INTRODUCTION TO BRAID GROUP CRYPTOGRAPHY

Parvez Anandam

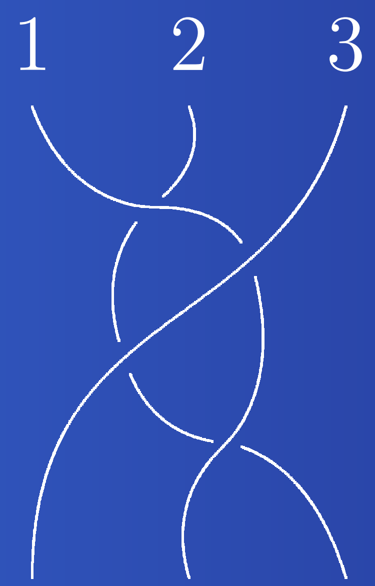
Why more cryptographies?

Current public key cryptographies are vulnerable to quantum computing attacks $\Rightarrow$ Increase their "genetic diversity"

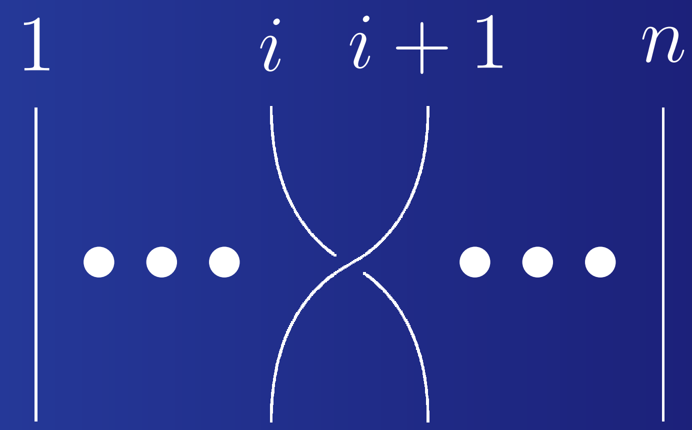
Hard problems:

1. Discrete Logarithm Problem (DH)
2. Factoring Problem (RSA)
3. Conjugacy Search Problem:
   Given $x, y \in G$ with $y = a^{-1}xa$ for some $a \in G$
   Find $b \in G$ such that $y = b^{-1}xb$.

Braid Groups



3-braid $\sigma_1^{-1}\sigma_2\sigma_1\sigma_2 = \sigma_2\sigma_1$



σ_i

Braid Group B_n

Artin Presentation of B_n

$$\left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geq 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle$$

B_n is non-abelian: $ab \neq ba$

Left-Canonical Form

$$b = \Delta^u A_1 A_2 \ldots A_l$$

Commutator based key agreement

1. A(lice) publishes $G_A = \langle x_1, \ldots, x_s \rangle \subseteq B_n$
2. B(ob) publishes $G_B = \langle y_1, \ldots, y_t \rangle \subseteq B_n$
3. A selects $a \in G_A$ and sends $a^{-1}y_1a, \ldots, a^{-1}y_ta$ to B.
4. B selects $b \in G_B$ and sends $b^{-1}x_1b, \ldots, b^{-1}x_sb$ to A.
5. A computes $K = a^{-1}(b^{-1}ab)$
6. B computes $K = (a^{-1}b^{-1}a)b$

Diffie-Hellman type key agreement

$$LB_n = \left\langle \sigma_1, \ldots, \sigma_{\lfloor n/2 \rfloor - 1} \right\rangle \subset B_n$$
$$UB_n = \left\langle \sigma_{\lfloor n/2 \rfloor + 1}, \ldots, \sigma_{n-1} \right\rangle \subset B_n$$

1. Public braid $x \in B_n$
2. A selects $a \in LB_n$ and sends $y_A = a^{-1}xa$ to B
3. B selects $b \in UB_n$ and sends $y_B = b^{-1}xb$ to A
4. A computes $K = a^{-1}y_B a = a^{-1}b^{-1}xab$
5. B computes $K = b^{-1}y_A b = a^{-1}b^{-1}xab$

Example using C++ library CBraid

```
x:       (0|3 2 4 1|4 2 1 3|1 3 4 2|)
a:       (0|2 1 3 4|2 1 3 4|2 1 3 4|)
b:       (0|1 2 4 3|1 2 4 3|1 2 4 3|)
y_A:    (-1|4 3 1 2|2 3 4 1|4 1 2 3|
         2 3 4 1|2 1 3 4|2 1 3 4|)
y_B:    (-2|4 3 1 2|3 4 2 1|3 2 1 4|
         4 3 1 2|1 4 3 2|1 2 4 3|)
A's k:  (-2|4 3 1 2|3 4 1 2|2 4 1 3|
         4 1 3 2|2 4 3 1|2 1 3 4|2 1 3 4|)
B's k:  (-2|4 3 1 2|3 4 1 2|2 4 1 3|
         4 1 3 2|2 4 3 1|2 1 3 4|2 1 3 4|)
```

Conclusion

Unfortunately, the conjugacy search problem in braid groups is more tractable than first thought

Still hope of finding a group where the conjugacy search problem is hard