Polynomial time cryptanalysis of the Commutator Key Exchange Protocol

Boaz Tsaban

Bar-Ilan University

Symbolic Computations and Post-Quantum Crypto Seminar
18 Oct '12

Key Exchange Protocols (KEPs)

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

$\exists$ Efficient & secure methods if they share a secret ("key"): Symmetric encryption (AES,…).

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

$\exists$ Efficient & secure methods if they share a secret (“key”): Symmetric encryption (AES,. . .).

How to decide a shared secret key over an insecure channel?

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

$\exists$ Efficient & secure methods if they share a secret ("key"):
Symmetric encryption (AES,...).

How to decide a shared secret key over an insecure channel?

Diffie–Hellman 1976. Key Exchange Protocol.

The most important breakthrough in cryptography.

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

$\exists$ Efficient & secure methods if they share a secret ("key"):
Symmetric encryption (AES,...).

How to decide a shared secret key over an insecure channel?

Diffie–Hellman 1976. Key Exchange Protocol.

The most important breakthrough in cryptography.

In this lecture: Only passive adversaries.
The kernel on which more involved PKC is built.

The Diffie–Hellman KEP

The Diffie–Hellman KEP

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle,\ \lvert G \rvert = p$	$b \in \{0, 1, \ldots, p-1\}$

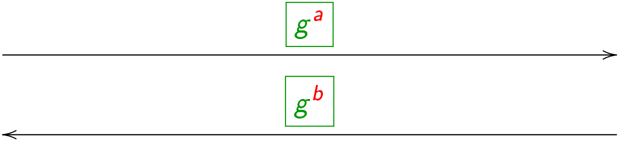
$$\xrightarrow{\boxed{g^{a}}}$$

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

$K = {\boxed{g^{b}}}^{a} = g^{ab}$	$K = {\boxed{g^{a}}}^{b} = g^{ab}$

The Diffie–Hellman KEP

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle, \; \lvert G \rvert = p$	$b \in \{0, 1, \ldots, p-1\}$



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

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

$K = \boxed{g^b}^{a} = g^{ab}$	$K = \boxed{g^a}^{b} = g^{ab}$

$$\underbrace{g^x \mapsto x}_{\text{Discrete Logarithm Problem}} \geq \underbrace{(g^a, g^b) \mapsto g^{ab}}_{\text{Diffie–Hellman Problem (DHP)}}$$

The Discrete Logarithm Problem

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

$G = (\mathbb{Z}_p, +)$. $g = 1$. "g^x" $= x \cdot g = x \cdot 1 = x$.

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

$G = (\mathbb{Z}_p, +)$. $g = 1$. "g^x" $= x \cdot g = x \cdot 1 = x$.

$G \leq (\mathbb{Z}_p^*, \cdot)$. Quite, but not enough, hard:

NFS. $n := \log_2(p)$: $\mathbf{2}^{(1.33 + o(1)) n^{1/3} (\log_2 n)^{2/3}}$.

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

$G = (\mathbb{Z}_p, +)$. $g = 1$. "g^x" $= x \cdot g = x \cdot 1 = x$.

$G \leq (\mathbb{Z}_p^*, \cdot)$. Quite, but not enough, hard:

NFS. $n := \log_2(p)$: $\mathbf{2}^{(1.33+o(1))n^{1/3}(\log_2 n)^{2/3}}$.

n	NFS Work Prediction	Year Broken
525	2^{47}	2002
578	2^{49}	2003
664	2^{52}	2005
768	2^{55}	2009
1024	2^{62}	2016?

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

$G = (\mathbb{Z}_p, +)$. $g = 1$. "g^x" $= x \cdot g = x \cdot 1 = x$.

$G \leq (\mathbb{Z}_p^*, \cdot)$. Quite, but not enough, hard:

NFS. $n := \log_2(p)$: $\mathbf{2}^{\,(1.33 + o(1)) n^{1/3} (\log_2 n)^{2/3}}$.

n	NFS Work Prediction	Year Broken
525	2^{47}	2002
578	2^{49}	2003
664	2^{52}	2005
768	2^{55}	2009
1024	2^{62}	2016?

$10,000$ bits prime for "eternal" security? Impractical.

The future of cryptography

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\to \cdots \to$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

But what is your alternative?

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

But what is your alternative?

Rivest-Shamir-Adleman (RSA, 1978). As easy as DLP in $\mathbb{Z}_p^*$.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

But what is your alternative?

Rivest-Shamir-Adleman (RSA, 1978). As easy as DLP in $\mathbb{Z}_p^*$.

Lattice-based? Maybe.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\to \cdots \to$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

But what is your alternative?

Rivest-Shamir-Adleman (RSA, 1978). As easy as DLP in $\mathbb{Z}_p^*$.

Lattice-based? Maybe.

How about noncommutative groups?

The Braid Diffie–Hellman KEP

Diffie–Hellman KEP 1976.

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle, \ \lvert G \rvert = p$	$b \in \{0, 1, \ldots, p-1\}$

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

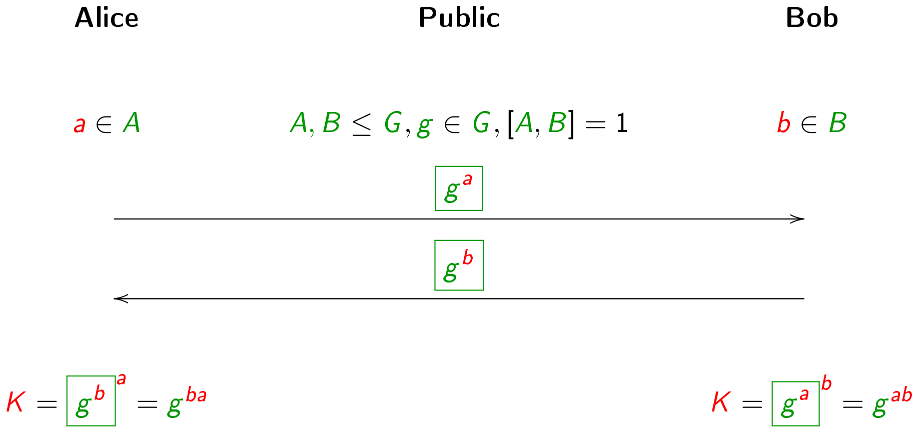
$$\xleftarrow{\quad \boxed{g^{b}} \quad}$$

$$K = \boxed{g^{b}}^{a} = g^{ab} \qquad\qquad K = \boxed{g^{a}}^{b} = g^{ab}$$

The Braid Diffie–Hellman KEP

Ko–Lee–Cheon–Han–Kang–Park 2000. G noncommutative.

$g^x := x^{-1}gx$.



Alice **Public** **Bob**

$a \in A$ $A, B \leq G, g \in G, [A, B] = 1$ $b \in B$

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

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

$K = \boxed{g^b}^{a} = g^{ba}$ $K = \boxed{g^a}^{b} = g^{ab}$

The braid group $\mathbf{B}_N$

The braid group $\mathbf{B}_N$

For our purposes, $\mathbf{B}_N$ is a group with elements

$$(i, p_1, \ldots, p_\ell),$$

$i \in \mathbb{Z}, \ell \in \mathbb{N} \cup \{0\}, p_1, \ldots, p_\ell \in S_N$,
satisfying certain properties.

The braid group $\mathbf{B}_N$

For our purposes, $\mathbf{B}_N$ is a group with elements

$$(i, p_1, \ldots, p_\ell),$$

$i \in \mathbb{Z}, \ell \in \mathbb{N} \cup \{0\}, p_1, \ldots, p_\ell \in S_N$,
satisfying certain properties.

Multiplication rule: Algorithm of complexity $N\ell^2$.

The braid group $\mathbf{B}_N$

For our purposes, $\mathbf{B}_N$ is a group with elements

$$(i, p_1, \ldots, p_\ell),$$

$i \in \mathbb{Z}, \ell \in \mathbb{N} \cup \{0\}, p_1, \ldots, p_\ell \in S_N$,
satisfying certain properties.

Multiplication rule: Algorithm of complexity $N\ell^2$.

We always ignore logarithmic factors.

The braid group $\mathbf{B}_N$

For our purposes, $\mathbf{B}_N$ is a group with elements

$$(i, p_1, \ldots, p_\ell),$$

$i \in \mathbb{Z}, \ell \in \mathbb{N} \cup \{0\}, p_1, \ldots, p_\ell \in S_N$,
satisfying certain properties.

Multiplication rule: Algorithm of complexity $N\ell^2$.

We always ignore logarithmic factors.

Inversion: Even faster.

The braid group $\mathbf{B}_N$

For our purposes, $\mathbf{B}_N$ is a group with elements

$$(i, p_1, \ldots, p_\ell),$$

$i \in \mathbb{Z}, \ell \in \mathbb{N} \cup \{0\}, p_1, \ldots, p_\ell \in S_N$,
satisfying certain properties.

Multiplication rule: Algorithm of complexity $N\ell^2$.

We always ignore logarithmic factors.

Inversion: Even faster.

Security parameters: $m := |i| + \ell$, N.

The Braid Diffie–Hellman KEP

The Braid Diffie–Hellman KEP

$G = \mathbf{B}_N$.

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$

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

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

$$K = \boxed{g^{b}}^{a} = g^{ba}$$

$$K = \boxed{g^{a}}^{b} = g^{ab}$$

The Braid Diffie–Hellman KEP

$G = \mathbf{B}_N$.

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$

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

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

$K = \boxed{g^b}^a = g^{ba}$

$K = \boxed{g^a}^b = g^{ab}$

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Faithful representation of $\mathbf{B}_N$

Faithful representation of $\mathbf{B}_N$

Lawrence–Krammer. $\mathsf{LK}\colon \mathbf{B}_N \longrightarrow \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

Faithful representation of $\mathbf{B}_N$

Lawrence–Krammer. $\mathsf{LK}\colon \mathbf{B}_N \longrightarrow \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

Bigelow 2001 (JAMS), Krammer 2002 (Annals):
LK representation is faithful for all N.

Faithful representation of $\mathbf{B}_N$

Lawrence–Krammer. $\mathrm{LK}\colon \mathbf{B}_N \longrightarrow \mathrm{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

Bigelow 2001 (JAMS), Krammer 2002 (Annals):
LK representation is faithful for all N.

Cheon–Jun 2003. LK Evaluation: Fast. Inversion: N^6 (acceptable).

Faithful representation of $\mathbf{B}_N$

Lawrence–Krammer. $\mathsf{LK}\colon \mathbf{B}_N \longrightarrow \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

Bigelow 2001 (JAMS), Krammer 2002 (Annals):
LK representation is faithful for all N.

Cheon–Jun 2003. LK Evaluation: Fast. Inversion: N^6 (acceptable).

$\therefore$ May work in the image of $\mathbf{B}_N$ in $\mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

Reducing to a matrix group over a finite field

Reducing to a matrix group over a finite field

Cheon–Jun 2003. Let $x = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$.

Reducing to a matrix group over a finite field

Cheon–Jun 2003. Let $x = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$.

1. The degrees of t in $\mathsf{LK}(x) \in \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$ is in $[-m, m]$.
2. The coefficients $\frac{c}{2^d}$ in $\mathsf{LK}(x)$ satisfy: $|c| \leq 2^{N^2 m}, |d| \leq 2Nm$.

Reducing to a matrix group over a finite field

Cheon–Jun 2003. Let $x = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$.

1. The degrees of t in $\mathsf{LK}(x) \in \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$ is in $[-m, m]$.
2. The coefficients $\frac{c}{2^d}$ in $\mathsf{LK}(x)$ satisfy: $|c| \leq 2^{N^2 m}, |d| \leq 2Nm$.

- $(2^{2Nm} t^m) \cdot \mathsf{LK}(\mathsf{x}) \in \mathsf{GL}_{\binom{N}{2}}(\mathbb{Z}[t])$;
- $|\text{coefficients}| \leq 2^{N^2(m+\epsilon)}$;
- Degree of $t \leq 2m$.

Reducing to a matrix group over a finite field

Cheon–Jun 2003. Let $x = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$.

1. The degrees of t in $\mathrm{LK}(x) \in \mathrm{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$ is in $[-m, m]$.
2. The coefficients $\frac{c}{2^d}$ in $\mathrm{LK}(x)$ satisfy: $|c| \leq 2^{N^2 m}, |d| \leq 2Nm$.

- $(2^{2Nm} t^m) \cdot \mathrm{LK}(\mathrm{x}) \in \mathrm{GL}_{\binom{N}{2}}(\mathbb{Z}[t])$;
- $|\text{coefficients}| \leq 2^{N^2(m+\epsilon)}$;
- Degree of $t \leq 2m$.

$\therefore$ For prime $p \gtrsim 2^{N^2 m}$ and irreducible $f(t)$ of degree $\gtrsim 2m$,

$$(2^{2Nm} t^m) \cdot \mathrm{LK}(x) = (2^{2Nm} t^m) \cdot \mathrm{LK}(x) \bmod (p, f(t)) \in \mathrm{GL}_{\binom{N}{2}}(\mathbb{Z}[t]/\langle p, f(t) \rangle).$$

Reducing to a matrix group (cont.)

BDH Problem. $(g^{a}, g^{b}) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$,
$\deg(f(t)) \gtrsim 2m$.

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$,
$\deg(f(t)) \gtrsim 2m$.

$\mathbb{F} := \mathbb{Z}[t]/\langle p, f(t)\rangle = \mathbb{Z}[t^{\pm 1}, \frac{1}{2}]/\langle p, f(t)\rangle$.

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$, $\deg(f(t)) \gtrsim 2m$.

$\mathbb{F} := \mathbb{Z}[t]/\langle p, f(t)\rangle = \mathbb{Z}[t^{\pm 1}, \frac{1}{2}]/\langle p, f(t)\rangle$.

$\mathbb{F}$ is a finite field. Field operations: $m^3 N^2$.

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$,
$\deg(f(t)) \gtrsim 2m$.

$\mathbb{F} := \mathbb{Z}[t]/\langle p, f(t)\rangle = \mathbb{Z}[t^{\pm 1}, \frac{1}{2}]/\langle p, f(t)\rangle$.

$\mathbb{F}$ is a finite field. Field operations: $m^3 N^2$.

$$(2^{2Nm}t^m) \cdot \mathsf{LK}(K) \in \mathsf{GL}_{\binom{N}{2}}(\mathbb{F}).$$

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1}b^{-1}gab$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$, $\deg(f(t)) \gtrsim 2m$.

$\mathbb{F} := \mathbb{Z}[t]/\langle p, f(t)\rangle = \mathbb{Z}[t^{\pm 1}, \frac{1}{2}]/\langle p, f(t)\rangle$.

$\mathbb{F}$ is a finite field. Field operations: $m^3 N^2$.

$$(2^{2Nm}t^m) \cdot \mathrm{LK}(K) \in \mathrm{GL}_{\binom{N}{2}}(\mathbb{F}).$$

$\therefore$ Suffices to break BDH KEP over $G = \mathrm{LK}[\mathbf{B}_N]/\langle p, f(t)\rangle \leq \mathrm{GL}_{\binom{N}{2}}(\mathbb{F})$.

Reducing to a matrix group (cont.)

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

BDH KEP. $K = g^{ab} = a^{-1} b^{-1} g a b$.

Let $K = (i, p_1, \ldots, p_\ell) \in \mathbf{B}_N$, $m = |i| + \ell$, $p \gtrsim 2^{N^2 m}$,
$\deg(f(t)) \gtrsim 2m$.

$\mathbb{F} := \mathbb{Z}[t]/\langle p, f(t)\rangle = \mathbb{Z}[t^{\pm 1}, \frac{1}{2}]/\langle p, f(t)\rangle$.

$\mathbb{F}$ is a finite field. Field operations: $m^3 N^2$.

$$(2^{2Nm} t^m) \cdot \mathrm{LK}(K) \in \mathrm{GL}_{\binom{N}{2}}(\mathbb{F}).$$

$\therefore$ Suffices to break BDH KEP over
$G = \mathrm{LK}[\mathbf{B}_N]/\langle p, f(t)\rangle \leq \mathrm{GL}_{\binom{N}{2}}(\mathbb{F})$.

$n := \binom{N}{2}$, roughly N^2. Henceforth, $G \leq \mathrm{GL}_n(\mathbb{F})$.

Representation attack

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases}$$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{cases}$$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\left\{ \begin{array}{rcl} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{array} \right. \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \left\{ \begin{array}{rcl} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{array} \right.$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \overset{\text{eff}}{\cong}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\left\{ \begin{array}{rcl} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{array} \right. \Longrightarrow \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \left\{ \begin{array}{rcl} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{array} \right.$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} = g \cdot a \\ a \cdot B = B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} = g \cdot \tilde{a} \\ \tilde{a} \cdot B = B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b = \boxed{g^a}^b =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\left\{ \begin{array}{rcl} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{array} \right. \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \left\{ \begin{array}{rcl} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{array} \right.$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b = \boxed{g^a}^b = g^{ab} =$

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} = g \cdot a \\ a \cdot B = B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} = g \cdot \tilde{a} \\ \tilde{a} \cdot B = B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b = \boxed{g^a}^b = g^{ab} = K$!

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \Longrightarrow \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b = \boxed{g^a}^b = g^{ab} = K$!

Possibly, $\tilde{a} \notin G$, but this works !

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\text{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \implies \tilde{a} \in \mathrm{M}_n(\mathbb{F}) \text{ s.t. } \begin{cases} \tilde{a} \cdot \boxed{g^a} & = & g \cdot \tilde{a} \\ \tilde{a} \cdot B & = & B \cdot \tilde{a} \end{cases}$$

Then $\boxed{g^b}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^b = \boxed{g^a}^b = g^{ab} = K$!

Possibly, $\tilde{a} \notin G$, but this works ! Complexity: $(n^2)^3 = N^{12}$.

Second Braid Diffie–Hellman KEP

Second Braid Diffie–Hellman KEP

Cha–Ko–Lee–Han–Cheon 2001.

Alice	**Public**	**Bob**
$a_1 \in A_1, a_2 \in A_2$	$A_1, A_2, B_1, B_2 \leq G, g \in G$	$b_1 \in B_1, b_2 \in B_2$
	$\xrightarrow{\boxed{a_1 g a_2}}$	
	$\xleftarrow{\boxed{b_1 g b_2}}$	
$K = a_1 \boxed{b_1 g b_2} a_2$		$K = b_1 \boxed{a_1 g a_2} b_2$

Second Braid Diffie–Hellman KEP

Cha–Ko–Lee–Han–Cheon 2001.

Alice	**Public**	**Bob**
$a_1 \in A_1, a_2 \in A_2$	$A_1, A_2, B_1, B_2 \le G, g \in G$	$b_1 \in B_1, b_2 \in B_2$
	$\xrightarrow{\boxed{a_1 g a_2}}$	
	$\xleftarrow{\boxed{b_1 g b_2}}$	
$K = a_1 \boxed{b_1 g b_2} a_2$		$K = b_1 \boxed{a_1 g a_2} b_2$

Cheon–Jun 2003. Similar representation attack:

$$c = a_1 g a_2 \iff \boxed{a_1^{-1}} \cdot c = g \cdot a_2.$$

Finding an invertible solution

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick “random” elements until invertible.

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick "random" elements until invertible.

Ts. Assume $\mathrm{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|\alpha_1 A_1 + \cdots + \alpha_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick "random" elements until invertible.

Ts. Assume $\mathrm{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|\alpha_1 A_1 + \cdots + \alpha_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Proof: $f(x_1, \ldots, x_m) := |x_1 A_1 + \cdots + x_m A_m| \in \mathbb{F}[x_1, \ldots, x_m]$, nonzero, degree n.

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick "random" elements until invertible.

Ts. Assume $\operatorname{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|\alpha_1 A_1 + \cdots + \alpha_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Proof: $f(x_1, \ldots, x_m) := |x_1 A_1 + \cdots + x_m A_m| \in \mathbb{F}[x_1, \ldots, x_m]$,
nonzero, degree n.

Schwartz 1980–Zippel 1989 Lemma.
$f(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ nonzero degree n.

$$\Pr(f(x_1, \ldots, x_m) \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick "random" elements until invertible.

Ts. Assume $\mathrm{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|\alpha_1 A_1 + \cdots + \alpha_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Proof: $f(x_1, \ldots, x_m) := |x_1 A_1 + \cdots + x_m A_m| \in \mathbb{F}[x_1, \ldots, x_m]$, nonzero, degree n.

Schwartz 1980–Zippel 1989 Lemma.
$f(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ nonzero degree n.

$$\Pr(f(x_1, \ldots, x_m) \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

In our case, $|\mathbb{F}| > 2^n \gg n$.

The Commutator Key Exchange Protocol

The Commutator Key Exchange Protocol

Anshel–Anshel–Goldfeld 1999.

The Commutator Key Exchange Protocol

Anshel–Anshel–Goldfeld 1999.

Alice	**Public**	**Bob**
$v(x_1, \dots, x_k) \in F_k$	$\langle a_1, \dots, a_k \rangle \leq G$	$w(x_1, \dots, x_k) \in F_k$
$a = v(a_1, \dots, a_k)$	$\langle b_1, \dots, b_k \rangle \leq G$	$b = w(b_1, \dots, b_k)$
	$\xrightarrow{\quad {b_1}^{a}, \dots, {b_k}^{a} \quad}$	
	$\xleftarrow{\quad {a_1}^{b}, \dots, {a_k}^{b} \quad}$	
$K = a^{-1} v({a_1}^{b}, \dots, {a_k}^{b})$		$K = w({b_1}^{a}, \dots, {b_k}^{a})^{-1} b$

The Commutator Key Exchange Protocol

Anshel–Anshel–Goldfeld 1999.

Alice	**Public**	**Bob**
$v(x_1,\dots,x_k) \in F_k$	$\langle a_1,\dots,a_k \rangle \le G$	$w(x_1,\dots,x_k) \in F_k$
$a = v(a_1,\dots,a_k)$	$\langle b_1,\dots,b_k \rangle \le G$	$b = w(b_1,\dots,b_k)$

$$\xrightarrow{\qquad\qquad\qquad {b_1}^{a},\dots,{b_k}^{a} \qquad\qquad\qquad}$$

$$\xleftarrow{\qquad\qquad\qquad {a_1}^{b},\dots,{a_k}^{b} \qquad\qquad\qquad}$$

$$K = a^{-1} v({a_1}^{b},\dots,{a_k}^{b}) \qquad\qquad K = w({b_1}^{a},\dots,{b_k}^{a})^{-1} b$$

$$a^{-1} v({a_1}^{b},\dots,{a_k}^{b}) = a^{-1} a^{b} = a^{-1} b^{-1} a b = (b^{a})^{-1} b = w({b_1}^{a},\dots,{b_k}^{a})^{-1} b$$

Linear Centralizer approach (Ts)

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!
2. $H = \langle g_1, \ldots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \ldots, g_k)$.

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!
2. $H = \langle g_1, \ldots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \ldots, g_k)$.
   $\therefore C_M(H)$ computable by solving

$$\begin{cases} xg_1 & = & g_1x \\ & \vdots & \\ xg_k & = & g_kx \end{cases}$$

linear equations in the n^2 entries of x, kn^6 operations.

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!
2. $H = \langle g_1, \ldots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \ldots, g_k)$.
   $\therefore C_M(H)$ computable by solving

$$\begin{cases} x g_1 & = & g_1 x \\ & \vdots & \\ x g_k & = & g_k x \end{cases}$$

   linear equations in the n^2 entries of x, kn^6 operations.
3. $C_M(g_1, \ldots, g_k)$ is a vector subspace of M.

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!
2. $H = \langle g_1, \ldots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \ldots, g_k)$. $\therefore C_M(H)$ computable by solving
$$\begin{cases} xg_1 & = & g_1x \\ & \vdots & \\ xg_k & = & g_kx \end{cases}$$
linear equations in the n^2 entries of x, kn^6 operations.
3. $C_M(g_1, \ldots, g_k)$ is a vector subspace of M.
4. $C_M(C_M(H))$ computable: $\dim(C_M(H)) \leq n^2$ equations.

Linear Centralizer approach (Ts)

Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces of M!
2. $H = \langle g_1, \ldots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \ldots, g_k)$.
   $\therefore C_M(H)$ computable by solving

   $$\left\{ \begin{array}{rcl} x g_1 & = & g_1 x \\ & \vdots & \\ x g_k & = & g_k x \end{array} \right.$$

   linear equations in the n^2 entries of x, kn^6 operations.
3. $C_M(g_1, \ldots, g_k)$ is a vector subspace of M.
4. $C_M(C_M(H))$ computable: $\dim(C_M(H)) \leq n^2$ equations.
5. Complexity: $kn^6 + n^2 n^6 = n^8$.

Linear Centralizer attack on Commutator KEP

Linear Centralizer attack on Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G \leq \mathrm{GL}_n(\mathbb{F})$.

Commutator KEP Problem. $({b_1}^{a}, \ldots, {b_k}^{a}, {a_1}^{b}, \ldots, {a_k}^{b}) \mapsto a^{-1}b^{-1}ab$.

Linear Centralizer attack on Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G \leq \mathrm{GL}_n(\mathbb{F})$.

Commutator KEP Problem. $({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1}b^{-1}ab$.

Attack (Ts):

1. Compute a basis for $C_M(C_M(b_1, \ldots, b_k))$.

Linear Centralizer attack on Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G \leq \mathrm{GL}_n(\mathbb{F})$.

Commutator KEP Problem. $({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1}b^{-1}ab$.

Attack (Ts):

1. Compute a basis for $C_M(C_M(b_1, \ldots, b_k))$.
2. Solve

$$\begin{array}{rcl} b_1 a & = & a \cdot \boxed{{b_1}^a} \\ & \vdots & \\ b_k a & = & a \cdot \boxed{{b_k}^a} \end{array} \quad ; \quad \begin{array}{rcl} a_1 b & = & b \cdot \boxed{{a_1}^b} \\ & \vdots & \\ a_k b & = & b \cdot \boxed{{a_k}^b} \end{array}$$

with a invertible, $b \in C_M(C_M(b_1, \ldots, b_k))$ invertible.

Linear Centralizer attack on Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G \leq \mathrm{GL}_n(\mathbb{F})$.

Commutator KEP Problem. $({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1}b^{-1}ab$.

Attack (Ts):

1. Compute a basis for $C_M(C_M(b_1, \ldots, b_k))$.
2. Solve

$$\begin{array}{rcl} b_1 a & = & a \cdot \boxed{{b_1}^a} \\ & \vdots & \\ b_k a & = & a \cdot \boxed{{b_k}^a} \end{array} \quad ; \quad \begin{array}{rcl} a_1 b & = & b \cdot \boxed{{a_1}^b} \\ & \vdots & \\ a_k b & = & b \cdot \boxed{{a_k}^b} \end{array}$$

   with a invertible, $b \in C_M(C_M(b_1, \ldots, b_k))$ invertible.
3. $\exists$ solution: (a, b). Let $(\tilde{a}, \tilde{b})$ be one.

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1 \tilde{a} & = & \tilde{a} \cdot \boxed{{b_1}^{a}} \\ & \vdots & \\ b_k \tilde{a} & = & \tilde{a} \cdot \boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1 \tilde{b} & = & \tilde{b} \cdot \boxed{{a_1}^{b}} \\ & \vdots & \\ a_k \tilde{b} & = & \tilde{b} \cdot \boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}$, a conjugate b_1 to the same thing):

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$b_1\tilde{a} \quad = \quad \tilde{a}\cdot{b_1}^{a}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}$, a conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot{b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \end{array}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot {b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}$, a conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot {b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot{b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$.

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot{b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot{b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b}$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot{b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b}$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot {b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}a\tilde{b}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{{b_1}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{{a_1}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot {b_1}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}a\tilde{b} = a^{-1}a^{\tilde{b}}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot\boxed{b_1{}^{a}} \\ & \vdots & \\ b_k\tilde{a} & = & \tilde{a}\cdot\boxed{b_k{}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} & = & \tilde{b}\cdot\boxed{a_1{}^{b}} \\ & \vdots & \\ a_k\tilde{b} & = & \tilde{b}\cdot\boxed{a_k{}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} & = & \tilde{a}\cdot b_1{}^{a} \\ b_1\tilde{a} & = & \tilde{a}a^{-1}\cdot b_1 a \\ b_1\cdot\tilde{a}a^{-1} & = & \tilde{a}a^{-1}\cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore\ \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore\ [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}a\tilde{b} = a^{-1}a^{\tilde{b}} = a^{-1}a^{b}$$

Linear Centralizer attack on Commutator KEP (contd.)

$$\begin{array}{rcl} b_1\tilde{a} &=& \tilde{a} \cdot \boxed{{b_1}^{a}} \\ &\vdots& \\ b_k\tilde{a} &=& \tilde{a} \cdot \boxed{{b_k}^{a}} \end{array} \quad ; \quad \begin{array}{rcl} a_1\tilde{b} &=& \tilde{b} \cdot \boxed{{a_1}^{b}} \\ &\vdots& \\ a_k\tilde{b} &=& \tilde{b} \cdot \boxed{{a_k}^{b}} \end{array}$$

$\tilde{a}, \tilde{b}$ invertible, $\tilde{b} \in C_M(C_M(b_1, \ldots, b_k))$.

$[\tilde{a}a^{-1}, b_1] = 1$ (since $\tilde{a}, a$ conjugate b_1 to the same thing):

$$\begin{array}{rcl} b_1\tilde{a} &=& \tilde{a} \cdot {b_1}^{a} \\ b_1\tilde{a} &=& \tilde{a}a^{-1} \cdot b_1 a \\ b_1 \cdot \tilde{a}a^{-1} &=& \tilde{a}a^{-1} \cdot b_1 \end{array}$$

Similarly for $b_2, \ldots, b_k$.

$\therefore \tilde{a}a^{-1} \in C_M(b_1, \ldots, b_k)$. $\therefore [\tilde{b}, \tilde{a}a^{-1}] = 1$.

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}a\tilde{b} = a^{-1}a^{\tilde{b}} = a^{-1}a^{b} = K \ !$$

Complexity

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Complexity

n^8 for computing $C_M(C_M(b_1, \dots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Complexity

n^8 for computing $C_M(C_M(b_1, \dots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Total: $n^9 m = N^{18} m^3$ offlien; $kn^7 m^3 = kN^{14} m^3$ online.

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Total: $n^9 m = N^{18} m^3$ offlien; $kn^7 m^3 = kN^{14} m^3$ online.

Using $\omega = \log_2 7$: $N^{16.8} m^3$ offlien; $kn^7 m^3 = kN^{13} m^3$ online.

Not practical: $100^{16.8} = 2^{111}$ (times m^3 and logarithmic factors...).

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Total: $n^9 m = N^{18} m^3$ offlien; $kn^7 m^3 = kN^{14} m^3$ online.

Using $\omega = \log_2 7$: $N^{16.8} m^3$ offlien; $kn^7 m^3 = kN^{13} m^3$ online.

Not practical: $100^{16.8} = 2^{111}$ (times m^3 and logarithmic factors...). But:

1. Worst-case polytime.

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Total: $n^9 m = N^{18} m^3$ offlien; $kn^7 m^3 = kN^{14} m^3$ online.

Using $\omega = \log_2 7$: $N^{16.8} m^3$ offlien; $kn^7 m^3 = kN^{13} m^3$ online.

Not practical: $100^{16.8} = 2^{111}$ (times m^3 and logarithmic factors...).
But:

1. Worst-case polytime.
2. First provable attack for small braid index N.

Complexity

n^8 for computing $C_M(C_M(b_1, \ldots, b_k))$.

Can be preprocessed!

kn^6 for solving the equations.

Field operations: $m^3 N^2 = m^3 n$.

Total: $n^9 m = N^{18} m^3$ offlien; $kn^7 m^3 = kN^{14} m^3$ online.

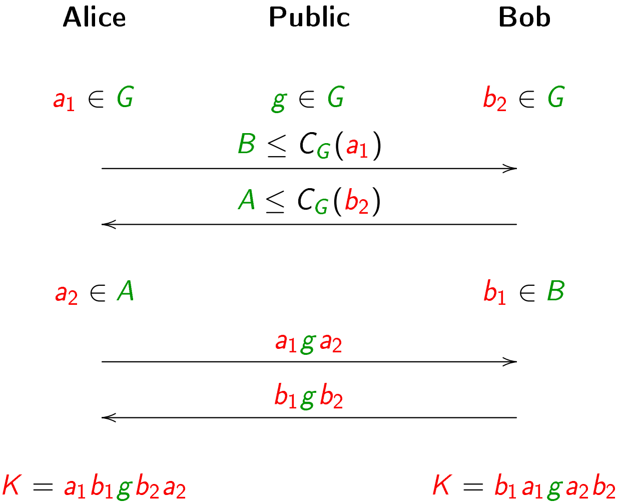
Using $\omega = \log_2 7$: $N^{16.8} m^3$ offlien; $kn^7 m^3 = kN^{13} m^3$ online.

Not practical: $100^{16.8} = 2^{111}$ (times m^3 and logarithmic factors...).
But:

1. Worst-case polytime.
2. First provable attack for small braid index N.
3. Just cubic in m. :)

The Centralizer KEP (Shpilrain–Ushakov 2006)

The Centralizer KEP (Shpilrain–Ushakov 2006)



Alice	**Public**	**Bob**
$a_1 \in G$	$g \in G$	$b_2 \in G$
	$\xrightarrow{B \leq C_G(a_1)}$	
	$\xleftarrow{A \leq C_G(b_2)}$	
$a_2 \in A$		$b_1 \in B$
	$\xrightarrow{a_1 g a_2}$	
	$\xleftarrow{b_1 g b_2}$	
$K = a_1 b_1 g b_2 a_2$		$K = b_1 a_1 g a_2 b_2$

Linear Centralizer Attack on Centralizer KEP

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B), a_2^{-1} \in C_M(C_M(A))$ invertible.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B)$, $a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \le C_G(a_1)$, $A \le C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \le C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B)$, $a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.
4. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2$

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \le C_G(a_1)$, $A \le C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \le C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B)$, $a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.
4. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2 \overset{!}{=} b_1 \tilde{a}_1 g \tilde{a}_2 b_2$

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B), a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.
4. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2 \overset{!}{=} b_1 \tilde{a}_1 g \tilde{a}_2 b_2 = b_1 a_1 g a_2 b_2 = K$!

Linear Centralizer Attack on Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B), a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.
4. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2 \overset{!}{=} b_1 \tilde{a}_1 g \tilde{a}_2 b_2 = b_1 a_1 g a_2 b_2 = K$!
5. Complexity $N^{16.8} m^3$.

The end of braid-based cryptography?

The end of braid-based cryptography?

Not quite:

1. Attack impractical for practical values of N.

The end of braid-based cryptography?

Not quite:

1. Attack impractical for practical values of N.
2. There are additional braid-PKC proposals (Dehornoy et al., Kalka, Kurt . . .).

The end of braid-based cryptography?

Not quite:

1. Attack impractical for practical values of N.
2. There are additional braid-PKC proposals (Dehornoy et al., Kalka, Kurt ...).
3. The other problems (CSP, Multiple CSP,...) on which braid-based PKC may be based.

The Triple Decomposition KEP (Kurt 2005)

The Triple Decomposition KEP (Kurt 2005)

Alice **Public** **Bob**

a, a_1, a_2, x_1, x_2

$$\begin{tikzcd}[row sep=small]
A & A_1 \arrow[d, dash] & A_2 \arrow[d, dash] & X_1 \arrow[d, dash] & X_2 \arrow[d, dash] & & \\
& Y_1 & Y_2 & B_1 & B_2 & B & \leq G
\end{tikzcd}$$

y_1, y_2, b_1, b_2, b

$$\xrightarrow{\boxed{ax_1},\ \boxed{x_1^{-1}a_1x_2},\ \boxed{x_2^{-1}a_2}}$$

$$\xleftarrow{\boxed{b_1y_1},\ \boxed{y_1^{-1}b_2y_2},\ \boxed{y_2^{-1}b}}$$

$$a\boxed{b_1y_1}a_1\boxed{y_1^{-1}b_2y_2}a_2\boxed{y_2^{-1}b} = \underbrace{ab_1a_1b_2a_2b}_{K} = \boxed{ax_1}b_1\boxed{x_1^{-1}a_1x_2}b_2\boxed{x_2^{-1}a_2}b$$

The Triple Decomposition KEP (Kurt 2005)

Alice **Public** **Bob**

a, a_1, a_2, x_1, x_2

$$\begin{array}{cccccc} A & A_1 & A_2 & X_1 & X_2 & \\ & | & | & | & | & \\ & Y_1 & Y_2 & B_1 & B_2 & B \end{array} \leq G$$

y_1, y_2, b_1, b_2, b

$$\xrightarrow{\boxed{ax_1},\ \boxed{x_1^{-1}a_1x_2},\ \boxed{x_2^{-1}a_2}}$$

$$\xleftarrow{\boxed{b_1y_1},\ \boxed{y_1^{-1}b_2y_2},\ \boxed{y_2^{-1}b}}$$

$$a\boxed{b_1y_1}a_1\boxed{y_1^{-1}b_2y_2}a_2\boxed{y_2^{-1}b} = \underbrace{ab_1a_1b_2a_2b}_{K} = \boxed{ax_1}b_1\boxed{x_1^{-1}a_1x_2}b_2\boxed{x_2^{-1}a_2}b$$

THANK YOU!