IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 19, Issue 3 Ser. 3 (May. – June. 2023), PP 01-04
www.iosrjournals.org

A Class of 3 –TA Codes

Anu Kathuria
The Technological Institute of Textile and Sciences, Bhiwani -127021

Abstract :

In this paper we propose an explicit construction of a new class of 3-TA (Traceable Codes) of size (2n-2) and length (2n-2), n > 1.By the definition of Traceable code in [3] for a code C being 3-TA , minimum distance d of the code is given by d$>$ $(1-\frac{1}{c^2})$n, n is the length of the code and c defines the number of colluders. In that paper we have tried to give the answer of the open problem mentioned in [4].Can we design c-TA codes for which q $< c^2$also? q defines the size of field and c defines the number of colluders. So here we propose a method consisting of (2n – 2) codewords satisfying q < c^2 and it comes out to be a 3-TA code.

Keywords : Traceable (TA) Code, Hamming Code, Latin Square, Combinatorics

---

Date of Submission: 13-06-2023 Date of Acceptance: 23-06-2023

I. Introduction :

Digital fingerprinting is a technique that is used to protect intellectual rights by preventing illegal redistribution of digital data (films,softwares,music etc). it is facilitated by collection of codes called fingerprinting codes. These fingerprinting codes examine the interpretation of fingerprints embedded into digital objects to use it as a method of protecting intellectual rights. Before selling any digital copy in the market a merchant just embeds some marks into the content. This marking, known as fingerprint allows buyer identification. Infact, a fingerprint is a string over an alphabet and a fingerprinting code is collection of fingerprints. it is embedded 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 marks on 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. Strong form of codes called Identifiable Parent Property(IPP) Codes have been introduced by Hollman and Van Lint[7].Other form of codes called traceability codes were introduced by Chor,Fiat and Naor [1]in 1994.TA codes are stronger than IPP codes and is a subclass of IPP codes and generally have efficient traitor tracing algorithm.IPP codes on the other hand are capable of identifying traitors requiring less restrictive conditions than TA codes at the expense of having not efficient traitor tracing algorithm.

Organization of the paper

This paper is organized as follows. In Section 2, we give basic definitions and necessary background of traceable codes. In Section 3,we start our discussion by defining Marking Assumption which we apply to construct this class of 3-TA codes. The main result of this paper is presented in form of a theorem stating that this construction discussed above is in general 3-TA code.

II. Definitions and Basic Results on Traceable Codes

Here we give definition of traceable codes and some basic properties of traceable codes to be used in further discussion.

2.1 Here we recall some basic definitions related to error correcting codes.

(i) Let Q be a finite set of alphabets. Then a subset C C $Q^n$is called a code of length n over Q. The elements of $Q^n$are called words and the elements of C are called codewords of length n.

(ii) Let a and b be two codewords , then the hamming distance between a and b d(a,b) is the number of coordinates in which they differ and the number of non zero coordinates of a word c is called the weight of c. The minimum distance d of C is d=min.{d(a,b) | a, b ϵ C}.

(iii) I(x,y)={i: x_i = y_i} for x={ $x_1, x_2 \ldots\ldots x_n$} , y={$y_{1,} y_2 \ldots\ldots . y_n$}$\epsilon Q^n$. Similarly we can define I(x,y,z…..) for any number of words x,y,z…..

(iv) A subspace C of F_q^n is called a linear code over $F_{q.}$ The dimension of the code is defined as the dimension of the subspace. A linear code with length n, dimension k and minimum distance d is denoted As [n, k ,d] code.

(v) A linear code C [n, k ,d] is a Maximium Distance Separable code if d=n-k+1

(vi) A code C with same distance for every pair of codewords is called equidistant code and if all the codewords carry same weight then it is called Equidistant Constant Weight Code.

2.2 Now let us define some terms related to fingerprinting codes

(i) Detectable and Undetectable Positions: Let X is a subset of Q^n. Then we say that the position iϵQ^n is undetectable for X if ith position of each word x ϵ X is occupied with the same alphabet, otherwise the position is detectable.
(ii)Coalition: it means two or more users meet for the purpose of creating an illegal copy of a digital object (see Marking Assumption (iv) also) by comparing their copies. A member of the coalition is called a pirate.

(iii) Descendant Set: For any two words a = $\{a_1, a_{2,} \ldots\ldots.. a_n\}$ and
b=$\{b_1, b_2 \ldots\ldots b_n\}$ in Q^n,the set of descendants is defined

D(a, b) = {x ϵQ^n | $x_i \epsilon$ { a_i, b_i},i=1,2,3…n}The above definition of descendant set can be naturally extended to any finite number of words a, b, c……

(iv) Marking Assumption: In the static form of fingerprinting scheme each digital content is divided into multiple segments, among which n segments are chosen for marking them with symbols which correspond to alphabets in Q. Each user receives a copy of the content with differently marked symbols .if a code C over Q of length n is used to assign the symbols for each segment to each user. Then each copy can be denoted as Codeword of C and each coordinate x_i of a codeword $\{x_1, x_2, \ldots. x_n\}$can be termed as symbol. Further assume that any coalition of c users is capable of creating a pirated copy whose marked symbols correspond to a word of Q^n that lie in the Descendant set of c users.

(v) Traceable Code: For x , y ϵ Q^n;define I(x, y)= {i : $x_i = y_i$ }. C is c-TA code provided that for all I and for all x ϵ $desc_c(C_{i)}$) there is atleast one codeword
y$\epsilon C_i (C_i$⊂ C) ; $|(x,y)|$>$|(x,z)|$ $for\ any\ z\epsilon\ C/C_{i..}$ The condition in terms of
distance is equivalent to d(x,y) < d(x,z).

(vi) Frameproof Code: A (v,b)-code T is called a c-frameproof code if ,for every W ⊂ T such that $|W| \leq c$, we have F(W) ∩ T=W. We will say that T is a c-FPC (v,b) for short. Thus, in a c-frameproof code the only codewords in the feasible set a coalition of at most c users are the codewords of the members of the coalition. Hence , no coalition of atmost c users can frame a user who is not in coalition.
(vi)Latin Square : A Latin Square of order q is a $q \times q$ array whose entries are from a set q of different symbols such that each row and each column of the array contains each symbol exactly once.

Theorem 2.2.1[4]: Suppose that C is an (n ,q^k ,d) code having distance
d>(1- 1/c^2)n. Then C is a c-TA code, where c = 2,3,4…….

III. Construction

In this section we describe the method for construction of a new class of 3-TA codes. Here we also try to give the answer of that open problem " Can we construct c-TA codes for which q < c^2 ?" For such code we show that size of the field is 5 and the code C comes out to be 3-TA code."

Marking Assumption
First we provide the marking assumption in view of definition of traceable codes.

(i) Pirates can make change only at detected positions.

(ii) Pirates can create one of the alphabet symbols matching any one of their copies in place of detected positions.

A class of 3-TA Codes: Construction

We now propose a method to construct 3-TA codes.

Phase 1. Consider the set Q= {0,1,2,3,4} of 5 symbols and obtain 8 codewords applying following steps.
(i) First construct a matrix M_1 of order (2n-2 × 2n-2) by writing the elements of Q.
(ii)For the first (n-1) codewords ,fix first two columns and last two columns in form of zeros. in this way there will be $\frac{n-1}{2}$ columns consisting of zero elements only.
(iii)For the rest of the$\frac{n-1}{2}$ columns we will use the remaining elements of Q i.e.1,2,3,4
(iv)In those columns permute the elements in form of elements of a Latin Square such that every element appears once in every row and in every column.
Here using the above instructions generate these four codewords over the elements {0,1,2,3,4}

0	0	1	2	3	4	0	0
0	0	2	3	4	1	0	0
0	0	3	4	1	2	0	0
0	0	4	1	2	3	0	0

Phase 2.

(i) First construct a matrix M_1 of order (2n-2 × 2n-2) by writing the elements of Q.

(ii)For the first (n-1) codewords , fix first two columns and last two columns in form of elements of Q. In those columns permute the elements in form of elements of a Latin Square such that every element appears once in every row and in every column.
(iii) For the rest of the $\frac{n-1}{2}$ columns we will use the zero elements of Q . So in this way there will be $\frac{n-1}{2}$ columns consisting of zero elements only.
Using above instructions we can generate four more new codewords. i.e.

1	2	0	0	0	0	3	4
3	4	0	0	0	0	1	2
4	1	0	0	0	0	2	3
2	3	0	0	0	0	4	1

Here in Section 4, we show that the code C consisting of 8 codewords is 3-TA code. Here we represent a theorem in that reference.

Theorem 1. : The code C constructed above is 3-TA code.
Proof : Let a = $a_1a_2a_3a_4a_5a_6a_7a_8$,
b = $b_1b_2b_3b_4\,b_5b_6b_7b_8$ and
c = $c_1\,c_2c_3c_4\;c_5\,c_6c_7c_8$ collude . Now $a_i, b_i \in$ { 0,1,2,3,4 }.
If a_i =b_i, then in the collusion word we must have the symbol a_i presented above as such.

Case (i) if $a_i \neq b_i \neq c_i$ and three codewords obtained in Phase 1, collude.
Suppose these codewords are

0	0	1	2	3	4	0	0
0	0	3	4	1	2	0	0
0	0	2	3	4	1	0	0

Here in that case interaction of a_i, b_i and c_i can produce a codeword d which is different just at the places 3rd ,4th, 5th and 6th .Because at remaining positions digits are same. For such places in case of new codeword d , all d_i's ∈ {1, 2, 3, 4}.Suppose the colluders generate a new codeword e = (0 0 $d_3d_4d_5d_6$0 0). Here $d_3$can be in any one of the values 1, 3 and 2. d_4 can belong to any one of the values 2,3 and 4. d_5 can be in any one of the values 3, 1 and 4. d_6 can be in any one of the values 1,2 and 4 . it is easy to verify that the distance d for the codeword e and other codewords obtained in Phase 2. is minimum against those codewords only who had actually participated in this conspiracy. That completes the poof of case (i).

Case (ii) if $a_i \neq b_i \neq c_i$ and three codewords obtained in Phase 2, collude.
Suppose these codewords are

1	2	0	0	0	0	3	4
3	4	0	0	0	0	1	2
4	1	0	0	0	0	2	3

Here in that case interaction of a_i, b_i and c_i can produce a codeword d which is different from the other three codewords at the places 1st,2nd and 7th,8th. As at other remaining positions the digits are same. For such places in case of any new codeword d , all d_i's ∈ {1, 2, 3, 4 }.Suppose the colluders generate a new codeword e = ($d_1 d_2$ 0 0 0 0 $d_7 d_8$) .Here d_1 ∈ {1,3,4}, d_2 ∈ { 2,4,1} and d_7 ∈ { 3,1,2} and d_8 ∈ {4,2,3}.such possible combinations in that case will be 81. It is easy to verify that distance d from the codeword e and all the codewords obtained in Phase 2.is minimum for those codewords only who had actually participated in conspiracy .That completes the proof of the case (ii).

Case (iii) if any three codewords of Phase 1 and Phase 2 collude, where two codewords belong to Phase 1 and any one codeword belong to Phase 2, Then

For these codewords;

0	0	1	2	3	4	0	0
0	0	4	1	2	3	0	0
1	2	0	0	0	0	3	4

If the colluders generate a new codeword e , where e = { e_1,$e_{2,}$, e_3,e_4,e_5, $e_{6,}e_7$,e_8}, e_1 ∈ { 0,1} and e_8 ∈ {0,4}. So for the new colluded codeword just according to the digit {0} at 1st , 2nd and at other places we can have an idea that whether the traitor or colluder is a codeword belonging to Phase 1 or Phase 2. For the first two positions in case of interaction of new codewords consist of two possibilities in terms of numbers i.e. { 0, 1} and { 0,2}.If for the colluded codeword {0} is at the first and second position then it can be easily concluded that the traitor is carrying any codeword of Phase 1. If the codeword consists of {0} at 7th and 8th position , then the final codeword consists of the codeword belonging to Phase 2 . if we count the distance d from the pirated codeword e and the codewords of traitors then distance d comes out to be minimum for these codewords. That completes the proof of case (iii).

Case (iv) : if any three codewords of Phase 1 and Phase 2 collude, where two codewords belong to Phase 2 and any one codeword belong to Phase 1, Then

For these codewords;

0	0	1	2	3	4	0	0
3	4	0	0	0	0	1	2
1	2	0	0	0	0	3	4

If the colluders generate a new codeword f , where f = {$f_{1,,}f_2$ ……..f_8}, f_1 ∈ { 0, 1,2} and f_8 ∈ {0,2,4}. So for the new colluded codeword just according to the digit {0} at 1st , 2nd and at other places we can have an idea that whether the traitor or colluder is a codeword belonging to Phase 1 or Phase 2. For the first two positions in case of interaction of new codewords consist of two possibilities in terms of numbers i.e. { 0, 1,3} and { 0,2,4}.If for the colluded codeword {0} is at the first and second position then it can be easily concluded that the traitor is carrying any codeword of Phase 2. If the codeword consists of {0} at 7th and 8th position , then the final codeword consists of the codeword belonging to Phase 1 . if we count the distance d from the pirated codeword f and the codewords of traitors then distance d comes out to be minimum for these codewords. That completes the proof of case (iv).

IV. Conclusion :

Here we define the construction of that code C , which consists of the N, number of codewords equal to (2q-2) and length (2q-2) , where q defines the size of the field and N defines the number of codewords. For that code C we find that $q < c^2$ and the code C even comes out to be 3- TA code. Moreover we have tried to solve the open problem mentioned in [4], in reference of construction of c-TA code satisfying $q< c^2$. In future we would like to define the construction of 4-TA codes.

REFERENCES:

[1]. B. Chor, A. Fiat and M. Naor, "Tracing Traitors" ,Crypto'94 (Lecture Notes in Computer Science),Berlin, Heidelberg ,New York ,vol.839, pp.480-491, 1994.

[2]. D. Boneh and J. Shaw," Collusion secure fingerprinting for Digital Data" in Advances in Cryptology-CRYPTO '95 (Lecture Notes in Computer Science),vol. 963,pp.463-465,New York ,1995.

[3]. D. Boneh and J. Shaw," Collusion secure fingerprinting for Digital Data" IEEE Transactions on Information Theory ,vol.44,pp. 1897-1905,1998.

[4]. D.R. Stinson , R. Wei ,"Combinatorial Properties and Constructions of traceability schemes and frameproof codes" SIAM Journal of Discrete Mathematics, vol.2 ,pp. 41-53,1998.

[5]. D.R. Stinson , T. Van Trung, R. Wei ,"Secure frameproof codes, Key Distribution Patterns and related structures "J. Statistical Planning Inference vol. 86(2),(2000),pp. 595-617.

[6]. Gerard Cohen , Encheva Sylvia "Frameproof codes against coalition of Pirates" Theoretical Computer Science ,vol.273(2002) pp. 295-304.

[7]. H.D.L. Hollman , Jack H., Van Lint "On Codes with identifiable Parent Property
"Journal of Combinatorial Theory , Series A-82, pp. 121-133, 1998.

[8] M. Fernandez and M. Soriano, " A new class of codes for Fingerprinting Schemes",Springer-Verlag ,Berlin Heidelberg 2005,pp. 398-409