A New Multi-Party Key Exchange Protocol and Symmetric Key Encryption Scheme over Non-commutative Group Rings

Turgut Hanoymak*, Ömer Küsmüş**

*Department of Mathematics, Van Yuzuncu Yil University, Van, Turkey, hturgut@yyu.edu.tr
**Department of Mathematics, Van Yuzuncu Yil University, Van, Turkey, omerkusmus@yyu.edu.tr
Corresponding Author; e-mail: hturgut@yyu.edu.tr
ORCID ID: 0000-0002-3822-2202, 0000-0001-7397-0735
Research Paper Received: 13.02.2019 Revised: 02.03.2019 Accepted: 31.03.2019

Abstract—The importance of secure communication over an insecure channel has increased day by day in almost all applications such as commercial purposes, money transactions, military and sanitary services. Therefore, many encryption algorithms based on various types of algebraic structures have become more considerable because of the underlying mathematically hard problems such as integer factorization, discrete logarithm, conjugacy search problem in group theory, finding the inverse of a given unit in group rings. Key exchange protocols also have monumental significance for generating shared keys between parties by exchanging cryptographic keys to allow a secure communication.
In this paper, we first briefly mention about the basics of group rings, the fundamental properties of units, Diffie-Hellman type key exchange protocol then we generalize this to a multi-party type key exchange protocol using units in a given group ring and finally we propose a symmetric key encryption scheme over a non-commutative group ring which is different from the encryption scheme in [1] by illustrating a concrete example. We also give a security analysis of the proposed protocol and comparisons with [1] and [8].

Keywords—Group rings, units, encryption schemes, key exchange, symmetric key

1. Introduction

The idea of public key cryptography was emerged for the first time by W. Diffie and M. E. Hellman [10] in 1976. Naturally, this system had been arised from insufficiency related to security of symmetric encryption methods. Hence, various public key cryptosystems (PKC) have been introduced and broken by researchers. In course of time, some concepts related to PKC such as *digitial signature protocols, key exchange protocols* have been designed and discussed.

The Diffie-Hellman key exchange protocol was the first practical method for establishing a shared secret key over an insecure channel. The method allows two parties that have no prior knowledge of each other to jointly construct a shared secret key

over an insecure communication channel.

Diffie-Hellman key agreement is not limited to generate a key which is shared by only two parties. Any number of parties can associate in an agreement by performing iterative calculations of the agreement protocol and exchanging data which is not necessarily to be kept secret. These processes are defined by researchers as *multi-party key exchange protocol* (MPKEP).

Although the most familiar implementation of the protocol uses a multiplicative group of integers modulo p where p is a prime number and a primitive root modulo p, different algebraic arguments can also be used for performing the same protocol as long as we can determine a mathematically hard problem.

Due to the fact that classical discrete logarithm problem can be solved in polynomial time via cyclic groups in the recent quantum computing systems, many researchers interest in preparing new more secure key exchange protocols using algebraic methods for when quantum cryptography is realized exactly. Partala has introduced an algebraic method related to key exchange protocols in [2]. In [1], the authors described a new symmetric and asymmetric encryption method using units in integral group rings of finite cyclic groups. Stickel gave a key exchange protocol and a public-key encryption algorithm over non-abelian groups [3]. Ezhilmaran and Muthukumaran have utilized decomposition problem in near-rings for composing a novel key exchange protocol and a public-key encryption scheme. They also investigated some attacks on their scheme [4]. Daghigh et al. proposed a key-exchange protocol using isogenies of elliptic curves [5]. Ilic discussed generalized discrete logarithm problem in projective special linear group $PSL(2,p)$ where p is a prime number [6]. Inam and Ali constituted a new public-key encryption scheme like ElGamal via circulant matrices defined over group rings [8]. In [9], some attacks against this system were presented. Micheli introduced an attack which runs in polynomial time against the non-commutative protocol proposed in [13], [14].

In this paper, we use non-commutative units in group rings for composing a new MPKEP and a symmetric key encryption scheme which are more complicated and secure than given in [1].

A group ring RG can be described as an R-module defined over a ring R with the basis G. Formally, RG is the set of all finite linear sums as follows

$$RG = \{\sum_{g_i \in G} \alpha_i g_i : \alpha_i \in R\}$$

Addition and multiplication on RG are defined as

$$(\sum_{g_i \in G} \alpha_i g_i) + (\sum_{g_i \in G} \beta_i g_i) = \sum_{g_i \in G} (\alpha_i + \beta_i) g_i$$

$$(\sum_{g_i \in G} \alpha_i g_i)(\sum_{g_j \in G} \beta_j g_j) = \sum_{g_i, h_j \in G} \gamma_{ij} g_i h_j$$

respectively where $\gamma_{ij} = \sum \alpha_i \beta_j$.

The operation over RG as $R \times RG \longrightarrow RG$ with $r(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} (r\alpha_g) g$ provides an R-module. It is possible to say that RG is a vector space with the basis G if R is a field. If R is the ring of integers $\mathbb{Z}$, then $\mathbb{Z}G$ is called by *integral group ring*. For more informations about algebraic properties of RG, readers can refer to [7] and [12].

Elements of special forms such as *nilpotents, idempotents, zero divisors* and *units* in group rings have always attracted special attentions and been a rich research area. Especially, determining the group of units which is displayed by $U(RG)$ defined as the set of multiplicative invertible elements in group rings is still an open problem.

Though there are some special types of units such as *trivial units, alternating units, unipotent units,*

bicyclic units and *Bass cyclic units*, there may exist units which are not of any special forms.

Properties of Units:

We can summarize the properties of units in the following items:

- $$U(RG) := \{u = \sum_{g \in G} \alpha_g g : \exists v \in RG, uv = 1\}$$
- Determining the inverse of a given unit in a group ring is a hard problem in general.
- The whole powers of units are also units.
- Unit group can be of finite or infinite order.
- Since there is no any ordering relation between units due to the fact that units behave like polynomials, we can not discuss the *density* of them.

2. MPKEP via Units

Let $A_1, A_2, ...A_n$ be n-parties want to communicate each other

- Secret keys (s_i) are selected from units of group rings.
- Public keys (p_i) are the powers of units which are also units.
- Every party sends own secret keys by using the public keys of other parties.
- For n participants, $n-1$ messaging rounds require.

Let u be a given unit with infinite order of a certain group ring.

- $\forall i$, A_i generates secret keys s_i.
- $\forall i$, A_i calculates public keys u^{s_i}.
- A_1 sends u^{s_1} to A_2, A_2 sends u^{s_2} to A_3, A_3 sends u^{s_3} to A_1 etc...
- A_1 calculates $(u^{s_3})^{s_1}$ and sends to A_2, A_2 calculates $(u^{s_1})^{s_2}$ and sends to A_3, A_3 calculates $(u^{s_2})^{s_3}$ and sends to A_1 etc...
- A_1 calculates $((u^{s_2})^{s_3})^{s_1}$, A_2 calculates $((u^{s_3})^{s_1})^{s_2}$, A_3 calculates $((u^{s_1})^{s_2})^{s_3}$, etc...
- Finally, every party A_i has the shared secret key $v = u^{s_1 s_2 ... s_n}$.

3. Symmetric Key Encryption via Units

Let Bob want to send a message m to Alice. He applies the following steps:

Encryption:

- $c = v*m*v^{-1}$ where v is a unit obtained above and (v, v^{-1}) is the secret shared key pair. Here $*$ is a non commutative operation; otherwise, we get $c = m$ meaninglessly. Notice that v^{-1} can be obtained from u^{-1} using the same protocol.

Decryption:

- $v^{-1} * c * v = v^{-1} * [v * m * v^{-1}] * v = m$

Remark A If the encryption procedure is $c = m * v$ as constructed in [1], then c is decrypted by multiplying the inverse of v as $m = c * v^{-1}$. However, in case of encrypting 1 as a message m, the secret key v is revealed which causes to the insecurity of the scheme. Because of this, we use both v and v^{-1} such that someone obtains $c = 1$ instead of the secret key v when $m = 1$. This is clearly not an advantage to the attacker. By this reason, we modify this system to $c = v*m*v^{-1}$. Reaching to v (or v^{-1}) in the current system is harder than in [1] because of both the complex structure of the algorithm and non-commutative polynomial multiplications as a most crucial point of the encryption scheme.

A Concrete Example

Let $S_3 = \langle a, b : a^3 = b^2 = 1, bab^{-1} = a^{-1} \rangle$ be the symmetric group of order 6.

- We know from [11] that $U(\mathbb{Z}S_3) = V \rtimes S_3$ where

$$V = \langle u_{b,a}, u_{ba,a}, u_{ba^2,a} \rangle$$

as non-commutative free group which is generated by bicyclic units in $\mathbb{Z}S_3$. Bicyclic units are infinite order [7]. Hence, we can generate infinitely many keys by taking any powers of generators in V.

- Alice and Bob can use the free group V to communicate securely as follows:
- Bob chooses a secret key as $v = u_{b,a}^{\alpha_1} u_{ba,a}^{\alpha_2} u_{ba^2,a}^{\alpha_3}$ where α_1, α_2 and α_3 are randomly chosen for making the secret key more complicated and obtains the inverse as $v^{-1} = u_{ba^2,a}^{-\alpha_3} u_{ba,a}^{-\alpha_2} u_{b,a}^{-\alpha_1}$.
- A message m of length $l(m) = n$ as

$$m = a_1 a_2 \dots a_n$$

is written as a group ring element by

$$m = x_1 + x_2 a + x_3 a^2 + x_4 b + x_5 ba + x_6 ba^2$$

(which is originally represented as the sequence $m = x_1 x_2 \dots x_6$) where each $x_i = a_{i_1} a_{i_2} \dots a_{i_k}$ are approprite block messages such that

$$l(m) = \sum_{i=1}^{6} l(x_i).$$

- Since $v \in V$ and $m \in \mathbb{Z}S_3$, Bob computes the ciphertext $c = v * m * v^{-1}$ of the form

$$c = y_1 + y_2 a + y_3 a^2 + y_4 b + y_5 ba + y_6 ba^2 \in \mathbb{Z}S_3.$$

and sends c to Alice by $c = y_1 y_2 \dots y_6$.

- Alice receives the encrypted message c and converts to the form

$$c = y_1 + y_2 a + y_3 a^2 + y_4 b + y_5 ba + y_6 ba^2$$

and thus she decrypts the ciphertext by the same protocol as $m = v^{-1} * c * v$ and get the plaintext.

Remark B

- Since the group ring $\mathbb{Z}S_3$ is a $\mathbb{Z}$-module with base $S_3 = \{1, a, a^2, b, ba, ba^2\}$. That is

$$\mathbb{Z}S_3 = \left\langle 1, a, a^2, b, ba, ba^2 \right\rangle$$

- Hence, if a message m has length ≤ 6 bits, it can be directly encrypted by assuming that some coefficients are 0.
- If not, m is converted to blocks of 6 parts.
- The security of the scheme is based on both discrete logarithm problem in units and non-commutative operations in group rings.

3.1. Computational Cost

As theoretically, since there is no deterministic method for finding the inverse of a given unit v in an integral group ring $\mathbb{Z}G$ where $G = \{g_1, g_2, ..., g_k\}$, we assume that the parties in the system know both v and v^{-1}. In our system, as we defined, both message m and the symmetric key pair (v, v^{-1}) are linear sums with k terms. Let $m = \sum_{i=1}^{k} \alpha_i g_i$, $v = \sum_{i=1}^{k} p_i g_i$ and $v^{-1} = \sum_{i=1}^{k} \beta_i g_i$ where α_i, p_i and β_i are in $\mathbb{Z}$. Since $n(x)$ denotes the number of bits in x, we can define

$$n(\alpha) = max\{n(\alpha_1), ..., n(\alpha_k)\}$$
$$n(p) = max\{n(p_1), ..., n(p_k)\}$$
$$n(\beta) = max\{n(\beta_1), ..., n(\beta_k)\}$$

Hence, if we say $n = max\{n(\alpha), n(p), n(\beta)\}$ for the worst case time complexity,

- Step 1:

$$c_1 = v * m = (\sum_{i=1}^{k} p_i g_i)(\sum_{i=1}^{k} \alpha_i g_i) = \sum_{i=1}^{k} x_i g_i$$

where $x_i = \sum_{j=1}^{k} \sum_{s=1}^{k} p_j \alpha_s$ such that

$$\forall l(x_i) \leq 2n$$

and the multiplications yield that

$$\underbrace{[O(n) \cdot O(n) + ... + O(n) \cdot O(n)]}_{k \ \ times} k$$

namely, $k^2 \cdot O(n^2) = O(n^2)$ running time.

- Step 2:

$$c = c_1 * v^{-1} = (\sum_{i=1}^{k} x_i g_i)(\sum_{i=1}^{k} \beta_i g_i) = \sum_{i=1}^{k} y_i g_i$$

where $y_i = \sum_{j=1}^{k} \sum_{s=1}^{k} x_j \beta_s$. The operations in this step take

$$\underbrace{[O(2n) \cdot O(n) + ... + O(2n) \cdot O(n)]}_{k \ \ times} k$$

that is $k^2 \cdot [O(2n) \cdot O(n)] = k^2 \cdot O(n^2) = O(n^2)$ running time. To sum up, our proposed encryption scheme runs in $O(n^2)$.

In [1], as the symmetric encryption scheme was proposed as $c = m * u$ with commutative polynomial multiplication, the worst case time complexity for that system can be said to be $O(n^2)$. However, although the time complexity of our current system is same as the system in [1], our currently proposed scheme includes non-commutative group operations and so this makes the system more secure as mentioned in the next subsection in which we will discuss some security notions. By the way, since the scheme in [8], [9] based on matrix multiplications which need $\approx O(n^3)$ number of bit operations, we can say that our proposed system is faster.

3.2. Security Analysis

One-wayness: Since determining whether an element which has especially great parameters in a group ring is a unit can be considered as a hard problem, the security of our scheme depends on this hardness assumption. This means that the scheme is one-way secure.

Ciphertext-only attack (COA): Since we can use units in which the parameters are large enough as symmetric keys and also the system is constructed via non-commutative operations in group rings, the attacker can not separate the ciphertext c as $v * m * v^{-1}$ explicitly without knowing v and v^{-1} which are infeasible to find. Thus, our scheme is secure against COA.

Known-plaintext attack (KPA): As the proposed scheme is performed based on a deterministic algorithm, every message has a unique ciphertext in this system. This makes our system vulnerable against this kind of attack. To avoid such a this kind of attack, we can add randomness to the message.

IND-CPA: As our scheme is deterministic, it does not satisfy *IND-CPA security* notion.

Malleability: The scheme is *malleable* because we can generate another ciphertext c' which depends on the ciphertext c of the message m which is unknown as follows: Let an attacker obtain the challenge ciphertext $c = v * m * v^{-1}$. He is able to generate another ciphertext

$$\begin{aligned} c' &= c * (v * m' * v^{-1}) \\ &= (v * m * v^{-1}) * (v * m' * v^{-1}) \\ &= v * m * (v^{-1} * v) * m' * v^{-1} \\ &= v * m * 1 * m' * v^{-1} \\ &= v * (m * m') * v^{-1} \end{aligned}$$

where m' is arbitrarily chosen by the attacker.

However, our scheme can be improved against chosen ciphertext attacks by padding some randomness as in RSA-OAEP [15]. For a message $m = \sum_{i=1}^{k} \alpha_i g_i$, we can add a random $r = \sum_{i=1}^{k} r_i g_i$ which has length $l(r)$ to the message m by $m||r = \sum_{i=1}^{k} (\alpha_i + r_i) g_i$. By doing this, we have a probabilistic encryption scheme by generating distinct ciphertexts for the same message m which does not give enough knowledge to find the challenge plaintext. In this case, encryption and decryption algorithms can be modified like OAEP using H and G which behave as truly random hash functions. If we denote zero element of length l_1 in a group ring as

$$0_{l_1} = \sum_{i=1}^{k} \underbrace{00...0}_{l_1 \ \ times} g_i$$

Then the proposed probabilistic scheme can be introduced as follows:

Modified Encryption:

$$\begin{aligned} c_1 &= G(r) \oplus (m||0_{l_1}) \\ c_2 &= H(c_1) \oplus r \\ c &= c_1||c_2 \end{aligned}$$

where these hash functions are defined as

$$H : \{0,1\}^{n+l_1} \longrightarrow \{0,1\}^{l(r)}$$

and

$$G : \{0,1\}^{l(r)} \longrightarrow \{0,1\}^{n+l(1)}$$

Modified Decryption:

$$\begin{aligned} c_1 &= c(0...n+l_1-1) \\ c_2 &= c(n+l_1...n') \\ r &= H(c_1) \oplus c_2 = H(c_1) \oplus [H(c_1) \oplus r] \\ c' &= G(r) \oplus c_1 = G(r) \oplus [G(r) \oplus (m||0_{l_1})] \\ d_1 &= c'(0...n-1) \\ d_2 &= c'(n...n+l_1-1) \\ d_1||d_2 &= m||0_{l_1} \end{aligned}$$

We know that if $d_2 = 0_{l_1}$ then the algorithm outputs the original message m.

4. Conclusion and Future Works

In this paper, we first summarize the fundamentals of group rings and properties of units and briefly mention about Diffie-Hellman key exchange protocol. We generalize it to a multi-party type key exchange protocol using units in a given group ring and propose a symmetric key encryption scheme over a non-commutative units in group rings by illustrating a concrete example. We finally discuss the security of the system. The modified system may be proven secure against chosen ciphertext attacks in the random oracle model as a future work.

Acknowledgments

The authors would like to thank to anonymous referees for their valuable suggestions and comments.

References

[1] T. Hanoymak, Ö. Küsmüş, *On Construction of Cryptographic Systems over Units of Group Rings*, Int. Elec. J. Pure Appl. Math. Vol:9, No:1, pp. 37-43, 2015.

[2] J. Partala, *Algebraic Generalization of Diffie-Hellman Key Exchange*, J. Math. Cryptol., Vol:12, No:1, 2017.

[3] E. Stickel, *A New Public Key Cryptosystem in Non-Abelian Groups*, Proc. of the Thirteenth Internat. Conf. on Information Systems Development. Vilnius Technika, Vilnius pp. 70-80, 2004.

[4] D. Ezhilmaran, V. Muthukumaran, *Key Exchange Protocol Using Decomposition Problem in Near-Ring*, Gazi University Journal of Science, 29(1), pp. 123-127, 2016.

[5] H. Daghigh, R. K. Gilan, F. S. Shahpar., *Diffie-Hellman Type Key Exchange Protocols Based on Isogenies*, Bulletin of the Iranian Mathematical Society, 43, pp.77-88, 2017.

[6] I. Ilic, *The Discrete Logarithm Problem in Non-Abelian Groups*, Dissertation, Florida Atlantic University, 2010.

[7] C. P. Milies, S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[8] S. Inam, R. Ali, *A New ElGamal-like Cryptosystem Based on Matrices over Groupring*, Neural Computing and Applications pp. 1279-1283, Vol:29, No:11, 2018.

[9] J. Jianwei, et al., *Cryptanalysis of an ElGamal-Like Cryptosystem Based on Matrices over Group Rings*, Chinese Conference on Trusted Computing and Information Security, Springer, pp. 255-269, Singapore, 2018.

[10] W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, Vol:22, No:6, pp. 644-654, 1976.

[11] E. Jespers, M. M. Parmenter, *Bicyclic Units in $\mathbb{Z}S_3$*, Bull. Soc. Math. Belg., Vol:44, pp. 141-145, 1992.

[12] D. S. Passman, *The Algebraic Structure of Group Rings*, Dover Publications, 2011.

[13] R. Alvarez, F. Martinez, J. Vincent, and A. Zamora., *A new public key cryptosystem based on matrices*, 6th WSEAS International Conference on Information Security and Privacy, Tenerife, Spain, 2007.

[14] H.K. Pathak, M. Sanghi., *Public key cryptosystem and a key exchange protocol using tools of non-abelian groups*, (IJCSE) International Journal on Computer Science an Engeneering, pages Vol 02, No 04, 10291033, 2010.

[15] M. Bellare, P. Rogaway., *Optimal Asymmetric Encryption – How to encrypt with RSA*. Extended abstract in Advances in Cryptology - Eurocrypt '94 Proceedings, Lecture Notes in Computer Science Vol. 950, A. De Santis ed, Springer-Verlag, 1995.