ElGamal Public-Key Cryptosystem Using Reducible Polynomials Over a Finite Field

A. N. El-Kassar
Beirut Arab University, Mathematics Department, Beirut, Lebanon

Ramzi A. Haraty
Lebanese American University P.O.Box 13-5053 Chouran, Beirut, Lebanon 1102 2801

April 29, 2004

Abstract

The classical ElGamal encryption scheme is described in the setting of the multiplicative group Z_p^*; the group of units of the ring of integers modulo a prime p, but it can be easily generalized to work in any finite cyclic group G. Among the groups of most interest in cryptography are the multiplicative groups F_q^* of the finite field F_q: These require finding irreducible polynomials $h(x)$ over Z_p; for some prime p; and constructing the quotient group $Z_p[x]/ < h(x) > = F_q$: Recently, El-Kassar et al. modified the ElGamal public-key encryption scheme from the domain of natural integers, Z, to the domain of Gaussian integers, Z[i] by extending the arithmetic needed for the modifications in this domains.

The ElGamal public-key cryptosystem is extended to quotient rings of polynomials over finite fields having cyclic group of units. The major finding is that the quotient rings need not be fields. In particular, when p is an odd prime, a second degree reducible polynomial over Z_p is used to easily implement the extended ElGamal public-key cryptosystems and to avoid finding irreducible polynomials.

1 Introduction

The ElGamal encryption scheme is typically described in the setting of the multiplicative group Z_p^*; the group of units of the ring of integers modulo a prime p, but it can be easily generalized to work in any finite cyclic group G. The security of the generalized ElGamal encryption scheme is based on the intractability of the discrete logarithm problem in the group G. The group G should be carefully chosen so that the group operations in G would be relatively easy to apply for efficiency. In addition, the discrete logarithm problem in G should be computationally infeasible for the security of the protocol that uses the ElGamal public key cryptosystem. The groups of most interest in cryptography are the multiplicative groups F_q^* of the finite field F_q, including the particular cases of the multiplicative groups Z_p^*, and the multiplicative group $F_{2^m}^*$ of the finite field F_{2^m} of characteristic two, see [6]. Also of interest is the group of units Z_n^* where n is a composite integer such that n is 2, 4, p^t, or $2p^t$, where p is an odd prime and t is an integer.

The classification of all Gaussian integers modulo β with a cyclic group of units was given by J. T. Cross [1]. So, one may consider the cyclic group of units of the quotient ring of Gaussian integers $Z[i]/ < \beta >$ where $\beta = 1 + i; (1 + i)^2; (1 + i)^3; p; (1 + i)p; \pi^n; (1 + i)\pi^n$; p is a prime integer of the form $4k + 3$ and π is a Gaussian prime with $\pi\bar{\pi}$ is an integer of the form $4k + 1$: Recently, El-Kassar et al. [3] described the computational procedures using arithmetic modulo Gaussian integers required for the extension of El-

Gamal encryption scheme to the domain of Gaussian integers.

In [7], J. L. Smith and J. A. Gallian, determined the structure of the group of units of the quotient ring $F_q[x]/<f(x)>$ where $f(x)$ is a polynomial in $F_q[x]$. Using this decomposition, El-Kassar et al. [4], gave a characterization of quotient rings of polynomials over finite fields with a cyclic group of units. The purpose of this paper is to use this classification to apply ElGamal encryption scheme to the setting of $F_q[x]/<f(x)>$ where $f(x)$ is a reducible polynomial in $F_q[x]$.

The rest of the paper is organized as follows: section 2 describes the classical ElGamal scheme. Section 3 presents the extension of ElGamal cryptosystem to the domain of Guassian integers. Section 4 presents the classification of quotient rings of polynomials $F_q[x]/<f(x)>$ having cyclic group of units. Section 5 describes the extension of ElGamal cryptosystem to the domain of polynomial rings over a finite field with cyclic group of units and section 6 presents a conclusion.

2 The Classical ElGamal Public Key Encryption Scheme

The classical ElGamal cryptosystem, see [2] and [6], can be described as follows. Let p be a large odd prime integer and let $Z_p = \{0, 1, 2, 3, \ldots, p-1\}$. Then, Z_p is a ring under addition and multiplication modulo p. Since p is prime, Z_p is actually a field under these operations. Moreover, $Z_p^* = \{1, 2, 3, \ldots, p-1\}$, the multiplicative group of the ring integers modulo p, is a cyclic group generated by some generator $\alpha \neq 1$ whose order is equal to $p-1$. That is, every element of Z_p^* is a power of α. Note that Z_p is a complete residue system modulo p and Z_p^* is a reduced residue system modulo p. For further algebraic properties, see [5] and [6].

Suppose that entity B wants to send a message m to entity A. Entity B proceeds as follows: B gets the public key generated by A, then computes the ciphered message $c = E_A(m)$ and sends it to A for decryption. To decipher it, A computes $D_A(c) = m$.

Entity A generates the public-key by first generating a large random prime p and a generator α of Z_p^*. Then A chooses randomly an integer a, $1 \leq a \leq p-2$, and computes $\alpha^a (\bmod p)$. The public key is $(p; \alpha; \alpha^a)$ and A's private key is a.

To encrypt the message m chosen from Z_p, entity B first obtains A's public-key $(p; \alpha; \alpha^a)$. Then B chooses a random integer k, where $2 \leq k \leq p-2$, computes $\gamma = \alpha^k \ (\bmod p)$ and $\delta \equiv m \cdot (\alpha^a)^k \ (\bmod p)$. The ciphertext is $c = (\gamma; \delta)$.

To decrypt the message c sent by B, A uses the private key and recovers the message m by computing $\gamma^{-a} . \delta \ (\bmod p)$.

Example 1 In order to generate the public key, entity A selects the prime $p = 359$ and a generator $\alpha = 124$ of Z_{359}^*. A chooses the private key $a = 292$ and computes $\alpha^a = 124^{292} \equiv 205 \ (\bmod 359)$. Therefore, A's public-key is $(p = 359; \alpha = 124; \alpha^a = 205)$ and A's private key is $a = 292$. To encrypt the message $m = 101$, B selects a random integer $k = 247$ and computes $\gamma = 291 \equiv 124^{247} (\bmod 359)$ and $\delta = 288 \equiv 101 . 205^{247} (\bmod 359)$. Then B sends $\gamma = 291$ and $\delta = 288$ to A. We note that B has 359 choices for m in Z_{359}. Finally, A computes $\gamma^{p-1-a} = 291^{66} \equiv 216 (\bmod 359)$ and recovers m by computing $216 \cdot 288 \equiv 101 \ (\bmod 359)$.

3 ElGamal Public Key Cryptosystem In the Domain of Gaussian Integers

In [3], the ElGamal public key encryption scheme was extended to the domain of Gaussian integers $Z[i] = \{a + bi | a, b \in Z\}$. Algorithms and examples illustrating these modifications were given. The arithmetics in the domain of Gaussian integers were applied to extend the ElGamal cryptosystem as follows. Let β be a Gaussian prime integer and let G_β be a set of representatives of the elements of the quotient ring $Z[i]/ < \beta >$. Then, G_β is a field under addition and multiplication modulo β having a cyclic multiplicative group G_β^*. Note that G_β is a complete residue system modulo β and G_β^* is a reduced residue system modulo β. If $\beta = \pi$, where

$q = \pi\bar{\pi}$ is a prime integer of the form $4k+1$, then $G_\pi = \{a : 0 \le a \le q-1\} = Z_q$; see [1]. This choice will be excluded since the calculations in this case are identical to those of the classical one. Hence, β is chosen to be a large prime integer p of the form $4k+3$ so that $G_\beta = \{a + bi : 0 \le a \le p-1, 0 \le b \le p-1\}$, where the number of elements in G_β is p^2 and in G_β^* is $\phi(\beta) = p^2 - 1$. Hence, the cyclic group used in the extended ElGamal cryptosystem has an order larger than the square of that used in the classical ElGamal cryptosystem with no additional efforts required for finding the prime p. Now, a generator α of G_β^* is selected and note that there are $\phi(p^2 - 1)$ generators in G_β^*. Then a random positive integer a is chosen so that the public-key is (p, α, α^a). Since a is a power of α, then a must be less than the order of the group power G_β^* which is $p^2 - 1$. This power of a is the private key.

To encrypt a message m, we first represent it as an element m in G_β. Then, a random positive integer k is selected to be used as a power so that k is less than $p^2 - 1$. The encrypted message is $c = (\gamma, \delta)$ where $\gamma = \alpha^k$ and $\delta = m.(\alpha^a)^k$. Note that the values of γ and δ must be elements of G_β and hence must be reduced modulo β. The message c is decrypted using the private key a to compute $\gamma^{-a}.\delta$.

Example 2 In order to generate the public-key, entity A selects the Gaussian prime $\beta = 359$ and a generator $\alpha = 1 + 11i$ of G_{359}^*. A chooses the private key $a = 86427$ and computes α^a modulo β, which is $\alpha^a = (1 + 11i)^{86427} \equiv 323 + 295i$ modulo 359. Therefore, A's public-key is $(p = 359, \alpha = 1 + 11i, \alpha^a = 323 + 295i)$ and A's private key is $a = 86427$. To encrypt the message $m = 101$, B selects a random integer $k = 115741$ and computes $\gamma = (1 + 11i)^{115741} \equiv 149 + 117i$ modulo 359 and $\delta = 101 \cdot (323 + 295i)^{115741} \equiv 147 + 209i$ modulo 359. Then B sends $\gamma = 149 + 117i$ and $\delta = 147 + 209i$ to A. We note that B has 128880 choices for m in G_{359}. Finally, A computes

$\gamma^{\beta^2 - 1 - a} = (149 + 117i)^{42453} \equiv 117 + 178i \pmod{359}$, and recovers m by computing $(117 + 178i) \cdot (147 + 209i) \equiv 101$ modulo 359.

4 Polynomial Rings Over a Field With Cyclic Group Of Units

The generalized ElGamal public key cryptosystem is usually studied in the setting of a finite field F_q and is based on working with the quotient ring $Z_p[x]/\langle h(x)\rangle$, where $h(x)$ is an irreducible polynomial over $Z_p[x]$, $q = p^n$, and p is a prime integer. In the following, we extend the ElGamal public key cryptosystem to the setting of quotient rings of polynomials over a field, $F_q[x]/\langle h(x)\rangle$, having a cyclic group of units where $h(x)$ is not necessarily irreducible. It is well known that if $h(x)$ is an irreducible polynomial of degree n, then $Z_p[x]/\langle h(x)\rangle = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_0, a_1, \dots, a_{n-1} \in Z_p\}$ is a field whose elements are the congruence classes modulo $h(x)$ of polynomials in $Z_p[x]$ with a degree less than that of $h(x)$. Note that the representatives of the elements of $Z_p[x]/\langle h(x)\rangle$ form a complete residue system modulo $h(x)$ in $Z_p[x]$. Moreover, $Z_p[x]/\langle h(x)\rangle$ is a finite field of order p^n and its nonzero elements form its cyclic group of units, $U(Z_p[x]/\langle h(x)\rangle)$, of order $\phi(h(x)) = p^n - 1$.

Now consider the factor ring $F_q[x]/ < f(x) >$, where F_q is a finite field of order q and $f(x)$ is a polynomial of degree n. Then $F_q[x]/ < f(x) > = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_0, a_1, \dots, a_{n-1} \in F_q\}$ is a ring whose elements are the congruence classes modulo $f(x)$ of polynomials in $F_q[x]$ with a degree less than that of $f(x)$. For each irreducible polynomial $h(x)$ of degree n over a finite field F_q, the factor ring $F_q[x]/ < h(x) >$ is a finite field of order q^n. Its group of units is isomorphic to the cyclic group $Z_{q^n - 1}$. In the case where $f(x)$ is not irreducible over F_q; the quotient ring $F_q[x]/\langle f(x)\rangle$ is not a field. However, $f(x)$ can be selected so that the group of units of the quotient ring $F_q[x]/\langle f(x)\rangle$ is cyclic. This can be done by using the structure of the group of units of $F_q[x]/\langle f(x)\rangle$ was given by Smith and Gallian [7]. Before we summarize their results we recall the following well-known results. For a finite commutative ring R with identity, we know from the fundamental theorem of finite abelian groups that $U(R)$ is isomorphic to a direct product of cyclic groups. Also, if R

is a direct sum of rings then its group of units is isomorphic to the direct product of the corresponding group of units of each of the summands.

Theorem 3 If $R = R_1 \oplus R_2 \oplus \cdots \oplus R_i$ then $U(R) \cong U(R_1) \times U(R_2) \times \cdots \times U(R_i)$.

Since $F_q[x]$ is a unique factorization domain, then $f(x)$ can be written as a product of powers of irreducible polynomials, $h_1(x)^{m_1}, h_2(x)^{m_2}, \ldots, h_k(x)^{m_k}$, in $F_q[x]$ and $F_q[x]/<f(x)> \cong F_q[x]/<h_1(x)^{m_1}> \oplus \cdots \oplus F_q[x]/<h_k(x)^{m_k}>$. In the case where $f(x)$ is not irreducible over F_q, theorem 1 can be applied and the problem reduces to that of finding the structure of $U(F_q[x]/<h(x)^m>)$, where $h(x)$ is irreducible over F_q. This result is stated as follows.

Lemma 4 If $f(x) = h_1(x)^{m_1} h_2(x)^{m_2} \cdots h_k(x)^{m_k}$, where all $h_i(x)$ are distinct irreducible polynomials in $F_q[x]$, then $U(F_q[x]/<f(x)>) \cong U(F_q[x]/<h_1(x)^{m_1}>) \times \cdots \times U(F_q[x]/<h_k(x)^{m_k}>)$.

The following theorems simplify the problem further.

Theorem 5 Let F_q be a finite field and let $h(x)$ be an irreducible polynomial in $F_q[x]$. If a is a root of $h(x)$ and $K = F_q(a)$, the extension of F_q by a, then $F_q[x]/<h(x)^m> \cong K[x]/<x^m>$.

Theorem 6 Let K be a finite field with p^n elements, where p is prime. Then, for any positive integer m, we have $U(K[x]/<x^m>) \cong Z_{p^n-1} \times \prod_{i=1}^{s} n(k_{i-1} - 2k_i + k_{i+1}) \cdot Z_{p^i}$ where $s = \min\{h \in Z \mid p^h \geq m\}$, $k_i = \max\{h \in Z \mid hp^i < m\}$ and $t \cdot Z_{p^i}$ means Z_{p^i} occurs in the product t times.

Note that the above lemma and theorems can be combined together to classify the group of units of any quotient ring of the form $F_q[x]/<f(x)>$.

Now we turn to the problem of classifying all quotient rings of polynomials $F_q[x]/<f(x)>$ with cyclic group of units. The results obtained in the remainder of this section are due to El-Kassar and Chehade, see [?]. If $h(x)$ is an irreducible polynomial over F_q of degree n, we have that $F_q[x]/<h(x)>$ is a field of order $q^n = p^{nd}$. Hence, $U(F_q[x]/<h(x)>)$ is cyclic with order $q^n - 1 = p^{nd} - 1$ and $U(F_q[x]/<h(x)>) \cong Z_{p^{nd}-1}$. Next we consider the case where $f(x)$ is a power of an irreducible polynomial $h(x)$, that is $f(x) = h(x)^m$. We note that if $h(x)$ is of degree 1, then $F_q[x]/<h(x)^m> \cong F_q[x]/<x^m>$. Also note that in order for $U(F_q[x]/<x^m>) \cong Z_{p^d-1} \times \prod_{i=1}^{s} d(k_{i-1} - 2k_i + k_{i+1}) \cdot Z_{p^i}$ to be cyclic, $s = 1$ since the order of each Z_{p^i} is divisible by p. We have two different cases for $U(F_q[x]/<h(x)>)$ to be cyclic depending on the characteristic of the field.

Theorem 7 Let F_q be a finite field of order $q = p^d$, where p is a prime integer, and let $h_j(x)$ be irreducible factor of $f(x)$ in $F_q[x]$ with $\deg h_j(x) = d_j$. Then, $U(F_q[x]/<f(x)>)$ is cyclic if and only if one of the following is true:

- i- $f(x)$ is irreducible and $U(F_q[x]/<f(x)>) \cong Z_{q^d-1}$.
- ii- $f(x) = h(x)^2$ and $U(F_q[x]/<f(x)>) \cong Z_{p-1} \times Z_p$ where $h(x)$ is linear and $F_q \cong Z_p$.
- iii- $f(x) = h_1(x) \cdot h_2(x) \cdots h_r(x)$ where $q = 2$, the d_j's are pairwise relatively prime and $U(F_q[x]/<f(x)>) \cong Z_{2^{d_1}-1} \times Z_{2^{d_2}-1} \times \cdots \times Z_{2^{d_r}-1}$
- iv- $f(x) = h_1(x) \cdot h_2(x) \cdots h_r(x)^2$ where $q = 2$, the d_j's are pairwise relatively prime, $h_r(x)$ is linear and $U(F_q[x]/<f(x)>) \cong Z_{2^{d_1}-1} \times Z_{2^{d_2}-1} \times \cdots \times Z_{2^{d_r}-1} \times Z_2$

5 ElGamal Public Key Cryptosystem over Quotient Rings of Polynomials over Finite Fields

Now we describe the extended ElGamal encryption scheme over quotient rings of polynomials $Z_p[x]/\langle h(x) \rangle$ where $h(x)$ is reducible. From the study above we conclude that in order for the group of units $U(Z_p[x]/\langle h(x) \rangle)$, where p is an odd prime, to be cyclic, $h(x)$ must be a square power of only one linear irreducible polynomial. That is, $h(x) = h_1(x)^2$, where $h_1(x) = ax + b$. This means that $U(Z_p[x]/\langle(ax+b)^2\rangle)$ is cyclic. But, $Z_p[x]/\langle(ax+b)^2\rangle \cong Z_p[x]/<x^2>$. Hence, we can extend the ElGamal scheme in the setting of the group of units of the ring $Z_p[x]/<x^2>$, of order $\phi(x^2) = p(p-1)$. We note that a polynomial $f(x)$ in $Z_p[x]$ belongs to the cyclic group $U(Z_p[x]/\langle x^2\rangle)$ if and only if $(f(x), x) = 1$. This is equivalent to say that x does not divide $f(x)$, where $f(x)$ is a linear polynomial. Hence, $U(Z_p[x]/\langle x^2\rangle) = \{c + dx \mid 1 \le c \le p-1, 0 \le d \le p-1\} \cong Z_{p-1} \times Z_p$. The extended ElGamal cryptosystem in this setting is given next through three algorithms.

First, to generate the corresponding public and private keys, entity A should use the following algorithm:

Algorithm 8 (Key generation)

1. Generate a large random prime p and a reducible polynomial $h(x)$ in $Z_p[x]$ as a square of a linear polynomial and compute $\phi(x^2) = p(p-1)$.
2. Find a generator $\alpha(x)$ of the multiplicative group $U(Z_p[x]/\langle x^2\rangle)$. That is, $U(Z_p[x]/\langle x^2\rangle) = \{e, \alpha(x), \alpha(x)^2, \ldots, \alpha(x)^{p^2-p-1}\}$.
3. Select a random integer a, $2 \le a \le \phi(x^2) - 1$. Note that the integer a should be a natural integer in the interval $[2, p^2 - p - 2]$.
4. Compute $\alpha(x)^a \pmod{x^2}$.
5. A's public key is $(p, x^2, \alpha(x), \alpha(x)^a)$, A's private key is a.

To encrypt a message $m(x) \in Z_p[x]/\langle x^2\rangle$, entity B should use the following algorithm:

Algorithm 9 (Encryption scheme)

1. Obtain A's authentic public key $(p, x^2, \alpha(x), \alpha(x)^a)$.
2. Select a random integer k, $2 \le k \le \phi(x^2) - 1$.
3. Represent the message as a polynomial $m(x) \in Z_p[x]/\langle x^2\rangle$.
4. Compute $\gamma(x) = \alpha(x)^k \pmod{x^2}$, and $\delta(x) \equiv m(x).(\alpha(x)^a)^k \pmod{x^2}$.
5. Send the ciphertext $(\gamma(x), \delta(x))$ to A.

To decrypt the ciphertext $(\gamma(x), \delta(x))$ sent by entity B, entity A should use the following algorithm:

Algorithm 10 (Decryption scheme)

1. Receives the ciphertext $(\gamma(x), \delta(x))$ sent by entity B.
2. Use the private key a to compute $\gamma(x)^{p^2-p-a} \pmod{x^2}$.
3. Recover the plaintext $m(x)$ by computing $\gamma(x)^{-a}.\delta(x) \pmod{x^2}$.

The following theorem proves that the decryption formula $\gamma(x)^{-a}.\delta(x) \pmod{x^2}$ allows the recovery of the original plaintext $m(x)$.

Theorem 11 Given a generator $\alpha(x)$ of the multiplicative group of the field $Z_p[x]/\langle x^2\rangle$. Define $\gamma(x)$ and $\delta(x)$ as in the algorithms such that $\gamma(x) = \alpha(x)^a \pmod{x^2}$ and $\delta(x) \equiv m(x).(\alpha(x)^a)^k \pmod{x^2}$. Let $s(x) = \gamma(x)^{-a}.\delta(x) \pmod{x^2}$, then $m(x) = s(x)$.

Proof. Since $\gamma(x) = \alpha(x)^a \pmod{x^2}$, where $\alpha(x)$ is a generator of the multiplicative group $U(Z_p[x]/\langle x^2\rangle)$, it follows that $\gamma(x)$ is in $U(Z_p[x]/\langle x^2\rangle)$ so that $(\gamma(x), x^2) = 1$. Therefore, using a version of Fermat's little theorem for polynomials over a finite field, we have that $\gamma(x)^{p(p-1)-1} \equiv 1 \pmod{x^2}$. Then, $\gamma(x)^{(p^2-p-1)-a} \equiv \gamma(x)^{-a} \equiv \alpha(x)^{-ak} \pmod{x^2}$ and thus $\gamma(x)^{-a}\delta(x) \equiv \alpha(x)^{-ak}.m(x).\alpha(x)^{ak} = m(x) \pmod{x^2}$. Since $m(x)$ and $s(x)$ are in the same complete residue system modulo x^2 and $s(x) \equiv m(x) \pmod{x^2}$, we have that $m(x) = s(x)$. Hence, $m(x)$ is recovered by reducing $\gamma(x)^{-a}.\delta(x)$ modulo x^2. ■

Example 12 For $p = 3$, $U(Z_3[x]/\langle x^2\rangle) = \{1, 2, 1+x, 2+x, 1+2x, 2+2x\}$ and $\phi(x^2) = 6$. Note that x^2 is the zero in $Z_3[x]/\langle x^2\rangle$. To find a generator to $U(Z_3[x]/\langle x^2\rangle)$, select the polynomial $\alpha(x) =$

$2+x$ in $U(Z_3[x]/\langle x^2\rangle)$. The order $\phi(x^2) = 6$ has two prime divisors 2 and 3. Since $(2+x)^2 = 4+4x+4x^2 = 4+4x \equiv 1+x \not\equiv 1$ over Z_3 and $(2+x)^3 = 2+3x+x^2 \equiv 2 \not\equiv 1$ over Z_3. Hence, $\alpha(x) = 2+x$ is a generator. To generate the corresponding public and private keys, entity A should first choose its own private key $a = 4$, then computes $\alpha(x)^a = \alpha(x)^4 = (2+x)^4 \equiv 1+2x \pmod{x^2}$. Thus, A's private key is $a = 4$ and public key is $(3, x^2, 2+x, 1+2x)$. To encrypt the message $m(x) = 2x+2$, entity B selects randomly an integer $k = 3$, then computes $\gamma(x) = \alpha(x)^k = (2+x)^3 \equiv 2 \pmod{x^2}$ and $\delta(x) = m(x).(\alpha(x)^a)^k = (2x+2).((2+x)^4)^3 \equiv 2+2x \pmod{x^2}$. The ciphertext is $c(x) = (\gamma(x), \delta(x))$. Hence, entity B sends the ciphertext $(2, 2x+2)$ to entity A. To decrypt the sent ciphertext $(2, 2x+2)$, entity B should use its own private key $a = 4$ to compute $\gamma(x)^{-a} \equiv \gamma(x)^{p(p-1)-a} = (2)^{6-4} \equiv 1 \pmod{x^2}$. Finally, the plaintext $m(x)$ can be recovered by computing $s(x) = \gamma(x)^{-a}.\delta(x) \equiv 1.(2x+2) = 2x+2 \pmod{x^2}$.

6 Conclusion

Using a characterization of quotient rings of polynomials over finite fields with a cyclic group of units, the ElGamal encryption scheme was extended to the setting of $F_q[x]/<f(x)>$ where $f(x)$ is a reducible polynomial in $F_q[x]$. Algorithms for the extended ElGamal cryptosystem in the setting of $Z_p[x]/\langle x^2\rangle$ were given along with their proofs. A numerical example was provided to illustrate the new method.

We conclude this paper by considering the following problem. In addition to the new setting, $Z_p[x]/\langle x^2\rangle$, where p is an odd prime, one may consider the case of extending ElGamal public-key cryptosystem using the reducible polynomials in cases (iii) and (iv) of theorem 7. Note that in this case one needs to find irreducible polynomials over Z_2, unlike the case considered in this paper. Also note that if p is an odd prime of the form $4k+1$, then $Z_p[x]/\langle x^2\rangle$ is not reduced to the classical case and when p is of the form $4k+3$, one may use either the setting $Z_p[x]/\langle x^2\rangle$ or $Z[i]/\langle p\rangle$ which are basically different.

References

[1] Cross, J. T. "The Euler's ϕ-function in the Gaussian integers", American Mathematical Monthly 90, 518-528, 1983.

[2] ElGamal, T., "A public-key cryrptosystem and a signature scheme based on discrete logarithms", Advances in Crypotology-Proceedings of CRYPTO 84(LNCS 196), 10-18, 1985.

[3] El-Kassar, A. N.; Rizk, M; Mirza, N. M.; Awad, Y. A. "El-Gamal public-key cryptosystem in the domain of Gaussian integers", Int. J. Appl. Math. 7 (2001), no. 4, 405–412.

[4] El-Kassar, A. N., Chihadi H., and Zentout D., "Quotient rings of polynomials over finite fields with cyclic group of units", Proceedings of the International Conference on Research Trends in Science and Technology, pp. 257-266, 2002.

[5] Gallian, J. A., "Contemporary Abstract Algebra", D.C., Heath and Company, 1991.

[6] Menezes, A., van Oorschot P. C., Vanstone, S. A., "Hand Book of Applied Cryptography", CRC Press, 1997.

[7] Smith, Judy L. and J.A.Gallian, "Factoring finite factor rings", Mathematics Magazine 58(1985):93-95.

This work is funded by the Lebanese American University