Journal of Informatics and Mathematical Sciences
Volume 5 (2013), Number 2, pp. 65–76
RGN Publications

http://www.rgnpublications.com

A Class of q-ary 2-IPP Codes

Sudhir Batra and Parvinder Singh

Abstract Sufficient conditions in terms of distance for the existence of binary 2-frameproof codes are obtained. A new class of q-ary 2-IPP codes has been explicitly constructed using latin square designs.

1. Introduction

Successive failure of copy prevention systems has caused copy detection systems to become the most promising option to protect the intellectual property of multimedia content. In copy detection, the merchant embeds an imperceptible mark into the content before selling it. This mark, known as fingerprint (or codeword), allows buyer identification. In fact, a fingerprint is a string over an alphabet and a fingerprinting code is a collection of fingerprints. The fingerprint is imbedded into digital objects such that it is not easy for a buyer to tamper with. However, if one has multiple copies of the same object with different fingerprints, he may compare the copies and detect where the marks are different and one might be able to change the mark on the detected positions. In this way, pirates may not only redistribute the copies illegally by changing fingerprints but can also frame innocent users. To prevent this Boneh and Shaw [2] introduced c-frameproof codes and c-secure codes. These codes are also available in the literature in more general form, i.e. in the form of separating codes [4]. Stinson and Wei [14] obtained the necessary and sufficient condition in terms of distance for the existence of binary 2-frameproof codes. In this paper, we also give two sufficient conditions for the existence of binary 2-frameproof codes. However these conditions are obtained by others in one form or the other but the form presented in this paper seems to be somewhat related to the optimal size of the codes so obtained.

2000 *Mathematics Subject Classification*. 68R05, 11T71, 05Bxx.
Key words and phrases. Frameproof code; IPP code; Hash family; Latin square design.

Hollmann, Vanlint, Linnartz and Tolhuizen [6] introduced identifiable parent property (IPP) codes. A code over q-alphabets has the w-identifiable parent property if no coalition of size atmost w can produce an q-tuple that cannot be traced back to atleast one member of the coalition. In this way, these codes are strong form of codes as compared to frameproof codes. These codes have been extensively studied in recent years. Using the relationships between IPP codes and combinatorial strutures several explicit classes of IPP codes have been derived [1, 3, 6, 11, 12, 13, 15]. In this paper, we use latin square designs to derive a new class of 2-IPP codes.

2. Frameproof Codes

2.1. Here we recall some definitions and results of [2] to be used in further discusion. These are summarized in (i)-(vii).

(i) Let Q be an alphabet of size q, representing the q different states of marks. The letters in Q will be denoted by the integers from 1 to q.

(ii) A set $T = \{w_{(1)}, w_{(2)}, \ldots, w_{(n)}\} \subseteq Q^l$ will be called an (l, n)-code. The codeword $w_{(i)}$ is assigned to user $u_{(i)}$, for $1 \leq i \leq n$.

(iii) Let set $T = \{w_{(1)}, w_{(2)}, \ldots, w_{(n)}\}$ be an (l, n)-code and C be coalition of users. For $i \in \{1, 2, \ldots, l\}$ we say that position i undetectable for C if the words assigned to users in C match in their ith position.

(iv) Let set $T = \{w_{(1)}, w_{(2)}, \ldots, w_{(n)}\}$ be an (l, n)-code and C be coalition of users. Let R be the set of undetectable positions for C. The feasible set, $F(C)$, is defined as: $F(C) = \{w \in (Q \cup (?))^l$ s.t. $w|R = w_u|R\}$ for some user u in C. In otherwords, the feasible set contains all words which match the coalition's undetectable position '?' (say).

(v) **Marking Assumption.** *It states that any coalition of c-users is only capable of creating an object whose fingerprint lies in the feasible set of coalition.*

(vi) A code T is c-frameproof if every set $W \subset T$ of size atmost c, satisfies $F(W) \cap T = W$.

(vii) The distance $d(w_{(1)}, w_{(2)})$ between two codewords $w_{(1)} = (x_1, x_2, \ldots, x_l)$ and $w_{(2)} = (y_1, y_2, \ldots, y_l)$ of a code of length l is the number of positions i in which $x_i \neq y_i$ for $1 \leq i \leq l$.

2.2. Boneh and Shaw [2] obtained a sufficient condition for combining a c-frameproof (l, p) code of size p and length l with a $(L, N, d)_p$ error-correcting code of length L, size N and minimum distance d over an alphabet of size p to obtain a c-frameproof code of length lL and size N. The idea of combining is to have a c-frameproof code of size larger than the size p of the (l, p) code by increasing the length from l to lL. This condition is given as follows.

Let T be a c-frameproof (l,p) code and C be a $(L,N,d)_p$ error correcting code. Let T' be the composition of T and C. Then T' is a c-frameproof code, provided $d > L(1-\frac{1}{c})$.

Remark 2.3. Since the size of (l,p) code and the size of alphabet set Q in $(L,N,d)_p$ error correcting code above is same i.e., p, we can define a 1-1 correspondence between the set Q and the (l,p) code. Then the composition of T and C is obtained by replacing alphabets of the codewords of (L,N,d) code by their corresponding images, i.e., codewords of the (l,p) code. In Theorem 2.6, we prove that a binary (L,N,d) error correcting code, where $d > L\left(1-\frac{1}{2}\right) = \frac{L}{2}$ is itself a 2-frameproof code. Before stating this theorem, we state the necessary and sufficient condition for the existence of 2-frameproof codes obtained by Staddon, Stinson and Wei [13, 14] as follows.

Theorem 2.4. *A (l,n) code T is 2-frameproof if and only if $d(w_{(i)},w_{(j)}) < d(w_{(i)},w_{(h)}) + d(w_{(h)},w_{(j)})$ for all $i \neq j \neq h \neq i$, where $w_{(i)},w_{(j)},w_{(h)} \in T$.*

Corollary 2.5. *A (l,n) code T is 2-frameproof if $d_{\max} < 2d_{\min}$, where $d_{\max} = \max\{d(w_{(i)},w_{(j)}) : w_{(i)},w_{(j)} \in T, i \neq j\}$ and $d_{\min} = \min\{d(w_{(i)},w_{(j)}) : w_{(i)},w_{(j)} \in T, i \neq j\}$.*

Theorem 2.6. *Let $T = \{(x_1,x_2,\dots,x_l) : x_i \in \{0,1\}, 1 \leq i \leq l\}$. Then*

(i) *T is a 2-frameproof code, provided for any $w_{(i)},w_{(j)} \in T$, $k \leq d(w_{(i)},w_{(j)}) \leq 2k-1$ for some $k \leq \frac{l}{2}$.*

(ii) *T is a 2-frameproof code, provided for any $w_{(i)},w_{(j)} \in T$, $d(w_{(i)},w_{(j)}) > \frac{l}{2}$.*

Proof. (i) Let $w_{(i)},w_{(j)} \in T$ and $d(w_{(i)},w_{(j)}) = m$. If a user $u_{(i)}$ with codeword $w_{(i)}$ colludes with another user $u_{(j)}$ with codeword $w_{(j)}$, then in view of the marking assumption 2.1(v), a collusion codeword can be formed by doing changes in all or some of those m positions where $w_{(i)}$ differs from $w_{(j)}$. Let $w_{(r)}$ be a codeword obtained after making t changes in $w_{(i)}$. Then $d(w_{(i)},w_{(r)}) = t$ and $d(w_{(j)},w_{(r)}) = m-t$, where $t < k$ or $k \leq t \leq 2k-1$. If $t < k$, then $d(w_{(i)},w_{(r)}) < k$. Therefore, $w_{(r)} \notin T$. If $k \leq t \leq 2k-1$, then $d(w_{(i)},w_{(r)}) = m-t \leq 2k-k-1 = k-1$. Therefore, again $w_{(r)} \notin T$. This proves (i).
(ii) Can be proved similarly as part (i). □

Remark 2.7. The results in (i) and (ii) of this theorem can also be proved directly by using Corollary 2.5 as follows:

(i) Take $d_{\min} = k$ and $d_{\max} = 2k-1$,

(ii) Take $d_{\min} > \frac{l}{2}$ and $d_{\max} = l$.

Remark 2.8. For binary codes, the largest number of codewords of length l whose mutual distance is d or more is denoted by $A(l,d)$. The values of $A(l,d)$ for different values of l and d are available in the literature. One such table is given by Conway and Sloane [5, 10].

From this table, the values of optimal size of 2-frameproof codes arisen due to part (ii) of Theorem 2.6 for certain lengths can be obtained. But the values of optimal size of 2-frameproof codes which are arisen due to part (i) of Theorem 2.6, are seemingly not available in the literature. It requires further investigation to obtain the values of optimal size of these 2-frameproof codes for various lengths.

We now give examples of 2-frameproof codes (need not be optimal) due to part (i) of Theorem 2.6, of length 6 and 10.

Example 2.9. (i) Let $l = 6$ and $k = 2 < \frac{6}{2}$. Then a 2-frameproof code is given as follows.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(ii) Let $l = 6$. Choose $k = 3 = \frac{6}{2}$. Then a 2-frameproof code obtained by an exclusive computation is as follows.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Example 2.10. (i) Let $l = 10$ and $k = 2 < \frac{10}{2}$. Then a 2-frameproof code is given as follows.

$$\text{(a)} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Example 2.11. (i) Let $l = 10$ and $k = 4 < \frac{10}{2}$. Then two 2-frameproof codes obtained by an exclusive computation are as follows.

$$
\text{(a)} \quad \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0\\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1\\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0\\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1\\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0\\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1\\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{bmatrix}
$$

$$
\text{(b)} \quad \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1\\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1\\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1\\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0\\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1\\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0
\end{bmatrix}
$$

3. IPP Codes

In this section we construct a new class of q-ary 2-IPP codes by using latin square designs. First we define IPP codes [6] in general and Gossip codes [15] in particular, which are in fact a class of IPP codes.

3.1. *w-IPP code*

Let Q be an alphabet of size q and Q^l denote the set of l-tuples over Q. A code C, of length l and size N over Q, is a subset of size N of Q^l and is called an (N, l, q)-code. A codeword c in C is an l-tuple $(c_1, c_2, \ldots, c_l)$. For a subset X of C, we define the set of descendents of X as

$$\operatorname{desc}(X) = \{a \in Q^l : a_i \in \{x_i : x \in X\}, 1 \leq i \leq l\}.$$

If $a \in \operatorname{desc}(X)$, then $x \in X$ is a parent of a. The set of descendents is a subset of Q^l that can be constructed by a coalition of users who have codewords in X. For a code C, define $\operatorname{desc}_w(C) = \{a \in Q^l : a \in \operatorname{desc}(X), X \subset C, |X| \leq w\}$.

A w-IPP code is a code with the property that for all words in $\operatorname{desc}_w(C)$ *at least one parent can be found.*

In view of the above definition of IPP code, we restate the marking assumption as follows:

3.2. *Marking Assumption*

(i) Colluders can make changes only at detected positions.

(ii) At a detected position, colluders can use one of the alphabet symbols matching with any one of their codewords at that position.

3.3. *Gossip Codes*

These are w-IPP codes, which can identify at least one user involved in creating an illegal copy under the above marking assumption, when w users collude. The construction of c-Gossip Codes by using t-designs was introduced in [7] and [8]. In [15] Gossip Codes were constructed with minimum possible code length specified for these codes (see [8]) in terms of alphabet size q, number of codewords M and collusion size c. In this paper a new class of q-ary 2-IPP codes, where $q > 3$ is an even number, has been explicitly constructed using latin square designs. We now give the construction of Gossip Codes presented in [8]. Let $B(M,q)$ be the 0/1-matrix consisting of l columns and M rows such that each column is created by placing $q-1$ ones and $M-q+1$ zeros. The parameters q and M are chosen such that $q \geq 3$ and $M \geq q+1$. The codeword matrix $G(M,q)$ is constructed from $B(M,q)$ by replacing the $q-1$ ones in each column, with the $q-1$ different non-zero symbols of Q and retaining the zeros unaltered. The code matrix $G(M,q)$ is called a Gossip Code and each column of this matrix is called a gossip column. For example, 2-Gossip$(7,7,4)$ code is given by the following matrix.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 3 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 3 & 0 & 3 \end{bmatrix}$$

Remark 3.1. The tracing method is based on the fact that every illegal fingerprint contains at least one non-zero symbol. Since every non-zero symbol appears exactly once in a gossip column. Hence this non-zero symbol traces at least one of the culprit.

3.4. *Some Combinatorial Structures*

In this section, we recall definitions of some structures used for the construction of 2-IPP codes (for ref. see [9]).

(i) *Latin Square Design.* Let X be a set of n elements $\{x_1, x_2, \ldots, x_n\}$. A latin square of order n is an $n \times n$ array of elements of X such that each row and each column of array contains each element of X exactly once.

(ii) *Perfect Hash Family.* An (n, m, w) perfect hash family is a set of functions $\mathscr{F}$ such that $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ for each $f \in \mathscr{F}$, and for any $X \subseteq \{1, 2, \ldots, n\}$ such that $|X| = w$, there exists at least one $f \in \mathscr{F}$ such that $f|X$ is one-to-one. When $|\mathscr{F}| = N$, an (n, m, w)-perfect hash family will be denoted by PHF $(N; n, m, w)$ can be depicted as an $N \times n$ matrix with enteries from $\{1, 2, \ldots, m\}$, having the property that in any w columns there exists at least one row such that the w enteries in the given w columns are distinct.

(iii) *Separating Hash Family.* An $(N; n, m)$ hash family $\mathscr{F}$ of N functions f : $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ is called an $(N; n, m, w_1, w_2)$ separating hash family denoted $(N; n, m, w_1, w_2)$-SHF if for any two disjoint subsets X, Y of $\{1, 2, \ldots, n\}$ and $|X| = w_1$ and $|Y| = w_2$ there is a function f in $\mathscr{F}$ such that $f(X)$ and $f(Y)$ are distinct.

3.5. A Class of q-ary 2-IPP Codes: Construction

Let $Q = \{0, 1, 2, \ldots, r\}$ be a set of alphabets, where $r\ (= q - 1) > 2$ is an odd number. We now use the following steps for the construction.

(I) Firstly we construct a latin-square design in which all the symbols on the main diagonal are distinct. For this, we use a recursive method described below:

(i) First row of the design consists of all the non-zero symbols of Q taken in any order. Let it be $(a_1, a_2, \ldots, a_r)$.

(ii) The elements of the second row are obtained by applying the permutation f, on the elements of the first row, given as:
$f : \{a_1, a_2, \ldots, a_r\} \to \{a_1, a_2, \ldots, a_r\}$ such that $f(a_i) = a_{i+1}$, $1 \leq i \leq r - 1$ and $f(a_r) = a_1$

(iii) The elements of the third row are obtained by permuting the elements of the second row in the same manner as the elements of the first row were permuted to obtain the second row. Following this recursive procedure, we can obtain rth row of the matrix from $(r-1)$th row. The resulting $r \times r$ matrix is a latin square design of order r having the additional property of distinct elements on the main diagonal. Let this matrix be denoted by $M_1 = [a_{ij}]_{r \times r}$

(II) We construct a matrix M_3 of order $r \times 2r$ using the matrices M_1 above and

$$M_2 = \begin{bmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_{rr} \end{bmatrix}$$

by placing the columns of the matrices M_1 and M_2 at alternate positions, starting from the first column of M_1, i.e., at the first position the column $(a_{11},a_{21},\dots,a_{r1})^t$ of M_1, at the second position place the column $(a_{11},0,0,\dots)^t$ of M_2, at the third position place the column $(a_{12},a_{22},\dots,a_{r2})^t$ of M_1, at the fourth position place the column $(0,a_{22},0,\dots,0)^t$ of M_2. Continuing like this place the column $(a_{r1},a_{r2},\dots,a_{rr})^t$ of M_1 at $(2r-1)$th position and the column $(0,0,\dots,a_{rr})^t$ of M_2 at $2r$th position. The resultant matrix so obtained is given below.

$$M_3 = \begin{bmatrix} a_{11} & a_{11} & a_{12} & 0 & 0 & 0 & \cdots & a_{1r} & 0 \\ a_{21} & 0 & a_{22} & a_{22} & 0 & 0 & \cdots & a_{1r} & 0 \\ \vdots & \vdots & \vdots & \vdots & & & & & \vdots \\ a_{r1} & 0 & a_{r2} & 0 & 0 & 0 & \cdots & a_{rr} & a_{rr} \end{bmatrix}$$

(III) We now construct a matrix M_5 of order $2r \times 2r$ using the matrices M_3 and $M_4 = \begin{bmatrix} a_{11} & 0 & 0 & a_{12} & \cdots & 0 & a_{1r} \\ 0 & a_{21} & a_{22} & 0 & \cdots & 0 & a_{2r} \\ \vdots & \vdots & \vdots & & & & \vdots \\ 0 & a_{r1} & 0 & a_{r2} & \cdots & a_{rr} & 0 \end{bmatrix}$ by placing the rows of these matrices at alternate positions, starting from the first row of M_3, i.e., at the first position place the row $(a_{11},a_{11},a_{12},0,\dots,a_{1r},0)$ of M_3, at the second position place the row $(a_{11},0,0,a_{12},\dots,0,a_{1r})$ of M_4, at the third position place the row $(a_{21},0,a_{22},a_{22},\dots,a_{2q},0)$ of M_3 and at the fourth position place the row $(0,a_{21},a_{22},0,\dots,0,a_{2r})$; continuing like this, place the row $(a_{r1},0,a_{r2},0,\dots,a_{rr},a_{rr})$ of M_3 at $(2r-1)$th position and $(0,a_{r1},0,a_{r2},\dots,a_{rr},0)$ at $2r$th position The matrix M_5 so constructed is as follows.

$$M_5 = \begin{bmatrix} a_{11} & a_{11} & a_{12} & 0 & a_{13} & 0 & \dots & a_{1r} & 0 \\ a_{11} & 0 & 0 & a_{12} & 0 & a_{13} & \dots & 0 & a_{1r} \\ a_{21} & 0 & a_{22} & a_{22} & a_{23} & 0 & \dots & a_{2r} & 0 \\ 0 & a_{21} & a_{22} & 0 & 0 & a_{23} & \dots & 0 & a_{2r} \\ \vdots & \vdots & \vdots & & & & & & \vdots \\ a_{r1} & 0 & a_{r2} & 0 & a_{r3} & 0 & \dots & a_{rr} & a_{rr} \\ 0 & a_{r1} & 0 & a_{r2} & 0 & a_{r3} & \dots & a_{rr} & 0 \end{bmatrix}.$$

Finally, augment a row $(a_{11},0,a_{22},0,\dots,a_{rr},0)$ with this matrix as a $(2r+1)$th row to obtain the desired matrix of order $(2r+1)\times 2r$.

We consider the resulting matrix $M = [c_{ij}]_{(2r+1)\times(2r)}$ a Hash family in which a column represents the values of a Hash function corresponding to the values $1,2,\dots,2r+1$. These columns are denoted by $h_1,h_2,\dots,h_{2r}$. The rows of this matrix are considered as $(2r+1)$ codewords those may be assigned to $(2r+1)$ users. These rows(users) are denoted by $u_1,u_2,\dots,u_{2r+1}$.

We prove that the collection of these $(2r+1)$ codewords is a 2-IPP code and for proving this, it suffices to prove the Theorem 3.8 in wake of the following theorem obtained in [6].

Theorem 3.2. *Let M be the matrix representing an (N, n, q) code C. Then C is a 2-IPP code if and only if M is simultaneously an $(N, n, q, 3)$-PHF and an $(N, n, q, 2, 2)$-SHF.*

Theorem 3.3. *The matrix M above represents a $(2r, 2r+1, q, 3)$ perfect hash family(PHF) and a $(2r, 2r+1, q, 2, 2)$ separating hash family (SHF).*

Proof. Using Definition 3.4(ii), for proving that M represents a $(2r, 2r+1, q, 3)$ PHF, it suffices to describe those rows which are having distinct elements in any of the three columns of the matrix M and for this Table 1 is provided. The first column of table contains all possible combinations of three columns of the matrix, the second column describes the corresponding rows having distinct elements in the chosen columns and $1 \le i, j, k \le r$; $i \ne j$

Table 1

Columns	Rows
$h_{2i-1}, h_{2j-1}, h_{2j}$	u_{2k-1} for all $k \ne j$, u_{2i}
h_{2i}, h_{2j-1}, h_{2j}	u_{2i-1}; u_{2k}, $k \ne i$
$h_{2i-1}, h_{2j-1}, h_{2k-1}$	u_{2k-1} for all k
h_{2i}, h_{2j}, h_{2k}	u_{2k} for all k
h_{2i}, h_{2j}, h_{2k-1}	u_{2i-1}; u_{2j-1}; u_{2k} for all $k \ne i$
$h_{2i-1}, h_{2j-1}, h_{2k}$	u_{2k-1} for all k; u_{2i}; u_{2j}

Using Definition 3.4(iii), for proving that M represents a $(2r, 2r+1, q, 2, 2)$ SHF, we give the following Table 2 in which it is revealed that there exists atleast one hash function h for any two subsets X and Y of the set $\{1, 2, \ldots, 2r+1\}$ such that with $|X| = 2 = |Y|$, $X \cap Y = \phi$ implies that $h(X) \cap h(Y) = \phi$. The last column of the table describes these functions corresponding to all possible combinations of the above said subsets X and Y of $\{1, 2, \ldots, 2r+1\}$ listed in the first two columns and $1 \le i, j, k \le r$; $i \ne j$.

This proves the theorem. □

4. Decoding Algorithm

(1) Since for $1 \le i$, $j \le r$, every column h_{2j} contains the non-zero symbols a_{ij} $(i \ne j)$ respectively in the rows u_{2i} and the symbol a_{jj} in the row u_{2j-1}. Therefore, a illegal codeword, made by the coalition of two users, containing a_{ij} at $2j$th position indicates that $u_{2i}(i \ne j)$ and $u_{2j-1}(i = j)$ are the parents of the codeword.

Table 2

A	B	Function(s)
$\{2i-1,2i\}$	$\{2j-1,2j\}$	$h_{2i-1}(A)=\{a_{ii}\}$, $h_{2i-1}(B)=\{0,a_{ji}\}$ $h_{2j-1}(A)=\{a_{jj}\}$, $h_{2j-1}(B)=\{0,a_{ij}\}$
$\{2i-1,2j\}$	$\{2j-1,2i\}$	$h_{2i}(A)=\{a_{ii},a_{ji}\}$, $h_{2i}(B)=\{0\}$ $h_{2j}(A)=\{0\}, h_{2j}(B)=\{a_{jj},a_{ij}\}$
$\{2i-1,2j-1\}$	$\{2i,2j\}$	$h_{2k-1}(A)=\{a_{ik},a_{jk}\}$, $h_{2k-1}(B)=\{0\}$ $h_{2k}(A)=\{0\}$, $h_{2k}(B)=\{a_{ik},a_{jk}\}$ for all $k\neq i,j$
$\{2r+1,2i-1\}$	$\{2j-1,2j\}$	$h_{2k-1}(A)=\{a_{ik},a_{kk}\}$, $h_{2k-1}(B)=\{a_{jk},0\}$ for all $k\neq j$
$\{2r+1,2i\}$	$\{2j-1,2j\}$	$h_{2i-1}(A)=\{a_{ii}\}$, $h_{2i-1}(B)=\{0,a_{ji}\}$
$\{2r+1,2i-1\}$	$\{2i,2j-1\}$	$h_{2k-1}(A)=\{a_{ik},a_{kk}\}$, $h_{2k-1}(B)=\{0,a_{jk}\}$ for all $k\neq i,j$ $h_{2j}(A)=\{0\}$, $h_{2j}(B)=\{a_{ij},a_{jj}\}$
$\{2r+1,2i-1\}$	$\{2i,2j\}$	$h_{2k-1}(A)=\{a_{ik},a_{kk}\}$, $h_{2k-1}(B)=\{0\}$ $h_{2k}(A)=\{0\}$, $h_{2k}(B)=\{a_{ik},a_{jk}\}$ for all $k\neq i,j$
$\{2r+1,2i\}$	$\{2i-1,2j-1\}$	$h_{2k-1}(A)=\{a_{kk},0\}$, $h_{2k-1}(B)=\{a_{ik},a_{jk}\}$ for all $k\neq i,j$
$\{2r+1,2i\}$	$\{2i-1,2j\}$	$h_{2i}(A)=\{a_{ii},0\}$, $h_{2i}(B)=\{a_{ii},a_{ji}\}$

(2) For $1\leq i,\,j\leq r$, every column h_{2j-1} contains the non-zero symbols $a_{ij}(i\neq j)$ respectively in the rows u_{2i-1}. Therefore, a illegal codeword containing a_{ij} $(i\neq j)$ at $(2j-1)$th position indicates that u_{2i-1} is the parent of the codeword.

(3) Since the codewords with non-zero symbols at the even positions have been discussed in (1) and non-zero symbols of the form $a_{ij}(i\neq j)$ at the odd positions have been discussed in (2). Further, observe that codeword having all zero's is not possible by the coalition of any two users. Therefore, the only illegal codewords which are left to be considered contain the symbols a_{ii} at one or more $(2i-1)$ positions, where $1\leq i\leq r$. For this consider the following observations from Table 2

   (i) For any two rows u_{2i-1}, u_{2j-1} there exists a function h_{2k-1} for all $k\neq i,j$ such that $h_{2k-1}(2i-1)=a_{ik}$ and $h_{2k-1}(2j-1)=a_{jk}$.

   (ii) For any two rows u_{2i-1}, $u_{2j}(j\neq i)$ there exist functions h_{2i} and h_{2j-1} such that $h_{2i}(2i-1)=a_{ii}$ and $h_{2i}(2j)=a_{ji}$.

   From these observations we conclude that the user u_{2i} is the parent of the codeword in which a_{ii} appears at one $(2i-1)$th position and u_{2r+1} is the parent of a codeword in which a_{ii}'s appear at two or more $(2i-1)$th positions.

Example 4.1. Let $q = 4$. Using the method of construction given in 3.5, the q-ary 2-IPP$(6, 7, 4)$ code obtained is as follows.

$$\begin{bmatrix} 1 & 1 & 3 & 0 & 2 & 0 \\ 1 & 0 & 0 & 3 & 0 & 2 \\ 3 & 0 & 2 & 2 & 1 & 0 \\ 0 & 3 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 3 & 3 \\ 0 & 2 & 0 & 1 & 3 & 0 \end{bmatrix}$$

5. Conclusions

(1) we see in Example 2.9 that for $k = 2$, $l = 6$, size of the code is 6 and for $k = 3$, $l = 6$, size of the code is 8. We see in Example 2.10 that for $k = 2,l = 10$, size of the code is 10 and for $k = 4,l = 10$, size of the code is 12. Using Table(see [5] and p. 26 of [10]), we observe that the optimal size of frameproof codes arisen due to part (ii) of Theorem 2.6, for $l = 6$ and $l = 10$ is respectively 4 and 6. This shows that for these lengths the respective optimal size of code due to part (i) of Theorem 2.6 is more than that of code due to part (ii) of Theorem 2.6. It requires further investigation to see whether it happens in general. Moreover, the optimal size of code due to part (i) of Theorem 2.6 seems to be depending on the value of k. This fact also requires further investigation for finding the optimal size of a code in general.

(2) Unlike Gossip Codes, 2-IPP codes defined in this paper contains non-zero symbols appearing more than once in certain columns.

(3) In the construction of 2-IPP codes (see Section 3.5) a restriction on q to be an even number is imposed. However one can also construct 2-IPP codes when q is odd. For example, if $q = 5$ then M_1 is given by

$$\begin{bmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

(4) Comparing the parameters of the 2-IPP$(6, 7, 4)$ code(due to construction 3.5) given in Example 4.1 with the parameters of 2-Gossip$(7, 7, 4)$ code (see Section 3.3) we see that the alphabet size is same in both the codes and the size of both the codes is also same, i.e., 7. But length of the code given in Example 4.1 is shorter than that of 2-Gossip$(7, 7, 4)$ code. Now since both the codes are 2-IPP codes, therefore due to shorter length, this particular 2-IPP code which is due to the construction discussed in this paper is better than 2-Gossip$(7, 7, 4)$ code.

References

[1] N. Alon, G. Cohen, M. Krivelievich and S. Litsyn, Generalized hashing and parent-identifying codes, *J. Combin. Theory Ser. A* **104** (2003), 207–215.

[2] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Trans. Infor. Theory* **44**(5) (1998), 1897–1905.

[3] B. Chor, A. Fiat and M. Naor, *Tracing Traitors*, *Proc. Crypto'94*, Springer-Verlag, New York **839** (1994), 257–270.

[4] G. Cohen, Sylvia B. Encheva and Hans Georg Schaathun, *On Separating Codes*, URL www.ii.uib.no/georg/sci/inf, February 2010.

[5] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, New York, 1988.

[6] H.D.L. Hollman, J.H. VanLint, J. Linnartz and L.M.G.M. Tolhuizen, On codes with identifiable parent property, *J. Combin. Theory Ser. A* **82** (1998), 121–133.

[7] T. Lindkvist, *Fingerprinting of digital documents*, Dissertation **706**, Linkoping University, Sweden (2001).

[8] T. Lindkvist, J. Lofvenberg and M. Svanstom, A class of traceability codes, *IEEE Trans. Infor. Theory* **48**(7) (2002), 2094–2096.

[9] K. Mehlhorn, Data Structures and Algorithms **1**, Springer-Verlag, 1984.

[10] Vera Pless, *Introduction to the Theory of Error-Correcting Codes*, A Wiley Interscience Publication, 1998.

[11] P. Sarkar and D.R. Stinson, *Frameproof and IPP Codes*, LNCS (INDOCRYPT 2001), Springer, 2001.

[12] A. Silverberg, J.N. Staddon and J.L. Walker, *Efficient Traitor Tracing Algorithm using List Decoding*, ASIACRYPT 2001, LNCS **2248** (2001), 175–192.

[13] J.N. Staddon, D.R. Stinson and R. Wei, Combinatorial properties of frameproof and tracebility codes, *IEEE Trans. Infor. Theory* **47** (2001), 1042–1049.

[14] D.R. Stinson and R. Wei, Combinatorial properties and construction of traceibility schemes and frameproof codes, *SIAM J. Discrete Math.* **11**(1998), 41–53.

[15] R.S. Veerubhotla, A. Saxena, V.P. Gulati and A.K. Pujari, Gossip codes for fingerprinting: construction, erasure analysis and pirate tracing, *Journal of Universal Comp. Sci.* **11**(1) (2005), 122–149.

Sudhir Batra, *Department of Mathematics, DCR University of Science and Technology, Murthal, Sonepat, India.*
E-mail: batrasudhir@rediffmail.com

Parvinder Singh, *Department of Computer Science and Engineering, DCR University of Science and Technology, Murthal, Sonepat, India.*
E-mail: parvinder23@rediffmail.com

Received December 10, 2011
Accepted May 23, 2012