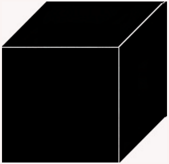
Black Box Groups

Şükrü Yalçınkaya
(joint work with Alexandre Borovik)

September 14, 2013

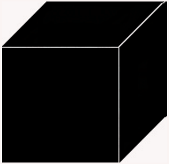
Black box groups

$$X = \langle x_1, \ldots, x_n \rangle$$



Black box groups

$$X = \langle x_1, \dots, x_n \rangle$$



- $x \cdot y$,
- x^{-1},
- $x = y$

We have a canonical projection

$$X \xrightarrow{\pi} G.$$

Examples

$X = \langle S \rangle$

- Matrix groups over finite fields
  - S a set of invertible matrices over a finite field
  - $X \leqslant \mathrm{GL}_n(q)$
  - Input length: $|S| n^2 \log q$

- Permutation groups
  - S a set of permutations of a domain Δ
  - $X \leqslant \mathrm{Sym}(\Delta)$
  - Input length: $|S||\Delta|$

Matrix Groups

Let $X = \langle x_1, \ldots, x_n \rangle \leqslant \mathrm{GL}_n(q)$ be a **big** matrix group so that $|X|$ is astronomical.

- Statistical study of random products of $x_1, \ldots, x_n$ is the only known approach to identification of X.
- Look for a 'short' and 'easy to check by random testing' first order formula which identifies X.

Verification algorithm

Let X be a black box group.
To check whether $X \not\cong G$ for a known group G.

Simplest approach:

Look for an element $x \in X$ such that $o(x) \nmid |G|$.

$$\exists x (x^{|G|} \neq 1).$$

Order oracle

- Determination of orders involves either
  - Factorization of integers into primes, or
  - Discrete logarithm problem over finite fields.

Order oracle

Let $x \in \mathrm{GL}_n(q)$.

$|x|$ is the minimal divisor d of $|\mathrm{GL}_n(q)|$ such that

$$x^d = 1.$$

Computation of x^d requires $< 2 \log d$ multiplications.

Square and multiply:

$$\begin{aligned} x^{100} &= x^{2^6+2^5+2^2} \\ &= x^{2^{2^{2^{2^{2^{2}}}}}} \cdot x^{2^{2^{2^{2^{2}}}}} \cdot x^{2^2} \end{aligned}$$

Order oracle

Way around the problem: Global exponent

Assume that we know a computationally feasible E such that $x^E = 1$ for all $x \in X$.

Factorize

$$E = 2^k m, \quad (2, m) = 1.$$

Black box group algorithms

Let X be a black box (simple) group

- Probabilistic Recognition
  - Determine the isomorphism type of X – X is $\mathrm{PSL}_2(13)$, Alt_9, etc.
- Constructive Recognition
  - Construct an explicit isomorphism between X and a known group G.

More on constructive recognition

Let X be a black box group encrypting a given group G.
An effective isomorphism

$$\varphi : G \to X$$

1. Given $g \in G$, construct efficiently the string $\varphi(g)$ representing g in X.
2. Given a string x produced by X, construct efficiently the element $\varphi^{-1}(x) \in G$ represented by x.

Obstacles in constructive recognition algorithms

Let X be a group of Lie type over a field of size q.

1. Construction of unipotent elements in X.
   - Involves selection of q randomly chosen elements.
   - Proportion of unipotent elements in Lie type groups over $\mathbb{F}_q$ is $O(1/q)$ [Guralnick and Lübeck]
   - Classical groups by Kantor and Seress.
2. Assumption of $\mathrm{SL}_2(q)$-oracle in big rank groups.
   - Discrete logarithm oracle and constructive recognition of $\mathrm{SL}_2(q)$.
   - Classical groups by Brooksbank and Kantor.
3. If X is given as a matrix group, then one needs to solve discrete logarithm problem—in $\mathbb{F}_q$, not in the prime field.

Our setup

We are given

1. A black box group X with no additional oracles, and
2. an exponent E of X, that is, $x^E = 1$ for all $x \in X$.

The decomposition $E = 2^k m$, $(m, 2) = 1$, suffices to produce efficient algorithms.

Producing involutions from random elements

Let X be a black box group,
$x \in X$ a random element,
$E = 2^k m$, m odd, a global exponent for X. Then

$$x^m, (x^m)^2, \ldots, 1 \neq (x^m)^{2^{l-1}}, 1$$
$$\mathrm{i}(x) = (x^m)^{2^{l-1}}$$

Theorem (Isaacs, Kantor, Spaltenstein)

The proportion of elements having an even order is at least 1/4 in a finite simple group of Lie type of odd characteristic.

Centralizers of involutions in black box groups (Cartan; Altseimer & Borovik; Bray)

X a black box group,
$i \in X$ an involution,
$x \in X$ a random element.

If $|ii^x| = m$ even, then $(ii^x)^{m/2}$ is an involution.

If $|ii^x| = m$ odd, then set $y := (ii^x)^{m+1/2}$. We have

$$i^y = i^x.$$

Centralizers of involutions in black box groups (Cartan; Altseimer & Borovik; Bray)

Define

$$\begin{array}{rcl} \zeta : X & \longrightarrow & C_X(i) \\ x & \mapsto & \begin{array}{ll} \zeta_0(x) = (ii^x)^{m/2}, & m = o(ii^x) \text{ even} \\ \zeta_1(x) = (ii^x)^{(m+1)/2}.x^{-1}, & m = o(ii^x) \text{ odd} \end{array} \end{array}$$

Centralizers of involutions in black box groups (Cartan; Altseimer & Borovik; Bray)

Define

$$\begin{array}{rcl} \zeta : X & \longrightarrow & C_X(i) \\ x & \mapsto & \begin{array}{ll} \zeta_0(x) = (ii^x)^{m/2}, & m = o(ii^x) \text{ even} \\ \zeta_1(x) = (ii^x)^{(m+1)/2}.x^{-1}, & m = o(ii^x) \text{ odd} \end{array} \end{array}$$

- the distribution of elements $\zeta_0(x)$ is invariant under the conjugation action of $C_X(i)$.
- the distribution of elements $\zeta_1(x)$ is invariant under the right multiplication in $C_X(i)$.

$G \cong (\mathrm{P})\mathrm{SL}_2(q)$

Let

- Let $u(t) = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$, $v(t) = \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$ where $t \in GF(q)$.
- $h(t) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}$, $n(t) = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$ where $t \in GF(q)^*$.

Definition

We call the elements $u(t), v(t), h(t)$ and $n(t)$ Steinberg generators of $G \cong \mathrm{SL}_2(q)$.

$G \cong \mathrm{(P)SL}_2(q)$

- $U = \langle u(t) \mid t \in GF(q) \rangle$ and $V = \langle v(t) \mid t \in GF(q) \rangle$ are called root subgroups.
- $H = \langle h(t) \mid t \in GF(q)^* \rangle$ is called a torus and $n(t)$ is called a Weyl group element.

Remark

- $U^{n(s)} = V$.
- $H \leq N_G(U) \cap N_G(V)$.
- *$n(s)$ inverts H, that is, $h(t)^{n(s)} = h(t^{-1})$.*

An algorithm for $G \cong \mathrm{(P)SL}_2(q)$, $q \equiv 1 \bmod 4$

Let $q = p^k$ for some $k \geq 1$, p prime.

1. Construct $\mathrm{(P)SL}_2(p) \cong G_0 \leq G$.
2. Construct a unipotent element $u \in G_0$.
3. Construct the torus T normalising the root subgroup containing u and the Weyl group element w inverting T.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

Then

- $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \leq G_0 \cong \mathrm{PSL}_2(p)$.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

Then

- $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \leq G_0 \cong \mathrm{PSL}_2(p)$.
- L is a maximal subgroup of G_0 or $L < \mathrm{Sym}_4 < \mathrm{G}_0$.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

Then

- $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \leq G_0 \cong \mathrm{PSL}_2(p)$.
- L is a maximal subgroup of G_0 or $L < \mathrm{Sym}_4 < \mathrm{G}_0$.
- $t \in G_0$.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

Then

- $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \leq G_0 \cong \mathrm{PSL}_2(p)$.
- L is a maximal subgroup of G_0 or $L < \mathrm{Sym}_4 < \mathrm{G}_0$.
- $t \in G_0$.
- If $|t| = (p \pm 1)/2 \geq 5$, then $\langle t, x \rangle = G_0$.

$G_0 \cong \mathrm{PSL}_2(p) \leq \mathrm{PSL}_2(q) \cong G$

Let

- t be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even;
- $s \in \langle t \rangle$ be the involution;
- $r \in G$ an involution which inverts t; and
- $x \in G$ an element of order 3 which normalises $\langle s, r \rangle$.

Then

- $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \leq G_0 \cong \mathrm{PSL}_2(p)$.
- L is a maximal subgroup of G_0 or $L < \mathrm{Sym}_4 < \mathrm{G}_0$.
- $t \in G_0$.
- If $|t| = (p \pm 1)/2 \geq 5$, then $\langle t, x \rangle = G_0$.
- Hence if $p \neq 5, 7$, then $\langle t, x \rangle \cong \mathrm{PSL}_2(p)$.

The element $x \in N_G(\langle r, s\rangle)$

Let $V = \{1, i, j, k\}$ be a Klein 4-subgroup and $g \in G$ be a random element.
Assume that

- ij^g has odd order m_1 and set $u_1 = (ij^g)^{\frac{m_1+1}{2}}$;
- $jk^{gu_1^{-1}}$ has odd order m_2 and set $u_2 = (jk^{gu_1^{-1}})^{\frac{m_2+1}{2}}$.

Then

- $j^{gu_1^{-1}} = i$ and $j = k^{gu_1^{-1}u_2^{-1}}$.
- $k^{gu_1^{-1}} \in C_G(i)$, and so $u_2 \in C_G(i)$.
- $j^{gu_1^{-1}u_2^{-1}} = i$.

Hence, putting $x = gu_1^{-1}u_2^{-1}$, we have

$$k^x = j, j^x = i, i^x = k.$$

Unipotent elements in $G \cong \mathrm{PSL}_2(p)$, $p \equiv 1 \bmod 4$

Lemma

Let $i \in G$ be an involution.

1. *There exists an element $g \in G$ such that ii^g has order p.*
2. *The probability that ii^g has order p for a random element $g \in G$ is at least $1/p$.*

Let $u = ii^g$ be a unipotent element for some random $g \in G$ and $U = \langle u \rangle$.

Unipotent elements in $G \cong \mathrm{PSL}_2(p)$, $p \equiv 1 \bmod 4$

Lemma

Let $i \in G$ be an involution.

1. *There exists an element $g \in G$ such that ii^g has order p.*
2. *The probability that ii^g has order p for a random element $g \in G$ is at least $1/p$.*

Let $u = ii^g$ be a unipotent element for some random $g \in G$ and $U = \langle u \rangle$.

Remark

If $p \equiv -1 \bmod 4$, then we construct $G_0 \cong \mathrm{PSL}_2(p^2)$ instead of $\mathrm{PSL}_2(p)$.

Torus in $G \cong \mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$

Let $u = ii^g$ be a unipotent element and $U = \langle u \rangle$.

Fact

There is a unique torus T containing a given involution $i \in G$. In particular, $T < C_G(i)$.

Lemma

$T < N_G(U)$.

Weyl group element in $G \cong \mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$

Let $u = ii^g$ be a unipotent element and $U = \langle u \rangle$ and $T < C_G(i)$. We have

$$C_G(i) = T \rtimes \langle w \rangle$$

where w is an involution inverting T.

Steinberg generators of $\mathrm{PSL}_2(q)$

Hence the elements

$$u, t, w$$

are the Steinberg generators of G where t is a generator of T.

Algorithm for $(\mathrm{P})\mathrm{SL}_2(q)$, $q \equiv 1 \bmod 4$

Theorem

Let X be a black box group encrypting $(\mathrm{P})\mathrm{SL}_2(q)$, where $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. Then there is a Monte-Carlo algorithm which constructs in X strings u, h, n such that there exists an isomorphism

$$\Phi : X \longrightarrow (\mathrm{P})\mathrm{SL}_2(q)$$

with

$$\Phi(u) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \Phi(h) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \Phi(n) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

where t is some primitive element of the field $\mathbb{F}_q$.
The running time of the algorithm is quadratic in p and polynomial in $\log q$.

Steinberg generators for classical groups of higher rank

Let G be a quasi-simple classical group of odd characteristic.

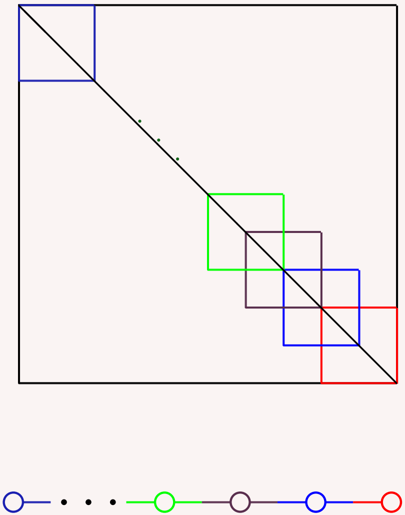
Let $\{K_0, K_1, \ldots, K_n\}$ be an extended Curtis-Tits system of G.

Remark

$K_i \cong (\mathrm{P})\mathrm{SL}_2(q)$.

Coordinated construction of the corresponding toral and Weyl group elements...

Curtis-Tits system for SL_n



Theorem

Let X be a black box classical group encrypting one of the groups $\mathrm{(P)SL}_{n+1}(q)$, $\mathrm{(P)Sp}_{2n}(q)$, $\mathrm{(P)}\Omega^{+}_{2n}(q)$ or $\Omega_{2n+1}(q)$ where $q \equiv 1 \bmod 4$. Then there is an algorithm which constructs

- *black boxes for an extended Curtis-Tits system $\{K_0, K_1, \ldots, K_n\}$ of X;*
- *black boxes for root subgroups $U_\ell < K_\ell$;*
- *a black box for a maximal torus T where $T < N_X(U_\ell)$;*
- *Weyl group elements $w_\ell \in K_\ell$, where $U_\ell^{w_\ell}$ is the opposite root subgroup of U_ℓ for all $\ell = 0, 1, \ldots, n$.*

The running time of the algorithm is quadratic in the characteristic p of the underlying field, and is polynomial in the Lie rank n of X and $\log q$.

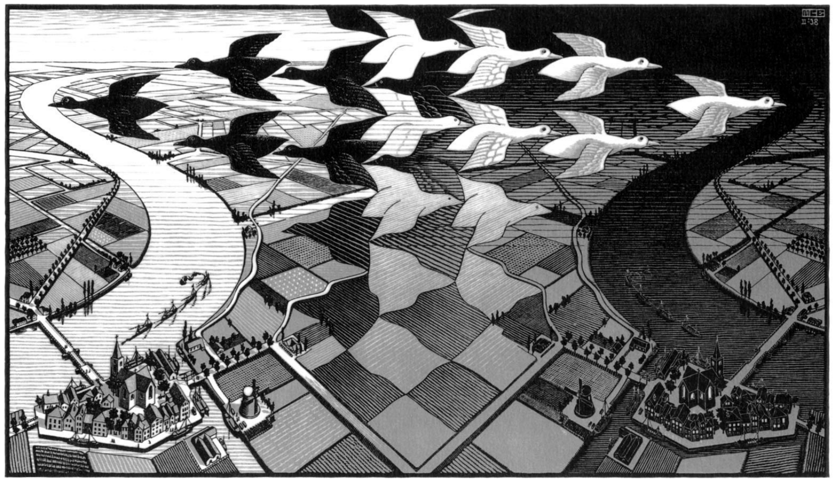
Morphisms of black box groups

- Morphisms are efficiently computable homomorphisms.
- Given X encrypting G, we find, in time polynomial in $\log |X|$, a cover $X \longleftarrow Y$ with better properties.
- Eventually reach

$$X \longleftarrow Y_1 \longleftarrow \ldots \longleftarrow Y_n = G,$$

an efficiently given group.

M.C. Escher, Day and Night, 1938



Automorphisms of black box groups

Let X be a black box group encrypting G.
Let $X = \langle x_1, y_1, z_1 \rangle = \langle x_2, y_2, z_2 \rangle$, so $\pi(x_i, y_i, z_i)$ generate G.
Assume that the map

$$\begin{array}{rccc} \pi: & x_1 \mapsto \pi(x_2) & y_1 \mapsto \pi(y_2) & z_1 \mapsto \pi(z_2) \\ & x_2 \mapsto \pi(x_1) & y_2 \mapsto \pi(y_1) & z_2 \mapsto \pi(z_1) \end{array}$$

extends to an automorphism ϕ of G.
Then, the black box group Y generated in $X \times X$ by the strings

$$(x_1, x_2), (y_1, y_2), (z_1, z_2)$$

encrypts G and possesses an unary operation, cyclic shift

$$\begin{array}{rcl} \alpha : Y & \longrightarrow & Y \\ (y_1, y_2) & \mapsto & (y_2, y_1) \end{array}$$

encrypting the automorphism ϕ of G.

Automorphisms

Theorem

Let X be a black box group encrypting a Lie type group $G(q)$, q odd and $q > 7$. Then we can construct, in polynomial in $\log q$ and the Lie rank of G, a cover

$$X \longleftarrow Y$$

where a black box group Y also encrypts $G(q)$ and has additional unary operations representing field and graph automorphisms of $G(q)$.

Frobenius map on $\mathrm{SL}_2(q)$

$$F : \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \mapsto \begin{bmatrix} a_{11}^p & a_{12}^p \\ a_{21}^p & a_{22}^p \end{bmatrix}.$$

Frobenius map on $\mathrm{SL}_2(q)$

$$F : \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \mapsto \begin{bmatrix} a_{11}^p & a_{12}^p \\ a_{21}^p & a_{22}^p \end{bmatrix}.$$

On Steinberg generators:

1. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{F^i} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$
2. $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{F^i} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$
3. $\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}^{F^i} = \begin{bmatrix} t^{p^i} & 0 \\ 0 & t^{-p^i} \end{bmatrix} = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}^{p^i}.$

Frobenius automorphism without unipotents

Let X be black box group encrypting $G = \mathrm{PSL}_2(q)$ and F a Frobenius automorphism on G.

- $i \in T < G$ be an involution.
- $j \in G$ an involution inverting T, $C_G(j) = S \rtimes \langle k \rangle$ where k inverts S.
- $E = \langle i, j \rangle < H = \mathrm{PSL}_2(p)$.
- T and S are conjugate by an element from H.
- F fixes E and leaves invariant T and S.
- F acts on T and S as power maps

$$\alpha_i : c \mapsto c^{\epsilon p},\ p \equiv \epsilon \bmod 4.$$

- In the images X_1 and X_2 of T and S, the maps

$$\Phi_i : x \mapsto x^{\epsilon p}$$

encrypt the restrictions of F to T and S.

Frobenius map on Lie type groups

Theorem

Let X be a black box encrypting a untwisted simple group of Lie type $G = G(p^k)$ over a field of order $q = p^k$ and $k > 1$. Then, we can construct, in polynomial in $\log|G|$,

- *a black box Y encrypting G,*
- *a morphism $X \longrightarrow Y$, and*
- *a morphism $\Phi : Y \longleftarrow Y$ which encrypts a Frobenius automorphism of G induced by the map $x \mapsto x^p$ on the field $\mathbb{F}_q$.*

Black box fields

Assume that $G = \mathrm{SL}_2(p^k)$.

1. Let $u, h, n \in G$ be unipotent, toral and Weyl group elements.
2. $U = \langle u \rangle^{\langle h \rangle} \cong \mathbb{F}_{p^k}^+$.
3. We shall construct a field structure $\mathbf{U}$ on U.
4. Addition: If $u_1, u_2 \in U$, then define

$$u_1 \oplus u_2 := u_1 u_2.$$

Black box fields

5. Multiplication:
   5.1 Set $u := \mathbf{1} \in \mathbf{U}$.
   5.2 Assumet that h has odd order m and set $\sqrt{h} = h^{(m+1)/2}$.
   5.3 Notice that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\begin{bmatrix} \sqrt{t} & 0 \\ 0 & \sqrt{t^{-1}} \end{bmatrix}} = \begin{bmatrix} 1 & t^{-1} \\ 0 & 1 \end{bmatrix}.$$

   5.4 Set $s := u^{\sqrt{h}}$, so s corresponds to t^{-1} in $\mathbf{U}$.
   5.5 Set $s^i = u^{(\sqrt{h})^i}$, $i = 1, 2, \ldots, k$.
   5.6 The elements $s, s^2, \ldots, s^k$ form a polynomial basis of $\mathbf{U}$ on $\mathbb{F}_p$.
   5.7 For $w \in U$, define

$$w \otimes s^i = w^{(\sqrt{h})^i}$$

and expand it linearly.

Black box fields

5. Multiplication continues:

5.8 Let F be the Frobenius map on U. Define the Frobenius trace $Tr : U \to \mathbb{F}_p$:

$$Tr(x) = x \oplus x^F \oplus \ldots \oplus x^{F^{k-1}},$$

and the trace form

$$\langle x, y \rangle = Tr(x \otimes y).$$

5.9 Compute the matrix $A = (a_{ij})$ where $a_{ij} = \langle s^i, s^j \rangle$.

5.10 If $w \in \mathbf{U}$, then $w = \alpha_1 s \oplus \alpha_2 s^2 \oplus \ldots \oplus \alpha_k s^k$. Computing $\beta_j = \langle w, s^j \rangle$, $j = 1, 2, \ldots, k$, we have

$$(\alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_k) A^{-1}.$$

5.11 Compute the structure constants $s^i \otimes s^j = \sum_{l=1}^{k} c_{ijl} s^l$.

Structure recovery

- Construction of a black box field $\mathbb{K}$ and an isomorphism

$$\mathbb{F}_q \longrightarrow \mathbb{K}.$$

- A probabilistic polynomial time morphism

$$G(q) \longrightarrow G(\mathbb{K}) \longrightarrow X.$$

Structure recovery

- Construction of a black box field $\mathbb{K}$ and an isomorphism

$$\mathbb{F}_q \longrightarrow \mathbb{K}.$$

- A probabilistic polynomial time morphism

$$G(q) \longrightarrow G(\mathbb{K}) \longrightarrow X.$$

Theorem

Let X be a black box group encrypting the group $(\mathrm{P})\mathrm{SL}_2(q)$, $q \equiv 1 \bmod 4$. Then there exists a Monte–Carlo algorithm constructing a structure recovery for X in time quadratic in the characteristic and polynomial in $\log q$.

Structure recovery in even characteristic

Structure recovery in even characteristic

Theorem

Let X be a black box group encrypting the group $(\mathrm{P})\mathrm{SL}_2(2^n)$. We assume that we are given an involution $u \in X$. Then there exists a Monte–Carlo algorithm constructing a structure recovery for X in time polynomial in n.

Inverse transpose map

Let $G = \mathrm{SL}_n(q)$ and φ denote the inverse transpose automorphism.

Fact

1. *If $n = 2$, then φ is an inner automorphism.*
2. *Otherwise, φ is not inner.*

Observe that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{\varphi} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}.$$

Inverse transpose map

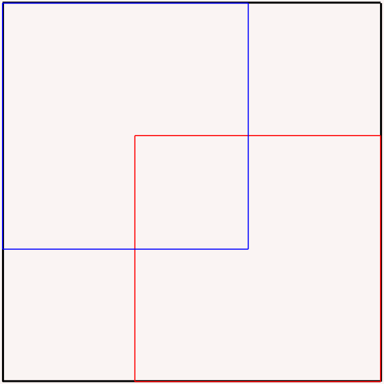
w	*Quadratic form*
$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$x^2 + y^2$
$\begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$	$x^2 + t^2 y^2$

$\mathrm{SU}_3(q) < \mathrm{SL}_3(q^2)$

Let $X = \mathrm{SL}_3(q^2)$ and $Y = \mathrm{SU}_3(q)$.
Let φ denote the inverse transpose map and F Frobenius map corresponding to $a \mapsto a^q$.
Then $\varphi \circ F$ is an automorphism of order 2 and

$$X_{\varphi \circ F} = Y.$$

$\mathrm{SU}_3(q) < \mathrm{SL}_3(q^2)$



Beautiful constructions

1. $G_2(q) < \Omega_7(q) < \Omega_8^+(q) < SL_8(q) < E_8(q)$.
2. ${}^3D_4(q) < \Omega_8^+(q) < SL_8(q) < E_8(q)$.
3. $\mathrm{Sp}_{2n}(q) < \mathrm{SU}_{2n}(q) < \mathrm{SL}_{2n}(q^2)$.

and more...