GENERALIZED TRACEABILITY CODES

Majid MAZROOEI[1], Ali ZAGHIAN[2]

In this paper, we introduce generalizations of frameproof, secure frameproof, traceability and identifiable parent property codes and will study some of their basic combinatorial properties.

Keywords: Frameproof, Identifiable parent property, Hash family, Traceability.

1. Introduction

Throughout this paper, Q is an alphabet of size q and $C \subseteq Q^n$ is a q−array code of length n. If $|C| = M$, then we call C an (n, M, q)−code. The elements of C are called code words and each code word will have the form $x = (x_1, \ldots, x_n)$, where $x_i \in Q$, $1 \leq i \leq n$. The matrix representation of the code C, denoted H(C), is an $M \times n$ matrix on q symbols where each row of the matrix corresponds to one of the code words.

Codes providing some forms of traceability (TA, for short) to protect copyrighted digital data against piracy have been extensively studied in the recent years. The weak forms of such codes are frameproof codes introduced by Boneh and Shaw [2], and secure frameproof codes. The more strong form of these codes are identifiable parent property (IPP, for short) codes which have been introduced by Hollmann, Van Lint, Linnartz and Tolhuizen [4] and defined as follows.

Let $C \subseteq Q^n$ be a q-array code. For any subset of code words $C_0 \subseteq C$, the set of descendants of C_0 , denoted desc(C_0), is defined by

$$\text{desc}(C_0) = \{x \in Q^n \mid x_i \in \{a_i : a \in C_0\}, 1 \leq i \leq n\}.$$

Thus desc(C_0) consists of all n−tuples that could be produced by a coalition holding the code words in C_0 . If $x \in \text{desc}(C_0)$, then we say that C_0 produces x.

Let w be an integer. Define the w−descendant code, denoted $\text{desc}_w(C)$, as follows:

$$\text{desc}_w(C) = \bigcup_{C_0 \subseteq C, |C_0| \leq w} \text{desc}(C_0)$$

Thus $\text{desc}_w(C)$ consists of all n−tuples that could be produced by some coalition of size at most w. Now the code C is called an (n, M, q, w)−identifiable parent property code (w−IPP) provided that, for all $x \in \text{desc}_w(C)$, it holds that

[1] Assistant Prof., Dept .of Mathematical Sciences, University of Kashan, Isfahan, Iran, P. O. Box: 87317-51167, e-mail: m.mazrooei@kashanu.ac.ir
[2] Assistant Prof., Dept. of Mathematics, Malek Ashtar University of Technology, Isfahan, Iran, P. O. Box: 83145-115, e-mail: a_zaghian@mut-es.ac.ir

$$\bigcap_{\{i:\, x\in \mathrm{desc}(C_i),|C_i|\le w\}} C_i \neq \emptyset$$

Another strong versions of such codes are TA schemes and TA codes introduced by Chor, Fiat and Naor in [3]. In fact, TA codes turn out to be a subclass of IPP codes and are defined as follows.

Let define $I(x,y) = \{i : x_i = yi\}$ for any $x, y \in Q^n$. Suppose $C \subseteq Q^n$ is an (n, M, q) − code and $w \geq 2$ is an integer. C is called a w−traceability code (w−TA) provided that, for all i and all $x \in \mathrm{desc}(C_i)$, $C_i \subseteq C$ and $|C_i| \leq w$, there is at least one code word $y \in C_i$ such that $|I(x,y)| > |I(x,z)|$ for any $z \in CC_i$.

Combinatorial properties of IPP codes and TA codes have been studied by Staddon, Stinson and Wei [9], Sarkar and Stinson [7], Barg, et al. [1], and also in [11]. The question of traitor tracing algorithms for IPP and TA codes is treated in [8], e.g. certain classes of TA codes are shown to have a faster tracing algorithm than their initially known linear runtime by using the list decoding techniques. New results on bounds of frame-proof codes and TA schemes can be found in [6].

Recently, a major theoretical challenge is to derive more codes which have efficient tracing algorithms. To do this, some authors have given some generalizations of IPP and TA codes. Sarkar and Stinson [7] defined an (n, M, q, w, t)−IPP code as a code $C \subseteq Q^n$ with the property that for every k coalitions $(1 \leq k \leq t)$ $C_1, \ldots, C_k$ of C, each of size at most w, $x \in \bigcap_{i=1}^{k} \mathrm{desc}(C_i)$ implies $\bigcap_{i=1}^{k} C_i \neq \emptyset$. They have studied this generalization in part. For example, they proved that a code C is an $(n, M, q, 2)$−IPP code if and only if it is an $(n, M, q, 2, 3)$−IPP code. Another generalization is given by Wu and Sattar [12] for TA codes. They have defined TA codes relative to any well-defined metric and an efficient tracing algorithm is presented for Lee-metric TA codes.

In this paper, we introduce new generalizations of frame-proof, secure frame-proof, identifiable parent property and traceability codes and will study them.

2. Generalized Traceability Codes

From now, $\alpha_1, \ldots, \alpha_n : C \to Q$ are maps and $\alpha = \{\alpha_1, \ldots, \alpha_n\}$. For any $x \in C$ and for any $X \subseteq C$, let $\alpha(x) = (\alpha_1(x), \ldots, \alpha_n(x))$ and $\alpha(X) = \{\alpha(x) \mid x \in X\}$. For any subset of code words $C_0 \subseteq C$, we define the set of α−descendants of C_0 , denoted $\mathrm{desc}_\alpha(C_0)$, by

$$\mathrm{desc}_\alpha(C_0) = \{x \in Q^n \mid x_i \in \{\alpha_i(a) : a \in C_0\}, 1 \leq i \leq n\}.$$

Now, for any integer $w \geq 2$ define the (α, w)−descendant code, denoted $\mathrm{desc}_{\alpha,w}(C)$, as follows:

$$\mathrm{desc}_{\alpha,w}(C) = \bigcup_{C_0 \subseteq C, |C_0| \leq w} \mathrm{desc}_\alpha(C_0)$$

Definition 2.1 Let C be an (n, M, q)−code and $w \geq 2$ be an integer. We say that:

1. (α, w)−Frameproof code: C is an (n, M, q, α, w)−frameproof code ((α, w)−FP), if for any $C_0 \subseteq C$ of size at most w, $x \in \text{desc}_\alpha(C_0) \cap \alpha(C)$ implies $x \in \alpha(C_0)$.

2. (α, w)−Secure frameproof code: C is an (n, M, q, α, w)−secure frameproof code ((α, w)−SFP), if for any subsets C_0, C_1 of C of cardinality at most w, $\text{desc}_\alpha(C_0) \cap \text{desc}_\alpha(C_1) \neq \emptyset$ implies $C_0 \cap C_1 \neq \emptyset$.

3. (α, w)−Traceability code: C is an (n, M, q, α, w)-traceability code ((α, w)−TA) if for any $C_0 \subseteq C$ of cardinality at most w and for any $x \in \text{desc}_\alpha(C)$, there exists $y \in C_0$ such that $|I(x, \alpha(y))| > |I(x, \alpha(z))|$ for all $z \in CC_0$.

4. (α, w)−Identifiable parent property code: C is an (n, M, q, α, w)−identifiable parent property code ((α, w)−IPP) provided that, for all $x \in \text{desc}_{\alpha,w}(C)$, it holds that

$$\bigcap_{\{i:\, |C_i| \leq w, x \in \text{desc}_\alpha(C_i)\}} C_i \neq \emptyset$$

Note that the original definitions of FP, SFP, IPP and TA codes will be obtained if we take $\alpha = \{\pi_1, \ldots, \pi_n\}$, where $\pi_i : C \to Q, 1 \leq i \leq n$, is the natural projection on the i−th component. Our first result determines the relations between our generalized traceability codes.

Proposition 2.2. The following relationships hold for any (n, M, q)−code.

$$(\alpha, w)\text{−TA} \Rightarrow (\alpha, w)\text{−IPP} \Rightarrow (\alpha, w)\text{−SFP} \Rightarrow (\alpha, w)\text{−FP}.$$

Proof. Assume that C is an (n, M, q, α, w)−TA code. We show that C is an (α, w)−IPP code. Let $x \in \text{desc}_{\alpha,w}(C)$. Then there exists $C_0 \subseteq C$, $|C_0| \leq w$, such that $x \in \text{desc}_\alpha(C_0)$. Let $y \in C_0$ such that $|I(x, \alpha(y))| \geq |I(x, \alpha(z))|$ for all $\in C_0$. Thus $|I(x, \alpha(y))| \geq |I(x, \alpha(z))|$ for any $z \in C$ by assumption. We show that for any $C_i \subseteq C$, $|C_i| \leq w$, $x \in \text{desc}_\alpha(C_i)$ implies $y \in C_i$, which proves that C is an (α, w)−IPP code. By assumption, there is $y' \in C_i$ such that $|I(x, \alpha(y'))| > |I(x, \alpha(z))|$ for any $z \in CC_i$. If $y \neq y'$, then we will have $|I(x, \alpha(y'))| > |I(x, \alpha(y))|$, which is a contradiction. Hence $y = y' \in C_i$.

It is easy to see that any (α, w)−IPP code is an (α, w)−SFP code. We just prove that if C is an (α, w)−SFP code, then C is an (α, w)−FP code. Let C_0 be a subset of C of size at most w and $x \in \text{desc}_\alpha(C_0) \cap \alpha(C)$. Thus there exists a code word $u \in C$ such that $x = \alpha(u)$. Let $C_1 = \{u\}$. Then $x \in \text{desc}_\alpha(C_1)$. By assumption, we have $C_0 \cap C_1 \neq \emptyset$ showing that $u \in C_0$. Hence $x \in \alpha(C_0)$ which completes the proof. ■

Proposition 2.3. Let C be an (n, M, q)−code and let

$$d_\alpha = \min\{d(\alpha(x), \alpha(y)) \mid x, y \in C, x \neq y\}.$$

Assume that $w \geq 2$ is an integer such that $d_\alpha > n(1 - \frac{1}{w^2})$. Then C is an (α, w)−TA code.

Proof. Let $\lambda = n(1 - w^2)$ and $\beta = w^2 - 1$. Assume that $C_0 \subseteq C$, $|C_0| \leq w$, be a set of code words and $x \in \text{desc}_\alpha(C0)$. For any $u \in \text{desc}_\alpha(C0)$, let $M(u) = \max\{|I(u, \alpha(c))| \mid c \in C_0\}$ and $M = \min_{u \in \text{desc}_\alpha(C_0)} M(u)$. For any $u \in desc_\alpha(C_0)$ and $\in C_0$, we have $|I(u, \alpha(c))| \leq M(u)$ which shows that $\sum_{c \in C_0} |I(u, \alpha(C)| \leq wM(u)$. On the other hand, we have $n \leq \sum_{c \in C_0} |I(u, \alpha(C)|$. Thus $n \leq wM(u)$ for any $u \in \text{desc}_\alpha(C0)$. Hence $\frac{n}{w} \leq M$. Now let $y \in C_0$ be a code word such that $|I(x, \alpha(y))| = M(x)$. Then for any $z \in CC_0$ we have

$$|I(x, \alpha(z)| \leq \sum_{c \in C_0} |I(\alpha(C), \alpha(z))| \leq \sum_{cC_0} \beta \leq w\beta < \frac{n}{w} \leq M(x).$$

This completes the proof.■

Example 2.4. Let $Q = F_{11}$ and $C = \{100, 411, 511\}$. Define the maps $\alpha_i : C \to Q\ (i = 1, 2, 3)$ such that $\alpha_i(100) = 2, \alpha_i(411) = 3$ and $\alpha_i(511) = 6$ for $i = 1, 2, 3$. Then we have $d_\alpha = 3 > 4$. This shows that C is an $(3, 3, 11, \alpha, 2)$−TA code while C is not a 2−TA code.

3. Generalized Traceability Codes and Hash Families

A finite set H of n functions $h : A \to B$, where $|A| = M > |B| = m$, is called an (n, M, m)−hash family, denoted by (n, M, m)−HF. An (n, M, m)−HF H can be presented as an $M \times n$ matrix on m symbols, where each column of the matrix corresponds to one of the functions in H. Sometimes it is easier to consider hash families as such matrices.

Definition 3.1. We consider the following kinds of hash families.

1. Perfect hash family: An (n, M, m)−HF H is called an (n, M, m, w)−perfect hash family ((n, M, m, w)−PHF) if for any subset X of A of size w, there is a function $f \in$ H such that f is injective on X.

2. Separating hash family: An (n, M, m)−HF H is called an (n, M, m, w_1, w_2) −separating hash family ((n, M, m, w_1, w_2)−SHF) if for any disjoint subsets X, Y of A with $|X| = w_1$ and $|Y| = w_2$, there is a function $f \in H$ such that $f(X)$ and $f(Y)$ are also disjoint.

The following theorem, due to Staddon, Stinson and Wei [9], makes a connection between perfect hash families and IPP codes.

Theorem 3.2. Let C be an (n, M, q)−code whose matrix representation is C. If C is an $(n, M, q, \lfloor (w + 2)^2/4 \rfloor)$−PHF, then C is an (n, M, q, w)−IPP code.

Stinson, Van Trung and Wei [10] obtained another connections between (secure) frame-proof codes and separating hash families, which is stated in the following theorem.

Theorem 3.3.

1. A code C is an (n, M, q, w)−FP code iff $H(C)$ is an $(n, M, q, w, 1)$−SHF.

2. A code C is an (n, M, q, w)−SFP code iff $H(C)$ is an (n, M, q, w, w)−SHF.

In this section, we will derive similar results of our generalizations of FP, SFP and IPP codes. Before it, we need the following definition.

Definition 3.4. Let C be an (n, M, q)−code, $\alpha_1, \ldots, \alpha_n : C \to Q$ be maps and $\alpha = \{\alpha_1, \ldots, \alpha_n\}$. We say that α is an injective family if for any $x, y \in C$, $\alpha(x) = \alpha(y)$ implies $x = y$.

Proposition 3.5. Let C be an (n, M, q)−code and $w \geq 2$ be an integer. If α is an $(n, M, q, w, 1)$−SHF, then C is an (α, w)−FP code. The converse holds if α is an injective family.

Proof. Assume that $C_0 \subseteq C, |C_0| = w$ and $x \in \text{desc}_\alpha(C_0) \cap \alpha(C)$. Thus there exists $u \in C$ such that $x = \alpha(u)$. We claim that $u \in C_0$ which show that C is an (α, w)−FP code. Let $C_1 = \{u\}$. if $u \notin C_0$ then $C_0 \cap C_1 = \emptyset$. Hence, by assumption, there is $1 \leq i \leq n$ such that $\alpha_i(u) \in \alpha_i(C_0)$, which is a contradiction because $\alpha(u) = x \in \text{desc}_\alpha(C_0)$.

Now assume that C is an (α, w)−FP code and α is an injective family. We prove that α is an $(n, M, q, w, 1)$−SHF. If not, then there exist disjoint subsets C_0, C_1 of C with $|C_0| = 1$ and $|C_1| = w$ such that for any $1 \leq i \leq n$, $\alpha_i(C_0) \cap \alpha_i(C1) \neq \emptyset$. This shows that there is a code word $a \in C_0$ such that $\alpha(a) \in \text{desc}_\alpha(C_1)$. Since C is an (α, w)−FP code, $\alpha(a) \in \alpha(C_1)$. Thus there exists $b \in C_1$ such that $\alpha(a) = \alpha(b)$, which, by our assumption, implies $a = b$. Hence $C_0 \cap C_1 \neq \emptyset$, a contradiction. Thus α is an $(n, M, q, w, 1)$−SHF.

Proposition 3.6. Let C be an (n, M, q)−code and $w \geq 2$ be an integer. Then C is an (α, w)−SFP code iff α is an (n, M, q, w, w)−SHF.

Proof. Assume that C is an (α, w)−SFP code. We show that α is an (n, M, q, w, w)−SHF. If not, then there exist disjoint subsets C_0, C_1 of C, both of size w, such that $\alpha_i(C0) \cap \alpha_i(C1) \neq \emptyset$ for all $1 \leq i \leq n$. This shows that for any $1 \leq i \leq n$, there exists $u_i \in C_0$ and $v_i \in C_1$ such that $\alpha_i(u_i) = \alpha_i(v_i)$. Hence $\text{desc}_\alpha(C_0) \cap \text{desc}_\alpha(C_1) \neq \emptyset$, which is a contradiction because C is an (α, w)−SFP code. Hence α should be an (n, M, q, w, w)−SHF.

Conversely, assume that α is an (n, M, q, w, w)−SHF. We prove that C is an (α, w)−SFP code. Let C_0, C_1 be disjoint subsets of C both of size w. We shall show that $\text{desc}_\alpha(C_0) \cap \text{desc}_\alpha(C_1) = \emptyset$. By assumption, there exists $1 \leq i \leq n$ such that $\alpha_i(C_0) \cap \alpha_i(C_1) = \emptyset$. This shows that $\text{desc}_\alpha(C_0) \cap \text{desc}_\alpha(C_1) = \emptyset$, as desired.

Proposition 3.7. Let C be an (n, M, q, α, w)−IPP code where $M \geq w + 1$. Then the set $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ is an $(n, M, q, w + 1)$−PHF.

Proof. If not, then there is $X \subseteq C$ such that $|X| = w + 1$ and for any $1 \leq j \leq n$, there are $x \neq x' \in X$ such that $\alpha_j(x) = \alpha_j(x') = u_j$. Let $u = (u_1, \ldots, u_n)$. Then for any $x \in X$, we have $u \in \text{desc}_\alpha(C_x)$ where $\bigcap_{x \in X} C_x = X - \{x\}$.

But for any $x \in X, |C_x| = w$ and we have which contradicts the fact that C is an (α, w)−IPP code. Hence the set α is an $(n, M, q, w+1)$−PHF.

Proposition 3.8. A code C is an $(n, M, q, \alpha, 2)$−IPP code iff the family α is both an $(n, M, q, 3)$−PHF and an $(n, M, q, 2, 2)$−SHF.

Proof. If C is an $(n, M, q, \alpha, 2)$−IPP code then α is both an $(n, M, q, 3)$−PHF and an $(n, M, q, 2, 2)$−SHF by propositions 3.6 and 3.7. Assume that α is both an $(n, M, q, 3)$−PHF and an $(n, M, q, 2, 2)$−SHF. We show that C is an $(n, M, q, \alpha, 2)$−IPP code. Let $x \in \text{desc}_\alpha(C_i)$, $i = 1, \ldots, r$, where $C_i = \{a_{i1}, a_{i2}\}$, $1 \le i \le r$, are distinct subsets of C. If $C_1 \cap C_2 = \emptyset$, then by assumption, there exists $1 \le i \le n$ such that $\alpha_i(C_1) \cap \alpha_i(C_2) = \emptyset$, which is a contradiction because $x \in \text{desc}_\alpha(C_1) \cap \text{desc}_\alpha(C_2)$. Hence $C_1 \cap C_2 \neq \emptyset$. Without loss of generality we may assume that $a_{11} = a_{21}$. Note that in this case we have $a_{12} = a_{22}$. We claim that $a_{11} \in C_j$ for all $j = 3, \ldots, r$. If not, then there exists $3 \le j \le r$ such that $a_{11} \in C_j$. Since $C_1 \cap C_j \neq \emptyset$, we will have $a_{12} \in C_j$. Similarly, $a_{22} \in C_j$. Hence $C_j = \{a_{12}, a_{22}\}$. By assumption, there exists $1 \le l \le n$ such that $\alpha_l(a_{11}), \alpha_l(a_{12})$ and $\alpha_l(a_{22})$ are distinct. Now there are 2 cases:

Case 1. $x_l = \alpha_l(a_{11})$: In this case we will have $x \in \text{desc}_\alpha(C_j)$, which is a contradiction.

Case 2. $x_l = \alpha_l(a_{12})$: In this case we will have $x \in \text{desc}_\alpha(C_2)$, which is a contradiction.

Hence $a_{11} \in C_k$ for all $k = 1, \ldots, r$, as desired.■

Theorem 3.9. Let C be an (n, M, q)− code. If the family $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ is an $(n, M, q, \lfloor (w+2)^2/4 \rfloor)$−PHF, then C is an (α, w)−IPP code.

Proof. If not, then there exist $x \in \text{desc}_{\alpha,w}(C)$ such that

$$\bigcap_{\{i:\, x \in \text{desc}_\alpha(C_i),\, |C_i| \le w\}} C_i = \emptyset.$$

Let $D = \bigcap_{\{i:\, x \in \text{desc}_\alpha(C_i),\, |C_i| \le w\}} C_i$ and define

$$r = \min\left\{ |D'| : D' \subseteq D, \bigcap_{C_i \in D'} C_i = \emptyset \right\}.$$

Without loss of generality, we may assume that $D' = \{C_1, \ldots, C_r\}$ is a family of r distinct elements of D which have no common code words and for any $1 \le i \le r$, $x \in \text{desc}_\alpha(C_i)$. Let $C_i = \{y^{(1)}, \ldots, y^{(\beta)}\}$. Hence for any $1 \le i \le r$, there exists $y^{(k_i)} \in \bigcup_{j=1, j\neq i}^{r} C_i$ such that $y^{(k_i)} \notin C_i$. This shows that for any $1 \le i \le r$, we have

$$|C_i - \{y^{(k_1)}, \ldots, y^{(k_r)}\}| \le w - (r-1).$$

which implies $\beta \le r + r(w - r + 1) = (w + 2 - r)r$. Since w is an integer, the last inequality shows that $\beta \le \lfloor (w+2)2/4 \rfloor$. Now, since α is an (n, M, q, β)−PHF,

there exists $1 \leq j \leq r$ such that $\alpha_j(y^{(1)}),\ldots,\alpha_j(y^{(\beta)})$ are distinct. On the other hand, there exists $1 \leq t \leq \beta$ such that $xj = \alpha_j(y^{(t)})$. Also there is some $C_l \in D'$ such that $y^{(r)} \in C_l$. Since there is no code word $u \in \cup_{C_i \in D'} C_i$ such that $\alpha_j(u) = y_j^{(r)}$, we have $x \notin \mathrm{desc}_\alpha(C_l)$ which is a contradiction. Hence C is an (α, w)−IPP code.■

In [5], it is proved that if $n \geq we^{\frac{w^2}{m}} \log M$, then there exists an (n, M, m, w)−PHF. Hence we have the following corollary.

Corollary 3.10. Let C be an (n, M, q)−code and $w \geq 2$ be an integer such that $n \geq \lfloor \frac{(w+2)^2}{4} \rfloor e^{\frac{(\lfloor \frac{(w+2)^2}{4} \rfloor)^2}{q}} \log M$. Then there are maps $\alpha_1,\ldots,\alpha_n : C \to Q$ such that C is an (α, w)−IPP code.

4. Conclusion

We generalized and studied codes providing some forms of traceability (FP, SFP, TA and IPP codes) to generate new families of such codes. Our generalized traceability codes enjoy the basic combinatorial properties of original ones. This motivates us to study decoding algorithms of our families in the future.

Acknowledgement

The first author is partially supported by the University of Kashan under grant number 235604/1.

REFERENCES

[1]. *A. Barg, G. Cohen, S. Encheva, G. Kabatiansky and G. Zemor*, A hypergraph approach to the identifying parent property: the case of multiple parents, SIAM J. Discrete. Math., **14** (2001), 423-431.

[2]. *D. Boneh and M. Franklin*, An efficient public key traitor tracing schemes, Advances in Cryptography - Crypto' 94 (Lecture Notes in Computer Science), Springer-Verlag **839** (1994), 257-270.

[3]. *B. Chor, A. Fiat and M. Naor*, Tracing Traitors, Advances in Cryptography - Crypto' 94 (Lecture Notes in Computer Science), Springer-Verlag **839** (1994), 257-270.

[4]. *H. D. L. Hollmann, J. H. Van Lint, J. P. LinnartzL. M. G. M. Tulhuizen*, On codes with identifiable parent property, J. Comp. Theory A, **82** (1998), 121-133.

[5]. *K. Mehlhorn*, On the program size of perfect and universal hash functions, Proceedings of the 23rd IEEE Symposium of Foundations of Computer Science (1982), 170-175.

[6]. *R. Safavi-Naini and Y. Wang*, New results on frameproof codes and traceability schemes, IEEE Trans. Infom. Theory, **47** (2001), 3029-3033.

[7]. *P. Sarkar, D. R. Stinson*, Frameproof and IPP codes, Progress in Cryptography (Lecture Notes in Computer Science), **2247** (2001), 117-126.

[8]. *A. Silverberg, J. N. Staddon and J. L. Walker*, Efficient traitor tracing algorithms using list decoding, ASIACRYPT 2001 (Lecture Notes in Computer Sciences), **2248** (2001), 175-192.

[9]. *J. N. Staddon, D. R. Stinson and R. Wei*, Combinatorial properties of frameproof and traceability codes, IEEE Trans. Infom. Theory, **47** (2001), 1042-1049.

[10]. *D. R. Stinson, T. Van Trung and R. Wei*, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, J. Statistical Planning and Inference, **86** (2000), 596-617.

[11]. *T. V. Trung and S. Martirosyan*}, On a class of traceability codes, Designs, Codes and Cryptography, **31** (2004), 125-132.

[12]. *Xin-Wen Wu and Abdul Sattar,* A new class of traceability schemes for protecting digital content against illegal re-distribution, IJCSNS Int. J. Comput. Sci. and Net. Sec., Vol. 11, 12 (2011).