International Electronic Journal of Pure and Applied Mathematics

Volume 9 No. 1 2015, 37-43
ISSN: 1314-0744
url: http://www.e.ijpam.eu
doi: http://dx.doi.org/10.12732/iejpam.v9i1.5

ON CONSTRUCTION OF CRYPTOGRAPHIC SYSTEMS OVER UNITS OF GROUP RINGS

Turgut Hanoymak[1], Ömer Küsmüş[2] §

[1,2]Department of Mathematics
Faculty of Science
Yüzüncü Yıl University
Van, TURKEY

Abstract: Encryption schemes can be derived from the units which are known as invertible elements in a group ring. Besides there are many studies on units in group rings in the literature, we can also see some studies of units in terms of applicability to cryptography and coding theory. In this work, we shall establish the relations between units and RSA problem. Our motivation is to construct a much stronger public key cryptosystem. It is clear that we must consider a mathematical hard problem to do this. Thus, we investigate some interesting properties of units which are no deterministic algorithm in general. Our notations follow [8].

AMS Subject Classification: 94A60, 11T71, 14G50, 81P68
Key Words: group rings, units, cryptography, public key

1. Introduction and Preliminaries

Cryptography is the most important argument in electronic information security and it has many uses. It is possible to see that there are many concepts such as private and public key cryptography, data encryption standarts, key exchange protocols, digital signatures and others [2], [4]. In terms of security, private key or symmetric key encryption systems are now inadequate and unsafe. In recent years, probably the most secured ones belong to public key schemes such as RSA, Diffie

Received: January 9, 2015

§Correspondence author

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

Hellman key exchange system and discrete logarithm problem [4]. All the mentioned systems, schemes and methods use some pure algebraic and number theoretical structures. For instance, there are many applications of groups related to this area [5], [6]. Especially, we can say RSA is mainly based on the structure of finite abelian groups and it works on invertible elements of $\mathbb{Z}_n$ such that $n = pq$ and p and q are very large prime numbers. However, this is a very hard work obviously. In as much as, it depends on the problem of factorization. As Hurley said, there are also many encryption methods constructed via combinatorial group theory which is a generalization of discrete logarithm problem to any groups using the difficulty of the so-called conjugacy search problem [1].

Now, let us give some basic definitions and structures in group rings and units. Let G be a group and R be a ring. The concept of group ring RG can be understood by the linear combination of elements of G over R. Namely, group ring RG is the set of all formal finite sums

$$\sum \gamma_g g$$

where $g \in G$, $\gamma_g \in R$ and only a finite number of coefficients γ_g are non-zero in this sum. This set is a ring with the operations defined in [8]. The invertible elements with respect to the multiplication in this set are said to be *unit*. As the set of units is a group under multiplication, it is mostly emphasized by *unit group* and displayed by $\mathcal{U}(RG)$. For more details, reader can take a glance at [8]. Throughout this paper, we consider a finite cyclic group which is generally shown by C_n of order n and the ring of integers $\mathbb{Z}$. Then, the group ring $\mathbb{Z}C_n$ is said to be *integral group ring*. If any unit u exists in a group ring RG, the inverse of u also exists and displayed by u^{-1} such that $u * u^{-1} = u^{-1} * u = e$ where e is the identity of RG and * denotes the multiplication.

Our technique is to consider a proper unit u and its inverse u^{-1} of $\mathbb{Z}C_n$ and to encrypt and decrypt the a message m by u and u^{-1} respectively. It is clear that there are many types of group rings and many special type of units such as trivial units, unipotent units, bicyclic units or bass cyclic units [8]. Hence, our idea on this technique can be derived. That is, we are very chanced to construct new and stronger encryption schemes when we use the arguments of this rich area. By considering different classifications of groups and rings, we can establish different group rings so different encryption algorithms. As Hurley said, the units of group rings have very interesting properties [1]. As an illustration, the product of any two units of special types may not give a unit of special type. This property can be seen as the hardness of the problem which the main logic of our algorithm depends on. Also, it is computationally hard (or impossible in cases of big orders) to obtain the units u_1 and u_2 from the product u_1u_2. In fact, this is logically similar to RSA [7]. This similarity can be stated informally by

$$\text{If } n = p.q, \text{ finding } p \text{ and } q \;\approx\; \text{If } u = u_1 * u_2, \text{ finding } u_1 \text{ and } u_2.$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

In general, we know that the arbitrary product of units is also a unit and finding the component units of this product is computationally impossible. That is for a given unit $v = u_1u_2...u_n$, to get each u_j is impossible. Then, especially, if $v = u^k$ for some positive integer k, the problem of getting u is similar to discrete logarithm problem [4]. Once again, informally, this case can be expressed as

$$\text{If } h = g^k \text{ in } G, \text{ finding } k \approx \text{If } v = u^k, \text{ finding } u$$

Due to the fact that, we can use units with existing encryption schemes to construct more stronger algorithms.In the next section, these algorithms are given with some concrete examples.

2. Algorithms

Now, we are ready to give algorithms which are based on symmetric and asymmetric key encryption via units of group rings.

2.1. Symmetric Encryption Scheme via Units

As Hurley told, if we want to encrypt a message m symmetrically, we should remember the property that if m is written as an element of the given group ring, one can not compute the components m and u from the product $m * u$ [1]. Therefore, two people who want to communicate in a secure way must know both u and u^{-1}. That is, for instance, If Turgut wants to send a message m in a secure way to Ömer, Turgut should choose a unit u and write m as an element of group ring. Afterwards, Turgut should also compute the product $m^{'} = m * u$ and send to Ömer. To decrypt the encrypted message $m^{'}$, Ömer use the inverse of the unit u and compute $m^{'} * u^{-1}$. At final, Ömer gets the original message m.

Example 1. Let us consider a message by representative $m = [2, 4, 7]$ and assume that we study on the units in integral group ring $\mathbb{Z}C_5$ since $C_5 =< a : a^5 = 1 >$ is a cyclic group of order 5. Karpilovsky showed in [3] that units of $\mathbb{Z}C_5$ is of the form $\mathcal{U}(\mathbb{Z}C_5) = \pm < a > \times < -1 + a + a^4 >$. One can see that the first part of this direct product consists of trivial units so torsion ones. Indeed, we always focus on the second part of this form consists of torsion-free units. We can generate infinitely number of non-trivial units by computing the powers of $u = -1 + a + a^4$ by some computer programming as Maple, Mathematica,...etc. For instance, we can easily get the following unit by Mathematica:

$$v = u^{10} = 6051 - 4895a + 1870a^2 + 1870a^3 - 4895a^4$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

and also convert the message $m = [2, 4, 7]$ to an element of $\mathbb{Z}C_5$ as $m = 2+4a+7a^2$. Then, we obtain the encrypted message $m * v$ as

$$\begin{aligned} \widetilde{m} &= (2 + 4a + 7a^2)(6051 - 4895a + 1870a^2 + 1870a^3 - 4895a^4) \\ &= 5612 - 19851a + 26517a^2 - 23045a^3 + 10780a^4 \end{aligned}$$

Thus, we can this encrypted message as:

$$\widetilde{m} = [5612, -19851, 26517, -23045, 10780]$$

Now, if the person who received the $\widetilde{m}$ knows the inverse of the unit $v = u^{10}$ as

$$v^{-1} = 6051 + 1870a - 4895a^2 - 4895a^3 + 1870a^4$$

that can decrypt the message $\widetilde{m}$ by

$$\begin{aligned} m &= \widetilde{m} * v^{-1} \\ &= \widetilde{m} * (6051 + 1870a - 4895a^2 - 4895a^3 + 1870a^4) \\ &= 2 + 4a + 7a^2 \end{aligned}$$

Hence, the original message is obtained as $m = [2, 4, 7]$.

2.2. Asymmetric Encryption Scheme via Units

In this subsection, we give an asymmetric key encryption scheme using partly RSA. One can notice that in RSA, while arguments are based on the ring $\mathbb{Z}_n$ for any positive integer n, our method is not based directly on the structure of $\mathbb{Z}_n$. This will easily be understood after we give the scheme.

Encryption. Let Bob want to send a message m to Alice

- Alice chooses two distinct prime numbers p, q and computes $n = pq$
- also computes $\varphi(n)$ and chooses e such that $\gcd(e, \varphi(n))$=1
- keeps secret d such that $ed \equiv 1 mod \varphi(n)$
- Bob represents m like an element of group ring
- Bob randomly chooses a unit u, finds u^{-1} and computes $c_1 = m^e * u$
- finally sends the ciphertext $c = (c_1, c_2)$ to Alice where $c_2 = v^e, v = u^{-1}$

Decryption:

- Alice takes c_2 and computes the d^{th} power of c_2 to get the inverse of the unit u

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

- at the end, Alice calculates $(c_1 * u^{-1})^d mod n$ to obtain the original message m

Now, let us illustrate this scheme using the units of the integral group ring of a cyclic group of order 5 again.

Example 2. As we mentioned early, Karpilovsky gave in [3] the structure of unit group of this integral group ring as:

$$\mathcal{U}(\mathbb{Z}C_5) = \pm C_5 \times < -1 + a + a^4 >$$

We can generate any power of the unit $-1+a+a^4$ using Mathematica. For instance,

$$u = -49 + 40a - 15a^2 - 15a^3 + 40a^4$$

is a unit in $\mathbb{Z}C_5$. The inverse of u can easily be obtained as:

$$v = -49 - 15a + 40a^2 + 40a^3 - 15a^4$$

Encryption.

- Let the message $m = 287$, $p = 17$ and $q = 23$.
- Then $n = 391$, $\varphi(391) = 352$.
- Also let e chosen as $e = 15$
  (In this case, $d = 47$).
- Let u and $u^{-1} = v$ be just as above.

$$\begin{aligned} c_1 &= m^e * u \\ &= 263 * (-49 + 40a - 15a^2 - 15a^3 + 40a^4) \\ &= (2 + 6a + 3a^2) * (-49 + 40a - 15a^2 - 15a^3 + 40a^4) \\ &= 97 - 94a + 63a^2 - 55a^4 \end{aligned}$$

and the second component

$$\begin{aligned} c_2 &= v^e \\ &= (-49 - 15a + 40a^2 + 40a^3 - 15a^4)^{15} \\ &= 264 + 94a + 360a^2 + 360a^3 + 94a^4 \end{aligned}$$

Here, notice that this calculation is made by taking modulo n of the 15^{th} powers of the coefficients one by one (not of the unit directly).

$$\begin{aligned} c &= (c_1, c_2) \\ &= (97 - 94a + 63a^2 - 55a^4, 264 + 94a + 360a^2 + 360a^3 + 94a^4) \end{aligned}$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

Decryption:

- Take $c_2 = 264 + 94a + 360a^2 + 360a^3 + 94a^4$.
- Compute the modulo n of the d^{th} powers of each coefficients of c_2 and denote by c_2^d.
- This straightforward calculation gives $v = u^{-1}$.
- Multiply c_1 by v and get $2 + 6a + 3a^2$.
- Represent the last expression as 263 and calculate $263^d \equiv mod n$.
- The message m is obtained as $263^{47} \equiv 287 mod 391$.

We should note that in this paper, one of the crucial points is that we work in integral group ring $\mathbb{Z}G$ of a finite abelian group G. That is, we consider $\mathbb{Z}_n$ as neither group nor a ring. It should be remembered that we wish to combine our method by the logic of RSA. Thus, we can not take modulo n of e^{th} (or d^{th}) directly power of a unit in a group ring as Euler theorem is invalid for elements of group rings. That is, formally if we consider the numbers e and d such that $ed \equiv 1 mod \varphi(n)$, we can say nothing related to

$$(\sum_{g \in G} \gamma_g g)^{ed} mod(n)$$

3. Conclusion

We gave some informations about the structure of group rings and units which are known as invertible elements in group rings. We considered a fix group ring and a fix parameterized unit for encryption-decryption. Our main aim was to construct a new public key encryption scheme combining units with RSA. As Hurley mentioned in [1], there are some advantages and disadvantages about encryption-decryption while we study by group rings. We write some of them as follows:

Advantages. It is obvious from our examples that we mainly consider a key pair instead of a single key as in the other encryption schemes. This provide a stronger encryption scheme compared to RSA. Here, it will be beneficial to say once again that the complicated parametric structure of units provide indeterministic peculiarities. In consequent, this technique is more secured than the others.

Disadvantages. Although combining two useful technique is seen as better in terms of security, processing the steps of encryption-decryption may take a long time. This case is pessimist in view of efficiency of the method.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 1 (2015)

4. Future Works

If recent researches which are concerning with the area are considered, it is easy to see that the mostly used techniques in cryptography are based on some remarkable mathematical hard problems such as factorization, discrete logarithm problem, conjugacy search problem,...etc [1]. As we mentioned in this note, finding units and their inverses in a group ring can be seen as one of such problems may be named by *Unit Problem in Application* in the future. These properties make the units very useful in this rich area. For instance, getting the unit u from u^k is not an easy problem while the positive integer k is secret. Using this specialty, researchers may deal with key exchange protocols, data encryption standarts and others over units of group rings. Of course, all these methods and algorithms should be tested by cryptanalysis. On the other hand, the authors think that units also have strength properties just as prime numbers.

References

[1] B. Hurley, T. Hurley, Group Ring Cryptography, *Int. J. Pure and Appl. Math.*, **69**, 2011, 67-86.

[2] J. Buchmann, *Introduction to Cryptography*, Springer-Verlag, New York (2001).

[3] G. Karpilovsky, *Commutative Group Algebras*, Marcel Dekker Inc., New York (1993).

[4] I. Anshel, M. Anshel, D. Goldfeld, An Algebraic Method for Public-Key Cryptography, *Math. Res. Lett.*, **6**, (1999), 287-291.

[5] P. Dehornoy, Braid-based Cryptography, *Contemp. Math.*, **360**, (2004), 5-33.

[6] V. Shpilrain, G. Zapata, Combinatorial Group Theory and Public Key Cryptography, *Appl. Algebra Engrg. Comm. Comput.*, **17**, (2006), 291-302.

[7] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York (1994).

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