Abstract

Braid groups were first introduced by Emil Artin in 1925. First cryptosystem, using Braid groups as a platform was discovered by Anshel et al in 2001. After the publication of this paper several cryptosystems on Braid groups had been designed. In this paper we have proposed a tripartite authenticated key agreement protocol using conjugacy problem which works in a braid
group. We have proved that our protocol meet the security attributes under the assumption that the Conjugacy Search Problem (CSP) is hard in braid group.

Reference

- B. C. Wang, Y. P. Hu, Signature scheme based on the root extraction problem over braid groups, ieeexplore.ieee.org, 2009
Tripartite Key Agreement Protocol using Conjugacy Problem in Braid Groups


Index Terms

Computer Science
Security

Key words
Braid group
Conjugacy Search Problem
authentication
tripartite key agreement