

New Developments in Commutator Key Exchange

R. Gilman, A.G.Miasnikov, A.D.Myasnikov, A. Ushakov

Commutator Key Exchange



- Introduced by Anshel-Anshel-Goldfeld (1999).
- Generated a lot of research related to braid groups.
- Several attacks claimed to be successful.
- Currently considered insecure.

Public Information

- A group G with a normal form N
- Subgroups $A = \langle a_1, \dots, a_m \rangle$ and $B = \langle b_1, \dots, b_n \rangle$

Alice:

Secret $a = u(a_1, \dots, a_m)$ in A

Sends $\{N(b_1^a), \dots, N(b_n^a)\}$

Computes $a^b = u(a_1^b, \dots, a_m^b)$

Shared key:

$$a^{-1}b^{-1}ab = [a,b]$$

Bob:

Secret $b = v(b_1, \dots, b_n)$ in B

Sends $\{N(a_1^b), \dots, N(a_m^b)\}$

Computes $b^a = v(b_1^a, \dots, b_n^a)$

Shared key:

$$(a^{-1}ba)^{-1}b = [a,b]$$

Two generic properties must be satisfied:

- 1 Large centralizers to prevent possibility of enumerating all possible keys
- 2 Keys must contain large peaks to prevent efficient decomposition in subgroup generators

Previously proposed protocols violate the conditions

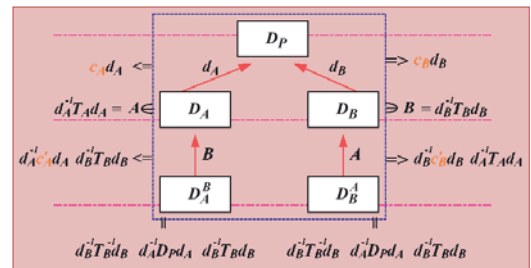
New key exchange solves both problems

1. Use tubular braids to guarantee centralizers of exponential growth (i.e. exponentially many elements of a given length)
2. Use Mihalova construction. The construction makes decomposition of a key an **unsolvable** problem in general. In practice we have keys which contain peaks of polynomial size. To "cut" such peaks it is required exponentially many trials.
3. **EXPERIMENTS SHOW NONE OF THE KNOWN ATTACKS CAN APPROXIMATE THE SOLUTION WITHIN REASONABLE ACCURACY**

$$P = \langle X \mid R \rangle$$

• D_P subgroup of $F(X) \times F(X)$

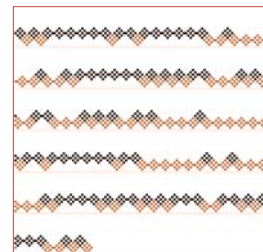
• $D_P = \langle (x,x), (1,r) \mid x \text{ in } X \text{ and } r \text{ in } R \rangle$



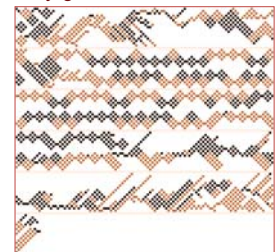
Visualization

- Integral part of data analysis
- Important for developing non-intuitive conjectures
- Heuristic algorithms
- Statistical studies

Unscrambled key



Key diffused by mixing conjugator



CRyptography And Groups (CRAG) Library

The Cryptography And Groups (CRAG) Library is a state of the art software package which provides an environment to test cryptographic protocols constructed from non-commutative groups.

- Provides both an interface and routines for computations.
- Implementations of basic algebraic objects.
- Contains implementation of non-classical heuristic approaches and tools to perform statistical and exploratory analysis of algebraic data
- Continually expanding

LIBRARY CONTENTS:

- Basic operations of words in a group, finite and infinite alphabets
- Advanced Denh's algorithm
- Free groups, Whitehead's graph, random automorphisms.
- Algorithms for subgroups of free groups
- Braid groups, Grigorchuk groups, Thompson groups, Free Metabelian Groups.
- Equations over finitely presented group
- Algorithms for graphs and automata.
- Algorithms for visualization of algebraic objects. Similarity measures
- Implementations of various cryptographic protocols and attacks based on group theoretic