ISSN: 0974-5823 Vol. 7 No. 3 March, 2022

International Journal of Mechanical Engineering

Data Authentication System by Using Non-commutative

[1]Sabreen Jassim Bani; [2]Yahya M. Abul–Abbass; [3]Salah A. Albermany;

[4]Kareem Abbas Alghurabi

[1]Al-furat Al-awsat Technical University/sabreen.bani@atu.edu.iq

[2] University of Kufa/ Salkareemalghurabi@yahoo.com

[3] University of Kufa/ salah.albermany@uokufa.edu.iq

[4]babylon University, Iraq/; kareemalghurabi@yahoo.com

.

Abstract

The group is among the most fundamental algebraic building blocks. Non-commutative algebraic structures, such as semigroups, groups, and rings, serve as the foundation for the cryptographic primitives, techniques, and systems used in this branch of cryptology. For resolving issues with key exchange, encryption-decryption, and authentication, non-commutative cryptographic methods have been devised. Using a newly proposed Non-commutative group, a novel data authentication scheme is suggested in this study. The suggested Non-commutative group overcomes the primary issue with the earlier groups, which is how to make it acceptable for authenticating purposes while also overcoming the difficulty of partition.

***Keywords*: Non-commutative cryptography, Authentication, Group.**

1. Introduction

Due of information overlap and easy access to information over the Internet, security considerations are now more important than ever [1]. In order to access the network facility, an intending principal must first offer authentication, which is primarily a secret process that relies on the usage of passwords and encryption keys [2]. Authentication, often known as origin integrity, is a way to gauge how certain one can be that the source of data is who it claims to be. An algebraic structure is a collection of elements with an operation (equally referred to as application) that maps any two elements in the set uniquely onto a third element. The axioms that an algebraic structure satisfies provide the specificity of the structure [3]. A group is a nonempty set G on which a binary operation (a, b) ab is defined meeting [4][5] the aforementioned criteria.

ab is in G if and only if a and b are members of G.

For all a, b, and c G, associativity equals (ab)c.

Identity: There is an element 1 in G such that for every an in G, a1 = 1a = a;

Reverse: If element an is present in G, then element a1 is present in G such that

$aa^{-1} = a^{-1}a = 1$.

If ab = ba for all a, b in a group G, then the binary operation is commutative and the group is abelian. In this instance, the binary operation is frequently expressed as an additive formula ((a, b) a + b), where identity is expressed as 0 rather than 1 [6][7].

2. Related Works

A novel and effective key agreement protocol with a trusted third party (TTP) is suggested in [8]. The proposed protocol makes use of a non-commutative group's property. They provided the protocol's security proof while

taking into account the fact that the decomposition and conjugacy search problems are challenging in a non-commutative group.

The hidden subgroup or subfield problem is the foundation of the suggested group in [9]. (HSP). Establishing cryptographic techniques for the extra-special group is the manuscript's main goal (ESG). For the resolution of an open problem, ESG demonstrates one of the most suitable non-commutative platforms. The key exchange, encryption-decryption, and authentication procedures are secured using random polynomials that are selected by the communicating parties. Supporters of Heisenberg, the dihedral order, and the quaternion group. In addition, this is improved from the basic group members to corresponding ring elements, which are used in cryptographic methods and are known to the monomial generations. In this sense, peculiar or special matrices exhibit the possible benefits. The proposed strategy is solely based on the customary sparse matrices, and an analysis report that satisfies the key cryptographic requirements is presented. Using length-based, auto orphism, and brute-force approaches, it is harder to break the order of this group.

In [10], they put out a revolutionary authentication mechanism that protects the provers' privacy. The suggested technique is symmetric-key based, making it suitable for resource-constrained applications in large-scale contexts. A common illustration of such an application is an RFID system, where the provers are inexpensive RFID tags and the total number of tags used may be very high. In their analysis of the suggested system, they demonstrate that it outperforms the well-known key-tree-based strategy for private authentication in terms of both efficiency and privacy.

Provide three braid-based authentication techniques in [11], two of which are interactive proofs of knowledge with zero prior information. Then we talk about how they could be implemented, using normal forms or a different braid approach called handle reduction, which can be quite effective in certain situations

3. Elements of the Proposed Authentication System

3.1 HAK Group

Let HAK(n.m) is an infinite non-commutative Group generate from a set A of order 4mn+1, where m >1, n≥1, and m, n∈$\mathbb{Z}$, let

$$F^{+n} \subseteq \mathbb{Z},\ F^{-n} \subseteq \mathbb{Z}, F = F^{+n} \cup F^{-n}, and\ F^{*} = \{0\} \cup F$$

where

$$F^{+n} = \{1,2,\dots,n\}, and\ F^{-n} = \{-1,-2,\dots,-n\}$$

then

$$A = \bigcup_{i=-n}^{n} A_i, \qquad m > 1, m \in \mathbb{Z}$$

$$where \quad A_i = \bigcup_{j=1}^{m} \{a(i)_j, a(i)_{-j}\}, \qquad i \in F^{+n}$$

$$and \quad A_{-i} = \bigcup_{j=1}^{m} \{a(-i)_j, a(-i)_{-j}\}, \qquad i \in F^{+n}$$

Such that

1- $e = a(0)_j$, The identity element, such that
$e * a(i)_j = a(i)_j * e = a(i)_j \ \ , i \in F, j = 1,2,..,m$
2- $p = a(0)_{-j}$, $j = 1,2,..,m$ such that $p * p = e$
3- $p * a(i)_j = a(i)_r$, $j \in F, and\ i = 1,2,\dots$

$$where\ r = \left(\frac{j}{|j|}\right)(|j| - (m+1))$$

4- $a(i)_j * p = a(i)_{-j} \quad j \in F\ , and\ \ i = 1,2, \ldots$

5- $a(i+1)_j = a(i)_{-|j|} * a(1)_r,\ \ i = 1,2, \ldots$

$$where\ r = \left(\frac{j}{|j|}\right)(|j| - (m+1))\ \ , and\ \ j \in F$$

Example (1): let $n = 1$, and $m = 2$, then

$$\mathrm{A}_1 = \{R_u, R_{-u}, L_d, L_{-d}\} \equiv \{a(1)_1, a(1)_{-1}\ , a(1)_2, a(1)_{-2}\},$$

such that

$$R_u^{-1} = R_u\ , R_{-u}^{-1} = L_{-d}, L_d^{-1} = L_d\ , and\ \ L_{-d}^{-1} = R_{-u}$$

Then

$$\mathrm{A}_{-1} = \left\{R_u^{-1}, L_{-d}^{-1}, L_d^{-1}, R_{-u}^{-1}\right\} \equiv \{a(-1)_1, a(-1)_{-2}\ , a(-1)_2, a(-1)_{-1}\}$$

$$A = \mathrm{A}_{-1} \cup\ \mathrm{A}_1$$

The generation set is $\{p\} \cup$ A of order 9.

$where\ p * p = e, and\ e * \alpha = \alpha * e = \alpha\ ,\ \forall\ \alpha \in A$

Representation of HAK Group of order 9

The representation of a group HAK(1,2) is, to begin with, simply a homomorphism

$$\phi: HAK(1,2)\ \rightarrow GL_2(\mathbb{R})$$

A matrix representation of degree 2 of HAK(1,2) over $\mathbb{R}$, where $\mathbb{R}$ is a real number set and $GL_2(\mathbb{R})$ is the group of matrices generated by the following set of Matrices , $e = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, p = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, and

$$R_u = \begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}, R_{-u} = \begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix}, L_d = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, L_{-d} = \begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}$$

$$R_u^{-1} = \begin{pmatrix}2^{-1} & 0\\ 0 & 1\end{pmatrix},\ L_{-d}^{-1} = \begin{pmatrix}0 & 1\\ 2^{-1} & 0\end{pmatrix}, L_d^{-1} = \begin{pmatrix}1 & 0\\ 0 & 2^{-1}\end{pmatrix}, L_{-d}^{-1} = \begin{pmatrix}0 & 2^{-1}\\ 1 & 0\end{pmatrix}$$

3.2 Protocols used in authentication

Let's say Bob wants to verify that Alice is the true sender of a message.

Assume that G is a non-commutative group and that A and B are its subgroups, with ab equaling ba for all an in A and b in B.

The selection and publication of an element w from G.

In order to publish the pair (w, t) where t = w s, Alice selects a private s from A.

Bob picks a r from B and challenges Alice with w' = w r.

Bob receives Alice's response, which is w" = (w ') s.

Bob determines if w" = t r. This would establish Alice's identity if it were true.

4. Conclusions

An innovative, secure authentication technique is introduced in this work. The suggested system is built around the use of a brand-new non-commutative group. The non-commutative group that the proposed system uses was developed to get over the drawbacks (the difficulty of division) of the original groups, making it appropriate for the proposed authentication system. In addition to being utilized for authentication, the suggested non-commutative group can also be used for coding and cryptography.

References

[1] Maria Papathanasaki, Leandros Maglaras and Nick Ayres (2022), Modern Authentication Methods: A Comprehensive Survey. AI, Computer Science and Robotics Technology 2022(0), 1–24.

[2] M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui, "New enhanced authentication protocol for Internet of Things," in *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1-9, March 2021, doi: 10.26599/BDMA.2020.9020010.

[3] Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. In: Information and software technology. Chile: Chillán; 2018.

[4] Kengo Matsumoto; "A Simple Purely Infinite C*-algebra Associated with A Lambda-graph System of The Motzkin Shift", MATHEMATISCHE ZEITSCHRIFT, 2004.

[5] Selene Sanchez-Flores; "The Lie Structure On The Hochschild Cohomology Of A Modular Group Algebra", ARXIV MATH.RA, 2011.

[6] Sonia Natale; "Hopf Algebra Extensions Of Group Algebras And Tambara-Yamagami Categories", ARXIV-MATH.QA, 2008.

[7] Flavio D'Alessandro; *"Free Groups of Quaternions"*, INT. J. ALGEBRA COMPUT., 2004.
[8] Atul C. , Manoj K., S.P. Tripathi, Varun S. , "An Authenticated Key Agreement Protocol Using Artin's Braid Group" , International Journal of Computer Sciences and Engineering, 2017.

[9] Gautam Kumar, Hemraj Saini, "Novel Noncommutative Cryptography Scheme Using Extra Special Group", *Security and Communication Networks*, vol. 2017, Article ID 9036382, 21 pages, 2017. https://doi.org/10.1155/2017/9036382

[10] G. Avoine, L. Buttyant, T. Holczer and I. Vajda, "Group-Based Private Authentication," 2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Espoo, Finland, 2007, pp. 1-6, doi: 10.1109/WOWMOM.2007.4351808.

[11] Hervé Sibert, Patrick Dehornoy, Marc Girault, Entity authentication schemes using braid word reduction, Discrete Applied Mathematics, Volume 154, Issue 2, 2006, Pages 420-436,

ISSN 0166-218X, https://doi.org/10.1016/j.dam.2005.03.015.