Saddle-point Solution of the Fingerprinting Capacity Game Under the Marking Assumption

Yen-Wei Huang
Beckman Inst., Coord. Sci. Lab and ECE Department
University of Illinois at Urbana-Champaign, USA
Email: huang37@illinois.edu

Pierre Moulin
Beckman Inst., Coord. Sci. Lab and ECE Department
University of Illinois at Urbana-Champaign, USA
Email: moulin@ifp.uiuc.edu

Abstract—We study a fingerprinting game in which the collusion channel is unknown. The encoder embeds fingerprints into a host sequence and provides the decoder with the capability to trace back pirated copies to the colluders.

Fingerprinting capacity has recently been derived as the limit value of a sequence of maxmin games with mutual information as the payoff function. However, these games generally do not admit saddle-point solutions and are very hard to solve numerically. Here under the so-called Boneh-Shaw marking assumption, we reformulate the capacity as the value of a single two-person zero-sum game, and show that it is achieved by a saddle-point solution.

If the maximal coalition size is \( k \) and the fingerprint alphabet is binary, we derive equations that can numerically solve the capacity game for arbitrary \( k \). We also provide tight upper and lower bounds on the capacity. Finally, we discuss the asymptotic behavior of the fingerprinting game for large \( k \) and practical implementation issues.

I. INTRODUCTION

Fingerprinting is a technique for copyright protection. It was first proposed by Wagner in 1983 [1] and has drawn a lot of attention in recent years. The content distributor embeds a unique mark, or fingerprint, within each licensed copy. By forming a group of users (pirates), the coalition can detect the fingerprints by inspecting the marks in each copy, and create a forgery that has only weak traces of their copies. A collusion-resistant fingerprinting system is designed to combat the collusive attacks.

Boneh and Shaw in [2] proposed the marking assumption for the fingerprinting problem. In this setup, fingerprints are a string of marks allocated throughout the host content. The locations of the marks are assumed unknown to the pirates. By comparing their available copies, the coalition can remove or replace the detected marks, but cannot modify those marks at which their copies agree. As a result, we can ignore the host sequence and consider only the fingerprints in our analysis.

Tardos in 2003 [3] invented a simple but efficient randomized fingerprinting code that invites many subsequent works, such as [4], [5]. Amiri and Tardos recently [6] (and independently of our work) further improved the rate by constructing a code based on a two-person zero-sum game. Although the code is far more efficient than the previous scheme, the intense computational complexity makes it less appealing for practical use.

A few researchers have also studied the problem from the information-theoretic point of view [6], [7], [8], [9], [10]. Here we focus on finding the maximum achievable rate, or capacity, of the fingerprinting system. Recently, Moulin in [9] provided the capacity formula in a general setup. We study specifically the marking assumption in this paper and show that the capacity is indeed the rate achieved in [6].

One concern is that neither the encoder nor the decoder knows the actual coalition size in real applications [11]. We show that this is actually not a big issue. The saddle-point property states that for a fingerprinting code designed for a maximal coalition size \( k \), there exists a unique saddle-point solution that achieves the capacity. That is, neither the content distributor nor the coalition can gain by deviating from its optimal strategy. As a result, the system is secure for any collusive attack of size no more than \( k \). Furthermore, even if the size-\( k \) anticipation is violated, no innocent user is accused [9]. The pirates are simply too powerful and we have not enough evidence to accuse them. Instead, the decoder gives us the more probable suspects which may allow the legal authority to do further investigation.

In this paper, we reformulate the capacity formula in [9] as the value of a single two-person zero-sum game and show that it admits a saddle-point solution. In the binary alphabet case, new capacity bounds are provided. The proofs not only show that the binary fingerprinting capacity is in \( \Theta(1/k^2) \), but they also provide secure strategies for both players of the game. Along with the numerical saddle-point solutions for small \( k \), we study the asymptotic behavior of the game for large \( k \).

The outline of the paper is as follows: In Section II we formally define fingerprinting capacity and review the capacity formula derived in [9]. The derivation of the single fingerprinting capacity game is shown in Section III and Section IV is devoted to the binary alphabet case.

II. PROBLEM STATEMENT

A. Notation

We use capital letters to represent random variables, and lowercase letters to their realizations. Boldfaces denote vectors, and calligraphic letters denote sets. For example, \( \mathbf{X} \in \mathcal{X}^n \) denotes a random vector \((X_1, \ldots, X_n)\), with each \( X_i \) taking values in \( \mathcal{X} \). The probability distribution of \( \mathbf{X} \) is denoted by \( p_{\mathbf{X}} \). The entropy of a random variable \( \mathbf{X} \) is denoted by \( H(\mathbf{X}) \). The mutual information of \( X \) and \( Y \), with joint pmf \( p \) is denoted by \( I_p(X;Y) = H(X) - H(X|Y) \). We also denote the...
binary entropy function by $h_2(p) \triangleq -p \log p - (1-p) \log (1-p)$ and $h_2(p) = (h_2(p_1), \ldots, h_2(p_n))'$. The KL divergence between two Bernoulli random variables with expectations $p$ and $q$ is denoted by $d_2(p||q) \triangleq p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}$. log denotes base 2 logarithm and $\ln$ denotes natural logarithm. Mathematical expectation is denoted by the symbol $\mathbb{E}$. The shorthands $f \sim g$ and $f \gtrsim g$ denote asymptotic relations $\lim_{k \to \infty} \frac{f(k)}{g(k)} = 1$ and $\liminf_{k \to \infty} \frac{f(k)}{g(k)} \geq 1$ respectively.

### B. Overview

Let $Q = \{0, 1, \ldots, q - 1\}$ denote a size-$q$ fingerprint alphabet, and $\mathcal{M} = \{1, \ldots, m\}$ denote the set of user indices. The fingerprint encoder assigns each user a length-$n$ fingerprint, using an encoding function

$$f_n : \mathcal{M} \times \mathcal{W}_n \to Q^n,$$

(1)

where the secret key $W_n \in \mathcal{W}_n$ is a random variable whose realization is known to the encoder and the decoder, but unknown to the pirates.

A coalition $\mathcal{K}$ is any size-$k$ subset of $\mathcal{M}$, and $X_{\mathcal{K}} = \{X_1, \ldots, X_k\}$ are the fingerprints available to the coalition. The collision channel produces the forgery $Y \in Q^n$ according to distribution $p_{Y|X_{\mathcal{K}}}$. The marking assumption states that if for some $j \in \{1, \ldots, n\}$, $x_{1,j} = \cdots = x_{k,j}$, then $y_j = x_{1,j}$.

Not knowing the actual fingerprint channel $p_{Y|X_{\mathcal{K}}}$, the single-output decoder

$$g_n : Q^n \times \mathcal{W}_n \to \mathcal{M}$$

(2)

accuses exactly one user based on the forgery $Y$ and the secret key $W_n$. The encoding and decoding functions $f_n$ and $g_n$ are deterministic, but a fingerprinting code is a random variable $(F_n, G_n)$ whose distribution is characterized by that of $W_n$. Under fingerprinting code $(F_n, G_n)$, the worst-case error probability is defined as

$$P_e^*(F_n, G_n, k) = \max_{\mathcal{K} \subseteq \mathcal{M}} \max_{|\mathcal{K}| \leq k} \Pr (G_n(Y, W_n) \notin \mathcal{K}),$$

(3)

where the second maximization is over all $p_{Y|X_{\mathcal{K}}}$ satisfying the marking assumption.

### C. Fingerprinting Capacity

We now define fingerprinting capacity and review the capacity formula [9] under the marking assumption. Capacity is achieved using a random coding scheme.

**Definition 2.1:** A rate $R$ is achievable for the $q$-ary alphabet and size-$k$ coalitions if there exists a sequence of fingerprinting codes $(F_n, G_n)$ for $m = \lceil 2^{nR} \rceil$ users such that

$$\lim_{n \to \infty} P_e^*(F_n, G_n, k) = 0.$$ (4)

**Definition 2.2:** Fingerprinting capacity $C_{k,q}$ is the supremum of all achievable rates for the $q$-ary alphabet and size-$k$ coalitions.

Now for a random variable $W$ defined over an alphabet $\mathcal{W} = \{1, 2, \ldots, l\}$, we define the embedding class

$$\mathcal{P}_X^w = \left\{ p_{X^n}(x^n, w) = p_W(w) \prod_{i=1}^k p_{X|X}(x_i|w) \right\},$$

(5)

the coalition class

$$\mathcal{P}_{Y|X}^w = \left\{ p_{Y|X}(y|x, W_n) = p_{Y|X}(y|x), \forall \pi; p_{Y|X}(y|x, W_n) = 1 \text{ if } y = x_1 = \cdots = x_k \right\},$$

(6)

where $\pi : \mathcal{K} \to \mathcal{K}$ is a permutation of the coalition $\mathcal{K}$, and the function

$$C_{k,q}^l = \frac{1}{k} \max_{\mathcal{K} \subseteq \mathcal{M}} \min_{p_{Y|X} \in \mathcal{P}_{Y|X}^w} I(X_{\mathcal{K}}; Y|W).$$

(7)

**Theorem 2.3:** [9, Theorem 3.4] The fingerprinting capacity $C_{k,q}$ for the $q$-ary alphabet and size-$k$ coalitions is

$$C_{k,q} = \lim_{l \to \infty} C_{k,q}^l.$$ (8)

Fingerprinting capacity is the limit value of a sequence of maxmin games. For any fixed $l$, $C_{k,q}^l$ is the maximin value of a two-person zero-sum game with the content distributor as the maximizer and the coalition as the minimizer. In the achievability proof, $W$ is a time-sharing random variable. As $l$ increases, it gives the content distributor more flexibility in choosing the codes. Hence the sequence $C_{k,q}^l, 1 \leq l \leq \infty$, is nondecreasing and admits a finite limit.

However, it is not an easy task to evaluate $C_{k,q}^l$ as well as the capacity-achieving probability distributions, even for small values of $l$. The reason is that a saddle-point solution is generally not guaranteed. For the binary alphabet ($q = 2$) and $l = 1$, we can derive that

$$C_{2,2}^1 = \frac{1}{k} 2^{-(k-1)},$$

which is not achieved by a saddle-point solution when $k > 2$. Also, this is very loose lower bound for $C_{k,2}$ comparing to the $\Theta(k^{-2})$ bound we will show in Sec. IV.C.

### III. THE TWO-PERSON ZERO-SUM GAME OF FINGERPRINTING CAPACITY

To establish the desired saddle-point property, we first reformulate the fingerprinting capacity as the value of a single maxmin game. Consider an auxiliary random vector $W$ drawn from the $q$-dimensional probability simplex

$$\mathcal{W}^q \triangleq \left\{ w \in \mathbb{R}^q : \sum_{x=0}^{q-1} \frac{w_x}{x+1} = 1 \text{ and } 0 \leq w_x \leq 1, x \in \mathcal{Q} \right\}$$

(9)

and the class of joint distributions

$$\mathcal{P}_{X^n|W} = \left\{ p_{X^n}(x^n, W_n) = p_W(w) \prod_{i=1}^k p_{X|W}(x_i|w) \right\},$$

where $p_{X|W}(x|w) = w_x$, $x \in \mathcal{Q}$. (10)

Then we can express $C_{k,q}$ as in the following theorem.
Theorem 3.1:

\[ C_{k,q} = \frac{1}{k} \max_{p_{X|X_K} \in \mathcal{P}_{X|X_K}} \min_{p_{Y|X} \in \mathcal{P}_{Y|X_K}} I(X_K;Y|W). \]  

Proof: Note that the class \( \mathcal{P}_{X|X_K} \) is compact and the payoff function is bounded, hence the maximizer exists. Denote the right-hand side of (11) by \( C'_{k,q} \). We can show that \( C'_{k,q} \geq C_{k,q} \) and \( C'_{k,q} \leq C_{k,q} \) respectively. For lack of space we skip the complete proof but give only the outline. For any finite l, let

\[ p_{X|X_K}^{l}(x_K,w) = p_{I|W}^{l}(w) \prod_{i \in K} p_{I_i|W}^{l}(x_i|w) \in \mathcal{P}_{X|X_K}. \]  

and \( p_{Y|X} \in \mathcal{P}_{Y|X_K} \) be the probability distributions that achieve \( I \). Let

\[ p_W(w) = \sum_{w \in S_w} p_{I|W}^{l}(w), \]  

where

\[ S_w = \left\{ w \in \mathcal{W} : p_{I|X_i|W}^{l}(x_i|w) = x_w, x \in \mathcal{Q} \right\}, \quad w \in \mathcal{W}^{q} \]  

then we can verify that the resulting \( p_{X|X_K} \) satisfies

\[ I(p_{X|X_K}, p_{Y|X_K}) = I(p_{X|X_K}, p_{Y|X_K}) = I(X_K;Y|W). \]  

Theorem 3.3 states the fingerprinting capacity as the maximin value of a two-person zero-sum game. Note that since \( p_{I|X_i|W}^{l} \) is actually fixed in the class of joint distributions defined in (10), the maximizer only has control over \( p_{I|X_i|W}^{l} \), which lies within the class of probability distributions over \( \mathcal{W}^{q} \), denoted by \( \mathcal{P}_{I|X_i|W}^{l} \). Also, the payoff function \( I(X_K;Y|W) \) is a linear function of \( p_{I|X_i|W}^{l} \) for fixed \( p_{I|X_i|W}^{l} \) and a convex function of \( p_{I|X_i|W}^{l} \) for fixed \( p_{I|X_i|W}^{l} \). By the minimax theorem [12], the game admits a saddle-point solution. In the game-theoretic point of view, this is a so-called convex game [13, §2.5]. The maximizer has an optimal mixed-strategy with a finite support and the minimizer has an optimal unique pure-strategy. Furthermore, the maximin value equals the minimax value of the same game restricting both players with pure strategies. The following theorem states these properties.

Theorem 3.2:

\[ C_{k, q} = \frac{1}{k} \max_{p_{I|X_i|W}^{l} \in \mathcal{P}_{I|X_i|W}^{l}} \min_{w \in \mathcal{W}^{q}} I(X_K;Y|W = w) \]

\[ = \frac{1}{k} \max_{p_{I|X_i|W}^{l} \in \mathcal{P}_{I|X_i|W}^{l}} \min_{w \in \mathcal{W}^{q}} I(X_K;Y|W). \]  

IV. CAPACITY FOR THE BINARY ALPHABET

We have established the existence of a saddle-point solution for the capacity game. For the rest of the paper, we focus on the binary alphabet case and see how the game can be solved.

A. Game Definition

We can simplify the game as follows:

1) **Fingerprinting Code.** \( Q = \{0, 1\} \). The auxiliary random vector \( W \) now has only one degree of freedom, and we redefine it as \( W \in \{0, 1\} \). \( p_{I|X_i|W}^{l} \) denotes its distribution, and \( p_{I|X_i|W}^{l} \) the support of \( p_{I|X_i|W}^{l} \). \( p_{I|X_i|W}^{l} \sim \text{Bernoulli}(W) \) is fixed.

2) **Collusion Channel.** Since \( p_{I|X|I_i|W}^{l} \in \mathcal{P}_{I|X|I_i|W}^{l} \) defined in (6) is invariant to permutations of \( X \), it takes the form \( p_{Y|Z} \), where \( Z = \sum_{i=1}^{k} X_i \in \{0, 1, \ldots, k\} \) is the number of 1’s in \( X \). Let \( p = (p_0, \ldots, p_k)' \), where \( p_0 = p_{Y|Z}(1|z), z = 0, \ldots, k \). The marking assumption enforces that \( p_0 = 0 \) and \( p_k = 1 \), and the collusion channel is then completely characterized by \( p \).

3) **Capacity.** If we let \( \alpha(w) = (\alpha_0(w), \ldots, \alpha_k(w))' \), where

\[ \alpha_z(w) \triangleq p_{Z|W}(z|w) = \binom{k}{z} w^z (1-w)^{k-z} \]  

is the binomial distribution with parameter \( w \in [0, 1] \), then we have

\[ \hat{C}(w, p) \triangleq I(X_K;Y|W = w) \]

\[ \hat{C}(w, p) = H(Y|W = w) - H(Y|X_K, W = w) \]

\[ = h_2 \left( \sum_{z=0}^{k} p_z \alpha_z(w) \right) - \sum_{z=0}^{k} h_2(p_z) \alpha_z(w) \]

Another representation of \( \hat{C}(w, p) \) is

\[ \hat{C}(w, p) = D(p_{Y|Z}||p_{Y|W}p_{Z|W}|W = w) \]

\[ = \sum_{z=0}^{k} \alpha_z(w) d_2(p_z|\alpha_z) \]  

The fingerprinting capacity game for the binary alphabet under the marking assumption can then be written as

\[ C_{k,2} = \frac{1}{k} \max_{p_{I|X_i|W}^{l} \in \mathcal{P}_{I|X_i|W}^{l}} \min_{w \in \mathcal{W}^{q}} \hat{C}(W, p) \]

\[ = \frac{1}{k} \min_{w \in \mathcal{W}^{q}} \max_{p_{I|X_i|W}^{l} \in \mathcal{P}_{I|X_i|W}^{l}} \hat{C}(W, p). \]

B. Analysis of the Convex Game

**Lemma 4.1:** If \( p^* \) is the minimizer in (20) and (21), then

\[ p_z^* = 1 - p_{k-z}, z = 0, \ldots, k. \]  

Also, if \( p_{I|X_i|W}^{l} \) is the maximizer of (20), then

\[ p_{I|X_i|W}^{l}(w) = p_{I|X_i|W}^{l}(1 - w), \forall w \in [0, 1]. \]  

We skip the complete proof of Lemma 4.1 here but only explain its idea. Note that \( p_z^* \) represents the probability of assigning \( Y \) as 1 when \( X_K \) has \( z \) 1’s and \( (k-z) \) 0’s. By symmetry we should expect in colluders’ capacity-achieving
strategy, the probability of assigning $Y$ as 0 when $X_K$ has $(k - z) ~1$’s and $z ~0$’s to also be $p^*_z$, i.e., $p^*_{k-z} = 1 - p^*_z$, $z = 0, \ldots, k$. Similarly, the capacity-achieving fingering codes should have the same distribution for 0 and 1, hence $p^*_W$ should be symmetric as stated.

Owing to the existence of the saddle-point solution, $p^*$ and $p^*_W$ must satisfy the following:

1) When $p = p^*$ is fixed, $\hat{C}(w, p^*)$ is a differentiable function over the unit interval. The support of $p^*_W$, $\mathbb{W}^*_S$, can only take values at the maximizers of $\hat{C}(w, p^*)$.

Hence we have

$$\left\{ \begin{array}{l} \hat{C}(w, p^*) = kC_{2k}, \quad \forall w \in \mathbb{W}^*_S. \\ \frac{\partial}{\partial w}\hat{C}(w, p^*) = 0 \end{array} \right. \quad (24)$$

2) When $p_W = p^*_W$ is fixed, and if we only consider $p$ that satisfies (22), then we have

$$E_{p_W}\left[ \frac{\partial}{\partial p_z}\hat{C}(W, p^*) \right] = 0, \quad z = 1, \ldots, \left\lfloor \frac{k-1}{2} \right\rfloor. \quad (25)$$

By the convexity in $p$ of the payoff function, we know that $|\mathbb{W}^*_S| \leq \left\lfloor \frac{k+1}{2} \right\rfloor$ (see [13, §2.5]). With a fixed support cardinality, we can obtain candidate capacity-achieving distributions $p^*$ and $p^*_W$ by solving (24) and (25), and then verify those candidate distributions are optimal by examining the second partial derivatives. Once $p^*$ and $p^*_W$ are found, we can get $C_{k,2}$ by substituting them into (20).

C. Bounds on Capacity

For general $k$, the following two theorems gives us $C_{k,2} = \Theta(1/k^2)$.

**Theorem 4.2:**

$$C_{k,2} \leq \frac{1}{k^2 \ln 2} = \frac{1.443 \ldots}{k^2}. \quad (26)$$

**Proof:**

Consider the so-called “interleaving attack” $p^\infty$ defined by

$$p^\infty = \frac{1}{k} \mathbb{I}_{z = 0, \ldots, k},$$

then we have

$$C_{k,2} = \frac{1}{k} \min_p \max_w \hat{C}(w, p) \leq \frac{1}{k} \max_w \hat{C}(w, p^\infty) \leq \frac{1}{k} \max_w \left\{ h_2(w) - \sum_{z=0}^{k} \alpha_z(w)h_2 \left( \frac{z}{k} \right) \right\} \leq \frac{1}{k^2 \ln 2},$$

where the last inequality results from [10, Theorem 4.3].

**Theorem 4.3:**

$$C_{k,2} \geq \frac{2}{k^2 \pi^2 \ln 2} = 0.292 \ldots. \quad (28)$$

**Proof:** Consider the continuous distribution

$$p^\infty_W(w) = \frac{1}{\pi \sqrt{w(1-w)}}, w \in (0,1), \quad (29)$$

Finally, (d) follows from the marking assumption: $\alpha'(0)p = 0$ and $\alpha'(1)p = 1$. ■

D. Asymptotic Behavior for Large Coalition

We solve the capacity games for small $k$’s using (24) and (25) in Sec. IV-B. Fig. 1 shows the capacity along with the upper and lower bounds. Amir and Tardos [6] stated without proof that $C_{k,2} \geq (k^2 2 \ln 2)^{-1}$. Our numerical results suggest that this bound is tight and that the convergence is fairly quick.

Evaluating the convex game of (20) or (21) for large $k$ is still a difficult task. However, Theorem 4.2 and 4.3 shed lights on the asymptotic behavior of the game. If a less powerful coalition simply chooses the interleaving attack as their strategy (a.k.a. “uniform channel” in [10] and “blind colluders” in [5]), Theorem 4.2 shows that the gain in rate is no more than a factor of two. In fact, one can show that
unifies the asymptotic distribution of designed to be independent of the collusion channel [5]. This joint in distribution. The same distribution was used in Tardos' Fig. 3 suggests, surprisingly, that slightly shorter even against a naive coalition who performs attack is asymptotically optimal. This also answers Furon solely the interleaving attack.

C(k) = (k^2 \ln 2)^{-1} for all w ∈ (0, 1) (based on results from [15, \S 1.6]). Fig. 2 shows the difference between p* and p∞ for different values of k. This suggests that the interleaving attack is asymptotically optimal. This also answers Furon et al.'s question in [5]: the fingerprinting code can only be slightly shorter even against a naive coalition who performs solely the interleaving attack.

An even bigger issue for the content distributor is that the computation of the optimal p∗ W is infeasible for large k. Luckily, Theorem 4.3 resolves this predicament. By using p∞ W of (29), the loss in rate is only by a factor of about 2.5. Fig. 3 suggests, surprisingly, that p∗ W converges to p∞ W in distribution. The same distribution was used in Tardos’ fingerprinting code in [3], which uses a simple decoder and is designed to be independent of the collusion channel [5]. This unifies the asymptotic distribution of p∗ W for the simple and joint decoders (see [9]): p∞ W is asymptotically optimal.

We conclude with the following conjecture:

Conjecture 4.4: When k → ∞, we have

Ck,2 ≈ (k^2 \ln 2)^{-1},

p* ≈ p∞,

and

pW → p∞ W in distribution.

ACKNOWLEDGMENT

The authors would like to thank N. Prasanth Anthapadmanabhan for illuminating discussions and helpful comments.

This research is supported by NSF under grants CCF 06-35137 and CCF 07-29061.

REFERENCES

[1] N. R. Wagner, “Fingerprinting,” in SP ’83: Proceedings of the 1983 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 1983, p. 18.
[2] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1897–1905, September 1998.
[3] G. Tardos, “Optimal probabilistic fingerprint codes,” in In 35th ACM STOC. ACM Press, 2003, pp. 116–125.
[4] B. Skorci, S. Katzenbeisser, and M. U. Celik, “Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes,” Des. Codes Cryptography, vol. 46, no. 2, pp. 137–166, 2008.
[5] T. Furon, A. Guyader, and F. Cérou, “On the design and optimization of Tardos probabilistic fingerprinting codes,” Information Hiding: 10th International Workshop, IH 2008, Santa Barbara, CA, USA, May 19-21, 2008, Revised Selected Papers, pp. 341–356, 2008.
[6] E. Amiri and G. Tardos, “High rate fingerprinting codes and the fingerprinting capacity,” in SODA ’09: Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2009, pp. 336–345.
[7] P. Moulin and J. A. O’Sullivan, “Information-theoretic analysis of information hiding,” IEEE Trans. Inf. Theory, vol. 49, no. 3, pp. 565–593, March 2003.
[8] P. Moulin, “Universal fingerprinting: Capacity and random-coding exponents,” in Proc. IEEE International Symposium on Information Theory ISIT 2008, 6–11 July 2008, pp. 220–224.
[9] ———. (2008, December) Universal fingerprinting: Capacity and random-coding exponents. [Online]. Available: http://arxiv.org/abs/0801.3837v2
[10] N. P. Anthapadmanabhan, A. Barg, and J. Dumer, “On the fingerprinting capacity under the marking assumption,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2678–2689, June 2008.
[11] T. Furon and L. Perez-Freire. (2009) Worst case attacks against binary probabilistic traitor tracing codes. [Online]. Available: http://arxiv.org/abs/0903.3480
[12] M. Sion, “On general minimax theorems,” Pacific Journal of Mathematics, vol. 8, no. 1, pp. 171–176, 1958.
[13] L. A. Petrosjan and N. A. Zenkevich, Game theory. World Scientific, 1996.
[14] T. M. Cover and J. A. Thomas, Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing). Wiley-Interscience, July 2006.
[15] G. G. Lorentz, Bernstein Polynomials, 2nd ed. AMS Bookstore, 1986.