Black Box Groups

Alexandre Borovik
(joint work with Şükrü Yalçınkaya)

Groups, Rings, and their Automorphisms, Lincoln
31th August – 2nd September 2016

31 August 2016
A modest offering: some \( p \)-elements (when they are a rarity)

**Question, Babai and Beals, 1999:** Given a few \( n \times n \) matrices \( x_1, \ldots, x_l \) over \( \mathbb{F}_{p^k} \) which generate \( X \cong \text{SL}_2(\mathbb{F}_{p^m}) \),

\[
\text{SL}_2(\mathbb{F}_{p^m}) \cong X = \langle x_1, \ldots, x_l \rangle \leq \text{GL}_n(\mathbb{F}_{p^k})
\]

find a non-trivial unipotent (that is, of order \( p \)) element in \( X \) in time polynomial in \( n, k, \) and \( \log p \).

**Answer, B and Yalçınkaya:** Done
Tested on groups such as \( \text{SL}_2(\mathbb{F}_{5463458053}) \).
Analogy with Lie group

When probed at ‘random’, groups of this size behave as if they are compact Lie groups.

Unipotent elements are nowhere to be found.

Probability of a random element in $\text{SL}_2(\mathbb{F})$ to be unipotent is

\[ \approx \frac{1}{|\mathbb{F}|} \]
A lesson from our study

We were lucky to treat the analogy with Lie groups with respect.

$$SO_3(\mathbb{R}) \nless \neq PGL_2(\mathbb{R}) = SO_{2,1}(\mathbb{R})$$

$$SO_3(\mathbb{F}_p) \simeq PGL_2(\mathbb{F}_p) = SO_{2,1}(\mathbb{F}_p)$$

Euclidean space vs. Lobachevsky space

The solution needs to be found at the level of geometry.
We were lucky to return back to the Babai-Szemeredi Axioms of 1984 and start from there.

\[
\begin{align*}
\text{black box} & \quad X \quad \overset{\pi}{\longrightarrow} \quad G \quad \text{encrypted group} \\
\text{strings} & \quad x \cdot y, \quad x^{-1}, \quad x = y \quad \text{random}
\end{align*}
\]
From finite groups to compact Lie groups

**BB1** \( X \) produces strings of fixed length \( l(X) \) encrypting random (almost) uniformly distributed elements from \( G \).

**BB2** \( X \) computes, in time polynomial in \( l(X) \), a string encrypting the product of two group elements given by strings or a string encrypting the inverse of an element given by a string.

**BB3** \( X \) decides, in time polynomial in \( l(X) \), whether two strings encrypt the same element in \( G \)—therefore identification of strings is a canonical projection

\[
\begin{array}{ccc}
X & \overset{\pi}{\longrightarrow} & G.
\end{array}
\]

**C** \( X \) extracts random square roots \( \sqrt{x} \) in \( \langle x \rangle \) (when they exist).
The letter $C$ in this axiom:

$C \; X$ extracts random square roots $\sqrt{x}$ in $\langle x \rangle$ (when they exist).

is for Élie Cartan (1869 – 1951).

I will return to that later.
This axiom is applicable to matrix groups over finite fields as well as to Lie groups.
More general result

**B and Yalçınkaya**: Let $X$ be a black box group encrypting a single-bonded (that is, type A, D, or E) simple algebraic group $G(F)$ with over a finite field of odd order. Assume that we are given the type of $G$ and the order of $F$. Then we can construct, in time polynomial in $\log |G(F)|$, a BB field $K$ and polynomial time homomorphisms

$$G(F) \to G(K) \leftrightarrow X$$

Other types of $G$: work in progress.
Groups of Lie type: separation of the functor from the field

- Groups of Lie type are functors from fields to groups.
- Almost all our computations involve subtle structures of ‘functorial’ nature, but do not use fields.
- Fields appear at much later stages of analysis, while the Weyl group features prominently from the beginning.

Interesting implications for cryptography.
Everything is a black box

In the ZF set theory, everything is a set, with some sets happen to be elements of other sets.

In the BB theory, everything is a black box; the strings that it produces are pointers to other black boxes.

Projective plane in $\text{PGL}_2(\mathbb{F}_q)$:

- **point** is (a **pointer** to) a black box producing random lines incident to this point
- **line** is (a **pointer** to) a black box producing random points incident to this line
Abstraction is Freedom

**Projective plane** in $\text{PGL}_3(\mathbb{F}_q)$:

- **point** is an involution with the label ‘*this is a point*’
- **line** is an involution with the label ‘*this is a line*’

**Axiom BB3:**

- A Black Box decides whether two strings encrypt the same element
- involutions are the same, but criteria of
  - being the same point
  - being the same line
  are different

Axiomatic approach gives us freedom to construct new black boxes from old ones.
Morphisms

Maps $\zeta : X \rightarrow Y$ computable in probabilistic time polynomial in $l(X)$ and $l(Y)$ which make the diagram commutative:

\[
\begin{array}{c}
X \overset{\zeta}{\rightarrow} Y \\
\downarrow \pi_X \quad \quad \quad \downarrow \pi_Y \\
G \overset{\phi}{\rightarrow} H
\end{array}
\]

We say that a morphism $\zeta$ encrypts the homomorphism $\phi$. 
Theorem (Lenstra Jr 1991; Maurer and Raub 2007)

Let $K$ and $L$ be black box fields encrypting the same finite field and $K_0$, $L_0$ their prime subfield. Then a morphism

$$K_0 \rightarrow L_0$$

can be extended, with the help of a polynomial time construction, to a morphism

$$K \rightarrow L.$$

In particular, for small primes $p$, every black box field of order $p^n$ is effectively isomorphic to $\mathbb{F}_{p^n}$. 
BB subgroups are morphisms

When we

• have a generating set \( y_1, \ldots, y_k \) for \( Y \leq X \), and

• sample the “product replacement algorithm” (or something similar), for \( Y \)

we deal with a morphism

\[ Y \hookrightarrow X. \]
Morphisms are BB subgroups

\[ \phi \]
\[ \begin{array}{c}
G \\
\downarrow \phi \\
H
\end{array} \]

is a homomorphism if and only if its graph

\[ F = \{(g, \phi(g)) : g \in G\} \]

is a subgroup of \( G \times H \).

\[ \zeta \]
\[ \begin{array}{c}
X \\
\downarrow \zeta \\
Y
\end{array} \]

is a BB subgroup \( Z \hookrightarrow X \times Y \) encrypting \( F \):

\[ Z = \{(x, \zeta(x)) : x \in X\} \]

with the natural projection

\[ \pi_Z : Z \rightarrow F \]

\[ (x, \zeta(x)) \mapsto (\pi_X(x), \phi(\pi_X(x))). \]
If $X$ is a BB group and $x \in X$, what kind of a black box we have to associate with $x$?

The black box

$$Z \leftrightarrow X \times X$$

for the graph of the inner automorphism

$$X \rightarrow X$$

$$y \mapsto y^x$$
Protomorphisms

A protomorphism is a BB subgroup $Z \hookrightarrow X \times Y$

$$Z = \{(x, \zeta(x)) : x \in X\}$$

encrypting the graph

$$F = \{(g, \phi(g)) : g \in G\} \triangleleft G \times H$$

of a homomorphism

$$G \xrightarrow{\phi} H$$

with no assumptions on computational complexity of $\phi$ and $\zeta$. 
Protomorphisms

• Every morphism is a protomorphism.

• The concept of protomorphism is much weaker than that of morphism, but it gives freedom of doing things.

• It fits well into ‘physical’ intuition as an ‘observation’ or ‘measurement’ followed by inter- or extrapolation.
Homomorphic encryption

\[ \mathcal{P} \text{ and } \mathcal{C} \text{ are sets of plaintexts and ciphertexts, respectively, and assume that we have some (say, binary) operators } \sqcap_{\mathcal{P}} \text{ on } \mathcal{P} \text{ and } \sqcap_{\mathcal{C}} \text{ on } \mathcal{C}. \]

An encryption function \( E \) is homomorphic if

\[ E(p_1 \sqcap_{\mathcal{P}} p_2) = E(p_1) \sqcap_{\mathcal{C}} E(p_2) \]

for all plaintexts \( p_1, p_2 \).
Alice, Bob, Clair

**Alice**: she encrypts plaintexts $p_1$ and $p_2$ and sends ciphertexts $E(p_1)$ and $E(p_2)$ to Bob.

**Bob** computes

$$q = E(p_1) \boxdot_c E(p_2)$$

and return $q$ to Alice

**Alice**: decrypts:

$$E^{-1}(q) = p_1 \boxdot_P p_2$$

Motivation: “cloud computing”. A big thing in the industry, but not very successful.
Impersonation attack

Assume that Clair controls the line and can impersonate both Alice and Bob.

- Then Clair has access to the graph of $E$ as a black box.
- If the ambient structure is $\text{PSL}_2(\mathbb{F})$, Clair can construct the map
  
  $\mathcal{G}(\mathbb{F}) \rightarrow \mathcal{G}(K) \leftrightarrow X$

  and . . .
- . . . send to Alice encrypted plaintext of her choice.
Moral of our story

Finite groups of Lie type used as ambient structure for cryptographic primitives are unlikely to be more secure than finite fields.
Lie groups as BB groups

- Imagine a communication, over the telephone, between BY (Borovik and Yalcinkaya) and MN (Mother Nature).
- MN knows the structure of the universe, in the form of a connected simple Lie group $X$.
- BY know that $X$ is a connected simple Lie group.
- BY can ask MN to produce random elements from $X$ and manipulate with them on their request.
BY: produce a random element from the group, call it $x$
MN: done
BY: take $\sqrt{x}$, call it $r$
MN: done
BY: take $\sqrt{x}$, call it $s$
MN: done
BY: compute $A = rs^{-1}$
MN: done
BY: is $A = 1$?
MN: no
BY: is $A^2 = 1$?
MN: yes
**B-Yalcinkaya:** If $X$ is compact, the type of $X$ can be determined in (probabilistically polynomial in rank $X$) many questions.

**B-Yalcinkaya:** The same is true for BB groups $X$ encrypting Lie type groups over fields of odd characteristic.
The Cartan decomposition

Construction of centralisers of involutions in Lie groups happened to be a reformulation of

Cartan decomposition

associated with involutions of Lie algebras (Élie Cartan 1869 – 1951).
The Lie groups analogue of construction of an unipotent element in $\text{PSL}_2(q)$:

Distinguish between $\text{SO}_3(\mathbb{R})$ and $\text{PSL}_2(\mathbb{C})$.

The real fun starts here.
From $\mathbb{F}_q$ to $\mathbb{C}$

**Foldes (2008):** $\text{PSL}_2(\mathbb{C})$ is “locally approximated” (in some explicit metric sense) by $\text{PSL}_2(p)$ for large primes $p$.

Continues attempts (Kustaanheimo, Coish, Ahmavaara et al.) to develop a formalism for quantum theory based on a large finite field: $\text{PSL}_2(\mathbb{C})$ is the orthochronous proper Lorentz group of the Minkowski space-time of special relativity theory.

**Zilber (2012):**
- $\mathbb{C}$ with respect to the Zariski language is approximable by finite fields.
- No locally compact field, other than algebraically closed, is approximable by finite fields.
Given: $\mathbf{K}$ encrypts $SO_3(\mathbb{R})$, $PGL_2(\mathbb{C})$, or $PGL_2(\mathbb{F}_{p^2})$.

Aim: construct an unipotent element.

\[
PGL_2(\mathbb{F}_{p^2}) \simeq SO_{2,1}(\mathbb{F}_{p^2});
\]

\[
PGL_2(\mathbb{C}) \simeq SO_{3,1}(\mathbb{R})
\]
Geometry of involutions, continued

- start producing involutions;
- involutions \( s, t \) define a line \( s \lor t \);
- polar points

\[ \pi(s \lor t) \]

and intersections of lines

\[ (s \lor t) \land (s' \lor t') \]

are found by reification of involutions;
- every step works with probability 1 or astronomically close to 1;
- we converge on the projective Euclidean geometry expressed by drawings;
- coordinatise the geometry by a BB field \( K \);
- finding an unipotent element amounts to hitting a singular (where the quadratic form vanishes)
Finding a unipotent element $x = (x_1, x_2, 1)$ means solving

$$x_1^2 + x_2^2 + 1 = 0.$$ 

which is always possible in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Get to the coordinate $x_1$ and $x_2$ by doubling and adding method starting with the unity of $\mathbb{K}$ . . .

. . . until your Euclidean world collapses (due to division by zero)

and you find yourself in the 2-dimensional cross section (because out computation is confined to the prime subfield of $\mathbb{K}$) of Minkowski space, that is, in the Lobachevsky plane.
In the Minkowski space

Translated into the Minkowski space, this construction amounts to constructing a light vector (that is, a vector on the light cone) by summing up fixed ‘microscopic’ magnitudes.

Constructing photons? ???
Adding quanta quantum by quantum???
Sometimes ‘NO’ is more precious than ‘YES’

**Question.** Asking questions to Mother Nature, can we distinguish between

\[ \text{SO}_3(\mathbb{R}) \quad \text{and} \quad \text{PSL}_2(\mathbb{C})? \]