Yu. Ishchuk, N. Zasjadkovych (Ivan Franko National University of L'viv, L'viv, Ukraine)

On Algorithms Inverting the Burau Representation

The Burau representation ρ of the braid group B_n has been exploited for cryptography based on the braid group. In process of solving braid conjugacy problem using linear algebra methods, it is essential to know, how to recover preimage braids from the image of this representation. We propose the inverting algorithms for Burau representation, which are different from [3].

Let us recall that the n-braid group B_n can be presented by the $n-1$ Artin generators $\sigma_1, \ldots, \sigma_{n-1}$ and relations $\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i, & if\ |i-j|>1 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & if\ |i-j|=1 \end{cases}$.

The Burau representation $\rho_B : B_n \to GL_n(\mathbb{Z}[x,x^{-1}])$ is defined by rule

$$\rho_B(\sigma_i) = diag(I_{i-1}, \begin{pmatrix} 1-x & x \\ 1 & 0 \end{pmatrix}, I_{n-i+1}) \ \text{ for all } \ i \in \{1,\ldots,n-1\}.$$

This representation is known to be unfaithful for all $n \geq 5$. Images $A = \rho_B(w)$ of braids $w \in B_n$ are called the Burau matrices, which satisfy following conditions $\sum_{i=1}^{n} a_{ji} = 1$ and $\sum_{i=1}^{n} a_{ij}x^i = x^j$, for all $j \in \{1,\ldots,n\}$.

In [1] Hughes used algorithm inverting ρ_B for security analysis of the braid group cryptosystem. The main idea is to reconstruct w from $\rho_B(w)$ generator by generator from right to left by assuming that the first column with highest degree entry in $A = \rho_B(w)$ indicates a last generator of w. Lee and Park [2] improved Hughes algorithm and proposed two new algorithms. These algorithms were compared [3] with respect to their success rate and elapsed time.

We proposed the algorithms inverting Burau representation of the submonoid B_n^+ of B_n and the braid group B_n. Our algorithms compute Artin generators of w from left to right and from both sides simultaneously. Using [4] we have obtained experimental results, which show that these algorithms have the higher success probabilities, but they are slower due to their self-correction process.

[1] J.Hughes, A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem // ACISP'02, LNCS. – v.2384. – 2002. – P.176-189.

[2] E.Lee and J.H.Park, Cryptoanalysis of the Public-Key Encryption based on Braid Groups // EUROCRYPT'03, LNCS. – v.2656. – 2003. – P.477-490.

[3] E.Lee, Inverting the Burau and Lawrence-Krammer Representations // Contemporary Mathematics.– v.418. – 2006. – P.153-160.

[4] Martin Schönert et al, GAP – Groups, Algorithms, and Programming – version 3 release 4 patchlevel 4. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1997.