Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 7, pp. 2873–2883
DOI : 10.47974/JDMSC-2655

Designing a new asymmetric encryption scheme based on a special group ring

Bilel Selikh
Department of Mathematics
Laboratoire de Mathématiques et Physique Appliquées
École Normale Supérieure de Bousaâda
Bousaâda 28001
Algeria

Abstract

In this work, we introduce a novel asymmetric encryption scheme founded on a non-commutative algebraic group defined over a specialized group ring, with the proposed system relying on the computational hardness of both the factorization with discrete logarithm problem (FDLP) and the conjugacy search problem (CSP), which holds a pivotal role in preserving the scheme's security. Security analysis confirms that the scheme meets basic cryptographic standards, providing a good level of protection against known cryptographic attacks.

Subject Classification (2020): *Primary 94A60, Secondary 16S34, 11T71.*

Keywords: *Group ring, Public key cryptography, Conjugacy search problem, Factorization with discrete logarithm problem.*

1. Introduction

Historically, the development of public key cryptography has been based on algebraic structures and hard number theoretic problems, including the integer factorization problem (IFP) and the discrete logarithm problem (DLP).

Prominent examples include the Diffie and Hellman algorithm in 1976 (see [1]), the RSA algorithm proposed by Rivest, Shamir, and Adleman (see [2]) in 1978, and the ElGamal cryptosystem (see [3]), which appeared in 1985. Yet with quantum computing threats getting more serious, and ciphers needing to be hardened against these, the rise in interest in non-commutative algebraic schemes is tangible (see [4-13]).

In this context, group rings and their associated algebraic structures have emerged as promising platforms for the design of public-key cryptosystems.

E-mail: selikh.bilel@ens-bousaada.dz;
bilel.selikh@univ-msila.dz

Recent works have demonstrated that cryptographic constructions based on group rings, integral group rings, and related algebraic units can provide rich non-commutative environments suitable for secure key exchange and encryption schemes (see [14],[15]). In particular, Mittal et al. proposed novel public-key cryptosystems exploiting the algebraic structure of group rings in combination with NTRU-like constructions, highlighting the potential of group ring-based frameworks in modern cryptography (see [14]). Similarly, Küsmüş and Hanoymak introduced a public-key encryption scheme relying on Bass cyclic units in integral group rings, further emphasizing the cryptographic relevance of non-commutative group ring structures (see [15]).

Motivated by these developments, the general linear group over group ring constitute a rich platform for constructing cryptographic schemes using the algebraic richness and non-commutative properties of these structures. Inspired by this idea several recent constructions have suggested protocols relying on the factorization with discrete logarithm problem, a computationally hard problem designed to give more resistance to the known attacks (see [8, 16]).

The proposed work develops a new public-key cryptosystem utilizing the structure of the general linear group built on a special group ring $\mathbb{F}_q[D_m]$ where $\mathbb{F}_q$ is a finite field of order q (q is a power of a prime p) and D_m is the dihedral group of order $2m$ ($m \geq 2 \in \mathbb{Z}$), we provide a description of the processes of key generation, encryption, and decryption. The security of our cryptosystem relies on the joint hardness of two problems: the factorization with discrete logarithm problem (FDLP) and the conjugacy search problem (CSP) (see [5, 17]). By embedding both problems in a non-abelian environment, the proposed system aims to achieve effective resistance against well-known classical attacks, including: Ciphertext-only attacks, Known-plaintext attacks, and Chosen-plaintext attacks.

This paper is organized as follows. The first section provides preliminary overview of essential definitions and concepts required throughout the paper. The second section presents the proposed public key cryptosystem, including the key generation, encryption, and decryption processes. The third section illustrates the system through a numerical example, while the final section analyzes and discusses the security of the proposed cryptographic scheme.

2. Preliminaries

We begin this section by introducing some definitions that will be important in what follows.

Definition 2.1: (FDLP). Consider a finite non commutative group G (of order $O(G) = n$) and two known elements $a, b \in G$. The FDLP asks for the identification of an element $t \in G$ together with an integer $s \in \mathbb{Z}$ satisfying: $b = a^s t$.

Definition 2.2: (Conjugacy Search Problem (CSP)). Consider a non commutative group G, and $a, b \in G$ be conjugate if their exists $x \in G$, such that $b = x^{-1}ax$. The conjugacy problem is to find the element x.

Remark 2.1: The security and computational hardness of the FDLP and CSP are discussed in [8, 13, 16]. Moreover, the common cryptographic attacks described in [10, 17] have been shown to be ineffective against these problems.

Definition 2.3: (Dihedral group). Let $m \geq 2 \in \mathbb{Z}$, the dihedral group D_m is given by:

$$\begin{aligned} D_m &= < \alpha, \beta | \alpha^m = \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} > \\ &= \{1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{m-1}, \beta, \alpha\beta, \dots, \alpha^{m-1}\beta\}, \end{aligned}$$

and $|D_m| = 2m$.

Definition 2.4: (Group ring [18]). Consider a field $\mathbb{K}$ and a group G. The group ring $\mathbb{K}[G]$ consists of all finite sums of the form:

$$\gamma = \sum_{g \in G} a_g g, \text{ where } a_g \in \mathbb{K}.$$

Given two elements $\gamma = \sum_{g \in G} a_g g$ and $\delta = \sum_{g \in G} c_g g$, the operations of addition and multiplication in $\mathbb{K}[G]$ are defined as follows:

$$\gamma + \delta = \left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} c_g g\right) = \sum_{g \in G} \left(a_g + c_g\right) g,$$

and

$$\gamma\sigma = \left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} d_h h\right) = \sum_{k \in G} \left(\sum_{gh=k \in G} a_g d_h\right) k.$$

Example 2.1: Consider the dihedral group $D_5 = \langle \alpha, \beta \mid \alpha^5 = \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} \rangle$, and the group ring $\mathbb{F}_5[D_5]$ with identity 1. Let $x, y \in \mathbb{F}_5[D_5]$, such that:

$$\begin{aligned} x &= \alpha + 2\beta; \\ y &= 3\alpha^4 + 4\alpha^3\beta + \beta. \end{aligned}$$

Then:

$$\begin{aligned} x + y &= \alpha + 3\beta + 3\alpha^4 + 4\alpha^3\beta; \\ xy &= 3\alpha^3 + \alpha\beta. \end{aligned}$$

Now, we consider the general linear group $GL_3(\mathbb{F}_5[D_5])$, consisting of all invertible 3×3 matrices under matrix multiplication. Let $\rho_1, \rho_2 \in GL_3(\mathbb{F}_5[D_5])$, such that:

$$\rho_1 = \begin{bmatrix} 2 & 0 & 0 \\ y & \alpha & 0 \\ x & 0 & 1 \end{bmatrix}, \ \rho_2 = \begin{bmatrix} 0 & \beta & 0 \\ 1 & 0 & 0 \\ y & x & 1 \end{bmatrix}.$$

Then:

$$\rho_1\rho_2 = \begin{bmatrix} 0 & 2\beta & 0 \\ \alpha & \beta y & 0 \\ y & x + \beta x & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2\beta & 0 \\ \alpha & 3\alpha^4\beta + 4\alpha^3 + 1 & 0 \\ 3\alpha^4 + 4\alpha^3\beta + \beta & \alpha + \alpha\beta + 2\beta + 2 & 1 \end{bmatrix}.$$

3. Cryptographic protocol

In this section, we present a cryptographic protocol that utilizes the general linear group over a group ring. This cryptosystem is based on two hard problems

are: the conjugacy search problem (CSP) and the factorization with discrete logarithm problem (FDLP).

Definition 3.1: (Public Key Cryptography (PKC) [19]). A public key cryptosystem is defined as a triplet $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ such that:

- $\mathcal{K}$ denotes a finite set referred to as the key space.
- $\mathcal{E}$ denotes a finite set referred to as the plaintext space.
- $\mathcal{D}$ denotes a finite set referred to as the ciphertext space.
- For every pair $(pk, sk) \leftarrow \mathcal{K}$, there exist an encryption function Enc and a decryption function Dec satisfying:
  1. For any plaintext $M \in \mathcal{E}$, the ciphertext is: $C = Enc(M, pk) \in \mathcal{D}$.
  2. For any ciphertext $C \in \mathcal{D}$, the plaintext is: $M = Dec(C, sk) \in \mathcal{E}$.
  3. For any plaintext $M \in \mathcal{E}$: $Dec(Enc(M, pk), sk) = M$.

Definition 3.2: (Homomorphic Encryption [20]). A public key encryption scheme $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ is said to be homomorphic if, for every key pair $(pk, sk) \leftarrow \mathcal{K}$, there exist algebraic structures $(\mathcal{M}, \circ)$, $(\mathcal{C}, \bullet)$ such that:

- $\mathcal{M}$ is the plaintext space and $Enc(\mathcal{M}, pk) \subseteq \mathcal{C}$ is the ciphertext space.
- For all messages $M_1, M_2 \in \mathcal{M}$, and for ciphertexts $C_1, C_2 \in \mathcal{C}$ where $C_1 = Enc(M_1, pk)$ and $C_2 = Enc(M_2, pk)$, we have:

$$Dec(C_1 \bullet C_2, sk) = M_1 \circ M_2.$$

3.1 *Our cryptosystem*

Our encryption scheme consists of three stages: key generation, encryption, and decryption. We consider two users, denoted by "Bilel" and "Amel". Suppose that "Bilel" wishes to transmit a message to "Amel" over a potentially insecure communication channel.

Let $\mathbb{F}_q[D_m]$ be the group ring, and define $G = GL_n(\mathbb{F}_q[D_m])$ the group of all invertible $n \times n$ matrices whose elements are in $\mathbb{F}_q[D_m]$. Let A be a commutative subgroup of G, and let $B \in G$ of order k (where k is very large). We denote by $C_G(B)$ the centralizer of B in G. The public parameters are: A, B, k, and G.

Key generation

Amel chooses $t, s, r, d \in \{2, \dots, k-1\}$, and $(U, V) \in (A \backslash C_G(B))^2$,

she computes: $\begin{cases} P_1 = B^t U; \\ P_2 = B^s U^3; \\ P_3 = B^r V; \\ P_4 = B^d V^3. \end{cases}$

Then takes: $\begin{cases} \text{The public key}: K_{pub} = (P_1, P_2, P_3, P_4); \\ \text{The private key}: K_{sec} = (t, s, r, d, U, V). \end{cases}$

Encryption

1. Bilel chooses at random an element $W \in A \backslash C_G(B)$ along with a secret positive integer z where $2 \leq z \leq k-1$, and then computes $C_1 = B^z W$.
2. The message is transformed by Bilel into a matrix M, belonging to the semigroup $M_n(\mathbb{F}_q[D_m])$.
3. Bilel encrypts the message M using the encryption function:

$$\begin{aligned} Enc: M_n(\mathbb{F}_q[D_m]) &\to GL_n(\mathbb{F}_q[D_m]) \\ M &\mapsto C_2 = TMT^{-1} \end{aligned}$$

where $\begin{cases} k_i = B^z P_i W, \text{ where } 1 \leq i \leq 4; \\ T = \prod_{i=1}^{4} k_i; \text{ and T be invertible.} \end{cases}$

4. Bilel sends the encrypted message $C = (C_1, C_2)$ to Amel .

Decryption

1. Amel computes: $\begin{cases} k_1 = B^t C_1 U; \\ k_2 = B^s C_1 U^3; \\ k_3 = B^r C_1 V; \\ k_4 = B^d C_1 V^3. \end{cases}$
2. Amel decrypts the message M using the decryption function:

$$\begin{aligned} Dec: GL_n(\mathbb{F}_q[D_m]) &\to M_n(\mathbb{F}_q[D_m]) \\ C_2 &\mapsto M = T^{-1} C_2 T \end{aligned}$$

Correctness

Since: $UW = WU$ and $VW = WV$, then:

$$\begin{cases} B^t C_1 U = B^t B^z W U = B^z (B^t U) W = B^z P_1 W = k_1; \\ B^s C_1 U^3 = B^s B^z W U^3 = B^z (B^s U^3) W = B^z P_2 W = k_2; \\ B^r C_1 V = B^r B^z W V = B^z (B^r V) W = B^z P_3 W = k_3; \\ B^d C_1 V^3 = B^d B^z W V^3 = B^z (B^d V^3) W = B^z P_4 W = k_4. \end{cases}$$

And we have, for any $M \in M_n(\mathbb{F}_q[D_m])$: $Dec \circ Enc(M) = Dec(TMT^{-1}) = T^{-1}TMT^{-1}T = M$.

Proposition 3.1: *Let M_1 and M_2 be two messages in the semigroup $M_n(\mathbb{F}_q[D_m])$, we have:*

$$Enc(M_1 M_2) = Enc(M_1) Enc(M_2).$$

Proof: Let M_1 and M_2 from the semigroup $M_n(\mathbb{F}_q[D_m])$, then:

$$\begin{aligned} Enc(M_1 M_2) &= T M_1 M_2 T^{-1} \\ &= T M_1 T^{-1} T M_2 T^{-1} \\ &= Enc(M_1) Enc(M_2). \end{aligned}$$

Corollary 3.1: *The cryptosystem proposed is homomorphic encryption.*

Remark 3.1: We regard the message as belonging to the semigroup $M_n(\mathbb{F}_q[D_m])$, as neither encryption nor decryption requires the inversion of the matrix M.

4. Numerical example

Let be the dihedral group $D_5 = \langle \alpha, \beta \mid \alpha^5 = \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} \rangle$. We consider the group $GL_3(\mathbb{F}_5[D_5])$, and define the abelian subgroup $A = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{bmatrix}; a, b \in \mathbb{F}_5[D_5] \right\}$ and $B = \begin{bmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha\beta & 0 \\ 0 & 0 & \beta \end{bmatrix}$ of order $k = 10$.

Key generation

Amel chooses the values of $t, s, r, d \in \{2, \dots, 9\}$ where $t = 2, s = 3, r = 4,$ and$d = 5$, along with the matrices $U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \beta & 1 \end{bmatrix}$ and$V = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^2 & \alpha\beta & 1 \end{bmatrix}$.

The following computations are then performed:

$$P_1 = B^2U = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \beta & 1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ \alpha & \beta & 1 \end{bmatrix};$$

$$P_2 = B^3U^3 = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha & 3\beta & 1 \end{bmatrix} = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3\beta & 0 \\ 3\alpha\beta & 3 & \beta \end{bmatrix};$$

$$P_3 = B^4V = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^2 & \alpha\beta & 1 \end{bmatrix} = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4 & 0 \\ \alpha^2 & \alpha\beta & 1 \end{bmatrix};$$

$$P_4 = B^5V^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha^2 & 3\alpha\beta & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 3\alpha^2\beta & 3\alpha & 1 \end{bmatrix}.$$

Amel's private key is $K_{sec} = (t, s, r, d, U, V)$, and the corresponding public key is $K_{pub} = (P_1, P_2, P_3, P_4)$.

Encryption

Bilel chooses $z = 7 \in \{2, \dots, 9\}$ and $W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix}$.

Then computes:

$$C_1 = B^7W = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ \alpha^3 & \alpha^4\beta & \beta \end{bmatrix};$$

$$k_1 = B^7 P_1 W = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ \alpha & \beta & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4\beta & 0 \\ \alpha\beta + \alpha^3 & 1 + \alpha^4\beta & \beta \end{bmatrix};$$

$$k_2 = B^7 P_2 W = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3\beta & 0 \\ 3\alpha\beta & 3 & \beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha + \alpha^3\beta & 3\beta + \alpha^4 & 1 \end{bmatrix};$$

$$k_3 = B^7 P_3 W = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4 & 0 \\ \alpha^2 & \alpha\beta & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha\beta & 0 \\ \alpha^2\beta + \alpha^3 & \alpha + \alpha^4\beta & \beta \end{bmatrix};$$

$$k_4 = B^7 P_4 W = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 3\alpha^2\beta & 3\alpha & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^3\beta & \alpha^4 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 3\alpha^2 + \alpha^3 & 3\alpha\beta + \alpha^4\beta & \beta \end{bmatrix};$$

$$T = (k_1 k_2)(k_3 k_4) = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4\beta & 0 \\ 4\alpha\beta + 2\alpha^3 & 4 + 2\alpha^4\beta & \beta \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3\beta & 0 \\ \alpha\beta + \alpha^2 + 3\alpha^2\beta + \alpha^3\beta & 3\alpha + \alpha\beta + \alpha^3 + \alpha^4 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ \alpha + 3\alpha^2 + \alpha^3 + 2\alpha^4 & \alpha + 2\alpha^2 + 3\alpha\beta + \alpha^4\beta & \beta \end{bmatrix},$$

and its inverse:

$$T^{-1} = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3 & 0 \\ 4\alpha^2\beta + 2\alpha^3\beta + 4\alpha^4\beta + 3 & 4\alpha^4\beta + 2\alpha^4 + 4\alpha^2 + 3\beta & \beta \end{bmatrix}.$$

Let the message $M = \begin{bmatrix} \alpha & \alpha^2\beta & 0 \\ \beta & 1 & 0 \\ \alpha^3 & 2 & 0 \end{bmatrix} \in M_3(\mathbb{F}_5[D_5])$. Then Bilel computes:

$$C_2 = TMT^{-1} = \begin{bmatrix} \alpha & \alpha^4\beta & 0 \\ \alpha^3\beta & 1 & 0 \\ 2\alpha + 3\alpha^2 + \alpha^3 + 3\alpha^4 + \alpha^2\beta + 2\alpha^3\beta + \alpha^4\beta + 2 & \alpha^4 + \alpha\beta + 4\alpha^2\beta + 3\alpha^3\beta + 2 & 0 \end{bmatrix}.$$

Then sends the ciphertext $C = (C_1, C_2)$ to Amel.

Decryption

For decryption, Amel computes:

$$k_1 = B^2C_1U = \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ \alpha^3 & \alpha^4\beta & \beta \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \beta & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4\beta & 0 \\ \alpha\beta + \alpha^3 & 1 + \alpha^4\beta & \beta \end{bmatrix};$$

$$k_2 = B^3C_1U^3 = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^3\beta & 0 \\ 0 & 0 & \beta \end{bmatrix}\begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ \alpha^3 & \alpha^4\beta & \beta \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha & 3\beta & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha + \alpha^3\beta & 3\beta + \alpha^4 & 1 \end{bmatrix};$$

$$k_3 = B^4C_1V = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^4 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ \alpha^3 & \alpha^4\beta & \beta \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^2 & \alpha\beta & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha\beta & 0 \\ \alpha^2\beta + \alpha^3 & \alpha + \alpha^4\beta & \beta \end{bmatrix};$$

$$k_4 = B^5C_1V^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{bmatrix}\begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2\beta & 0 \\ \alpha^3 & \alpha^4\beta & \beta \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3\alpha^2 & 3\alpha\beta & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^4 & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 3\alpha^2 + \alpha^3 & 3\alpha\beta + \alpha^4\beta & \beta \end{bmatrix};$$

and $T^{-1}C_2T = (k_1k_2k_3k_4)^{-1}C_2(k_1k_2k_3k_4) = \begin{bmatrix} \alpha & \alpha^2\beta & 0 \\ \beta & 1 & 0 \\ \alpha^3 & 2 & 0 \end{bmatrix} = M.$

Security

We study three famous attacks:

1. **COA security model:**

   Let us take the ciphertext $C = (C_1, C_2)$ corresponding to the plaintext M_i where $i \in \mathbb{N}^*$. This leads to the system:

   $$\begin{cases} C_1 = B^{\alpha_i} W_i; \\ C_2 = T M_i T^{-1}. \end{cases}$$

   Consequently, recovering the plaintext from the ciphertext requires knowledge of α_i and W_i. However, this task is as difficult as solving the problem of finding the conjugation in a non commutative group and the factorization with the discrete logarithm problem [8, 16]. As a result, it is infeasible to determine (α, W). Instead, the attacker assumes a randomly invertible element $W_0 = W$, leading to $W_0^{-1} C_1 = B^{\alpha_i}$. The consequence is a complex system of equations that cannot be solved efficiently.

2. **KPA security model:**

   Given a known plaintext ciphertext pair (C_i, M_i) for $i \in \mathbb{N}^*$, an attacker's objective is to determine the plaintext M_{i+1} linked to the ciphertext C_{i+1}. In our designed public-key cryptosystem (PKC), new private keys (α, W) are selected for each encryption process, ensuring that the session key (α, W, T) varies with every session. As a result, knowing a previous plaintext-ciphertext pair does not reveal any details concerning later pairs, there by ensuring the security of our protocol against this type of threat.

3. **CCA security model:**

   In a chosen ciphertext setting, an attacker can determine the original message that corresponds to a given ciphertext $C = (C_1, C_2)$. By choosing an invertible matrix $M' \in M_n(\mathbb{F}_q[D_m])$ at random, the attacker can compute a modified ciphertext $C' = (C_1, C_2 M')$, which results in MM'. Subsequently, the attacker can derive the original plaintext by computing $MM'M'^{-1} = M$. Nevertheless, in the system we propose, the ciphertext is structured as $C_2 = TMT^{-1} = (\prod_{i=1}^{4} k_i) M (\prod_{i=1}^{4} k_i)^{-1}$. Given that B and W do not commute, executing this attack is not possible.

Conclusion

In this work, we proposed a cryptosystem based on the factorization with discrete logarithm problem (FDLP) and cojugacy search problem (CCP) utilizing the general linear group constructed on the group ring $\mathbb{F}_q[D_m]$. Through our analysis, we showed that the proposed scheme offers a good level of security and can resist several known attacks commonly targeting such cryptographic protocols.

Acknowledgment

The author would like to thank reviewers for their valuable comments and constructive suggestions, which helped improve the quality of this paper.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Information Theory*, vol. 22, no. 6, pp. 644-654 (1976).

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126 (1978).

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Information Theory*, vol. 31, no. 4, pp. 469-472 (1985).

[4] R. Alvarez, F. Martinez, J. Vicent, and A. Zamora, "A new public key cryptosystem based on matrices," in *Proc. WSEAS Int. Conf. Information Security and Privacy*, pp. 36-39 (2007).

[5] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings," *Groups Complexity Cryptology,* vol. 5, no. 1, pp. 97-115 (2013).

[6] S. Kanwal and R. Ali, "A cryptosystem with noncommutative platform groups," *Neural Computing and Applications*, vol. 29, no. 11, pp. 1273-1278 (2018).

[7] C. M. Koupparis, Non-Commutative Cryptography: Diffie-Hellman and CCA-Secure Cryptosystems Using Matrices over Group Rings and Digital Signatures, Ph.D. dissertation, City University of New York, New York, NY, USA (2012).

[8] S. Makhlouf and K. Guenda, "A new public key cryptosystem based on group rings," *Advances in Mathematics: Scientific Journal,* vol. 12, no. 2, pp. 357-366 (2023).

[9] A. J. Menezes and Y.H. Wu, "The discrete logarithm problem in GL(n,q)," *Ars Combinatoria,* vol. 47, pp. 23-32 (1997).

[10] G. Micheli, "Cryptanalysis of a non-commutative key exchange protocol," *Advances in Mathematics of Communications*, vol. 9, no. 2, pp. 247-253 (2015).

[11] G. Mittal, S. Kumar, S. Narain, and S. Kumar, "Group ring based public key cryptosystems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 6, pp. 1683-1704 (2021).

[12] B. Selikh, On elliptic curves and application to cryptography, Ph.D. dissertation, Department of Mathematics, University of M'sila, Algeria (2022).

[13] B. Selikh, A. Chillali, D. Mihoubi, and N. Ghadbane, "A new public key cryptosystem based on the non-commutative ring R," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 1, pp. 75-93 (2024).

[14] G. Mittal, S. Kumar, and S. Kumar, "Novel public-key cryptosystems based on NTRU and algebraic structure of group rings," *Journal of Information and Optimization Sciences*, vol. 42, no. 7, pp. 1507-1521 (2021).

[15] Ö. Küsmüs and T. Hanoymak, "A novel public-key encryption scheme based on Bass cyclic units in integral group rings," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 2, pp. 579-589 (2022).

[16] I. Gupta, A. Pandey, and M. K. Dubey, "A key exchange protocol using matrices over group rings," *Asian-European Journal of Mathematics,* vol. 12, no. 5, pp. 1950075 (2019).

[17] M. Eftekhari, "A Diffie-Hellman key exchange protocol using matrices over non-commutative rings," *Groups Complexity Cryptology,* vol. 4, no. 1, pp. 167-176 (2012).

[18] D. S. Passman, The Algebraic Structure of Group Rings. New York, NY, USA: Wiley (1977).

[19] A. Chatterjee and K. M. M. Aung, Fully Homomorphic Encryption in Real World Applications, Computer Architecture and Design Methodologies. Singapore: Springer Nature (2019).

[20] C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment, Information Security and Cryptography Series. Heidelberg, Germany: Springer-Verlag (2003).

Received August, 2025