Kỷ yếu Hội nghị Quốc gia lần thứ VIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR); Hà Nội, ngày 9-10/7/2015
DOI: 10.15625/vap.2015.000201

RISKE, A NOVEL CPA-SECURE SECRET-KEY ENCRYPTION SCHEME BASED-ON INVERTIBLE ELEMENTS IN BINARY QUOTIENT POLYNOMIAL RINGS

Cao Minh Thắng[1], Nguyễn Bình[1]
[1] Học viện Công nghệ Bưu chính Viễn thông
thangcm@ptit.edu.vn; nguyenbinh@ptit.edu.vn

ABSTRACT *- Invertible elements in quotient polynomial rings have been exploited to construct some interesting public-key cryptosystems such as NTRU and pNE. In this paper, we first introduce a special class of binary quotient polynomial rings in which the set of invertible elements is very large. By exploiting that set, we propose a novel a secret-key encryption scheme which not only operate efficiently but also secure under the chosen plain-text attack (or CPA-secure).*

Keywords *- CPA-secure, secret-key, cryptosystem, invertible elements, binary quotient polynomial rings.*

I. INTRODUCTION

The applications of invertible elements in polynomial rings $R_{n,q} = Z_q[x]/(x^n - 1)$ in cryptography are typically in constructing a famous probabilistic public-key cryptosystem NTRU [4] and some variants such as CTRU [6] and especially pNE [5] which operates in $R_{2^s,q} \mid s \in Z^+$ and is so far the unique provably-secure variant of NTRU.

The advantage of using invertible elements in encryption schemes is the computation speed. The modular multiplication in polynomial rings $R_{n,q}$ take $O(n^2)$ operations. By exploiting this feature, along with security related to some hard problems over lattices, NTRU is faster and generally considered as a reasonable alternative to the encryption schemes based on integer factorization and discrete logarithm over finite fields and elliptic curves and is standardized in IEEE P.1363.1 standard in 2008.

Binary quotient polynomial rings $R_{n,2} = Z_2[x]/(x^n + 1)$, a class of $R_{n,q}$, although popularly used in error-correcting codes, have been not widely applied in cryptography except a special class of special class of $R_{n,2}$ where $n = 2^N \mid N \in Z^+$. In 2002, the cyclic multiplicative groups in $R_{2^N,2}$ are exploited to propose a secret-key cryptosystem and in [7] which is then developed as a new variant of DES in [8].

In section III we show that there is a large set of invertible elements in $R_{n,2} = Z_2[x]/(x^n + 1)$ where $n = 2^N \mid N \in Z^+$ (Theorem 1) and propose an efficient algorithm for computing inverse in those rings. By exploiting that set, in section IV, we construct a novel probabilistic secret-key encryption scheme, named RISKE, which is fast and proved secure under the chosen plain-text attacks (CPA-secure) (Theorem 3). The conclusion and proposal about further research is mentioned in Section V.

II. PRELIMINARIES

In this section, we firstly recall some notions about provably secure encryption scheme. Besides, the binary quotient polynomial rings is introduced as a necessary background for the next parts.

A. EAV-secure and CPA-secure encryption schemes

Definition 1: An encryption scheme, denoted by $\Pi(\mathcal{G},\mathcal{E},\mathcal{D},\mathcal{K},\mathcal{P},\mathcal{C})$, *is constructed by three algorithms* $\mathcal{G}$ *(key generation)* $\mathcal{E}$ *(encryption) and* $\mathcal{D}$ *(decryption) along with three spaces* $\mathcal{P}$ *(plain-text space),* $\mathcal{C}$ *(cipher-text place) and* $\mathcal{K}$ *(key space).*

Definition 2 (definition 3.4 [1]*): With variable* $n \in Z^+$, *a function* $f(n)$ *is called* negligible *if for every polynomial* $p(n)$ *there exists an integer* N_0 *such that for all* $n > N_0$ *it holds that* $f(n) < \frac{1}{p(n)}$.

Proposition 1: 2^{-n}, $2^{-\sqrt{n}}$ *and* $n^{-\log n}$ *are all* negligible.

Lemma 1: Function $f(n) = 1/(2^n - 1)$ *is* negligible.

Proof: Since $2^{n+1} > 2^n - 1$ with $n \geq 0$, we have $1/(2^n - 1) < 2^{-(n+1)}$. On the other hand, by Proposition 1, 2^{-n} is negligible thus $2^{-(n+1)}$ is also negligible. Hence, for every polynomial $p(n)$ there exists an integer N_0 such that for all $n > N_0$ it holds that

$$2^{-(n+1)} < \frac{1}{p(n)} \text{ and thereby } \frac{1}{2^n - 1} < \frac{1}{p(n)}.$$

According to Definition 2, $f(n) = 1/(2^n - 1)$ is negligible. □

Lemma 2: If $q(n)$ is a polynomial of n then $q(n).2^{-n}$ is negligible.

Proof: Since 2^{-n} is negligible, there exists an integer N_0 such that for all $n > N_0$ it holds that $2^{-n} < \frac{1}{p(n)}$ for polynomial $p(n) = q(n).r(n)$ where $r(n)$ is arbitrary. As a result, there always exists an integer N_0 such that for all $n > N_0$ it holds that $q(n).2^{-n} < \frac{1}{r(n)}$ for every $r(n)$ thereby $q(n).2^{-n}$ is negligible. □

Definition 3 ([3]*, page 63* [1]*): The definition of eavesdropping indistinguishability experiment on a secret-key encryption scheme, denoted as* $\text{SecK}^{\text{eav}}_{\mathcal{A},\Pi}(n)$*, is the following procedure.*

1. Adversary $\mathcal{A}$ chooses a pair of message m_0, m_1 of the same length. Notice that the length of m_0, m_1 may be different to n.
2. A key k of the length n is randomly chosen from key-space $\mathcal{K}$ and a random bit $b \leftarrow \{0,1\}$ is chosen. A cipher-text $c \leftarrow \mathcal{E}_k(m_b)$ is computed and given to $\mathcal{A}$. We call c the challenge cipher-text.
3. $\mathcal{A}$ outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise. If $\text{SecK}^{\text{eav}}_{\mathcal{A},\Pi}(n)$ then we say $\mathcal{A}$ succeeded.

Definition 4 ([3]*, page 82* [1]*): The formal definition of CPA indistinguishability experiment on a secret-key encryption scheme, denoted as* $\text{SecK}^{\text{cpa}}_{\mathcal{A},\Pi}(n)$*, is the following procedure.*

1. Adversary $\mathcal{A}$ is given oracle (unlimited) access to $\mathcal{E}_k$ and outputs a pair of message m_0, m_1 of the same length. Notice that the length of m_0, m_1 may be different to n.
2. A key k of the length n is randomly chosen from key-space $\mathcal{K}$, a random bit $b \leftarrow \{0,1\}$ is chosen and a cipher-text $c \leftarrow \mathcal{E}_k(m_b)$ is computed and given to $\mathcal{A}$. We call c the challenge cipher-text.
3. $\mathcal{A}$ continues to have oracle access to $\mathcal{E}_k$ outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise. If $\text{SecK}^{\text{cpa}}_{\mathcal{A},\Pi}(n)$ then we say $\mathcal{A}$ succeeded.

Definition 5 (definition 3.21 [1]*): A secret-key encryption scheme Π has indistinguishable encryptions in the presence of eavesdropper, denoted as EAV-secure, if for all probabilistic-time adversaries $\mathcal{A}$*

$$\Pr[\text{SecK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mu(n)$$

where $\mu(n)$ is negligible.

Definition 6: A secret-key encryption scheme Π has indistinguishable encryptions under a chosen plain-text attack (or CPA-secure) if for all probabilistic-time adversaries $\mathcal{A}$

$$\Pr[\text{SecK}^{\text{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mu(n)$$

where $\mu(n)$ is negligible.

It can be realized that the attack in CPA indistinguishabity experiment, where adversary has unlimited access to encryption procedure $\mathcal{E}$, is stronger than that in eavesdropping one. Hence, we can say, CPA-secure is more secure than EAV-secure.

B. Binary quotient polynomial rings

Definition 7: The binary quotient polynomial ring $R_{n,2} = Z_2[x]/(x^n - 1)$ *is the set of polynomials* f *which have degree smaller than an integer* n *and coefficients in binary rings* Z_2. *For convenience, we denote* $R_{n,2}$ *by* R_n *in which 2 is implicit.*

An element $f \in R_n$ can be represented as $f = \sum_{i=0}^{n-1} f_i.x^i$ in polynomial-form or $f = (f_0, f_1, ..., f_{n-1})$ in vector-form. In R_n, the multiplication operation, denoted by '$*$', is given explicitly as a cyclic convolution product modulo $x^n - 1$. I.e., if $h = f * g$ then h has coefficients

$$h_k = (\sum_{i+j=k \bmod n} f_i.g_j) \bmod 2 \mid 0 \le k \le n-1.$$

The addition operation in R_n is denoted by '$+$' and thus if $h = f + g$ then

$$h = \sum_{i=0}^{n-1} h_i.x^i \mid h_i = (f_i + g_i) \bmod 2.$$

Definition 8: The Hamming weight of arbitrary polynomial R_n *is denoted as* $w(f)$.

Definition 9: In R_n, *a polynomial* $w(f)$ *is invertible if there exists some* g *such that* $f * g = 1$.

Definition 10: The set of polynomials having odd Hamming weight in R_n *is denoted as* I_n.

It is clear that $|I_n| = |R_n|/2 = 2^{n-1}$, that is, the number of polynomials having odd Hamming weight is a half of total number of polynomials in R_n.

Definition 11: The ratio of the number of invertible elements over the total number of polynomials in R_n *is denoted as* K_n.

III. INVERTIBLE ELEMENTS IN $R_n \mid n = 2^N, N \in Z^+$

In this section we show that, in $R_n \mid n = 2^N, N \in Z^+$ denoted by R_{2^N}, all elements having odd Hamming weight is invertible. Specifically, the total number of invertible elements in this ring is 2^{n-1} which is a large function of variable n.

Lemma 3: In R_n, *if* $w(f) = 2k$ *and* $w(g) = 2l$ *where* $k, l \in Z^+$ *then* $w(f + g)$ *is even.*

Proof: By presenting polynomials as $f = \sum_{i=0}^{n-1} f_i x^i$ and $g = \sum_{i=0}^{n-1} g_i x^i$, respectively, we have

$$h = f + g = \sum_{i=0}^{N-1} h_i.x^i$$

where $h_i = (f_i + g_i) \bmod 2$. Since $f_i, g_i \in GF(2)$ then $h_i = 0$ if and only if $f_i = g_i$. Let S denote the set containing the values i such that $f_i = g_i = 1$. It easy to see that

$$w(h) = w(f) - |S| + w(g) - |S| = 2(k + l - |S|). \square$$

In more general, if h is the summation of polynomials having even Hamming weight then $w(h)$ is even.

Lemma 4: In R_n, *if* $w(f)$ *is even then* $\forall g \in R_n$, $w(g * f)$ *is even.*

Proof: Suppose that the presentation of g is $g = \sum_{i=0}^{N-1} g_i x^i$ we have

$$h = g * f = \sum_{i=0}^{n-1} g_i.x^i * f.$$

Since $w(g_i.x^i * f) = g_i.w(f)$ and is thus always even, by Lemma 3, $w(h)$ is even. $\square$

Lemma 5: In R_n, all polynomials having even Hamming weight are not invertible.

Proof: Suppose that $f \in R_n$ is a polynomial having even Hamming weight. By Lemma 5, $\forall g \in R_n$, $w(g*f)$ is always even. Since $w(1)$ then there does not exist any polynomial h such that $w(f*h)=1$. As a result, we can say, f is not invertible in R_n.

As a consequence, the maximum number of invertible elements in R_n is equal to $|I_n| = 2^{n-1}$ and the maximum of K_n is $|I_n|/|R_n| = 1/2$.

Lemma 6: In R_n, if f is a polynomial having $\deg f \le n-2$ and $s = (w(f)+1) \bmod 2.x^{n-1} + f$ then $w(s)$ is always odd.

Proof: Since $\deg f \le n-2$, $w(s) = w(f) + w(g)$ where $g = w(f) \bmod 2.x^{n-1}$. If $w(f)$ is even then $w(f) \bmod 2 + 1 = 1$ and $w(g) = 1$ thereby $w(s)$ is odd. Otherwise, $w(g) = 0$ then $s = f$ and $w(s) = 1$ is also odd. □

Theorem 1: In R_{2^N}, all polynomials in $f \in I_{2^N}$ are invertible. Consequently, the number of invertible elements in those rings is 2^{N-1} and K_{2^N} gets maximum.

Proof: With $n = 2^N$, f can be presented as $f = \sum_{i=0}^{2^N-1} f_i x^i$. Since $f_i \in Z_2$, $f_i^2 = f_i \bmod 2$ and

$$f^2 = (\sum_{i=0}^{2^N-1} f_i x^i)^2 = \sum_{i=0}^{2^N-1} (f_i x^i)^2 = \sum_{i=0}^{2^N-1} f_i^2 (x^i)^2 = \sum_{i=0}^{2^N-1} (f_i \bmod 2).x^{2.i \bmod 2^N}$$

thereby

$$f^{2^N} = (\sum_{i=0}^{2^N-1} f_i x^i)^{2^N} = \sum_{i=0}^{2^N-1} (f_i \bmod 2).x^{2^N.i \bmod 2^N} = \sum_{i=0}^{2^N-1} (f_i \bmod 2) = w(f) \bmod 2.$$

If $f \in I_{2^N}$ then $w(f)$ is odd thus $w(f) \bmod 2 = 1$. As a result, $f^{2^N} = 1$. Let $g = f^{2^N-1}$ we have $g*f = 1$ and g is the inverse of f in R_{2^N}. Since $|I_{2^N}| = 2^{N-1}$, $K_{2^N} = 1/2$ and gets maximum. □

For example, when $N = 2$, in R_4, there are totally 16 polynomials including zero and I_4 consists of 8 elements

$$\{1, x, x^2, x^3, 1+x+x^2, 1+x+x^3, 1+x^2+x^3, x+x^2+x^3\}$$

with 8 corresponding inverses

$$\{1, x^3, x^2, x, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2, 1+x+x^3\}.$$

In [2], I_{2^N} is proved a cyclic multiplicative group and 2^N is pointed out the maximum order of all polynomials $f \in R_{2^N}$ i.e., $\text{ord}(f)$ divides 2^N. Hence, we can find the inverse of f more efficiently by the following algorithm instead of computing $g = f^{2^N-1}$.

Algorithm 1: Algorithm for finding the inverse of invertible element in R_{2^N}

INPUT: A polynomial $f \in I_{2^N}$.

OUTPUT: A polynomial $g \in I_{2^N}$ such that $g*f = 1$.

ALGORITHM:

1. Set $f \leftarrow g$.
2. Set $a \leftarrow f^2 \bmod 2$.
3. For i from 1 to $n-1$ do
   a. If $f*g = 1$ return g.
   b. Set $g \leftarrow g*a$.

c. Set $a \leftarrow a^2$.

For example, in R_8 , to find the inverse of $f = x^5 + x^4 + x^3$, because $ord(f) = 2^2 = 4$ using above algorithm, we can compute $g = f^3$, at step $i = 2$, instead of computing $g = f^7$.

IV. RISKE CRYPTOSYSTEM

In section II.III, we see that, all polynomial having odd Hamming weight in R_{2^N} are invertible. By exploiting this feature, in this section we propose a new probabilistic secret-key encryption scheme, called RISKE (Random Invertible Secret-Key Encryption scheme), which is then proved CPA-secure. The underlying algebraic structure of RIKSE is summarized in Table 1.

Table 1: Underlying algebraic structure and theoretical performance analysis of RISKE

Parameters	Value
Polynomial ring	$R_L = Z_2[x]/(x^L + 1) \mid L = 2^l, l \in Z^+$
Key space	$\mathcal{K} = \{k \in I_L \mid 0 < \deg k \le N - 1\}$
Key-size	$N < L$
Plain-text space	$\mathcal{P} = \{m \in R_L \mid \deg m \le L - 1\}$
Plain-text length	$L - 1$
Cipher-text space	$\mathcal{C} = R_L$
Cipher-text length	L

A. Key generation

With $\mathcal{K} = \{I_L \mid 0 < \deg k \le n - 1\}$, sender and receiver share a random invertible polynomial $k \in \mathcal{K}$ as common secret-key. Since, $\deg k \le n - 1$ we can present k by n bits thereby key-space.

The condition $\deg k > 0$ is to ensure that we cannot use $k = 1$ as secret-key in RISKE. Consequently,

$$|\mathcal{K}| = 2^{n-1} - 1 .$$

B. Encryption

To encrypt $(L-1)-bits$ plain-text m , the sender first computes $L-bits$

$$M = \big(w(m) + 1\big) \bmod 2 . x^{L-1} + m \tag{1.1}$$

then outputs $L-bits$ cipher-text

$$c = M * k \tag{1.2}$$

Notice that, by Lemma 6, $w(M)$ is always odd thereby, according to Theorem 1, both M and c are invertible in R_L .

C. Decryption

To decrypt $L-bits$ cipher-text c , receiver first computes $L-bits$

$$M = c * k^{-1} \tag{1.3}$$

where k^{-1} is inverse of k in R_L obtained by Algorithm 1, thereby recovers $(L-1)-bits$ plain-text as

$$m = M_{L-1} . x^{L-1} + M \tag{1.4}$$

where M_{L-1} is the coefficient of monomial x^{L-1} in polynomial presentation of M .

D. A small example

Sender and receiver choose $L = 2^3 = 8$ and $N = 5$ to construct RIKSE.

1. Key generation

Sender and receiver share $5-bits$ secret-key $k = (00111)$ in binary form or $k = x^2 + x + 1$ in polynomial form. Notice that $w(k) = 3$ and the inverse k^{-1} of k in R_8 , computed by Algorithm 1, is $k^{-1} = k^7 = x^7 + x^5 + x^4 + x^2 + x$.

2. Encryption

To encrypt $7-bits$ plain-text message $m=(1010011)$ in binary form or $m=x^6+x^4+x+1$ in polynomial form, sender firstly, by (1.1), computes $8-bits$ $M=x^7+x^6+x^4+x+1$ and then, by (1.2), sends $8-bits$ cipher-text

$$c=M*k=x^5+x^4+x^3+x+1$$

in polynomial form or $c=(00111011)$ in binary-form to receiver.

3. Decryption

To decrypt $8-bits$ cipher-text message $c=(00111011)$, receiver firstly, by (1.3), computes $8-bits$

$$M=k^{-1}*c=x^7+x^6+x^4+x+1$$

and then, by (1.4), with $M_7=1$, recovers $7-bits$ cipher-text

$$m=x^7+(x^7+x^6+x^5+x+1)=x^6+x^4+x+1.$$

E. Theoretical security analysis

1. Security under the eavesdropping indistinguishability experiment

Theorem 2: RISKE encryption scheme is EAV-secure.

Proof: Recall that, given $c=M*k$ we can get $M=k^{-1}*c$ where k^{-1} is inverse of k. Although $\mathcal{A}$ does not have secret-key, $\mathcal{A}$ can try each $k\in\mathcal{K}$ to compute M'. Hence, the probability for $\mathcal{A}$ decrypts successfully is

$$\Pr[M'=M]=\Pr[k^{-1}*c=M]=\Pr[k^{-1}=M*c^{-1}]$$

where c^{-1} is the inverse of c in R_L.

Since k is chosen randomly in $\mathcal{K}$ while M' and c^{-1} are fixed. Consequently,

$$\Pr[M'=M]=\Pr[k^{-1}=M*c^{-1}]=\frac{1}{|\mathcal{K}|}.$$

In the EAV-experiment, with $c=M_b*k$ received from encryption procedure, adversary $\mathcal{A}$ can obtain $b'=b$ by simply guessing with success probability 1/2 or trying all $k\in\mathcal{K}$ to compute $M=k^{-1}*c$ until $M=M_b$. Suppose that $\mathcal{A}$ has to try $p(N)$ times to obtain $M=M_b$, where $p(n)$ is a polynomial function of N to make sure that this attack can be deployed in polynomial time, we have

$$\Pr[\mathrm{SecK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]=\frac{1}{2}+p(n).\big(\Pr[M=M_0].\Pr[b=0]+\Pr[M=M_1].\Pr[b=1]\big)$$

$$=\frac{1}{2}+p(n).\left(\frac{1}{2|\mathcal{K}|}+\frac{1}{2|\mathcal{K}|}\right)=\frac{1}{2}+\frac{p(n)}{|\mathcal{K}|}=\frac{1}{2}+\frac{p(n)}{2^{n-1}-1}.$$

Since $p(n)$ is still a polynomial, by Lemma 1,

$$\frac{p(n)}{2^{(n-1)}-1}$$

is a negligible. As a result, according to Definition 5, RISKE encryption scheme is EAV-secure. □

2. Security under the CPA indistinguishability experiment

Theorem 3: RISKE encryption scheme is CPA-secure.

Proof: Recall that, given a pair of cipher-text c and corresponding plain-text M_b from encryption procedure and if we have $c'=M_b*k$ then

$$\Pr[c'=c]=\Pr[c=M_b*k]=\Pr[k=c^{-1}*M_b^{-1}],$$

where M_b^{-1} is the inverse of M_b in R_l.

In addition, since k is chosen randomly in $\mathcal{K}$ while M_b^{-1} and c^{-1} are fixed,

$$\Pr[c' = c] = \Pr[k = c^{-1} * M_b^{-1}] = \frac{1}{|\mathcal{K}|}$$

In CPA indistinguishing experiment, adversary $\mathcal{A}$ can obtain $b' = b$ by one of two following ways:

1) Using the same algorithm to find b in EAV distinguishing experiment;
2) Randomly choosing $b \in \{0,1\}$ and querying encryption algorithms $q(n)$ times with input M_b to get output c' until reaching $c' = c$. Notice that $q(n)$ is a polynomial function of n to make sure that this attack can be deployed in polynomial time.

Thus, we have

$$\begin{aligned}\Pr[\mathrm{SecK}^{\mathrm{cpa}}_{\mathcal{A},\Pi}(n) = 1] &= \Pr[\mathrm{SecK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1] + q(n).\Pr[c' = c] \\ &= \Pr[\mathrm{SecK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1] + q(n).\frac{1}{|\mathcal{K}|} \\ &= \frac{1}{2} + \frac{p(n)+q(n)}{|\mathcal{K}|} = \frac{1}{2} + \frac{p(n)+q(n)}{2^{n-1}-1}.\end{aligned}$$

Since $g(n) = p(n) + q(n)$ is also a polynomial, by Lemma 1 and Lemma 2,

$$\frac{g(n)}{2^{(n-1)}-1}$$

is a negligible. Therefore, according to Definition 6, RISKE encryption scheme is CPA-secure. □

F. Theoretical performance analysis

The important advantage of RISKE is computation speed, both algorithms for encryption and decryption of RISKE are one modular polynomial addition and one multiplication in R_L and cost $\mathrm{O}(L^2)$ bit operations.

The disadvantage of RIKSE is that we must choose $k \in \mathcal{K}$ uniformly at random i.e., each session needs a random and fresh secret-key shared between sender and receiver. By this reason, RIKSE should be used in combination with some public-key encryption scheme to construct a hybrid cryptosystem in which long plain-text message is encrypted by RIKSE while the random secret-key for each session is encrypted by associated public-key cryptosystem. That hybrid encryption scheme will inherits both the convenience of asymmetric-key cryptosystem and the efficiency of symmetric one.

G. Parameter selection

Since RISKE is CPA-secure, the probability for adversaries to break RIKSE is negligible. However, to prevent brute-force attack, the value N must be large enough. For practical application we propose N at least 1024 thereby $l > 10$. In that case, the key-security and message-security of RISKE are at least $2^{N-1} = 2^{1023}$. For applications requiring high security, we recommend N is about 4096.

Besides, the larger is L than N, the more efficient is RISKE. Hence, in practice, we can use RISKE to enhance the efficiency of public-key cryptosystem having large message-expansion factor such as NTRU and pNE.

V. CONCLUSION

As mentioned above, although RISKE is efficient, for practice uses, choosing a suitable public-key cryptosystem to encrypt and share the random secret-key is an interesting issue for future works. Besides, since RISKE is based-on I_n finding other classes of quotient polynomial rings R_n which have large K_n (i.e., maximum or nearly maximum) is another open topic for our further research.

VI. REFERENCES

[1] Jonathan Katz, Yehuda Lindell (2007), Introduction to Modern Cryptography: Principles and Protocols, Chapman & Hall/CRC Cryptography and Network Security Series.

[2] Nguyen Binh, Le Dinh Thich (2002), The order of polynomials and algorithms for defining the order of polynomial over polynomial rings, VICA-5, Hanoi, Vietnam.

[3] S. Goldwasser and S. Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28(2) :270-299, 1984.

[4] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: Alice ring-based public key cryptosystem. Lecture Notes in Computer Science Volume 1423, pp 267-288, Springer Verlag 1998.

[5] Stehle, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Paterson, K.G.(ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg (2011).

[6] Gaborit, P., Ohler, J., Sole, P.: CTRU, a Polynomial Analogue of NTRU, INRIA. Rapport de recherche, N.4621 (November 2002), (ISSN 0249-6399).

[7] Nguyễn Bình. Crypto-system based on cyclic geometric progressions over polynomial ring (Part I). REV'02.2002.

[8] Hồ Quang Bửu, Ngô Đức Thiện, Trần Đức Sự. Xây dựng hệ mật trên các cấp số nhân cyclic của vành đa thức, Tạp chí Khoa học và Công nghệ, Chuyên san năm thứ 3, Học viện Công nghệ Bưu chính viễn thông số 50 (2A), 2012, trang 109-119.

RISKE, MỘT SƠ ĐỒ MẬT MÃ AN TOÀN VỚI CÁC TẤN CÔNG BẰNG BẢN RÕ ĐƯỢC CHỌN DỰA TRÊN CÁC PHẦN TỬ KHẢ ĐẢO TRONG VÀNH ĐA THỨC NHỊ PHÂN CÓ BẬC HỮU HẠN

Cao Minh Thắng, Nguyễn Bình

TÓM TẮT *- Các phần tử khả nghịch trong vành đa thức có bậc hữu hạn đã được khai thác để xây dựng một số hệ mật khá thú vị như NTRU hay pNE. Trong bài báo này, trước tiên, chúng tôi sẽ giới thiệu một lớp đặc biệt của các vành đa thức có bậc hữu hạn và hệ số nhị phân, trong đó, tập các phần tử khả nghịch là rất lớn. Bằng cách khai thác tập các phần tử này, chúng tôi đề xuất một sơ đồ mật mã khóa bí mật mới không những có hiệu quả mã hóa cao mà còn an toàn với các tấn công bằng bản rõ được chọn (hay còn gọi là CPA-secure).*