We are IntechOpen, the world's leading publisher of Open Access books
Built by scientists, for scientists

4,400
Open access books available

117,000
International authors and editors

130M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

6

Polynomial-Time Codes Against Averaging Attack for Multimedia Fingerprinting

Hideki Yagi and Tsutomu Kawabata
The University of Electro-Communications
Japan

1. Introduction

With rapid advances of information technologies, a large amount of digital contents, especially multimedia, can be processed by electronic devices such as computers and smartphones. Protecting the copyrights of digital contents is of paramount importance, and *digital fingerprinting* has attracted a lot of attention for this purpose. In digital fingerprinting, a user's ID called a *fingerprint* is embedded into an original content with a watermarking technique, and then the fingerprinted contents are distributed to users.

Digital fingerprinting requires robustness against *collusion attacks*, in which more than one illicit user colludes to forge illegal contents. In the context of multimedia fingerprinting, well-known collusion attacks are the *interleaving attack* (Boneh & Shaw, 1998; Fernandez & Soriano, 2004; Silverberg et al., 2003; Staddon et al., 2001) and the *averaging attack* (Trappe et al., 2003; Wu et al., 2004). The averaging attack is particularly effective when fingerprint's watermark is embedded into host multimedia via the *spread spectrum* technique. Trappe et al. have devised collusion-secure codes, called *anti-collusion* (AC) codes, against the averaging attack based on block designs (Trappe et al., 2003). The AC codes given by Trappe et al. are also called AND-AC codes. Subsequently, several studies have proposed a method for increasing coding rates of AC codes based on a various class of block designs and related methods. Some examples are based on group-divisible design (Kang et al., 2006), finite geometries and low-density matrices (Yagi et al., 2009), and cover-free families of sets (Li et al., 2009). In order to further increase the coding rate, concatenated coding in which an outer error correcting code is concatenated with an inner AC code, has been proposed (Yagi et al., 2007). This method seems attractive since any AND-AC codes can be used as the inner codes. Whereas the concatenated codes given by (Yagi et al., 2007) greatly improve the coding rates of AC codes, the codes need *exponential-time* complexity in the code length for decoding (detecting the colluders).

In this chapter, we consider a method for constructing AC codes with *polynomial-time* encoding and decoding algorithms based on concatenated coding. We give a sufficient condition on outer error correcting codes assuring that the concatenated AC codes have a designed resilience. A polynomial-time decoding algorithm is proposed based on the list-decoding of error correcting codes. A key idea is that after the inner decoding, from the set of candidate outer symbols, we randomly create a sequence, which is input to the list-decoding of the

outer code. If the outer code's parameters satisfy the derived condition, the list-decoding algorithm can output at least one colluder's codeword correctly. We repeat this procedure until *all* the colluders' codewords are found. The proposed coding method guarantees the perfect detection of *all* the colluders in the absence of noise. Although, for fixed code length and resilience, the number of codewords of the proposed concatenated codes is smaller than that of codes in (Yagi et al., 2007), it asymptotically approaches the exponential order in the overall code length, resulting in a greater number of codewords than those of the AC codes in (Trappe et al., 2003) and (Yagi et al., 2009). In the proposed concatenated coding, any AC codes can be used as the inner code. Using AC-codes given by (Kang et al., 2006) and (Li et al., 2009) as the inner codes, we obtain analogous results.

In related work, some coding and decoding methods have been proposed for the interleaving attack (also known as the attack based on the *marking assumption*), in which one of colluders i-th codeword symbol is selected as the i-th codeword symbol of the forged fingerprint (e.g., (Boneh & Shaw, 1998; Staddon et al., 2001)). In (Silverberg et al., 2003) and (Fernandez & Soriano, 2004), the list decoding of fingerprinting codes is used. This work assures that at least one of the colluders is identified with polynomial time complexity in the code length. It seems that, in our problem setting, i.e., against the averaging attack, the realization of efficient coding is much easier because the forged fingerprint can have more information under the averaging attack. This is true in the sense that we can identify all the colluders with AC codes. However, the code construction is rather hard in terms of coding rate, since the use of orthogonal sequences in AC codes (Trappe et al., 2003; Wu et al., 2004) prevents the code size from growing exponentially in the code length. In this chapter, we aim at realizing the polynomial-time complexity in the code length as well as increasing the code size greatly based on concatenated coding and list decoding of outer codes.

The proposed method is attractive in the sense that we can construct it in a deterministic way for given parameters and implement encoding and decoding with polynomial-time complexity in the code length. However, its code size still grows *semi-exponential* in the code length. This means that the *coding rate* of this code, which is defined as the logarithm of the code size per codeword symbol, goes to zero as the code length tends to infinity. Recently, it has been pointed out by (Koga, 2010) that there exist AC codes with a strictly positive coding rate although the way of constructing such codes is still unknown. In the last part of this chapter, we show that there exist polynomial-time AC codes with a strictly positive coding rate, based on the argument given by (Koga, 2010).

2. Fingerprinting model

2.1 Digital fingerprinting

When distributing a digital content to users, a codeword (*fingerprint*) corresponding to each user is embedded into the original content by a watermarking technique. Some illicit users may collude and attempt to forge their fingerprints (*collusion attack*) so that their fingerprints are not revealed from an illegally utilized content. The detector of colluders estimates colluders' fingerprints from the forged fingerprint.

Let $\Gamma = \{1, 2, \ldots, |\Gamma|\}$ be the set of users of a digital content, where $|\cdot|$ expresses the cardinality of its argument set. We denote a codeword of user $j \in \Gamma$ by $\boldsymbol{b}_j = (\boldsymbol{b}_j^{(1)}, \boldsymbol{b}_j^{(2)}, \ldots, \boldsymbol{b}_j^{(N)}) \in$

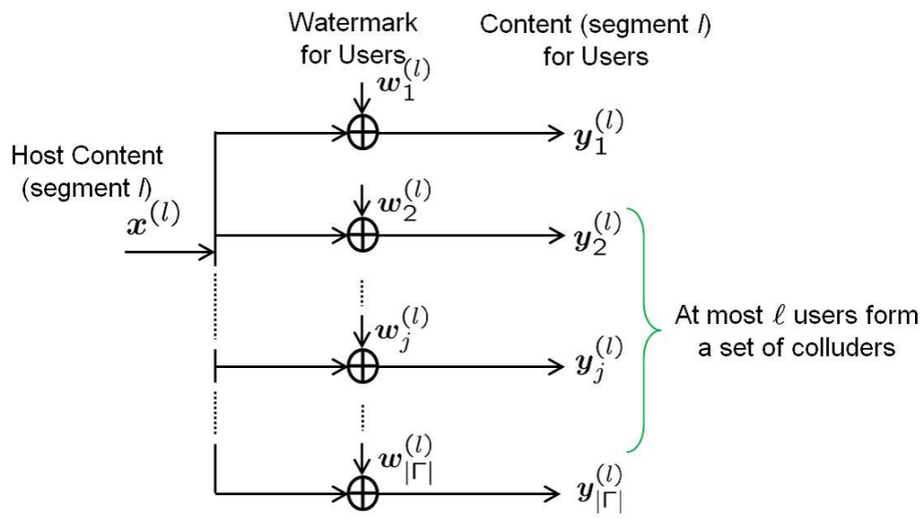


Fig. 1. A encoding procedure for multimedia fingerprinting using the spread spectrum technique. $\oplus$ denotes the real number addition of $\boldsymbol{w}_j^{(l)}$ with the host content $\boldsymbol{x}$.

$\{0,1\}^{n\times N}$ where $\boldsymbol{b}_j^{(l)} = (b_{j1}^{(l)}, b_{j2}^{(l)}, \ldots, b_{jn}^{(l)})^{\mathrm{T}} \in \{0,1\}^n$ for $l = 1, \ldots, N$ (T denotes the transposition). Let

$$\{\boldsymbol{u}_i \in \mathcal{R}^M | \, ||\boldsymbol{u}_i||^2 = 1, i = 1, 2, \ldots, n\} \tag{1}$$

be a set of n orthogonal sequences of unit power. The fingerprint watermark $\boldsymbol{w}_j = (\boldsymbol{w}_j^{(1)}, \boldsymbol{w}_j^{(2)}, \ldots, \boldsymbol{w}_j^{(N)})$ is created via the *spread spectrum* technique in which $\boldsymbol{w}_j^{(l)}$ is generated by $\{\boldsymbol{u}_i \in \mathcal{R}^M | \, i = 1, 2, \ldots, n\}$ and $\boldsymbol{b}_j^{(l)}$ as

$$\boldsymbol{w}_j^{(l)} = \sum_{i=1}^{n} (2b_{ji}^{(l)} - 1)\boldsymbol{u}_i. \tag{2}$$

Note that there always exists a set of n orthogonal sequences for every $M \geq n$. Then the created watermark signal is embedded into a host signal. Denoting the host signal by $\boldsymbol{x} = (\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(N)}) \in \mathcal{R}^{M\times N}$, the distributed content to user $j \in \Gamma$ is[1] $\boldsymbol{y}_j = \boldsymbol{x} + \boldsymbol{w}_j \in \mathcal{R}^{M\times N}$. A encoding procedure is illustrated in Fig. 1.

Since fingerprints are embedded with a watermark technique, any user cannot detect their own fingerprint $\boldsymbol{w}_j$ from the watermarked content $\boldsymbol{y}_j$. Therefore illicit users may collude to disturb their fingerprints by creating a forged content from their distributed contents.

2.2 Assumed collusion attack

We consider a set of colluders of size $h \geq 1$, denoted by $\mathcal{S}_c \subseteq \Gamma$, and without loss of generality, we assume $\mathcal{S}_c = \{1, 2, \ldots, h\}$. The attacked host signal by a set of colluders $\mathcal{S}_c$ is expressed as

[1] More precisely, each $\boldsymbol{w}_j$ is multiplied by some value called Just-Difference Noticeable (JDN) coefficient (Podilchuk & Zeng, 1998), before it is added to the host signal.

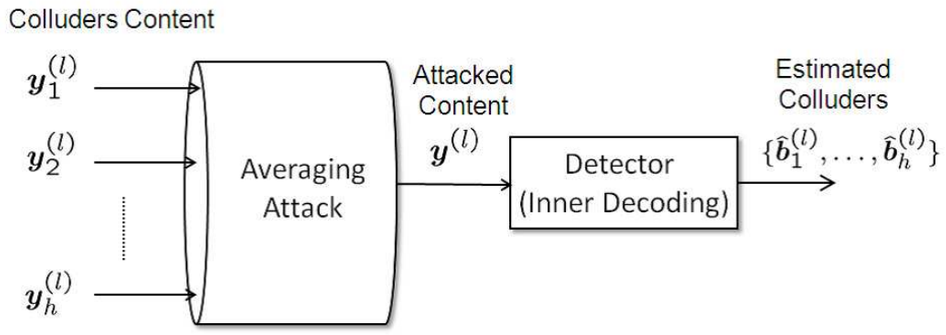


Fig. 2. Illustration of the averaging attack at segment l conducted by $\mathcal{S}_c = \{1, 2, \ldots, h\}$. The sequence $\hat{\boldsymbol{b}}_j^{(l)}$ is an estimate which corresponds to $\boldsymbol{b}_j^{(l)}$.

$\boldsymbol{y} = (\boldsymbol{y}^{(1)}, \boldsymbol{y}^{(2)}, \ldots, \boldsymbol{y}^{(N)})$ such that

$$\boldsymbol{y}^{(l)} = \frac{1}{h} \sum_{j=1}^{h} \boldsymbol{y}_j^{(l)} \tag{3}$$

for $l = 1, 2, \ldots, N$. From (2) and the relation $\boldsymbol{y}_j^{(l)} = \boldsymbol{x}^{(l)} + \boldsymbol{w}_j$, (3) can also be expressed as

$$\boldsymbol{y}^{(l)} = \boldsymbol{x}^{(l)} + \frac{1}{h} \sum_{j=1}^{h} \sum_{i=1}^{n} (2b_{ij}^{(l)} - 1)\boldsymbol{u}_i, \tag{4}$$

for $l = 1, \ldots, N$. The detector of the colluders estimates the set of colluders $\mathcal{S}_c$ from the attacked host signal $\boldsymbol{y} \in \mathcal{R}^M$. This attack is called the *averaging attack*, which is an effective collusion attack in multimedia fingerprinting (Trappe et al., 2003; Wu et al., 2004). Figure 2 illustrates the averaging attack at segment l conducted by $\mathcal{S}_c = \{1, 2, \ldots, h\}$.

In practical situations, additive noise $\boldsymbol{z} \in \mathcal{R}^{M \times 1}$ is added to $\boldsymbol{y}^{(l)}$ in (4). However, we assume the absence of noise for the time being to focus on designing codes as in (Trappe et al., 2003). Later, some extension will be discussed to deal with noise.

2.3 Concatenated anti-collusion code

In this chapter, we consider concatenated coding, which increases the coding rates of AC codes in (Trappe et al., 2003), (Yagi et al., 2009), etc. In concatenated coding, we use two kinds of codes, namely an *outer code* and an *inner code* (Forney, 1966).

Let $\mathcal{C}^o \subseteq \mathrm{GF}^N(q)$ be a q-ary linear (N, K, D) error correcting code of length N, the number of information symbols, K, and minimum distance D (Lin & Costello, 2004), which is used as the outer code. We denote any codeword by $\boldsymbol{c}_j = (c_j^{(1)}, c_j^{(2)}, \ldots, c_j^{(N)}) \in \mathcal{C}^o$.

The encoder first generates a codeword of the outer code $\mathcal{C}^o$, and then each symbol $c_j^{(l)} \in \mathrm{GF}(q)$ for $l = 1, 2, \ldots, N$ is mapped into a codeword $\boldsymbol{b}_j^{(l)} \in \mathcal{B}$, where $\mathcal{B} \subseteq \{0, 1\}^{n \times 1}$ is a binary AC code (Trappe et al., 2003) of length n (Fig. 3). The mapping of a symbol $c_j^{(l)} \in \mathrm{GF}(q)$ to a

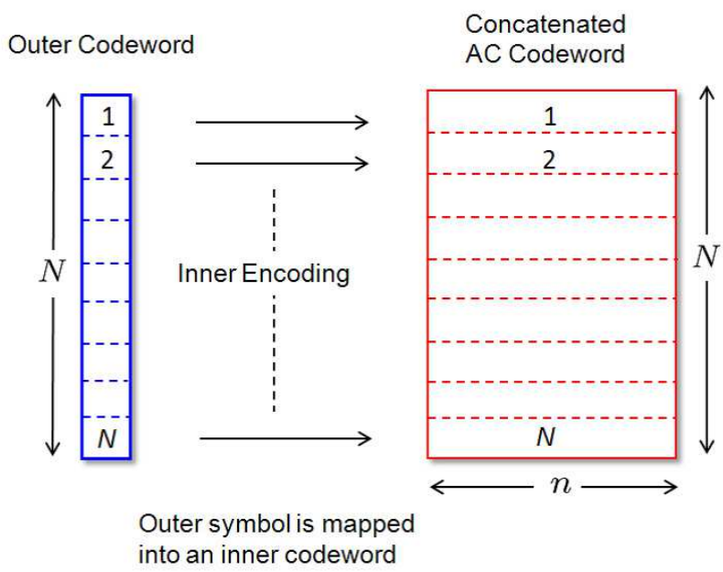


Fig. 3. Encoding procedure for a concatenated AC code. A codeword of the outer code is first generated, and each symbol is mapped into a codeword of the inner code. The total length of the concatenated AC code is $N_0 = Nn$, where N and n are the code length of the outer code and the inner code, respectively.

codeword $\boldsymbol{b}_j^{(l)} \in \mathcal{B}$ is unique and pre-determined. The code $\mathcal{B}$ is used as the inner code $\mathcal{C}^i$. We assume that $|\mathcal{B}| \geq q$ for one-to-one correspondence between q symbols of the outer code and a subset of codewords of $\mathcal{B}$. The mapped codeword is $\boldsymbol{b}_j = (\boldsymbol{b}_j^{(1)}, \ldots, \boldsymbol{b}_j^{(N)}) \in \{0,1\}^{n \times N}$. We denote the binary *concatenated code* of length $N_0 := Nn$ by $\mathcal{C} \subseteq \{0,1\}^{n \times N}$. After generating $\boldsymbol{b}_j \in \mathcal{C}$, we compute a watermark of each inner codeword $\boldsymbol{b}_j^{(l)} \in \mathcal{B}$, denoted by $\boldsymbol{w}_j^{(l)}$, by (2). If we use a trivial error correcting code, namely the (1,1,1) error correcting code, then this concatenated code reduces to the AC code in (Trappe et al., 2003) or (Yagi et al., 2009).

3. Inner codes and outer codes

3.1 Inner codes: AC codes based on finite geometries

Trappe et al. (Trappe et al., 2003) have devised anti-collusion (AC) codes, which are used as inner codes in our concatenated coding scheme. For the purpose of simple explanation, we assume $N = 1$ in this subsection. First, we give the definition of the AC codes.

Definition 1. Assume the *non-blind* scenario, in which the host signal $\boldsymbol{x}$ is known to the detector. If a set of colluders $\mathcal{S}_c$ satisfies $h \leq \ell$ for some positive integer $\ell \geq 2$, the code which can find all the colluders in $\mathcal{S}_c$ is referred to as an *ℓ-resilient AC code*. The parameter ℓ is called the *resilience* of the AC codes. □

Lemma 1 (Yagi et al., 2009)**.** *Assume that a binary matrix satisfies (i) the Hamming weight of each column is at least k, and (ii) any pair of distinct two columns has at most t 1-components in common.*

Then, the AC code whose codewords are all column vectors of this matrix is a $(\lceil k/t \rceil - 1)$*-resilient AC code. i.e., if* $h \leq \lceil k/t \rceil - 1$*, any set of colluders* $\mathcal{S}_c$ *can be uniquely detected*[2]. □

Remark 1. Let $\mathcal{Q}(\mathcal{S}_c)$ be the set of symbol positions where all of the fingerprints in $\mathcal{S}_c$ take the 0-component. Then an ℓ-resilient AC code in (Trappe et al., 2003) and (Yagi et al., 2009) uniquely identifies the set $\mathcal{Q}(\mathcal{S}_c)$ for any $\mathcal{S}_c$ with $h \leq \ell$. □

From Remark 1, since an ℓ-resilient AC code uniquely identifies $\mathcal{Q}(\mathcal{S}_c)$ for any $\mathcal{S}_c$ of size less than or equal to ℓ, the code reveals the set of colluders $\mathcal{S}_c$. For a detailed procedure of the inner decoding, refer to (Trappe et al., 2003).

In (Yagi et al., 2009), an algebraic construction of ℓ-resilient AC codes has been proposed based on finite geometries. We will use these AC codes as the inner code in concatenated coding for a comparison purpose though any AC codes can also be used. For a prime p and two positive integers m and s $(m \geq 2, s \geq 1)$, the m-dimensional *Euclidean geometry* $\mathrm{EG}(m, p^s)$ over a Galois field $\mathrm{GF}(p^s)$ consists of *points*, *lines*, and *hyperplanes*. Any points in $\mathrm{EG}(m, p^s)$ are p^{ms} m-dimensional vectors over $\mathrm{GF}(p^s)$, and they form an m-dimensional vector space V over $\mathrm{GF}(p^s)$. For μ such that $0 \leq \mu \leq m$, a μ-dimensional hyperplane (generally, called a *μ-flat*) is a μ-dimensional subspace of V and its cosets, and any μ-flat contains $p^{\mu s}$ points. Points correspond to 0-flats. Any pair of two μ-flats, (F_1, F_2), has at most one $(\mu - 1)$-flat in common, which implies F_1 and F_2 have at most $p^{(\mu-1)s}$ points in common. In a Euclidean geometry $\mathrm{EG}(m, p^s)$, there are

$$f_{\mathrm{EG}}(\mu) = p^{(m-\mu)s} \prod_{i=1}^{\mu} \frac{p^{(m-i+1)s} - 1}{p^{(\mu-i+1)s} - 1} \tag{5}$$

μ-flats in total.

Letting $n_0 = f_{\mathrm{EG}}(0)$, consider an $n_0 \times f_{\mathrm{EG}}(\mu)$ matrix $B_\mu = (b_{ij})$. An element b_{ij} in a matrix B_μ takes $b_{ij} = 1$ if point i is contained in μ-flat j, or takes $b_{ij} = 0$ otherwise. This matrix B_μ is called the *incident matrix of μ-flats over points* in $\mathrm{EG}(m, p^s)$. Allocating the j-th column vector $\boldsymbol{b}_j$ of B_μ to the j-th user's fingerprint, the obtained code $\mathcal{B}_\mu = \{\boldsymbol{b}_j\}$ is called the *μ-th order EG-AC code*.

Lemma 2 (Yagi et al., 2009)**.** *For given* $\mathrm{EG}(m, p^s)$*, the μ-th order EG-AC code* $\mathcal{B}_\mu$ *is a* $(p^s - 1)$*-resilient AC code of length* $n_0 = p^{ms}$ *and the number of codewords* $f_{\mathrm{EG}}(\mu)$. □

We mention parameters of EG-AC codes (Yagi et al., 2009). Let μ^* express dimension μ that maximizes $f_{\mathrm{EG}}(\mu)$. The number of codewords is $f_{\mathrm{EG}}(\mu^*) = \nu n_0^{\frac{1}{4}(m+2)}$ with some $1 \leq \nu < 2^{\frac{m}{2}}$. This means that the number of codewords increases in polynomial order $\Theta(n_0^{\frac{1}{4}(m+2)})$ of code length n_0.

3.2 Outer codes: Existing condition on error correcting codes

We state a previous condition on outer error-correcting codes (Yagi et al., 2007).

[2] $\lceil v \rceil$ expresses the minimum integer not less than v.

We define the Hamming distance between a sequence and a sequence set. Let $\boldsymbol{c}_j = (c_j^{(1)}, c_j^{(2)}, \ldots, c_j^{(N)}) \in \mathcal{C}^o$ such that $c_j^{(l)} \in \mathrm{GF}(q)$ for $l = 1, 2, \ldots, N$ be a codeword of the outer code $\mathcal{C}^o$. We define the following sets:

$$\mathcal{Y}^{(l)} = \{c_j^{(l)} | \, j \in \mathcal{S}_c\}, \tag{6}$$

and

$$\mathcal{Y} = \mathcal{Y}^{(1)} \times \mathcal{Y}^{(2)} \times \cdots \times \mathcal{Y}^{(N)} = \prod_{l=1}^{N} \mathcal{Y}^{(l)}. \tag{7}$$

The set $\mathcal{Y}^{(l)}$ expresses the set of symbols over $\mathrm{GF}(q)$ which give $\boldsymbol{y}^{(l)}$ (recall that there is one-to-one correspondence between symbols over $\mathrm{GF}(q)$ and a subset of inner codewords). We define the Hamming distance between a symbol $v \in \mathrm{GF}(q)$ and the set $\mathcal{Y}^{(l)}$ as

$$\delta(v, \mathcal{Y}^{(l)}) = \begin{cases} 0, & \text{if } v \in \mathcal{Y}^{(l)}; \\ 1, & \text{otherwise.} \end{cases} \tag{8}$$

We define the Hamming distance between a codeword $\boldsymbol{c}_j = (c_j^{(1)}, c_j^{(2)}, \ldots, c_j^{(N)}) \in \mathcal{C}^o$ such that $c_j^{(l)} \in \mathrm{GF}(q), l = 1, 2, \ldots, N$, and the set $\mathcal{Y}$ as

$$d_H(\boldsymbol{c}_j, \mathcal{Y}) = \sum_{l=1}^{N} \delta(c_j^{(l)}, \mathcal{Y}^{(l)}). \tag{9}$$

Definition 2. For a set of colluders $\mathcal{S}_c$ such that $h \leq \ell$ and any codeword $\boldsymbol{c}_j \in \mathcal{C}^o$ with $j \in \Gamma \setminus \mathcal{S}_c$, if at least r codewords $\boldsymbol{c}_i$ such that $i \in \mathcal{S}_c$ satisfy

$$d_H(\boldsymbol{c}_i, \mathcal{Y}) < d_H(\boldsymbol{c}_j, \mathcal{Y}), \tag{10}$$

then the concatenated code $\mathcal{C}$ is called the (ℓ, r)-*resilient concatenated AC (CAC) code* for $\mathcal{Y}$. □

The following theorem states a condition on the outer code $\mathcal{C}^o$ assuring that a concatenated code $\mathcal{C}$ becomes an (ℓ, h)-resilient AC code.

Theorem 1 (Yagi et al., 2007)**.** *Assume that we use an ℓ-resilient AC code $\mathcal{B}$ as the inner code. If $h \leq \ell$ and a q-ary (N, K, D) error-correcting code such that*

$$D > N\left(1 - \frac{1}{\ell}\right) \tag{11}$$

is used as the outer code, the concatenated code $\mathcal{C}$ is an (ℓ, h)-resilient CAC code for $\mathcal{Y}$. □

The (ℓ, r)-resilient CAC codes enable us to detect at least r colluders in $\mathcal{S}_c$ by simply calculating the Hamming distance after obtaining each $\mathcal{Y}^{(l)}$ for $l = 1, 2, \ldots, N$ via the inner decoding. However, we need to exhaustively search codewords in $\mathcal{C}^o$, and a decoding algorithm requires exponential time complexity in outer code length N, i.e., $O(q^N)$. In (Yagi et al., 2007), the use of the Reed-Solomon (RS) codes is suggested as the outer codes. The RS code is an instance of the maximum distance separable (MDS) codes which meet Singleton's bound

$D \leq N - K + 1$ with equality, and $N = q - 1$ for a prime power q (Lin & Costello, 2004). In this case, the decoding complexity is expressed as $O(2^{N \log N})$. Further, $N_0 = \Theta(N^{\frac{m+6}{m+2}})$ since $n = \Theta(N^{\frac{4}{m+2}})$. Therefore, the overall decoding complexity[3] is $O(2^{N_0 \log N_0})$.

4. Polynomial-time concatenated AC codes

4.1 Condition on outer codes with ℓ-resilience

A main idea to give polynomial-time decodable concatenated codes is that after the inner decoding, we randomly create a sequence from the candidate symbol set $\mathcal{Y}$. Upon input of this sequence, a list-decoding algorithm for the outer code outputs at least one colluder's codeword. Like this, we consider iterating the following procedure:

(i) Set $\tau := 1$ and $\mathcal{Y}_0^{(l)} := \mathcal{Y}^{(l)}$ for each $l = 1, \ldots, N$.

(ii) Randomly pick a symbol $\tilde{y}_\tau^{(l)}$ from $\mathcal{Y}_{\tau-1}^{(l)}$ for each $l = 1, \ldots, N$, and set $\tilde{\mathcal{Y}}_\tau^{(l)} := \{\tilde{y}_\tau^{(l)}\}$ and $\tilde{\boldsymbol{y}}_\tau := (\tilde{y}_\tau^{(1)}, \ldots, \tilde{y}_\tau^{(N)})$.

(iii) Find all $j \in \Gamma$ such that

$$d_H(\boldsymbol{c}_j, \tilde{\boldsymbol{y}}_\tau) \leq N(1 - 1/\ell), \tag{12}$$

and the set of found colluders is denoted by $\mathcal{S}_{c,\tau}$. We define $\mathcal{Y}_\tau^{(l)}$ and $\mathcal{Y}_\tau$ in a similar way to (6) and (7), respectively, by replacing $\mathcal{S}_c$ with $\mathcal{S}_c \setminus \bigcup_{i=1}^{\tau} \mathcal{S}_{c,i}$ (notice that $|\mathcal{Y}_\tau^{(l)}| \leq |\mathcal{Y}_{\tau-1}^{(l)}|$ for every $l = 1, \ldots, N$).

(iv) Set $\tau := \tau + 1$, and go to step (ii). We repeat this procedure until there are no codewords satisfying (12).

Proposition 1. *Assume that the inner code is an ℓ-resilient AC code $\mathcal{B}$. If $h \leq \ell$ and a q-ary (N, K, D) error-correcting code such that*

$$D > N\left(1 - \frac{1}{\ell^2}\right) \tag{13}$$

is used as the outer code, the concatenated code $\mathcal{C}$ is an (ℓ, h_τ)-resilient CAC code for each $\tilde{\mathcal{Y}}_\tau$, where $h_\tau = |\mathcal{S}_{c,\tau}|$.

(Proof) Let $\boldsymbol{c}_j = (c_j^{(1)}, c_j^{(2)}, \ldots, c_j^{(N)}) \in \mathcal{C}^o$ such that $c_j^{(l)} \in \mathrm{GF}(q)$ for $l = 1, 2, \ldots, N$ be the j-th users' outer codeword. By the definition of $\mathcal{S}_{c,\tau}$, there are h_τ colluders whose $\boldsymbol{c}_i, i \in \mathcal{S}_{c,\tau}$, satisfy $d_H(\boldsymbol{c}_i, \tilde{\boldsymbol{y}}_\tau) \leq N(1 - 1/\ell)$. On the other hand, since any fingerprint $\boldsymbol{c}_j, j \in \Gamma \setminus \mathcal{S}_c$, agrees at most $(N - D)$ symbols with each fingerprint $\boldsymbol{c}_i, i \in \mathcal{S}_{c,\tau}$, any $\boldsymbol{c}_j$ agrees at most $\ell(N - D)$ symbols with $\tilde{\boldsymbol{y}}_\tau$. Therefore we have

$$\begin{aligned} d_H(\boldsymbol{c}_j, \tilde{\boldsymbol{y}}_\tau) &= N - \ell(N - D) \\ &> N - \ell N + \ell N\left(1 - \frac{1}{\ell^2}\right) = N\left(1 - \frac{1}{\ell}\right). \end{aligned} \tag{14}$$

[3] The complexity of encoding is $O(N_0^2)$ in the concatenated coding.

Since $d_H(\boldsymbol{c}_i, \tilde{\boldsymbol{y}}_\tau) \leq N(1-1/\ell)$, (14) implies $d_H(\boldsymbol{c}_j, \tilde{\boldsymbol{y}}_\tau) > d_H(\boldsymbol{c}_i, \tilde{\boldsymbol{y}}_\tau)$. Therefore we can correctly detect h_τ colluders in $\mathcal{S}_{c,\tau}$ by comparing the Hamming distance from $\tilde{\boldsymbol{y}}_\tau$. □

The condition (13) is the same as the condition of ℓ-traceability (TA) codes against the interleaving attack (Staddon et al., 2001; Silverberg et al., 2003), which identify at least one colluder in $\mathcal{S}_c$ of size less than or equal to ℓ. The condition (13) is weaker than (11) in the sense that (13) is sufficient to satisfy (11).

By Singleton's bound, the minimum distance of a linear error correcting code satisfies $D \leq N - K + 1$. Since it is desirable to make D as large as possible, we may well use the RS code satisfying $D = N - K + 1$ as the outer code. For given prime power q, there always exists a lengthened/shortened RS code for every $N \leq q$ if $K \geq 1$ and $D = N - K + 1$. Other promising candidates for the outer code are algebraic geometry (AG) codes or near-MDS expander codes in (Guruswami, 2004), which asymptotically meet Singleton's bound. All these codes can be decoded by the Guruswami-Sudan (GS) list-decoding algorithm (Guruswami, 2004), which corrects up to $N(1-\sqrt{(K-1)/N})$ errors with the polynomial time complexity in N (Silverberg et al., 2003).

4.2 Decoding algorithm for concatenated AC codes

We propose a polynomial-time decoding algorithm for a concatenated code $\mathcal{C}$ base on Proposition 1. As in (Fernandez & Soriano, 2004) and (Silverberg et al., 2003) for ℓ-TA codes against the interleaving attack, we employ a code $\mathcal{C}^o$ that can be decoded by the GS list-decoding algorithm. The detail decoding procedure is described as follows:

[Proposed Decoding Algorithm]

(1) For each $\boldsymbol{y}^{(l)}$, $l = 1, \ldots, N$ given by (4), find all the members in $\mathcal{Y}^{(l)}$ via the decoding of the inner AC code.

(2) Set $\tau_{\max} := \max_{1 \leq l \leq N} |\mathcal{Y}^{(l)}|$, $\tau := 1$ and $\mathcal{Y}_0^{(l)} := \mathcal{Y}^{(l)}$ for each $l = 1, \ldots, N$.

(3) Randomly pick $\tilde{y}_\tau^{(l)} \in \mathcal{Y}_{\tau-1}^{(l)}$ for each $l = 1, \ldots, N$, and set $\tilde{\boldsymbol{y}}_\tau := (\tilde{y}_\tau^{(1)}, \ldots, \tilde{y}_\tau^{(N)})$.

(4) Execute the GS list-decoding algorithm for $\tilde{\boldsymbol{y}}_\tau$, and find the set $\mathcal{S}_{c,\tau}$.

(5) Set $\mathcal{Y}_\tau^{(l)}$ for $l = 1, \ldots, N$ as

$$\mathcal{Y}_\tau^{(l)} := \begin{cases} \mathcal{Y}^{(l)} \setminus \bigcup_{i=1}^{\tau-1} \mathcal{Y}_i^{(l)}, & \text{if } \mathcal{Y}^{(l)} \neq \bigcup_{i=1}^{\tau-1} \mathcal{Y}_i^{(l)}, \\ \mathcal{Y}^{(l)}, & \text{otherwise,} \end{cases} \tag{15}$$

and set $\mathcal{Y}_\tau := \prod_{l=1}^{N} \mathcal{Y}_\tau^{(l)}$.

(6) If $\tau = \tau_{\max}$ or $|\bigcup_{i=1}^{\tau} \mathcal{S}_{c,i}| = \tau_{\max}$, then output $\bigcup_{i=1}^{\tau} \mathcal{S}_{c,i}$ as colluders and halt the algorithm. Otherwise, set $\tau := \tau + 1$ and go to step (3).

We note that in step (1), which corresponds to the inner decoding, $\mathcal{Y}^{(l)}$ for $l = 1, \ldots, N$ are correctly found although we cannot see $\mathcal{S}_c$ itself. We show that if the outer code satisfies the condition (13), then $\mathcal{S}_{c,\tau}$ is correctly found at step (4) in each iteration by the following lemmas:

Lemma 3. *If $h \leq \ell$ and an outer code satisfying (13) is concatenated with an ℓ-resilient AC code, there is some $l \in \{1, \ldots, N\}$ such that $|\mathcal{Y}^{(l)}| = h$. i.e., the maximum number of iterations of the proposed decoding algorithm is $\tau_{\max} = h$.*

(Proof) If $h = 2$, then there is at least D positions such that $|\mathcal{Y}^{(l)}| = 2$ because the Hamming distance of any two outer codewords is at least D. For the case $h \geq 3$, the symbols of user 1's codeword $\boldsymbol{c}_1$ and user 2's codeword $\boldsymbol{c}_2$ are different in at least D positions and we denote this position set by $\mathcal{D}$. Then user 3's codeword $\boldsymbol{c}_3$ cannot agree more than $N - D$ symbols with each of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ in the position indexed by $\mathcal{D}$. i.e.,

$$|\{i|c_{ji} = c_{3i}, i \in \mathcal{D}\}| \leq N - D, \text{ for } j = 1, 2. \tag{16}$$

Therefore, there are at least $D - 2(N - D)$ positions in which all three codewords disagree. When we consider the forth codeword $\boldsymbol{c}_4$, the same argument gives at least $D - (2 + 3)(N - D)$ positions in which all four codewords disagree. By induction, among $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_\nu\}$ such that $\nu \leq h$, the number of positions in which all the codewords $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\nu$ disagree is at least

$$\begin{aligned} &D - (2 + 3 + \cdots + (\nu - 1))(N - D) \\ &\qquad > D - \frac{1}{2}(\ell - 2)(\ell + 1)(N - D). \end{aligned} \tag{17}$$

Since (13) is satisfied, the r.h.s. of (17) is further bounded by

$$\frac{N}{2}\left(1 + \frac{1}{\ell}\right) \tag{18}$$

from below. Equation (18) implies that the lemma holds. □

Lemma 4. *If $h \leq \ell$ and the outer code satisfies (13), all the codewords satisfying (12) for given $\tilde{\boldsymbol{y}}_\tau$ are correctly found at step (4).*

(Proof) If (13) is satisfied, then we can easily check

$$N(1 - 1/\ell) < N\left(1 - \sqrt{(K - 1)/N}\right) \tag{19}$$

where the r.h.s. expresses the correcting radius of the GS list-decoding algorithm (Silverberg et al., 2003). Therefore all the codewords satisfying (12) are found in step (4). □

The next theorem states the number of colluders captured by the proposed decoding algorithm in the absence of noise.

Theorem 2. *If $h \leq \ell$ and we use an ℓ-resilient AC code $\mathcal{B}$ as the inner code and an (N, K, D) error correcting code satisfying (13) as the outer code, then the proposed decoding algorithm finds all the colluders in $\mathcal{S}_c$.*

(Proof) In the first iteration $\tau = 1$, obviously there is at least one colluder's codeword $\boldsymbol{c}_j \in \mathcal{C}^o$ which is in the distance $d_H(\boldsymbol{c}_i, \tilde{\boldsymbol{y}}_1) \leq N(1 - 1/\ell)$ and can be decoded by the GS list-decoding. This implies that all the colluders can be found if $h = 2$.

Let some $h, 3 \leq h \leq \ell$, be given, and we first assume that in each iteration only one colluder's codeword is found before iteration $\tau, 2 \leq \tau \leq h$. In iteration τ, we assume that the colluders

found so far are denoted by $\tilde{\boldsymbol{c}}_1, \ldots, \tilde{\boldsymbol{c}}_{\tau-1}$ for simplicity. Let a function $\Delta(\tau)$ be defined as

$$\Delta(\tau) = D - (\tau - 1)(N - D) \tag{20}$$

Since any two codewords agree in at most $N - D$ positions, each of remaining $\tilde{\boldsymbol{c}}_\tau, \ldots, \tilde{\boldsymbol{c}}_h$ agrees at least $\Delta(\tau)$ positions with $\mathcal{Y}_{\tau-1}$, which has been calculated at step (5) in iteration $\tau - 1$. By using (13), $\Delta(\tau)$ is bounded as

$$\Delta(\tau) > N(1 - \tau/\ell^2). \tag{21}$$

When randomly picking $\tilde{\boldsymbol{y}}_\tau$ at step (3) in iteration τ, there is at least one codeword among $\tilde{\boldsymbol{c}}_\tau, \ldots, \tilde{\boldsymbol{c}}_h$ which agrees greater than or equal to $\Delta(\tau)/(h - \tau + 1)$ positions with $\tilde{\boldsymbol{y}}_\tau$, which is bounded as

$$\Delta(\tau)/(h - \tau + 1) > N(1 - \tau/\ell^2)/(h - \tau + 1). \tag{22}$$

The r.h.s. of (22) is greater than N/ℓ since

$$\begin{aligned} \frac{N}{h - \tau + 1}\left(1 - \frac{\tau}{\ell^2}\right) - \frac{N}{\ell} &= \frac{N\{\ell(\ell - h) + \ell\tau - \ell - \tau\}}{(h - \tau + 1)\ell^2} \\ &\geq \frac{N(h\tau - h - \tau)}{(h - \tau + 1)\ell^2}, \end{aligned} \tag{23}$$

where we substitute $h = \ell$ to obtain the last inequality. The r.h.s. of (23) is apparently greater than zero for $h \geq 3$ and $\tau \geq 2$. This in turn implies that there is at least one codeword $\boldsymbol{c}_j, \tau \leq j \leq h$, such that $d_H(\boldsymbol{c}_j, \tilde{\boldsymbol{y}}_\tau) \leq N(1 - 1/\ell)$ and it can be found by the GS-list decoding algorithm.

The case where in some iteration $\tau' < \tau$, more than one colluder's codeword is found can be proved in a similar way. □

We state the time complexity of the proposed decoding algorithm by assuming an RS code is used as the outer code. As for the inner decoding (step (1)), we conduct the exhaustive search of all the combinations of ℓ or less inner codewords. The number of inner codewords is $q = O(N)$, so the time complexity for each inner decoding is $O(N^\ell)$, which is polynomial time in code length N_0. In each iteration, we execute the GS list-decoding algorithm for the outer code, which requires the time complexity of $O(N^{15})$ for iteration $\tau = 1$ when $h = \ell$ and of $O(N^4)$ for iteration $\tau \geq 2$ (or $\tau \geq 1$ when $h < \ell$). Since the maximum number of iteration is ℓ, the overall decoding complexity is bounded by $\max\{O(N^{\ell+1}), O(N^{15})\}$ when $h = \ell$. When $h < \ell$, we can also show that the overall decoding complexity is bounded by $\max\{O(N^{\ell+1}), O(hN^4)\}$.

4.3 Coding rates of concatenated AC codes

As for the inner code $\mathcal{C}^i = \mathcal{B}$, we require only the condition that $|\mathcal{B}| \geq q$, where q is the number of symbols of an outer code $\mathcal{C}^o$. If $|\mathcal{B}|/q > 1$, we can divide the CAC codes into several groups. Define $g = \lfloor |\mathcal{B}|/q \rfloor$. We first divide an inner code $\mathcal{B}$ into g disjoint subsets $\mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \ldots, \mathcal{B}^{(g)}$ such that $|\mathcal{B}^{(i)}| \geq q, i = 1, 2, \ldots, g$. By using each $\mathcal{B}^{(i)}$ as the inner codes, we obtain g disjoint concatenated codes, denoted by $\mathcal{C}^{(1)}, \mathcal{C}^{(2)}, \ldots, \mathcal{C}^{(g)}$. The overall code $\mathcal{C} =$

$\bigcup_{i=1}^{g} \mathcal{C}^{(i)}$ is an ℓ-resilient CAC code with size $F_0 := gq^K$ if each concatenated code $\mathcal{C}^{(i)}$ is an ℓ-resilient AC code. Coding rate R_0 of $\mathcal{C}$ is given by $R_0 = (\log_2 gq^K)/N_0$.

Example 1. We show the numbers of codewords of five CAC codes $\mathcal{C}$ which consist of EG-AC inner codes $\mathcal{C}^i = \mathcal{B}$ and MDS outer codes $\mathcal{C}^o$ (shortened RS codes (Lin & Costello, 2004)). For comparison, we show conventional EG-AC codes $\mathcal{B}_\mu$ (Yagi et al., 2007) with the same resilience and the code length. Table 1 shows the parameters of original and concatenated EG-AC codes and Table 2 shows the logarithm of the number of codewords for each code. From Table 2, it can be found that the CAC codes is effective. In particular, as the code length becomes large, the effectiveness of the CAC codes is enhanced. □

We now analyze the asymptotic number of codewords by assuming an (N, K, D) RS code satisfying (13) and an EG-AC code of the maximal order μ^* are used as the outer code and the inner code, respectively. For simplicity, we assume $q = N$, which means that the lengthened RS code is used. The EG-AC code of the maximal order μ^* satisfies $f_{\mathrm{EG}}(\mu^*) = \nu n^{\frac{1}{4}(m+2)}$ with some $\nu, 1 \le \nu < 2^{\frac{m}{2}}$ (Yagi et al., 2009). There exists an $m > 3$ such that $\nu n^{\frac{1}{4}(m+1)} < q \le \nu n^{\frac{1}{4}(m+2)}$, and hence

$$\nu n^{\frac{1}{4}(m+1)} < N \le \nu n^{\frac{1}{4}(m+2)} \tag{24}$$

from $N = q$. Note that the condition (13) is equivalent to $K < N/\ell^2 + 1$ since $K = N - D + 1$, but there always exit RS codes with $K \ge N/\ell^2$ (this can be confirmed by setting $D = \lceil N(1 - 1/\ell^2) \rceil$). Then the total number of codewords $F_0 := q^K = N^K$ satisfies

$$F_0 \ge 2^{N \log N/\ell^2}. \tag{25}$$

Since the overall length of the concatenated code is $N_0 = Nn$ where $n \le (N/\nu)^{\frac{4}{m+1}}$ from (24), we have $N \ge (N_0 \nu^{\frac{4}{m+1}})^{\frac{m+1}{m+5}}$, and (25) becomes

$$F_0 \ge 2^{\nu' \cdot \frac{m+1}{(m+5)} \cdot \frac{\log N_0}{\ell^2} \cdot N_0^{\frac{m+1}{(m+5)}}} \tag{26}$$

where $\nu' = \nu^{\frac{4}{m+5}}$. Furthermore, by carefully investing the parameters of EG-AC codes, we find

$$m^2 + 6m + 2m \log_{\ell+1} 2 = 4 \log_{\ell+1} N_0, \tag{27}$$

resulting in $m = \Theta(2(\log_{\ell+1} N_0)^{\frac{1}{2}})$. We have $m \to \infty$ as $N_0 \to \infty$ and $\nu' \ge 1$. Thus, for any $\epsilon, 0 < \epsilon < 1$, there exists a concatenated AC code such that

$$F_0 \ge 2^{\frac{(1-\epsilon) N_0^{1-\epsilon} \log N_0}{\ell^2}} \tag{28}$$

with sufficiently large N_0. Equation (28) implies that the number of codewords increases arbitrarily closely in the exponential order of $N_0 \log N_0/\ell^2$, which is equal to a single RS code of length N_0. Thus, the number of codewords of the proposed concatenated codes is much greater than those of the AC codes in (Yagi et al., 2009).

No.	EG-AC code $\mathcal{B}_\mu$		Concatenated EG-AC code $\mathcal{C}$			
			Inner Code $\mathcal{C}^i$		Outer Code $\mathcal{C}^o$	
	(m, p^s)	n	(m, p^s)	n	(N, K, D)	q
(i)	$(4, 3^1)$	81	$(2, 3^1)$	9	$(9, 3, 7)$	11
(ii)	$(6, 3^1)$	729	$(3, 3^1)$	27	$(27, 7, 21)$	32
(iii)	$(7, 3^1)$	2187	$(4, 3^1)$	81	$(27, 7, 21)$	81
(iv)	$(8, 3^1)$	6561	$(4, 3^1)$	81	$(81, 21, 61)$	81
(v)	$(6, 2^2)$	4096	$(3, 2^2)$	64	$(64, 8, 57)$	64

Table 1. Parameters of original and concatenated EG-AC codes

No.	Resilience ℓ	Code length Nn	# of Information Symbols	
			$\log_2 \lvert\mathcal{B}_\mu\rvert$	$\log_2 \lvert\mathcal{C}\rvert$
(i)	2	81	10.19	10.38
(ii)	2	729	19.80	35.00
(iii)	2	2187	26.16	44.38
(iv)	2	6561	32.52	133.14
(v)	3	4096	24.52	48.00

Table 2. Examples of the number of codewords of original and concatenated EG-AC codes

4.4 Conditions of outer codes with ℓ-resilience and e-error correcting capability

The ℓ-resilient AC codes in Sect. 3.1 do not have error-correcting capability. On the other hand, with concatenated coding, we can make ℓ-resilient CAC codes have such capability. In the presence of noise in (4), i.e.,

$$\boldsymbol{y}^{(l)} = 1/h \sum_{j=1}^{h} \boldsymbol{y}_j^{(l)} + \boldsymbol{z} \tag{29}$$

where $\boldsymbol{z} \in \mathcal{R}^{n\times 1}$ is a vector of additive noise, this is particularly important because some of inner decoders may result in mis-correction (Trappe et al., 2003). For some non-negative integer e, we derive conditions on an outer code $\mathcal{C}^o$ assuring that a concatenated code $\mathcal{C}$ have an (ℓ, r)-resilience and e-error correcting capability[4].

Proposition 2. *Assume that an ℓ-resilient AC code $\mathcal{B}$ is used as the inner code, and an (N, K, D) error correcting code satisfying*

$$D > N\left(1 - \frac{1}{\ell^2}\right) + \frac{(\ell+1)e}{\ell^2} \tag{30}$$

is used as the outer code. If $h \leq \ell$ and the number of inner decoders whose outputs are in error is less than or equal to e, the concatenated code $\mathcal{C}$ is an (ℓ, h_τ)-resilient CAC code for each $\tilde{\mathcal{Y}}_\tau$ (defined in Sect. 4.1), where $h_\tau = |\mathcal{S}_{c,\tau}|$.

(Proof) Let $\boldsymbol{c}_j = (c_j^{(1)}, c_j^{(2)}, \ldots, c_j^{(N)}) \in \mathcal{C}^o$ such that $c_j^{(l)} \in \mathrm{GF}(q)$ for $l = 1, 2, \ldots, N$ be the j-th users' outer codeword. There are h_τ colluders such that each of $\boldsymbol{c}_i, i \in \mathcal{S}_{c,\tau}$ agrees at least

[4] We can introduce *erasure* symbols instead of error symbols as in (Fernandez & Soriano, 2004), which was introduced against the interleaving attack.

$(N-e)/\ell$ symbols in $\tilde{\mathcal{Y}}_\tau$, i.e., we have

$$d_H(\boldsymbol{c}_i, \tilde{\mathcal{Y}}_\tau) \leq N - (N-e)/\ell. \tag{31}$$

On the other hand, any fingerprint $\boldsymbol{c}_j, j \in \Gamma \setminus \mathcal{S}_c$ agrees at most $\ell(N-D)+e$ symbols in $\tilde{\mathcal{Y}}_\tau$. We have

$$\begin{aligned} d_H(\boldsymbol{c}_j, \tilde{\mathcal{Y}}_\tau) - d_H(\boldsymbol{c}_i, \tilde{\mathcal{Y}}_\tau) &\geq N - \ell(N-D) - e \\ &\quad -(N-(N-e)/\ell) > 0, \end{aligned} \tag{32}$$

for $\ell \geq 2$. Therefore the condition (10) is satisfied. □

Theorem 3. *Assume that we use an ℓ-resilient AC code $\mathcal{B}$ as the inner code and an (N, K, D) error correcting code satisfying (30) as the outer code. If the number of inner decoders whose outputs are in error is less than or equal to e, then the proposed decoding algorithm finds all the colluders in $\mathcal{S}_c$.* □

It follows from (13) and (30) that the e-error correcting capability requires a more stringent condition on D by $(\ell+1)e/\ell^2$. In this case, we can also use an MDS or a near-MDS code as the outer code $\mathcal{C}^o$.

5. Existence of polynomial-time AC codes with a positive rate

The proposed method given in the previous section is of importance from the fact that we can construct it in a deterministic way for given parameters and implement encoding and decoding with polynomial-time complexity in n. Theorem 2 indicates that the size of the concatenated AC codes still grows *semi-exponential* in the code length, and the *coding rate* of this code goes to zero as n tends to infinity. Recently, it has been pointed out by (Koga, 2010) that there exist AC codes with a strictly positive coding rate although it is not clear how to construct such codes. Here, we show that there exist polynomial-time AC codes with a strictly positive coding rate, based on the argument given by (Koga, 2010).

First, we review a result on the coding rate of ℓ-resilient AC codes shown by (Koga, 2010).

Theorem 4 (Koga, 2010)**.** *For given $\ell \geq 2$, there exists at least one ℓ-resilient AC code with the coding rate*

$$R = \frac{1}{4^\ell + 1}. \tag{33}$$

for sufficiently large n. □

Theorem 4 is an " existence theorem" which indicates only the existence of good AC codes but does not imply how to construct such codes. In addition, encoding and decoding complexity is in the exponential order of n, which seems impractical even though such codes can be obtained. The next theorem shows the existence of ℓ-resilient AC codes that can be encoded and decoded with polynomial order complexity in n.

Theorem 5. *For given $\ell \geq 2$, there exists at least one ℓ-resilient concatenated AC code that can encoded and decoded with polynomial order complexity in n with the coding rate*

$$R = \frac{1}{\ell^2(4^\ell + 1)}. \tag{34}$$

for sufficiently large n.

(Proof) This theorem can be easily proven by noticing that the coding rate is decreased by the factor of $1/\ell^2$ if concatenated coding is used. □

From Theorem 5, we can reduce the encoding and decoding complexity to a great extent by allowing the coding rate decreases by the factor of $\frac{1}{\ell^2}$. However, it is guaranteed that the existence of an ℓ-resilient concatenated AC code whose coding rate is still strictly positive for all $\ell \geq 2$.

6. Conclusion

In this chapter, for multimedia fingerprinting, concatenated coding in which the outer code is a near-MDS error correcting code and the inner code is a class of AC codes in (Trappe et al., 2003) and (Yagi et al., 2009), was proposed. Using AC codes given by (Kang et al., 2006) and (Li et al., 2009) as the inner codes, a similar result can be obtained. Based on list-decoding for the outer code, we proposed a polynomial-time decoding algorithm. Furthermore, we derived a condition assuring that concatenated AC codes have e-error correcting capability.

In the last part of this chapter, we have shown the existence of AC codes that can be encoded and decoded with polynomial time complexity and have a positive rate. It is of interest to investigate how to construct such codes in a deterministic way.

7. References

Boneh, D. & Shaw, J. (1998). Collusion-secure fingerprinting for digital data, *IEEE Trans. Inform. Theory*, vol. 44, pp. 1897–1905.

Guruswami, V. (2004). *List Decoding of Error-Correcting Codes* (Lecture Notes in Computer Science, vol. 2282) Springer Berlin/Heidelberg.

Fernandez, M. & Soriano, M. (2004). Soft-decision tracing in fingerprinted multimedia content, *IEEE Multimedia*, vol. 11, no. 2, pp. 38–46.

Forney, Jr., G. D. (1966). *Concatenated Codes*, MIT Press, Cambridge, MA.

Kang, I. K. Sinha, K. & Lee, H. K. (2006). New digital fingerprint code construction scheme using group-divisible design, *IEICE Trans. Fundamentals*, vol. E89-A, no. 12, pp. 3732-3735.

Koga, H. (2010). On the capacity of the AND anti-collusion fingerprinting codes, (in Japanese) *IEICE Technical Report*, vol. 109, no. 444, pp. 439–444.

Li, Q. Wang, X. Li, Y. Pan, Y. & Fan, P. (2009). Construction of anti-collusion codes based on cover-free families, *Proc. Sixth International Conference on Information Technology: New Generations, ITNG 2009*, Las Vegas, USA.

Lin, S. & Costello Jr., D. J. (2004). *Error Control Coding: Fundamentals and Applications, 2nd ed.*, Prentice-Hall, Upper Saddle River.

Podilchuk, C. & Zeng, W. (1998). Image adaptive watermarking using visual models, *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525–540.

Silverberg, A. Staddon, J. & Walker, J. L. (2003). Applications of list decoding to tracing traitors, *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1312–1318.

Staddon, J. N. Stinson, D. R. & Wei, R. (2001). Combinatorial properties of frameproof and traceability codes, *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042–1049.

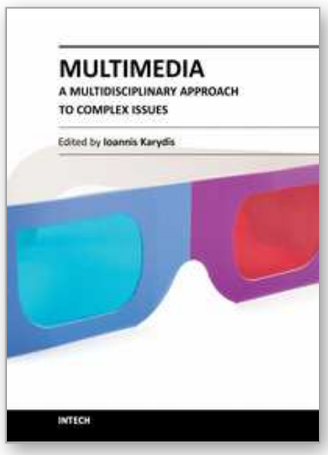
Trappe, W., Wu, M., Wang, Z. J. & Liu, K. J. R. (2003). Anti-collusion fingerprinting for multimedia, *IEEE Trans. Signal Processing*, vol. 51, pp. 1069–1087.

Wu, M., Trappe, W., Wang, Z. J. & Liu, K. J. R. (2004). Collusion-resistant fingerprinting for multimedia, *IEEE Signal Processing Magazine*, vol. 21, pp. 15–27.

Yagi, H. Matsushima, T. & Hirasawa, S. (2007). Short concatenated fingerprinting codes for multimedia data, *Proc. of 45th Annual Allerton Conference*, pp.1040–1045, Illinois, USA.

Yagi, H. Matsushima, T. & Hirasawa, S. (2009). Fingerprinting codes for multimedia data against averaging attack, *IEICE Trans. Fundamentals*, vol.E-92, no.1, pp.207–216.

IntechOpen



Multimedia - A Multidisciplinary Approach to Complex Issues
Edited by Dr. Ioannis Karydis

ISBN 978-953-51-0216-8
Hard cover, 276 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

The nowadays ubiquitous and effortless digital data capture and processing capabilities offered by the majority of devices, lead to an unprecedented penetration of multimedia content in our everyday life. To make the most of this phenomenon, the rapidly increasing volume and usage of digitised content requires constant re-evaluation and adaptation of multimedia methodologies, in order to meet the relentless change of requirements from both the user and system perspectives. Advances in Multimedia provides readers with an overview of the ever-growing field of multimedia by bringing together various research studies and surveys from different subfields that point out such important aspects. Some of the main topics that this book deals with include: multimedia management in peer-to-peer structures & wireless networks, security characteristics in multimedia, semantic gap bridging for multimedia content and novel multimedia applications.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Hideki Yagi and Tsutomu Kawabata (2012). Polynomial-Time Codes Against Averaging Attack for Multimedia Fingerprinting, Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis (Ed.), ISBN: 978-953-51-0216-8, InTech, Available from: http://www.intechopen.com/books/multimedia-a-multidisciplinary-approach-to-complex-issues/polynomial-time-codes-against-averaging-attack-for-multimedia-fingerprinting

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen