# RABIN PUBLIC-KEY CRYPTOSYSTEM IN RINGS OF POLYNOMIALS OVER FINITE FIELDS

**A. N. El-Kassar***
**Department of Mathematics**
**Beirut Arab University**
**P. O. Box 11-5020**
**Beirut, Lebanon**
**E-mail: ak1@bau.edu.lb**

**Ramzi Haraty**
**Division of Computer Science and Mathematics**
**Lebanese American University**
**P.O.Box 13-5053 Chouran**
**Beirut, Lebanon 1102 2801**
**E-mail : rharaty@lau.edu.lb**

**Y. A. Awad**
**Department of Mathematics**
**Lebanese International University**
**P. O. Box 5**
**Lebanon, West Bekaa**
**E-mail: yawad@liu.edu.lb**

**Abstract**

Rabin public-key encryption scheme is extended to the domain of polynomials over finite fields. The arithmetics needed for this extension are developed. The computational details and the modified algorithms are described. Numerical examples illustrating the modified algorithms are provided and the advantages of the modified scheme are pointed out.

Keywords: Public-Key Cryptosystem, Rabin Algorithm, Polynomials, Finite Fields

## 1 Introduction

Rabin public-key encryption scheme is one of the widely used public-key cryptosystems. It is the first public-key cryptosystem proven to be secure. Just like the other well-known cryptosystems, RSA and ElGamal cryptosystems, Rabin algorithm is described in the settings of the ring $\mathbf{Z}_n$, the ring of integers modulo a composite integer $n$. Many aspects of the arithmetics in the domain of integers $\mathbf{Z}$ can be carried over to other domains such as $F[x]$, the domain of polynomials over a finite field, and to the domain of Gaussian integers $\mathbf{Z}[i] = \{a+bi \mid a, b \in \mathbf{Z}, i = \sqrt{-1}\}$, see [5] for an introduction to the algebraic properties of $F[x]$ and $\mathbf{Z}[i]$. However, the computational details of the arithmetics in these domains are different from those of $\mathbf{Z}$, see [8] for an introduction on arithmetics in $\mathbf{Z}$. Recently, various extensions of the well-known cryptosystems have been introduced. El-Kassar et al. [3] and El-Kassar and Haraty [4] modified the ElGamal public-key encryption schemes from the domain of natural integers to the two principal ideal domains $\mathbf{Z}[i]$ and $F[x]$, by extending the arithmetic needed for the modifications to these domains. Extensions of the RSA cryptosystems can be found in [1]. Haraty et al. [6,7] performed comparative studies of the modified algorithms and the classical ones. Kojok [9] et al. extended the ElGamal signature scheme to the domain of Gaussian integers.

In this paper, we extend the computational procedures behind the Rabin public-key cryptosystem using arithmetics modulo a polynomial in $F[x]$. First, we review the classical Rabin public-key cryptosystem. Then, we modify the computational methods in the domain of quotient rings of polynomials over a finite field. Finally, we show how the modified computational methods can be used to extend the Rabin algorithm to the domain $F[x]/\langle f(x)\rangle$. We also show that the extended algorithm requires a little additional effort than the classical one and accomplishes much greater security.

## 2 The Classical Rabin Cryptosystem

The classical Rabin cryptosystem can be described as follows: Entity $A$ generates the public-key by first generating two large random prime integers, $p$ and $q$, roughly of the same size, and computes $n = pq$. The public key is $n$ and the private key is the pair $(p, q)$. Suppose that entity $B$ wants to send a message $m \in \mathbf{Z}_n$ to entity $A$. To encrypt a message $m$ chosen from $\mathbf{Z}_n$, entity $B$ first obtains $A$'s public-key $n$. Then $B$ computes $c = m^2 \pmod{n}$. The ciphertext is $c$. To decrypt the message $c$ sent by $B$, entity $A$ uses his own private-key $(p,q)$ and an appropriate method to recover the original message $m$ by finding the square roots $m_1$, $m_2$, $m_3$, and $m_4$, of $c$ modulo $n$, see [10] pp. 99,102. The message is one of these square roots.

**Example 1.** Entity $A$ generates the public-key by first generating two random primes $p = 277$ and $q = 331$, each roughly the same size, then computes $n = pq = 91687$. The public-key is $n = 91687$ and $A$'s private-key is the pair ($p = 277$, $q = 331$). Now suppose that entity

$B$ wants to send the message $m = 40569$, chosen from $\mathbf{Z}_{91687} = \{0, 1, 2,... , 91686\}$, to entity $A$. To encrypt the $m$, entity $B$ first obtains $A$'s public-key $n$. Then, entity $B$ computes $c \equiv m^2 \pmod{n} \equiv 40569^2 \pmod{91687} = 62111$. Hence, the ciphertext is $c = 62111$. Finally, to decrypt the ciphertext $c$ sent by entity $B$, entity $A$ uses his private-key and any algorithm to find the four square roots of $c$ modulo $n$, $m_1 = 69654$, $m_2 = 22033$, $m_3 = 40569$, and $m_4 = 51118$. Entity $A$ somehow decides that the original message was $m = 40569$.

## 3 Rings of Polynomials over Finite Fields

Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$, the ring of polynomials of a finite field $F$. Let $\gcd(f(x), g(x))$ be the greatest common divisor of $f(x)$ and $g(x)$ whose leading coefficient is 1 (monic polynomial). The polynomial gcd $(f(x), g(x))$ can be uniquely written in the form

$$\gcd(f(x), g(x)) = a(x) f(x) + b(x) g(x),$$

for some $a(x), b(x) \in F[x]$. The extended Euclidean algorithm is the process of finding $\gcd(f(x), g(x)$ and writing it in the form $a(x) f(x) + b(x) g(x)$.

Given a polynomial $f(x) \in F[x]$ of degree $n$, deg $f(x) = n$. Let $F[x]/\langle f(x)\rangle$ denote the factor ring or quotient ring of $F[x]$ modulo the ideal $\langle f(x)\rangle$ generated by $f(x)$. The elements of $F[x]/\langle f(x)\rangle$ are the equivalence classes of polynomials in $F[x]$ of degree less $n$. That is,

$$F[x]/\langle f(x)\rangle = \{[a_0 + a_1 x + ... + a_{n-1}x^{n-1}] \mid a_0, a_1, ..., a_{n-1} \in F\}.$$

An element $[h(x)]$ of $F[x]/\langle f(x)\rangle$ is invertible iff $\gcd(f(x), g(x)) = 1$. The polynomial congruence relation $a(x) \equiv b(x) \pmod{f(x)}$ is an equivalence relation and all properties of congruencies of integers hold for polynomials. The set of all congruence classes modulo $f(x)$ is $F[x]/\langle f(x)\rangle$, so that $a(x) \equiv b(x) \pmod{f(x)}$ is equivalent to $[a(x)] = [b(x)]$ in $F[x]/\langle f(x)\rangle$. A complete residue system modulo $f(x)$ denoted by $A(f(x))$ is a set of distinct polynomials in $F[x]$ of degree less than $n$. Then $A(f(x))$ can be written as

$$A(f(x)) = \{a_0 + a_1 x + ... + a_{n-1} x^{n-1} \mid a_0, a_1, ..., a_{n-1} \in F\}.$$

The reduced residue system modulo $f(x)$ is

$$R(f(x)) = \{g(x) \in A(f(x)) \mid \gcd(f(x), g(x)) = 1\}.$$

Let $a(x) \in F[x]$. The multiplicative inverse of $a(x)$ modulo $f(x)$ is a polynomial $b(x) \in F[x]$ such that $a(x).b(x) \equiv 1 \pmod{f(x)}$. Note that the multiplicative inverse of $[a(x)]$ in $F[x]/\langle f(x)\rangle$ is $[b(x)]$ satisfying $[a(x)][b(x)] = 1$ in $F[x]/\langle f(x)\rangle$. The inverse exists and is unique modulo $f(x)$ provided that $\gcd(a(x), f(x)) = 1$.

The Chinese remainder theorem can be extended to $F[x]$ as follows. Let $m_1(x), m_2(x), ..., m_i(x)$ be pairwise relatively prime polynomials over a field $F$ and let $a_1(x), a_2(x), ..., a_i(x) \in F[x]$. Then the system of congruencies

$$f(x) \equiv a_j(x) \pmod{m_j(x)},\ 1 \le j \le i,$$

has a common solution which is unique modulo the product $m_1(x)m_2(x)...m_i(x)$.

Let $F$ be a finite field of order $p^n$, where $p$ is an odd prime. Let $f(x)$ and $g(x)$ be two relatively prime polynomials in $F[x]$. We say that $g(x)$ is a quadratic residue (q.r.) of $f(x)$ if the congruence $\zeta(x)^2 \equiv g(x) \pmod{f(x)}$ has a solution. Otherwise $g(x)$ is a quadratic nonresidue (q.n.r) of $f(x)$. Note if $\zeta_0(x)$ is a quadratic residue modulo $f(x)$, then $f(x) - \zeta_0(x)$ is also a quadratic residue. Also note that the congruence $\zeta(x)^2 \equiv g(x) \pmod{f(x)}$ has either no solution or exactly two incongruent solutions whenever $f(x)$ is an irreducible polynomial $f(x)$ in $F[x]$.

The Euler phi function of $f(x)$, denoted by $\phi(f(x))$, is defined to be the number of elements in $R(f(x))$. If $\gcd(f(x), g(x)) = 1$, then $\phi(f(x).g(x)) = \phi(f(x)).\phi(g(x))$. If $h(x)$ is an irreducible of degree $m$, then $\phi(h(x)) = (p^n)^m - 1$ and $\phi(h(x)^\alpha) = (p^{nm})^{\alpha-1}[p^{nm}-1]$, see[2]. The number of quadratic residues of $h(x)$ can be shown to be $\phi(h(x))/2$, see [1]. In particular, if $F = \mathbf{Z}_p$, then $h(x)$ has exactly $(p^n-1)/2$ quadratic residues modulo $h(x)$. The Legendre Symbol for polynomials in $F[x]$ is defined by

$$\left(\frac{g(x)}{h(x)}\right) = \begin{cases} 1 & \text{if} \quad g(x) \text{ is q.r. of } h(x) \\ -1 & \text{if} \quad g(x) \text{ is a q.n. of } h(x) \\ 0 & \text{if} \quad g(x) \text{ divides } h(x) \end{cases}$$

In the following we state a series of results needed for the extension of Rabin cryptosystem. The proofs of these results can be found in [1].

**Theorem 1.** (Wilson's Theorem in $F[x]$)
Let $h(x)$ be an irreducible polynomial in $F[x]$. Then,

$$\prod_{f(x) \in R(h(x))} f(x) \equiv -1 \pmod{h(x)}.$$

The above theorem can be used to prove the following extension of Euler's criterion to $F[x]$.

**Theorem 2.** (Euler's criterion in $F[x]$)
Let $h(x)$ be an irreducible polynomial in $F[x]$. Then,

$$\left(\frac{g(x)}{h(x)}\right) \equiv g(x)^{\frac{\phi(h(x))}{2}} \pmod{h(x)}.$$

The following theorem shows that the congruence $\zeta(x)^2 \equiv g(x) \pmod{\eta(x)}$, where $\eta(x)$ is a product two distinct irreducible polynomials, has four incongruent solutions modulo $\eta(x)$. The theorem can be used along with Euler's criterion in $F[x]$ to modify an algorithm, [6] p. 102, for finding the square roots modulo $\eta(x)$.

**Theorem 3.** Suppose that $\eta(x)$ is a product of two distinct irreducible polynomials $h(x)$ and $\gamma(x)$ in $F[x]$. If the congruence $\zeta(x)^2 \equiv g(x) \pmod{\eta(x)}$ has a solution $\zeta_0(x)$, then there are exactly four incongruent solutions modulo $\eta(x)$.

Using the above results the algorithms for finding square roots are extended to the domain of $F[x]$ as follows.

**Algorithm 1.** (Finding roots modulo an irreducible polynomial)
*INPUT*: an irreducible polynomial $h(x)$ in $F[x]$ and $a(x) \in R(h(x))$.
*OUTPUT*: the two square roots of $a(x)$ modulo $h(x)$, provided $a(x)$ is a quadratic residue modulo $h(x)$.

1. Use Euler's criterion (Theorem 1) to compute Legendre symbol $\left(\frac{a(x)}{h(x)}\right)$.
2. If $\left(\frac{a(x)}{h(x)}\right) = -1$, then return ($a(x)$ does not have a square root modulo $h(x)$) and terminate.
3. Select $b(x) \in R(h(x))$ at random until one is found with $\left(\frac{b(x)}{h(x)}\right) = -1$.
4. By repeated division by 2, write $\phi(h(x)) = 2^s t$, where $t$ is odd.
5. Compute $a(x)^{-1} \pmod{h(x)}$ using the extended Euclidean algorithm for polynomials.
6. Set $c(x) \leftarrow (b(x))^t \pmod{h(x)}$ and $r(x) \leftarrow \left(a(x)\right)^{\frac{t+1}{2}} \pmod{h(x)}$.
7. For $i$ from 1 to $s-1$ do the following:

   7.1 Compute $d(x) = \left(r(x)^2 a(x)^{-1}\right)^{2^{s-i-1}} \pmod{h(x)}$.

   7.2 If $d(x) \equiv -1 \pmod{h(x)}$, then set $r(x) \leftarrow r(x).c(x) \pmod{h(x)}$.

   7.3 Set $c(x) \leftarrow (c(x))^2 \pmod{h(x)}$.
8. Return $(r(x), -r(x))$.

**Algorithm 2.** (Finding roots modulo a product of two distinct irreducible polynomials)
*INPUT*: A polynomial $\eta(x) = h(x).\gamma(x)$, $h(x)$ and $\gamma(x)$ are distinct irreducible polynomials, and $a(x)$ is a quadratic residue modulo $\eta(x)$.
*OUTPUT*: the four square roots of $a(x)$ modulo $\eta(x)$.

1. Use Algorithm 1 to find the two square roots $r(x)$ and $-r(x)$ of $a(x)$ modulo $h(x)$.
2. Use Algorithm 1 to find the two square roots $s(x)$ and $-s(x)$ of $a(x)$ modulo $\gamma(x)$.
3. Use the extended Euclidean algorithm in $F[x]$ to find $c(x)$ and $d(x)$ such that $c(x)h(x) + d(x)\gamma(x) = 1$.
4. Set $m_1(x) \leftarrow (r(x)d(x)\gamma(x) + s(x)c(x)h(x)) \pmod{\eta(x)}$ and $m_2(x) \leftarrow (r(x)d(x)\gamma(x) - s(x)c(x)h(x)) \pmod{\eta(x)}$.
5. Return $(\pm m_1(x) \pmod{\eta(x)}, \pm m_2(x) \pmod{\eta(x)})$.

## 4 Rabin Cryptosystem in $F[x]$

This section is devoted to the generalization of Rabin public-key cryptosystems to polynomial rings over the finite field $F[x]$. Arithmetic over polynomials discussed above can be applied to extend Rabin cryptosystem. For simplicity, we let $F = \mathbf{Z}_p$ and the general case can be easily obtained in a similar manner. First, choose an odd prime integer $p$, and two irreducible polynomials $h(x)$ and $g(x)$ in $\mathbf{Z}_p[x]$ of degrees $r$ and $s$ respectively. Then, find the polynomial $\eta(x) = h(x)g(x)$ of degree $n = r + s$ in $\mathbf{Z}_p[x]$. Hence, the public-key is $(p, \eta(x))$ and the private-key is $(h(x), g(x))$. Note that the number of elements in $A(\eta(x))$ is $p^n$ and the number of elements in the reduced residue system $R(\eta(x))$ is $\phi(\eta(x)) = (p^s-1)(p^r-1)$.

To encrypt the message $m(x) \in A(\eta(x))$, we find the polynomial $c(x) \in R(\eta(x))$ with $c(x) \equiv (m(x))^2 \pmod{\eta(x)}$ in $\mathbf{Z}_p[x]$. The ciphertext is $c(x)$. To decrypt the ciphertext $c(x)$, we apply algorithm 2 to find the four polynomial square roots of $c(x)$ modulo $\eta(x)$ in $\mathbf{Z}_p[x]$. Finally, we select some how the original message $m(x)$ among them, see [10].

Next, we describe the algorithms of the extended Rabin public-key cryptosystem to polynomials. First, to generate the public and private-keys, entity $A$ should use the following algorithm:

**Algorithm 3.** (Key generation for Rabin public-key encryption over polynomials)

1. Generate a large random odd prime integer $p$.
2. Generate two distinct irreducible polynomials $h(x)$ and $g(x)$ in $\mathbf{Z}_p[x]$.
3. Reduce $\eta(x) = h(x)g(x)$ in $\mathbf{Z}_p[x]$.
4. $A$'s public-key is $(p, \eta(x))$.
5. $A$'s private-key is $(h(x), g(x))$.

To encrypt the selected message $m(x)$ chosen from $A(\eta(x))$, entity $B$ should use the following algorithm:

**Algorithm 4.** (Rabin public-key encryption over polynomials)

1. Obtain $A$'s authentic public-key $(p, \eta(x))$.
2. Represent the message as a polynomial $m(x) \in A(\eta(x))$.
3. Reduce $c(x) \equiv m(x)^2 \pmod{\eta(x)}$ in $\mathbf{Z}_p[x]$.
4. Send the ciphertext $c(x)$ to entity $A$.

Finally, to decrypt the ciphertext $c(x)$ sent by entity $B$, entity $A$ should use the following algorithm:

**Algorithm 5.** (Rabin public-key decryption over polynomials)

1. Use Algorithm 2 to find the four square roots $m_1(x)$, $m_2(x)$, $m_3(x)$, and $m_4(x)$, of $c(x)$ modulo $\eta(x)$ in $\mathbf{Z}_p[x]$.
2. The message sent was either $m_1(x)$, $m_2(x)$, $m_3(x)$, or $m_4(x)$. Entity $A$ somehow decides which of these the original message $m(x)$ is.

**Example 2.** (Rabin encryption over polynomials with artificially small parameters) To generate the public-key, entity $A$ generates a random odd prime integer $p = 5$ and two irreducible polynomials $h(x) = x^2 + 3x + 1$ and $g(x) = x^3 + 2x^2 + 4x + 2$ in $\mathbf{Z}_5[x]$. Then, entity $A$ reduces the polynomial $\eta(x) = h(x)g(x) \equiv x^5 + x^3 + x^2 + 2$ in $\mathbf{Z}_5[x]$. Hence, $A$'s public-key is

$$(p = 5, \eta(x) = x^5 + x^3 + x^2 + 2),$$

and $A$'s private-key is the pair

$$(h(x) = x^2 + 3x + 1, g(x) = x^3 + 2x^2 + 4x + 2).$$

Suppose that $m(x) = x^3 + x + 2$ be a polynomial in the complete residue system modulo $\eta(x) = x^5 + x^3 + x^2 + 2$ $\mathbf{Z}_5[x]/< x^5 + x^3 + x^2 + 2>$. To encrypt the message $m(x)$, entity $B$ reduces in $\mathbf{Z}_5[x]$ the polynomial

$$c(x) \equiv m^2(x) \equiv x^4 + 3x^3 + x^2 + 2x + 4 \pmod{x^5 + x^3 + x^2 + 2}.$$

Hence, the ciphertext is $c(x) = x^4 + 3x^3 + x^2 + 2x + 4$.

To decrypt the ciphertext message sent by entity $B$, entity $A$ should use algorithm 2 to find the four polynomial square roots $m_1(x)$, $m_2(x)$, $m_3(x)$, and $m_4(x)$ in $\mathbf{Z}_5[x]$. Applying algorithm 2, we have that the original message is one of the following polynomials:

$$m_1(x) = 2 + x + x^3,$$
$$m_2(x) = 4 + 4x + 2x^2 + 4x^4,$$
$$m_3(x) = 1 + x + 3x^2 + x^4,$$
$$m_4(x) = 3 + 4x + 4x^3.$$

Finally, entity $A$ somehow decides that $m(x) = x^3+x+2$ of those square roots is the original message.

## 5 Conclusion

Using arithmetics in rings of polynomials over finite fields, $\mathbf{Z}_p[x]/<h(x)>$, where $p$ is an odd prime and $h(x)$ is an irreducible polynomial in $\mathbf{Z}_p[x]$ of degree $n$, Rabin public-key encryption scheme was modified from the domain of natural integers to $\mathbf{Z}_p[x]/<h(x)>$. The computational procedures in the new setting were described and the advantages of the new scheme were pointed out. The following are some of these advantages: First, generating the odd prime $p$ in both the classical and the modified methods requires the same amount of efforts. The complete residue system $\mathbf{Z}_n$ has $pq$ elements, while the complete residue system $\mathbf{Z}_p[x]/<h(x)>$ has $p^n$ elements. Therefore, the modified method provides an extension to the range of chosen messages, which makes trials more complicated. The computations involved in the modified method do not require computational procedures that are much different from those used in the classical method. Rabin encryption involves a single modular squaring and that makes it extremely fast operation. Rabin decryption is not as fast as encryption, but comparable in speed to other cryptosystems such as RSA decryption.

A drawback of Rabin public-key scheme is the task of selecting the correct message from among the four possibilities. This can be overcome by adding some prespecified redundancy to the original message before encryption. For example, the last few digits of the message may be replicated. Then, the one square root of the four which possesses this redundancy will be selected. Another drawback of Rabin public-key scheme in $F[x]$ is the determination of the two irreducible polynomials. However, the extra security provided by the modified method justifies the additional effort.

## Refrences


[1] Y. A. Awad, "M.S. Thesis", Beirut Arab University, 2002.

[2] A. N. El-Kassar, "Doctorate Dissertation", University of Southwestern Louisiana, 1991.

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

[4] A. N. El-Kassar, Ramzi A. Haraty, "ElGamal Public-Key Cryptosystem Using Reducible Polynomials Over a Finite Field", IASSE 2004, pp. 189-194, 2004.

[5] J. A. Gallian, "Contemporary abstract algebra", 4th edition, Houghton Mifflin Company, Boston, 1998.

[6] Ramzi A. Haraty, Hadi Otrok, A. N. El-Kassar, "A Comparative Study of ElGamal Based Cryptographic Algorithms", ICEIS vol. 3 , pp. 79-84, 2004.

[7] Ramzi A. Haraty, A. N. El-Kassar, Hadi Otrok, “A Comparative Study of RSA Based Cryptographic Algorithms”, IASSE 2004, pp. 183-188, 2004.

[8] A. R. Kenneth, "Elementary number theory and its applications", AT&T Bell Laboratories in Murray Hill, New Jersey, 1988.

[9] Badrie Kojok, A.N. El-Kassar, Fida Raad, “Elgamal Signature Scheme In The Domain Of Gaussian Integers”, RTST 2002, pp. 275-282, 2002.

[10] A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC press, 1997.