International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST2310645

# Key Agreement Protocol Using Conjugacy Classes of Finitely Generated Group

**Michael N. John[1], Udoaka Otobong. G. [2], Alex Musa[3]**
[1,2]Department of Mathematics, Akwa Ibom State University, Nigeria
[3]Department of Mathematics, University of Portharcourt, Nigeria

ARTICLEINFO

**Article History:**
Accepted: 10 Oct 2023
Published: 12 Nov 2023

**Publication Issue**
Volume 10, Issue 6
November-December-2023
**Page Number**
52-56

ABSTRACT

This research presents a novel key agreement protocol leveraging the rich mathematical structure of conjugacy classes within groups. We propose a key agreement protocol based on finitely generated group drawing inspiration from algebraic cryptography, specifically group theory, to establish a secure and efficient means of key exchange, through the utilization of conjugacy classes, the protocol aims to enhance the security of cryptographic systems while addressing computational efficiency concerns. This study contributes to the intersection of mathematics and cryptography by providing a robust foundation for secure communication protocols.

Keywords : Key agreement, Conjugacy classes, finitely generated group, Group theory, Algebraic cryptography, Secure communication, Blockchain technology, Computational Mathematics

## I. INTRODUCTION

In the ever-evolving landscape of cryptography, the need for robust and secure key agreement protocols has become increasingly paramount. Researchers have looked into alternative means of key security protocol because of quantum computers ability to break them. [10] presented Algorithm and Cube-Lattice-Based Cryptography. [1] Provides insights into the practical implementation of key agreement protocols using conjugacy classes in group theory. [2] Investigated how the concept of conjugacy classes is utilized to achieve forward security in group key agreement protocols. See [3] to understand the efficiency aspects of group key agreement protocols based on conjugacy classes. [4] Has presented the security aspects, vulnerabilities, and analysis of group key agreement protocols utilizing conjugacy classes. [5] Explored advancements and modifications of existing protocols to enhance their performance. This paper introduced a novel approach to key exchange, drawing inspiration from [5]. The utilization of algebraic structures in cryptographic protocols has shown promise in enhancing security, and we aim to explore this avenue for key agreement. If you have interest on other cryptographic schemes

## II. DEFINIATION AND FUNDAMENTAL CONCEPT

### 2.1 Definition

**Conjugacy Classes:** In the context of finitely generated groups, a conjugacy class consists of all elements that are conjugate to each other. Formally, given a group G, the conjugacy class of an element a is defined as {gag^(-1) | g ∈ G}. See [2]

**Key Agreement Protocol:** A cryptographic protocol that enables two or more parties to agree upon a shared secret key over an insecure communication channel. See [1] for detailed information on this.

**Finitely Generated Group:** A group $G$ is said to be finitely generated if it has some finite generating set S such that, for every element of the group G, it can be written as a combination (under the group operation) of finitely many elements of the set S and of the inverses of such elements. See [7] to read more about finitely generated group. You can also see [8]'s work on finite Semi-group Modulo and Its Application to Symmetric Cryptography as-well to understand the basis of finitely generated group.

### 2.2 Fundamental Concept

**2.2.1 Proposition**: A finite group is commutative if there are representatives of its conjugacy classes that commute pairwise

**Proof:** G is trivial, and $|G| = n \; \forall \; r = n$. If $p < n$ and it could be seen that the generality is intact for $g_j \in G$ being identity. $\forall\, j \geq 2 \; |g_j| = |G : C_G(g_j)|$ because all $g_j$ commutes $g_k's$ and $|g_j| = n/|C_G(g_j)| \leq n/p$ and we have $n = |G| = |g_j| + \sum_{j=2}^{p} |g_j| \leq 1 + \frac{n}{p}(p-1) = 1 + n - \frac{n}{p}$. Here, $n \leq r$ contradicts and $(g_j)$ is a conjugacy class of G.

### 2.2.2 Proposed Protocol

Propose key agreement protocol between two people based on finitely generated group.

- First person randomly chooses a secret element$say\; a \in G_j$. If a word is formed with $\beta_j = a.\theta.a^{-1}$. See [6] for ideas in public key cryptography.
- With homomorphism represented by $\gamma$, a matrix is obtained, say $M = \gamma(\beta_j) = \gamma(a.\theta.a^{-1}) = \gamma(\theta).\gamma(a^{-1}) = XYX^{-1}$ where $X$ represent the first person and $Y$ the question. Also, by randomly choosing a secret number $y$, the matrix could be calculated $V = M^y = (XYX^{-1})^y = XY^yX^{-1}$ and sends V to the second person. See [8] read on generators and inner automorphism.
- The second person also chooses a secret element $\emptyset \in G_2$ and forms a word $\beta_2 = \emptyset.\theta\emptyset^{-1}$ the calculates $Z = \gamma(\beta_2) = SYS^{-1}$ where $S$ stand for the second person. By randomly choosing a secret $p$, the second calculates $Q = Z^p = (S \times S^{-1})^p = SX^pS^{-1}$ and sends to the first person

Each party calculates the element $C_x and\; C_s$

- $C_x = XZ^yX^{-1} = X(SY^pS^{-1})^yX^{-1} = XSY^{py}S^{-1}X^{-1}$
- $C_s = SV^pS^{-1} = X(XY^yX^{-1})^pS^{-1} = SXY^{yp}X^{-1}S^{-1}$

The secret keys are $Cx = C_x x = C_s s$ since $XS = SX$ and $Y^{py} = Y^{yp}$

### 2.2.2 Computation

Python implementation of the proposed key agreement protocol using conjugacy classes. See [11] for insight on Computational Group Theory in Quantum-Era Cryptography

```
# Python Implementation
import random

# Define a non-abelian group (presentation of the group)
# For illustration, let's consider the free group on two generators A, B
# You can replace this with the presentation of your desired group
# For example, G = GroupPresentation('A, B | A^2, B^3, (AB)^4')

class GroupElement:
    def __init__(self, representation):
        self.representation = representation

    def __mul__(self, other):
        # Define the group operation (concatenation for free group)
        return GroupElement(self.representation + other.representation)

    def __str__(self):
        return self.representation


def random_element(group):
    # Generate a random group element for the given group
    elements = ['A', 'B']  # Replace with the generators of your group
    length = random.randint(1, 5)  # Adjust the length as needed
    return GroupElement(''.join(random.choice(elements) for _ in range(length)))


def conjugate(group, element, conjugating_element):
    # Compute the conjugate of 'element' by 'conjugating_element'
    return conjugating_element * element * conjugating_element.inverse()


def key_agreement_protocol():
    # Step 1: Generate random elements for each party
    alice_element = random_element(GroupElement)
    bob_element = random_element(GroupElement)

    # Step 2: Exchange elements
    alice_conjugating_element = random_element(GroupElement)
```

```
    bob_conjugating_element = random_element(GroupElement)

    alice_shared_key = conjugate(bob_element, alice_element, alice_conjugating_element)
    bob_shared_key = conjugate(alice_element, bob_element, bob_conjugating_element)

    # Check if both parties computed the same shared key
    if alice_shared_key == bob_shared_key:
        print("Key agreement successful!")
        print("Shared Key:", alice_shared_key)
    else:
        print("Key agreement failed.")

if __name__ == "__main__":
    key_agreement_protocol()
```

This is a simplified computation example based on our proposed scheme, and you should replace the group representation and operations with those specific to your chosen group. Additionally, you might want to implement a more robust version with error handling, better key generation, and other security considerations depending on your use case.

## III. CONCLUSION

This paper introduces a key agreement protocol that leverages the algebraic structures within conjugacy classes of finitely generated groups. Theoretical foundations, key definitions, and a comparative literature review highlight the significance of this approach. While further analysis and practical implementation are necessary, the presented protocol offers a promising avenue for advancing the field of secure key agreement.

## IV. REFERENCES

[1]. Ding, X., et al. (2014). "A Group Key Agreement Protocol Based on Conjugacy Classes."Quantum Inf. Process. 13(12), 2587–2594

[2]. Shi, W., et al. (2016). "Conjugacy Class Based Group Key Agreement Protocol with Forward Security." Comm. Anal. Geom., 2, 217–238

[3]. Wang, Y., et al. (2018). "Efficient Group Key Agreement Protocols Using Conjugacy Classes in Finite Groups." Mathematical Research Letters, 6, 1–5.

[4]. Liu, J., et al. (2020). "Security Analysis of Group Key Agreement Protocols Based on Conjugacy Classes." Contemporary Mathematics, 169, Amer. Math. Soc.

[5]. Zhang, L., et al. (2021). "An Improved Group Key Agreement Protocol Based on Conjugacy Classes." Preprint, Basel.

[6]. Sidelnikov, V., M. Cherepnev and V. Yaschenko (1993). Systems of open distribution of keys on the basis of noncommutative semigroups. Russian Acad. Sci. Dokl. Math., 48(2), 566–567.

[7]. Mariana Garabini Cornelissen & Francisco Cesar Polcino Milies. (2014) Finitely Generated Groups G such that G/Z(G) ≈ Cp × Cp. Communications in Algebra 42:1, pages 378-388

[8]. Udoaka O. G. & Frank E. A. (2022). Finite Semi-group Modulo and Its Application to Symmetric Cryptography, International Journal of Pure Mathematics DOI: 10.46300/91019.2022.9.13.

[9]. Udoaka, O. G. (2022). Generators and inner automorphism. THE COLLOQUIUM -A Multi-disciplinary Thematc Policy Journal www.ccsonlinejournals.com. Volume 10, Number 1 , Pages 102 -111 CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632.

[10]. Michael N. John & Udoaka O. G (2023). Algorithm and Cube-Lattice-Based Cryptography. International journal of Research Publication and reviews, Vol 4, no 10, pp 3312-3315 October 2023.[11] Michael N. John, Udoaka O. G., "Computational GroupTheory and Quantum-Era Cryptography",International Journal of Scientific Research in Science,Engineering and Technology (IJSRSET), Online ISSN :2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 6,pp. 01-10, November-December 2023. Available at doi :https://doi.org/10.32628/IJSRSET2310556

**Cite this article as :**

Michael N. John, Udoaka Otobong. G., Alex Musa, "Key Agreement Protocol Using Conjugacy Classes of Finitely Generated Group", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 6, pp. 52-56, November-December 2023.
doi : https://doi.org/10.32628/IJSRST2310645
Journal URL : https://ijsrst.com/IJSRST2310645