November 2001

New results on frame-proof codes and traceability schemes

R. Safavi-Naini
University of Wollongong, rei@uow.edu.au

Yejing Wang
University of Wollongong

New results on frame-proof codes and traceability schemes

Abstract

In this correspondence we derive lower bounds on the maximum number of codewords in a class of frame-proof codes and traceability schemes, and give constructions for both with more codewords than the best known.

Keywords

error-correcting codes, frame-proof codes, -sets, traceability schemes

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Safavi-Naini ,R & Wang, Y, New results on frame-proof codes and traceability schemes, IEEE Transactions on Information Theory, November 2001, 47(7) 3029-3033.

first-order Reed–Muller code. However, unlike the results of [8], this approach cannot be used for higher order constellations.

REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1996.

[2] J. A. Davis and J. Jedwab, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed–Muller codes," *Electron. Lett.*, vol. 33, pp. 267–268, 1997.

[3] ——, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2397–2417, Nov. 1999.

[4] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 82–87, 1961.

[5] R. D. J. van Nee, "OFDM codes for peak-to-average power reduction and error correction," in *Proc. IEEE GLOBECOM 1996*, London, U.K., Nov. 1996, pp. 740–744.

[6] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals," *IEICE Trans. Fundamentals*, vol. E80-A, pp. 2136–2143, 1997.

[7] K. G. Paterson, "Generalized Reed–Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 104–120, Jan. 2000.

[8] K. G. Paterson and A. E. Jones, "Efficient decoding algorithms for generalized Reed–Muller codes," *IEEE Trans. Commun.*, vol. 48, pp. 1272–1285, Aug. 2000.

New Results on Frame-Proof Codes and Traceability Schemes

Reihaneh Safavi-Naini, *Member, IEEE*, and Yejing Wang

***Abstract*—In this correspondence we derive lower bounds on the maximum number of codewords in a class of frame-proof codes and traceability schemes, and give constructions for both with more codewords than the best known.**

***Index Terms*—Error-correcting codes, frame-proof codes, S_t-sets, traceability schemes.**

I. INTRODUCTION

Frame-proof codes were introduced by Boneh and Shaw [1] to provide protection against illegal copying. When a merchant wants to sell a digital product to a buyer, he inserts a sequence of marks into the object which is unique to the buyer and so allows the merchant to distinguish different copies. The set of mark sequences used by the merchant forms a fingerprinting code. The code is assumed to be publicly known. The buyer does not know where the marks are inserted and so cannot remove them. However a group of colluding buyers can compare their copies, find out all the places that their marks are different, change the marks, and produce an illegal copy. In a c-frame proof code, if up to c buyers collude they cannot construct a copy with a valid sequence of marks, and so they cannot frame another buyer.

Manuscript received May 11, 2000; revised March 26, 2001.

The authors are with the School of Information Technology and Computer Science, University of Wollongong, Wollongong 2522, Australia (e-mail: rei@uow.edu.au; yejing@uow.edu.au).

Communicated by N. I. Koblitz, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(01)08971-4.

Boneh and Shaw proved [1], [2] that there exists a binary c-frame-proof code with the number n of codewords satisfying

$$n = 2^{\ell/(16c^2)} \tag{1}$$

where ℓ is the length of the codewords, and $c > 0$ is an arbitrary integer. In a recent paper, Staddon, Stinson, and Wei [3] proved an upper bound on the number of codewords in a c-frame-proof code over an alphabet of size $q \geq 2$, the bound is given as follows:

$$n \leq q^{\lceil \ell/c \rceil} + 2c - 2. \tag{2}$$

Traceability schemes were introduced by Chor, Fiat, and Naor [4], and are used in the context of broadcast encryption schemes. *Broadcast encryption* systems [5] allow targeting of an encrypted message to a privileged group of receivers. Each receiver has a decoder with a set of keys that allows him to decrypt encrypted messages if he is in the target group. Resilience of a broadcast encryption system is measured by a parameter m which is the size of the largest colluding group, disjoint from the privileged set, who cannot learn the message. A group of up to c colluders may want to construct a *pirate decoder* to decode the content. Broadcast encryption systems can provide traceability which means when a pirate decoder is found at least one of the colluders can be identified. Traceability schemes were studied in [6]–[9]. In a traceability scheme, each authorized user has a decoder with a set of k keys from a base key set K of size ℓ that uniquely determines the owner and allows him to decrypt the broadcast. Chor *et al.* [4] proved that for two positive integers ℓ and c, there exists a c-traceability scheme with

$$n = 2^{\ell/(8c^4)} \tag{3}$$

decoders, where ℓ is the total number of keys.

Stinson and Wei [6] proved an upper bound on the number of decoders in a c-traceability scheme

$$n \leq \frac{\binom{\ell}{t}}{\binom{k-1}{t-1}} \tag{4}$$

where $t = \lceil \frac{k}{c} \rceil$ and k is the number of keys contained in each decoder.

In this correspondence, we prove lower bounds on the maximal number of codewords in frame-proof codes and traceability schemes, and show that for some choices of parameters the bounds are tighter than the previously known bounds. We also give a construction for each that has the highest number of codewords compared with all the previously known constructions.

The correspondence is organized as follows. In Section II, we recall the basic results used in the rest of the correspondence. In Section III, we will prove a new lower bound on the number of codewords in a c-frame-proof code and a c-traceability scheme. New constructions for c-frame-proof codes and c-traceability schemes are given in Section IV, where we also discuss our results and compare the parameters of our construction with the known ones. In Section V. we conclude the correspondence.

II. PRELIMINARIES

A. c-Frame-Proof Codes

Frame-proof codes provide protection against framing attack. That is, in a c-frame-proof code, a collusion of up to c colluders cannot construct a copy of the object containing the codeword of a buyer not in the colluding set. The formal definition is as follows.

Let Σ be an alphabet of size $q \geq 2$. An (ℓ, n)-code Γ over Σ is defined as an n-subset of Σ^ℓ. Let "?" denote any symbol not in Σ, and let $\Sigma' = \Sigma \cup \{?\}$.

Definition 1: Let Γ be an (ℓ, n)-code over Σ, and

$$C = \{v_1, \ldots, v_b\} \subseteq \Gamma.$$

1) A bit position $i \in \{1, 2, \ldots, \ell\}$ is said to be undetectable for C if $v_1, v_2, \ldots, v_b$ have the same value at position i. Denote by $R(C)$ the set of all undetectable positions of C.
2) The feasible set $F(C)$ of C is defined as

$$F(C) = \left\{x \in (\Sigma')^{\ell} : x\big|_{R(C)} = v\big|_{R(C)}\right\}, \qquad \text{for } v \in C.$$

Frame-proof codes, introduced in [1], [2], are based on the following marking assumption which we also will use in this correspondence.

Marking Assumption: A collusion of size at most c is only capable of creating a codeword lying in the feasible set of the collusion.

Definition 2: A code Γ is called a c-frame-proof code if every subset $C \subseteq \Gamma$ of size at most c satisfies $F(C) \cap \Gamma = C$.

B. c-Traceability Schemes

In a traceability scheme every user has k decryption keys. A collusion of users may use their keys to create a "pirate" decoder consisting of at least k keys belonging to the collusion. The broadcaster has a tracing algorithm. Once a pirate decoder is captured, the broadcaster is able to trace those who have taken part in producing the pirate decoder. In the tracing algorithm proposed in [6], the tracing algorithm finds an *exposed user*, whose decoder has the highest number of keys in common with the pirate decoder. The following definition is from [6]. We follow this definition and tracing algorithm.

Definition 3: Suppose any exposed user v is a member of the collusion C whenever a pirate codeword x is produced by C and $|C| \leq c$. Then the scheme is called a c-traceability scheme.

A c-traceability scheme was described [6] as a set system $(X, \mathcal{B})$ with certain property. Suppose X is a set and $\mathcal{B}$ is a family of k-subsets of X where each k-subset is called a block. A traceability scheme can be thought of as a set system where a block corresponds to a decoder with k keys from the key set X.

Theorem 1 [6]: There exists a c-traceability scheme if and only if there exists a set system $(X, \mathcal{B})$ such that $|B| = k$ for every $B \in \mathcal{B}$, with the following property:

> For any $b \leq c$ blocks $B_1, B_2, \ldots, B_b \in \mathcal{B}$ and for any k-subset $F \subseteq \bigcup_{j=1}^{b} B_j$, there does not exist a block $B \in \mathcal{B} \setminus \{B_1, B_2, \ldots, B_b\}$ such that $|F \cap B_j| \leq |F \cap B|$ for $1 \leq j \leq b$.

C. Known Bounds on Error-Correcting Codes

In this section, we recall some known results from coding theory. Consider a binary code. Let $A(\ell, 2\delta, w)$ denote the maximum number of codewords in a code of length ℓ, constant weight w, and minimum Hamming distance 2δ. Let λ_{ij} be the dot product of two codewords v_i, v_j, that is, the number of places that the two codewords have a one and $\lambda = \max_{i,j} \lambda_{ij}$. Hence $\delta = w - \lambda$. The following are well-known upper and lower bounds on the number of codewords.

Theorem 2 ([10], Graham–Sloane Bound): Let q be a prime power such that $q \geq \ell$, $\delta \geq 3$. Then

$$A(\ell, 2\delta, w) \geq \frac{1}{q^{\delta-1}} \binom{\ell}{w}.$$

Theorem 3 ([11], Johnson Bound):

$$A(\ell, 2\delta, w) \leq \left\lfloor \frac{\delta \ell}{w^2 - w\ell + \delta\ell} \right\rfloor$$

provided that the denominator is positive.

In the following, $H(X) = -X \log X - (1-X)\log(1-X)$ denotes the binary entropy function, and all logarithms are in base 2. We will also be using the following bound due to Stirling.

Theorem 4 (Stirling's Formula): For any integer $\ell \geq 1$

$$\ell^{\ell+1/2} e^{-\ell} (2\pi)^{1/2} e^{1/(12\ell+1)} \leq \ell! \leq \ell^{\ell+1/2} e^{-\ell} (2\pi)^{1/2} e^{1/(12\ell)}. \quad (5)$$

Lemma 1: For any given $\sigma > 0$

$$\frac{1}{\ell} \log \binom{\ell}{k} > H\left(\frac{k}{\ell}\right) - \sigma$$

provided that ℓ satisfies the following:

$$\frac{\log \ell}{\ell} < \sigma \quad \text{and} \quad \ell > \left(13 + \sqrt{13^2 + 48\sigma}\right) \Big/ 12\sigma. \quad (6)$$

Proof: Using the Stirling formula (5) we have

$$\begin{aligned}
&\frac{1}{\ell} \log \binom{\ell}{k} \\
&\quad = \frac{1}{\ell} \log \frac{\ell!}{k!(\ell-k)!} \\
&\quad \geq \frac{1}{\ell} \log \frac{\ell^{\ell+1/2} e^{1/(12\ell+1)}}{k^{k+1/2} e^{1/(12k)} \cdot (\ell-k)^{\ell-k+1/2} e^{1/(12\ell-12k)} (2\pi)^{1/2}} \\
&\quad = \left(1 + \frac{1}{2\ell}\right) \log \ell - \left(\frac{k}{\ell} + \frac{1}{2\ell}\right) \log k - \left(1 - \frac{k}{\ell} + \frac{1}{2\ell}\right) \\
&\qquad \cdot \log(\ell - k) + \frac{1}{\ell} \log \left(e^{\frac{1}{12\ell+1} - \frac{1}{12k} - \frac{1}{12\ell-12k}} (2\pi)^{-1/2}\right) \\
&\quad = H\left(\frac{k}{\ell}\right) + \frac{1}{2\ell} \log \frac{\ell}{2(\ell-k)k\pi} \\
&\qquad + \frac{1}{\ell} \left(\frac{1}{12\ell+1} - \frac{1}{12k} - \frac{1}{12\ell-12k}\right) \log e \\
&\quad > H\left(\frac{k}{\ell}\right) + \left[\frac{1}{2\ell} \log \frac{\ell}{2(\ell-k)k\pi}\right. \\
&\qquad \left. + \frac{1}{\ell} \left(\frac{1}{12\ell+1} - \frac{1}{12k} - \frac{1}{12\ell-12k}\right)\right].
\end{aligned}$$

Let ℓ and k satisfy i) $\frac{\log \ell}{\ell} < \sigma$, ii) $\ell > (13 + \sqrt{13^2 + 48\sigma})/12\sigma$, and without loss generality assume $k \leq \ell/2$. Then the expression on the right-hand side can be written as

$$\begin{aligned}
&-\left[\frac{1}{2\ell} \log \frac{\ell}{2(\ell-k)k\pi} + \frac{1}{\ell} \left(\frac{1}{12\ell+1} - \frac{1}{12k} - \frac{1}{12\ell-12k}\right)\right] \\
&\quad = \frac{1}{2\ell} \log 2(\ell-k)\pi k/\ell + \frac{1}{\ell} \left(-\frac{1}{12\ell+1} + \frac{1}{12k} + \frac{1}{12\ell-12k}\right) \\
&\quad < \frac{1}{2} \frac{\log \ell\pi}{\ell} + \frac{1}{\ell} \left(\frac{1}{12k} + \frac{1}{12\ell-12k}\right) \\
&\quad < \frac{1}{2} \frac{\log \ell}{\ell} + \frac{1}{\ell} + \frac{1}{\ell} \left(\frac{1}{12} + \frac{1}{6\ell}\right) < \sigma
\end{aligned}$$

and so we have the following result:

$$\frac{1}{\ell}\log\binom{\ell}{k} > H\left(\frac{k}{\ell}\right) - \sigma. \qquad \square$$

III. Lower Bounds

Consider binary constant-weight codes only. Suppose ℓ, n, w, 2δ, λ are the same as in Section II-C. We will prove lower bounds on the maximum number of codewords in frame-proof codes and traceability schemes, when the size c of collusion is maximum. First, we restate Theorem 2 as follows.

Theorem 5: Let q be a prime power such that $q \geq \ell$, $\delta \geq 3$. Then for any $\sigma > 0$ and ℓ satisfying (6), the maximum number of codewords n satisfies

$$n > \frac{1}{q^{\delta-1}}\, 2^{(H(\frac{w}{\ell})-\sigma)\ell}. \tag{7}$$

Proof: Using Graham–Sloane bound (Theorem 2) and Lemma 1, we have

$$n \geq \frac{1}{q^{\delta-1}}\binom{\ell}{w} = \frac{1}{q^{\delta-1}}\, 2^{\frac{1}{\ell}\log\binom{\ell}{w}\cdot\ell} > \frac{1}{q^{\delta-1}}\, 2^{(H(\frac{w}{\ell})-\sigma)\ell}. \qquad \square$$

A. A Bound on c-Frame-Proof Codes

Lemma 2: If $w > c\lambda$, then the code Γ is a c-frame-proof code.

Proof: If Γ is not c-frame-proof there exists a subset C of colluders with $|C| \leq c$ such that $C \subset F(C) \cap \Gamma$. That is, there exists a v such that $v \in F(C) \cap \Gamma$ but $v \notin C$. Let $C = \{v_1, v_2, \ldots, v_b\}$, $b \leq c$. Suppose v and v_j overlap in k_j positions, $1 \leq j \leq b$. Then $k_j \leq \lambda$. By Marking Assumption, v has a 1 in a position if and only if at least one v_i has a 1 in that position. Therefore,

$$wt(v) \leq k_1 + k_2 + \cdots + k_b \leq b\lambda \leq c\lambda$$

which contradicts $wt(v) = w > c\lambda$. $\square$

Lemma 3: Let $w > c\lambda$ and

$$n > \frac{1}{A}\cdot\frac{\ell}{w}\cdot(c-1)$$

where

$$A = \begin{cases} 1, & \text{if } \frac{\ell}{w} \text{ is an integer} \\ \lceil \frac{\ell}{w} \rceil - \frac{\ell}{w}, & \text{otherwise.} \end{cases}$$

Then we have $c \leq \frac{\ell}{w}$.

Proof: Using Johnson bound (Theorem 3) we have

$$n \leq \frac{w\ell - \lambda\ell}{w^2 - \lambda\ell} \tag{8}$$

if $w^2 - \lambda\ell > 0$. Suppose the lemma is not true, that is, assume

$$c > \ell/w. \tag{9}$$

Then, since by assumption $w > c\lambda$ we have $\ell/w < c < w/\lambda$, and so $w^2 > \lambda\ell$ and the Johnson bound (8) can be applied. The function $f(x) = (w\ell - \ell x)/(w^2 - \ell x)$ is increasing with x when $x \in (-\infty, w^2/\ell)$ or $(w^2/\ell, +\infty)$. Note that $\lambda < w/c < w^2/\ell$, and from (8) we have

$$n \leq \frac{w\ell - \lambda\ell}{w^2 - \lambda\ell} \leq \frac{w\ell - \frac{w}{c}\ell}{w^2 - \frac{w}{c}\ell} = \frac{w\ell(c-1)}{w\ell\left(\frac{cw}{\ell} - 1\right)} = \frac{c-1}{\frac{cw}{\ell} - 1}.$$

That is,

$$c \leq \frac{\ell}{w}\left(1 + \frac{c-1}{n}\right). \tag{10}$$

If ℓ/w is an integer, and n satisfies the condition

$$n > \frac{\ell}{w}\cdot(c-1)$$

then

$$\frac{\ell}{w}\cdot\frac{c-1}{n} < 1$$

and hence

$$\left\lfloor \frac{\ell}{w}\cdot\frac{c-1}{n} \right\rfloor = 0.$$

Since c is an integer, so (10) gives

$$c \leq \left\lfloor \frac{\ell}{w}\left(1 + \frac{c-1}{n}\right)\right\rfloor = \frac{\ell}{w} + \left\lfloor \frac{\ell}{w}\cdot\frac{c-1}{n}\right\rfloor = \frac{\ell}{w}$$

which contradicts (9).

If ℓ/w is not an integer, and n satisfies the condition

$$n > \frac{1}{\lceil \frac{\ell}{w}\rceil - \frac{\ell}{w}}\cdot\frac{\ell}{w}\cdot(c-1)$$

then

$$\left\lceil \frac{\ell}{w}\right\rceil - \frac{\ell}{w} > \frac{\ell}{w}\cdot\frac{c-1}{n}$$

and so

$$\left\lceil \frac{\ell}{w}\right\rceil > \frac{\ell}{w}\left(1 + \frac{c-1}{n}\right). \tag{11}$$

As c is an integer, we know that (9) is equivalent to

$$c \geq \left\lceil \frac{\ell}{w}\right\rceil. \tag{12}$$

Equation (11) means that there is no integer c that satisfies both (10) and (12), and so (9) cannot be assumed. $\square$

Theorem 6: Let q be a prime power. Suppose there exists a c-frame-proof code with length $\ell \leq q$, constant weight w, and $c = \ell/w$. Then, for any $\sigma > 0$ and ℓ satisfying (6), the maximum number of codewords n satisfies

$$n > \frac{1}{q^{\delta-1}}\, 2^{(H(\frac{1}{c})-\sigma)\ell}. \tag{13}$$

Let $(0, 1)$ be the real number interval between 0 and 1, and let $x_0 \in (0, 1)$ be such that $H(x_0) = x_0$. It is easy to see that

$$\max_{x\in(0,1)}\{H(x) - x\} = H(1/2) - 1/2 = 1/2.$$

For any positive number $\sigma < 1/2$, there exists an $x \in (0, x_0)$ such that $H(x) - x > \sigma$, or in other words, there is a c such that $H(1/c) - 1/c > \sigma$. By choosing ℓ such that

$$\ell > \frac{1}{H\left(\frac{1}{c}\right) - \frac{1}{c} - \sigma}(\delta - 1)\log q \tag{14}$$

we have

$$\frac{1}{q^{\delta-1}}\, 2^{(H(\frac{1}{c})-\sigma)\ell} > 2^{\ell/c} > 2^{\ell/16c^2}$$

and so (13) gives a higher lower bound than the bound (1) of Boneh *et al.*. We note that ℓ must also satisfy (6), and so ℓ must satisfy both (6) and (14).

B. A Bound on c-Traceability Schemes

Let ℓ denote the total number of keys, $\lambda(v_i, v_j)$ be the cardinality of the set of keys common between decoder v_i and v_j, and

$\lambda = \max_{i,j} \lambda(v_i, v_j)$. Stinson and Wei [12] have proved the following lemma.

Lemma 4: If $k > c^2\lambda$, then the code is a c-traceability scheme.

Theorem 1 gives a combinatorial approach to c-traceability schemes. The incidence of the set system $(X, \mathcal{B})$ can be regarded as a binary code of length $|X|$, constant weight k, with $|\mathcal{B}|$ codewords. The notations $\lambda_{ij} = \lambda(v_i, v_j)$, and λ are the same as in Section II-C.

Lemma 5: Suppose $n \geq \ell$. If $k > c^2\lambda$, then

$$c^2 \leq \frac{\ell}{k}.$$

The proof of Lemma 5 is similar to that of Lemma 3, and omitted here.

Theorem 7: Let q be a prime power. Suppose there exists a c-traceability scheme with ℓ keys, $\ell \leq q$, such that there are k keys in each decoder, and $c^2 = 2\ell/k$. Then, for any $\sigma > 0$ and ℓ satisfying (6), the maximum number of decoders n satisfies

$$n > \frac{1}{q^{\delta-1}} 2^{(H(\frac{1}{c^2})-\sigma)\ell}. \tag{15}$$

Using an argument similar to the one given for bound (13), we can show that if $0 < \sigma < 1/2$, there is an integer c such that $H(1/c^2) - 1/c^2 > \sigma$, and so

$$\frac{1}{q^{\delta-1}} 2^{(H(\frac{1}{c^2})-\sigma)\ell} > 2^{\ell/c^2} > 2^{\ell/8c^4}$$

which means that (15) is a tighter bound than bound (3) of Chor*et al.*

IV. Construction

In [10], Graham and Sloane used S_t-sets to construct error-correcting codes. We use a similar approach to construct frame-proof codes and traceability schemes.

Definition 4: A set $S = \{s_1, s_2, \ldots, s_n\} \subseteq Z_m$ is called an S_t-set of size n and modulus m if all the sums

$$s_{i_1} + s_{i_2} + \cdots + s_{i_t}$$

for $i_1 < i_2 < \cdots < i_t$, are distinct in Z_m.

Constructions of S_t-sets can be found in [13], [14].

Theorem 8 [13, Theorem 17]: Let q be a prime power, and $\delta \geq 2$ be an integer. There exists an S_δ-set of size q and modulus $q^\delta - 1$.

The set S is constructed as follows. Let q be a prime power, $\delta \geq 2$ be an integer, and F_q and F_{q^δ} be fields of q and q^δ elements, respectively. Let $\xi \in F_{q^\delta}$ be a primitive element. Define

$$S = \{s: 0 \leq s < q^\delta - 1 \text{ such that } \xi^s = \xi + a, \text{ for some } a \in F_q\}. \tag{16}$$

S is a subset of integers and $|S| = q$. Let $S = \{s_1, s_2, \ldots, s_q\}$. S is an S_δ-set of size q and modulus $q^\delta - 1$.

Theorem 9 (Graham and Sloane, [10, Theorem 9]): If there exists an S_δ-set of size ℓ and modulus m then there exists a code, having length ℓ, constant weight w, minimal distance $2\delta + 2$, such that the number of codewords is

$$n \geq \frac{1}{m}\binom{\ell}{w}.$$

The code is constructed as follows. Suppose S is defined as in (16). Let $\ell = q$, w be an integer such that $\delta < w < q$, Γ_w^ℓ be the set of all binary vectors of length ℓ and constant weight w, and $Z_{q^\delta-1} = \{0, 1, 2, \ldots, q^\delta - 2\}$. Define a map

$$\phi: \Gamma_w^\ell \longrightarrow Z_{q^\delta-1}$$

such that

$$\phi(v) = \sum_{s_i \in S,\, a_i = 1} s_i (\bmod q^{\delta-1}), \quad \text{for } \forall\, v = (a_1, \ldots, a_\ell) \in \Gamma_w^\ell.$$

For every $i \in Z_{q^\delta-1}$ define a code $\Gamma_i = \phi^{-1}(i)$. All these codes are with length ℓ and constant weight w. In particular, take $\Gamma_{\max}$ such that

$$|\Gamma_{\max}| = \max_i |\Gamma_i|.$$

Clearly,

$$|\Gamma_{\max}| \geq \frac{1}{\ell^\delta - 1}\binom{\ell}{w}.$$

The minimum distance of this code is $2\delta + 2$.

By careful choice of parameters of $\Gamma_{\max}$ we can obtain frame-proof codes and traceability schemes.

A. A Frame-Proof Code

Fix an integer $c > 1$. Let $\sigma > 0$ be as follows:

$$\sigma = \frac{1}{2}\left(H\left(\frac{1}{c}\right) - \frac{1}{c}\right). \tag{17}$$

Take integers ℓ, w as follows:

$$w = \frac{\ell}{c}. \tag{18}$$

Take integer δ such that

$$\left(1 - \frac{1}{c}\right)w - 1 < \delta \leq \left(H\left(\frac{1}{c}\right) - \frac{1}{c} - \sigma\right)\frac{\ell}{\log \ell}. \tag{19}$$

The left inequality in (19) shows that $w - \frac{1}{c}w < \delta + 1 = w - \lambda$, and, consequently, $w > c\lambda$. So, using Lemma 2, $\Gamma_{\max}$ is a c-frame-proof code. The right inequality in (19) shows that

$$2^{(H(\frac{1}{c})-\frac{1}{c}-\sigma)\ell} \geq \ell^\delta$$

and so

$$2^{(H(\frac{1}{c})-\sigma)\ell} > (\ell^\delta - 1)2^{\ell/c}$$

which shows that

$$\frac{1}{\ell^\delta - 1} 2^{(H(\frac{1}{c})-\sigma)\ell} > 2^{\ell/c}.$$

Let ℓ also satisfy (6). Then

$$\begin{aligned} |\Gamma_{\max}| &\geq \frac{1}{\ell^\delta - 1}\binom{\ell}{w} = \frac{1}{\ell^\delta - 1} 2^{\frac{1}{\ell}\log\binom{\ell}{w}\ell} \\ &> \frac{1}{\ell^\delta - 1} 2^{(H(\frac{w}{\ell})-\sigma)\ell} = \frac{1}{\ell^\delta - 1} 2^{(H(\frac{1}{c})-\sigma)\ell} \\ &> 2^{\ell/c}. \end{aligned}$$

Note: ℓ should also satisfy

$$\log \ell < \frac{1}{2} \cdot \frac{c^2}{c-1}\sigma \tag{20}$$

for the existence of δ from (19). Hence the following theorem is obtained.

Theorem 10: For a given integer $c > 1$, there exists a c-frame-proof code which has the following parameters:

1) the length ℓ satisfies (6) and (20);
2) the number n of codewords satisfies

$$n > 2^{\ell/c};$$

3) the maximal number c of colluders tolerated is

$$c = \frac{\ell}{w}$$

where w is the weight of the code.

B. A Traceability Scheme

A similar approach can be used to construct a c-traceability scheme. Fix an integer $c > 1$. Let $\sigma > 0$ be as follows:

$$\sigma = \frac{1}{2}\left(H\left(\frac{1}{c^2}\right) - \frac{1}{c^2}\right). \tag{21}$$

Take integers $\ell,\ k$ such that

$$k = \frac{\ell}{c^2}. \tag{22}$$

Take an integer δ such that

$$\left(1 - \frac{1}{c^2}\right)k - 1 < \delta \le \left(H\left(\frac{1}{c^2}\right) - \frac{1}{c^2} - \sigma\right)\frac{\ell}{\log \ell}. \tag{23}$$

The left inequality in (23) shows that $k - \frac{1}{c^2}k < \delta + 1 = k - \lambda$, and, consequently, $k > c^2\lambda$. So using Lemma 4, $\Gamma_{\max}$ is a c-traceability scheme. The right inequality in (23) shows that

$$2^{(H(\frac{1}{c^2}) - \frac{1}{c^2} - \sigma)\ell} \ge \ell^{\delta}$$

so

$$2^{(H(\frac{1}{c^2}) - \sigma)\ell} + 2^{\ell/c^2} > \ell^{\delta} 2^{\ell/c^2}$$

that is,

$$2^{(H(\frac{1}{c^2}) - \sigma)\ell} > (\ell^{\delta} - 1)2^{\ell/c^2}$$

which shows that

$$\frac{1}{\ell^{\delta} - 1}\, 2^{(H(\frac{1}{c^2}) - \sigma)\ell} > 2^{\ell/c}.$$

Let ℓ also satisfy (6). Then

$$\begin{aligned} |\Gamma_{\max}| &\ge \frac{1}{\ell^{\delta} - 1}\binom{\ell}{k} = \frac{1}{\ell^{\delta} - 1}\, 2^{\frac{1}{\ell}\log\binom{\ell}{k}\ell} \\ &> \frac{1}{\ell^{\delta} - 1}\, 2^{(H(\frac{k}{\ell}) - \sigma)\ell} = \frac{1}{\ell^{\delta} - 1}\, 2^{(H(\frac{1}{c^2}) - \sigma)\ell} \\ &> 2^{\ell/c^2}. \end{aligned}$$

Note: ℓ should also satisfy

$$\log \ell < \frac{1}{2} \cdot \frac{c^4}{c^2 - 1}\,\sigma \tag{24}$$

for the existence of δ from (23). Hence the following theorem is proved.

Theorem 11: For a given integer $c > 1$, there exists a c-traceability scheme which has the followng parameters:

1) the total number ℓ of keys satisfies (6) and (24);
2) the number n of users satisfies

$$n > 2^{\ell/c^2};$$

3) the maximal number c of colluders tolerated is

$$c^2 = \frac{\ell}{k}$$

where k is the number of key each user has.

V. Conclusion

In this correspondence, we obtained lower bounds on the number of codewords in a c-frame-proof code and a c-traceability scheme. We showed that for some choices of parameters the bounds are tighter than the best known ones. We also gave a construction for each class of codes that has the highest number of codewords compared to all the known codes in the corresponding class.

References

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in *Advances in Cryptology—CRYPTO'95 (Lecture Notes in Computer Science}*. Berlin, Germany: Springer-Verlag, 1995, vol. 963, pp. 453–465.

[2] ——, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1897–1905, Sept. 1998.

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

[4] B. Chor, A. Fiat, and M. Naor, "Tracing traitors," in *Advances in Cryptology—CRYPTO'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 839, pp. 257–270.

[5] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology—CRYPTO'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 773, pp. 480–491.

[6] D. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *SIAM J. Discr. Math.*, vol. 11, pp. 41–53, 1998.

[7] K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," in *Advances in Cryptology—EUROCRYPT'98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1462, pp. 502–517.

[8] E. Gafni, J. Staddon, and Y. L. Yin, "Efficient methods for integrating traceability and broadcast encryption," in *Advances in Cryptology—CRYPTO'99 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1666, pp. 372–387.

[9] J. Garay, J. Staddon, and A. Wool, "Long-lived broadcast encryption," in *Advances in Cryptology—CRYPTO 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 333–352.

[10] R. L. Graham and N. J. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 37–43, Jan. 1980.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[12] D. R. Stinson and R. Wei, "Key preassigned traceability schemes for broadcast encryption," in *Proc. SAC'98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1556, pp. 144–156.

[13] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[14] H. Halberstam and K. F. Roth, *Sequences*. New York: Springer-Verlag, 1983.