International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 56.67 | Impact Factor (2017): 5.156

# Using Diffie-Hellman Key - Exchange in RADG

**Mohaned Issa[1], Adil. Alramahi[2]**

[1, 2]University of Kufa. Faculty of Computer Science and Mathematics, Najaf, Iraq

**Abstract:** ***In this paper used a Diffie-Hellman key exchange with data of representation braid group to generation keys, encryption, and decryption method by using RADG (Reaction Automata Direct Graph) cryptosystem.***

**Keywords:** key-exchange, RADG cryptosystem, braid group

## 1. Introduction

The confidentiality in Cryptography is the science of encryption and decryption depend on many mathematical concepts, such as braid groups which are infinite non-commutative groups [1]. There are many relationships between non-commutative groups and Theoretical of cryptosystems with Key Agreement Protocols based on groups, because used the conjugacy problem (or transformation problem) for a group[2], it is undecidable for many classes of groups [3], and it be used in public-key cryptography. The special case RADG ( Reaction Automata Direct Graph) cryptosystem, Albermany, and Ghazanfar proposed a new cryptosystem for creation random multi-cipher text for the same plaintext[4] by use Direct graph, which is based on automata direct graph with special node called state, and other reaction states, which is by divided the state into two collection sets , the first set Q of normal set , it's have a subset set J called jump set, and the second R set called reaction set, each sets of R, and Q except J , have λ values inside the state [4]. Albermany, and Fatima Radi proposed new two method depended on RADG cryptosystem , called BRADG, and RBC, use key block cipher based on structure of unbalanced Fiestel, and new S-boxes[5]. Alwan proposed design is changeable, and faster, it's developed to RADG, by use Multi-Reaction states, called MRADG [6]. Nathim Rasool solved the problem of transition states in design by proposed system depend it on chaotic map equation, (for example logistic map equation), called CRADG [ 7 ]. Mahdi use the RADG in to development the stream cipher automata algorithm [8], Albakaa use McElliece, and Diffie-Hellman to improving RADG system [9].

The propose of the Diffie and Hellman ( or Deffie-Hellman) for key exchange was one of the first public-key protocols 1976 [10],there were a lot of people have been proposed public-key cryptosystem (PKC) and broken [11] , the famous public-key cryptosystem is depend on the prime numbers such as RSA [8] and its variants.

Another approach is it use hard problems based on the braid groups such as Anshel-Anshel-Goldfeld [12], with number of cryptographic protocols using non-commutative groups including Cha-Ko-Lee-Han-Cheon braid groups [11]. The braid groups $B_n$ is an infinite non-commutative group of n-braids, where n>1.

$B_n$ is defined as:

$$B_n = \left\langle \sigma_1, \sigma_2, \sigma_3, \ldots \sigma_{n-1} \middle| \begin{matrix} \sigma_i\sigma_j = \sigma_j\sigma_i \ \ if\ |i-j| \geq 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \ if\ |i-j| = 1 \end{matrix} \right\rangle$$

In n-braid groups $B_n$ , where n is braid index , m=*floor*(n/2), the lower braid $LB_n$ (also called as left braid) and upper braid $UB_n$ (also called as right braid) are define as $LB_n=<\sigma_1,\sigma_2,\ldots,\sigma_{m-1}>$ and $UB_n=<\sigma_{m+1},\sigma_{m+2},\sigma_{m+3},\ldots,\sigma_{n-1}>$ , For any value of $a\in LB_n$ and $b\in UB_n$ we have ab=ba . The elements of $B_n$ can be interpreted as deometric n strand braids [10] .

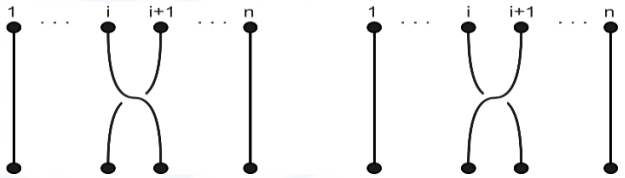



**Figure 1.1:** The elementary braids $\sigma_i^{-1}, \sigma_i$ [13]

## 2. Burau Representation of braid Group

In 1930 Burau presented his representation for braid groups by the map

$$\gamma_n : B_n \rightarrow GL_n(\mathbb{Z}[t,t^{-1}])$$

defined by

$$\sigma_i \rightarrow I_{i-1} \oplus \begin{bmatrix} 1-t & t \\ 1 & 0 \end{bmatrix} \oplus I_{n-(i+2)}$$

Where $I_k$ denote the square identity matrix of size k [14].
The Burau representation classified into two types , first type Reducible representation where the image $\gamma_n(\sigma_i)$ of a generator $\sigma_i$ of is $B_n$ represented by the matrix irreducible representation where the images of generator $\sigma_1,\sigma_{n-1}$ and $\sigma_i$ $(2\leq i\leq n-2)$ of $B_n$ by $\gamma_n$ are represented as matrix of above description, but Birman showed the Burau representation $\gamma_n$ is faithful when ≤3 , In 1999 , S. Bigelow showed this map is unfaithful when n≥5 , It is not known whether

$$\gamma_4 : B_n \rightarrow GL_4(\mathbb{Z}[t,t^{-1}])$$

## 3. Reaction Automata Direct Graph (RADG)

Mathematical model of (RADG) is effected by graph theory expressed by sextuple {Q,R,Σ,Ψ,J,T} where the function

$F_Q(n,\lambda)$ is number of cases which consist of Design of the set Q which contains jump state.

The jump state in the set Q is represented with $|J| \leq |n/2|$, it is clearly noticed that

$$F_Q(n,\lambda) \leq n^{(n-k)(\lambda-1)} (n-1)^{(n-k)}$$

where k = 1,…, |n/2|, (n-k)≥λ [4]

## 4. Diffie-Hellman key exchange over braid Groups

Cheon et al. found in Ko's research group had an idea of the possibility of using Diffie-Hellman key exchange based on braid group, There are many protocols that pertain to the original Devi-Hellman procedure can also rework this way, consider the subgroups of upper braids $UB_n=<\sigma_{m+1},\sigma_{m+2},\sigma_{m+3},\ldots,\sigma_{n-1}>$, and lower braids $LB_n=<\sigma_1,\sigma_2,\ldots,\sigma_{m-1}>$ , where m=floor(n/2)

**Protocol:**

- Public key: let $p \in B_n$.
- Private keys: Alice choose $x \in LB_n$, and Bob choose $y \in UB_n$
- Alice send to Bob $p'=xpx^{-1}$, and Bob send $p''=ypy^{-1}$
- Shared secret key $K=xpy^{-1}x^{-1}$
- K shared: Alice $K=xp''x-1=xpy^{-1}x^{-1}$
- Bob $K=yp'y^{-1}=yxpx^{-1}y^{-1}$

## 5. Implementation of method

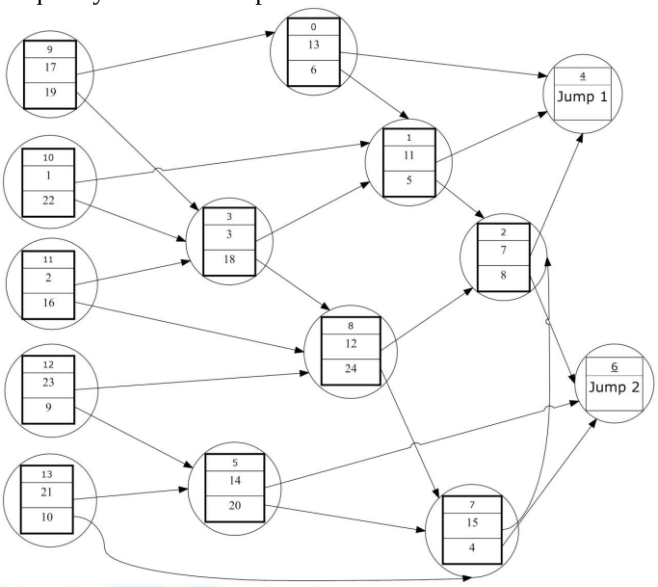
Suppose the message is "hello" the encryption steps for the first letter illustrates in the below table:

| Index message | Message bit | State index | value | Jump state |
|---|---|---|---|---|
| 0 | 0 | 3 | 3 | |
| 1 | 1 | 1 | 11 | J |
| 2 | 1 | 13 | 10 | |
| 3 | 0 | 7 | 15 | J |
| 4 | 1 | 11 | 16 | |
| 5 | 0 | 8 | 12 | |
| 6 | 0 | 2 | 7 | |
| 7 | 0 | 1 | 11 | Short path |

The cipher text is [14,8,19,3,20,13,15,13] the summation this values mod 256 equal to 105 represent the letter i . Start random at state number 3 , the message entered to state is "0" then select the corresponding cipher text is "3" as shown in figure below . The transition function drive to the next state which is "1" , the message enter to state number 1 is "1" ; to determine what the value choose from the values of λ {11,5} ; and choice "5" that corresponding to the message value "1" . transition function drive to jump state which also transfer to Reaction state and choice state randomly from them. And so on … ; at the final stage to ensure that we finish the encryption process in the set Q we apply short path . At the short path if the penultimate state is drive to Jump state, force it to choice the close state to finish in the set Q .

## 6. Conclusion

In this paper ,we proposed a new design is based on the concept of braid groups and RADG (Reaction Automata Direct Graph) ,the algorithm depends on Diffie-Hellman key exchange over braid group with RADG cryptosystem. The output of ciphertexts are random, to increase statistical frequency to broke of ciphertext.




## References

[1] Alexei Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2008). Group-based Cryptography. Berlin: Birkhäuser Verlag.

[2] *Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society. ISBN 9780821853603.*

[3] *Benjamin Fine, et. al. Aspects of Nonabelian Group Based Cryptography: A Survey and Open Problems. arXiv:1103.4093*

[4] Salah A. Albermany, Ghazanfar A. Safdar ; keyless security in Wireless Networks, Wireless Personal Communications Journal, DOI 10.1007/s1127-014-1954-1, Springer

[5] *Salah A. Albermany, Fatima Radi Hamade, Ghazanfar Ali Safdar. New random block cipher algorithm, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT).*

[6] *Salah A. Albermany , Ali H. Alwan , " RADG design On Elliptic Curve Cryptography " , ICCIIDT Conference UK , 11-12 October 2016 .*

[7] *Salah Albermany, Maryam Nathim, Zahir Hussain, CRADG: A chaotic RADG security system, Journal of Engineering and Applied Sciences, 12: 4118-4122. 10.3923/jeasci.2017.4118.4122*

[8] *Salah A.K. Albermany, Duha Amer and Kamal, S-RADG: A Stream Cipher RADG Cryptography. Journal of Engineering and Applied Sciences, 13: 2317-2321, 2018.*

[9] *Zahraa Naseer, and Salah Albermany , McEliece in RADG using Diffie-Hellman Security System IJSER journal Publication for Volume 9, Issue 5, May 2018.*
[10] *W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Informaton Theory 22 (1976), 644–654.*
[11] *I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography, Mathematical Research Letters 6 (1999) 287–291.*
[12] *E. Artin, Theory of braids, Annals of Math. 48 (1947), 101–126.*
[13] *Eda, K. and T. Kaneto, Infinitary braid groups. arXiv preprint arXiv:1704.02591, 2017.*
[14] *Chiodo, M., An introduction to braid theory. Msc, University of Melbourne, 2005.*

## Author Profile

**Adil. Alramahi** I am adopted as appointed to the University of Kufa, the title of scientific researcher in the year 1992 and then got Al master's degree in mathematics / stability of large systems enacted in 1995 and then got the title of a teacher in 1999 and then assistant professor in 2002, professor and professorship in 2014 that I got a doctorate in 2005 in mathematics / fractal geometry. During functional my career exercised several leadership as assistant of dean or head of department and the presidency or membership of the ministerial committees and universal. Several research in magazines and conferences, local and international, such as Basra, London, Paris, Zurich and Los conferences .My research interests in the areas of fractals , stability , encoding , information and numerical analysis.