Braid Cryptosystem Notes

November 21, 2019

1 Braid Cryptographic System

1.1 Braids

A braid is a member of the Group B_n.

1.1.1 Left and Right Canonical Forms

For any $w \in B_n$ $\exists$ a unique representation called the left canonical form.

$$\begin{aligned}&w = \Delta^u A_1 A_2 ... A_l, u \in Z', A \in \Sigma_n \text{ without the following elements } \{e, \Delta\}\\&\text{where } A_i A_{i+1}\text{is left weighted for } 1 \leq i \leq l-1\\&\text{where } \Sigma_n \text{ is the set of all permutation braids.}\end{aligned}$$

1.2 Sub-Groups of the Braid Group

There are two commuting subgroups of B_n.

$$\begin{aligned}LB_n < B_n &\text{ generated by } \{\sigma_1, ..., \sigma_{[n/2]}\}\\UB_n < B_n &\text{ generated by } \{\sigma_{n/2+1}, ..., \sigma_{n-1}\}\\a \in B_n &\text{ commutes w/} b \in UB_n : ab = ba\end{aligned}$$

Notice how σ_3 is missing, we do this in order to be able to commute the upper and lower group. We do this using the second part of the braid definition

1.3 Braid Cryptographic System

Let's define the Braid Cryptographic System.

$$\begin{aligned}n &: \text{the Braid index}\\l &: \text{the Canonical Index}\end{aligned}$$

1.3.1 Commuter-based Key Agreement

There are many variants of the conjugacy search problem.

1.3.2 Generalized Conjugacy Search

Given: $x, y \in B_n$ s.t. $y = a^{-1}xa$ for some $a \in LB_n$
Find: $b \in LB_n$ s.t. $y = b^{-1}xb$
(note: can replace LB_n w/ UB_n)

Deliverables

11/21/2019

1. Finish Notes (TP) (COMPLETE)
2. Install/Demo CBraid (reference 6 of Anandam) (JL, BK, TP) (COMPLETE)
3. Learn Cryptosystem part (RM) (COMPLETE)