Secure communication applications of the Chinese remainder theorem

Wei Wang*
College of Sciences
Xi'an Shiyou University
Xi'an, 710065
P. R. China
wwmath@xsyu.edu.cn

Peng Xi Yang
College of Sciences
Xi'an Shiyou University
Xi'an, 710065
P. R. China
1054088317@qq.com

Yao Xing
Xi'an Presicion Machinery Research Institute
Xi'an, 710075
China
310513842@qq.com

Abstract. In this paper, we extend the Chinese remainder theorem in the number theory to several applications: (1) Lagrange interpolation formula is proved to be an extension of the Chinese remainder theorem in the polynomial ring. (2) By applying The Chinese Remainder Theorem in distributive lattice, a communication scheme is proposed. (3) Adjusting and combing the Chinese remainder theorem with RSA public-key cryptosystem, a dynamic secure communication on identity is proposed.

Keywords: chinese remainder theorem, secure communication, polynomial ring, distributive lattice.

1. Introduction

With the widely application of the computer and the continuous development of network, communication system security problems cannot be ignored. The inherent openness and limitations of network makes the security problem increasingly obvious [2,3].

To protect information security has become the consensus of the whole society. Great attention and commitment have been given to the communication security system.

∗. Corresponding author

In order to prevent information security risks, new security technology and standard constantly appear. Encryptography also get great development as the key technology in recent years [4,5,10-11].

The Chinese remainder theorem in number theory is essentially solving the congruence equations. In the modern number theory, the Chinese remainder theorem theory is of great importance, and also gains some applications in several different algebras [1,6,13]. Besides the theoretical applications, the Chinese remainder theorem theory also gains some applications in information security. For example, [10] constructed a secret sharing schemes based on Chinese Remainder Theorem.

Ring and lattice theory play a vital role as branches of algebra and in recent years, and significance of ring and lattice theory also become gradually apparent as their applications occur in many fields [9,12,14-15].

Lagrange's interpolation formula includes interpolation by vector polynomials and by rational vector functions with prescribed pole characteristics. The formula is applied to obtain representations of the inverses of CauchyVandermonde matrices generalizing former results. The shamir threshold scheme and some password authentication schemes in encryptography are essentially based on Lagrange interpolation formula [2,3].

Just as normal subgroups play a crucial role in the theory of groups, ideals play an analogous role in the study of rings and lattice. The theory of ideals functions well not only in algebras, but also in Computer Science. Nowadays, ideals of different algebras were further studied.

In this paper, after Lagrange interpolation formula is proved just by extending the Chinese remainder theorem to the polynomial ring, we further construct a dynamic secure communication scheme on identity by extending the Chinese remainder theorem to distributive lattice.

The outline of this paper is organized as follows. In Section 2, preliminaries of definitions and results are given. In Section 3, based on the Chinese Remainder Theorem in Number Theory, Lagrange interpolation formula is proved to be as an expression of the Chinese Remainder Theorem in the polynomial ring. In Section 4, the Chinese Remainder Theorem in distributive lattice are constructed and applied to secure communication application. In Section 5, an identity-based dynamic secure communication scheme is proposed.

2. Preliminaries

Definition 2.1 ([12])**.** A ring is a nonempty set R together with two binary operations (usually denoted as addition (+) and multiplication) such that

(1) $(R, +)$ is an abelian group;

(2) $(ab)c = a(bc)$ for all $a, b, c \in R$ (associative multiplication);

(3) $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ (left and right distributive laws).

If in addition: $ab = ba$ for all $a, b \in R$, then R is said to be a commutative ring. If R contains an element 1_R such that $1_R a = a1_R = a$ for all $a \in R$, then R is said to be with identity.

Definition 2.2 ([8], the Chinese remainder theorem)**.** Suppose $n \geq 2$, and $m_1, m_2, \ldots, m_n$ are n positive mutually prime integers. Let $M = m_1 m_2 \ldots m_n = m_1 M_1 = m_2 M_2 = \ldots = m_n M_n$, here $M_i = \frac{M}{m_i}, i = 1, 2, \ldots, n$, then for the following congruence equations group

$x \equiv b_1 (\mathrm{mod}\ m_1)$,
$x \equiv b_2 (\mathrm{mod}\ m_2)$,
$\vdots$
$x \equiv b_n (\mathrm{mod}\ m_n)$,

the minimum solution is $x_0 = b_1 M_1' M_1 + b_2 M_2' M_2 + \ldots + b_n M_n' M_n (\mathrm{mod}\ M)$, here positive integer M_i' satisfying: $M_i' M_i \equiv 1 (\mathrm{mod}\ m_i), (i = 1, \ldots n)$ i.e., M_i' is the inverse element of M_i with respect to m_i.

Definition 2.3 ([12])**.** Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R. If S is itself a ring under these operations then S is called a subring of R. A subring I of a ring R is a left ideal provided $r \in R$ and $x \in I \Rightarrow rx \in I$. I is a right ideal provided $r \in R$ and $x \in I \Rightarrow xr \in I$. I is an ideal if it is both a left and right ideal.

Theorem 2.4 ([12], Chinese Remainder Theorem on ring)**.** *Let $A_1, \ldots, A_n$ be ideals in a ring R, such that $R^2 + A_i = R$ for all i, and $A_i + A_j = R$ for all $i \neq j$. If $b_1, \ldots, b_n \in R$, then there exists $b \in R$ such that $b \equiv b_i (mod\ A_i)(i = 1, \ldots n)$. Furthermore b is uniquely determined up to congruence modulo ideal $A_1 \cap A_2 \cap \ldots \cap A_n$.*

Remark 2.5. If R has an identity, then $R^2 = R$, whence $R^2 + A = R$ for every ideal A of R.

Definition 2.6 ([15])**.** A nonempty set L with binary operations $\wedge$ and $\vee$ is called a lattice if for $x, y, z \in L$:

(1) $x \wedge x = x \vee x = x$,
(2) $x \wedge y = y \wedge x$, $x \vee y = y \vee x$,
(3) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$,
(4) $(x \wedge y) \vee x = (x \vee y) \wedge x = x$.

A binary relation $\leq$ is defined as for $x, y \in L$, $x \leq y$ if $x \wedge y = x$ or $x \vee y = y$. Then we can find that binary relation $\leq$ is a partially ordered relation.

A lattice L is called bounded if there exists $0, 1 \in L$, such that $0 \leq x \leq 1$ for any $x \in L$.

Definition 2.7 ([14])**.** For any $x, y, z \in L$,a lattice L is called distributive if:

(5) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,
(6) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Definition 2.8 ([5], RSA public-key system)**.** RSA is one of the best secure algorithms till now [6].

RSA public-key system:

(1) Choose two large different prime numbers p and q.

(2) Compute $n = pq$, $\varphi(n) = (p-1)(q-1)$.

(3) Find e($1 < e < \varphi(n)$), such that $g.c.d.(e, \varphi(n)) = 1$, set e as public encryption key.

(4) Compute d, such that $de \equiv 1(\text{mod } \varphi(n))$, set d as confidential decryption key.

(5) Encryption process: for plain text $m \in Z_n$, cipher text c is $c = m^e \text{mod } n$.

(6) Decryption process: for cipher text $c \in Z_n$, plain text m is $m = c^d \text{mod } n$.

Definition 2.9 ([12], Lagrange interpolation formula)**.** Suppose $X_i = (x_{i1}, x_{i2}, \ldots, x_{in})(i = 1, 2, \ldots, m)$, then there exists a polynomial $f_i(x)$, such that $f_i(x_j) = x_{ij}(i = 1, 2, \ldots, m, j = 1, 2, \ldots, n)$. If we define so-called Lagrange basic polynomial $l_p(x)$ as $l_p(x) = \prod_{p,p\neq q} \frac{x-q}{p-q}, (p = 1, 2, \ldots, n)$. Let $f_i(x) = \sum_p l_p(x)x_{ip}(i = 1, 2, \ldots, m, j = 1, 2, \ldots, n)$, then we can find that $f_i(j) = x_{ij}(i = 1, 2, \ldots, m, j = 1, 2, \ldots, n)$. $f_i(x)$ is called Lagrange interpolation polynomial.

3. The Chinese remainder theorem of polynomials ring-Lagrange interpolation formula

Lagrange interpolation formula is constructed usually from a Lagrange basic polynomial. In fact, Lagrange interpolation formula can be proved to be as an expression of the Chinese Remainder Theorem in the polynomial ring as the following.

Theorem 3.1. *Suppose $n \geq 2$, and $x - x_1, x - x_2, \ldots, x - x_n$ are n positive mutually prime polynomials, Let $X = (x-x_1)(x-x_2)\ldots(x-x_n) = (x-x_1)X_1 = (x-x_2)X_2 = \ldots = (x-x_n)X_n$, then for the following congruence equations group:*

$$F(x) \equiv F(x_1) mod\,(x - x_1),$$
$$F(x) \equiv F(x_2) mod\,(x - x_2),$$
$$\vdots$$
$$F(x) \equiv F(x_n) mod\,(x - x_n),$$

the minimum degree polynomial solution is $F(x) = F(x_1)X_1'X_1 + F(x_2)X_2'X_2 + \ldots + F(x_n)X_n'X_n = \sum_i F(x_i)\frac{\prod_{j,j\neq i}(x-x_j)}{\prod_{j,j\neq i}(x_i-x_j)}$, here polynomial solution X_i' satisfied $X_i'X_i \equiv 1(mod\ -x_i), (i = 1, 2, \ldots, n)$ i.e.,X_i' is the inverse element of X_i with respect to $x - x_i$.

Lemma 3.2. *Let $X_i = \prod_{j,j\neq i}(x - x_j)$,then the corresponding inverse element X_i' of X_i is $X_i' = \frac{1}{\prod_{j,j\neq i}(x_i-x_j)}(i = 1, 2, \ldots, n)$.*

Proof. $X_iX_i' \text{mod } (x - x_i) = X_iX_i'|_{x=x_i} = \frac{\prod_{j,j\neq i}(x-x_j)}{\prod_{j,j\neq i}(x_i-x_j)}|_{x=x_i} = \frac{\prod_{j,j\neq i}(x_i-x_j)}{\prod_{j,j\neq i}(x_i-x_j)} = 1$
The theorem holds by the uniqueness of X_i'. □

Remark 3.3. Lagrange interpolation formula can be proved to be as an expression of the Chinese Remainder Theorem in the polynomial ring. If the modules are set properly, some other important interpolation formula can also obtained as an expression of the Chinese Remainder Theorem in the polynomial ring.

4. The Chinese remainder theorem in distributive lattice

4.1 Congruence relation on ideals of distributive lattice

Definition 4.1 ([15])**.** A nonempty subset I of a lattice L is called an ideal of L if it satisfies

(1) $x \in L$, $y \in I$, $x \leq y \Rightarrow y \in I$,

(2) $x \in I$, $y \in I \Rightarrow x \vee y \in I$.

Theorem 4.2. *Suppose I be an ideal of a distributive lattice L. A binary relation $\equiv$ is defined as for $\forall a, b \in L$, $a \equiv b(mod\, I)$ if for some $d \in I$, $a \vee d = b \vee d$, then the binary relation $\equiv$ is a congruence relation on L.*

Proof. It is easy to see that binary relation $\equiv$ has reflexivity and symmetry.

Suppose for $a, b, c \in L$, $a \equiv b(\text{mod } I)$ and $b \equiv c(\text{mod } I)$, then there exist $d, e \in I$, such that $a \vee d = b \vee d$, $b \vee e = c \vee e$. So $a \vee (d \vee e) = b \vee d \vee e = b \vee e \vee d = c \vee (d \vee e)$, and $d \vee e \in I$, then $a \equiv c(\text{mod } I)$. So binary relation $\equiv$ is an equivalent relation.

Suppose $a \equiv b(\text{mod } I)$, then there exists some $d \in I$, such that $a \vee d = b \vee d$, then $\forall c \in L$, $(a \vee d) \vee c = (b \vee d) \vee c$, i.e., for some $d \in I$, $(a \vee c) \vee d = (b \vee c) \vee d$, then $a \vee c \equiv b \vee c(\text{mod } I)$.

In the same way, $a \equiv b(\text{mod } I)$, then there exists some $d \in I$, such that $a \vee d = b \vee d$, then $\forall c \in L$, $(a \wedge c) \vee d = (a \vee d) \wedge (c \vee d) = (b \vee d) \wedge (c \vee d) = (b \wedge c) \vee d$, then $a \wedge c \equiv b \wedge c(\text{mod } I)$.

Suppose $a \equiv b(\text{mod } I)$ and $c \equiv d(\text{mod } I)$, then $a \vee c \equiv b \vee c(\text{mod } I)$ and $b \vee c \equiv b \vee d(\text{mod } I)$, so $a \vee c \equiv b \vee d(\text{mod } I)$.

In the same way, we can get $a \wedge c \equiv b \wedge d(\text{mod } I)$. □

Remark 4.3. Suppose I be an ideal of a distributive lattice L. A congruence relation $\equiv$ can be induced by I. If we use $[x]_I$ to denote the equivalent class of $x \in L$, i.e., $L/I = \{[x]_I | x \in L\}$. If we define $[x]_I \vee [y]_I = [x \vee y]_I$, $[x]_I \wedge [y]_I = [x \wedge y]_I$, then $(L/I, \wedge, \vee)$ is a distributive lattice.

Theorem 4.4. *Suppose I be an ideal of a lattice L. If $a \in I$, then $[a]_I = I$.*

Proof. Suppose for $x \in [a]_I$, there exist $d \in I$, such that $x \vee d = a \vee d$, since $x \leq x \vee d = a \vee d \in I$. So $x \in I$. On the other hand, if $x \in I$, then $x \vee a \in I$, since $x \vee (x \vee a) = a \vee (x \vee a)$, then $x \equiv a(\text{mod } I)$, i.e., $x \in [a]_I$. □

Corollary 4.5. *Suppose I be an ideal of a lattice L. If $a \in I$, then $\forall d \in L$, $a \equiv a \wedge d(mod\, I)$.*

Proof. $\forall d \in L$ and $a \in I$, $a \vee a = (a \wedge d) \vee a$, so $a \equiv a \wedge d (\text{mod } I)$. □

Definition 4.6. Suppose I_1, I_2 be two ideals of a lattice L. An ideal I generated by $I_1 \cup I_2$ is called the sum of ideals I_1 and I_2, denoted by $I = I_1 + I_2$.

Lemma 4.7. *Suppose I_1, I_2 be two ideals of a lattice L. Then $I_1 + I_2 = \{x|$ for some $a \in I_1, b \in I_2, x \leq a \vee b\}$.*

Proof. Suppose $I = \{x|$ for some $a \in I_1, b \in I_2, x \leq a \vee b\}$, then any ideal J containing I_1, I_2 must contain I: if $x \in I$, then for some $a \in I_1$, $b \in I_2$, $x \leq a \vee b$, $x \leq a \vee b \in J$, we get $x \in J$. i.e., $I \subseteq J$. And we have $I_1 + I_2 \supseteq I$.

Next we prove that I is an ideal. Suppose $x \leq y$ and $y \in I$, then for some $a \in I_1, b \in I_2, x \leq y \leq a \vee b$, so $x \in I$. If $x, y \in I$, then for some $a, a_1 \in I_1$, $b, b_1 \in I_2$, we have $x \leq a \vee b$, $y \leq a_1 \vee b_1$, so $x \vee y \leq (a \vee b) \vee (a_1 \vee b_1) = (a \vee a_1) \vee (b \vee b_1)$, and $a \vee a_1 \in I_1$, $b \vee b_1 \in I_2$, we have $x \vee y \in I$.

It is easy to see that $I_1 \subseteq I$, $I_2 \subseteq I$, so $I_1 + I_2 \subseteq I$. □

Corollary 4.8. *Suppose I_1, I_2 be two ideals of a distributive lattice L. Then $I_1 + I_2 = \{a \vee b|$ for some $a \in I_1, b \in I_2\}$.*

Proof. Suppose $x \in I_1 + I_2$, then for some $a \in I_1$, $b \in I_2$, we have $x \leq a \vee b$. And $x = x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b)$, since $x \wedge a \leq a \in I_1$, $x \wedge b \leq b \in I_2$, we get $x \wedge a \in I_1$, $x \wedge b \in I_2$. i.e., $I_1 + I_2 \subseteq \{a \vee b|$ for some $a \in I_1, b \in I_2\}$. And we have $I_1 + I_2 \supseteq \{a \vee b|$ for some $a \in I_1, b \in I_2\}$. □

4.2 The Chinese Remainder Theorem in distributive lattice

Based on the above results, we can construct the Chinese Remainder Theorem in distributive lattice.

Theorem 4.9. *Suppose $I_1, I_2, \ldots, I_n$ be ideals of a distributive lattice L, such that $L = I_k + \bigcap_{i \neq k} I_i, k = 1, \ldots, n$. If $b_1, b_2, \ldots, b_n \in L$, then there exist $b \in L$, such that $b \equiv b_i (mod\ I_i), i = 1, 2, \ldots, n$. And b is uniquely determined with respect to module ideal $I_1 \cap I_2 \cap \ldots \cap I_n$.*

Proof. For every k, $b_k \in L = I_k + \bigcap_{i \neq k} I_i, k = 1, \ldots n$. When $a_k \in I_k$, $r_k \in \bigcap_{i \neq k} I_i$, $b_k = a_k \vee r_k$. On the other hand, $a_k \in I_k$, then $b_k \vee a_k = a_k \vee r_k \vee a_k = r_k \vee a_k$, so $b_k \equiv r_k (\text{mod } I_k), k = 1, \ldots n$. $r_k \in \bigcap_{i \neq k} I_i$, then for all $d \in L$, $r_k \equiv r_k \wedge d (\text{mod } I_i), (i \neq k)$. Let $d = r_i$, then $r_k \equiv r_k \wedge r_i (\text{mod } I_i)(i \neq k)$. Let $b = r_1 \vee r_2 \vee \ldots \vee r_k \vee \ldots \vee r_n \equiv r_1 \vee r_2 \vee \ldots \vee r_k \vee \ldots \vee r_n \equiv (r_1 \wedge r_k) \vee (r_2 \wedge r_k) \vee \ldots \vee r_k \vee \ldots \vee (r_n \wedge r_k) (\text{mod } I_k) \equiv r_k (\text{mod } I_k), (k = 1, 2, \ldots, n)$. So we get $b \equiv b_k (\text{mod } I_k)(k = 1, \ldots n)$.

Then we prove the uniqueness.

Suppose there exist $c \in L$, such that $c \equiv b_k (\text{mod } I_k)(k = 1, \ldots n)$. Then $b \equiv c (\text{mod } I_k)(k = 1, \ldots n)$. So there exists $d_k \in I_k$, such that $b \vee d_k = c \vee d_k, (k = 1, \ldots n)$. $(b \vee d_1) \wedge (b \vee d_2) \wedge \ldots \wedge (b \vee d_n) = (c \vee d_1) \wedge (c \vee d_2) \wedge \ldots \wedge (c \vee d_n)$, i.e., $b \vee (d_1 \wedge d_2 \wedge \ldots \wedge d_n) = c \vee (d_1 \wedge d_2 \wedge \ldots \wedge d_n)$, then we get $b \equiv c (\text{mod } \bigcap_i I_i)$. □

4.3 A new communication scheme based on the Chinese remainder theorem in distributive lattice

Based on the Chinese Remainder Theorem in distributive lattice, we can further propose a secure communication scheme as follows.

Theorem 4.10. *Suppose* $L = \{$*the polynomial space on* $GF(2)\}$*. A binary relation* $\leq$ *is defined as for* $x \leq y, (x, y \in L) \Leftrightarrow y|x$*, then* $(L, \leq)$ *is a partial ordered set.*

Proof. $\forall f(x), g(x), h(x) \in L$,

(1) $f(x)|f(x) \Leftrightarrow f(x) \leq f(x)$;

(2) $f(x)|g(x), g(x)|f(x) \Rightarrow f(x) = g(x) \Leftrightarrow f(x) \leq g(x), g(x) \leq f(x) \Rightarrow f(x) = g(x)$;

(3) $f(x)|g(x), g(x)|h(x) \Rightarrow f(x)|h(x) \Leftrightarrow g(x) \leq f(x), h(x) \leq g(x) \Rightarrow h(x) \leq f(x)$.

$(L, \leq)$ is a partial ordered set. □

Theorem 4.11. *Suppose* $L = \{$ *the polynomial space on* $GF(2)\}$*. For* $\forall f(x)$, $g(x) \in L$, $f(x) + g(x)$ *and* $f(x)g(x)$ *exist, i.e.* L *is a commutative ring. The binary operations* $\vee, \wedge$ *are defined as*

(1) $f(x) \vee g(x) = g.c.d.(f(x), g(x))$*;*

(2) $f(x) \wedge g(x) = l.c.m.(f(x), g(x))$*,*

then $f(x) \vee g(x)$ *and* $f(x) \wedge g(x)$ *exist,* $(L, \vee, \wedge)$ *is a distributive lattice.*

Lemma 4.12. *Suppose* I *be an ideal of a lattice* L*. Then* $I = \{m(x)p(x)|m(x) \in L\}$*, here* $p(x)$ *is the irreducible polynomial on* L*.*

Proof. Suppose $f(x) \in L, g(x)|f(x)$ and $g(x) \in I$, then $g(x) = m_1(x)p(x), f(x) = h(x)g(x) \Rightarrow f(x) = h(x)m_1(x)p(x) \Rightarrow f(x) \in I$, i.e., $f(x) \in L, f(x) \leq g(x)$ and $g(x) \in I$, then we get $f(x) \in I$. On the other hand, $\forall f(x), g(x) \in I, f(x) \vee g(x) \in I$. □

Theorem 4.13. *The unique solution determined by the module*

$$\bigcap_i I_i = \{m(x) \bigcap_i p_i(x), m(x) \in L\}$$

is $F(x) = \sum_j f_j(x) \prod_{i \neq j} p_i(x)$.

Proof. Let $p_i(x) \in I_i$, since $(f_j(x) \prod_{i \neq j} p_i(x)) \vee p_i(x) = 0 \vee p_i(x) = p_i(x)$, we get $f_j(x) \prod_{i \neq j} p_i(x) \equiv 0 (\mathrm{mod}\ I_k)$, and from $(\prod_{i \neq j} p_i(x), p_k(x)) = 1$, we have $u(x)(\prod_{i \neq j} p_i(x)) + v(x)p_k(x) = 1$, then $u(x)(f_k(x) \prod_{i \neq j} p_i(x)) + v(x)f_k(x)p_k(x) = f_k(x)$, so $(f_k(x) \prod_{i \neq j} p_i(x), p_k(x)) = f_k(x)$, by $(f_k(x) \prod_{i \neq j} p_i(x)) \vee p_k(x) = f_k(x) \vee p_k(x)$, we get $(f_k(x) \prod_{i \neq j} p_i(x)) \mathrm{mod}\ I_k = f_k(x)$, for any $k, (k = 1, 2, \ldots, n)$, $F(x) \mathrm{mod}\ I_k = \sum_j f_j(x) \prod_{i \neq j} p_i(x) \mathrm{mod}\ I_k = (f_1 p_2 p_3 \ldots p_n + p_1 f_2 p_3 \ldots p_n + p_1 p_2 p_3 \ldots f_n) \mathrm{mod}\ I_k = f_k(x)$, then $F(x)$ is the unique solution. □

Based on the above analysis, a secure communication scheme can be designed as follows: after the sender and the receiver of the communication chose n modules on L: $I_1, I_2, \ldots, I_n$, the sender can send solution of the congruence equations group $F(x)$ directly through the channel, the receiver can obtain $f_i(x)(i = 1, 2, \ldots, n)$ by $F(x) \bmod I_i$, then the receiver can get original information flow safely and effectively, so as to achieve the requirements of the secure communication.

System only need to transfer $F(x)$ secretly, transfer volume decreases. Even if $F(x)$ is obtained by an intruder, since he couldn't know the module and order, it is difficult to use $F(x)$ to get the original sequence; When the receiver needs to restore sequence, he only needs to perform modular operations, which is simpler and faster.

Remark 4.14. The Chinese Remainder Theorem can be constructed in distributive lattice, not in lattice, because the congruence relation is defined just based on the properties of distributive lattice.

5. Identity based dynamic secure communication scheme

There has been a growing interest in the use of chaotic techniques for enabling secure communication in recent years. The use of Chaotic techniques can enhance communication security, while it is inferior in low bit error rates (BER) performance as compared to conventional communication schemes.

In this section, by constructing the Chinese remainder theorem with respect to ID_j combing RSA public-key cryptosystem, a new kind of secure communication is obtained with the same secure level and less complexity compared with the techniques mentioned above.

Assume that there is n users $u_i, (i = 1, 2, \ldots, n)$ in the system, ID_i is the identifier of u_i (such that $i \neq j, (ID_i, ID_j) = 1$). System Center(SC) chooses two different large prime numbers p and q, and calculate $n = pq$(public), $\varphi(n) = (p-1)(q-1)$(confidential by SC). The system selects encryption key e_i (public)and decryption key d_i(confidential by u_i) for each user u_i, such that $e_i d_i \equiv 1 (\bmod\ \varphi(n))$, and $1 < d_i < ID_i$.

For congruence equation:

$x \equiv d_i (\bmod\ ID_i)$

SC get the solution x_0 (public)based on the Chinese Remainder Theorem. SC chooses Two-way function f(public).

Communication process: Suppose there is a user u_i who will want to communicate with u_j, then u_i get the decryption key d_j(confidential by u_j) by computing $d_j = x_0 \bmod ID_j$, and compute $f^{d_j}(m, T)$, T is the sending time, m is the message. When u_j received $f^{d_j}(m, T)$, he computes $(f^{d_j}(m, T))^{e_j} \bmod n$, then gets T and m. If T meets the requirements, accepts m, otherwise refuses m.

Remark 5.1. The improvement of the secure communication system over the RSA is that on one hand by combing RSA public-key cryptosystem and the Chinese remainder theorem the scheme just stores public x_0 instead of public key list, store volume decreases; on the other hand the scheme keeps the same level security of RSA, while avoids complicated power operations.

6. Conclusion

Based on the Chinese remainder theorem of polynomials, Lagrange interpolation formula is found to be an extension of the Chinese remainder theorem in the polynomial ring. And two new communication schemes based on the Chinese Remainder Theorem in distributive lattice and combined with RSA are proposed.

7. Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (Grant No. 11571281 and No. 61175055) and Shaanxi Provincial and Xi'an Shiyou University College Students Innovation and Entrepreneurship Training Program Funding Project(Grant No. 201819062).

References

[1] J.D. Eduardo, R.P. Yu, *The intimate relationship between the McNaughton and the chinese remainder theorems for MV-algebras,* Studia Logica, 2013 (101), 483-485.

[2] T.C. Lu, *Information encryption technology*, Sichuan Science and Technology Press, Chengdu, 1989.

[3] S. Bruce, *Applied cryptography,* China machine Press, Beijing, 2000.

[4] Y.M. Nie, P. Qiu, *Network information security technology,* Science Press, Beijing, 2001.

[5] K.D. Lu, *Computer cryptography data confidentiality and security in computer network (second edition),* Tsinghua University Press, Beijing, 1998.

[6] G. Xu, *On solving a generalized chinese remainder theorem in the presence of remainder errors*, in: Akbary A., Gun S. (eds) Geometry, Algebra, Number Theory, and Their Information Technology Applications. GANITA 2016, Springer Proceedings in Mathematics & Statistics, vol 251, Springer, Cham.

[7] B. Sury, *Multivariable chinese remainder theorem*, Resonance, 20 (2015), 206-216.

[8] S.H. Min, S.J. Yan, *Elementary number theory,* Higher Education Press, Beijing, 2003.

[9] W.J. Chen, W.A. Dudek, *Ideals and congruences in quasi-pseudo-MV algebras,* Soft Computing, 22 (2018), 3879-3889.

[10] Y. Ning, F. Miao, W. Huang, K. Meng, Y. Xiong, X. Wang, *Constructing ideal secret sharing schemes based on chinese remainder theorem*, In: Peyrin T., Galbraith S. (eds) Advances in Cryptologysia Crypt 2018, Lecture Notes in Computer Science, vol 11274, Springer, Cham.

[11] H.L. Yu, Y.C. Lin, B. Sivakumar, Y.M. Kuo, *A study of the temporal dynamics of ambient particulate matter using stochastic and chaotic techniques*, Atmospheric Environment, 69 (2013), 37-45.

[12] T.W. Hungerford, *Algebras*, Springer-Verlag, New York, 1974.

[13] Y.B. Jun, S.M. Hong, *Chinese remainder theorems in BCI-algebras*, Soochow Journal of Mathematics, 24 (1998), 219-230.

[14] F. Forouzesh, *Fuzzy P-ideals in MV-algebras,* Italian Journal of Pure and Applied Mathematics, 37 (2017), 259-272.

[15] G. Birkhoof, *Lattice theory,* American Mathematical Society Colloquium, 1940.

Accepted: 30.03.2019