UDC 681.3.06

ElGamal Public-Key Cryptosystem in Multiplicative Groups of Quotient Rings of Polynomials over Finite Fields

A. N. El-Kassar[1] and Ramzi A. Haraty [2]

[1] Beirut Arab University, Mathematics Department,
P. O. Box 11-5020, Beirut, Lebanon
ak1@bau.edu.lb
[2] Lebanese American University
P.O. Box 13-5053 Chouran, Beirut,
Lebanon 1102 2801
rharaty@lau.edu.lb

Abstract. The ElGamal encryption scheme is described in the setting of any finite cyclic group G. Among the groups of most interest in cryptography are the multiplicative group $\mathbf{Z}_p^*$ of the ring of integers modulo a prime p, and the multiplicative groups $F_{2^m}^*$ of finite fields of characteristic two. The later requires finding irreducible polynomials $h(x)$ and constructing the quotient ring $\mathbf{Z}_2[x]/<h(x)>$. El-Kassar et al. modified the ElGamal scheme to the domain of Gaussian integers. El-Kassar and Haraty gave an extension in the multiplicative group of $\mathbf{Z}_p[x]/<x^2>$. Their major finding is that the quotient ring need not be a field. In this paper, we consider another extension employing the group of units of $\mathbf{Z}_2[x]/<h(x)>$, where $h(x)=h_1(x)h_2(x)..h_r(x)$ is a product of irreducible polynomials whose degrees are pairwise relatively prime. The arithmetic needed in this new setting is described. Examples, algorithms and proofs are given. Advantages of the new method are pointed out and comparisons with the classical case of $F_{2^m}^*$ are made.

1. Introduction

The ElGamal encryption scheme is typically described in the setting of the multiplicative group $\mathbf{Z}_p^*$, 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 $\mathbf{Z}_p^*$, and the multiplicative group $F_{2^m}^*$ of the finite field F_{2^m} of characteristic two. Also of interest is the group of units $\mathbf{Z}_n^*$ where n is a composite integer such that n is 2, 4, p^t, or 2 p^t, where p is an odd prime and t is an integer.

Cross [1] gave a classification of all Gaussian integers ß such that the group of units of the quotient ring $\mathbf{Z}[i]/\langle ß \rangle$ is cyclic. So, one may consider ElGamal public-key cryptosystem using the cyclic group of units of $\mathbf{Z}[i]/\langle ß \rangle$, where ß = $1+i$, $(1+i)^2$, $(1+i)^3$, p, $(1+i)p$, π^n, $(1+i)\,\pi^n$, p is a prime integer of the form $4k+3$, and π is a Gaussian prime with $|\pi|^2$ is a prime 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 ElGamal encryption scheme to the domain of Gaussian integers.

In [8], Smith and Gallian determined the structure of the group of units of the quotient ring $F_q[x]/\langle f(x) \rangle$, 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. In [5], this classification was applied to ElGamal encryption scheme to the setting of $\mathbf{Z}_p[x]/\langle x^2 \rangle$. The purpose of this paper is to use this classification to apply ElGamal encryption scheme to the setting of $F_q[x]/\langle f(x) \rangle$, where $f(x)$ is a reducible polynomial in $F_q[x]$. In particular, we consider ElGamal encryption scheme in the setting of the group of units of $\mathbf{Z}_2[x]/\langle h(x) \rangle$, where $h(x) = h_1(x)h_2(x)..h_r(x)$ is a product of irreducible polynomials whose degrees are pairwise relatively prime.

The rest of the paper is organized as follows: section 2 describes the classical ElGamal scheme. In section 3, we summarize the extension, given in [3], of ElGamal cryptosystem to the domain of Gaussian integers. Section 4 presents the classification, obtained in [4], of quotient rings of polynomials $F_q[x]/\langle f(x) \rangle$ having cyclic group of units. Section 5 describes the extension, given in [5], of ElGamal cryptosystem in the setting of $\mathbf{Z}_p[x]/\langle x^2 \rangle$. Section 6 introduces the new method in the setting of quotient rings of polynomials over a finite field, other than $\mathbf{Z}_p[x]/\langle x^2 \rangle$, having cyclic group of units. Section 7 points out some of the advantages of the new method and compares it to the classical case of F_{2^m}. Finally, section 8 concludes the paper.

2. The Classical ElGamal Public Key Encryption Scheme

The classical ElGamal cryptosystem, see [2] and [7], can be described as follows. Let p be a large odd prime integer and let $\mathbf{Z}_p = \{0, 1, 2, 3, ..., p-1\}$. Then, $\mathbf{Z}_p$ is a ring under addition and multiplication modulo p. Since p is prime, $\mathbf{Z}_p$ is actually a field under these operations. Moreover, $\mathbf{Z}_p^* = \{1, 2, 3, ..., p-1\}$, the multiplicative group of the ring integers modulo p, is a cyclic group generated by some generator $\theta \neq 1$ whose order is equal to $p-1$. That is, every element of $\mathbf{Z}_p^*$ is a power of θ. Note that $\mathbf{Z}_p$ is a complete residue system modulo p and $\mathbf{Z}_p^*$ is a reduced residue system modulo p. For further algebraic properties, see [6] and [7].

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 θ of $\mathbf{Z}_p^*$. Then A chooses randomly an integer a, $1 \leq a \leq p-2$, and computes $\theta^a \pmod p$. The public key is (p, θ, θ^a) and A's private key is a.

To encrypt the message m chosen from $\mathbf{Z}_p$, entity B first obtains A's public-key (p, θ, θ^a). Then B chooses a random integer k, where $2 \leq k \leq p-2$, computes $\gamma \equiv \theta^k \pmod p$ and $\delta \equiv m \cdot (\theta^a)^k \pmod p$. 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 $\gamma^{-a}.\delta \pmod p$.

Example 1. In order to generate the public key, entity A selects the prime $p = 359$ and a generator $\theta = 124$ of $\mathbf{Z}_{359}^*$. A chooses the private key $a = 292$ and computes $\theta^a = 124^{292} \equiv 205 \pmod{359}$. Therefore, A's public-key is ($p = 359$, $\theta = 124$, $\theta^a = 205$) and A's private key is $a = 292$. To encrypt the message $m = 101$, B selects a random integer $k = 247$ and computes $\gamma = 291 \equiv 124^{247} \pmod{359}$ and $\delta = 288 \equiv 101 \cdot 205^{247} \pmod{359}$. Then B sends $\gamma = 291$ and $\delta = 288$ to A. We note that B has 359 choices for m in $\mathbf{Z}_{259}$. Finally, A computes $\gamma^{p-1-a} = 291^{66} \equiv 216 \pmod{359}$ and recovers m by computing $216 \cdot 288 \equiv 101 \pmod{359}$.

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 $\mathbf{Z}[i] = \{a+bi \mid a, b \in \mathbf{Z}\}$. 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 ß be a Gaussian prime integer and let $G_ß$ be a set of representatives of the elements of the quotient ring $\mathbf{Z}[i]/\langle ß \rangle$. Then, $G_ß$ is a field under addition and multiplication modulo ß having a cyclic multiplicative group G_β^*. Note that $G_ß$ is a complete residue system modulo ß and G_β^* is a reduced residue system modulo ß. If ß = π, where $q = |\pi|^2$ is a prime integer of the form $4k+1$, then $G_\pi = \{a \mid 0 \le a \le q-1\} = \mathbf{Z}_q$, see [1]. This choice will be excluded since the calculations in this case are identical to those of the classical one. Hence, ß is chosen to be a large prime integer p of the form $4k+3$ so that $G_ß = \{a+bi \mid 0 \le a \le p-1, 0 \le b \le p-1\}$, where the number of elements in $G_ß$ is p^2 and in G_β^* is $\phi(ß) = p^2-1$. 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 θ 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, θ, θ^a). Since a is a power of θ, 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 $G_ß$. 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 $\gamma \equiv \theta^k \pmod{ß}$ and $\delta \equiv m.(\theta^a)^k \pmod{ß}$. Note that the values of γ and δ must be elements of $G_ß$ and hence must be reduced modulo ß. The message c is decrypted using the private key a to compute $\gamma^{-a}.\delta$ modulo ß.

Example 2. In order to generate the public-key, entity A selects the Gaussian prime ß = 359 and a generator θ = 1+11i of G_{1+11i}^*. A chooses the private key a = 86427 and computes θ^a modulo ß, which is $\theta^a = (1+11i)^{86427} \equiv 323+295i \pmod{359}$. Therefore, A's public-key is (p = 359, θ = 1+11i, θ^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 $\gamma = (1+11i)^{115741} \equiv 149+117i \pmod{359}$ and $\delta = 101 \cdot (323+295i)^{115741} \equiv 147+209i \pmod{359}$. Then B sends γ = 149+117i and δ = 147+209i to A. We note that B has 128880 choices for m in G_{359}. Finally, A computes $\gamma^{ß^2-1-a} = (149+117i)^{42453} \equiv$

$117+178i \pmod{359}$, and recovers m by computing $(117+178i)\cdot(147+209i) \equiv 101 \pmod{359}$.

4. Quotient Rings of Polynomials over a Field with Cyclic Groups 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 $\mathbf{Z}_p[x]/\langle h(x)\rangle$, where $h(x)$ is an irreducible polynomial over $\mathbf{Z}_p[x]$, $q = p^n$, and p is a prime integer. In the following, we extend the ElGamal public key cryptosystem to the setting of quotient ring 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 $\mathbf{Z}_p[x]/\langle h(x)\rangle = \{a_0+a_1x+...+a_{n-1}x^{n-1} \mid a_0, a_1,..., a_{n-1}\in\mathbf{Z}_p\}$ is a field whose elements are the congruence classes modulo $h(x)$ of polynomials in $\mathbf{Z}_p[x]$ with degree less than that of $h(x)$. Note that the representatives of the elements of $\mathbf{Z}_p[x]/\langle h(x)\rangle$ form a complete residue system modulo $h(x)$ in $\mathbf{Z}_p[x]$. Moreover, $\mathbf{Z}_p[x]/\langle h(x)\rangle$ is a finite field of order p^n and its nonzero elements form its cyclic group of units, $U(\mathbf{Z}_p[x]/\langle h(x)\rangle)$, of order $\phi(h(x)) = p^n-1$.

Now consider the factor ring $F_q[x]/\langle f(x)\rangle$, where F_q is a finite field of order q and $f(x)$ is a polynomial of degree n. Then $F_q[x]/\langle f(x)\rangle = \{a_0+a_1x+...+a_{n-1}x^{n-1} \mid a_0, a_1,..., a_{n-1}\in F_q\}$ is a ring whose elements are the congruence classes modulo $f(x)$ of polynomials in $F_q[x]$ with 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 $F_q[x]/\langle h(x)\rangle$ is a finite field of order q^n. Its group of units is isomorphic to the cyclic group $\mathbf{Z}_{q^n-1}$. 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 $F_q[x]/\langle f(x)\rangle$ given by Smith and Gallian [8]. 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 1. If $R = R_1 \oplus R_2 \oplus ... \oplus R_i$, then $U(R) = U(R_1)\times U(R_2)\times ...\times U(R_i)$.

Since $F_q[x]$ is a unique factorization domain, then $f(x)$ can be written as a product of powers of irreducible polynomials, $f(x) = h_1(x)^{m_1} h_2(x)^{m_2} \ldots h_r(x)^{m_r}$, in $F_q[x]$ and $F_q[x]/\langle f(x)\rangle \cong F_q[x]/\langle h_1(x)^{m_1}\rangle \oplus \ldots \oplus F_q[x]/\langle h_r(x)^{m_r}\rangle$. 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 $U\left(F_q[x]/\langle h(x)^m\rangle\right)$, where $h(x)$ is irreducible over F_q. This result is stated as follows.

Lemma 1. If $f(x) = h_1(x)^{m_1} h_2(x)^{m_2} \ldots h_r(x)^{m_r}$, where the polynomials $h_i(x)$, $1 \le i \le r$, are distinct irreducible polynomials in $F_q[x]$, then $U\left(F_q[x]/\langle f(x)\rangle\right) \cong U\left(F_q[x]/\langle h_1(x)^{m_1}\rangle\right) \times \ldots \times U\left(F_q[x]/\langle h_r(x)^{m_r}\rangle\right)$.

The following theorems simplify the problem further.

Theorem 2. 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 $F_q[x]/\langle h(x)^m\rangle \cong K[x]/\langle x^m\rangle$.

Theorem 3. Let K be a finite field with p^n elements, where p is prime. Then, $U(K[x]/\langle x^m\rangle) \cong \mathbf{Z}_{p^n-1} \times \prod_{i=1}^{s} n(k_{i-1} - 2k_i + k_{i+1}) * \mathbf{Z}_{p^i}$, where m is any positive integer, $s = \min\{ h \in \mathbf{Z} \mid p^h \ge m\}$, $k_i = \max\{h \in \mathbf{Z} \mid hp^i < m\}$, and $t * \mathbf{Z}_{p^i}$ means $\mathbf{Z}_{p^i}$ occurs in the product t times.

The above lemma and theorems can be combined to classify the group of units of any quotient ring of the form $F_q[x]/\langle f(x)\rangle$. Now we turn to the problem of classifying all quotient rings of polynomials $F_q[x]/\langle f(x)\rangle$ with cyclic group of units. The results obtained in the remainder of this section are found in [4]. If $h(x)$ is an irreducible polynomial over F_q of degree n, we have that $F_q[x]/\langle h(x)\rangle$ is a field of order $q^n = p^{nd}$. Hence, $U(F_q[x]/\langle h(x)\rangle)$ is cyclic with order $q^n - 1 = p^{nd} - 1$ and $U(F_q[x]/\langle h(x)\rangle) \cong \mathbf{Z}_{p^{nd}-1}$.

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 $U(F_q[x]/\langle h(x)^m\rangle) \cong U(F_q[x]/\langle x^m\rangle)$. Also note that in order for $U\left(F_q[x]/\langle f(x)\rangle\right) \cong \mathbf{Z}_{p^d-1} \times \prod_{i=1}^{s} d(k_{i-1} - 2k_i + k_{i+1}) * \mathbf{Z}_{p^i}$ to be cyclic, the product $\prod_{i=1}^{s} d(k_{i-1} - 2k_i + k_{i+1}) * \mathbf{Z}_{p^i}$ must contain at most one nontrivial factor since the order of each $\mathbf{Z}_{p^i}$ is divisible by p. The different cases

when $U(F_q[x]/<h(x)>)$ are cyclic depend on the characteristic of the field and are characterized in the following theorem.

Theorem 4. Let F_q be a finite field of order $q = p^n$, where p is a prime integer, and let $h_1(x)$, $h_2(x)$, …, $h_r(x)$ be the distinct irreducible factors of $f(x)$ in $F_q[x]$ whose degrees, deg $h_j(x) = d_j$, $1 \le j \le r$, are pairewise relatively prime. Then, $U(F_q[x]/<f(x)>)$ is cyclic if and only if one of the following is true:

i) $f(x) = h_1(x)$ is irreducible and $U(F_q[x]/<f(x)>) \cong \mathbf{Z}_{q^{d_1}-1}$.

ii) $f(x) = h_1(x)^2$, where $h_1(x)$ is linear, $q = p$ and $U(F_q[x]/<f(x)>) = U(\mathbf{Z}_p[x]/<f(x)>) \cong \mathbf{Z}_{p-1} \times \mathbf{Z}_p$.

iii) $f(x) = h_1(x)h_2(x)...h_r(x)$, $q = 2$, and $U(F_q[x]/<f(x)>) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r}-1}$.

iv) $f(x) = h_1(x)h_2(x)...h_r(x)^2$, $q = 2$, $h_1(x)$ is linear, and $U(F_q[x]/<f(x)>) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r-1}-1} \times \mathbf{Z}_2$.

5. ElGamal Public Key Cryptosystem over $\mathbf{Z}_p[x]/<x^2>$

Now we describe the extended ElGamal encryption scheme over quotient rings of polynomials $\mathbf{Z}_p[x]/<h(x)>$ where $h(x)$ is reducible. From the study above we conclude that in order for the group of units $U(\mathbf{Z}_p[x]/<h(x)>)$, where p is an odd prime, to be cyclic, $h(x)$ must be a square power of only one linear irreducible polynomial. That is, $U(\mathbf{Z}_p[x]/<(ax+b)^2>)$ is cyclic. But, $\mathbf{Z}_p[x]/<(ax+b)^2> \cong \mathbf{Z}_p[x]/<x^2>$. Hence, we can extend the ElGamal scheme in the setting of the group of units of the ring $\mathbf{Z}_p[x]/<x^2>$, of order $\phi(x^2) = p(p-1)$. In $\mathbf{Z}_p[x]/<x^2>$, x^2 is zero. Also, a polynomial $f(x)$ in $\mathbf{Z}_p[x]$ belongs to the cyclic group $U(\mathbf{Z}_p[x]/<x^2>)$ if and only if $\gcd(f(x), x) = 1$. Equivalently, x does not divide the linear polynomial $f(x)$ so that $U(\mathbf{Z}_p[x]/<x^2>) = \{c+dx \mid 1 \le c \le p-1, \quad 0 \le d \le p-1\} \cong \mathbf{Z}_{p-1} \times \mathbf{Z}_p$.

The extended ElGamal cryptosystem in this setting is given in the following three algorithms. First, to generate the corresponding public and private keys, entity A should use the following algorithm:

Algorithm 1. (Key generation)

1. Generate a large random prime p and select the reducible polynomial $h(x)$ in $\mathbf{Z}_p[x]$ to be a square of a linear polynomial, say x^2, and compute $\phi(x^2) = p(p-1)$.
2. Find a generator $\alpha(x)$ of the multiplicative group $U(\mathbf{Z}_p[x]/<x^2>)$. That is, $U(\mathbf{Z}_p[x]/<x^2>) = \{1, \alpha(x), \alpha(x)^2, ..., \alpha(x)^{p^2-p-1}\}$.

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 $m(x) \in \mathbf{Z}_p[x]/\langle x^2 \rangle$, entity B should use the following algorithm:

Algorithm 2. (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 $m(x) \in U(\mathbf{Z}_p[x]/\langle x^2 \rangle)$.
4. Compute $\gamma(x) \equiv \alpha(x)^k \pmod{x^2}$ 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 3. (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 5. Given a generator $\alpha(x)$ of the multiplicative group of the ring $\mathbf{Z}_p[x]/\langle x^2 \rangle$, define $\gamma(x)$ and $\delta(x)$ by $\gamma(x) \equiv \alpha(x)^a \pmod{x^2}$ and $\gamma(x) \equiv m(x).(\alpha(x)^a)^k \pmod{x^2}$. If $s(x) \in \mathbf{Z}_p[x]/\langle x^2 \rangle$ such that $s(x) \equiv \gamma(x)^{-a}.\delta(x) \pmod{x^2}$, then $m(x) = s(x)$.

Proof. Since $\gamma(x) \equiv \alpha(x)^a \pmod{x^2}$, where $\alpha(x)$ is a generator of the multiplicative group $U(\mathbf{Z}_p[x]/\langle x^2 \rangle)$, it follows that $\gamma(x)$ is in $U(\mathbf{Z}_p[x]/\langle x^2 \rangle)$ so that $\gcd(\gamma(x), x^2) = 1$. 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 $\gamma(x)^{-a}\delta(x) \equiv \alpha(x)^{-ak}.m(x).\alpha(x)^{ak} \equiv m(x) \pmod{x^2}$. Since $m(x)$ and $s(x)$ belong to the same reduced 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 3. For $p = 3$, $U(\mathbf{Z}_3[x]/\langle x^2\rangle) = \{1, 2, 1+x, 2+x, 1+2x, 2+2x\}$ and $\phi(x^2) = 6$. Note that x^2 is the zero in $\mathbf{Z}_3[x]/\langle x^2\rangle$. To find a generator to $U(\mathbf{Z}[x]/\langle x^2\rangle)$, select the polynomial $\alpha(x) = 2+x$ in $U(\mathbf{Z}_3[x]/\langle x^2\rangle)$. The prime divisors of $\phi(x^2) = 6$, the order of the group $U(\mathbf{Z}_3[x]/\langle x^2\rangle)$, are 2 and 3. Since $(2+x)^{(6/3)} = 4 + 4x + 4x^2 = 4 + 4x \equiv 1+x \neq 1 \pmod{x^2}$ over $\mathbf{Z}_3$ and $(2+x)^{(6/2)} = 2+3x+x^2 \equiv 2 \neq 1 \pmod{x^2}$ over $\mathbf{Z}_3$, we have that $\alpha(x) = 2+x$ 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. ElGamal Cryptosystem in $\mathbf{Z}_2[x]/\langle h_1(x).h_2(x)...h_r(x)\rangle$

Now we describe the extended ElGamal encryption scheme in the quotient rings of polynomials $\mathbf{Z}_2[x]/\langle h(x)\rangle$, where $h(x)$ is reducible not of the form $(ax+b)^2$. From theorem 4, we conclude that in order for the group of units $U(\mathbf{Z}_2[x]/\langle h(x)\rangle)$ to be cyclic, $h(x) = h_1(x).h_2(x)...h_r(x)$ where the $d_j's$ are pairwise relatively prime and $U(\mathbf{Z}_2[x]/\langle h(x)\rangle) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r}-1}$, or $f(x) = h_1(x).h_2(x)...h_r(x)^2$ with $U(\mathbf{Z}_2[x]/\langle h(x)\rangle) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r-1}-1} \times \mathbf{Z}_2$. Hence, we can extend the ElGamal scheme in the setting of the group of units $U(\mathbf{Z}_2[x]/\langle h(x)\rangle) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r}-1}$, of order $\phi(h(x)) = \left(2^{d_1}-1\right)\left(2^{d_2}-1\right)..\left(2^{d_r}-1\right)$. We note that a polynomial $h(x)$ in $\mathbf{Z}_2[x]$ belongs to the cyclic group $U(\mathbf{Z}_2[x]/\langle h(x)\rangle) \cong \mathbf{Z}_{2^{d_1}-1} \times \mathbf{Z}_{2^{d_2}-1} \times ... \times \mathbf{Z}_{2^{d_r}-1}$ if and only if $\gcd(f(x), h(x)) = 1$. This is equivalent to say that $\gcd(f(x), h_j(x)) = 1$, for every j, $1 \le j \le r$.

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 4. (Generating the Key)

1. Select pairwise relatively prime integers $d_1, d_2, ..., d_r$.
2. Find irreducible polynomials $h_2(x), h_2(x), ..., h_r(x)$ over $\mathbf{Z}_2$ with $\deg h_j(x) = d_j$.

3. Form $h(x) = h_1(x).h_2(x)...h_r(x)$.
4. Find $\phi(h(x)) = \left(2^{d_1}-1\right)\left(2^{d_2}-1\right)..\left(2^{d_r}-1\right)$.
5. Find a generator α(x) of the multiplicative group $U(\mathbf{Z}_2[x]/<h(x)>)$. That is, $U(\mathbf{Z}_2[x]/<h(x)>) = \{ 1, \alpha(x), \alpha(x)^2, ..., \alpha(x)^{\phi(h(x))-1}\}$.
6. Select a random integer a, $2 \le a \le \phi(h(x))-1$.
7. Compute $\alpha(x)^a \pmod{h(x)}$.
8. A's public key is $(h(x), \alpha(x), \alpha(x)^a)$; A's private key is a.

To encrypt a message $m(x) \in \mathbf{Z}_2[x]/<h(x)>$, entity B should use the following algorithm:

Algorithm 5. (Encryption scheme)

1. Obtain A's authentic public key $(h(x), \alpha(x), \alpha(x)^a)$.
2. Select a random integer k, $2 \le k \le \phi(h(x))$.
3. Represent the message as a polynomial $m(x) \in \mathbf{Z}_2[x]/<h(x)>$.
4. Compute $\gamma(x) \equiv \alpha(x)^k \pmod{h(x)}$ and $\delta(x) \equiv m(x).(\alpha(x)^a)^k \pmod{h(x)}$.
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 6. (Decryption scheme)

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

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

Theorem 6. Given a generator $\alpha(x)$ of the multiplicative group of the ring $\mathbf{Z}_2[x]/<h(x)>$, where $h(x) = h_1(x).h_2(x)...h_r(x)$ is a product of irreducible polynomials with deg $h_j = d_j$ and the $d_j's$ are pairwise relatively prime. Define $\gamma(x)$ and $\delta(x)$ by $\gamma(x) \equiv \alpha(x)^a \pmod{h(x)}$ and $\gamma(x) \equiv m(x).(\alpha(x)^a)^k \pmod{h(x)}$. If $s(x) \in \mathbf{Z}_p[x]/<h(x)>$ such that $s(x) \equiv \gamma(x)^{-a}.\delta(x) \pmod{h(x)}$, then $m(x) = s(x)$.

Proof. Since $\gamma(x) \equiv \alpha(x)^a \pmod{h(x)}$, where $\alpha(x)$ is a generator of the multiplicative group $U(\mathbf{Z}_2[x]/<h(x)>)$, it follows that $\gamma(x)$ is in

$U(\mathbf{Z}_2[x]/\langle h(x)\rangle)$ so that $\gcd(\gamma(x), h(x)) = 1$. Therefore, using a version of Fermat's little theorem for polynomials over a finite field, we have that $\gamma(x)^{\phi(h(x))} \equiv 1 \pmod{h(x)}$. Then, $\gamma(x)^{\phi(h(x))-a} \equiv \gamma(x)^{-a} \equiv \alpha(x)^{-ak} \pmod{h(x)}$ and thus $s(x) \equiv \gamma(x)^{-a}\delta(x) \equiv \alpha(x)^{-ak}.m(x).\alpha(x)^{ak} \equiv m(x) \pmod{h(x)}$. Since $m(x)$ and $s(x)$ are in the same complete residue system modulo $h(x)$ and $s(x) \equiv m(x) \pmod{h(x)}$, we have that $m(x) = s(x)$. Hence, $m(x)$ is recovered by reducing $\gamma(x)^{-a}.\gamma(x)$ modulo $h(x)$.

Example 4. For $d_1 = 2$ and $d_2 = 3$. Select the irreducible polynomials $h_1(x) = x^2 + x + 1$ and $h_2(x) = x^3 + x + 1$. Then $h(x) = h_1(x).h_2(x) = (x^2 + x + 1).(x^3 + x + 1) = x^5 + x^4 + 1$ and $\mathbf{Z}_2[x]/\langle h(x)\rangle = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2, x^3, 1 + x^3, x + x^3, 1 + x + x^3, x^2 + x^3, 1 + x^2 + x^3, x + x^2 + x^3, 1 + x + x^2 + x^3, x^4, 1 + x^4, x + x^4, 1 + x + x^4, x^2 + x^4, 1 + x^2 + x^4, x + x^2 + x^4, 1 + x + x^2 + x^4, x^3 + x^4, 1 + x^3 + x^4, x + x^3 + x^4, 1 + x + x^3 + x^4, x^2 + x^3 + x^4, 1 + x^2 + x^3 + x^4, x + x^2 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4\}$. Note that the order of $\mathbf{Z}_2[x]/\langle x^5 + x^4 + 1\rangle$ is $2^{d_1}.2^{d_2} = 2^2.2^3 = 32$. Also note that $x^5 = x^4 + 1$ in $\mathbf{Z}_2[x]/\langle h(x)\rangle$. Now $U(\mathbf{Z}_2[x]/\langle h(x)\rangle) = \{1, x, 1 + x, x^2, 1 + x^2, x + x^2, x^3, x + x^3, x^2 + x^3, 1 + x^2 + x^3, 1 + x + x^2 + x^3, x^4, 1 + x^4, 1 + x^4, x^2 + x^4, 1 + x + x^2 + x^4, x^3 + x^4, 1 + x^3 + x^4, x + x^3 + x^4, x + x^2 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4\}$ and $\phi(h(x)) = \left(2^{d_1} - 1\right)\left(2^{d_2} - 1\right) = (2^2 - 1)(2^3 - 1) = 21$. To find a generator to $U(\mathbf{Z}_2[x]/\langle h(x)\rangle)$, select the polynomial $\alpha(x) = x$ in $U(\mathbf{Z}_2[x]/\langle h(x)\rangle)$. The order $\phi(h(x)) = 21$ has two prime divisors 3 and 7. Since $(x)^3 \neq 1$ over $\mathbf{Z}_2[x]/\langle h(x)\rangle$ and $(x)^{\square} = x^2(x^{\square}) = x^2(x^4+1) = x^{\square} + x^2 = x(x^{\square}) + x^2 = x(x^4 + 1) + x^2 = x^{\square} + x + x^2 = x^4 + x + x^2 + 1 \neq 1$ in $\mathbf{Z}_2[x]/\langle h(x)\rangle$. Hence, $\alpha(x) = x$ is a generator. To generate the corresponding public and private keys, entity A should first choose its own private key $a = 11$, then computes $\alpha(x)^a = \alpha(x)^{11} = (x)^{11} \equiv 1 + x^2 + x^3 \pmod{h(x)}$. Thus, A's private key is $a = 11$ and public key is $(h(x), \alpha(x), \alpha(x)^a) = (x^5 + x^4 + 1, x, x^3 + x^2 + 1)$. To encrypt the message $m(x) = x^4 + x^2 + 1$, entity B selects randomly an integer $k = 17$, then computes $\gamma(x) = \alpha(x)^k = (x)^{1\square} \equiv 1 + x \pmod{h(x)}$ and $\delta(x) = m(x).(\alpha(x)^a)^k = (x^4 + x^2 + 1).(1 + x^2 + x^3)^{1\square} \equiv 1 + x^3 \pmod{h(x)}$. Hence, entity B sends the ciphertext $(1+x, 1+x^3)$ to entity A. To decrypt the sent ciphertext $(1+x, 1+x^3)$, entity A should use its own private key $a = 11$ to compute $\gamma(x)^{-a} \equiv \gamma(x)^{\phi(h(x))-a} = (1+x)^{21-11} \equiv x^2 \pmod{h(x)}$. Finally, the plaintext $m(x)$ can be recovered by computing $s(x) = \gamma(x)^{-a}.\delta(x) \equiv x^2.(1+x^3) = x^4 + x^2 + 1 \pmod{h(x)}$.

7. Efficiency and Security of ElGamal Cryptosystem in the Domain of Polynomials over a Finite Field

The ElGamal encryption scheme can described in any finite cyclic group G. The security of the ElGamal encryption scheme is based on the intractability of the discrete logarithm problem in G. The group G should be carefully selected for efficiency and security so that the operation in G can be easily applied and the discrete logarithm problem in G should be computationally infeasible. Among groups meeting these criteria that have received the most attention are the multiplicative group of $\mathbf{Z}_p$ and the multiplicative group of the finite field of characteristic two F_{2^m}. We proposed three modifications of ElGamal encryption employing the group of units of:

1. $\mathbf{Z}[i]/\langle\beta\rangle$, where β is a prime Gaussian integer of the form $p = 4k+3$;
2. $\mathbf{Z}_p[x]/\langle x^2\rangle$, where p is an odd prime integer;
3. $\mathbf{Z}_2[x]/\langle h(x)\rangle$, where $h(x) = h_1(x).h_2(x)...h_r(x)$ is a product of irreducible polynomials with deg $h_j(x) = d_j$ and the $d_j's$ are pairwise relatively prime.

These modifications generalize the two classical cases of $\mathbf{Z}_p^*$ and $F_{2^m}^*$. In the first two cases, the cyclic groups used have orders larger than the square of that used in $\mathbf{Z}_p^*$. Thus, the message space is enlarged with no additional efforts required for finding the prime p. Moreover, the computational procedures in these groups are not much different from those used in the classical case. Hence, we propose to work in the setting of $\mathbf{Z}_p[x]/\langle x^2\rangle$ whenever the prime p generated is of the form $4k+1$. If the prime p generated is of the form $4k+3$, then we propose to work either in $\mathbf{Z}_p[x]/\langle x^2\rangle$ or $\mathbf{Z}[i]/\langle\beta\rangle$.

The third case generalizes the classical ElGamal scheme in the multiplicative group of a finite field F_{2^m} of characteristic two. Let G_1 be the multiplicative group $F_{2^m}^*$ and let G_2 be the multiplicative group of the quotient ring $\mathbf{Z}_2[x]/\langle h(x)\rangle$, where $h(x) = h_1(x).h_2(x)...h_r(x)$ is a product of irreducible polynomials with deg $h_j(x) = d_j$ and the $d_j's$ are pairwise relatively prime. In the following, we list some remarks comparing the two methods.

- Cryptographic applications in rings of characteristic two, such as $\mathbf{Z}_2[x]/\langle h(x)\rangle$, are of particular interest. The arithmetic in these rings can be efficiently performed both in software and in hardware.
- The field F_q is constructed by generating an irreducible polynomial $f(x)$ of degree m in $\mathbf{Z}_2[x]$ and forming $\mathbf{Z}_2[x]/\langle f(x)\rangle = F_{2^m}$. Therefore, the operations in G_1 and G_2 are the same.

- The order of G_1 is 2^m-1 and the order of G_2 is $\left(2^{d_1}-1\right)\left(2^{d_2}-1\right)..\left(2^{d_r}-1\right)$.
- In both cases irreducible polynomials must be found, one in the classical case and two or more in the new settings. This may suggest that the classical case is more efficient. However, finding irreducible polynomials of small degree can be obtained much more quickly than finding one irreducible polynomial of large degree.
- Efficient implementation of the arithmetic in $\mathbf{Z}_2[x]/<h(x)>$ can usually be achieved if the irreducible polynomial chosen has few non-zero terms. In particular, efficient algorithms for finding Irreducible trinomials exist, see [7].
- Given an irreducible polynomial $h_j(x)$ of degree d_j over $\mathbf{Z}_p$, there are more efficient methods for generating new irreducible polynomials of the same degree from $h_j(x)$. Hence, once G_2 has been generated, it is easier to generate another with the same order. In particular, if $x^d + x^k + 1$ is irreducible over $\mathbf{Z}_2$ then so is $x^d + x^{d-k} + 1$.
- A generator in F_q can be found by randomly selecting an element and checking its order. The algorithm is based on the factorization of the order of the multiplicative group $q-1=2^m-1$, which is a very large number and maybe hard to factor. Theorem 1 may be applied to find a generator $\alpha(x)$ for the multiplicative group of $\mathbf{Z}_2[x]/<h(x)>$ as follows. Find a generator to each of the multiplicative groups of $\mathbf{Z}_2[x]/<h_j(x)>$, $1 \le j \le r$, and combine these generators using the Chinese Remainder Theorem to obtain $\alpha(x)$. This method should be faster because it depend on the factorization of the smaller orders $2^{d_1}-1, 2^{d_2}-1, ..., 2^{d_r}-1$.
- A polynomial $h(x)$ is a primitive polynomial if x is a generator of $U(\mathbf{Z}_2[x]/<h_j(x)>)$. Let $f(x) \in \mathbf{Z}_p[x]$ be an irreducible polynomial of degree d. There is an efficient algorithm for testing whether or not $f(x)$ is a primitive polynomial whenever the factorization of the integer 2^d-1 is known. In particular, if 2^d-1 is a prime, then every polynomial in $U(\mathbf{Z}_2[x]/<h(x)>)$ is generator including x so that x is primitive. Hence, if d_j is selected so that $2^{d_j}-1$ is prime, then x is a generator for the factor $U(\mathbf{Z}_2[x]/<h_j(x)>)$. A table listing either a primitive trinomial or a primitive pentanomial of degree d over $\mathbf{Z}_2$ is given in [7], where d is an exponent of one of the first 27 Mersenne primes (primes of the form 2^d-1).
- By theorem 1, $\dfrac{\mathbf{Z}_2[x]}{<h(x)>}$ and $\dfrac{\mathbf{Z}_2[x]}{<h_1(x)>} \oplus ... \oplus \dfrac{\mathbf{Z}_2[x]}{<h_r(x)>}$ are isomorphic so that Entity A may choose to work in

$\frac{\mathbf{Z}_2[x]}{<h_1(x)>} \oplus ... \oplus \frac{\mathbf{Z}_2[x]}{<h_r(x)>}$ and use the isomorphism to convert the computation to and from $\frac{\mathbf{Z}_2[x]}{<h(x)>}$. Entity B would not know whether or not $\frac{\mathbf{Z}_2[x]}{<h(x)>}$ is a field and must work in this setting.

- The new proposed scheme has the property that breaking it requires both factoring the modulus $h(x)$ and solving the discrete logarithm problem. If a cryptanalyst somehow learns the factors of $h(x)$, then in order to recover plaintext from ciphertext it is still left with the task of solving the discrete logarithm problem modulo the factors of $h(x)$.

8. Conclusion

Using a characterization of quotient rings of polynomials over finite fields with a cyclic group of units, the ElGamal encryption scheme was extended in two different ways in the setting of $F_q[x]/<f(x)>$ where $f(x)$ is a reducible polynomial in $F_q[x]$. Algorithms for the extended cryptosystem in the setting of $\mathbf{Z}_p[x]/<x^2>$ were given along with their proofs. Numerical example was provided to illustrate the new method. Also, the case of extending ElGamal cryptosystem to the settings of the multiplicative group of the ring $\mathbf{Z}_2[x]/<h(x)>$, where $h(x) = h_1(x).h_2(x)...h_r(x)$ is a product of irreducible polynomials with deg $h_j = d_j$ and the $d_j's$ are pairwise relatively prime, was considered. In this case one need to find irreducible polynomials over $\mathbf{Z}_2$ and no large prime is generated. A list some of advantages of the new method over the classical case in working in a finite field of characteristic two along with and remarks on the efficiency were given. These remarks and comparative studies of the methods will be investigated in future work.

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 Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology-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, no. 4, 405-412. (2001)
4. El-Kassar, A. N., Chihadi, H., 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, 257-266. (2002)
5. El-Kassar, A. N., Haraty, R.: ElGamal Public-Key Cryptosystem Using Reducible Polynomials Over a Finite Field. Proceedings of the ISCA 13th International Conference on Intelligent and Adaptive Systems and Software Engineering, ISCA 2004, Nice, France, 189-194. (2004)
6. Gallian, J. A.: Contemporary Abstract Algebra. D.C., Heath and Company. (1991)
7. Menezes, A., van Oorschot, P. C., Vanstone, S. A.: Hand Book of Applied Cryptography, CRC Press. (1997)
8. Smith, J. L., Gallian, J.A.: Factoring Finite Factor Rings, Mathematics Magazine 58, 93-95. (1985)

Abdul Nasser Kassar is an associate professor of at Mathematics Beirut Arab University in Beirut, Lebanon. He received his B.S., M.S., and Ph.D. degrees in Mathematics from University of South Western Lousiana in Lafayette, Louisiana. His research interests include cryptography, abstract algebra, and number theory. He has well over 30 journal and conference paper publications.

Ramzi A. Haraty is an associate professor and the chairman of the Division of Computer Science and Mathematics at the Lebanese American University in Beirut, Lebanon. He is also the Chief Financial Officer of the Arab Computer Society. He received his B.S. and M.S. degrees in Computer Science from Minnesota State University - Mankato, Minnesota, and his Ph.D. in Computer Science from North Dakota State University - Fargo, North Dakota. His research interests include database management systems, artificial intelligence, and multilevel secure systems engineering. He has well over 80 journal and conference paper publications. He is a member of Association of Computing Machinery, Arab Computer Society and International Society for Computers and Their Applications.