Braid Cryptosystem Notes

November 14, 2019

1 Braid Cryptographic System - 11/14/2019

n : the Braid index
l : the Canonical Index

1.1 Sub-Groups of the Braid Group

Two commuting subgroups of B_n

}

UB$_n < B_n$ generated by {$\sigma_{n/2}$+ 1, ..., σ_{n-1} }
a $\in B_n$ commutes w/$b \in UB_n : ab = ba$
$LB_n < B_n$ generated by $\{\sigma_1, ..., \sigma_{n/2}$
}
UB$_n < B_n$ generated by {$\sigma_{n/2}$+ 1, ..., σ_{n-1} }
a $\in B_n$ commutes w/$b \in UB_n : ab = ba$

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

1.2 Commuter-based Key Agreement

There are many variants of the conjugacy search problem.

1.2.1 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)

2 Deliverables 11/21/2019

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