Internal P-set and Security Transmission-identification of Information

YU Xiu-qing
Department of Mathematics Dezhou University Dezhou253000 China
School of Mathematics and System Science Shandong University Jinan250100 China
Email: sddzyxq@163.com

Abstract—P-sets (packet sets) is a pair of sets composed of internal P-set and outer P-set, and it has dynamic characteristics. Based on internal P-set, several concepts such as $\mathcal{F}$-internal contained information, $\mathcal{F}$-internal contained dependence, and $\mathcal{F}$-internal remainder information are presented. In addition, existing theorem, single-dependence transmission theorem, and attribute dependence theorem about $\mathcal{F}$-internal contained information are proposed. To express the dynamic degree of varying of $\mathcal{F}$-internal contained information, the concepts of $\mathcal{F}$-internal contained coefficient and $\mathcal{F}$-internal contained degree are given. Furthermore, discovery-identification principle of $\mathcal{F}$-internal contained information is provided. An algorithm of information transmission-identification is given. At the end, the feasibility of the algorithm is illustrated by an example.

Index Terms—internal P-set, $\mathcal{F}$-internal contained coefficient, security transmission of information, recovery-identification of information, algorithm

I. INTRODUCTION

Since 1990s, network provides a rapid and convenient approach to exchange information. It also brings out some new problems, especially security ones during information transmission. This paper makes use of a new mathematical theory, i.e. P-sets to propose a new algorithm about encrypt, security transmission, and discovery-identification about information.

In 2008, Professor Shi [1, 2] proposed P-sets by introducing dynamic characteristics into Cantor set $X$. P-sets is a pair of sets composed of the internal P-set $X^r$ and outer P-set $X^\ell$ together. So it has dynamic characteristics. Shi and Yu etc. [3-15] gave applications of P-sets in the field of information systems. For P-sets with dynamic characteristics, if some attributes are transferred into attribute set $\alpha$ of $X$ continually, then a sequence of internal P-set $X^r_1, X^r_2, \ldots, X^r_n, X^r$ such that $X^r_1 \subseteq X^r_2 \subseteq \ldots \subseteq X^r_n \subseteq X^r$ are gotten, if some attributes in $\alpha$ are deleted ($\alpha \neq \phi$) continually, a sequence of outer P-set $X^\ell_1, X^\ell_2, \ldots, X^\ell_n, X^\ell$ such that $X^\ell_1 \subseteq X^\ell_2 \subseteq \ldots \subseteq X^\ell_n \subseteq X^\ell$ are gotten. These two sequences are main characteristics of P-sets.

Give further explanation on the sequence of internal P-set $X^r_i \subseteq X^r_{i+1} \subseteq \ldots \subseteq X^r_n \subseteq X^r$. Suppose that $X^r_i$ and $X^r_j$, $i < j$ satisfy $X^r_i \subseteq X^r_j$ implies that $X^r_i$ is contained in $X^r_j$. Similarly, $X^r_j$ is contained in $X^r_{i+1}$, $X^r_n$ is contained in $X^r_{n-1}$, and so on. Moreover, that $X^r_j$ is contained in $X^r_n$ results from new attribute elements transferred into attribute set $\alpha_i'$ of internal P-set $X^r_i$. Based on the characteristics of internal P-set, several concepts including $\mathcal{F}$-internal contained information and $\mathcal{F}$-internal contained information dependence are presented. Corresponding theorems, discovery-identification principle of $\mathcal{F}$-internal contained information, and an Algorithm on the transmission of information are obtained.

II. P-SETS AND ITS STRUCTURE

Assumption Function sets $\mathcal{F} = \{f_1, f_2, \ldots, f_n\}$ and $\mathcal{F}' = \{f_1', f_2', \ldots, f_n'\}$ are two families which transfer functions constitute. The functions $f$ in $\mathcal{F}$ and $f'$ in $\mathcal{F}'$ are transfer functions. The element $x_i$ is in set $X_i$, while the attribute $a_i$ is in attribute set $\alpha$. The transfer function $f$ implies $\exists x_i \in U, a_i \in X, f(a_i) = x_i \in X$. or $\exists \beta_i \in V, \beta_i \in \alpha, f(\beta_i) = \alpha_i' \in \alpha'$. The transfer function $f'$ implies $\exists x_i \in X, f'(x_i) = a_i \in X$ or $\exists \alpha_i \in \alpha, f'(\alpha_i) = \beta_i \in \alpha$. Interested reader can consult the literatures [1-2]. Let $X$ be a common set, $\alpha$ be the attribute set of $X$, $U$ be a finite element universe, and $V$ be a finite attribute universe. Everything takes place in nonempty and finite sets, unless specified. The real number $\text{card}(X)$ decreases when the real number $\text{card}(\alpha)$ increases, and vice versa, where the symbol $\text{card}(\cdot)$ denote the cardinal number of a set for abbreviation. Let $X = \{x_1, x_2, \ldots, x_n\} \subseteq U$ be a finite common set, and $\alpha = \{a_1, a_2, \ldots, a_n\} \subseteq V$ be the attribute set of $X$. The set $X^r$ such that

$$X^r = X - X^-.$$  (1)

is called internal packet set of $X$, briefly called internal P-set.

in formula (1), the set $X^-$ is a subset of $X$, and
in general, the set $X^r$ is said to be $F$ -element deleted set of $X$ .

if the attribute set $\alpha^r$ of $X^r$ satisfies

$$\alpha^r = \alpha \cup \{ \beta | f(\beta) = \alpha' \in \alpha, f \in F \}.$$  

(3)

where, for a new attribute $\beta$ out of $\alpha$ , transfer function $f$ in $F$ turns $\beta$ into $\alpha' \in f(\beta)$ and $\alpha'$ is in $\alpha$ .

Let $X = \{x_1, x_2, \ldots, x_n\} \subset U$ be a common set, and $\alpha = \{a_1, a_2, \ldots, a_m\} \subset V$ be the attribute set of $X$ . The set $X^r$ such that

$$X^r = X \cup X^r,$$

(4)

is called outer packet set of $X$ , called outer P-set for short.

In formula (4), the set $X^r$ such that

$$X^r = \{u | u \in U, u \notin X, f(u) \in X, f \in F \},$$

(5)

is said to be $F$ -element supplemented set.

If the attribute set $\alpha^r$ of $X^r$ satisfies

$$\alpha^r = \alpha - \{ a_i | f(a_i) = \beta_i \in \alpha, f \in F \},$$

(6)

where, for $a_i$ in $\alpha$ , $f$ in $F$ turns $a_i$ into $\beta_i = f(a_i) \in \alpha$ , in which $\alpha$ is the attribute set of $X$ , and $\alpha^r \neq \phi$ .

The pair of sets composed of internal P-set $X^r$ and outer P-set $X^r$ , is called P-sets (packet sets) generated by the common set $X$ , briefly called P-sets. It is denoted by

$$\langle X^r, X^r \rangle.$$  

(7)

Common set $X$ is usually called the ground set of P-sets.

Because of dynamic characteristics of P-sets, the general expression formula of P-sets is as follows.

$$\{(X^r, X^r) | i \in 1, j \in 1 \}.$$  

(8)

where I and J are finite index sets.

From formulas (1)-(8), we can easily get the relationship between P-sets and the common set as follows.

**Theorem 1** (The relation theorem between P-sets and the common set) Let P-sets $(X^r, X^r)$ be generated by common set $X$ , then

$$\langle X^r, X^r \rangle_{F, \tau_{pq}} = X.$$  

(9)

**Theorem 2** (Dynamic characteristics theorem of P-sets) Let P-sets $(X^r, X^r)$ be generated by common set $X$ , then

$$X^r \subseteq X \subseteq X^r.$$  

(10)

From formula (10), obviously, internal P-set $X^r$ is contained in set $X$ , while set $X$ is contained in outer P-set $X^r$ , which the name of P-sets is derived from

III. $F$ -INTERNAL INFORMATION AND $F$ -INTERNAL INFORMATION DEPENDENCE

For the convenience of discussion and avoiding misunderstanding, the sets $X, X^r, X^r$, and $X^r$ are called information. $X, X^r, X^r$, and $X^r$ are denoted by $(x), (x)^r, (x)^r$, and $(x)^r$ respectively, namely, $(x) = X, (x)^r = X^r, (x)^r = X^r$.

**Definition 1** $(x)$ is called an information in information universe $U$ , written as

$$(x) = \{x_1, x_2, \ldots, x_n\}.$$  

(11)

in which, for $i = 1, 2, \ldots, q$ , $x_i \in (x)$ is said to be an information element in $(x)$ , if $(x)$ has attribute set $\alpha$ , and

$$\alpha = \{a_1, a_2, \ldots, a_q\}.$$  

(12)

if attribute set $\alpha^r$ of $(x)^r$ satisfies

$$\alpha^r = \alpha \cup \Delta \alpha^r,$$

(14)

where $\Delta \alpha^r$ such that $\Delta \alpha^r = \{a | a' \in \alpha, f \in F \}$ , is said to be a supplemented set. $p$ and $q$ are positive integer number such that $p \leq q$ in formulas (11) and (13).

**Definition 3** $\Delta(x)^r$ is called remainder information of $(x)^r$ relative to $(x)$ , briefly called $F$ -remainder of $(x)^r$ , written as

$$\Delta(x)^r = (x) - (x)^r.$$  

(15)

where $(x)^r$ is $F$ -internal contained of $(x)$ .

**Definition 4** Let $(x)$ and $(x)'$ be information in information universe $U$ , $(x)$ called single-dependence to $(x)'$ , written as

$$(x)' \Rightarrow (x),$$  

(16)

if attribute set $\alpha$ of $(x)$ and attribute set $\alpha'$ of $(x)'$ satisfy $\alpha \subseteq \alpha'$ .

**Definition 5** Let $(x)$ and $(x)'$ be information in information universe $U$ , $(x)$ is called bi-dependence to $(x)'$ , written as

$$(x)' \Leftrightarrow (x),$$  

(17)

if attribute set $\alpha$ of $(x)$ and attribute set $\alpha'$ of $(x)'$ satisfy $\alpha = \alpha'$ .
where symbols \( \Rightarrow \) and \( \Leftrightarrow \) are derived from mathematical logic, \( \Rightarrow \) is equivalence to \( \subseteq \), \( \Leftrightarrow \) means \( = \).

Using definitions 1–5, we can easily obtain

**Proposition 1** Let \((x)^F\) be \(F\) - internal contained of \((x)\), then \((x)^F \Rightarrow (x)\).

**Proposition 2** Let \(\Delta(x)^F\) be \(F\) -remainder of \((x)^F\) relative to \((x)\), then \(\Delta(x)^F \Rightarrow (x)\).

**Proposition 3** Let \((x)^F\) and \(\Delta(x)^F\) be \(F\) - internal contained of \((x)\) and \(F\) -remainder of \((x)^F\), respectively. Then \(\Delta(x)^F\) and \((x)^F\) satisfy \(\Delta(x)^F \cup (x)^F = (x)\) and \(\Delta(x)^F \cap (x)^F = \phi\).

**Theorem 3** (\(F\)-contained existing theorem) Let \(\alpha\) be an attribute set of \((x)\), if \(\exists \beta \in V, \beta \in \alpha, \text{ and } f \in F\) changes \(\beta\) into \(f(\beta) = \alpha'\), then there exists information \((x)^F\) such that \((x)^F\) is contained in \((x)\), namely

\[(x)^F = (x)^F, \tag{18}\]

where the attribute set of \((x)^F\) is \(\alpha^r\), and \(\alpha' = \alpha \cup \{f(\beta)\}\).

**Proof** Let \((x)^F\) be an information whose attribute set is \(\alpha^r\). Because the equation \(\alpha^r = \alpha \cup \{f(\beta)\}\) implies \(\alpha \subseteq \alpha^r\), \((x)^F\) and \((x)^F\) satisfy \((x)^F \subseteq (x)^F\), or equivalently \((x)^F\) is \(F\) - internal contained in \((x)\) according to definition 2, namely \((x)^F = (x)^F\).

**Theorem 4** (Single-dependence transmission theorem of \(F\)-contained contained) Let \((x)^F, (x)^F, \text{ and } (x)^F\) be \(F\) - internal contained of \((x)\), if they satisfy

\[(x)^F \Rightarrow (x)^F, (x)^F \Rightarrow (x)^F, \tag{19}\]

then

\[(x)^F \Rightarrow (x)^F; \tag{20}\]

**Theorem 5** (Bi-dependence transmission theorem of \(F\)-internal contained) Let \((x)^F, (x)^F, \text{ and } (x)^F\) be \(F\) - internal contained of \((x)\), if they satisfy \((x)^F \Leftrightarrow (x)^F, (x)^F \Leftrightarrow (x)^F\)

then

\[(x)^F \Leftrightarrow (x)^F; \tag{21}\]

**Theorem 6** (Attribute-dependence theorem of \(F\)-internal remainder) Let \(\Delta(x)^F, \Delta(x)^F, \text{ and } \Delta(x)^F\) be \(F\) - internal remainders of \((x)^F, (x)^F, \text{ and } (x)^F\) relative to \((x)\) respectively. \(\Delta(x)^F, \Delta(x)^F, \text{ and } \Delta(x)^F\) satisfy single dependence relation, written as \(\Delta(x)^F \Rightarrow \Delta(x)^F \Rightarrow \Delta(x)^F\)

if, and only if

\[\Delta(x)^F \Rightarrow \Delta(x)^F \Rightarrow \Delta(x)^F; \tag{22}\]

where \(\Delta(x)^F, \Delta(x)^F, \text{ and } \Delta(x)^F\) are attribute supplement sets of \((x)^F, (x)^F, \text{ and } (x)^F\) respectively.

**Proof** Since attribute supplement sets \(\Delta(x)^F, \Delta(x)^F, \text{ and } \Delta(x)^F\) satisfy \(\Delta(x)^F = \Delta(x)^F, \text{ i.e., } \Delta(x)^F \subseteq \Delta(x)^F \subseteq \Delta(x)^F\).

There exists \(\alpha \cup \Delta(x)^F \subseteq \alpha \cup \Delta(x)^F \subseteq \alpha \cup \Delta(x)^F\) or written as \(\beta \subseteq \alpha' \subseteq \alpha'\). Consequently, there is \((x)^F \subseteq (x)^F\) \(\subseteq (x)^F\), so \((x)^F \subseteq (x)^F \subseteq (x)^F \), i.e. \(\Delta(x)^F \subseteq \Delta(x)^F \subseteq \Delta(x)^F\).

Suppose \(\Delta(x)^F\) - internal remainder \(\Delta(x)^F, \Delta(x)^F, \text{ and } \Delta(x)^F\) satisfy \(\Delta(x)^F \Rightarrow \Delta(x)^F \Rightarrow \Delta(x)^F\), i.e. \(\Delta(x)^F \subseteq \Delta(x)^F \subseteq \Delta(x)^F\), so there exists \((x)^F \subseteq (x)^F \subseteq (x)^F \subseteq (x)^F \). From formula (15), the relationship \(\Delta(x)^F = (x)^F \Rightarrow (x)^F = (x)^F\) is gotten, then there exists the formula \(\alpha^r\) \(\Rightarrow\) \(\alpha^r\), hence, \(\alpha' \Rightarrow \alpha^r \Rightarrow \alpha^r \Rightarrow \alpha^r \Rightarrow \alpha^r\), namely, formula (22) is true.

**Theorem 7** (Unidentification theorem about \(F\)-internal contained) Let \((x)^F\) be \(F\) - internal contained in \((x)\), If attribute supplement set \(\Delta(x)^F (x)^F\) satisfies \(\Delta(x)^F = \phi\) then

\[\text{UNI}((x)^F, (x)^F), \tag{23}\]

where \(\text{UNI}\) is an abbreviation of unidentification.

The proof is an immediate consequence of formula (14) and the dependence relationship between information and its attribute set.

**IV. \(F\)-INTERNAL CONTAINED MEASUREMENT AND RECOVERY-IDENTIFICATION**

**Definition 5** The real number \(\rho^F\) is called \(F\)-internal contained degree of \((x)^F\) relative to \((x)\), called \(F\)-internal contained degree for short, if

\[\rho^F = \text{card}(F)^F / \text{card}(F), \tag{25}\]

The real number \(\rho^F\) is called \(F\)-internal remainder of \((x)^F\) relative to \((x)\), called \(F\)-internal remainder degree for short, if

\[\rho^F = \text{card}(\Delta(x)^F) / \text{card}(F), \tag{26}\]

**Definition 6** The real number \(\eta^F\) is called \(F\)-internal contained coefficient of \((x)^F\) relative to \((x)\), briefly called \(F\)-internal contained coefficient of \((x)^F\), if

\[\eta^F = \| (x)^F \| / \| (x)^F \|, \tag{27}\]

The real number \(\rho^F\) is called \(F\)-internal remainder coefficient of \((x)^F\) relative to \((x)\), briefly called \(F\)-internal remainder coefficient of \((x)^F\), if

\[\eta^F = \| \Delta(x)^F \| / \| (x)^F \|, \tag{28}\]
where \((y)^F = (y_1, y_2, \ldots, y_r), (v) = (y_1, y_2, \ldots, y_r)\) and \(\Delta(y) = (y) - (y)^F\) are information value of \((x)^F = \{x_1, x_2, \ldots, x_s\}\) and \(x = \{x_1, x_2, \ldots, x_r\}\), respectively, in which \(y_i\) is numerical value of information element \(x_i\). \(\|\phi\|^F\) and \(\|\phi\|^v\) are formulated as \(\|\phi\|^F = (\sum_{i=1}^s y_i)^{1/2}\) and \(\|\phi\|^v = (\sum_{i=1}^r y_i)^{1/2}\).

From formulas (1) - (3) and definition 5 and definition 6, the following propositions are easily gotten.

**Proposition 4** Let the real number \(\rho^r\) be \(F\)-internal contained degree of \((x)^F\), \(\rho^r\) satisfies

\[ 0 < \rho^r \leq 1, \]  
(29)

**Proposition 5** Let the real numbers \(\rho^r\) and \(\Delta \rho^r\) be \(F\)-internal contained degree and \(F\)-internal remainder degree of \((x)^F\) respectively, they satisfy

\[ \rho^r + \Delta \rho^r = 1 \]  
(30)

**Proposition 6** Let the real number \(\eta^r\) be \(F\)-internal contained coefficient of \((x)^F\), \(\eta^r\) satisfies

\[ 0 \leq \eta^r \leq 1, \]  
(31)

By using definitions 5-7, propositions 1, and propositions 4, we can obtain conclusions as follows.

**Proposition 7** (The first relation theorem about \(F\)-internal remainder) Let \(\Delta(x)^F, \Delta(x)^v\) and \(\Delta(x)^r\) be \(F\)-internal remainders of \((x)^F, (x)^v\) and \((x)^r\) respectively, if they can form a single -dependence sequence such that

\[ \Delta(x)^F \Rightarrow \Delta(x)^v \Rightarrow \Delta(x)^r, \]  
(32)

then

\[ \Delta \rho^r \leq \Delta \rho^v \leq \Delta \rho^r, \]  
(33)

where, the real numbers \(\Delta \rho^r, \Delta \rho^v\) and \(\Delta \rho^r\) are \(F\)-internal remainder degree of \((x)^F, (x)^v, (x)^r\) respectively.

**Corollary 1** Let \(\Delta(x)^F, \Delta(x)^v\) and \(\Delta(x)^r\) be \(F\)-internal remainders of \((x)^F, (x)^v, (x)^r\) respectively. If they can form a single-dependence sequence such that

\[ \Delta(x)^F \Rightarrow \Delta(x)^v \Rightarrow \Delta(x)^r, \]  
(34)

then

\[ \rho^r \leq \rho^v \leq \rho^r, \]  
(35)

where \(\rho^r, \rho^v\) and \(\rho^r\) are \(F\)-internal contained coefficients of \((x)^F, (x)^v\) and \((x)^r\) respectively.

**Theorem 9** (The second relation theorem of \(F\)-internal remainder) Let \(\Delta(x)^F, \Delta(x)^v\) and \(\Delta(x)^r\) be \(F\)-internal remainder of \((x)^F, (x)^v\) and \((x)^r\) respectively. If they satisfy

\[ \Delta(x)^F \Rightarrow \Delta(x)^v \Rightarrow \Delta(x)^r, \]  
(36)

then

\[ \Delta \eta^r \leq \Delta \eta^v \leq \Delta \eta^r, \]  
(37)

where the real numbers \(\Delta \eta^r, \Delta \eta^v\) and \(\Delta \eta^r\) are \(F\)-internal remainder coefficients of \((x)^F, (x)^v\), and \((x)^r\) respectively.

**Corollary 2** Let \(\Delta(x)^F, \Delta(x)^v\) and \(\Delta(x)^r\) be \(F\)-internal remainders of \((x)^F, (x)^v\) and \((x)^r\) respectively. If they satisfy

\[ \Delta(x)^F \Rightarrow \Delta(x)^v \Rightarrow \Delta(x)^r, \]  
(38)

then

\[ \eta^r \leq \eta^v \leq \eta^r, \]  
(39)

where the real numbers \(\eta^r, \eta^v\) and \(\eta^r\) are \(F\)-internal contained coefficients of \((x)^v, (x)^r\) and \((x)^r\) respectively.

**Theorem 10** (Bi-dependence theorem of \(F\)-internal remainder) Let \(\Delta(x)^F, \Delta(x)^v, \Delta(x)^r\) be \(F\)-internal remainders of \((x)^F, (x)^v, (x)^r\) respectively. If they satisfy \(\Delta(x)^F \Leftrightarrow \Delta(x)^v \Leftrightarrow \Delta(x)^r\), then

\[ \Delta \rho^r = \Delta \rho^v = \Delta \rho^r, \]  
(40)

**Corollary 3** Let \(\Delta(x)^F, \Delta(x)^v\) and \(\Delta(x)^r\) be \(F\)-internal remainders of \((x)^F, (x)^v, (x)^r\) respectively. If they satisfy \(\Delta(x)^F \Leftrightarrow \Delta(x)^v \Leftrightarrow \Delta(x)^r\), then

\[ \Delta \eta^r = \Delta \eta^v = \Delta \eta^r, \]  
(41)

where identification is abbreviated to IDE.

**Proof** Since \(\Delta \rho^r - \Delta \rho^r \neq 0\) implies \(\rho^r \neq \rho^r\), from formula (27) there exists \(\rho^r = \text{card}(x)^F / \text{card}(x) \neq \rho^r = \text{card}(x)^F / \text{card}(x)\), i.e., \(\text{card}(x)^F \neq \text{card}(x)^r\). Thus we have formula (42).

**V. AN ALGORITHM OF \(F\)-INTERNAL CONTAINED IN INFORMATION TRANSFER**
In this section, the paper gives an algorithm about information transmission based on knowledge discussed in sections above. Suppose \( \alpha \) is the attribute set of information \((x), (x) = \{x_1,x_2,\ldots,x_p\} \) and \( \alpha = \{\alpha_1,\alpha_2,\ldots,\alpha_p\} \). If A sends \((x)\) to B safely, an algorithm is described in the following manner.

**Step 1** A adds new attributes \( \alpha',\alpha',\ldots,\alpha' \), out of \( \alpha \) into \( \alpha = \{\alpha_1,\alpha_2,\ldots,\alpha_p,\alpha',\alpha',\ldots,\alpha'\} \). Accordingly, information \((x)\) is turned to \((x)' = \{x_1,x_2,\ldots,x_h\} \) with \( h < p \). So \( F \) - internal remainder \( \Delta(x)' \) of \((x)'\) is equal to \( \{x_{h+1},x_{h+2},\ldots,x_p\} \), namely \( \Delta(x)' = \{x_{h+1},x_{h+2},\ldots,x_p\} \). Thus we can figure out \( F \) - internal remainder degree \( \Delta x' \) according to formula (26), and \( F \) - internal remaining coefficient \( \Delta x' \) according to formula (28).

**Step 2** A delivers \((x)'\), \( \Delta x' \) and \( \Delta x' \) to B in public, then B receives them.

**Step 3** A encrypts \( \Delta (x)' \) of \((x)'\) and delivers encrypted \( \Delta(x)' \) to B.

**Step 4** B receives encrypted \( \Delta(x)' \) and cracks it to obtain \( \Delta(x)' \).

**Step 5** B need check \( \Delta(x)' \) in case encrypted \( \Delta(x)' \) is changed during delivering process. B figures out \( \Delta x' = \text{card}(\Delta(x)') / \text{card}((x') and \( \Delta y' = ||(y)'|| / ||(y)'|| \) respectively. B compares \( \Delta x' \) and \( \Delta y' \) with \( \Delta x' \) and \( \Delta y' \) received in step 2 respectively. If B draws the conclusion \( \Delta x' = \Delta x' \), \( \Delta y' = \Delta y' \), then B carries out step 6, or B returns to step 2.

**Step 6** B can get correct information \((x)\)' such that \( (x)' = (x) \cup \Delta(x)' \). Then stop. Because this algorithm decreases encrypted information elements, it not only decreases cracking workload, but also ensures information to be transferred safely. Especially it provides approach that can check whether received information is true or not.

The following example comes from an information system.

For convenience, the names of \( x_i, x_j, i \in \{1,2,3,4,5\} \), \( j \in \{1,2,3,4,5,6\} \) are omitted.

A transferred \((x) = \{x_1,x_2,x_3,x_4,x_5\} \) to B and C. B received encrypted information transferred by A, cracked it, and obtained \( \Delta(x)' \). Furthermore, B tested and came to conclusion \( \Delta x' = \Delta x' = 1/3, \Delta y' = \Delta y' = 0.62 \). Thus B got the true information from A, and there was \((x)' = (x)' = \{x_1,x_2,x_3,x_4,x_5\} \) to B and C secretly. The detailed is in table 1 and table 2.

C did similarly and got information \( \Delta(x)' \), but he came to conclusion \( \Delta x' = \Delta x' = 1/3, \Delta y' = ||(y)'|| / ||(y)'|| \) ≠ \( \Delta x' \). So C judged that encrypted \( \Delta(x)' \) had been changed during transfer process. This accorded with check result. In fact, information element \( x_i \) in \( \Delta(x)' \) had been changed to \( x_i' \), and \( x_i' \in \Delta(x)' \). That is as table 3. Thus \( \Delta(x)' \) obtained by C is wrong, i.e., and \( \Delta(x)' \neq \Delta(x)' \). C had to return to step 2, and asked A to repeat step 2 again.

**VI. CONCLUSION**

This paper gives concepts of information internal contained and internal contained dependence based on P-set which has dynamic characteristic, discusses safe transfer-identification of information. Furthermore, a new algorithm is gotten. This algorithm not only decreases workload of encrypting information, but also provides an approach that can be used to identify received information based on P-set. The theory presented in this paper can be also used in data transfer and virus recovery-identification.

<table>
<thead>
<tr>
<th>TABLE 1</th>
<th>INFORMATION (x) TRANSFERRED BY A, EIGENVALUE SEQUENCE (y) AND ATTRIBUTE α OF (x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x)</td>
<td>x_1</td>
</tr>
<tr>
<td>α</td>
<td>α_1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 2</th>
<th>F-INTERNAL REMAINDER Δ(x)’, EIGENVALUE SEQUENCE Δ(y)’ AND ATTRIBUTE SET α’ OF F-INTERNAL CONTAINED (x)’ TRANSFERRED BY A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δ(x)’</td>
<td>x_1</td>
</tr>
<tr>
<td>Δ(y)’</td>
<td>0.63</td>
</tr>
<tr>
<td>α’</td>
<td>α_1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 3</th>
<th>F-INTERNAL REMAINDER Δ(x)’’, EIGENVALUE SEQUENCE Δ(y)’’ AND ATTRIBUTE SET α’’ OF F-INTERNAL CONTAINED (x)’’ RECEIVED BY C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δ(x)’’</td>
<td>x_1</td>
</tr>
<tr>
<td>Δ(y)’’</td>
<td>0.53</td>
</tr>
<tr>
<td>α’’</td>
<td>α_1</td>
</tr>
</tbody>
</table>

ACKNOWLEDGMENT
The authors wish to thank Prof. SHI Kai-quan. This work was supported in part by Shandong province Natural Science Foundation of China under Grant No. ZR2010AL019.

REFERENCES


Biography
YU Xiu-qing (1968-), female, native of Dezhou, Shandong, Prof. at School of Mathematics. Dezhou University, engages in rough system theory and applications.