ADSUJSR 13 (2) (2025) 107-118
Adamawa State University Journal of Scientific Research (ADSUJSR)
ISSN: 2705-1900 (Online); ISSN: 2251-0702 (Print)
https://www.adsujsr.adsu.edu.ng

THEORETICAL APPLICATION OF FINITE SIMPLE GROUPS IN CRYPTOGRAPHY

M. M. Dashar and D. Samaila*
Department of Mathematics, Adamawa State University Mubi, Nigeria
**Corresponding author email: samaila506@adsu.edu.ng*

Received in November 2025
Accepted in December 2025

Abstract
Finite simple group have been a fascinating area of research in abstract algebra, and their application in cryptography have shown promising results, particularly in the development of secure cryptographic protocols. Application of finite simple groups represents a profound theoretical achievement with significant implications for cryptography. This study investigates the fundamental properties, security implications, challenges, and practical applications of finite simple groups in cryptographic systems. The study explores the structural application of finite simple groups into Cyclic, Alternating, Lie-type, and Sporadic families, highlighting their unique attributes such as high order, irreducibility, and automorphism group complexity, which make them favorable for advanced cryptographic schemes. Key findings demonstrate that finite simple groups enhance cryptographic robustness due to their resistance to factorization and brute-force attacks, although challenges such as computational inefficiencies and compatibility with established standards remain barriers to widespread adoption. The study also discusses strategies to optimize the application of finite simple groups in cryptography, including hybrid cryptographic models and algorithmic refinements to enhance efficiency. Furthermore, recommendations are provided for leveraging finite simple groups in the post-quantum era, integrating them into cryptographic standards, and fostering further research through educational resources and practical tools. By addressing these challenges and embracing innovative strategies, finite simple groups hold the potential to significantly advance cryptographic security and resilience against emerging cyber threats.

Keywords: Finite group, Simple group, Encryption, Decryption, Key exchange, Permutation

Introduction

The concept of fundamental finite groups was developed by the influential studies of 19th-century mathematicians like Evariste Galois and Camille Jordan, and is one of the most groundbreaking advances in the study of modern mathematics. An abstract algebra group is a collection of objects with a binary operation that meets the four most important properties closure, associativity, identity and invertibility. In the case where the set has a finite number of elements, it is known as a finite group. The simplest of these is a group that cannot be broken down into smaller, nontrivial normal subgroups. That is, with the exception being the trivial subgroup, which only contains the identity element, all other subgroups are left invariant by the group operation. The classification theory of finite simple groups holds that all finite simple groups belong to one of a few broad categories, such as cyclic groups of prime order, Lie-type groups, and the sporadic groups or the erratic groups. This theory is one of the most elaborate results of abstraction in mathematics (Canda, et al, 2021).

The classification theory in its turn is a witness to the strength of abstraction and interrelatedness of the disciplines of mathematics. It brings together algebra, geometry, and topology by showing that every finite

simple group can be classified in well-defined families (such as Lie-type groups or alternating groups or any of the 26 sporadic groups) including the famous Monster group and Mathieu groups. These purely abstract mathematical frameworks have very broad extrapolations into other fields outside of pure mathematics. Their work lies behind various disciplines such as theoretical physics, computer sciences, and cryptography. These complex symmetries of these groups are important in the study of particle interactions in physics, efficient algorithms in computer science and the development of strong encryption schemes in secrecy. The classification theorem is therefore not only a fundamental building block to the group theory but also a point of departure to further discovery and innovations in all sciences (Bucur, et al, 2021).

Sheng (2022) claims that the classification of finite simple groups is critical in modern cryptography especially in designing and analyzing cryptographic algorithms and security protocols. An example here is the use of public-key cryptography, which can be based on computationally hard mathematical problems, including integer factorization and discrete logarithms. Finite simple group theory can be used to enhance the RSA encryption scheme which relies on the intractability of large composite numbers by constructing more robust cryptographic primitives. Likewise, the key exchange protocol of Diffie-Hellman which forms the basis of secure digital communication is made secure through the difficulty of finding the discrete logarithms in finite cyclic groups. The vulnerability to attacks based on breakthroughs in number theory or computational algebra can be addressed by choosing appropriate finite simple groups such as those of prime order or elliptic curve groups, and therefore, make encryption systems more robust. More so, finite simple groups are relevant towards the study of structural principles of contemporary cryptographic systems. Some sporadic groups, like the Monster group, find use in the error-correcting codes and information theory due to their very extraordinary symmetry (Canda, et al, 2021). A better understanding of such groups would allow cryptographers to come up with more effective coding and data transmission techniques that are more secure. The classification theory is an influential analysis instrument to evaluate cryptographic algorithms, where researchers can test how different cryptographic primitives can withstand a group-theoretic or an algebraic attack. Knowledge gained through finite group taxonomy is, therefore, indispensable in the creation of the next-generation cryptography systems capable of resisting any emerging cyber threats in the world that is becoming more digitalized.

Most of the current cryptographic designs use the properties of finite cyclic groups of prime order, particularly in the secure key exchange protocol like the Diffie-Hellman. Such prime-order groups are currently of fundamental importance to guarantee the security and efficiency of various cryptography systems, and as illustrated by Lynn, Prabhakaran, and Sahai (2018), this is especially true in the post-quantum cryptography sector. Special cases of finite simple groups, elliptic curve groups are the basis of elliptic curve cryptography (ECC)- a scheme with small sizes of keys but high security. In addition, elliptic curves and some sporadic groups have been used in error-correcting codes, as demonstrated by Ivanov and Liebeck (2020), who examined the way these groups are structured to give a better code design. Cyclic groups are also used as a mathematical basis of quantum cryptographic protocols such as quantum key distribution (QKD). They are important in this sense because they provide a certain degree of unbreakable communication channels that are not susceptible to eavesdropping (Gottesman, 2021). It is on this basis that the current study aims at exploring how a finite simple group has been used in cryptography and how classification of finite simple groups can be used to construct and analyze cryptographic protocols in current security architecture.

An important point regarding this research is the analysis of finite simple groups in terms of the mathematical foundations. This incorporates the investigation of their algebraic framework, their order and their rules of operation, which meet with the requirements of closure, associativity, identity, and invertibility. This mathematical rigor guarantees that cryptographic schemes defined using such groups have stability, predictability and are resistant to algebraic attacks. Besides, classification theory of finite simple groups is another tool that acts as a unifying theory and helps cryptographers to choose appropriate groups to use in certain security measures. The cryptographic strength of these groups has been boosted by the mathematical beauty of the groups themselves, as well as providing a better insight into how the complicated algebraic groups can be translated in to viable cybersecurity solutions.

The paper also explores the usage of finite simple groups in the current cryptographic applications such as in public-key encryptions, key exchange algorithms, and cryptographic signatures. Specifically, the work points out the role of cyclic and elliptic curve groups of prime order in popular cryptographic schemes like RSA, Diffie-Hellman and elliptic curve cryptography (ECC). Such applications illustrate that the theoretical concepts that form the group theory can be translated directly to resolving real world issues in data security, authentication and privacy. Finite simple groups are invaluable through such applications to make them efficient, scalable, and robust when it comes to cryptographic design. After all, this study highlights the interdependence of pure mathematics and applied cryptography. The study will fill the gap between theoretical group theory and practical cybersecurity requirements by using finite simple groups based on their design, mathematical structure, and functional applications. These lessons learnt during this analysis are likely to play a role in the further development of cryptography systems, particularly towards novel threats like quantum computing. By so doing, the study does not only contribute to the knowledge on finite simple groups but also reiterates the relevance of these groups over time in fostering integrity and confidentiality of information in the digital era.

By studying the algebraic geometry of finite simple groups, cryptographers obtain a guideline to the development of novel encryption algorithms. The exact and highly structured design of these groups makes them the best choice to build cryptographic primitives that resist stationary as well as quantum attacks. Through analyzing their algebraic properties, researchers are able to devise algorithms that can apply these symmetries to deliver their key generation, authentication and data protection mechanisms in a stronger manner. The developments would not only enhance the existing cryptography procedures, but also help in the creation of entirely new systems in which the core principles of group theory are used (Cohen, et al, 2016).

In addition to this, the paper highlights how an appreciation of finite simple groups can in turn be used to tackle existing vulnerabilities of cryptographic systems through a mathematical perspective. The modern encryption algorithms are susceptible to many of the current encryption systems because of the improvement in the computational capabilities and algorithmic approaches. The internal symmetries of finite simple groups, which are finite, complex, and well-defined provide the opportunity to design cryptographic schemes which are more resistant by nature to cryptanalysis. Using the principles of group theory, it becomes feasible to make the encryption resistant to known attacks and predict the new threats, which will guarantee the reliability of safe communication systems in the long run. The security environment of digital communication and transactions can therefore be changed using the finite simple group theory. With their properties incorporated into the design of encryption, developers can produce cryptographic systems that are not only mathematically beautiful, but also practically resistant to attack by contemporary technology (Zhang, et al, 2024). This does not only improve the data confidentiality and integrity but also creates better trust in computerized infrastructures like online banking, e-commerce, and safe exchange of data. The theory of finite simple groups provides the structure of the cryptography techniques which have to keep up with new cybersecurity threats.

Essentially, the research is not limited to theoretical mathematics- the work is not only a connection between abstract algebra and real-world cybersecurity innovation. The detailed study of finite simple groups allows developing new cryptographic methods which are based on validated mathematical principles. With the growth of digital systems and more advanced threats, the information obtained during this research might result into more secure and reliable encryption systems, and therefore, the general security posture of the global digital communications and safeguarding of sensitive information in the contemporary world.

Related Literatures

By examining how the following mathematical structures could improve security and efficiency in cryptographic systems, this chapter reviewed and investigated the work of many authors on pertinent material, including the usage of finite non-abelian simple groups in cryptography: Creating Hard Factorizations, Finding Minimal Length Logarithmic Signatures, Cryptographic Constructions Using Factorization Sequence, Public-Key Constructions from Logarithmic Signatures, The Geodesic Problem and Cayley Hash Functions, Fully Homomorphic Encryption Schemes, Simple Groups, and All-Inclusive Encryption.

Finite Simple Groups

Most secure cryptographic functions like Cayley hash functions based on a mathematical foundation using finite simple groups and are particularly important in efficiently and securely hashing large datasets (Kahrobael, et al, 2024). These functions utilize the intricate structural characteristics and symmetries of finite simple groups so they provide a collision resistance and computational difficulty- some of the essential criteria of contemporary cryptographic hashing. A simple group is simply described as a non-trivial group, which has no other normal subgroups other than itself and a trivial group, so it is considered to be an indivisible and basic unit of group theory. Not only does the study of these groups enrich the theoretical knowledge of the abstract algebra, but also it is directly related to designing cryptographic schemes which are resistant to attacks and can perform large scale secure calculations. Besides simple groups, quasi-simple groups (which are perfect groups (i.e. equal to their own commutator subgroup (G = [G, G]), and whose inner automorphism group is simple, are also considered in the study (with the name Inn(G) indicating the latter). These quasi-simple groups have most of the properties of finite simple groups useful in cryptography, such as their structural complexity and symmetry. Since cryptographic systems are based on finite, discrete data structures, the work is specifically on finite forms of these groups. Their finite nature guarantees the practicality of cryptographic algorithms with respect to the computational systems and mathematical rigor and predictability. One of the most important achievements of modern-day mathematics has been the classification of all finite simple groups, which had been worked on by many mathematicians over decades and was finally finished in the early 2000s. The grandiose theorem demonstrates that all finite simple groups fall into the following well-known categories: prime-order cyclic groups, alternating groups, groups of Lie type, or one of 26 exceptional sporadic groups. This tedious classification offers an easy roadmap to locating and analyzing all conceivable finite simple groups, and serves as a cornerstone to both mathematicians and cryptographers. The fact that only these families are known implies that all finite simple structures that are used in cryptographic algorithms can be studied in a very precise mathematical context. In contrast to classical groups, exceptional groups are all restricted to a maximum rank of 8 and often do not have natural matrix representations. Prime powers q are used to index each of the 10 infinite families of these groupings. The Suzuki groups, represented by Sz(2r), which are defined over fields of order 2r, serve as an illustration

Geodesic Problem and Cayley Hash Functions

Holmes, 2018, suggested that the Geodesic Problem of finite groups is intertwined with the creation of the sound infrastructural systems of public-key cryptography that could withstand a broad range of attacks. The Geodesic Problem, which is to determine the shortest representation, or geodesic, of an element in a group with respect to a given generating set, is a problem that is computationally hard to solve in many finite groups. It is this difficult computational task that makes such groups desirable in cryptographic purposes since the hardness of problem solving in such groups offers an excellent basis of secure encryption protocols. With the complexity of the Geodesic Problem, cryptographic protocols can be developed whose security relies on mathematically provable intractability, and this can make the systems of public-key cryptography more resilient to both classical and modern cryptanalytic attacks. One of the most basic cryptography primitives is a hash function. It is a mathematical operation where the input message of any length is inputted into the function to generate a fixed length output, a hash or digest. Hash functions have become a part of most cryptography applications, such as digital signatures, message authentication codes, and checking integrity

of data. The key security characteristics that a hash function should have are preimage resistance and collision resistance. Preimage resistance can be guaranteed such that, given a hash value (nN), it is computationally infeasible to determine an input (mM) so that (h(m) = n). Instead, collision resistance ensures that it is highly unlikely that you will be able to discover two different inputs (m_1, m_2M) that produce the identical hash value (h(m_1) = h(m_2)). These properties render the hash functions inevitable in the provision of data authenticity and integrity in the digital communications (Brakerski, et al, 2019).

It is on these principles that Vdovina (2017) contributed to the current body of knowledge on group-theoretic cryptography by introducing hash functions defined in Cayley graphs of finitely generated groups. This methodology is based on previous studies by Bosset and Camion who investigated the connection between group structures and cryptographic hashing. A Cayley graph is a mathematical graph that describes the structure of a group in the following way: the elements of the group are the nodes and the operations of the group are the edges, hence visually encoding the algebraic relationships in the group. With the use of finite groups to create such graphs, the hash functions obtained have strong mathematical characteristics due to group theory, such as high nonlinearity, unpredictability, and resistance to algebraic attacks.

This hash function based on groups present a number of benefits concerning hash functions based on conventionally constructed hash functions. Their dependence upon the complexity of finite generated groups is such that inverting or forecasting the output of the hash involves solving problems of computational difficulty, like the Geodesic Problem or word problem of group theory, which are known to be infeasible in large or non-commutative groups. More so, the hash functions can also be constructed to guarantee both the use of diffusion as well as confusion, which are some of the main cryptographic principles that do not allow attackers to use knowledge of the original message to deduce any meaningful information about the message through its hash. It renders this type of group-based hashing especially well adapted to applications where a high degree of resistance against collision and preimage attack is needed.

Overall, the present approach to cryptographic design that incorporates the finite group theory and the construction of Cayley graphs illustrates the profound mutualism between the abstract algebra and the concrete security. The computational hardness of the Geodesic Problem combined with structured symmetries of finite groups provide a solid model of constructing future-generation cryptographic primitives. Such innovations do not only enhance the mathematical basis of hashing and encryption; but they also open the path to cryptographic systems that are capable of response to new threats including quantum computing threats (Son, et al, 2024).

Cryptographic Constructions

To achieve better efficiency and security, a number of generating sets have been suggested in the design of Cayley hash functions over the special linear group (SL2(q)). But every one of these generating sets has eventually been shown to be susceptible to one form or another of cryptographic attack, showing structural vulnerability in its design. Bromberg, et al, 2015, proposed a new method based on a generating set of the quasi-simple group (SLn(p)) where (p) is a prime number to deal with the vulnerabilities. This generalization makes the group size bigger and thus more structurally complex and computationally hard target problems. Here, the Geodesic Problem, to find a minimal representation of an element in the group, is the same as one would approach a system of (n2) multivariate polynomials with (n2) variables over the finite field (Fp). In worst-case scenario, this problem is NP-hard, and, thus, in theory, it is resistant to efficient algorithmic solutions and, therefore, of interest in cryptographic use. In spite of these theoretical benefits, the proposed solution continues to have major security issues especially in ensuring collision resistance. Despite the parameters having been chosen to guarantee the efficiency of the assessment of the hash-function, the fact that there are numerous valid reconstructions of the identity element of the group presents a fatal flaw. It implies that any combination of group operations may produce the same output hash value, and result in collisions. These collisions compromise one of the fundamental characteristics of a secure hash function, namely they enable an attacker to produce distinct messages that have the same hash value. The report by EUROCRYPT (2023) indicates that such collisions can be easily made by any insertion of such alternative factorizations into a word to prove that even highly mathematical constructions need rigorous testing and optimization to attain genuine cryptographic security (Shpilrain, et al, 2016). This highlights the fine line between computational efficiency and security that has to be taken into

account when it comes to designing group-theoretic hash functions.

Creation of Hard Factorizations

Sub-exponential-length words can be generated in sub-exponential time for any $SL_2(2k)$ generating sets. However, there isn't a strategy that works for every generating set or group.For any $SL_2(2k)$ generating sets, sub-exponential-length words can be produced in sub-exponential time. Nevertheless, no single technique is effective for all generating sets or groups.The development of MST1 depends on the use of a trapdoor and the public wild logarithmic signature α. The use of α as a non-transversal logarithmic signature was suggested by González, Magliveras, and Steinwandt (2023), suggesting that none of the αi are cosets of non-trivial subgroups of G.The development of MST1 depends on the use of a trapdoor and the public wild logarithmic signature α. The use of α as a non-transversal logarithmic signature was suggested by González, Magliveras, and Steinwandt (2023), suggesting that none of the αi are cosets of non-trivial subgroups of G.

Magliveras, Svaba, van Trung, and Zajac (2015) further cryptanalyzed MST3 after its security was questioned in (Gonzalez Vasco, Rötteler, & Steinwandt, 2016). They showed that factoring with respect to the random covers utilised is not always a challenging operation. In recent years, other plans have been put up. For instance, a safe method for producing hard group factorizations appropriate for use in cryptography.

METHODOLOGY

Building on the theoretical underpinnings, theorems, and literature covered in section two above, this section focused on the research methodology. We used a theoretical and analytical method to investigate the properties, security implications, problems, and prospective uses of finite simple groups in cryptography. The method is centred on theoretical analysis, as well as data analysis techniques applicable to cryptographic applications of finite simple groups.

Design of the Study

The theoretical methodology of the given research includes a literature review, theoretical analysis, as well as, in some instances, the case-study assessments. It is a design structure whenever the basic properties, and cryptographic potential of finite simple groups can be analysed in detail.

The paper reviewed the most significant works on the Classification Theorem in order to gain a better understanding of the applications of finite simple groups in cryptography. The unique characteristics and arrangements of every family, namely: cyclic, alternating, Lie-type, and sporadic were also studied. In all families, a hypothetical study was carried out of characteristics like group order, generators, and automorphism groups, and characteristics that enhance cryptographic methods.

The found features were contrasted to the cryptographic requirements including complexity, irreducibility, and symmetry to demonstrate how they can be used to provide cryptographic security.

Finite Simple Group Classification Methods

One of the most important algebraic discoveries is to better realise the cryptographic uses of finite simple groups. Any non-simple group can be simplified to simple composition factors in a similar manner that integers are simplified to prime factors by taking their normal subgroups and quotient group. The theorems that were used to classify finite groups were as follows: a statement that holds on a group may be lowered down to a challenge on simple members of the group.

Any of these can be used to characterize a finite simple group's isomorphism. A Lie-type alternating group that belongs to one of sixteen infinite families is called a prime-order cyclic group.

Theorem 1: Prime-order cyclic groups are known as simple abelian groups.

Theorem 2: For $n \geq 5$, the alternating group A_n is a simple group.

Construction of Logarithmic Signatures with Short Length

Group theory in cryptography leads to a number of interesting mathematical problems including the problem of how long logarithmic size signatures can be. The size of covers, or the size of representations of group elements, is an important parameter in cryptographic systems, especially those based on group-based constructions, and to a larger extent, it has a direct impact on the computational efficiency and storage needs in practice. A logarithmic signature offers a systematic manner of representing

every element of a finite group (G) as a product of elements chosen out of the smaller groups, which provides them with a compact and systematic representation that can be used in encryption, authentication, and key exchange procedures. The main issue, thus, is to find the minimal possible logarithmic signature which nevertheless makes it possible to represent all group elements uniquely, which would provide a more efficient and more secure cryptographic implementation (Gonzalez, et al, 2016). Their methodology offers a method of building and analyzing logarithmic signatures in a mathematically rigorous fashion and allows finding effective group decompositions to be used in cryptography. This relationship between group order factorization and signature length is not only useful in increasing overall theoretical knowledge, but also in terms of practical implementation because shorter logarithmic signatures will result in faster computation and less data overhead, which is of great importance in current cryptographic design.

Public-Key Constructions from Logarithmic Signatures

Since the 1980s, many attempts have been made to derive one-way functions by exploiting the computational properties of what are called factorization sequences of finite groups, including trapdoor functions, which are one-way functions for which pre-images can be easily computed given additional information. Now, choose $\alpha = (\alpha_1,...,\alpha_s)$ and $\alpha_i = (\alpha_{i1},...,\alpha_{ini})$, assuming that $i = 1,...,s$ and $\alpha_{ij} \in G$. Let G be a finite group. When a set of permutations works on n locations where $n < |G|$, then G is acknowledged. For $g \in G$ with regard to α, the factorization sequence is $(i_1,...,i_s) \in N_s$ and $g = \alpha_{1i1} \cdots \alpha_{sis}$. Infact, g can be represented as an ordered product of components in the blocks of α in a variety of ways, or not at all, depending on the specific element $g \in G$. The value of $n[\alpha, g]$ indicates the number of different factorization sequences for g that are caused by α. For any g in G, $n[\alpha, g] > 0$, therefore α is a cover. The logarithmic signature of each g in G is present if $n[\alpha, g] = 1$. The logarithmic signature (α) is timed if factorization sequences can be constructed in polynomial time in the degree of G, otherwise, it is wild. Choosing one element from each α_i makes it "easy" to generate group elements if the group rule can be computed fast. However, the opposite procedure may need more computation.

Cryptographic Constructions Using Factorization Sequence

Permutation Group Mappings (PGM), the first private-key cryptography architecture built on a factorization sequence, was introduced by González, et al, 2023. It uses logarithmic signatures to produce one-way functions for permutation groups. The public-key cryptosystem MST1, which builds on the same concept but introduces a second trapdoor, may be used to construct the one-way function in PGM. Several academics have proposed the MST2 version, which is based on a special kind of cover known as a mesh. It may be difficult to factor group components and manage random covers for large subsets of finite non-abelian groups with large centres. Gentry, et al, 2020, adapted these techniques for use with these structures and proposed MST3. We now talk about MST1, the most fundamental of these constructions. $Z_m = \{0, 1, ..., m - 1\}$, is the modulo m of the ring of integers for a natural number m. Given a well-known finite permutation group G, give it a tame logarithmic signature η. Any logarithmic signature can have its mappings created using $\alpha = (\alpha_1, ... ,\alpha_s)$.

Data Collection

The data collection strategy focusses on gathering essential theoretical material and practical case studies from primary sources, such as academic papers and cryptographic standards.

Primary Sources: Academic journals, cryptographic standards, and authoritative books on group theory and cryptography will serve as primary sources for theoretical analysis.

Cryptographic Scheme Analysis: The study examined existing cryptographic techniques that use finite simple groups, focusing on key exchange, encryption, and digital signatures. This study examined the efficiency of finite simple group properties in providing strong security features, particularly in high-complexity algorithms.

RESULTS AND DISCUSSION

Classification of Finite Simple Groups

Finite simple group classification is the most significant finding in algebra. In the same way that integers are prime factorized, any non-simple group can ultimately be reduced to simple composition factors by taking its normal subgroups and quotient group. This turns a claim about a group into an issue

with regard to its essential elements. An arrangement of subgroups is a group G's composition series".

The following composition series is satisfied by the cyclic group Z_{12} for $\{e\} = H_0 \leq H_1 \leq H_2 \cdots \leq H_{k-1} \leq H_k = G$, where $H_i \trianglelefteq H_{i+1}$ and each composition element H_{i+1}/H is a simple group for $0 \leq i \leq k - 1$.

$$\{e\} \trianglelefteq Z_3 \trianglelefteq Z_6 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_6 = Z_2$, $Z_6/Z_3 = Z_2$, $Z_3/Z_1 = Z_3$

$$\{e\} \trianglelefteq Z_2 \trianglelefteq Z_6 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_6 = Z_2$, $Z_6/Z_2 = Z_3$, $Z_2/Z_1 = Z_2$

$$\{e\} \trianglelefteq Z_2 \trianglelefteq Z_4 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_4 = Z_3$, $Z_4/Z_2 = Z_2$, $Z_2/Z_1 = Z_2$

The following conclusions are produced by the finite group classification theorem:

Theorem 3: Prime-order cyclic groups are known as simple abelian groups.

Proof: (⇒) To be prime order, G must be a simple abelian group. Consider the fundamental group G of abelian functions. Thus, G is by definition a nontrivial group. G is a finite group, as we first demonstrate. For illustration Take the non-identity element $g \in G$ as an example. Then $\langle g\rangle \leq G$. All of G's subgroups are normal as G is abelian. $\langle g\rangle = G$ is required since G is simple. G is simple, but if g's order is not finite, then $\langle g^2\rangle$ is an appropriate normal subgroup of $\langle g\rangle = G$. As a result, g's order is restricted. The group $G = \langle g\rangle$ is consequently finite. Assume that $p = |g| = |G|$. FSOC states that if $m > 1$, $n > 1$, then $p = mn$ is a composite number. For this reason, G_m is a prop. Consequently, g's order is limited. This means that the group $G = \langle g\rangle$ is finite. Assume $p = |g| = |G|$ instead. $P = mn$ is a composite number, according to FSOC, if $m > 1, n > 1$. Gm is therefore a prop. Thus, G's order is restricted. Thus, $G = \langle g\rangle$ is a group that is finite.

(⇐) It follows that the group $G = \langle g\rangle$ is finite. Suppose $p = |g| = |G|$. FSOC states that $p = mn$ is a composite number if $m > 1, n > 1$. Gm is a prop for this reason. Therefore, G's order is limited. G is therefore a finite group ($G = \langle g\rangle$). Then, $|\langle g\rangle| \mid |G|$.

This means that $|\langle g\rangle|$ has to be p. $G = \langle g\rangle$ follows because G is a cyclic group, or more specifically, an abelian group.If the order of any normal subgroup $H \leq G$ is either 1 or p, then all of them must be trivial or G. G is hence a simple function. G is a basic abelian group as a consequence.

Theorem 4: A group A_n is simple for $n \geq 5$.

i. A_n contains each 3-cycle for $n \geq 3$.

ii. The 3-cycles generate A_n for $n \geq 3$.

iii. Suppose that for $n \geq 3$, r,s are different fixed elements of {1,2,...,n}. A_n is then produced by the *n* 3-cycles of the kind (r, s, i) for $1 \leq i < n$, $i = r$, $i = s$.

iv. Assume that $N \trianglelefteq A_n$ for n^3. If N contains a 3-cycle, then $N = A_n$.

v. N is considered a nontrivial normal subgroup of A_n for $n \geq 5$. Then, at least one of the following conditions needs to be met. N and A_n are invariably equal.

Case I: There is a 3-cycle in N.

Case II: At least one of the disjoint cycles in N has a length longer than three.

Case III: $\sigma = \mu (a_4, a_5, a_6) (a_1, a_2, a_3)$ is the disjoint product.

Case IV: The disjoint product of the type $\sigma = \mu(a_1, a_2, a_3)$ is included in N if an even number of disjoint 2-cycles result in μ.

Case V: An even number of discontinuous 2-cycles multiplied by μ yields a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$.

Sporadic Groups

There are 26 irregular groups that make up the monster group, 20 of which are called "Happy Family" subquotients, and six more are called "Pariah groups." There will be a quick overview of transitive group activities before exploring the first generation

of the Happy Family, commonly known as Mathieu groups.

When a map G × S → S exists such that the following statements are true for every s ∈S, then a group G acts on a set S.

(i) Identity: S results from the identity element's action eGs = s
(ii) Associativity: When s is in S and g, h in G, g(hs) = (gh)s

A group is transitive when it operates on a nonempty set if there is only one orbit; if g exists for every x_1 and y_1 in S, then y_1 equals gx_1; and if for each pair of points (x_1, x_2), and (y_1,y_2), $y_i = gx_i$. Orb(s) = {gs | g ∈ G} is given as the orbit of an element s ∈ S. It displays the collection of objects to which G forwards each s. The TA group action is k-transitive if any set {x_1, ..., y_k} has a group member g and 2k unique components such that $y_i = gx_i$. A permutation that shifts 1 to each other integer in the set makes S_n's typical action on {1,2, ..., n} transitive when n ≥ 1. Hence, {1,2,...,n} is the orbit for 1.

First Generation: Mathieu Groups

Emile L'eonard Mathieu is credited with discovering the initial scattered groupings between 1861 and 1873. Aside from symmetric and alternating groups, Mathieu groups were established in response to a desire to study multiple transitive permutations.

Table 1: Mathieu groups

Group	Order	Transitivity
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	sharp 4 -fold
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	sharp 5 -fold
M_{21}	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	2-transitive
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	3 -transitive
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	4 -transitive
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	5 -transitive

Up until the second half of the 20th century, there were few known sporadic groups.

Second Generation: Leech Lattice

In 1967, John Leech discovered the Leech lattice Λ_{24} while investigating the kissing number problem, which seeks to determine the densest arrangement of spheres in higher dimensions. John Conway discovered the Leech lattice's automorphism group the following year, in 1968. Specifically, he found the group of isometries that fix the centre, which creates an ordered group. $222 \cdot 39 \cdot 54 \cdot 72 \cdot 11 \cdot 13 \cdot 23$ is the value of $Aut(\Lambda 24)| \equiv |C_o0|$.

C_o0 possesses simple sub-quotients that form occasional groupings, despite the fact that C_o0 itself is not simple. Below are the ordering of the second generation sporadic group, with no additional context.

Group	Order
Conway $_1$, *Co* $_1$	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Conway $_2$, *Co* $_2$	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Conway $_3$, *Co* $_3$	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Higman-Sims, *HS.*	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$

McLaughlin, *McL*	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Hall-Janko, *HJ* or J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
Suzuki, *Suz*	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7$

Third Generation: Monster Group

A permutation that shifts 1 to each other integer in the set makes S_n's typical action on {1,2,...,n} transitive when $n \geq 1$. Hence, 1,2,...,n} is the orbit for 1.

Twenty of the twenty-six sporadic groups are associated with monster M, the biggest of the three sporadic group levels. Both Bernd Fischer and Robert Griess made major contributions to the construction of the Monster in 1982. Consequently, it is also known as the Fischer-Griess monster. Fischer was also in charge of the triplet of baby monster B and intermittent monster B. The second Mathieu is comparable to F_{i22}, F_{i23}, and F_{i24}. Oddly, the animal and its offspring are members of the orders.

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \times 10^{53}$$

$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33}$$

Group	Order
Monster, M.	$\approx 8 \cdot 10^{54}$,
Baby Monster, B	$\approx 4 \cdot 10^{33}$,
Fischer 24, Fi 24	$\approx 1 \cdot 10^{24}$,
Fischer 23, Fi 23	$\approx 4 \cdot 10^{18}$, ,
Fischer 22, Fi 22	$\approx 6 \cdot 10^{13}$,
Harada–Norton, HN	$\approx 2 \cdot 10^{14}$,
Thompson, Th	$\approx 9 \cdot 10^{17}$,
Held, He	$\approx 4 \cdot 10^{9}$,

Pariahs

It is believed that the 20 Happy Family members are subdivisions of the Monster gang. However, there are six Pariah groupings that have little in common with the previously mentioned irregular categories. The groups for Pariah are listed below.

Table 2: Pariah group

Group	Order
Rudvalis, *Ru*	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
O'Nan, *ON*	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$

Lyons, $_{24}$, *Ly*	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Janko $_4$, J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Janko $_3$, J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
Janko$_1$, J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$

Group Properties to Cryptographic Mechanisms

Cryptographic techniques are fundamentally dependent on the properties of these finite simple groups.

Irreducibility: Finite simple groups are irreducible; hence, they possess no normal subgroups, rendering any decomposition of their structure impossible. This irreducibility is critical in public-key cryptography because it ensures the security of systems like RSA and ECC, where reversing operations (such as factoring big products) are computationally difficult.

Symmetry and Complexity: Symmetry in alternating and Lie-type groups introduces an element of unpredictability that is useful in cryptographic functions that need permutation and complex transformation features, such as block cyphers. The complexity of group operations in non-abelian groups improves security by making computations more difficult to invert, which is a desirable feature for cryptographic hash functions.

Automorphism Groups: In some cryptographic protocols, e.g. symmetry based, the automorphism structure is used to provide increased complexity to transformations and thus increase the difficulty of specific cryptographic attacks, e.g. lattice-based cryptographic systems.

Security implications of using Finite Simple Group in Cryptography

In order to analyze the security implications of finite simple group usage in cryptography and to evaluate their resistance to attack, we are going to consider each component of the methodology, although with a specific focus directed towards the particular nature of finite simple groups and their applicability to certain cryptographic operations which are key exchange, encryption, and digital signing.

Analysis of Cryptographic Condition

Finite Simple Groups is Key Cryptographic Schemes. Finite simple groups are considered highly complex and they have structural properties that provide benefits to cryptographic schemes, as they raise the computation cost. Their potential applications in the different cryptography applications are revealed in the following study:

Key Exchange Protocols: Finite simple groups are highly complex and have distinctive structural characteristics, which may enhance the cryptographic procedures by making it more difficult to compute. Their potential applications in different cryptographic schemes are shown in the following study:

Encryption Algorithms: Finite simple groups (having complex structure, e.g. alternating and some irregular group) can enhance symmetric encryption algorithms by bringing high complexity and irreducibility to the transformations of encryptions. This would render any decryption process without the key computationally expensive, which would be to the advantage of methods like Advanced Encryption Standard (AES) had it been designed with additional security measures added in the form of finite group transformations.

Digital Signatures: Non-abelian simple groups, notably alternating and Lie-type groups, show promise for digital signature methods in which the security is based on the impossibility of certain computations, such as locating an element that matches to a specific permutation. The structural asymmetry of these groups increases their robustness, making it difficult for adversaries to counterfeit signatures without solving computationally difficult challenges.

Security Analysis Techniques

To analyse the robustness of cryptographic methods that contain finite simple groups, it is necessary to consider typical attack vectors and how features of

finite simple groups contribute to resistance to attacks.

Attack Surface Analysis:

Brute Force Attacks: In finite simple groups, brute-force searches are not feasible because of their enormous size and unsuitable subgroups, especially of Lie-type and sporadic groups. As an illustration, in a group of large prime order, a foe would need to search through a massive quantity of elements to speculate on keys or de-encrypt, which is unfeasible under the computational possibility of a realistic quantity of time.

Factorization and Discrete Logarithm Attacks: The structure of finite simple groups is such that common factorisation or discrete logarithm attacks are difficult. The discrete logarithm problem remains difficult in non-abelian groups like alternating or Lie-type groups, enhancing the security of protocols like ElGamal encryption and Elliptic Curve Cryptography (ECC). Groups of prime order especially cyclic groups are more resistant to such attacks since the group order has no divisor, hence the discrete logarithm problem is made simpler.

Advanced Attacks: This represents the second major security challenge facing applications.<|human|>Advanced Attacks: This is the second security challenge facing applications.

Quantum Attacks: The simple finite groups themselves (not using cyclic structure) may provide more quantum attack resistance since quantum algorithms like the Shor algorithm are less efficient on non-cyclic forms. Cryptographic techniques that are less resistant to Shor have the potential to be offered by the use of sporadic groups, e.g., though such studies are still at their infancy.

Collision Resistance in Hashing: Cryptographic hashing techniques can be applied to collision resistance by alternating between groups and group-specific Lie-type groups. This resistance is based on the fact that elements have a great complexity and structural arrangement and therefore it is hard to find two different inputs when two different inputs are used that can produce the same output in these group operations, which enhances the security of hash functions.

Comparative to Other Group-Based Cryptographic Approaches.

In order to gain a clearer idea of the advantages and disadvantages of using finite simple groups in cryptography, we shall compare them with alternative group-based systems such as the elliptic curve based cryptography and the integer factorization based cryptography.

An Elliptic Curve Cryptography (ECC) is a set of cryptography algorithms utilizing elliptic curves. Finite simple groups, especially Lie-type and alternating groups, have the advantage of providing high levels of security without having a high vulnerability to specific attacks that make use of structural properties with elliptic curves.

Disadvantages: ECC is usually cheaper in cost of computation and is therefore very popular in practice since it uses smaller key sizes and performs faster. Finite simple groups which are not abelian, conversely, might be resource intensive since their computation is often complicated.

Benefits of Finite simple groups: The security of RSA is based on the difficulty of factoring very large integers, whereas the security of finite simple groups can exploit an even harder problem, the discrete logarithm problem in non-abelian groups, which is difficult even with large keys.

Disadvantages: Finite simple groups are theoretically simpler and stronger, but in practice may be difficult to implement because of the need to use larger data structures and extra overhead processing, particularly with sporadic groups. RSA, conversely, possesses properly developed implementation and optimization methods.

Problems of incorporating Finite Simple Group-based Cryptography.

In order to examine the issues and constraints related to the incorporation of finite simple group-based cryptographic primitives into real-world systems, we may consider the elements of efficiency, scalability, and interopability with standard cryptographic protocols using the described methodology. A detailed discussion of these considerations, with a particular focus on the peculiarities of finite simple groups and their implications on the design of practical cryptography, follows.

Efficiency/Scalability Investigation.

Finite simple groups represent a theoretically secure cryptographic group because of its structural

complexity, although cryptographic algorithm implementations with such groups may be computationally hard. Here is the analysis of challenges related to efficiency:

Time Complexity: Algorithms based on finite simple group, especially non-abelian group like alternating or Lie-type group, often have a greater time complexity because they do not have simpler subgroup structure and because operations which are not commutative require more processing. The time taken to process becomes very large as there is more group membership hence real time cryptographic applications which need to be fast and speedy is not possible.

Space Complexity: The space complexity may be large due to the need to have large data structures to model elements in non-cyclic and non-abelian finite simple groups. This becomes particularly so when the group is sporadic, which may have elements and processes of enormous size that require enormous memory distributions. The problem with such space demands is experienced in resource constrained scenarios like mobile devices or IoT systems which has little storage and processing power.

Scalability: Some finite simple groups such as cyclic groups of prime order, among others, are better scaled because they have a relatively simple structure, and non-abelian groups do not scale well as the size of a group increases, making them inoperable in applications that require high volume or high speed processing (such as cloud-based encryption).

Cryptographic Standards Compatibility

Cryptographic primitives based on finite simple groups face a variety of compatibility problems with standard cryptographic systems, such as the standards of NIST and ISO.

Standardization Gaps: The current cryptographic standards such as RSA and ECC are based on elliptic curves and integer factorisation as their public-key cryptography. There exist limited standards in finite simple group-based cryptography, because prior implementations were not highly used due to their complexity and resource demands. This standardisation restricts the integration with systems that have to follow NIST or ISO standards.

Interoperability Challenges: Finite simple groups can be a source of interoperability problems because of their structural constraints and operations are different and may not be compatible with other standard group-based encryption mechanisms. As an illustration, the algorithms based on finite simple groups might fail to work effectively with the current protocols that use cyclic or abelian group, including TLS (Transport Layer Security), which is optimised around RSA or ECC.

The Increased Resource Needs: Finite simple groups are often hard to compute with, which makes algorithms with such groups demand more computer resources than elliptic curve algorithms. Since the NIST and ISO standards prefer algorithms that have been proven to be efficient with respect to the consumption of resources, finite simple group-based methods might face problems with acceptance before they can be refined to be more efficient in the consumption of resources.

Practical Limitations Case Studies

Cryptographic systems based on finite simple groups have been attempted to some degree. Some of the most notable problems that are experienced during real life applications or in experimental case studies are as follows.

Bottlenecks of Key Exchange Protocols: Attempts to apply non-abelian finite simple groups especially Lie-type groups in key exchange protocols have been limited by the large computational costs of their group operands. The fact that it takes a longer time to do a key exchange with these groups than a more common elliptic curve-based technique has restricted its application in scenarios where timing is important.

Comments on Implementation Problems: Cryptographic experts often note that it is very hard to build systems based on finite simple groups in a very efficient manner. As a case in point, the use of the structural properties of alternating and sporadic groups into cryptography systems can require very specialised knowledge, which can make the systems less accessible and challenging to maintain. This complicates the challenge of accepting such systems particularly whereby, there are more conventional methods of getting the same security like ECC.

Resource-Constrained Environment Integration Constraints Experiments with finite simple groups in low-computational capability environments such as IoT devices have shown that their larger memory and computing needs make them infeasible. With current developments in the integration of the Internet of

Things and mobile devices in cryptographic applications, the high complexity of finite simple groups based algorithms to execute efficiently on limited hardware is a crippling limitation.

Strategy Formulation

Algorithmic Adjustments: The use of finite simple groups in existing cryptographic algorithms or the development of new algorithms would require some modifications to make use of the unique properties. The following are some of the proposed changes:

Algorithms Modifications to Key Exchange and Encryption: Strategies of key exchange protocols might involve the modification of existing Diffie-Hellman-like algorithms to take advantage of non-abelian finite simple groups, and therefore provide increased protection due to not being commutative. Encryption methods may exploit the high order nature of groups like alternating groups to produce keys with larger search space to make brute-force search more computationally intensive.

Hybrid Models based on Finite Simple Groups and Elliptic Curves: A hybrid approach to a combination of finite simple group response with elliptic curve cryptography (ECC) can also enjoy the security benefits of both approaches. As an illustration, finite simple groups can be employed at those points where the complexity is required and ECC provides efficiency that ensures that the resulting hybrid schemes are not only secure but also deployable.

Immunity to Quantum Threats: Quantum computing will be a great threat to many common encryption systems. Smaller non-abelian finite simple groups can be useful in quantum-resilient cryptography because of their inherent computational complexity. Algorithms such as lattice-based encryption, which exploit hard group-theoretic problems in finite simple groups, can be used to add additional quantum resistance by solving cryptographic problems that quantum algorithms would find harder to solve.

Implementation Techniques

Effective use of the cryptography using finite simple groups entails not only dealing with the theoretic complexity, but also with the practical use. Some key techniques include:

Optimized Group Element Representations: Finite simple groups, especially of high order or more complicated non-abelian structure, are often computationally expensive to represent and manipulate. It is possible to use compressed or modular representations of group elements, and thus make these groups more efficient in applications of real-time cryptography with security.

Streamlined Computations of Non-Abelian Groups: These techniques can be made more realistic by parallelising the operations or by specialised algorithms exploiting the structure of the group, which are available in non-abelian groups. These cryptographic schemes can be made more realistic with the help of algorithms that make it easier to accomplish multiplication and inversion in finite simple groups.

Error- Correcting Mechanisms: Cryptographic systems using finite simple groups can be subjected to error-correcting algorithms in order to provide integrity especially in distributed environments. When using finite simple groups with limited hardware resources, where the computational cost and possible error occurrences rises due to the increased computational cost, error correction is necessary.

Conclusion

The study comes into conclusion by agreeing that finite simple groups are central in enhancing cryptographic security. This paper has given a thorough general summary of how these mathematical constructions are useful in the cryptographic systems in terms of their structural properties, security advantages and the difficulties that accompany them. Their inherent complexity, great deal of symmetry and subgroup composition, which often demands non-triviality pose finite simple groups with properties that make them especially resistant to a number of cryptanalytic attacks. Their application during cryptography adds another level of algebraic challenge, which strengthens encryption schemes as well as leads to the creation of more secure algorithms.

Nevertheless, the research also states the practical constraints which prevent the extensive implementation of finite simple groups in cryptography applications in the real world. Computational efficiency, scalability of algorithms, and the ability to conform to existing cryptographic standards are some of the issues that need to be resolved so that broader implementation can be supported. Nonetheless, as suggested research

methodologies show, in strategic and meticulous application to cryptography systems, finite simple groups have the capability of making a massive enhancement to the defense against traditional and modern cyber-attacks. Finally, the finite simple groups will be a promising mathematical basis of the future generation of secure cryptographic systems providing new directions of higher data security and digital confidence.

Conflict of Interest

The authors have declared no conflict of interest regarding the manuscript.

REFERENCES

Brakerski, Z., & Vaikuntanathan, V. (2019). Fully homomorphic encryption with sublinear noise. *Journal of Cryptology*, 32(4), 974-1028.

Bromberg, L., Shpilrain, & V., Vdovina, A. (2015). Navigating in the cayley graph of *sl*2(F*p*) and applications to hashing. *Semigroup Forum 94*(2), 314–324.

Bucur, D., & Grigore, A. (2021). Advances in factorization techniques for cryptographic applications. *Journal of Cryptographic Engineering, 13*(2), 145-167.

Canda, V., van Trung, T., & Horvath, S. (2021). Recent developments in cryptographic constructions based on group factorization. *Applied Cryptography and Computational Algebra*, 45(2), 88-102.

Cohen, D., & Frey, S. (2016). *Group theory and its applications to cryptography*. Cambridge University Press.

Gentry, C., & Halevi, S. (2020). A simple and efficient fully homomorphic encryption scheme. *International Journal of Information Security*, 19(4), 439-467.

Gonzalez Vasco, J., Rötteler, M., & Steinwandt, R. (2016). Security Analysis of MST3 with Logarithmic Signatures. *Journal of Cryptology, 29*(3), 442-463.

González, M. I., Magliveras, V., & Steinwandt, R. (2023). Group-theoretic cryptography and recent advancements in the application of permutation groups in cryptography. *Journal of Cryptographic Algorithms*, 33(4), 451-476.

Gottesman, D. (2021). *The Heisenberg representation of quantum computers and applications to quantum cryptography.* arXiv preprint arXiv:2102.01077.

Holmes, W. (2018). Logarithmic Signatures and Group Theory Applications in Cryptography. *Cryptographic Review, 34*(2), 202-225.

Ivanov, A., & Liebeck, M. (2020). *Sporadic groups and error-correcting codes*: Mathematical foundations and applications. Oxford University Press.

Kahrobaei, D., Vasco, S., & McKemmie, D. (2024). Applications of finite non-abelian simple groups in cryptography. *Journal of Cryptography, 35*(1), 112-134.

Lynn, B., Prabhakaran, M., & Sahai, A. (2018). Positive results and techniques for obfuscation. *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC '18).* https://doi.org/10.1145/3188745.3188798

Magliveras, S., Svaba, R., van Trung, N., & Zajac, P. (2015). Cryptographic Applications of Suzuki 2-Groups. *Journal of Cryptographic Engineering, 9*(4), 89-110.

Sheng, T. (2022). Finite simple groups in modern cryptographic protocols. *Journal of Cryptographic Engineering, 20*(3), 205-220.

Shpilrain, V., & Sosnovski, B (2016). Compositions of linear functions and applications to hashing. *GroupsComplex. Cryptol 8*(2), 155–16.

Son, J., Kim, M., Choi, S., Kim, H., & Park, J. (2024). Equity-Transformer: Solving NP-Hard Min-Max Routing Problems as Sequential Generation with Equity Context. *Proceedings of the AAAI Conference on Artificial Intelligence, 38*(18), 20265-20273.

Vdovina, A. (2017). *Group-theoretic hash functions based on Cayley graphs of finitely generated*

groups. Following the work of Bosset and Camion.

Zhang, C., Ji, K., Wang, T., Zhang, B., Zhou, H.-S., Wang, X., & Ren, K. (2024). On the complexity of cryptographic groups and generic group models. *Cryptology ePrint Archive, Paper 2024/1452*.