\alpha_1, \alpha_2, \alpha_3$ of $\mathbb{F}_{q^3}$.

Then $\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^6}$.

Define $\psi_0 : \mathbb{F}_q^3 \hookrightarrow \mathbb{F}_{q^6}^*$

$$\psi_0(u_1, u_2, u_3) = \frac{u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 + x}{u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 + x^{q^3}}.$$

Then $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\psi_0(u_1, u_2, u_3)) = 1$.

Let $U = \{(u_1, u_2, u_3) \in \mathbb{F}_q^3 \mid N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\psi_0(u_1, u_2, u_3)) = 1\}$.

Representation for $G_{6,q}$

$$\psi_{0\restriction U} : U \hookrightarrow G_{6,q}.$$

Representation for $G_{6,q}$

$$\psi_{0\restriction U} : U \hookrightarrow G_{6,q}.$$

By Hilbert's Theorem 90,

$$\psi_0(U) \supseteq G_{6,q} \setminus \{1\},$$

so ψ_0 restricts to an isomorphism $\psi_0 : U \xrightarrow{\sim} G_{6,q} \setminus \{1\}$.

Representation for $G_{6,q}$

$$\psi_{0\restriction U} : U \hookrightarrow G_{6,q}.$$

By Hilbert’s Theorem 90,

$$\psi_0(U) \supseteq G_{6,q} \setminus \{1\},$$

so ψ_0 restricts to an isomorphism $\psi_0 : U \xrightarrow{\sim} G_{6,q} \setminus \{1\}$. U is a surface defined by a quadratic equation, so projecting U from a generic point P gives an isomorphism

$$\mathbb{F}_q^2 \setminus S \xrightarrow{\sim} U \setminus \{P\} \xrightarrow{\sim} G_6 \setminus \{1, \psi_0(P)\}$$

for S a smaller dimensional set ($|S| \sim q$).

Example:

$$q = 2,5 \text{ mod. } 9, \;\; x = \zeta_3, \;\; y = \zeta_9 + \zeta_9^{-1},$$

$$S = \{(v_1, v_2) \in \mathbb{F}_q^2 \mid v_1^2 + v_2^2 - v_1 v_2 - 1 = 0\}$$

$$\begin{array}{ccc} \mathbb{F}_q^2 \setminus S & \longleftrightarrow & G_{6,q} \setminus \{1, \zeta_3^2\} \\ (v_1, v_2) & \longmapsto & \frac{1+v_1y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1v_2)x}{1+v_1y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1v_2)x^2} \\ \left(\frac{u_2}{u_1}, \frac{u_3}{u_1}\right) & \longleftarrow & \beta_1 + \beta_2 x \end{array}$$

where

$$(1+\beta_1)/\beta_2 = u_1 + u_2 y + u_3(y^2 - 2).$$

Arithmetic in the primitive subgroup for $n = 6$

Alternatives in $G_{6,q}$: (Granger, Page, Stam - 2004)

1. use the bijection $\mathbb{F}_q^2 \setminus S \leftrightarrow G_{6,q}$ to transfer the group law from $G_{6,q}$ to $\mathbb{F}_q^2 \setminus S$
   (Mult: 24M+43A+I, Square: 21M+38A+I)
2. arithmetic in $\mathbb{F}_{q^6}$ regarded as a degree six extension of $\mathbb{F}_q$
   (Mult: 18M+53A, Square: 6M+21A)
3. arithmetic in $\mathbb{F}_{q^6}$ regarded as a quadratic extension of a cubic extension of $\mathbb{F}_q$
   (Mult: 18M+54A, Square: 12M+33A)

Question: can these figures be improved? What about the other cases?

Representation for $G_{30,q}$

van Dijk, Woodruff - 2004: construct an almost-bijection

$$G_{30,q} \times \mathbb{F}_q^* \times \mathbb{F}_{q^6}^* \times \mathbb{F}_{q^{10}}^* \times \mathbb{F}_{q^{15}}^* \longrightarrow \mathbb{F}_{q^2}^* \times \mathbb{F}_{q^3}^* \times \mathbb{F}_{q^5}^* \times \mathbb{F}_{q^{30}}^*$$

which corresponds to a birational isomorphism

$$T_{30}(\mathbb{F}_q) \times \mathbb{F}_q^{32} \longrightarrow \mathbb{F}_q^{40}.$$

The isomorphism comes from the equation

$$\phi_{30}(x)(x-1)(x^6-1)(x^{10}-1)(x^{15}-1) =$$

$$(x^2-1)(x^3-1)(x^5-1)(x^{30}-1).$$

Representation for $G_{30,q}$

van Dijk, Granger, Page, Rubin, Silverberg, Stam, Woodruff - 2005:

using the equations

$$\phi_{30}(x)\phi_6(x) = \phi_6(x^5), \quad \phi_{210}(x)\phi_{30}(x)\phi_6(x) = \phi_6(x^{35})$$

they construct explicit bijections (defined almost everywhere)

$$G_{30,q} \times \mathbb{F}_q^2 \sim G_{30,q} \times G_{6,q} \longrightarrow G_{6,q^5} \sim \mathbb{F}_q^{10}$$

and

$$G_{210,q} \times \mathbb{F}_q^{22} \sim G_{210,q} \times G_{30,q} \times G_{6,q} \longrightarrow G_{6,q^{35}} \sim \mathbb{F}_q^{70}$$

3. Discrete Logarithm Problem

Compare the DLP in $\mathbb{F}_{q^n}^*$ and $G_{n,q}$.

- $G_{n,q} \subseteq \mathbb{F}_{q^n}^*$, so DLP in $G_{n,q}$ is at most as hard as DLP in $\mathbb{F}_{q^n}^*$.

To solve $\beta = \alpha^m$ in $\mathbb{F}_{q^n}^*$:

1. solve the DLP $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}}(\alpha)^m = N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^l}}(\beta) \in \mathbb{F}_{q^l}^*$ for each $l|n, l \neq n$
2. this determines the value of m mod.
$$lcm\{\phi_l(q)\ : l|n, l \neq n\}$$
3. remaining information comes from solving a DLP in $G_{n,q}$

- So the DLP in $G_{n,q}$ is as hard as the DLP in $\mathbb{F}_{q^n}^*$.

How often is the order of $G_{n,q}$ prime?

Gower, 2006:

as a consequence of the Bateman-Horn conjecture

$$P_{m,n}(N) = |\{p \leq N \text{ prime} \mid \phi_n(p^m) \text{ prime}\}| = o\left(\frac{N}{\log^2 N}\right)$$

N	$P_{1,6}(N)$	$P_{1,30}(N)$	$P_{2,6}(N)$	$P_{2,30}(N)$
10 000	127	103	186	63
50 000	401	379	616	228
100 000	695	669	1061	

Question: study the decomposition pattern of $\phi_n(q)$.

Gaudry's method for abelian varieties

A abelian variety of dim. d represented via equations.

$P \in A$ represented via coordinates

$$(x,y) = (x_1,\ldots,x_d,y_1,\ldots,y_e).$$

Choose equations $f_1(x,y_1), f_2(x,y_1,y_2),\ldots, f_e(x,y)$ for A (compute Gröbner basis).

Gaudry’s method for abelian varieties

A abelian variety of dim. d represented via equations.

$P \in A$ represented via coordinates

$$(x,y) = (x_1,\ldots,x_d,y_1,\ldots,y_e).$$

Choose equations $f_1(x,y_1), f_2(x,y_1,y_2),\ldots, f_e(x,y)$ for A (compute Gröbner basis).

$$\mathcal{F} = \{(x_1,0,\ldots,0,y_1,\ldots,y_e) \mid x_1,y \in \mathbb{F}_q\}$$

$\mathbb{F}_q$-rational points of a union of curves, if irreducible

$$|\mathcal{F}| = q + O(\sqrt{q})$$

$\mathcal{F}$ not contained in an abelian subvariety of A.

Gaudry’s method for abelian varieties

Decomposition on the factor base:

$$P = P_1 + \ldots + P_n, \;\; P_i \in \mathcal{F}$$
$$(x,y) = (\varphi_1(P_1,\ldots,P_n),\ldots,\varphi_{d+e}(P_1,\ldots,P_n))$$

φ_i rational functions, need to solve a system of equations (Gröbner basis computation).

Linear algebra: as usual.

Theorem: A abelian variety of dim. d over $\mathbb{F}_q$, then there is a probabilistic algorithm that solves the DLP in A with complexity $O(q^{2-2/d})$ up to logarithmic factors in q.

N.B.: constant grows fast with d.

Index calculus on G_{6,q^m}

Granger-Vercauteren, 2005:

$q^m = 2,5$ mod. 9, $S = \{(v_1, v_2) \in \mathbb{F}_{q^m}^2 \mid v_1^2 + v_2^2 - v_1 v_2 - 1 = 0\}$

$$\begin{array}{rcl} \psi : \mathbb{F}_{q^m}^2 \setminus S & \longrightarrow & G_{6,q^m} \setminus \{1, \zeta_3^2\} \\ (v_1, v_2) & \longmapsto & \frac{1+v_1 y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1 v_2)x}{1+v_1 y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1 v_2)x^2} \end{array}$$

where $x = \zeta_3, y = \zeta_9 + \zeta_9^{-1}$. $\mathbb{F}_{q^m} = \mathbb{F}_q[t]/(f(t))$

$$\mathcal{F} = \psi(t\mathbb{F}_q) = \left\{ \frac{1 + (at)y + (1 - (at)^2)x}{1 + (at)y + (1 - (at)^2)x^2} : a \in \mathbb{F}_q \right\}$$

Index calculus on G_{6,q^m}

Expected running time of the algorithm:

$$O((2m!)q(2^{12m} + 3^{2m}\log q) + m^3q^2).$$

Result of Gaudry predicts $O(q^{2-1/m})$ as $q \longrightarrow \infty$.

At least as fast as Pollard-ρ in G_{6,q^m} if $m \geq 3$.

Gröbner basis computations to decompose elements over the factor base.

$G_{30,q} \subseteq G_{6,q^5}$ so the method applies and is more efficient than Pollard-ρ.

Closing remarks:

1. using algebraic tori we can achieve a compact representation of the elements of the primitive subgroup
2. work to be done in representation of the elements and efficiency of computation
3. study the decomposition pattern of the order of these groups
4. study further the DLP

Thank you for your attention!