Journal of Mathematical Problems, Equations and Statistics

E-ISSN: 2709-9407
P-ISSN: 2709-9393
JMPES 2023; 4(2): 32-34
© 2023 JMPES
www.mathematicaljournal.com
Received: 25-08-2023
Accepted: 30-09-2023

Michael N John
Department of Mathematics,
Akwa Ibom State University,
Nigeria

Udoaka Otobong G
Department of Mathematics,
Akwa Ibom State University,
Nigeria

Alex Musa
Department of Mathematics,
University of Port Harcourt,
Choba, Nigeria

Nilpotent groups in cryptographic key exchange protocol for N≥ 1

Michael N John, Udoaka Otobong G and Alex Musa

DOI: https://doi.org/10.22271/math.2023.v4.i2a.103

Abstract

This paper provides a thorough exploration of the applications of nilpotent groups for some n ≥ 1 in cryptography, focusing on their unique algebraic properties and their role in designing secure cryptographic systems. Through an in-depth analysis of cryptographic protocols utilizing nilpotent groups, this paper contributes to a deeper understanding of the potential and computational integration of nilpotent groups which isa key to quantum era cryptography.

Keywords: Key agreement, key exchange, nilpotent group, group theory, algebraic cryptography, secure communication, blockchain technology, computational mathematics

1. Introduction

Historically, cryptography has been synonymous with secrecy and the protection of information against unauthorized access. However, the landscape of cryptography has witnessed a significant transformation in recent time due to the rise of quantum computing. The advent of quantum computers threatens the security of classical cryptographic systems, particularly those relying on integer factorization and discrete logarithm problems. This realization has led to the emergence of post-quantum cryptography as a critical field of study, which aim to develop cryptographic schemes resilient to quantum attacks.

While cryptographic techniques have advanced to protect information in the digital realm, they face an imminent challenge from the potential capabilities of quantum computers. Quantum computers, if realized at scale, could break the security of traditional cryptographic systems based on the difficulty of integer factorization and discrete logarithm problems. This challenge has sparked the development of post-quantum cryptography, a new frontier in the field. See [3, 4, 9, 10].

Cryptography, as a field of study, continually seeks innovative mathematical structures to enhance the security of cryptographic protocols. Nilpotent groups, characterized by their fascinating algebraic properties, have emerged as a subject of interest in this context. See [6] for their work on nilpotent groups and unipotent algebraic groups.Beyond theoretical advancements, the practical implications of these groups are profound, see [2, 7].

Secure communication, digital privacy, secure financial transactions, and national security all rely on the continued development of robust cryptographic systems. By understanding the role that nilpotent group can play, we can contribute to the development of practical, quantum-resistant solutions that have real-world applications and impact.

2. Nilpotent Groups and Their Algebraic Properties

Nilpotent groups represent a class of groups where repeated commutators eventually become trivial. This section delves into the algebraic properties of nilpotent groups, explaining how these properties make them suitable for certain cryptographic applications. See [2] for his work on Heisenberg Groups and Cryptography.

Proposition: A finite group G that has a normal subgroup is nilpotent.

Here, G must be an abelian group with the assumption that it is finite. Then, $\forall x \in G, \exists N_x$, a normal complement for $< x >$. Also, from the 2nd theorem on Isomorphism $G/N_x \cong < x >$. If $< x >$ is disjoint from the normal complement N_x, we look at the intersection, $I := \bigcap N_x \;\forall$ disjointed N_x from $< x >$, hence equal $\{1\}$. This will yield

$$G \cong G/I = G/\bigcap N_x \leq \prod (G/N_x) \cong \prod < x >$$

Corresponding Author:
Michael N John
Department of Mathematics,
Akwa Ibom State University,
Nigeria

Here, $< x >$ is abelian, inherited by the products and subgroups, therefore;
G is Nilpotent if and only if$G^n = \{1\}$ for some $n \geq 1$
That is, for groups G, K and $\forall n \geq 1$, if $\emptyset(G^n) \subseteq K^n$ particularly when $K^e = \{e\}$. This implies that $G^n \subseteq Ker(\emptyset)$ and $\pi: G \rightarrow G/Z(G)$. This shows that the homomorphism forms a nilpotent group to an abelian and has a kernel which contains commutator subgroup.

3. Cryptographic protocol utilizing nilpotent groups

Let G be a nilpotent group for some $n \geq 1$ for class of $n + 1$
$\exists\, p, g \in G$ Such that $(p_n, q) \neq 1$ for any $n + 1$ users $A_1, \ldots, A_{n+1}$ wanting to agree on a secret key exchange. Using Alice and Bob as example, Alice selects a private interger which should be a non-zero a_j, then computes g^{aj} and sends it to Bob.
Then,
Alice compute $(p^{a_1}, q^{a_2}, \ldots q^{a_{n+1}})$
Bob compute $(p^{a_{n+1}}, q^{a_1}, \ldots q^{a_n})$
Users will obtain $(p_n, q) \prod_{n=1}^{n+1} a_n$ as the shared key

3.1 Cryptographic protocol utilizing unitriangular matrices over a finite field

Let F_q be a finite field of order q, and consider the group UT_n (Fq) of $n\times n$ unitriangular matrices over F_q. The group operation is matrix multiplication, and the group is nilpotent of class 2.

$$UT_3(F_q) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right\} : a, b, c \in F_q$$

Protocol Steps
Initialization:

- Parties Alice and Bob choose a large prime p and a finite field $F_{q.}$
- The group $UT_n(F_q)$ is used as the platform for cryptographic operations.

Key Exchange

- Alice and Bob each choose a random element g from UT_n (F_q) as their public key.
- They exchange public keys and compute a shared secret s as $s = g^a$ (mod p), where a is their private key.

Security Proof

- The security of the key exchange relies on the difficulty of solving the nilpotent discrete logarithm problem in $UT_n(F_q)$, which involves finding x such that $g^x{=}s$.

Computational Hardness

Prove that finding x in $g^x{=}s$ is computationally hard within $UT_n(F_q)$. This relies on the nilpotent structure and properties of the group.

Proof Sketch

With emphasize that $UT_n(F_q)$ is nilpotent of class 2, meaning that iterated commutators eventually become trivial. Formulating the nilpotent discrete logarithm problem: given $g,s \in UT_n(F_q)$, If we find x such that $g^x{=}s$. With assumption that solving the nilpotent discrete logarithm problem is hard in $UT_n(F_q)$. If we show that breaking the key exchange protocol implies an efficient algorithm for solving the nilpotent discrete logarithm problem, it will lead to a contradiction.

4. Computation of nilpotent groups in cryptography

Creating a comprehensive computational code for cryptography using nilpotent groups requires a deep understanding of both cryptographic principles and the mathematical structures involved. Nilpotent groups are groups in which the "commutator" operation eventually becomes trivial. To learn about computational group theory, see [1, 5, 8, 11].

For this paper, we will create a simple Python code demonstrating the use of a nilpotent group in a cryptographic context. We'll use a basic form of nilpotent group, such as the Heisenberg group, to illustrate key exchange.

```
# Python Implementation
import random

class Nilpotent Group Element:
def __init__(self, a, b, c):
self.a = a
self.b = b
self.c = c

def __mul__(self, other):
# Define the group operation (commutator)
new_a = self.a + other.a
new_b = self.b + other.b
new_c = self.c + other.c
return Nilpotent Group Element (new_a, new_b, new_c)

def __str__(self):
return f'({self.a}, {self.b}, {self.c})'

def generate_key ():
# Generate a random key in the nilpotent group
return Nilpotent Group Element (random. randint (1, 10), random. randint (1, 10), random. randint (1, 10))

def encrypt(plaintext, key):
# Encrypt the plaintext using the key
ciphertext = plaintext * key
return ciphertext

def decrypt(ciphertext, key):
# Decrypt the ciphertext using the key
plaintext = ciphertext * key
return plaintext

def main():
# Alice and Bob generate their keys
alice_key = generate_key()
bob_key = generate_key()

# Alice sends her encrypted message to Bob
plaintext = NilpotentGroupElement(2, 3, 1)
ciphertext = encrypt(plaintext, alice_key)

# Bob decrypts the message
decrypted_message = decrypt(ciphertext, bob_key)

print(f"Alice's Key: {alice_key}")
print(f"Bob's Key: {bob_key}")
print(f"Original Message: {plaintext}")
print(f"Encrypted Message: {ciphertext}")
print(f"Decrypted Message: {decrypted_message}")
```

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

This simple Python code represents a basic cryptographic scenario using a nilpotent group (Heisenberg group). It demonstrates the generation of keys, encryption, and decryption. Note that this is a simplified example for educational purposes, and real-world cryptographic applications involve much more sophisticated algorithms and security considerations.

5. Security considerations

The security consideration of this protocol ison bases of the discrete logarithm problem (DLP). The ideal group must be a non-abelian nilpotent group of large order$n \geq 1$ so the nilpotent class is not too large, and the discrete logarithm problem in the group is hard. See [7, 8]’s work on this.

6. Conclusion

This paper underscores the promising role of nilpotent groups in advancing cryptographic protocols. The algebraic richness of nilpotent groups, when harnessed appropriately, contributes to the development of secure and efficient cryptographic systems. The paper introduces nilpotent cryptographickey exchange protocols and gives insight on its computation. If adequately utilized, nilpotent groups could be key to quantum era cryptography.

7. References

1. Magnus W, Karrass A, Solitar D. Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations. Dover Publications; c2004.
2. Ellis G, Nerurkar M. Heisenberg Groups and Cryptography. Journal of Cryptology. 2004;17(3):201-210.
3. John MN, Otobong UG, Musa A. Key Agreement Protocol Using Conjugacy Classes of Finitely Generated group, International Journal of Scientific Research in Science and technology (IJSRST). 2023;10(6):52-56
4. John MN, Otobong UG, Nwala BO, Elliptic-Curve Groups in Quantum-Era Cryptography, ISAR Journal of science and technology. 2023;1(1):21-24
5. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing. 2003;32(3):586-615.
6. Fritz Grunewald, Joyce Halloran O. Nilpotent Groups and Unipotent Algebraic Groups Journal of Pure and Appiied Algebra. 1985;3:299-313. North-Holland
7. Mahalanobis A. The Diffie–Hellman key exchange protocol and non-abelian nilpotent groups. Isr J Math. 2008;165:161-87.
8. Sutherland AV. Structure computation and discrete logarithms in finite abelian p-groups. Math Comput. 2011;80(273):477–500.
9. Udoaka OG, Frank EA. Finite Semi-group Modulo and Its Application to Symmetric Cryptography, International Journal of Pure Mathematics; c2022. DOI: 10.46300/91019.2022.9.13.
10. Michael John N, Udoaka OG. Algorithm and Cube-Lattice-Based Cryptography. International journal of Research Publication and reviews. October 2023;4(10):3312-3315.
11. Michael John N, Udoaka OG. Computational Group Theory and Quantum-Era Cryptography, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN :2394-4099, Print ISSN: 2395-1990. 10(6):01-10, November-December 2023. Available at doi :https://doi.org/10.32628/IJSRSET2310556