트래시빌리티 부호 계열의 구조

Construction of A Class of Traceability Codes

마역단, 얀이얼, 이문호
Yizhou Ma, Yier Yan, Moon Ho Lee

Abstract - In order to protect copyrighted materials, codes may be embedded in the content to trace the traitors. Traceability (TA) codes, as a kind of such codes, have been extensively studied in the intervening years for use as a piracy deterrent. In this correspondence, we proposed a method to construct a class of traceability codes and gave out some parameters results of such codes.

Key Words :Traitor tracing, traceability (TA) codes, minimum distance.

1. Introduction

Nowadays, digital commercial products, such as CDs, DVDs, encrypted pay-TV programs are getting more and more popular because of the higher quality and lower cost than previous products. And digital copy of these products can also provide the same quality as the original but with almost negligible cost. In order to protect the copyright, we need some traitor tracing schemes to deter users from making illegal copies and find them out. One way to accomplish this would be to embed a unique digital fingerprint into the content which is to be protected. Such schemes have been considered and described as traceability (TA) codesin several papers and correspondences lately, for instance, [1]-[4]. In this paper, we propose a method to construct a class of traceability codes.

The rest of this paper is organized as follows. In Section II, we give definitions, notation, and background on TA codes. In the following section, we present our method to construct a class of TA codes.Then some results about the new constructed codes are given in Section IV. In Section V, concluding remarks summarize this paper.

2. Traceability Codes

In this section we present definitions, notation, and background on traceability codes using the standard coding theory terminology and notation.

Let Γ be a q-ary code of length n and size q^k, $\Gamma \in Q^n$, where Q is a finite alphabet and $|Q| = q$, $|\Gamma| = q^k$. Elements of Q^n are called words. An element of Γ, called a codeword, can be written as $w = (w_1, w_2, ..., w_n)$ where $w_i \in Q$. For example: $Q = \{0,1\}$, $|Q| = 2$. If $n = 2$, $Q^2 = \{00,01,10,11\}$. $\Gamma = \{00,11\}$ is a subset of Q^2, and $w = (0,0)$ or $w = (1,1)$ is a codeword.

Let $\Gamma_\omega = \{w^{(1)}, w^{(2)}, ...w^{(\omega)}\} \subset \Gamma$ be a subset of Γ, called a coalition. If $w_i^{(1)} = w_i^{(2)} = ... = w_i^{(\omega)}$, then the position i is called undetectable, otherwise it is called detectable. For any coalition $\Gamma_\omega \subseteq \Gamma$, we define the set of descendants of Γ_ω, denoted by

$$Desc(\Gamma_\omega) = \{w \in Q^n : w_i \in \{w_i^{(1)}, w_i^{(2)}, ..., w_i^{(\omega)}\}$$

for all $1 \le i \le n\}$.

The set $Desc(\Gamma_\omega)$ consists of the n-tuples that could be produced by the coalition Γ_ω. An element w of

저자 소개
* 마역단 : 全北大學 情報通信工學科 博士課程
** 얀이얼: 全北大學 情報通信工學科 博士課程
*** 이문호: 全北大學 情報通信工學科 敎授・工博

$Desc(\Gamma_\omega)$ is called a descendant of Γ_ω. For example:

Γ	Γ_3	$Desc(\Gamma_3)$
0000000		
1001011	1001011	
0101110		1001011
0111001	0111001	0011000
1100101		…….
1011100	1011100	
1110010		

and $w_4^{(1)} = w_4^{(2)} = w_4^{(3)} = 1$, so location 4 is undetectable, while others are detectable.

Let $I(x,y) = \{i : x_i = y_i\}$ for $x, y \in Q^n$. For example: $x = (1001011)$, $y = (1010001)$, $I(x,y) = \{1,2,5,7\}$.

Definition 1. Γ is an ω- traceability code if for any subset Γ_ω with ω codewords of Γ, if $x \in Desc(\Gamma_\omega)$, then there is at least one codeword $y \in \Gamma_\omega$ such that $|I(x,y)| > |I(x,z)|$ for any $z \in \Gamma \setminus \Gamma_\omega$.

In other words, Γ is an ω- traceability code if, whenever a coalition of size at most ω produces a pirate word x, there is an element of the coalition which is closer to x than any codeword not in the coalition.

Theorem 1. If Γ is a (n, q^k)-code having length n, dimension k and minimum distance $d > n\left(1 - \frac{1}{\omega^2}\right)$, then Γ is an ω- traceability code.

Proof. Assume $x \in Dese(\Gamma_\omega)$, there is at least one $y \in \Gamma_\omega$, such that $|I(x,y)| \geq \frac{n}{\omega}$

(otherwise $|I(x,y)| < \frac{n}{\omega}$, $\sum_{i=1}^{\omega} |I(x,y_i)| < n$. It is a contradiction with $x \in Dese(\Gamma_\omega)$).

Since $d > n\left(1 - \frac{1}{\omega^2}\right)$, we have $d(z,y) > n\left(1 - \frac{1}{\omega^2}\right)$, where $z \in \Gamma \setminus \Gamma_\omega$, i.e. $|I(z,y)| < n - n\left(1 - \frac{1}{\omega^2}\right) = \frac{n}{\omega^2}$

therefore

$$|I(z,x)| \leq |I(z,\Gamma_\omega)| \leq \sum_{i=1}^{\omega} |I(z,y_i)|$$

$$< \omega \cdot \frac{n}{\omega^2} = \frac{n}{\omega} \leq |I(x,y)|,$$

Γ is an ω- traceability code.

3. Code Construction

We propose the following code construction. For each $q \geq 3$ and $m \geq q+1$, we construct the $m \times n$ base matrix B with $q-1$ "1"s and $m-q+1$ "0"s in each column in a systematic manner where $n = C_m^{q-1}$. Then we can obtain the code matrix C by replacing the "1"s in the base matrix B with nonzero elements of Q in also a systematic mannerand leaving the "0"s unchanged. Each row of the matrix C is a codeword which is composed of the TA code.

Following is one example with the parameters of $q = 4$, $m = 5$, $n = C_m^{q-1} = C_5^3 = 10$.

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

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

4. Analysis Results

According to the construction procedure, the Hamming weight of all the codewords in C is

$$w = C_{m-1}^{q-2}.$$

And the minimum distance is

$$d = C_{m-1}^{q-2} + C_{m-2}^{q-2}.$$

Theorem 2: Let $W \subseteq C$ be an arbitrary ω-subcode of cdewwords with $\omega \geq 2$. Then for all $x \in desc(W)$ it satisfies that

$$\min_{y \in W} d(x,y) \leq \left\lfloor \frac{\omega - 1}{\omega}\left(n - C_{m-\omega}^{q-1}\right) \right\rfloor.$$

Proof: Let $x \in desc(W)$.There are $C_{m-\omega}^{q-1}$ undetectable coordinates. In the detectable coordinates, x must be equal to at least one of the coedwords, so

$$\sum_{y \in W} d(x,y) \leq (\omega - 1)\left(n - C_{m-\omega}^{q-1}\right).$$

And at least one of the terms in the sum must be smaller than the average, therefore

$$\min_{y \in W} d(x,y) \leq \left\lfloor \frac{\omega - 1}{\omega}\left(n - C_{m-\omega}^{q-1}\right) \right\rfloor.$$

Theorem 3: Let $W \subseteq C$ be an arbitrary ω-subcode of cdewwords with $\omega \geq 2$. Then for all $x \in desc(W)$ it satisfies that

$$\min_{z \in C \backslash W} d(x,z) \geq C_{m-1}^{q-2} + C_{m-\omega-1}^{q-\omega-1}.$$

Proof: Let $x \in desc(W)$ and $z \in C \backslash W$. As all nonzero elements in a coordinate are different, x and z differ at least in the coordinates j where $z_j \neq 0$, and the coordinates j where $z_j = 0$ and $v_j \neq 0$ for all codewords $v \in W$. Therefore, we can obtain

$$\min_{z \in C \backslash W} d(x,z) \geq C_{m-1}^{q-2} + C_{m-\omega-1}^{q-\omega-1}$$

Referring to the definition of TA codes, Theorem 4 is straightforward.

Theorem 4: Let $\omega \geq 2$, if it satisfies

$$\frac{\omega - 1}{\omega}\left(n - C_{m-\omega}^{q-1}\right) < C_{m-1}^{q-2} + C_{m-\omega-1}^{q-\omega-1}$$

C is an ω-TA code.

From [3], a code is ω-TA code if

$$\omega^2 < \frac{n}{n-d}.$$

So for the present construction, this bound is

$$\omega^2 < \frac{m(m-1)}{(m-q)(m-q+1)}.$$

4. Concluding Remarks

In this paper we present a method to construct a class of TA codes. Based on the this systematic construction, we also study the properties and give out the condition under which this code is appliable to traitor tracing.

참 고 문 헌

[1] B. Chor, A. Fiat and M. Naor. Tracing traitors, in "Advances in Cryptology – Crypto '94", Lecture Notes in Computer 839 (1994),480-491.

[2] Lindkvist, "Fingerprinting of digital cocuments,"Lkinkoping Studies in Science and Technology, Dissertation 706, 2001.

[3] J. N. Staddon, D. R. Stinson , and R. Wei, "Combinatorial properties of frameproof and traceability coes," IEEE Trans. Inform. Theory, vol. 47, pp. 1042-1049, Mar. 2001.

[4] Yizhou Ma, Chang-hui Choe, Moon Ho Lee "A Class of Traceability Codes with an Efficient Tracing Algorithm," in Proceedings of ICSEA 06, pp. 63.