Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 41-51

On the Capacity of Fingerprinting Codes against AND, Averaging, and Related Attacks

Gou Hosoya[1], Hideki Yagi[2], Manabu Kobayashi[3], and Shigeichi Hirasawa[4]

[1]Department of Management Science, Faculty of Engineering, Tokyo University of Science,
1–3 Kagurazaka, Shinjuku-ku, Tokyo 162–8601, Japan
hosoya@m.ieice.org

[2]Department of Communication Engineering and Informatics, The University of Electro-Communications,
1–5–1 Chofugaoka, Chofu, Tokyo 182–8585, Japan

[3]Department of Information Science, Faculty of Engineering, Shonan Institute of Technology,
1–1–25, Tsujidonishikaigan, Fujisawa-shi, Kanagawa 251–8511, Japan

[4]Research Institute for Science and Engineering, Waseda University,
3–14–9 Okubo, Shinjuku-ku, Tokyo 169–0072, Japan

Abstract: **A new attack model in which the number of colluders is distributed according to a certain probability distribution is introduced. Two classes of collusion attacks which include well-known collusion attacks in the context of multimedia fingerprinting are provided. For these two attack classes, achievable rates without the knowledge of the size of actual colluders are derived. Then, achievable rates for some particular attacks are investigated. For the AND attack, the achievable rate derived in this paper coincides with the previously known achievable rate although the attack model in this paper does not assume that the decoder knows the actual number of colluders. Moreover, for the averaging attack, it is shown that the derived achievable rate can be achieved by binary linear codes.**
Keywords: fingerprinting code, achievable rate, capacity, multiple-access channel, collusion attack

I. Introduction

Due to rapid spread of wide-band networks, security against illegal attacks becomes more important. The applications of such problems, for example, watermarking [19], [23], fingerprinting [21], network protocol [22], and detection of attacks to information systems [20], have been studied well.

In a distribution system of digital contents, illicit users may collude to produce illegal copies of an original content. *Digital fingerprinting* [2], [3], [7]–[12], [14]–[18] is one of the key techniques to protect digital contents against piracy. For distributors of digital contents, it is desired to detect some or all members of the colluders from pirated copies. In a fingerprinting system, information which is unique to each user is embedded into a host content (covertext) to identify illicit users.

In the context of *multimedia fingerprinting*, Trappe et al. [17] have proposed anti-collusion fingerprinting codes based on spread spectrum embedding against the *averaging attack*, and these codes can detect all the colluders when the number of colluders is less than or equal to some constant k. The anti-collusion fingerprinting codes by Trappe et al. are based on two-stage coding; a codeword of fingerprinting codes against the *AND attack* is first encoded, and orthogonal spread spectrum sequences are concatenated with the encoded codeword. The application of such fingerprinting codes for large user groups has been discussed in [7] and recently an effective detection method has been proposed [9].

Recently, Koga [8] has introduced a probabilistic model in which the AND attack is conducted by at most k users, and has shown an achievable rate under the condition that all the colluders should be detected with a vanishingly small error probability as the code length n increases. However, in the model of [8], the probability that the number of colluders is strictly less than k goes to zero exponentially with n. This implies that the number of colluders is assumed to be *known* a-priori to the digital fingerprinting system. From the practical point of view, however, the assumed maximum number of colluders, k, should be set larger than the expected number of colluders in order to guarantee the security. Theoretical analysis of this model is similar to deriving the capacity region of multiple access channels (MAC) [1], [4], [5], and deriving lower and upper bounds on achievable rates of fingerprinting codes based on the marking assumption [3] have been studied in [2], [14], [15]. Also constructions of fingerprinting codes can be found in [16], [10]. P. Moulin [11], [12] has considered a fairly wide class of collusion attacks based on information theoretic framework, and has derived the capacity of digital fingerprinting codes against any number of colluders and any attack in an assumed attack class.

The main technique is a generalization of *universal coding* based on constant composition codes (e.g., [4]). Based on the results shown in [11] and [12], it is expected that the coding and decoding scheme by [11] and [12] can also be applied to the attack model introduced in [8], and the derived achievable rate may coincide with the capacity against the AND attack. However, it is still difficult to implement the universal coding, in which constant composition codes and maximum empirical mutual information decoding are used, in practical systems.

In this paper, as a generalization of the attack model considered in [8], we introduce a new attack model in which the number of colluders is distributed according to a certain probability distribution $\Pr[|S|] = \ell, \ell = 2, \ldots, k$, where S and k denote the set of colluders and the maximum number of colluders, respectively. We assume that the encoder and the decoder of anti-collusion codes know only the maximum number of colluders k but not the actual probability distribution. We define two classes of collusion attacks which include many collusion attacks in the context of multimedia fingerprinting [17], [18]. For these two attack classes, we derive a lower bound on the maximum achievable rates for the unknown size of the actual colluders. Based on the derived achievable rates, we investigate achieve rates for some particular attacks. For the AND attack, our bound coincides with that given by Koga [8] although our model does not assume that the decoder knows the actual number of colluders. For the averaging attack, it is clarified that the derived achievable rate is larger than the previously known one [10]. We give some numerical results, and it is shown that the derived achieve rate can be attained by an ensemble of binary random linear codes against the averaging attack as claimed in [10]. The approach of this paper is similar to [11] and [12] in the sense that only the maximum number of colluders is assumed for a class of attacks. However, our coding scheme is not universal in contrast to [11] since we need to assume that the decoder knows the probability distribution of an attack. It is our primary contribution that for these introduced attack classes, we give an achievability scheme that may be implemented by an ensemble of random linear codes or random coset codes. We generalize the technique of *jointly typical set decoding* [5] to allow mismatched likelihood functions in terms of the number of colluders. From our result, it is clarified that an ensemble of random linear codes themselves can be used against the averaging attack. On the other hand, for the other well-known attacks such as the AND attack, the erasure attack, etc, the combination of random coset codes and a well-known symbol mapping technique devised by Gallager [6, Sect. 6.2] is sufficient to attain the derived achievable rates.

This paper is organized as follows: Section II is preliminaries where we will give a fingerprinting system and assumed attack classes (Attack Classes A and B). In Section III, achievable rates for Attack Classes A and B are derived. Numerical examples will be presented in Section IV and proofs for lemma and theorem will be given in Section V. Finally conclusion will be given in Section VI.

II. Preliminaries

A. Notation

Throughout this paper, the base of $\log$ is two. For the random variable Z, let z and $\mathcal{Z}$ be its realization and a set of random variables. For integers $1 \leq i \leq j$, let the sequence of random variables $Z_i, Z_{i+1}, \ldots, Z_j$ be denoted by Z_i^j. A sub-sequence of Z_i^j, whose positions are indexed by $V = \{i_1, \ldots, i_{|V|}\}$, is denoted by $Z(V)$, i.e., $Z(V) = Z_{i_1}, \ldots, Z_{i_{|V|}}$. Let $P_Z(z) := \Pr[Z = z]$ be a probability mass function on a set $\mathcal{Z}$. For a set W and its subset $V \subseteq W$, let V^c be the complement set $W \setminus V$ of V.

B. Fingerprinting System

Assume that a digital fingerprinting system provides a digital content for M users. The index set of users is denoted by $U = \{1, \ldots, M\}$. A unique codeword is assigned to each user. Note that each user cannot detect the assigned codeword from the distributed content. Let $C = \{\boldsymbol{x}_i | i \in U\} \subseteq \{0,1\}^n$ be an anti-collusion fingerprinting code where n denotes the codeword length, and $\boldsymbol{x}_i \in \{0,1\}^n$ denotes a codeword of user $i \in U$. The rate R of the anti-collusion fingerprinting code C is defined by

$$R = \frac{\log M}{n}. \tag{1}$$

Let k denote the maximum number of colluders. Let the probability mass function of the number of colluders be denoted by $P_L(\ell) := \Pr[L = \ell]$, $\ell = 1, \ldots, k$, where ℓ is the size of a set of colluders. When $L = l$, each of ℓ colluders is uniformly and independently chosen from the set of users U. Following the attack model in [8], we consider the number of colluders to be less than ℓ when the same users are chosen from U[1]. Then the probability of users $i_1, \ldots, i_\ell$, $i_j \in U$, being the colluders is $\frac{1}{M^\ell}$ where $i_j, j = 1, \ldots, \ell$, expresses the index of a user chosen from U at the j-th trial[2]. Throughout this paper, we assume that the maximum number of colluders k is known to both the encoder and the decoder, whereas the probability distribution $P_L(\ell)$ is unknown to them. We sometimes denote the set of the colluders S of size ℓ by $S(\ell)$. Let the codeword symbol corresponding to user $i_j \in S(\ell), j = 1, \ldots, \ell$, be $X_j \in \mathcal{X}_j := \{0,1\}$. Let Y be a forged symbol made by colluders S. For a given $S(\ell)$, the forgery y is determined by the collusion attack

$$f^{(\ell)} : \mathcal{X}_1 \times \ldots \times \mathcal{X}_\ell \to \mathcal{Y}. \tag{2}$$

We denote the conditional probability distribution corresponding to $f^{(\ell)}$ by

$$P^{(\ell)}(y|x_1, \ldots, x_\ell) := P_{Y|X_1^L,L}(y|x_1, \ldots, x_\ell, \ell). \tag{3}$$

Example 1 (AND Attack) *In the AND attack, the output alphabet is $\mathcal{Y} = \{0,1\}$, and the probability distribution is given by*

$$P^{(\ell)}(1|x_1, \ldots, x_\ell) = \begin{cases} 1, & \text{if } x_i = 1, i \in S; \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

[1] It is readily shown that for a large n and a given $\epsilon > 0$, $\Pr[|S| < \ell | L = \ell] \leq \epsilon$.

[2] The attack model in [8] corresponds to the AND attack with $P_L(k) = 1$.

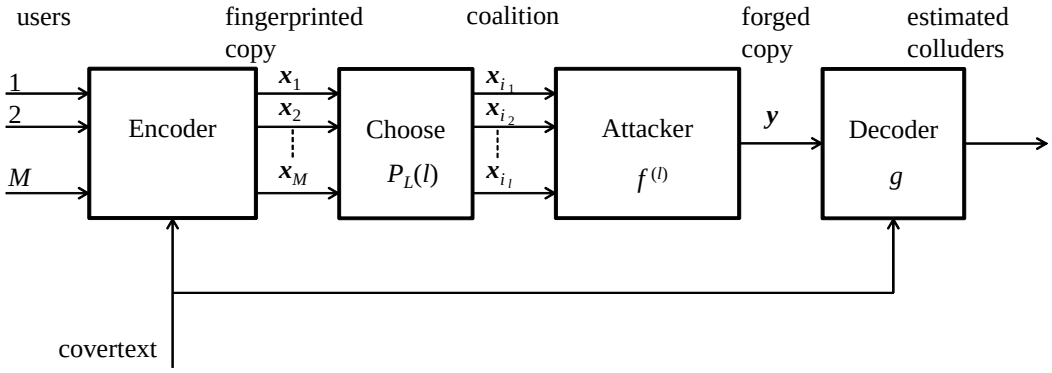

Figure. 1: System model

□

Example 2 (Averaging Attack) *In the* averaging attack *(e.g., [10]), the output symbol is given by the arithmetic average of the ℓ inputs by regarding inputs 0 and 1 as real numbers, so the output alphabet is expressed as*

$$\mathcal{Y} = \{0,1\} \cup \bigcup_{\ell=0}^{k} \bigcup_{m=1}^{\ell-1} \left\{ \frac{m}{\ell} \right\}, \tag{5}$$

where the probability distribution of this attack is given by

$$P^{(\ell)}(\tfrac{m}{\ell}|x_1,\ldots,x_\ell) = \begin{cases} 1, & \text{if } |\{i|x_i = 1, i \in S\}| = m; \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$

for $m = 1,\ldots,\ell$. □

Example 3 (Erasure Attack) *Let the output alphabet for the* erasure attack *be $\mathcal{Y} = \{0,1,e\}$ (e is an erased symbol). Then the probability distribution of this attack is given by*

$$P^{(\ell)}(a|x_1,\ldots,x_\ell) = \begin{cases} 1, & \text{if } |\{i|x_i = 1, i \in S\}| = a\ell; \\ 0, & \text{otherwise,} \end{cases} \tag{7}$$

for $a = 0, 1$ and is expressed as

$$P^{(\ell)}(e|x_1,\ldots,x_\ell) = \begin{cases} 1, & \text{if } 1 \le |\{i|x_i = 1, i \in S\}| \le \ell - 1; \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

□

Assume that the attack model (with the transition probabilities $P^{(\ell)}(\boldsymbol{y}|\cdot)$ and the output alphabet $\mathcal{Y}$) is known to the decoder. When the decoder receives $\boldsymbol{y} \in \mathcal{Y}$, it tries to estimate all the colluders in S by using

$$g : \mathcal{Y}^n \to \bigcup_{\ell=1}^{k} U^\ell. \tag{9}$$

For a set of colluders $S = \{i_1,\ldots,i_\ell\}$, if the output of the decoder satisfies $g(\boldsymbol{y}) \neq S$, we call this event *undetected*. The average error probability of detecting colluders of size ℓ, $P_{\mathrm{e}|\ell}^{(n)}$, is defined by

$$P_{\mathrm{e}|\ell}^{(n)} = \frac{1}{M^\ell} \times \sum_{(i_1,\ldots,i_\ell)\in U^\ell} \Pr\big[g(\boldsymbol{y}) \neq (i_1,\ldots,i_\ell)|\ S = \{i_1,\ldots,i_\ell\}\big]. \tag{10}$$

Taking average over the size ℓ of colluders, the average decoding error probability $P_{\mathrm{e}}^{(n)}$ is given by

$$P_{\mathrm{e}}^{(n)} = \sum_{\ell=1}^{k} P_L(\ell) P_{\mathrm{e}|\ell}^{(n)}. \tag{11}$$

Figure 1 shows the system model.

Definition 1 *A* rate R *is said to be* achievable *if there exists a sequence of (n, M) codes such that for every $\epsilon > 0$,*

$$R \le \frac{\log M}{n} + \epsilon,$$
$$P_{\mathrm{e}}^{(n)} \le \epsilon,$$

for all sufficiently large n. □

Definition 2 *The* capacity *of the fingerprinting codes, denoted by C_k, is defined as the supremum of all achievable rates.* □

Moulin defined the capacity for a given set of colluders [11], [12]. The definition of this paper is slightly different from the one in [11] and [12].

C. Assumed Attack Model

Assume that codeword symbols of each user $X_j \in \mathcal{X}_j, i_j \in S(\ell)$, $j = 1,\ldots,k$, are independently generated for each other by a probability distribution $Q(x_i) = P_{X_i}(x_i)$. Since the codeword symbols are mutually independent,

$$P_{X(V)}(x(V)) = \prod_{i\in V} Q(x_i), \tag{12}$$

is satisfied for an arbitrary subset $V \subseteq S$. The joint entropies $H^{(\ell)}(X(V), Y)$ and $H^{(\ell)}(X(V), Y|X(V^c))$, and the joint mutual information $I^{(\ell)}(X(V); Y)$ and $I^{(\ell)}$

$(X(V);Y|X(V^c))$ are defined with respect to the probability distributions $Q(x_i)$ and $P^{(\ell)}(y|x_1,\ldots,x_\ell)$.
For arbitrary $1 \le \ell \le k$ and $V \subseteq S$, $H^{(\ell)}(X(V))$ depends only on $Q(x(V)) = \prod_{i\in V} Q(x_i)$, so we have

$$\begin{aligned} H^{(\ell)}(X(V)) &= H(X(V)) \\ &= |V|H(X_1), \end{aligned} \tag{13}$$

where $H(X_1)$ is entropy of the random variable X_1. Moreover for an arbitrary $1 \le \ell \le k$ and for any pairs (V_1, V_2) such that $V_1, V_2 \subseteq S$, $|V_1| = |V_2|$, we have

$$H(X(V_1)) = H(X(V_2)). \tag{14}$$

We give the definition of the first attack model.
Definition 3 (Attack Class A) *We define the* Attack Class A *by the set of $(P^{(\ell)}(\cdot|\cdot), \mathcal{Y})$ satisfying the following conditions:*

(i) Each forged symbol y_j is identically and independently distributed, i.e.,

$$\begin{aligned} &P^{(\ell)}(\boldsymbol{y}|\boldsymbol{x}_{i_1},\ldots,\boldsymbol{x}_{i_\ell}) \\ &\quad = \prod_{j=1}^{n} P^{(\ell)}(y_j|x_{i_1 j},\ldots,x_{i_\ell j}). \end{aligned} \tag{15}$$

(ii) For all the pairs $V_1, V_2 \subseteq S$, $|V_1| = |V_2| \le \ell$, if $\{x_i | i \in V_1\} = \{x_i | i \in V_2\}$, where the number of duplications is taken into account, then

$$P^{(\ell)}(y|x(V_1)) = P^{(\ell)}(y|x(V_2)), \tag{16}$$

for all $y \in \mathcal{Y}$.

(iii) For arbitrary $V \subseteq S, |V| = i$, and $P_{X(V)}(x(V)) = \prod_{s\in V} Q(x_s)$, $1 \le i < j \le k$, we have

$$H^{(i)}(Y|X(V)) < H^{(j)}(Y|X(V)). \tag{17}$$

□

Intuitively, condition (i) indicates the memoryless property of the attack, and condition (ii) indicates that this attack class depends only on the number of colluders, not the combination of colluders. The collusion attack satisfying condition (i) is included in the class of the strongly exchangeable collusion channels [12]. The collusion attack satisfying condition (ii) is included in the class of the permutation invariant collusion channels [12]D
It can be easily shown that the AND attack, the averaging attack, and the erasure attack belong to the Attack Class A[3].
Next we show the following lemma.
Lemma 1 *Assume an attack belonging to the Attack Class A. For an arbitrary $1 \le \ell \le k$ and for all the pairs $V_1, V_2 \subseteq S, |V_1| = |V_2| \le \ell$, we have*

$$H^{(\ell)}(Y|X(V_1)) = H^{(\ell)}(Y|X(V_2)), \tag{18}$$
$$H^{(\ell)}(X(V_1),Y) = H^{(\ell)}(X(V_2),Y), \tag{19}$$
$$H^{(\ell)}(X(V_1)|Y) = H^{(\ell)}(X(V_2)|Y), \tag{20}$$
$$I^{(\ell)}(X(V_1);Y) = I^{(\ell)}(X(V_2);Y), \tag{21}$$
$$I^{(\ell)}(X(V_1);Y|X(V_1^c)) = I^{(\ell)}(X(V_2);Y|X(V_2^c)), \tag{22}$$

[3]For the other attacks such as the max-min attack [7] also belong to this attack class.

(Proof) We have Eq. (18) directly from condition (ii) of the Attack Class A. Applying Eq. (14) for Eq. (18), we have Eq. (19). We obtain Eq. (20) directly from Eq. (19). For Eq. (21), if we set $s = |V_1| = |V_2|$, then

$$\begin{aligned} I^{(\ell)}(X(V_1);Y) &= H^{(\ell)}(Y) - H^{(\ell)}(Y|X(V_1)) \\ &= H^{(\ell)}(Y) - H^{(\ell)}(Y|X(V_2)) \\ &= I^{(\ell)}(X(V_2);Y), \end{aligned} \tag{23}$$

yielding Eq. (21). In a similar manner, we can obtain Eq. (22). □
From Lemma 1, for an attack belonging to the Attack Class A, we have, for example, $H^{(\ell)}(Y,X_1,X_2) = H^{(\ell)}(Y,X_2,X_3)$ and $I^{(\ell)}(X_1,X_2;Y|X_3) = I^{(\ell)}(X_2,X_3;Y|X_1)$.
The following lemma is used to derive our main results shown in the next section.
Lemma 2 *Assume an attack belonging to the Attack Class A. For arbitrary $3 \le \ell \le k$ and $0 \le a \le s-2$ with $2 \le s < \ell$, we have*

$$\begin{aligned} &\frac{1}{s-a}\left(H^{(\ell)}(Y|X_1^a) - H^{(s)}(Y|X_1^s)\right) \\ &\quad \le \frac{1}{s-(a+1)}\left(H^{(\ell)}(Y|X_1^{a+1}) - H^{(s)}(Y|X_1^s)\right). \end{aligned} \tag{24}$$

(Proof) See Subsect. V-B. □
Throughout this paper, we assume that jointly typical set decoding is used. If maximum likelihood (ML) decoding is used, the decoding error probability is always less than or equal to that of jointly typical set decoding. Then at least the rate which is achievable by jointly typical set decoding can be achieved via ML decoding.
Next we define a subclass of the Attack Class A.
Definition 4 (Attack Class B) *If an attack belongs to the Attack Class A, and $(P^{(\ell)}(\cdot|\cdot), \mathcal{Y})$ satisfies the following condition, then this attack is said to be in the* Attack Class B.

(iv) For an arbitrary $P_{X_1^j}(x_1^j) = \prod_{s=1}^{j} Q(x_s)$, $1 \le i < j \le k$, we have

$$H^{(i)}(Y|X_1^i) \le H^{(j)}(Y|X_1^j). \tag{25}$$

□

For an arbitrary $2 \le \ell \le k$, the AND attack and the averaging attack satisfy $H^{(\ell)}(Y|X_1^\ell) = 0$. Therefore these deterministic attacks belong to the Attack Class B. The interleaving attack [2] also belongs to this attack class.
Applying Lemma 2 for the case of the Attack Class B, we have the following lemma.
Lemma 3 *Assume an attack belonging to the Attack Class B. Then for arbitrary $2 \le \ell \le k$ and $1 \le s \le \ell$, we have*

$$\frac{1}{s}\left(H^{(\ell)}(Y) - H^{(s)}(Y|X_1^s)\right) \ge \frac{1}{s} I^{(\ell)}(X_1^\ell;Y). \tag{26}$$

(Proof) From condition (iv) of the Attack Class B,

$$\begin{aligned} &\frac{1}{s}\left(H^{(\ell)}(Y) - H^{(s)}(Y|X_1^s)\right) \\ &\qquad \ge \frac{1}{s}\left(H^{(\ell)}(Y) - H^{(\ell)}(Y|X_1^\ell)\right) \\ &\qquad = \frac{1}{s} I(X_1^\ell;Y), \end{aligned} \tag{27}$$

is satisfied. □

III. Achievable Rates for Attack Classes A and B

In this section, we provide an achievable rate for both the Attack Classes A and B.
We show the following theorem.

Theorem 1 *Assume an attack belongs to the Attack Class A. Then for an arbitrary fixed k, we have*

$$C_k \geq \sup_{Q(X)} \min_{\ell=2,\ldots,k} \min_{s=2,\ldots,\ell} \left\{ \frac{1}{s} \left(H^{(\ell)}(Y) - H^{(s)}(Y|X_1^s) \right) \right\}, \quad (28)$$

where the probability distribution of ℓ random variables $X_1, X_2, \ldots, X_\ell$ is given by

$$P_{X_1^\ell}(x_1^\ell) = \prod_{j=1}^{\ell} Q(x_j). \quad (29)$$

(Proof) See Subsect. V-C. □

For the Attack Class B, we have the following corollary.

Corollary 1 *Assume that an attack belongs to the Attack Class B. Then for an arbitrary fixed k, we have*

$$C_k \geq \sup_{Q(X)} \min_{\ell=2,\ldots,k} \left\{ \frac{1}{\ell} I^{(\ell)}(X_1^\ell; Y) \right\}, \quad (30)$$

where the probability distribution of ℓ random variables $X_1, \ldots, X_\ell$ is given by

$$P_{X_1^\ell}(x_1^\ell) = \prod_{j=1}^{\ell} Q(x_j). \quad (31)$$

(Proof) For an attack belonging to the Attack Class B, the property in Lemma 3 is valid. Thus for a given ℓ and from Eq. (28) we have

$$\min_{s=2,\ldots,\ell-1} \left\{ \frac{1}{s} H^{(\ell)}(Y) - H^{(s)}(Y|X_1^s) \right\} \geq \frac{1}{\ell} I^{(\ell)}(X_1^\ell; Y). \quad (32)$$

□

IV. Case Study for Several Attacks

In the previous section, we derive achievable rates for the attack classes A and B. In this section, by using these results, we show some numerical results for particular attacks such as the AND attack, the erasure attack, and the averaging attack described in Examples 1 – 3. Notice that these attacks belong to the Attack Class B. Therefore from Corollary 1, the rate presented in the right-hand side of Eq. (30) is achievable.

A. Achievable Rate against AND Attack

Koga [8] has derived a lower bound on the capacity against the AND attack via the analysis over the Multiple Access Channel (MAC) [1], assuming that the number of actual colluders is fixed to k. For an arbitrary k, it has been shown that a lower bound on the capacity satisfies $C_k \geq \frac{1}{k}$. In other words, there exists code sequences of rate $R = \frac{1}{k}$ whose decoding error probability goes to 0 asymptotically with n. The model assumed in [8] satisfies $\lim_{n\to\infty} P_L(k) = 1$, $\ell = 1, \ldots, k$. So the system requires good codes against a set of colluders S of size k, which is the maximum size of assumed colluders. However for the practical usage, the number of colluders ℓ is distributed, so the system may be designed with the maximum number of colluders larger than the expected size of colluders.
We have introduced the attack model with its colluder size disturbed according to an unknown distribution $P_L(\ell)$, and we have derived an achievable rate for two attack models by Theorem 1 and Corollary 1. If $P_L(L) = 1$, then our model is equal to the model in [8], so it can be seen that our model is a generalization of the model in [8] when the attack model is restricted to the AND attack.
Since the AND attack is a deterministic attack, $H(Y|X_1^\ell) = 0$ holds. Mutual information $I(X_1^\ell; Y)$ is expressed as

$$\begin{aligned} I(X_1^\ell; Y) &= H(Y) \\ &= h(p^\ell), \end{aligned} \quad (33)$$

where p denotes the probability that each codeword symbol in C is 1, i.e., $\Pr[X_i = 1] = p$. Substituting Eq. (33) to Eq. (30), we have

$$\begin{aligned} C_k &\geq \sup_{Q(X)} \frac{1}{k} h(p^k) \\ &= \frac{1}{k}. \end{aligned} \quad (34)$$

The maximum value in the right-hand side of Eq. (34) is achieved when p satisfies $p^k = 0.5$, since for $0 \leq a \leq 1$, $h(a)$ is maximized when $a = 0.5$, and $h(0.5) = 1$. Therefore we can evaluate p from $p = 0.5^{\frac{1}{k}}$. Thus the same achievable rate as in [8] is obtained for the generalized attack model in this paper.

Example 4 *For $k = 4$, the achievable rate for the AND attack is given by $p = 0.5^{\frac{1}{4}} \simeq 0.840896$.* □

B. Achievable Rate against Other Attacks

We show the derived achievable rate for the erasure attack and the averaging attack.

1) Achievable Rate against Erasure Attack

For the erasure attack, $H(Y|X_1^\ell) = 0$ is also satisfied as in the case of the AND attack, so we have

$$\begin{aligned} I(X_1^\ell; Y) &= H(Y) \\ &= -p^\ell \log p^\ell - \tilde{p}^\ell \log \tilde{p}^\ell \\ &\quad -(1 - p^\ell - \tilde{p}^\ell) \log(1 - p^\ell - \tilde{p}^\ell). \end{aligned} \quad (35)$$

where $\tilde{p} = 1 - p$. Substituting Eq. (35) to Eq. (30), we obtain

$$C_k \geq \sup_{Q(X)} \frac{1}{k} \big\{ -p^k \log p^k - \tilde{p}^k \log \tilde{p}^k \\ -(1 - p^k - \tilde{p}^k) \log(1 - p^k - \tilde{p}^k) \big\}. \quad (36)$$

It can be easily shown that right-hand side of Eq. (36) is always greater than or equal to that of Eq. (34). Thus it can yield a larger achievable rate for the erasure attack compared with the AND attack. The solution of p that takes the maximum in right-hand side of Eq. (36) cannot be evaluated explicitly, so we show numerical results in Subsect. IV-C.

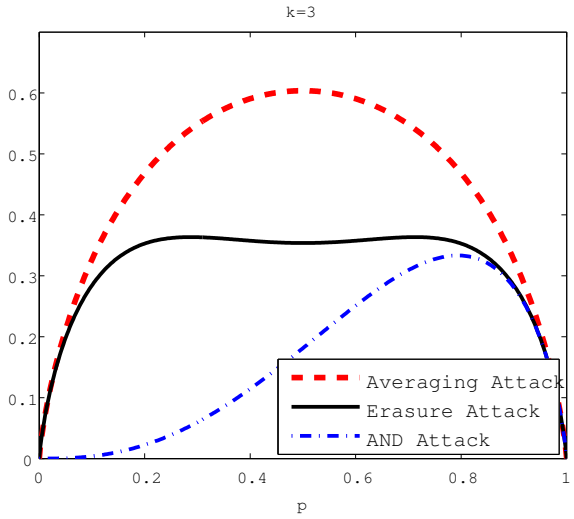

Figure. 2: Calculation result for the AND attack (Eq. (34)), the erasure attack (Eq. (36)), and the averaging attack (Eq. (38)) when $k = 3$

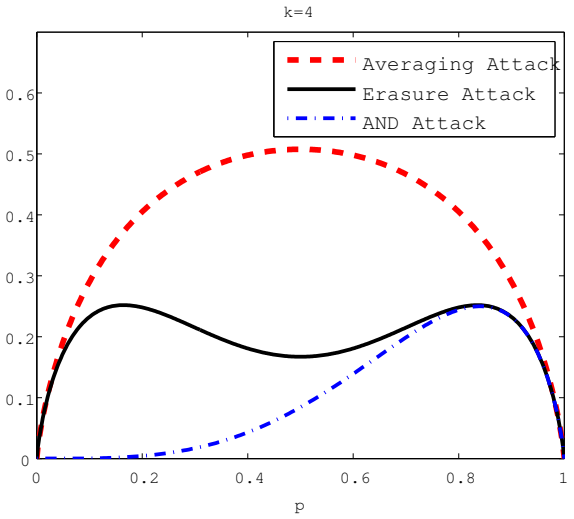

Figure. 3: Calculation result for the AND attack (Eq. (34)), the erasure attack (Eq. (36)), and the averaging attack (Eq. (38)) when $k = 4$

2) Achievable Rate against Averaging Attack

For the averaging attack, $H(Y|X_1^\ell) = 0$ is also satisfied, so we have

$$\begin{aligned} I(X_1^\ell;Y) &= H(Y) \\ &= -\sum_{i=0}^{\ell}\binom{\ell}{i}p^i(1-p)^{\ell-i} \\ &\quad \times \log\binom{\ell}{i}p^i(1-p)^{\ell-i}. \end{aligned} \tag{37}$$

Substituting Eq. (37) to Eq. (30), we have

$$\begin{aligned} C_k \geq \sup_{Q(X)}\Big\{-\frac{1}{k}\sum_{i=0}^{k}\binom{k}{i}p^i(1-p)^{k-i} \\ \times \log\binom{k}{i}p^i(1-p)^{k-i}\Big\}. \end{aligned} \tag{38}$$

It is readily shown that right-hand side of Eq. (38) is always greater than or equal to that of Eq. (36). Thus the achievable rate for the averaging attack is larger than those of the erasure attack and the AND attack.

Note that the right-hand side of Eq. (38) is characterized by the entropy of a binomial distribution, and it has been shown that the entropy of a binomial distribution is Schur convex [13] and symmetric. From this, the mutual information of the averaging attack is symmetric with respect to $p = 0.5$ for every k and takes the maximum on this point.

Remark 1 *For every k, the achievable rate for the averaging attack is achieved with binary random linear codes ($p = 0.5$).* □

C. Numerical Examples for Several Attacks

Figures 2 – 4 show the calculation results for the AND attack given in Eq. (34), the erasure attack given in Eq. (36), and the averaging attack given in Eq. (38) with $k = 3, 4, 5$, respectively. From these figures, we have the following observations:

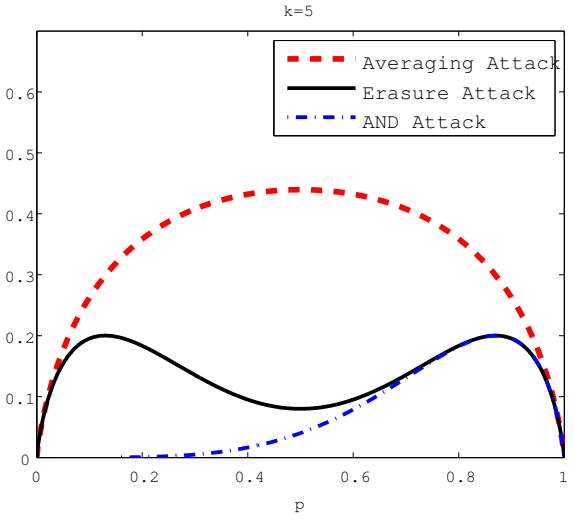

Figure. 4: Calculation result for the AND attack (Eq. (34)), the erasure attack (Eq. (36)), and the averaging attack (Eq. (38)) when $k = 5$

(1) For the AND Attack and the Erasure Attack

The AND attack and the erasure attack attain their maximum at $p \neq 0.5$ for $k > 2$. For the AND attack, p which gives the maximum value $\frac{1}{k}$ when $k = 3, 4, 5$ is $p \simeq 0.793701$, 0.840896, 0.870551, respectively. For the erasure attack, there are two points of p that give the maximum. It is clear that the achievable rates against the erasure attack is larger than that against the AND attack. The difference of the rates between these two attacks becomes negligible as k increases. For the AND and the erasure attacks, the rate may be achievable with the combination of the random coset codes or Gallager's well-known symbol mapping technique [6, Sect. 6.2].

(2) For the Averaging Attack

The averaging attack attains its maximum at $p = 0.5$ for every k which is obvious from the discussion in the previous subsection. Thus unlike the AND attack and the erasure attack, it is clarified that the rate in Eq. (38) is achievable with

an ensemble of random linear codes ($p = 0.5$).
Overall the achievable rates become smaller as the maximum number of colluders k increases for all of these attacks. It is a natural statement because it becomes difficult to detect a collusion when the number of colluders is large.

V. Proof of Lemma 2 and Theorem 1

A. Property of Mutual Information

Before proving Lemma 2 and Theorem 1, we first show the following lemma about a property of mutual information. This lemma is valid for an arbitrary attack $(P^{(\ell)}(\cdot|\cdot), \mathcal{Y})$.

Lemma 4 *For arbitrary $2 \le \ell \le k$ and $\tilde{V} \subseteq V \subseteq S$, we have*

$$\frac{1}{|V|} I^{(\ell)}(X(V); Y|X(V^c)) \le \frac{1}{|\tilde{V}|} I^{(\ell)}(X(\tilde{V}); Y|X(\tilde{V}^c)). \quad (39)$$

□

Moreover we define a set of jointly typical sequence $A_\epsilon^{(\ell,n)}$ [5] as follows:

Definition 5 (ϵ-jointly typical sequence) *For every $\epsilon > 0$,*

$$\begin{aligned} A_\epsilon^{(s,n)} := \Big\{ & (\boldsymbol{x}_{i_1}, \ldots, \boldsymbol{x}_{i_s}, \boldsymbol{y}) \\ & \in (\mathcal{X}_{i_1})^n \times \cdots \times (\mathcal{X}_{i_s})^n \times \mathcal{Y}^n, \\ & \left| -\frac{1}{n} \log P^{(s)}(\boldsymbol{x}(V), \boldsymbol{y}) - H^{(s)}(X(V), Y) \right| \le \epsilon, \\ & \left| -\frac{1}{n} \log Q(\boldsymbol{x}(V)) - H(X(V)) \right| \le \epsilon \\ & \qquad \text{for all } V \subseteq U, |V| \le s \Big\}, \end{aligned} \quad (40)$$

is called the set of ϵ-jointly typical sequences *where $Q(\boldsymbol{x}(V))$ and $P^{(s)}(\boldsymbol{x}(V), \boldsymbol{y})$ are joint probability distributions such that*

$$Q(\boldsymbol{x}(V)) := \prod_{j=1}^{|V|} Q(\boldsymbol{x}_{i_j}), \quad (41)$$

$$P^{(s)}(\boldsymbol{x}(V), \boldsymbol{y}) := Q(\boldsymbol{x}(V)) \cdot P^{(s)}(\boldsymbol{y}|\boldsymbol{x}_{i_1}, \ldots, \boldsymbol{x}_{i_{|V|}}), \quad (42)$$

and $V = \{i_1, \ldots, i_{|V|}\}$. □

B. Proof of Lemma 2

Denote $A := s - (a+1)$. To prove this lemma, we need to show

$$(A+1)\left(H^{(\ell)}(Y|X_1^{a+1}) - H^{(s)}(Y|X_1^s)\right) - A\left(H^{(\ell)}(Y|X_1^a) - H^{(s)}(Y|X_1^s)\right) \ge 0. \quad (43)$$

Then we have

$$\begin{aligned} & (A+1)\left(H^{(\ell)}(Y|X_1^{a+1}) - H^{(s)}(Y|X_1^s)\right) \\ & \qquad - A\left(H^{(\ell)}(Y|X_1^a) - H^{(s)}(Y|X_1^s)\right) \\ & = (A+1)H^{(\ell)}(Y|X_1^{a+1}) \\ & \qquad - AH^{(\ell)}(Y|X_1^a) - H^{(s)}(Y|X_1^s) \\ & = -AI^{(\ell)}(X_{a+1}; Y|X_1^a) \\ & \qquad + H^{(\ell)}(Y|X_1^{a+1}) - H^{(s)}(Y|X_1^s) \\ & \ge -AI^{(\ell)}(X_{a+1}; Y|X_1^a) + H^{(\ell)}(Y|X_1^{a+1}) \\ & \qquad - H^{(\ell)}(Y|X_1^s) \\ & = -AI^{(\ell)}(X_{a+1}; Y|X_1^a) + I^{(\ell)}(X_{a+2}^s; Y|X_1^{a+1}), \end{aligned} \quad (44)$$

where the inequality follows from condition (iii) of the Attack Class A. Using Eq. (22), the right-hand side of Eq. (44) is lower bounded as

$$\begin{aligned} & -AI^{(\ell)}(X_{a+1}; Y|X_1^a) + I^{(\ell)}(X_{a+2}^s; Y|X_1^{a+1}) \\ & = -AI^{(\ell)}(X_1; Y|X_2^{a+1}) + I^{(\ell)}(X_1^A; Y|X_{A+1}^s) \\ & = -AI^{(\ell)}(X_1; Y|X_2^{a+1}) \\ & \qquad + \sum_{j=1}^{A} I^{(\ell)}(X_j; Y|X_1^{j-1}, X_{A+1}^s) \\ & \ge 0, \end{aligned} \quad (45)$$

where the inequality follows from Eq. (22) and the relation

$$\begin{aligned} & \sum_{j=1}^{A} I^{(\ell)}(X_j; Y|X_1^{j-1}, X_{A+1}^s) \\ & \qquad = \sum_{j=1}^{A} I^{(\ell)}(X_1; Y|X_2^{j+a+1}) \\ & \qquad \ge AI^{(\ell)}(X_1; Y|X_2^{a+1}). \end{aligned} \quad (46)$$

Thus we have Eq. (24). □

C. Proof of Theorem 1

We give a sketch of the proof as follows:

1) *Codebook Generation*: For a given distribution P_X, we first generate independent 2^{nR} i.i.d. sequences $\boldsymbol{x}(i), i \in U$ at random according to $P_{X^n}(\boldsymbol{x}(i)) = \prod_{j=1}^n Q(x_j(i))$.
2) *Codeword Assignment*: For user $i \in U$, the codeword $\boldsymbol{x}(i)$ is allocated.
3) *Colluder Detection*: Given a forgery $\boldsymbol{y} \in \mathcal{Y}^n$ generated by a set of colluders $S(\ell^*)$ ($\ell^* \le k$), we consider the following detection algorithm.
   (i) Set $\ell := 2$. Fix $\epsilon > 0$ sufficiently small.
   (ii) Find $(\boldsymbol{x}(i_1), \ldots, \boldsymbol{x}(i_\ell))$ which is ϵ-jointly typical with $\boldsymbol{y}$. If there exists a unique tuple satisfying $(\boldsymbol{x}(\hat{i}_1), \ldots, \boldsymbol{x}(\hat{i}_\ell), \boldsymbol{y}) \in A_\epsilon^{(\ell,n)}$ (notice that $\hat{i}_1 \le \cdots \le \hat{i}_\ell$), then output $\hat{S} := \{\hat{i}_1, \ldots, \hat{i}_\ell\}$ and terminate the algorithm. If there exists such tuples more than one, declare a failure of the detection.
   (iii) If $\ell = k$, then declare a failure of the detection and terminate the algorithm. Otherwise set $\ell := \ell + 1$ and go to step (ii).

The detection algorithm immediately stops the algorithm if it finds $\boldsymbol{y}$ in $A_\epsilon^{(\ell,n)}$ by incrementing ℓ from 2.

4) *Analysis of Probability of Detection Error*: We prove the theorem for the case $k \geq 4$, $\ell^* = 3$ for simplicity. The case for $\ell^* \leq k$ can be similarly proven.

Since assigning codewords to users is symmetric, without loss of generality, we assume $S(\ell^*) = \{1, 2, 3\}$. Let $E^{(s)}_{i_1,\ldots,i_s}, 2 \leq s \leq k$, be the event that the users $(\boldsymbol{x}(i_1), \ldots, \boldsymbol{x}(i_s), \boldsymbol{y})$ are jointly typical, i.e., $(\boldsymbol{x}(i_1), \ldots, \boldsymbol{x}(i_s), \boldsymbol{y}) \in A_\epsilon^{(s,n)}$. The average probability of detection for error $S = S(\ell^*)$, denoted by $\overline{P}^{(n)}_{\mathrm{e}|\ell^*}(S)$, is over-bounded as

$$\begin{aligned}\overline{P}^{(n)}_{\mathrm{e}|\ell^*}(S) = \Pr\Bigg[&(E^{(3)}_{123})^c \cup \bigcup_{i,j\in S} E^{(2)}_{ij} \cup \bigcup_{i\in S}\bigcup_{j\geq 4} E^{(2)}_{ij} \\ &\cup \bigcup_{i,j\geq 4} E^{(2)}_{ij} \cup \bigcup_{i,j\in S}\bigcup_{\ell\geq 4} E^{(3)}_{ij\ell} \\ &\cup \bigcup_{i\in S}\bigcup_{j,\ell\geq 4} E^{(3)}_{ij\ell} \cup \bigcup_{i,j,\ell\geq 4} E^{(3)}_{ij\ell}\Bigg]. \end{aligned} \tag{47}$$

Note that $\overline{P}^{(n)}_{\mathrm{e}|\ell^*}(S)$ does not depend on k for a given ℓ^*. Taking an union over all the events, we have

$$\begin{aligned}\overline{P}^{(n)}_{\mathrm{e}|\ell^*}(S) \leq{}& \Pr[(E^{(3)}_{123})^c] + \sum_{i,j\in S}\Pr[E^{(2)}_{ij}] \\ &+ \sum_{i\in S}\sum_{j\geq 4}\Pr[E^{(2)}_{ij}] + \sum_{i,j\geq 4}\Pr[E^{(2)}_{ij}] \\ &+ \sum_{i,j\in S}\sum_{\ell\geq 4}\Pr[E^{(3)}_{ij\ell}] + \sum_{i\in S}\sum_{j,\ell\geq 4}\Pr[E^{(3)}_{ij\ell}] \\ &+ \sum_{i,j,\ell\geq 4}\Pr[E^{(3)}_{ij\ell}]. \end{aligned} \tag{48}$$

Next we bound each term on the right-hand side of Eq. (48). Using the asymptotic equipartition property (AEP) and for a sufficiently large code length, the first term can be bounded as $\Pr[(E^{(3)}_{123})^c] \leq \epsilon$.

The second term is upper-bounded as

$$\sum_{i,j\in S}\Pr[E^{(2)}_{ij}] \leq \sum_{i,j\in S}\sum_{(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y})\in A_\epsilon^{(2,n)}} P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y}), \tag{49}$$

where $P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y})$ is a marginal probability given by

$$\begin{aligned}&P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y}) \\ &\quad= \sum_{\boldsymbol{x}'\in\{0,1\}^n} Q(\boldsymbol{x}_i)Q(\boldsymbol{x}_j)Q(\boldsymbol{x}')P^{(3)}(\boldsymbol{y}|\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{x}'). \end{aligned} \tag{50}$$

Due to the AEP, Eq. (49) becomes

$$\begin{aligned}\sum_{i,j\in S}\Pr[E^{(2)}_{ij}] &\leq 3|A_\epsilon^{(2,n)}|2^{-n(H^{(3)}(X_i,X_j,Y)-\epsilon)} \\ &\leq 2^{-n(H^{(3)}(X_i,X_j,Y)-H^{(2)}(X_i,X_j,Y)-3\epsilon)}. \end{aligned} \tag{51}$$

Using Eqs. (13) and (14),

$$\begin{aligned}&H^{(3)}(X_i,X_j,Y) - H^{(2)}(X_i,X_j,Y) \\ &\quad= H^{(3)}(Y|X_1,X_2) - H^{(2)}(Y|X_1,X_2), \end{aligned} \tag{52}$$

holds and from condition (iii) of the Attack Class A, we have

$$H^{(3)}(Y|X_1,X_2) > H^{(2)}(Y|X_1,X_2). \tag{53}$$

Therefore it can be seen that the right-hand side of Eq. (51) goes to 0 exponentially with n.

Let us consider the third term. This term is over-bounded as

$$\sum_{i\in S}\sum_{j\geq 4}\Pr[E^{(2)}_{ij}] \leq 3\cdot 2^{nR}\sum_{(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y})\in A_\epsilon^{(2,n)}} P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y}). \tag{54}$$

Since $\boldsymbol{x}_j$ is independent of the pair $(\boldsymbol{x}_i,\boldsymbol{y})$, we have

$$P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y}) = Q(\boldsymbol{x}_j)P^{(3)}(\boldsymbol{x}_i,\boldsymbol{y}), \tag{55}$$

where $P^{(3)}(\boldsymbol{x}_i,\boldsymbol{y})$ is a marginal probability calculated as in Eq. (50). Due to the AEP, Eq. (54) is further over-bounded as

$$\begin{aligned}&\sum_{i\in S}\sum_{j\geq 4}\Pr[E^{(2)}_{ij}] \\ &\quad\leq 2^{-n(H(X_j)+H^{(3)}(X_i,Y)-H^{(2)}(X_i,X_j,Y)-R-3\epsilon)} \\ &\quad= 2^{-n(H^{(3)}(Y|X_2)-H^{(2)}(Y|X_1,X_2)-R-3\epsilon)}. \end{aligned} \tag{56}$$

Notice that the equality in Eq. (56) is due to the facts that $H^{(2)}(X_i,X_j,Y) = H^{(2)}(Y|X_i,X_j)+H(X_i)+H(X_j)$ and $H^{(3)}(X_i,Y) = H^{(3)}(Y|X_i)+H(X_i)$, and from an equality in Lemma 1. Thus if[4]

$$H^{(3)}(Y|X_2) - H^{(2)}(Y|X_1,X_2) > R, \tag{57}$$

then right-hand side of Eq. (56) goes to 0 exponentially with n.

Next for the fourth term, we have

$$\sum_{i,j\geq 4}\Pr[E^{(2)}_{ij}] \leq 2^{2nR}\sum_{(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y})\in A_\epsilon^{(2,n)}} P^{(3)}(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{y}). \tag{58}$$

Since $(\boldsymbol{x}_i,\boldsymbol{x}_j)$ and $\boldsymbol{y}$ are independent of each other, from the AEP, Eq. (58) is further over-bounded by

$$\begin{aligned}&\sum_{i,j\geq 4}\Pr[E^{(2)}_{ij}] \\ &\quad\leq 2^{-n(H(X_i)+H(X_j)+H^{(3)}(Y)-H^{(2)}(X_i,X_j,Y)-2R-4\epsilon)} \\ &\quad= 2^{-n(H^{(3)}(Y)-H^{(2)}(Y|X_1,X_2)-2R-4\epsilon)} \end{aligned} \tag{59}$$

Therefore from the equality in Lemma 1, if

$$\frac{1}{2}\left(H^{(3)}(Y) - H^{(2)}(Y|X_1,X_2)\right) > R, \tag{60}$$

the right-hand side of Eq. (59) goes to 0 exponentially with n.

For the fifth, the sixth, and the seventh terms, the analysis is the same as the analysis for decoding error probability over the MAC [1]. Therefore similar to the analysis given in [8], if

$$\min_{1\leq s\leq \ell^*}\left\{\frac{1}{s}I(X_1^s;Y|X_{s+1}^{\ell^*})\right\} > R, \tag{61}$$

these terms can be made arbitrarily small as n becomes large.

[4]This condition is satisfied if $\max\{I^{(2)}(X_1;Y|X_2), I^{(3)}(X_1;Y|X_2)\} > R$.

From Lemma 4, substituting $\ell^* = 3$, we have

$$\min_{s=1,2,3}\left\{\frac{1}{s}I^{(3)}(X_1^s;Y|X_{s+1}^3)\right\} = \frac{1}{3}I^{(3)}(X_1,X_2,X_3;Y). \tag{62}$$

Thus

$$\frac{1}{3}I^{(3)}(X_1,X_2,X_3;Y) > R, \tag{63}$$

is a sufficient condition for the fifth, the sixth, and the seventh terms converging to 0.

From the above discussions, we have the following constraint on the rate

$$\min\left\{I^{(3)}(X_1;Y|X_2,X_3), \frac{1}{2}I^{(3)}(X_1,X_2;Y|X_3), \right.$$
$$\frac{1}{3}I^{(3)}(X_1,X_2,X_3;Y), H^{(3)}(Y|X_2) - H^{(2)}(Y|X_1,X_2),$$
$$\left.\frac{1}{2}\big(H^{(3)}(Y) - H^{(2)}(Y|X_1,X_2)\big)\right\} > R. \tag{64}$$

From Lemmas 2 and 4, Eq. (64) is equivalent to

$$\min\left\{\frac{1}{3}I^{(3)}(X_1,X_2,X_3;Y), \right.$$
$$\left.\frac{1}{2}\big(H^{(3)}(Y) - H^{(2)}(Y|X_1,X_2)\big)\right\} > R. \tag{65}$$

We can see that there exists at least one sequence of codes for all sufficiently large n achieving arbitrary small decoding error probability if the rate satisfies Eq. (65).

Using a similar argument, we have a constraint similar to Eq. (65) for the general case $4 \le \ell^* \le k$:

$$\min\left\{\frac{1}{\ell^*}I^{(\ell^*)}(X_1^{\ell^*};Y), \right.$$
$$\frac{1}{\ell^*-1}\big(H^{(\ell^*)}(Y) - H^{(\ell^*-1)}(Y|X_1^{\ell^*-1})\big),$$
$$\frac{1}{\ell^*-2}\big(H^{(\ell^*)}(Y) - H^{(\ell^*-2)}(Y|X_1^{\ell^*-2})\big), \ldots,$$
$$\left.\frac{1}{2}\big(H^{(\ell^*)}(Y) - H^{(2)}(Y|X_1,X_2)\big)\right\} > R. \tag{66}$$

If we fix the maximum number of colluders k, Eq. (66) must be satisfied for and for all $\ell^* = 2,\ldots,k$. Therefore there exists at least one sequence of codes for all sufficiently large n achieving arbitrary small decoding error probability if Eq. (28) holds. □

VI. Conclusion

In this paper, we introduced a new attack model in which the number of colluders is distributed according to a certain probability distribution. We gave two classes of collusion attacks which include known collusion attacks in the context of multimedia fingerprinting. For these two attack classes, we derived achievable rates when only the type of attacks and the maximum number of colluders are known. Based on the derived formulas, we investigated achievable rates for the cases of some particular attacks. For the AND attack, the derived lower bound coincides with that given by Koga [8], although our attack model does not assume that the decoder knows the actual number of colluders.

Although we have discussed based on jointly typical set decoding, it is natural to extend this argument for ML decoding and derive random coding exponents. This remains as future studies.

Acknowledgments

This work was partially supported by JST's Special Coordination Funds for Promoting Science and Technology, and MEXT under Grant-in-Aid for Young Scientists (B) No. 22760270.

References

[1] R. Ahlswede, The capacity region of a channel with two senders and two receivers, *Ann. Prob.*, vol. 2, no. 5, pp. 805–814, Oct. 1974.

[2] N. P. Anthapadmanabhan, A. Barg, and I. Dumer, On the fingerprinting capacity under the marking assumption, *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2678–2689, Jun. 2008.

[3] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Trans. Inform. Theory*, vol. 54, no. 5 , pp. 1897–1905, Sep. 1998.

[4] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Akademiai Kiado: 2nd edition, 2011.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* 2nd Edition, New York: John Wiley & Sons, 2006.

[6] R.G. Gallager, *Information Theory and Reliable Communications*, New York: John Wiley & Sons, 1968.

[7] S. He and M. Wu, Collusion-resistant video fingerprinting for large user group, *IEEE Trans. Inform. Forensics and Security*, vol. 2, no. 4, pp. 697–709, Dec. 2007.

[8] H. Koga, On the capacity of the AND anti-collusion fingerprinting codes, in *IEICE Technical Report (in Japanese)*, no. IT2009-140, pp. 439–444, Mar. 2011.

[9] M. Kuribayashi, Interference removal operation for spread spectrum fingerprinting scheme, *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 2, pp. 403–417, Apr. 2012.

[10] S.-C. Lin, M. Shahmohammadi, and H. El Gamal, Fingerprinting with minimum distance decoding, *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 1, pp. 59–69, Jan. 2009.

[11] P. Moulin, Universal fingerprinting: Capacity and random-coding exponent, in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, pp. 220–224, Jul. 2008.

[12] P. Moulin, Universal fingerprinting: Capacity and random-coding exponent, *available at arxiv*, 2011.

[13] L.A. Shepp and I. Olkin, Entropy of the sum of independent bernoulli random variables and of the multinomial distribution, *Technical report, Standford University*, no. 131, pp.1–8, Jul. 1978.

[14] A. Somekh-Baruch and N. Merhav, On the capacity game of private fingerprinting systems under collusion attacks, *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 884–899, Mar. 2005.

[15] ——, Achievable error exponents for the private fingerprinting game, *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1827–1838, May 2007.

[16] G. Tardos, Optimal probabilistic fingerprint codes," *J. ACM (JACM)*, vol. 55, no. 2, pp. 1–24, May, 2008.

[17] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, Anti-collusion fingerprinting for multimedia, *IEEE Trans. Signal Proccessing*, vol. 51, no. 4, pp. 1069–1087, Apr. 2003.

[18] M. Wu, W. Trappe, W. Wang, Z.J. Wang, and K.J.R. Liu, Collusion-resistant fingerprinting for multimedia, *IEEE Signal Proccessing Magazine*, vol. 21, no. 2, pp. 15–21, Mar. 2004.

[19] J. Wang, S. Lian, Y. Dai, G. Liu, and Z. Ren, Secure semi-fragile multi-feature watermarking authentication scheme, *Journal of Information Assurance and Security*, vol.3, pp.195–204, 2006.

[20] M.-C. Lee, Y.-J. He, and Z. Chen, On improving an algebraic marking scheme for detecting DDoS attacks, *Journal of Information Assurance and Security*, vol.3, pp.279–288, 2008.

[21] H. Le and T.D. Bui, Online fingerprint identification with a fast and distortion tolerant hashing, *Journal of Information Assurance and Security*, vol.4, pp.117–123, 2009.

[22] B.S. Verkhovsky, Information assurance protocols: efficiency analysis and implementation for secure communication, *Journal of Information Assurance and Security*, vol.3, pp.263–269, 2008.

[23] M. Zamani, A.B.A. Manaf, R.B. Ahmad, F. Jaryani, H. Taherdoost, S.S. Chaeikar, and H.R. Zeidanloo, A novel approach for genetic audio watermarking, *Journal of Information Assurance and Security*, vol.5, pp.102–111, 2010.

Author Biographies

Gou Hosoya received the B.E. degree, M.E. degree, and Dr.E. degree in Industrial and Management Systems Engineering from Waseda University, Tokyo, Japan, in 2002, 2004, and 2008, respectively. From 2008 to 2011, he was a research associate at the Department of Industrial and Management Systems Engineering, Waseda University. He is currently an assistant professor at the Department of Management Science, Faculty of Engineering, Tokyo University of Science, Tokyo, Japan.
His research interests are coding theory and information theory. He is a member of the IEEE and the Institute of Electronics, Information and Communication Engineers (IEICE).

Hideki Yagi received the B.E., M.E., and Dr.E. degrees in Industrial and Management Systems Engineering from Waseda University, Tokyo, Japan, in 2001, 2003 and 2005, respectively. He was with the Media Network Center, Waseda University, from 2005 to 2008, and he was an Assistant Professor at the Center for Frontier Science and Engineering, the University of Electro-Communications, Tokyo, Japan, from 2008 to 2012. He is currently an Associate Professor at the Department of Communication Engineering and Informatics, the University of Electro-Communications. In the academic years of 2008 (three months) and 2010 (six months), he was with the Department of Electrical Engineering, Princeton University, NJ, U.S.A., as a Visiting Fellow.
His research interests include information theory, coding theory and information security. He is a member of the IEEE and the Institute of Electronics, Information and Communication Engineers (IEICE).

Manabu Kobayashi received the B.E. degree, M.E. degree and Dr.E. degree in Industrial and Management Systems Engineering form Waseda University, Tokyo, Japan, in 1994, 1996, and 2000, respectively. From 1998 to 2001, he was a research associate at the Department of Industrial and Management Systems Engineering, Waseda University. He is currently an associate professor at the Department of Information Science, Faculty of Engineering, Shonan Institute of Technology, Kanagawa, Japan.
His research interests are coding theory, information theory, and data mining. He is a member of Information Processing Society of Japan, the Institute of Electronics, Information and Communication Engineers (IEICE), and the IEEE.

Shigeichi Hirasawa received the B.S. degree in mathematics and the B.E. degree in electrical communication engineering from Waseda University, Tokyo, Japan, in 1961 and 1963, respectively, and the Dr.E. degree in electrical communication engineering from Osaka University, Osaka, Japan, in 1975. From 1963 to 1981, he was with the Mitsubishi Electric Corporation, Hyogo, Japan. From 1981 to 2009, he was a professor of the School of Science and Engineering, Waseda University, Tokyo, Japan. From 2009, he has been a Professor Emeritus, Waseda University, and a Honorary Fellow of Research Institute for Science and Engineering, Waseda University.
In 1979, he was a visiting scholar in the Computer Science Department at the University of California, Los Angeles (CSD, UCLA), CA. He was a visiting researcher at the Hungarian Academy of Science, Hungary, in 1985, and at the University of Trieste, Italy, in 1986. In 2002, he was also a visiting faculty at CSD, UCLA. From 1987 to 1989, he was the Chairman of the Technical Group on Information Theory of the Institute of Electronics, Information and Communication Engineers (IEICE). He received the 1993 Achievement Award and the 1993 Kobayashi-Memorial Achievement Award from IEICE. In 1996, he was the president of the Society of Information Theory and Its Applications (Soc. of ITA).

His research interests are information theory and its applications, and information processing systems. He is an IEEE Life Fellow, an IEICE Fellow, and a member of the Information Processing Society of Japan.