CRYPTOSYSTEM BASED ON PLATFORM GROUP OF AMALGAMATED FREE PRODUCT OF BRAID GROUP AND THOMPSON GROUP

SHIV DATT KUMAR[1] AND & SUMIT K. UPADHYAY
MATHEMATICS DEPARTMENT,
MOTILAL NEHRU NATIONAL INSTITUTE OF TECHNOLOGY
ALLAHABAD, INDIA
RAMJI LAL
INDIAN INSTITUTE OF INORMATION TECHNOLOGY,
ALLAHABAD, INDIA

1. Introduction

Most of the classical cryptographic schemes use Abelian groups. Diffie and Hellman [9] have given a key exchange protocol using finite cyclic groups. After that many key exchange protocol came using nonabelian groups as platform group. In recent years non-commutative groups, specially Braid groups (introduced by Artin)[5, 7, 8] and Thomson group have emerged as suitable plateform group for cryptographic protocols.

The idea of using the braid group as a platform for cryptosystems was first introduced in 1999 by Anshel, Anshel and Goldfeld in the paper "An algebraic method for public key Cryptography". However, recent results about the linearity of braid groups and Lawrence - Krammer representations have made these cryptosystems vulnerable to linear algebra based attacks. In particular J. Hughes has shown in his paper "**A linear algebraic attack on the braid group cryptosystem** "(www.network.com/hughes)[5] that key generation methods discussed in the paper "New key agreement protocols in Braid Group Cryptography" are not secure. Conjugacy search problem in braid group may not provide a sufficient level of security (See [5]). Selecting a suitable platform group is non trivial matter.

In this talk, in the spirit of Diffie Hellman protocol we discuss a crypto system based on platform group, which is generated using amalgamated free product of braid group and Thomson group amalgamated through a subgroup H whose commutator subgroup lies in the centre of H

We propose a new plateform group, which is amalgamated free product of Braid groups and Thompson groups. The useful feature of amalgamated free product of Braid groups and Thompson groups is that this is more secure than Braid groups and Thompson groups, but are not too complicated to work with.

Email: [1]sdt@mnnit.ac.in.

1.1. **New non-commutative protocol.** Consider braid group $B = \langle x_1, x_2, \ldots, x_i, \ldots | x_i x_j = x_j x_i$, whenever $|i-j| \geq 2$ and $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \rangle$ and Thompson group $T = \langle y_0, y_1, y_2, \ldots | y_k y_i = y_i y_{k+1} (k > i) \rangle$. Let $\{w_i | i \epsilon \lambda\}$ and $\{u_i | i \epsilon \lambda\}$, where λ is an indexed set, be set of words in $\{x_i\}$ and $\{y_i\}$ respectively. Let $H = \langle w_1, w_2, \ldots, w_n \rangle$ and $K = \langle u_1, u_2, \ldots, u_n \rangle$ be the subgroups of B and T respectively. Consider $G = \langle x_1, x_2, \ldots, x_n, \ldots, y_0, y_1, \ldots | x_i x_j = x_j x_i$ whenever $|i-j| \geq 2$ and $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}, y_k y_i = y_i y_{k+1} (k > i), w_1 = u_1, \ldots, w_n = u_n, w_i u_j w_i^{-1} u_j^{-1} w_l = w_l w_i u_j w_i^{-1} u_j^{-1} \rangle$ which is the amalgamated free product of B and T with subgroups H and K of B and T respectively. By the definition of G, it is clear that H is nilpotent group of class 2. This is used as a platform group. The group G and H & K are made public.

- Alice computes $A = w_{i_1}^{\varepsilon_1} \ldots w_{i_L}^{\varepsilon_L}$, where $\varepsilon_k = \pm 1$ & $w_{i_k} \epsilon H$ and sends $(A^{-1} u_1 A, A^{-1} u_2 A, \ldots, A^{-1} u_n A)$ to receiver.
- Bob computes $B = u_{j_1}^{\delta_1} \ldots u_{j_l}^{\delta_l}$, where $\delta_k = \pm 1$ & $u_{j_k} \epsilon K$ and sends $(B^{-1} w_1 B, \ldots, B^{-1} w_n B)$ to sender.
- Alice computes $K_1 = (A^{-1} B^{-1} w_1 B A, \ldots, A^{-1} B^{-1} w_n B A)$ and Bob computes $K_2 = (B^{-1} A^{-1} u_1 A B, \ldots, B^{-1} A^{-1} u_n A B)$.
  Since $B^{-1} A^{-1} u_i A B = A^{-1} B^{-1} (B A B^{-1} A^{-1}) u_i A B$
  $= A^{-1} B^{-1} u_i (B A B^{-1} A^{-1}) A B$
  $= A^{-1} B^{-1} u_i B A$
  $= A^{-1} B^{-1} w_i B A$ (From the definition of G)
- Their secret key $K = K_1 = K_2$

To break, the protocol an adversary needs a solution to conjugacy search problem, because K is conjugate to $(A^{-1} u_1 A, A^{-1} u_2 A, \ldots, A^{-1} u_n A)$ and $(B^{-1} w_1 B, \ldots, B^{-1} w_n B)$.

- The conjugacy search problem even if the presented group is known to be nilpotent group of class 2, appears to be infeasible and therefore difficult for adversary to decrypt.

References

[1] Anshel, I.; Anshel, M.; Goldfeld, D., An algebraic method for public key cryptography,Math. Res. Lett. 6, 287-291, 1999.

[2] Srivastava, G., Dixit, S.D., Transversal Structure Based Key Establishment Protocols, Contem. Engg. Sciences 2 (11), 543-552, 2009.

[3] I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld, New key agreement protocols in braid group cryptography, *Proc. of CT-RSA 2001, LNCS,* **2020***, Springer-Verlag, 1-15.*

[4] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, 22 (6), 1976, 644-654.

[5] J.Hughes A linear algebraic attack on the braid group cryptosystem"(www.network.com/hughes).

[11] A. Chaturvedi and S. Sunder, A Secure Key Agreement Protocol Using Braid Groups, Int. J. Networking, and application, Vol 01 (05), 327-330"