American Journal of Applied Mathematics
2026, Vol. 14, No. 2, pp. 46–52
https://doi.org/10.11648/j.ajam.20261402.12

SciencePG
Science Publishing Group

Research Article

# Finite Subgroup Automorphism of Infinite Group and Its Application to Symmetric Cryptography

**Frank Emmanuel Akpan***

Department of Mathematics and Statistics, Federal University, Otuoke, Nigeria

## Abstract

The study of automorphisms of algebraic structures plays a central role in understanding their internal symmetries and structural behavior. This work investigates the automorphism structure induced by *finite subgroups within infinite groups*, with particular emphasis on how these automorphisms can be characterized, classified, and effectively utilized. The focus is on the interaction between a finite subgroup and the ambient infinite group, analyzing how subgroup-preserving automorphisms extend to global automorphisms and how constraints imposed by finiteness influence the overall automorphism group. Special attention is given to classes of infinite groups such as abelian, conjugacies, and certain residually finite groups where finite subgroup automorphisms exhibit rich and tractable behavior. Building on this theoretical framework, this work explores *applications to symmetric cryptography,* where algebraic symmetry and complexity are essential for secure cryptographic design. Finite subgroup automorphisms are shown to provide a promising foundation for constructing cryptographic primitives, including key generation mechanisms, conjugacy-based encryption schemes, and secure mixing transformations. The inherent difficulty of reversing automorphism actions in large infinite groups, combined with the controlled structure of finite subgroups, offers a balance between computational efficiency and cryptographic strength. In overall, this work bridges abstract group theory and practical cryptographic applications, demonstrating that finite subgroup automorphisms of infinite groups constitute a viable and mathematically robust framework for advancing symmetric cryptographic systems.

## Keywords

Isomorphism, Homomorphism, Normal Subgroups, Automorphism, Cryptography, Conjugate Elements, Equivalence Class, Equivalence Relation

## 1. Introduction

Group theory, a central branch of abstract algebra, plays a crucial role in the understanding of symmetry and structure in mathematical systems. Among the vast array of concepts within group theory, the study of automorphisms from a group to itself has proven fundamental to understanding the internal symmetries and structural transformations of algebraic objects. Automorphisms not only reveal the intrinsic structure of a group but also allow us to classify groups up to structural similarity. While the study of automorphisms is well-developed for finite groups, especially due to their concrete structure and computability, the behavior of automorphisms in infinite groups presents additional layers of complexity., of particular interest is the interaction between *finite subgroups* and the automorphism group of an infinite group. Understanding

*Correspondence: Frank Emmanuel Akpan (frankea@fuotuoke.edu.ng)

**Received:** 16 February 2026; **Accepted:** 2 March 2026; **Published:** 16 March 2026

how finite subgroups can be preserved, permuted, or acted upon by automorphisms of the whole group provides insight into the group's global structure. This work focuses on finite subgroup automorphisms within infinite groups, a topic that bridges finite and infinite group theory. The goal is to explore conditions under which automorphisms preserve finite subgroups, characterize such automorphisms, and examine its applications specifically to cryptography for algebraic structures that are particularly rich, such as the symmetric or permutation group $S_3$.

A " Finite subgroup automorphism of an infinite groups" refers to a group where the number of elements is finite embeded in an infinite group such that the correspondence f is an isomorphism while still preserving its structure. Howbeit, the group being acted upon (the Infinite group) contains infinitely many elements; essentially, it means that while there are only a limited number of distinct transformation you can apply to the Infinite group, the group itself is still infinitely large.

Although, not every Infinite group will have a finite subgroup of automorphism, studying finite group automorphism of infinite groups can be useful in various areas of mathematics, including algebraic topology and its Theory with diverse applications including cryptography. The concept of *finite subgroup automorphisms (Inner Automorphim or conjugacy) of infinite groups* refer to the ways in which finite subgroups behave under automorphisms of a larger infinite group. Specifically, one may ask: How are finite subgroups preserved, fixed, or permuted by the automorphism group of an infinite group? What restrictions or structures emerge from such interactions? This area is not only theoretically appealing but also important in applications such as Cryptography and the study of Lie groups.

## 1.1. Statement of the Problem

Infinite groups often contain abundance of finite subgroups, each with potentially unique structural properties. However, not all automorphisms of an infinite group necessarily preserve these finite subgroups. This raises several questions: Under what conditions do automorphisms preserve the structure of finite subgroups? Can every automorphism of a finite subgroup extend to an automorphism of the whole infinite group? The problem of this study is: How do we apply finite automorphism subgroup of infinite group for solution to several real life problems, in Particular to cryptography? This study aims to investigate these questions and provide a systematic analysis of how finite subgroups behave under the automorphisms of infinite groups and apply the results to symmetric cryptography.

## 1.2. Literature Review

An automorphism of a group G is a bijective homomorphism from G to itself. The set of all such mappings forms a group under composition, denoted Aut (G). This concept is crucial in understanding the symmetries of a group structure. Early works by Carley A. and Dedekind M. laid the foundation for automorphism theory [2]. More recent treatments provided in-depth classifications of inner automorphisms (conjugation by group elements) and outer automorphisms (those not arising from conjugation) [4, 6, 13]. These works emphasize that for infinite groups, especially non-abelian ones, Aut(G) can be vastly more complex than in the finite case.

## 1.3. Infinite Groups and Their Subgroups

Infinite groups include cyclic groups like $Z_n$, free groups, and linear groups such as $GL_n(R)$. These groups often contain many finite subgroups. For example, torsion elements forming finite cyclic subgroups in general linear groups or orthogonal groups showed that certain infinite locally finite groups always contain infinite abelian subgroups, which has implications for their automorphism structure [1, 7, 14]. The existence of a rich variety of finite subgroups in these groups presents challenges when classifying automorphisms.

## 1.4. Automorphisms Preserving Finite Subgroups

A central theme of this study is to investigate automorphisms that preserve (or fix setwise) finite subgroups. Automorphisms may:

1) Fix every element of a finite subgroup (trivial action),
2) Fix the subgroup as a set but permute elements (e.g., via inner automorphisms),
3) Map one finite subgroup to another isomorphic one.

In the case of the infinite cyclic group $(Z_n,\times)$ for instance, automorphisms are determined by multiplication by ±1, which preserve all finite subgroups (trivial in this case). In free groups, the work of Dempwolff focused on automorphisms that preserve cyclic or more generally, finite-rank subgroups [4].

Studies by [5, 11, 15] extended these ideas to consider automorphisms of infinite p-groups and their fixed points, indicating deeper structural constraints.

## 1.5. Review of Literature on Cryptography

D'Alconzo, Di Scala, Frank, E. A., Udoaka, O. G., González Vasco, M. I., Kahrobaei, D., and McKemmie, E. defined Cryptography as the practice and the study of methods of protecting or securing communication from third party [5, 8, 9].

More generally, Cryptography is concerned with the practice of setting out protocols for secure communication without the influence or interference of third party. Cryptography is related to various aspect of information security. Symmetric cryptography is all about the sender and the receiver of a message using the same key for encryption and decryption respectively.

González Vasco, M. I., Kahrobaei, D., McKemmie, E., Kamali Ardekani, Davvaz B., Mellaro M., Canelli R. and Krawczyk H. suggested a new algorithm which should be used for encryption and decryption of messages and images where one sends an encrypted message to another party without the interference of a third party [9, 11, 12].

Dan Boneh and Jiang describe how both black and white images in tagged image file format could be encrypted and decrypted using blowfish algorithm and other Algorithms [3, 10].

## 2. Material and Methodology

### 2.1. Conjugate (Inner Automorphism) Elements

*Theorem 1*

Let G demote a group (finite or infinite) and let H < G be a finite subgroup. For every h∈H, there exists a conjugate of h in G.

Moreover, if g∈G, then ghg$^{-1}$ ∈gHg$^{-1}$ and gHg$^{-1}$ is also finite.

*Proof*

Two elements "a" and "b" in G are said to be conjugate elements if there exist an element g ∈ G such that $a = gbg^{-1}$, the element 'a' is called the conjugate of the element 'b'. Also, the element 'b' is called the conjugate of the element 'a' if $b = gag^{-1}$. This means that if H < G, for g, h∈G, the conjugate of h by g is ghg$^{-1}$. Now, take g = e (identity of G). Then, ehe$^{-1}$ = h. This shows that every element is conjugate to itself. So, conjugate always exists. Next, is to show that these conjugate elements is finite. Consider the map $\phi_g$: H → gHg$^{-1}$, $\phi_g$ (h) = ghg$^{-1}$. Notice that this map is well defined, Bijective and satisfies the group isomorphism condition. Hence, $\left|gHg^{-1}\right| = |H|$.

*Corollary*

The following are true about conjugate elements.

1) In the operation $a = gbg^{-1}$ or $b = gag^{-1}$, the elements are equivalence relations.
2) The equivalence classes formed are called conjugate classes. In this work, such equivalence classes is of importance and are used for the encryption and decryption algorithms of the cryptosystem.

### 2.2. Properties of Conjugate Elements

Let G demote a finite subgroup automorphism of infinite group where $G = \{a_1, a_2, a_3, \ldots. a_n\}$ and $a_i \in G. \ni a; = gb\ g^{-1}, \forall a;, b; \in G.$ The equivalence classes formed by the conjugate elements which are conjugate classes satisfy the following.

1) Same order:

A conjugate element has the same order.

*Theorem 2. Order of an Element*

Let G be a finite group and H a subgroup automorphism of G.. An element a ∈ $G$ has an order n if there exist a positive number n such that $a^n = e$ and the order of 'a' divides the order of G.

*Proof.*

Let G be a finite group and a∈G. Consider the cyclic subgroup generated by a defined by < a> = {e,a,a2,a3,…..} using the definition of order of an element. Now, by Lagrange theorem, since < a> itself is a subgroup of G, we have $|\langle a\rangle| \mid |G|$. But $|\langle a\rangle| = |a|$. Hence, $|a| \mid |G|$.

2) Preserve Structure:

Conjugation is an inner automorphism (ie it preserves the group operation).

### 2.3. Examples of Algebraic Structures With Conjugate Elements

(a) Consider $GL(n, \mathbb{R})$. The general linear group. Let $A, B \in GL(n, \mathbb{R})$. If A and B are conjugate elements. Then, $B = PAP^{-1}$ *and* $A = PBP^{-1}$. The following are true about A and B.

(i) Same determinant (ii) Same eigen values (iii) Trace are also same.

(b) The Algebraic Structure $S_3$

Consider the group $S_3$ which is finite, $S_3$ is the symmetric group of order 6. ie $|S_3| = 6$, group automorphism is satisfied in $S_3$. Furthermore, $S_3$ has conjugate elements that have all the properties listed above. Infact, let $S_3 = \{\emptyset_0, \emptyset_1, \emptyset_{2_2}, \varphi_1, \varphi_2, \varphi_3\}$, we shall show that the finite group $S_3$ has three partitions. The first partition is $\emptyset_0 = e$, the next partition is $\{\emptyset_{1,}, \emptyset_2\}$ and the third partition is $\{\varphi_1, \varphi_2, \varphi_3\}$. First, we list the element of $S_3$ with the operation being the usual composition of functions since $S_3$ elements are themselves functions.

$$\left\{\emptyset_0 = e = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = (1)\right\}$$

$$\left\{\begin{matrix} \emptyset_1 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = (132) \\ \emptyset_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (123) \end{matrix}\right\}$$

$$\left\{\begin{matrix} \varphi_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = (2\ 3) \\ \varphi_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = (1\ 2) \\ \varphi_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = (1\ 3) \end{matrix}\right\}$$

Notice the three partitions as signifies by the braces above. Suppose that we pick any element say from $p_1, p_2$ where

$p_1, p_2$ *and* $p_3$ denote the first, second and third partition respectively, suppose further that $\varphi_1$ is picked. Then, we want to find the corresponding element which is the conjugate of $\emptyset_1$. Recall that an element 'a' is a conjugate element to 'b' if $a = gbg^{-1}$ *or* $b = gag^{-1}$ where b is the conjugate to 'a' Note that $gg^{-1} = e$, so that $gcg^{-1} = g(c)g^{-1} = ce = ec = c$.

$$\text{Now, } \varphi_1^{\,2} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \varphi_2 = (123)$$

$$\varphi_2^{\,2} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \varphi_1 = (132)$$

$$\text{Also } \psi_1^{\,2} = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \emptyset_o = e$$

$$\psi_2^{\,2} = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \emptyset_o = e$$

$$\psi_3^{\,2} = \begin{pmatrix} a & b & a \\ c & a & c \end{pmatrix} 0 \begin{pmatrix} a & b & c \\ c & b & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \emptyset_o = e$$

$$\varphi_2 o\ \varphi_1 = \varphi_1\ o\ \varphi_2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \emptyset_o = e$$

$$\psi_1 o\ \psi_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \varphi_2$$

$$\psi_2 o\ \psi_1 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} 0 \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \varphi_1$$

$$\psi_1 o\ \psi_3 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & v \end{pmatrix} = \varphi_1$$

$$\psi_3 o\ \psi_1 = \begin{pmatrix} a & b & c \\ a & b & b \end{pmatrix} 0 \begin{pmatrix} a & b & c \\ b & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \varphi_2$$

$$\psi_2 o\ \psi_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \varphi_2$$

$$\psi_3 o\ \psi_2 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \varphi_1$$

Next, we want to take a function from each partition and investigate whether they can satisfy the conjugacy properties. (*ie* $\varphi_1 o \psi_1, \varphi_1 o \psi_2$ *and* $\varphi_1 o \psi_3$ etc. first. We compute

$$\varphi_1 o\ \psi_1 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \psi_2$$

$$\psi_1 o\ \varphi_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = \psi_3$$

$$\varphi_1 o\ \psi_2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = \psi_3$$

$$\psi_2 o\ \varphi_1 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \psi_1$$

$$\varphi_1 o\ \psi_2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = \psi_3$$

From the above we notice that $\forall ab \in P$, where P is any partition of $S_3, ab \neq ba$. This property makes it difficult for any attacker to break any cryptographic system designed using finite automorphism of infinite group structure.

Our interest in this section is on the conjugate element. If 'a' and 'b' are two elements from any finite group. Then $a = g^{-1}bg = gbg^{-1} = gg^{-1}(b) = b(gg^{-1}) = be = eb = b$ . In our above investigations, we see that the only elements satisfying the conjugate properties are:- $\varphi_1 = \psi_3\{\psi_2 o \psi_1\}\psi_3^{-1}, o\ \psi_2 = \varphi_1\{\psi_1 o \psi_2\}\varphi_2, o\ \psi_1 = \psi_2\{\psi_2\ o\ \varphi_1\}\psi_2^{-1}$ etc. we can apply this concept to cryptographic system to encrypt and decrypt data. Such cryptographic system can with stand any attacker. In what follows, we show how this concept could be used in cryptography.

## 2.4. Automorphism - Based Cryptosystem

In this section, it is shown the methods or ways in which conjugate based cryptosystem works. Recall that for any elements 'a' and 'b' in G, we say that 'a' is conjugate to 'b' if $a = gbg^{-1}. a, b, g \in G$ a finite subgroup or group. With this concept, it is possible to encrypt or decrypt any text. Suppose that a sender A wants to send a message to a receiver B, recall further that the set $S_3 = \{\emptyset_o, \varphi_1, \varphi_2, \psi_1, \psi_{2,} \psi_3\}$. The message could be stored in say $\phi_1$. Thus, instead of the sender A to send $\varphi_1$ to the receiver B, he/she encrypt the message using $\psi_3\{\psi_2 o\ \psi_1\}\psi_3^{-1}$. Then, the receiver B decrypt it to get $\varphi_1$.

Note: $\varphi_1 = \psi_3\{\psi_2 o\ \psi_1\}\psi_3^{-1}$, $\varphi_1$ could also be equal to $\psi_2\{\psi_3 o\ \psi_2\}\psi_2^{-1}$ etc. in most cases, the decryption processes is linked to four digits password so that by entering these digits representing, $\psi_2, \psi_3, \psi_2\ and\ \psi_1^{-1}$, the message is decrypted. The receiver may want to change the original password to any digits of his/her choice for subsequent used. This idea could be used in other finite algebraic structures.

# 3. Application of Finite Automorphism Subgroup of Infinite Group

## 3.1. Symmetric Cryptography

Consider the finite group structures $S_3, D_4$ and in general $D_{2n}$. These finite group structures contain conjugate elements and the elements are partitioned into equivalence classes and are equivalence relation. Let us consider a specific structure $S_3$, the permutation or symmetric group.

$S_3 = \{\emptyset_0, \phi_1, \phi_2, \psi_1, \psi_2, \psi_3\}$.

The set $S_3$ has three partitions namely:- $\{\emptyset_0 = e\}, \{\phi_1, \phi_2\}\ and\ \{\psi_1, \psi_{2,} \psi_3\}$. Where e is the identity element, $\phi_1\ and\ \phi_2$ are the rotations and $\psi_1, \psi_{2,}\ and\ \psi_3$ are the symmetries of the vertices of an equilateral triangle respectively. For any two elements, 'a' and 'b' if $a = gbg^{-1}$ then, "a" is said to be the conjugate of "b" and $b = gag^{-1}$ implies that 'b' is the conjugate of "a".

## 3.2. Conjugate – Based Cryptographic Scheme

Due to the interference of third party in sensitive information both digital and non-digital, there is need for protecting information in order to avoid access by unauthorized persons. The idea of conjugate elements from finite algebraic structures which is automormophism in nature could be applied to cryptography in order to keep information safe in a cryptographic scheme from attackers. The procedures below show how to set up a cryptographic system using the idea of finite subgroup automorphism of infinite group. For $S_3 = \{\emptyset_0, \phi_1, \phi_2, \psi_1, \psi_{2,} \psi_3\}$.

Suppose that a person A wants to send the word "Be security conscious" to a recipient B. the sender A must store this message in any element of $S_3$ and encrypt it using the conjugate of the element in which the word was encrypted. The receiver after receiving the conjugate elements, decrypt it in order to get the original message using the equivalent class of the encrypted element. In computer programming, such encryption and decryption processes involve entering of password or codes which is programmed to represent the equivalent conjugate elements. The practical procedures is demonstrated below.

## 3.3. Practical Examples

Consider the finite group $S_3$. Suppose that Mr. A wants to send the message "Be security conscious" since each element of the group $S_3$ is a function, he can store the message in any element say $\phi`_1$ as follows;- $\phi`_1 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ Be & security & concious \end{pmatrix}$. Then, instead of sending the message using $\phi`_1$, he sends the message using the conjugate elements of $\phi`_1$ which is $\psi_3\{\psi_2 o\ \psi_1\}\psi_3^{-1}$. That is:- $\phi`_1 = \psi_3\{\psi_2 o\ \psi\}\psi_3^{-1}$.

The same is true for any element of the finite algebraic

structure $S_3$, messages can be stored in the same way. Thereafter, their respective conjugate elements of the stored element (s) is/are sent to the recipient, the recipient then decrypt them to get the original message using the equivalent conjugate. The fact that $\forall\, a, b \in S_3, ab \neq ba$ makes it more difficult for an attacker to break this cryptographic scheme.

### 3.3.1. Example

Send the message "The Area is not very safe". Show the encryption and decryption processes using the idea of conjugate elements of a finite algebraic structure $S_3$.

### 3.3.2. Solution

Let Mr. A denote the sender. Mr. B, the recipient

Then $S_3 = \{\emptyset_0\emptyset, \emptyset_2, \varphi_1, \varphi_2, \varphi_3\}$. Mr. A chooses an element of $S_3$ *say* $\varphi_2$ . So that $\varphi_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} f(a) & f(b) & s(c) \\ the & is & very \\ Area & not & safe \end{pmatrix}$ . $\varphi_2 = \varphi_1\{\emptyset_1, o\varphi_1\}\emptyset_2 = \varphi_2\{\emptyset_1 o \varphi_1\}\varphi_2^{-1}$

Mr A encrypts the message by storing it in $\psi_2$ using the conjugate elements of $\psi_2$ *ie* $\phi_1\{\phi_1, o\ \phi_1\}\phi_2$ *or* $\psi_2\{\phi_1\ o\psi_1\}\psi_2^{-1}$ send it to Mr. B. The recipient Mr. B then decrypt the message using the four digits password which represent the four conjugates elements. The procedures for manual decryption is shown below

$$\psi_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} f(a) & f(b) & s(c) \\ the & is & very \\ Area & not & safe \end{pmatrix} = \phi_1\{\phi_1, o\ \psi_1\}\phi_2$$

$$= \phi_1\,\phi_2\{\phi_1 o \psi_1\} \ldots \otimes$$

Note: that $\phi_1\, o\, \phi_2 = e \Longrightarrow \phi_1 o\, \phi_1^{-1} = e$ it means that $\phi_1\ and\ \phi_2$ are also conjugate elements. From equation $\otimes$, we have:

$\psi_2 = \phi_1\{\phi_1, o\ \psi_1\}\psi_1^{-1} = \phi_1\,\phi_1\{\phi_1 o \psi_1\} \ldots \otimes\otimes$

But $\phi_1 o \psi_1 = \psi_2$. Thus, from $\otimes\otimes$, $\psi_2 = \phi_1\phi_1^{-1}(\psi_2) = e\psi_1 = \psi_2 e = \psi_2$.

## 4. Summary, Conclusion and Recommendations

This work was carried out to investigate the application of finite automorphism subgroup of infinite group to symmetric cryptography. Based on this, the investigations in this study reveal that finite automorphism subgroup of infinite group is very effective in applications to symmetric cryptography. Thus, the following summary is made:

1) Finite automorphism subgroup of infinite group is an effective coding technique for both digital and non-digital data.
2) For any finite subgroup of infinite group, conjugates element becomes more effective when equivalent conjugates are large. We form a Finite automorphism conjugates of infinite group and use if for the encryption/decryption processes which are very impossible for attackers to break.
3) It is very difficult for any third party to have access to the message encrypted using finite automorphism subgroup of infinite group when applied to symmetric cryptography.

## 5. Conclusion

From investigations of this work, it can be concluded that the application of finite automorphism subgroup of infinite group to symmetric cryptography remains an effective coding technique and can be used to fight cultism, kidnapping and other social vices, thereby reducing such unlawful act if not eliminated totally.

## 6. Recommendations

The following recommendations are made by the researcher.

1) That all Security Agencies such as the Police, Army, Navy etc should encrypt all security Messages (information) both digital and Non-digital using the idea of finite automorphism subgroup of infinite group to avoid access by third parties since it has been proven by this study to be an effective encryption and decrypt on techniques. This will prevent security breaches.
2) Government Agencies should also encrypt sensitive document especially those that access to unauthorized persons are not allowed.
3) Qualified Mathematicians, Statisticians, Computer Scientists and programmers should be employed in all Security and Government Agencies to ensure that finite automorphism subgroup of infinite group is constructed adequately and are properly applied by computer programmers and cryto- Analists to Symmetric Cryptography in order to reduced or stop the access to sensitive documents by unauthorized persons from information regarding security.

## 7. Suggestions

1) This reseach work is restricted to the investigation of finite automorphism subgroups of infinite group and their applications to symmetric cryptography. It will be of benefit to the society if more investigations are made on their applications to many other problems facing the society.
2) It will also be of benefit if a study is carried out on infinite automorphism subgroup of infinite group and their applications for solutions to problems facing the society.

## Abbreviations

| | |
|---|---|
| $GL(n, \mathbb{R})$ | The General Linear Group of n Dimensions with Entries from $\Re$ |
| $S_3$ | The Permutation or Symmetric Group |
| $D_{2n}$ | The Dihedral Group of Order 2n |
| $\|G\|$: | The Order of a Group |
| $\|a\|$ | The Order of an Element 'a' |
| < a> | Generator |
| Aut(G) | Automorphism of a Group G |
| $Z_n$ | The Integer Modulo n |

## Author Contributions

**Frank Emmanuel Akpan:** Conceptualization

## Conflicts of Interest

The author declares no conflicts of interest.

## References


[1] Anju, & Jakhar, M. S. (2025). *Analyzing class-preserving automorphisms in infinite permutation groups*. International Journal of Applied and Behavioral Science.

[2] Cayley A. and Dedekind M. (1977). Symmetric Generation of Groups. Encyclopedia of Mathematics Volume 111. Cambridge university Press. Cambridge.

[3] Dan Boneh (2001). Identity- based encryption from the well-pairing. Annual International Encryption conference. 213-229.

[4] Dempwolff, U. (2026). *Automorphism groups of power functions*. Journal of Group Theory and Cryptography Methods, 17(4).

[5] D'Alconzo, G., & Di Scala, A. J. (2023). *Representations of group actions and their applications in cryptography*. IACR ePrint 2023/1247.

[6] Dummit D. S. and Foote R. M. (2004). Abstract Algebra (3rd Edition), John willy and sons Inc.

[7] Francesco De Geovanni and Catrina Ranone (2012). Infinite groups with many generalized normal subgroups. International journal of group theory. 1(3).

[8] Frank, E. A. and Udoaka, O. G. (2022). Finite Semigroup Modulo and its Application to Symmetric Cryptography. International journal of Pure Mathematics. Vol. 9, pp. 90-98, Art 13.

[9] González Vasco, M. I., Kahrobaei, D., & McKemmie, E. (2024). *Applications of finite non-abelian simple groups to cryptography in the quantum era*. La Matematica, 3, 588–603.

[10] Jiang, K. (2025). *A novel commitment construction framework based on cryptographic group actions*. IACR ePrint 2025/400.

[11] Kamali Ardekani and Davvaz B. (2022). On Subgroup Latices and Fuzzy Subgroups of finite groups $U_6$. Fuzzy Information and Engineering journal. Vol. 14, No 2. 152-166.

[12] Mellaro M., Canelli R. and Krawczyk H. (2009). Keying Hash function for Message authentication. Journal of Cryptology. 22(1), 1-61.

[13] Rotman, J. J. (1998). Journey into Mathematics: An Introduction to Proofs. adlibris.

[14] Scott Harper (2004). The spread of Finite and Infinite groups. Cambrige University Press.

[15] Zhang, Y., Liu, S., & Zeng, L. (2025). *Full automorphism group of (m,2)-graph in finite classical polar spaces*. Axioms, 14(8), 614.