GROUP RING BASED ELGAMAL TYPE PUBLIC KEY CRYPTOSYSTEMS

Gaurav Mittal$^{1,2}$, Sunil Kumar$^2$, Shiv Narain$^3$, and Sandeep Kumar$^2$

$^1$Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, India
$^2$DRDO, India
$^3$Department of Mathematics, Arya P. G. College, Panipat, India
emails: gmittal@ma.iitr.ac.in, sunilkumar@hqr.drdo.in,
math.shiv@gmail.com, sandeepkumar@hqr.drdo.in

Abstract. In this paper, we propose two cryptosystems based on group rings and existing cryptosystem. First one is Elliptic ElGamal type group ring public key cryptosystem whose security is greater than security of cryptosystems based on elliptic curves discrete logarithmic problem (ECDLP). Second is ElGamal type group ring public key cryptosystem, which is analogous to ElGamal public key cryptosystem but has comparatively greater security. Examples are also given for both the proposed cryptosystems.

Mathematics Subject Classification (2010): 94A60, 20C05, 20C07

Keywords: group ring, units, cryptography, public key cryptography

1. Introduction

Cryptography is the study of mathematical techniques for achieving Privacy, Authentication, Integrity and Non-repudiation, i.e. PAIN. For the secrecy and authenticity of sensitive information, cryptosystems are used extensively. The one and only aim of these cryptosystems is to ensure end-to-end communication between two or more parties such that the information encrypted at one end is understood only at the other end. For end-to-end secure communication, various symmetric ciphers have been developed till 1970’s, for instance, classical substitution ciphers, transposition ciphers, rotor machines (see [11]) etc. Since then many symmetric ciphers came in the picture but security-wise some of the best known are DES and AES both based on the concepts of confusion and diffusion introduced by Claude Shannon [12], however, in the current scenario DES is no longer in use because the key length does not withstand against the brute force attack.

One of the greatest revolution in cryptography is the development of asymmetric or public key cryptography. Some of the well known public key cryptosystem or ciphers are RSA, ElGamal, NTRU (see [9,11]) etc. The security of most of the public key cryptosystem depend on the hardness of solving some underlying mathematical problem with a trapdoor like integer factorization, discrete logarithmic, shortest non-zero vector in the lattice etc. and most of these problems arise in number theory [9]. Combinatorial group theory has also attracted
much interest for the construction of public key cryptosystems [1, 2, 4]. The hard underlying mathematical problem associated with most of these cryptosystems is conjugacy search problem which can be considered as the generalization of discrete logarithm problem to groups other than \( \mathbb{F}_p \) where \( p \) is some prime. During the recent years, elliptic curves over finite fields have drawn the attention of many researchers, see [6, 7]. The interesting problem of adding two points on an elliptic curve was a very subtle issue and theory behind it leads to the fascinating field of mathematics known as Algebraic Geometry. For additional reading devoted to elliptic curve cryptography, see [13, 14]. To the best of our knowledge, algebraic structure known as group rings has not been used in cryptography up to first decade of 21st century. Hurley [15] discussed the various applications of group rings to the areas of communication. In [5], the first known symmetric key cryptosystem using group rings was demonstrated with few examples which show how to combine RSA and unit of group ring and how to use large power of a unit as a public key but no public key cryptosystem was discussed explicitly.

In this paper, we discuss two novel group rings based public key cryptosystems. First one is Elliptic ElGamal type group ring public key cryptosystem and second one is ElGamal type group ring public key cryptosystem without the involvement of Elliptic curves. Elliptic ElGamal public key cryptosystem which is analogous to ElGamal is discussed in [9]. The main difficulty with this cryptosystem is non-obvious way of attaching the plaintext messages and elements of elliptic curve over finite field. We try to resolve this problem in our work by combining the elements of group ring with that of elliptic curves in a unique manner. The sounding effect of these proposed public key cryptosystems is their enhanced security in comparison to that of existing cryptosystems. This enhanced security can be well understood for traditional classical computers but in the coming era of quantum computers where public key cryptosystems (in particular, RSA, ECDSA) are no longer safe [16, 18, 19], this can play a vital role because of the involvement of two operations in group ring which are connected via distributive law.

Rest of the paper is designed as follows: Section 2 pertains to preliminary definitions and discussion of both the novel cryptosystems. Examples related to these schemes are discussed in Section 3. Section 4 is related to discussion of availability of units of group rings and last section comprises some concluding remarks.

2. Cryptographic systems in group rings

In the present section, we propose two public key cryptosystems in group rings. But before that, we provide some preliminary definitions and results requisite for our work.

**Definition 2.1.** *Group Ring: Let* \( R \) *be a ring with unity and* \( G \) *be a group. The set*

\[
RG = \left\{ \sum_{j=1}^{t} r_j g_j : r_j \in R, g_j \in G \right\}
\]


of all finite sums is known as group ring. As name suggests, RG is a group, ring, and module over R. See [10] for more information on group rings. For \( a, b \in RG \), \( a \ast b \) denotes the product of \( a \) and \( b \).

**Definition 2.2.** Unit of a group ring: Let \( u \in RG \). This \( u \) is a unit of \( RG \) if there exists an element \( v \in RG \) such that

\[
u \ast v = v \ast u = 1.
\]

Set of all units of \( RG \) forms a group under the operation \( \ast \).

**Definition 2.3.** Normalized unit of a group ring: Let

\[u = \sum_{i=1}^{k} \alpha_i g_i \in RG \text{ with } \alpha_i \in R \text{ and } g_i \in G \text{ be a unit of } RG.\]

This \( u \) is said to be normalized if

\[
\alpha_1 + \alpha_2 + \cdots + \alpha_k = 1.
\]

Set denoted by \( V(RG) \) of all the normalized units of \( RG \) forms a group under the operation \( \ast \).

**Definition 2.4.** Discrete Logarithmic Problem (DLP): Let \( g, h \) be two elements of \( \mathbb{F}_p \) such that \( h \) is some power of \( g \). Then DLP is the problem of finding an integer \( n \) such that

\[h = g^n.\]

**Definition 2.5.** Discrete Logarithmic Problem (DLP) in group ring: Let \( u \) be an element of \( RG \) and \( v \) be another element of \( RG \) which is some power of \( u \). Then, DLP in group ring is determination of an integer \( x \) such that

\[v = u^x.\]

**Definition 2.6.** Elliptic Curve: Consider the Weierstrass equation

\[E : Y^2 = X^3 + RX + S.\]

Set of all the solutions of \( E \) together with an extra point \( O \) that lives at infinity is an elliptic curve. Here \( R \) and \( S \) are constants which satisfy

\[4R^3 + 27S^2 \neq 0.\]

Further, if we consider only those elements of \( E \) which also belong to \( \mathbb{F}_p \times \mathbb{F}_p \), then the set

\[E(\mathbb{F}_p) = \{(x, y) : (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \text{ and } y^2 = x^3 + Rx + S\} \cup \{O\}\]

is an elliptic curve over the finite field \( \mathbb{F}_p \) with \( R, S \in \mathbb{F}_p \).

**Definition 2.7.** Elliptic Curve Discrete Logarithmic Problem (ECDLP): Let \( P, Q \) be two points on elliptic curve \( E(\mathbb{F}_p) \). Then ECDLP is the problem of determination of an integer \( n \) such that

\[Q = nP,\]

provided such an integer exists.

Next, we give the explicit formulas to add and subtract any two points on an elliptic curve. For proof see [9, Theorem 5.6].

**Theorem 2.1.** Let \( P \) and \( Q \) be any two points on the elliptic curve \( E(\mathbb{F}_p) \).

1. If \( P = O \), then \( P + Q = Q \). Similarly, if \( Q = O \), then \( P + Q = P \).
2. Otherwise, write \( P = (x_1, y_1) \) and \( Q = (x_2, y_2) \).
(3) If \( x_1 = x_2 \) and \( y_1 + y_2 = 0 \), then \( P + Q = O \).

(4) Otherwise, define \( \lambda \) by

\[
\lambda = \begin{cases} 
3x_1^2 + R & \text{if } P = Q \\
2y_1 & \text{if } P \neq Q. 
\end{cases}
\]

Then \( P + Q = (x_3, y_3) \) with

\[
x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1.
\]

Now, we discuss the important task of associating each data or number to be encrypted with the elements of group ring \( RG \) where \( R \) is the ring with identity and \( G = \{g_1, g_2, \ldots\} \) is either finite or countable group. In our study, we either consider \( R = \mathbb{F}_p \) for some prime \( p > 0 \) or \( R = \mathbb{Z} \).

### 2.1. Connection between given data and elements of group ring.

Suppose that all the digits of the data to be encrypted are elements of \( R \), for instance, data consists of elements ranging from 0 to \( p - 1 \) for some prime \( p \) and \( R = \mathbb{Z}_p \). Given any arbitrary data, write it in blocks of length \( t \) where \( t \in \mathbb{Z}^+ \). Further, any arbitrary data block \( m = m_1m_2 \cdots m_t \) with \( m_i \in R \) can be considered as an element of group ring \( RG \) via the following representation

\[
r = \sum_{i=1}^{t} m_i g_i, \quad g_i \in G.
\]

For above representation to be unique, order of \( G \) must be at least \( t \) and therefore we assume the same, i.e. \( |G| \geq t \) and can be at most countable. If length of the message is not a multiple of \( t \), then padding can be done with 0’s.

### 2.2. Elliptic ElGamal type group ring public key cryptosystem.

Given a message \( r = \sum_{i=1}^{t} m_i g_i \), write it uniquely as a row vector

\[
r = [m_1 \quad m_2 \quad \cdots \quad m_t]
\]

where \( m_i \) is the coefficient of element \( g_i \) in \( r \). Choose a point \( P = (x_1, y_1) \) on the elliptic curve \( E(\mathbb{F}_p) \) and a unit \( u \) of group ring \( RG \) such that order of \( u \) is large. This unit is not made public. Further, secretly choose two positive integers \( (n_1, n_2) \) and use these integers to compute

\[
Q = n_1 P = (x_2, y_2) \quad \text{and} \quad A = u^{n_2}
\]

where \( A \in RG \). Set \((P, Q, A)\) as the public key for encryption and \((n_1, u^{-n_2})\) as the private key for decryption. Now select a random one time key \( n_3 \) and let \( n_3 Q = (x_3, y_3) \). This key is used for encrypting only one message or some fixed number of blocks that needs to be decided in the beginning and then discarded.
2.2.1. Encryption. For encryption, message $r$ is encrypted using public key to obtain the ciphertext $(C_1, C_2)$ where

$$C_1 = n_3P, \quad C_2 = (r \oplus n_3Q) * A$$

where the $\oplus$ operation is defined as

$$r \oplus n_3Q = \begin{bmatrix} m_1 & m_2 & \cdots & m_t \end{bmatrix} \oplus (x_3, y_3)$$

$$= \begin{bmatrix} m_1 + x_3 + y_3 & m_2 + x_3 + y_3 & \cdots & m_t + x_3 + y_3 \end{bmatrix}$$

with $n_3Q = (x_3, y_3)$, $2n_3Q = (x_4, y_4)$, $3n_3Q = (x_5, y_5)$, $\cdots$, $tn_3Q = (x_{t+2}, y_{t+2})$

and since $m_i, x_i, y_i \in \mathbb{F}_p$, above addition is defined. Rationale behind the $\oplus$ operation is to combine an element of group ring with an element of elliptic curve such that the result is an element of group ring. So, the ciphertext $(C_1, C_2)$ has two parts where $C_1$ is the element of elliptic curve and $C_2$ is the element of group ring. This ciphertext is then send to the receiver say Alice.

**Remark 2.1.** If the message $m$ is of the form

$$\begin{bmatrix} m_1 & 0 & m_4 & 0 & \cdots & 0 \end{bmatrix},$$

then we can simply encrypt it in the form $\begin{bmatrix} m_1 & 0 & m_4 \end{bmatrix}$. But the 0 entries in between the non-zero entries of the message cannot be skipped and needs to be considered in order to uniquely obtain the plaintext from ciphertext.

**Remark 2.2.** Suppose that the operation $\oplus$ is of the form

$$r \oplus n_3Q = \begin{bmatrix} m_1 & m_2 & \cdots & m_t \end{bmatrix} \oplus (x_3, y_3)$$

$$= \begin{bmatrix} m_1 + x_3 + y_3 & m_2 + x_3 + y_3 & \cdots & m_t + x_3 + y_3 \end{bmatrix}$$

where we are adding $x_3 + y_3$ in every message digit. This added block can leak some information about the message if there are consecutive zeros in the message. To avoid such a situation we added the multiples of $(x_3, y_3)$ in the message digits.

2.2.2. Decryption. Since Alice knows $u^{-n_2}$, she computes

$$C_2 * u^{-n_2} = (r \oplus n_3Q) * A * u^{-n_2} = r \oplus n_3Q.$$

Alice also knows $n_1$ and she use this to obtain

$$n_1C_1 = n_1n_3P = n_3n_1P = n_3Q.$$

Thereafter, she computes the multiples of $n_3Q$ and perform the decryption operation $\ominus$, i.e.

$$(C_2 * u^{-n_2}) \ominus n_1C_1 = (r \oplus n_3Q) \ominus (x_3, y_3)$$

$$= \begin{bmatrix} m_1 + x_3 + y_3 & m_2 + x_3 + y_3 & \cdots & m_t + x_{t+2} + y_{t+2} \end{bmatrix} \ominus (x_3, y_3)$$
\[
\begin{bmatrix} m_1 & m_2 & \cdots & m_t \end{bmatrix} = \sum_{i=1}^{t} m_i g_i = r
\]

where \( \oplus \) operation means subtracting \( x_3 + y_3, x_4 + y_4, \cdots, x_{t+2} + y_{t+2} \) from the corresponding elements of row vector.

**Remark 2.3.** We can also consider \( R = \mathbb{Z} \) in Elliptic ElGamal type group ring public key cryptosystem in place of \( \mathbb{F}_p \). In that case, whole encryption scheme remains same with the only difference that operation \( \oplus \) involves usual addition instead of addition modulo \( p \).

**Remark 2.4.** For Elliptic ElGamal type group ring public key cryptosystem, we can also consider fields of different characteristics. For instance, we can consider \( E(\mathbb{F}_p) \) and \( R = \mathbb{Z}_q \) where \( p \) and \( q \) are some primes. If \( p < q \), then the operation \( \oplus \) involves addition modulo \( q \) and we directly add the elements of elliptic curves to that of group ring. If \( p > q \), then first we need to convert the elements of elliptic curve to elements modulo \( q \) and then apply operation \( \oplus \) which again involves addition modulo \( q \). An example related to this situation is discussed in Section 3.

2.2.3. **Logic behind the name.** Proposed encryption scheme is a novel approach involving the important operation of combining the elements of a group ring with those of Elliptic curve. The parameters involved are similar to ElGamal and hence the cryptosystem is named as Elliptic ElGamal type group ring public key cryptosystem.

2.2.4. **Security of the scheme.** To obtain the plaintext from ciphertext, adversary in between needs to:

1. solve ECDLP.
2. determine inverse of power a unit or unit from its power.

In \( \mathbb{F}_p^* \), there are algorithms for solving DLP and the fastest known algorithm has subexponential running time known as index calculus method [9]. But there are no such algorithms for solving ECDLP. The fast known algorithm takes approximately \( \sqrt{p} \) times to solve ECDLP (for example Pollard’s \( \rho \) method [9]), i.e. to say that there is no polynomial time algorithm to solve ECDLP.

Now we discuss the hardness of inverse computation problem in group rings. There exist units which can be constructed by some formula (let’s say known type units), for instance, unipotent units, central units, Bass cyclic units, Bicyclic units [10]. On taking power of a known type unit, resulted unit may not be of known type and it becomes computationally infeasible to determine the inverse of a such a unit for large groups. Determination of unit from its power also adds the difficulty of DLP. Further, if the group operations are complicated, e.g. operations in Braid groups, Sporadic groups etc., then the problem of inverse computation of power of a unit of any type becomes much more difficult without knowing the unit. Moreover, we can also combine the units of known type to get units of unknown type, for instance \( A = (u_1u_2)^{n_1} \) where \( u_1 \) and \( u_2 \) are units of known type and it becomes computationally infeasible to obtain the inverse of
such a unit without knowing the inverse of constituent units. So, in general we can say that it is safe to use power of units, power of product of units as the public keys.

Hence, the novel scheme is much more secure than the schemes whose security relies on solving ECDLP, e.g. Elliptic Elgamal public key cryptosystem. In the current scenario, recommended key sizes (in bits) are 2048, 3072, 7680, · · · for RSA and Diffie-Hellman whereas 224, 256, 384, · · · for the elliptic curves. This means elliptic curves have an edge over RSA and Diffie-Hellman in terms of key size despite the highly structured nature of $E(\mathbb{F}_p)$. If we consider an elliptic curve over a prime $p$ having size 224 bits, then we can say that Elliptic ElGamal type group ring public key cryptosystem has a security equivalent to security of cryptosystems on $E(\mathbb{F}_{p'})$ where size of $p'$ is $224 + k$ bits for some positive integer $k$ where $k$ depends on the structure of the unit group of group ring.

Now we introduce our second cryptosystem. For this cryptosystem too, parameters involved are similar to ElGamal (although cryptosystem is entirely different) and hence we name it as ElGamal type group ring public key cryptosystem.

2.3. **ElGamal type group ring public key cryptosystem.** Secretly choose a unit $u \in RG$ of large order and two positive integers $n_1$ and $n_2$. Then find $A_1 = u^{n_1}$. Choose another unit $v \in RG$ of large order (open in public domain) and set $A_2 = v^{n_2}$. Declare $(A_1, A_2, v)$ as the public key and $(A_1^{-1}, n_2)$ as the corresponding private key. Now as in ElGamal, select a random ephemeral key $k$.

2.3.1. **Encryption.** For encryption, find the ciphertext $(C_1, C_2)$ where

$$C_1 = v^k, \quad C_2 = (r \ast A_1) \ast A_2^k.$$

This ciphertext is then send to Alice.

2.3.2. **Decryption.** As the second part $n_2$ of private key is known to Alice, she finds $(C_1)^{-n_2}$ and use this to obtain

$$C_2 \ast v^{-n_2k} = r \ast A_1.$$

On multiplying above with $A_1^{-1}$ (first part of private key), Alice gets the message $r$.

2.3.3. **Security of the scheme.** To obtain plaintext from the ciphertext, Eve needs private key, i.e. $n_2$ and $A_1^{-1}$ which requires the determination of unit from its power and inverse of a given unit respectively. In other words, Eve’s first task is to solve the DLP in group ring which is much harder than DLP in groups because a group ring involve two operations connected via distributive law whereas a group involves only one operation. So far there is no threat to DLP from classical computers for properly chosen groups which means DLP in group rings is also safe. But there exist quantum algorithms to solve DLP in finite groups, however, nothing is known to solve DLP in group rings or non-abelian groups [19]. Therefore, we can say that DLP in group rings is much harder than DLP in groups, even in quantum word. Hardness of Eve’s second
task, i.e. inverse computation problem is already discussed in Subsection 2.2.4. Therefore, we conclude that ElGamal type group ring public key cryptosystem is much more secure than the existing ElGamal cryptosystem.

**Remark 2.5.** For ElGamal type group ring public key cryptosystem, $R$ can be ring of integers also. In that case too, we write the message in blocks of length $t$ with $|G| \geq t$. Example involving integral group ring is discussed in next section.

3. Examples

In this section, we discuss some examples of the group ring public key cryptosystems defined in the preceding section. From now onwards, we write GRPKC as a short form for group ring public key cryptosystem. Most of the results including determination of units, computation of powers of units and their corresponding inverses can be obtained using GAP (Groups, Algorithm and Programming) [17], MAGMA or MATLAB.

3.1. Elliptic ElGamal type GRPKC. For the better understanding of Elliptic ElGamal type GRPKC, we give a simple example by considering the small parameters. Suppose that the message $m$ of arbitrary size consists of only English alphabets (this restriction is made only for understanding), let’s say $\{A, B, \cdots, Z\}$. So, we map these alphabets on the elements of $\mathbb{F}_{29}$ by the mapping

$$
\{A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, \cdots, Z \rightarrow 25\}.
$$

Suppose the message is “ARMY”. We consider $G = C_{29} = \langle g \rangle$, i.e. cyclic group of order 29. In terms of element of group ring, we write the message in the form

$$
r = 0e + 17g + 12g^2 + 24g^3 = \begin{bmatrix} 0 & 17 & 12 & 24 \end{bmatrix}.
$$

Consider the elliptic curve

$$
E(\mathbb{F}_{29}) : y^2 = x^3 + 4x + 20 \mod 29
$$

and a point $P = (8, 10)$ on it. We consider the trivial unit $g$ of $\mathbb{F}_{29}G$ and choose the private key $(n_1, g^{-n_2}) = (4, g^{-3})$. Public key is $(P, Q, A)$ where

$$
Q = (6, 17), \quad A = g^3.
$$

Let $n_3 = 3$ and using Theorem 2.1, we get

$$
n_3Q = (3, 28), \quad 2n_3Q = (24, 22), \quad 3n_3Q = (8, 19), \quad 4n_3Q = (5, 22).
$$

Now we find the ciphertext $(C_1, C_2)$ corresponding to message $r$. Using $n_3 = 3$, we get $C_1 = 3P = (16, 2)$. Further, we have

$$
(r \oplus n_3Q) = \begin{bmatrix} 0 & 17 & 12 & 24 \end{bmatrix} \oplus (3, 28)
$$

$$
= \begin{bmatrix} 0 + 3 + 28 & 17 + 24 + 22 & 12 + 8 + 19 & 24 + 5 + 22 \end{bmatrix}
$$

8
Above yields
\[ C_2 = (r + n_3Q) \ast A = 2g^3 + 5g^4 + 10g^5 + 22g^6 = [0 \ 0 \ 2 \ 5 \ 10 \ 22]. \]

Therefore the ciphertext is
\[ (C_1, C_2) = \left((16, 2), [0 \ 0 \ 2 \ 5 \ 10 \ 22] \right). \]

For decryption, Alice first of all use the second part of her private key to get
\[ C_2 \ast g^{-3} = [0 \ 0 \ 2 \ 5 \ 10 \ 22] \ast g^{-3} = (2g^3 + 5g^4 + 10g^5 + 22g^6) \ast g^{-3} = 2 + 5g + 10g^2 + 22g^3 = [2 \ 5 \ 10 \ 22]. \]

Now Alice use first part \( n_1 \) of her private key to obtain
\[ n_1C_1 = 4(16, 2) = (3, 28) \]

and multiples of \((3, 28)\). Clearly Alice needs to compute only 4 multiples of \((3, 28)\) as the remaining terms are zero in \( C_2 \ast g^{-3} \). Decrypted message is
\[ (C_2 \ast g^{-3}) \oplus (3, 28) = \left[2 \ 5 \ 10 \ 22 \right] \oplus (3, 28) = \left[ 2 - 3 - 28 \ 5 - 24 - 22 \ 10 - 8 - 19 \ 22 - 5 - 22 \right] = \left[0 \ 17 \ 12 \ 24 \right] = \text{ARMY}. \]

We have chosen trivial unit for this example so that it can be done manually. In the upcoming examples, we consider non-trivial units which actually make the scheme worthy.

3.2. **Elliptic ElGamal type GRPKC for \( R = \mathbb{Z} \) and \( G = D_{10} \).** In this subsection, we provide an example which highlights the importance of Remark 2.3. We consider the integral group ring of group \( G = D_{10} \) which means message has integer values. \( G \) can be represented as
\[ G = \langle r, s \mid r^5 = 1 = s^2, sr = r^4s \rangle = \{1, r, r^2, r^3, s, rs, r^2s, r^3s, r^4s\}. \]

Consider the element \( u = 1 - 2\pi - 2r^2 + r^3 + 3r^4 \) of \( RG \). It can be verified that \( u \) is a unit of \( RG \) with \( u^{-1} = -2 + 3r - 2r^2 + r^3 + r^4 \). Now, consider the elliptic curve
\[ E(\mathbb{F}_{263}) : y^2 = x^3 + 2x + 3 \mod 263 \]

and a point \( P = (200, 39) \) on it. Choose the private key \((10, u^{-8})\) with the corresponding public key \((P, Q, A)\) where
\[ Q = 10P = (47, 78), \ \ A = u^8 = -1576239 + 602070r + 1948339r^2 + 602070r^3 - 1576239r^4 \]
and
\[ u^{-8} = 602070 + 602070r - 1576239r^2 + 1948339r^3 - 1576239r^4 \]
Let $n_3 = 5$ and using Theorem 2.1, we get

\[ n_3Q = (180, 115), \quad 2n_3Q = (5, 123), \quad 3n_3Q = (128, 81), \quad 4n_3Q = (127, 213) \quad 5n_3Q = (17, 189) \]

\[ 6n_3Q = (102, 90), \quad 7n_3Q = (74, 155), \quad 8n_3Q = (142, 89), \quad 9n_3Q = (144, 228) \quad 10n_3Q = (139, 12). \]

Now we find the ciphertext $(C_1, C_2)$ corresponding to message

\[ r' = [1 \quad 2 \quad -1 \quad 6 \quad 0 \quad 8 \quad 0 \quad 3 \quad 9 \quad -5]. \]

Using $n_3 = 5$, we get $C_1 = 5P = (251, 155)$. Further, we have

\[ (r' \oplus n_3Q) = [1 \quad 2 \quad -1 \quad 6 \quad 0 \quad 8 \quad 0 \quad 3 \quad 9 \quad -5] \oplus (180, 115) \]

\[ = [296 \quad 130 \quad 208 \quad 346 \quad 206 \quad 200 \quad 229 \quad 234 \quad 381 \quad 146] \mod 2^{10} \]

Above yields

\[
C_2 = (r' \oplus n_3Q) \ast A = 251904460 + 255117992r - 94232542r^2 - 313356578r^3 - 99432146r^4 + 277795332s + 294897228rs - 9538493r^2s - 353942935r^3s - 123209942r^4s.
\]

Therefore the ciphertext is $(C_1, C_2)$. Decryption can be done similarly as shown in subsection 3.1. Clearly, this example shows the beautiful mixing of points of elliptic curve and the message. Now we discuss an example as said in Remark 2.4.

### 3.3. Elliptic ElGamal type GRPKC for $R = \mathbb{F}_2$ and $G = D_{10}$. We assume that message is in bits or in other words $R = \mathbb{F}_2$, $G$ is Dihedral group of order 10 with the same representation considered in last example. Clearly, the group ring $RG$ has 1024 elements. Consider the element

\[ u = r^2 + r^4 + s \]

of $RG$. It can be verified that $u$ is a unit of $RG$ with inverses

\[ u^{-1} = 1 + r + r^3 + r^4 + s + rs + r^4s. \]

Rest of the setting including choice of elliptic curve, selection of point $P$ on elliptic curve, public key and private key is exactly same to the one considered in last example. So, the private and public keys are $(10, u^{-8})$ and $(P, Q, A)$ respectively where

\[ Q = 10P = (47, 78), \quad A = u^8 = 1 + r + r^2 + rs + r^2s + r^3s + r^4s \quad \text{and} \quad u^{-8} = r^4 + rs + r^4s. \]

Let $n_3 = 5$ and using Theorem 2.1 we can get the multiples of $n_3Q$ as done in last example. Now we find the ciphertext $(C_1, C_2)$ corresponding to message

\[ r' = [1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]. \]

Using $n_3 = 5$, we get $C_1 = 5P = (251, 155)$. Further, we have

\[ (r' \oplus n_3Q) = [1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1] \oplus (180, 115) \]

\[ = [296 \quad 128 \quad 209 \quad 340 \quad 206 \quad 192 \quad 229 \quad 231 \quad 372 \quad 151] \mod 2^{10} \]
Above yields
\[ C_2 = (r' + n_3Q) * A = 1 + r^2 + r^4 + s + rs + r^4s = [1 0 1 0 1 1 0 0 1]. \]

Therefore the ciphertext is \((C_1, C_2)\). For decryption, Alice first of all use the second part of her private key to get \(C_2 * A^{-1}\). Now Alice use first part \(n_1\) of her private key to obtain \(n_1C_1 = (180, 115)\) and its multiples. Clearly Alice needs to compute only 10 multiples of (180, 115) which is decided by the length of group. These multiples are then added to \(C_2 * A^{-1}\) under modulo 2 to get the original message.

Now we discuss some examples for the feel of ElGamal GRPKC. All the three examples discussed above involve small parameters, but for the practical implementation of these schemes, we need to work with large numbers or in other words, large power of units. In the next example, we take care of this thing and consider large (reasonably) parameters.

3.4. ElGamal type GRPKC for an abelian group. Let \(r = 11110100001\) is the message, \(R = \mathbb{F}_2\) and \(G\) is cyclic group of order 11, i.e.
\[ G = \{g^i : 0 \leq i \leq 10\} \]
and we denote \(g_i = g^i\). Clearly, the group ring \(RG\) has 2048 elements. Given message as an element of group ring is
\[ r = 1 + g + g^2 + g^3 + g^5 + g^{10} = [1 1 1 0 1 0 0 0 0 1]. \]
Take a unit \(u = 1 + g + g^3\) (verify that \(u^{-1} = 1 + g + g^3 + g^6 + g^7 + g^8 + g^{10}\)) having order 1023 and calculate
\[ A_1 = u^{400} = g^2 + g^4 + g^6 + g^7 + g^{10}. \]
Further, choose another unit
\[ v = 1 + g + g^2 + g^4 + g^5 + g^6 + g^8 + g^9 + g^{10} \]
with \(v^{-1} = 1 + g + g^3 + g^6 + g^9\) and a secret positive integer \(n_2 = 33\). Public key is \((A_1, A_2, v)\) with \(A_2 = v^{33}\). Private key is \((A_1^{-1}, 33)\) with
\[ A_1^{-1} = 1 + g + g^2 + g^5 + g^7 + g^8 + g^{10}. \]
Using public key the obtained ciphertext with ephemeral key \(k = 19\) is \((C_1, C_2)\) where
\[ C_1 = v^{19} = g^5 + g^7 + g^9 \]
and
\[ C_2 = (r * A_1) * A_2^k = (r * u^{400}) * v^{627} = 1 + g^2 + g^4 + g^6 + g^9 + g^{10} \]
\[ = [1 0 1 0 1 0 1 0 0 1]. \]
After obtaining the ciphertext \((C_1, C_2)\), Alice computes \((C_2 \cdot C_1^{-n_2}) \cdot A_1^{-1}\) using her private key to get the message.

Next example is related to Integral ElGamal GRPKC.

3.5. ElGamal type GRPKC for \(R = \mathbb{Z}\) and \(G = C_8\). Let \(RG\) be the integral group ring with \(G = C_8 = \langle x \rangle\), cyclic group of order 8. We denote \(g_i = x^i, 0 \leq i \leq 7\) and consider the message blocks of length 8 for encryption. Let

\[
 r = [0 \ 1 \ -10 \ 17 \ 0 \ 0 \ 0 \ -4]
\]

is the message to be encrypted. In terms of element of group ring, \(r\) can be written as

\[
 r = x - 10x^2 + 17x^3 - 4x^7.
\]

Here we choose small parameters otherwise the expressions becomes so large to print here but one can choose arbitrary large numbers. Consider the element \(u = 2e + x - x^3 - x^4 - x^5 + x^7\) of \(RG\). It can be verified that \(u\) is a unit of \(RG\) with \(u^{-1} = 2e - x + x^3 - x^4 + x^5 - x^7\) having infinite order. Take \(n_1 = 2\) and calculate

\[
 A_1 = u^2 = 9e + 6x - 6x^3 - 8x^4 - 6x^5 + 6x^7 \quad \text{with} \quad A_1^{-1} = 9e - 6x + 6x^3 - 8x^4 + 6x^5 - 6x^7.
\]

Further, consider another unit

\[
 v = 50e + 35x - 35x^3 - 49x^4 - 35x^5 + 35x^7 \quad \text{with} \quad v^{-1} = 50e - 35x + 35x^3 - 49x^4 + 35x^5 - 35x^7
\]

of \(RG\) and secret positive integer \(n_2 = 2\). Public key is \((A_1, A_2, v)\) where

\[
 A_2 = v^2 = 9801e + 6930x - 6930x^3 - 9800x^4 - 6930x^5 + 6930x^7
\]

and private key is \((A_1^{-1}, 2)\). Using public key the obtained ciphertext with ephemeral key \(k = 1\) is \((C_1, C_2)\) where \(C_1 = v\) and

\[
 C_2 = (r \cdot A_1) \cdot v^2 = -4708320e - 2021231x + 1849862x^2 + 4637345x^3 + 4708320x^4
\]

\[
 + 2021232x^5 - 1849872x^6 - 4637332x^7.
\]

After obtaining the ciphertext \((C_1, C_2)\), Alice computes \((C_2 \cdot v^{-2}) \cdot u^{-1}\) using her private key to obtain the message.

We end this section by giving an example in which we set a public key which is multiplication of Bass cyclic unit and Bicyclic unit of integral group ring. This public key or unit has an advantage that it is not of the known type and therefore it becomes computationally infeasible to obtain the inverse of such a unit.
3.6. ElGamal type GRPKC for $R = \mathbb{Z}$ and $G = S_5$. Let $RG$ be the integral group ring with $G = S_5$, i.e. symmetric group of degree 5. We denote $G = \{g_i, 0 \leq i \leq 119\}$ (for any order of our choice) and consider the message blocks of length 120 for encryption. Now before the setting of public key, we recall the definitions of Bass cyclic and Bicyclic units.

**Definition 3.1.** Bass cyclic unit: Let $g$ be an element of a group $G$ having order $n$. Choose an integer $i$ coprime to $n$ such that $1 < i < n - 1$. Then the element

$$u = (1 + g + g^2 + \cdots + g^{i-1}) \phi(n) + \frac{1 - g^{\phi(n)}}{n} \hat{g}$$

is a unit of integral group ring $RG$. Here $\phi(n)$ denotes the Euler’s totient function and $\hat{g} = 1 + g + g^2 + \cdots + g^{n-1}$.

**Definition 3.2.** Bicyclic unit: Let $g, h$ be two elements of a group $G$ such that $|g| = n$. Then the element

$$u = 1 + (g - 1)h\hat{g}$$

is a bicyclic unit of integral group ring $RG$ corresponding to $g$ and $h$ where $\hat{g}$ has the same meaning as in Definition 3.1.

For additional reading on these units see [10]. Let $g = (1 \ 4 \ 2 \ 5 \ 3)$ be an element of $S_5$ having order 5 and $i = 3$. Then the Bass cyclic unit $x$ corresponding to $g$ and $i$ is

$$x = 1 \ast (1) - 2 \ast (1 \ 2 \ 3 \ 4 \ 5) + 3 \ast (1 \ 3 \ 5 \ 2 \ 4) - 2 \ast (1 \ 4 \ 2 \ 5 \ 3) + 1 \ast (1 \ 5 \ 4 \ 3 \ 2).$$

Further, consider elements $(1 \ 2 \ 3 \ 4 \ 5)$ and $(1 \ 2)$ of $S_5$ and use these to obtain the corresponding bicyclic unit

$$y = 1 \ast (1) + 1 \ast (2 \ 3 \ 4 \ 5) - 1 \ast (2 \ 5 \ 4 \ 3) - 1 \ast (1 \ 2) + 1 \ast (1 \ 2 \ 4)(3 \ 5) - 1 \ast (1 \ 3 \ 4 \ 5) + 1 \ast (1 \ 3 \ 5 \ 2 \ 4)$$

$$+ 1 \ast (1 \ 4 \ 3 \ 2) - 1 \ast (1 \ 4)(2 \ 3 \ 5) + 1 \ast (1 \ 5) - 1 \ast (1 \ 5 \ 3)(2 \ 4).$$

Let $u = x \ast y$ where

$$u = 1 \ast (1) - 5 \ast (4 \ 5) + 5 \ast (3 \ 4) - 3 \ast (2 \ 3) + 3 \ast (2 \ 3 \ 4 \ 5) - 5 \ast (1 \ 2 \ 3 \ 4) - 2 \ast (1 \ 2 \ 3 \ 4 \ 5) + 5 \ast (1 \ 2 \ 3 \ 5)$$

$$- 3 \ast (1 \ 2 \ 4 \ 5) + 3 \ast (1 \ 2 \ 4)(3 \ 5) + 5 \ast (1 \ 3 \ 2 \ 4) + 3 \ast (1 \ 3 \ 5 \ 2 \ 4) - 5 \ast (1 \ 3 \ 5 \ 2 \ 4) + 3 \ast (1 \ 3 \ 5 \ 2 \ 4)$$

$$- 3 \ast (1 \ 3 \ 4)(2 \ 5) + 3 \ast (1 \ 4 \ 3 \ 2)$$

$$- 3 \ast (1 \ 4 \ 2)(3 \ 5) - 2 \ast (1 \ 4 \ 2 \ 5 \ 3) - 5 \ast (1 \ 4 \ 3)(2 \ 5) + 5 \ast (1 \ 4)(2 \ 5 \ 3) + 1 \ast (1 \ 5 \ 4 \ 3 \ 2) - 5 \ast (1 \ 5 \ 3 \ 2) + 5 \ast (1 \ 5 \ 4 \ 3 \ 2) - 3 \ast (1 \ 5 \ 4 \ 3) + 3 \ast (1 \ 5)$$

with

$$u^{-1} = -2 \ast (1) - 1 \ast (2 \ 3 \ 4 \ 5) + 1 \ast (2 \ 5 \ 4 \ 3) + 1 \ast (1 \ 2) - 2 \ast (1 \ 2 \ 3 \ 4 \ 5) - 1 \ast (1 \ 2 \ 4)(3 \ 5) + 1 \ast (1 \ 3 \ 4 \ 5) - 1 \ast (1 \ 3 \ 5 \ 2 \ 4)$$

$$+ 1 \ast (1 \ 3 \ 5 \ 2 \ 4) - 1 \ast (1 \ 4 \ 3 \ 2) + 1 \ast (1 \ 4)(2 \ 3 \ 5) + 3 \ast (1 \ 4 \ 2 \ 5 \ 3) + 1 \ast (1 \ 5 \ 4 \ 3 \ 2) - 1 \ast (1 \ 5) + 1 \ast (1 \ 5 \ 3 \ 2 \ 4).$$

Choose another unit

$$v = -15 \ast e + 6 \ast (1 \ 2 \ 3 \ 4 \ 5) + 6 \ast (1 \ 3 \ 5 \ 2 \ 4) - 15 \ast (1 \ 4 \ 2 \ 5 \ 3) + 19 \ast (1 \ 5 \ 4 \ 3 \ 2)$$
with
\[ v^{-1} = 6 \cdot e + 19 \cdot (1 \ 2 \ 3 \ 4 \ 5) + 6 \cdot (1 \ 3 \ 5 \ 2 \ 4) - 15 \cdot (1 \ 4 \ 2 \ 5 \ 3) - 15 \cdot (1 \ 5 \ 4 \ 3 \ 2). \]

Let the message to be encrypted is
\[ r = -1 \cdot (2 \ 3 \ 4 \ 5) + 2 \cdot (1 \ 2 \ 4)(3 \ 5) - 3 \cdot (1 \ 3)(2 \ 5 \ 4) + 4 \cdot (1 \ 4 \ 3 \ 2) - 5 \cdot (1 \ 5). \]

Take \( n_1 = 1 \) and \( n_2 = 3 \) which means public key is \( (A_1 = u, A_2 = v^3, v) \) where
\[ v^3 = 12816 \cdot e - 33552 \cdot (1 \ 2 \ 3 \ 4 \ 5) + 41473 \cdot (1 \ 3 \ 5 \ 2 \ 4) - 33552 \cdot (1 \ 4 \ 2 \ 5 \ 3) + 12816 \cdot (1 \ 5 \ 4 \ 3 \ 2). \]

Corresponding private key is \( (A_{-1}^1, 3) \). Using public key the obtained ciphertext with ephemeral key \( k = 2 \) is \( (C_1, C_2) \) where
\[ C_1 = 273 \cdot e + 273 \cdot (1 \ 2 \ 3 \ 4 \ 5) - 714 \cdot (1 \ 3 \ 5 \ 2 \ 4) + 883 \cdot (1 \ 4 \ 2 \ 5 \ 3) - 714 \cdot (1 \ 5 \ 4 \ 3 \ 2) \]
and
\[ C_2 = (r \cdot A_1) \cdot (v^3)^2 = -56 \cdot (1) + 40 \cdot (3 \ 4 \ 5) - 228001425142 \cdot (2 \ 3 \ 4 \ 5) - 26 \cdot (2 \ 3 \ 5) - 9 \cdot (2 \ 4 \ 5) + 51 \cdot (24)(3 \ 5) - 56 \cdot (1 \ 2 \ 3 \ 4 \ 5) + 40 \cdot (1 \ 2 \ 3 \ 5 \ 4) - 26 \cdot (1 \ 2 \ 4 \ 5 \ 3) + 51 \cdot (1 \ 2 \ 5 \ 3 \ 4) - 9 \cdot (1 \ 2 \ 5 \ 4 \ 3) + 51 \cdot (1 \ 3 \ 2 \ 5 \ 4) - 26 \cdot (1 \ 4 \ 2) - 286125243291 \cdot (1 \ 4 \ 3 \ 2) - 9 \cdot (1 \ 4 \ 3) + 51 \cdot (1 \ 4 \ 5 \ 3) - 56 \cdot (1 \ 4 \ 2 \ 5 \ 3) + 40 \cdot (1 \ 4 \ 3 \ 2 \ 5) - 56 \cdot (1 \ 5 \ 4 \ 3 \ 2) + 40 \cdot (1 \ 5 \ 2) + 317747755613 \cdot (1 \ 5) - 26 \cdot (1 \ 5)(3 \ 4) - 9 \cdot (1 \ 5)(2 \ 3) + 51 \cdot (1 \ 5 \ 2 \ 3 \ 4). \]

After obtaining the ciphertext \( (C_1, C_2) \), Alice can easily obtain the message.

4. Units of Group Rings using GAP

Both the encryption schemes of proposed cryptosystems involve units of group rings and therefore in this section we discuss about the units of group rings. There are only few recipes for the construction of units but still a vast literature is available on units of group rings. Using LAGUNA package of GAP [3], group \( V(RG) \) of normalized units of group algebra \( RG \) with \( R = F_p \) for some prime \( p > 0 \) and a finite \( p \)-group can be computed efficiently for smaller sizes of \( RG \). Further, as the unit group \( U(RG) \) of \( RG \) is \( F_p^* \times V(RG) \) which means we can efficiently compute the complete unit group. But with the increase in size of \( |G| \), GAP is very inefficient, for instance, the computation of number of elements and generators of normalized unit group of \( V(F_5 G) \) where \( G \) is a cyclic group of order 5 takes 38 minutes (approx) and program may crash for groups of size greater than 5000. Despite of this drawback, GAP still covers a large class of unit groups. For finite groups other than \( p \)-groups, units can be obtained using the Wedderga package of GAP [8] with the additional restrictions that \( R \) is semisimple and \( |G| \) is invertible in \( R \). Basically Wedderga package is not for the calculation of units directly. Its main purpose is to find the Wedderburn decomposition [10] of a group algebra. From this wedderburn decomposition, we can easily obtain the structure of unit groups. Without the use of LAGUNA and Wedderga we can also generate the units of integral group rings as well as any modular group ring using GAP.
5. Conclusion

From security point of view, we already discussed that both the proposed cryprosystems have greater security than that of existing cryptosystems. In the coming era of Quantum computers, this enhanced security would play a great role because no such quantum algorithm is known to solve DLP in group rings. Novelty of this work is the involvement of group rings and their units in the field of public key cryptography. As mentioned there is a huge literature available on the structure of unit group of group rings but very few articles are there in which unit group is computed explicitly in terms of elements of group ring. Since the latter is more important for frequent use of group rings in cryptography, much more efforts are required for the explicit representation of the unit group in terms of the elements of group ring.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, Math. Res. Lett., 6, (1999), 287-291.
[2] D. Garber, Braid group cryptography, https://arxiv.org/abs/0711.3941.
[3] V. Bovdi, A. Konovalov, R. Rossmanith, C. Schneider, LAGUNA - Lie algebras and units of group Algebras, https://gap-packages.github.io/laguna/, Version 3.8.0 (2017).
[4] L. Shpilrain, G. Zapata, Combinatorial group theory and public key cryptography, Appl. Algebra Engrg. Comm. Comput., 17(3-4), (2006), 291-302.
[5] B. Hurley, T. Hurley, Group ring cryptography, Int. J. Pure Appl. Math., 69(1), (2011), 67-86.
[6] N. Koblitz, Introduction to elliptic curves and modular forms, Springer, (1993).
[7] N. Koblitz, A course in number theory and cryptography, Springer, (1994).
[8] G. K. Bakshi, O. B. Cristo, A. Herman, A. Konovalov, S. Maheshwary, A. Olteanu, A. Olivieri, Á. del Río and I. V. Geldar, Wedderga - wedderburn decomposition of group algebras-a GAP package, https://gap-packages.github.io/wedderga/, Version 4.9.5 (2018).
[9] J. Hoffstein, J. Pipher, J. H. Silverman, An introduction of mathematical cryptography, Springer, (2008).
[10] C. P. Milies, S. K. Schgal, An Introduction to group rings, Kluwer, (2002).
[11] W. Stallings, Cryptography and network security, Pearson, (2017).
[12] C. Shannon, Communication theory of secrecy systems, Bell systems technical journal, 4, (1949).
[13] I. F. Blake, G. Seroussi, N. P. Smart, Elliptic curves in cryptography, volume 265 of London mathematical society note series, Cambridge university press, (2000).
[14] A. Menezes, Elliptic curves public key cryptosystems, The Kluwer international series in engineering and computer science, 234, Kluwer academic publishers, (1993).
[15] T. Hurley, Group rings for communications, Int. J. Group Theory, 4(4), (2015), 1-23.
[16] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press., (1994).
[17] GAP, Groups, Algorithms, Programming, https://www.gap-system.org.
[18] J. Proos, C. Zalka, *Extension of Shor’s to ECDSA*, https://arxiv.org/pdf/quant-ph/0301141.pdf, (2003).

[19] D. J. Bernstein, J. Buchmann, E. Dahmen, *Post quantum cryptography*, Springer, (2009).