COMMUNICATION THEORETIC ANALYSIS OF DIGITAL FINGERPRINTING UNDER LINEAR AVERAGING GAUSSIAN ATTACK

by

Özgür Dalkılıç

B.S., in Electrical and Electronics Engineering, Boğaziçi University, 2006

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Department of Electrical and Electronics Engineering
Boğaziçi University

2009

ACKNOWLEDGEMENTS

First of all, I would like to thank my thesis supervisor M. Kıvanç Mıhçak with whom I took my first steps into the area of academic research. Not only his academic supervision but also his friendship is among the most valuable gains I obtained during this study.

I would like to thank members of thesis jury, Assist. Prof. F. Kerem Harmancı and Assist. Prof. S. Serdar Kozat, for their attention and helpful comments.

As a friend and a colleague, Ersen Ekrem, deserves my highest gratitudes for his initial work and ideas, and his encouragement during my all MSc. study.

I also would like to thank to Eray Varlık who greatly helped me for this thesis, worked as hard as me on this thesis's descendent problems and contributed to our conference paper with his large yet growing knowledge on mathematics.

My dear family have always their part in any achievemnt of mine and it is not an exception for this study.

Years spent on this study become bearable with my friends to whom I would like to express my sincere thanks: Ekin Şahin, Ufuk Mat, Onur Özyeşil, and Yücel Altuğ.

Also, I want to thank TÜBİTAK for their financial support via the full Graduate Studies Scholarship, No. 2210.

ABSTRACT

COMMUNICATION THEORETIC ANALYSIS OF DIGITAL FINGERPRINTING UNDER LINEAR AVERAGING GAUSSIAN ATTACK

In this thesis, performance of correlation detector is investigated from a communication theoretic perspective for additive fingerprinting under Gaussian averaging attack. First, digital fingerprinting problem is modeled as a communication system: Presence of users in the collusion is embodied by binary messages, fingerprints are represented as modulating waveforms and linear averaging collusion attack is modeled as a multiple-access channel. It is stated that correlation detector, which calculates the correlation between a specific fingerprint and the colluded copy, is an analogue of the well known matched filter. It is obvious that matched filter is suboptimum for colluder detection so multiple-access interference causing this suboptimality is quantified. Because of the focused detection and decision at the receiver bit error probability is considered as the basic performance measure and generic bit error probability expression that is valid for any additive codebook is derived. In terms of fingerprint codebooks orthogonal, simplex and Gaussian fingerprints are studied. For each codebook minimum achievable bit error probability is obtained and collusion resistance expression is derived based on bit error probability. Furthermore asymptotic behavior of minimum bit error probability is investigated with respect to signal length, number of users and noise power. Error exponents are also calculated and rate of variation of bit error probability at asymptotes is studied.

ÖZET

DOĞRUSAL GAUSS ORTALAMA SALDIRISI ALTINDA SAYISAL PARMAK-İZİ'NİN İLETİŞİM TEORİSİ AÇISINDAN İNCELEMESİ

Bu çalışmada, ilintili algılayıcının ortalama-Gauss saldırısına maruz kalmış sayısal toplanır parmak-izleri için başarımının iletişim teorisi açısından incelemesi yapılmaktadır. İlk olarak, sayısal parmak-izi meselesi bir iletişim sistemi olarak modellenmiştir: Kullanıcıların saldırıda bulunup bulunmamaları 0 ve 1 olarak simgelenmekte, parmak-izleri kipleyici dalga biçimi olarak kullanılmakta ve doğrusal ortalama saldırısı çok kullanıcılı iletişim kanalı olarak ifade edilmektedir. Saldırıya maruz kalmış sinyal ile belli bir parmak-izi arasındaki ilintiyi ölçen ilintili algılayıcının iletişim sistemlerindeki uyumlu süzgece denk olduğu belitrtilmiştir. Uyumlu süzgecin çok kullanıcılı kanallar için en iyi alıcı olmadığı ortaya konulmuş ve buna neden olan çoklu erişim girişimi açık bir şekilde nicelenmiştir. Alıcı tarafında uygulanan odaklı sezim ve karar nedeniyle bit hata olasılığı geçerli başarım ölçütü olarak kullanılmış ve bütün toplanır parmak-izleri için geçerli olan genel bit hata olasılığı türetilmiştir. Bu çalışmada belli parmak-izleri olarak dik, simpleks ve Gauss parmak-izleri ele alınmaktadır. Her parmak-izi için gerçekleştirilebilir en küçük hata olasılığı hesaplanmış ve saldırı direnci ifadesi bit hata olasılığına bağlı olarak elde edilmiştir. Bundan başka bit hata olasılığının sonuşur davranışı sinyal uzunluğuna, kullanıcı sayısına ve gürültü gücüne göre incelenmiştir. Ayrıca hata üstelleri de hesaplanarak bit hata olasılığının sonuşurdaki değişim hızı da ortaya konulmuştur.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS/ABBREVIATIONS

$\mathbb{R}$	The set of real numbers
$\mathbb{R}^N$	N dimensional real space
$Pr(.)$	Probability
$E(.)$	Expectation
$\mathcal{N}(\mu, \sigma^2)$	Gaussian distribution with mean μ and variance σ^2
$\mathcal{N}(\mu, \mathbf{\Sigma})$	Gaussian distribution with mean vector μ and covariance matrix $\mathbf{\Sigma}$
$\mathbf{I}_N$	Identity matrix of size NxN
$\Gamma(.)$	Gamma function
$Q(.)$	Q function
$exp(.)$	Natural exponential
$log(.)$	Natural logarithm
$\mathbf{q}$	Fingerprint vector
$\mathbf{q}_k$	Fingerprint vector of kth user
$\|\mathbf{q}\|$	Norm of vector $\mathbf{q}$
$\mathbf{q}^T$	Transpose of vector $\mathbf{q}$
$\mathbf{x}_k$	Fingerprinted signal of kth user
$\mathbf{s}$	Original fingerprint-free content, host signal
$\mathbf{y}$	Attacked signal
SC	Set of colluders
M	Total number of users
K	Number of colluders
b	Binary value representing the presence of users in the collusion
$\hat{b}$	Decision on b
$\mathbf{n}$	Noise vector
$\omega(\mathbf{b})$	Hamming weight of vector $\mathbf{b}$
D_E	Distortion constraint on the embedder
D_A	Distortion constraint on the attacker
v_k	Output of the kth matched filter

$\mathbf{v}$	Output of matched filters whose kth entry is v_k
τ	Threshold
$\mathbf{Q}$	Cross-correlation matrix for a fingerprint codebook
γ_k	Interference term from fingerprints at the output of kth matched filter
θ_k	Probability of user k being in the collusion
$C(n,k)$	Number of size k combinations of a size n set
α	Maximum cross-correlation value between codewords of a codebook
β	Minimum cross-correlation value between codewords of a codebook
P_e^k	Bit error probability of kth user
$P_e^{*,k}$	Bit error probability of kth user for the codebook represented by $*$
$P_{e,min}^*$	Minimum bit error probability of the codebook represented by $*$
τ_{opt}^*	Optimum threshold for the codebook represented by $*$
K^*	Collusion resistance of the codebook represented by $*$
e^*	Error exponent of the codebook represented by $*$
$\tilde{P}_e^*$	Approximate bit error probability of the codebook represented by $*$
MAI	Multiple-Access Interference
i.i.d.	Independent Identically Distributed
AWGN	Additive White Gaussian Noise
WNR	Watermark to Noise Ratio

1. INTRODUCTION

Digital material such as video and audio is easily accessible and modifiable by third parties because of its nature. Protection of such a vague property from unauthorized access and illegal redistribution needs special techniques. Watermarking, whose basic idea is to hide useful information into data, is one of these techniques. In watermarking visible or invisible signature data, which is generally retrievable, is embedded into the digital content that is intended to be protected. Consequently digital watermarking differs from classical cryptographic security methods by allowing the content to be tracked and protected without need of data secrecy.

Fingerprinting is a special category of watermarking. It is specifically used for tracking and tracing digital content. In fingerprinting a unique signature data, which is named as fingerprint, is embedded into each copy of the multimedia content where original data can be called as the host signal. Decoding the embedded fingerprint from the marked data reveals the identity of the content owner. Hence digital fingerprinting can be utilized for tracing the distributed copies of multimedia content, preventing illegal redistribution by identifying the owner of a specific copy and spotting the sources of leakages from a data source that has to be kept secret. Considering the online music and video stores selling copies of multimedia content over the internet and the growing peer-to-peer sharing networks significance of digital copyright management and role of watermarking in this context can be grasped with a deeper understanding. As an example; a traitor ripping his own copyrighted movie from legal vendor DVD can be identified and put in front of court by decoding the fingerprint from reproduced copies that are obtained from sharing networks or pirate shops.

Any act of modifying the marked content in order to remove the embedded fingerprint is called an attack and users involving in this act are named as attackers. Any fingerprinting system is desired to be robust against attacks, i.e. the detector should be able to reliably identify attacking users from their fingerprints by inspecting the attacked data. Collusion attack, in which a group of attackers combine their marked

data in order to remove the fingerprints, is the most considered attack in the literature. Collusion resistance is defined as the maximum number of colluders that can be identified while keeping the error probability sufficiently small and it is one of the basic performance merits of a copyright protection system. Most of the work in the literature focus on constructing collusion resistant fingerprint codes or designing and analyzing attack models in terms of collusion resistance.

From the technical point of view digital fingerprinting, as a special class of watermarking, has some special considerations and requirements. To begin with, decoding of embedded fingerprints from digital data is generally non-blind which means original mark-free host signal is available at the detector. Furthermore fingerprints are inserted into digital data so that they are invisible or at least imperceptible by human senses. Remembering that fingerprinted data is marketed and distributed to end users perceptual quality of the multimedia content is of great importance and it should not degrade with insertion of hidden data. Thus fingerprint embedder should control the amount of distortion introduced by data hiding. Besides the fingerprint system and the embedder, attacking schemes are also restrained by the amount of distortion on the digital content. Attacker should not degrade the perceptual quality of the content beyond predefined limits while trying to remove the embedded fingerprints.

Research focus in fingerprint literature can be roughly grouped into two factions. First one is the design and analysis of robust fingerprints and embedding techniques. The second one is the analysis of attack schemes and performance of fingerprinting methods under proposed attacks. We start with introducing the attack types commonly utilized in the literature. Then we describe the embedding techniques and portray various fingerprint codes along with their performance measures under the aforementioned attacks.

Collusion is the most widely utilized and studied attack class in the literature [1], [2], [3], [4], [5], [6]. In collusion a group of malicious users, which is called a collusion clique, combine their copies with the intention to obtain a new copy that is free of fingerprints or with little trace of fingerprints. There are several types of collusion

attacks that can be classified into two groups as linear and nonlinear. Averaging attack is a simple yet effective type of linear attack. It consists of averaging colluders' copies and adding small amount of noise on top of the averaged data. In [7] it has been shown that by employing linear averaging attack with Gaussian noise any fingerprinting system can be successfully broken by $O\left(\sqrt{N/\log(N)}\right)$ adversaries where N is the length of the fingerprints. Moreover linear averaging attack is optimal in the sense that attack distortion is minimized [3]. On the other hand nonlinear collusion attacks manipulate the digital content by using maximum, minimum values or some other nonlinear operators on the fingerprinted data [5], [6]. Another nonlinear attack where colluders generate a forged copy by interleaving their own fingerprinted copies is studied in [4].

An early mark embedding technique is to hide the fingerprint by modifying the quantization values of the host signal, most notably the least significant bits of the data, [8], [9]. A more recent and extensively used additive embedding technique is spread spectrum watermarking [10], [11] which borrows ideas of modulation and spreading from communication theory [12]. In spread spectrum watermarking fingerprint is added to the data, i.e. modulate the host signal, in spatial domain, in frequency domain or in another domain of interest depending on the application [1]. It has been shown that spread spectrum watermarking is highly resistant to collusion attacks [13], [10]. Another class of embedding method is given the name quantization index modulation [14]. They were shown to be more robust against many attacks than spread spectrum methods and to be optimal for Gaussian channels.

One of the earliest collusion resistant fingerprint code construction is introduced in [2] by Boneh and Shaw where generic digital data, obeying the marking assumption stated therein, is marked by bits at specific positions. In this work it was shown that described fingerprint code is capable of identifying one user with high probability if the code length is sufficiently large. Improved code construction methods over Boneh-Shaw fingerprinting were proposed in [15], [16], [17] where better collusion resistance results were obtained.

Using spread spectrum embedding described in [10] a large variety of fingerprint codes, which are more resilient and robust against linear multi-user collusion attacks, can be constructed. In [18] authors show that spread spectrum codes can stand fairly firm against nonlinear geometric attacks. Modulating the host signal using orthogonal codes is one effective approach for colluder identification under linear averaging attack [19]. Although orthogonal codes enjoy optimum detection and easy-to-analyze models they are limited by the number of users that can be accommodated. Layered coding approaches combining error correcting codes and spread spectrum embedding are also studied in [20]. In [21] anticollusion codebooks are introduced whose any size-K subset is unique and hence can be identified by the detector. Another class of fingerprint codes are simplex fingerprints proposed in [22]. In N dimensional space, they maximize the minimum distance between codewords which governs the probability of error expression. Stochastic codebook generation is another option for code construction. Collusion resistance of randomly generated Gaussian fingerprints is examined in [13]. Additionally authors in [23] explored spread spectrum bounded Gaussian fingerprints under gradient attack.

Literature work focusing on the fingerprint detector side is not as fruitful as the work on code design or attack analysis. Correlation detector which quantifies the similarity between fingerprints and forged signal via correlation based detection statistics is the most commonly used structure for detecting spread spectrum fingerprints. Decision at the detector can be made by hard thresholding the correlator outputs or using the maximum value of the outputs [19]. In [21] soft thresholding and sequential detection with their performance results are presented. As the basic performance criterion on fingerprinting systems collusion resistance is comprehensively examined in the literature [2], [19], [7]. Detection and error probabilities for various codebooks and attack classes are of similar interest as the collusion resistance. In [19], [5] authors considered the probability of detecting at least one colluder and probability of falsely accusing at least one innocent and they derived collusion resistance results upon these cost functions. For simplex fingerprints probability of error derivations are presented in [22] but exact expression is not given. Moreover collusion resistance and asymptotic behavior of simplex fingerprints are not investigated in the literature. In [24], [25] fin-

gerprinting problem is treated from an information theoretic perspective and capacity and achievable rates are derived.

The fundamental motivation of this work is the relatively poor analysis and development on fingerprint detector structures. To the best of our knowledge probability of error, expecially bit error probability, and its exact expression for various codebooks such as simplex and Gaussian are not investigated deeply in the literature. Analysis of collusion resistance and asymptotic behavior for simplex and Gaussian fingerprints are also open problems. It is obvious that besides codebook design detector structure heavily affects the performance of the fingerprinting system. Therefore thorough performance analysis of conventional detectors and design of new detector structures has the potential to be a valuable effort in fingerprinting literature. Main contributions for this thesis can be summarized as follows:

In this work a communication theoretic analysis of the fingerprinting problem is presented from the detector point of view. Digital fingerprinting is modeled as a communication system where embedder is the transmitter, collusion attack is the communication channel and the fingerprint detector is the receiver. Information sent through the channel is represented as a binary value embodying the presence of a user in the collusion clique and additive fingerprint codes are modeled as modulating waveforms of these binary messages. As the attack channel linear averaging attack with Gaussian noise, i.e. averaging Gaussian attack, is considered and it is shown that averaging attack corresponds to a multiple-access communication channel. In our setup conventional correlation detector is the analogue of well known matched filter and the decision statistic for a specific user is the output of the detector matched to that user's fingerprint codeword. Since the detector works in a 'focused' fashion bit error probability of a user is used as the main performance figure. A generic bit error probability expression that is valid for any given additive codebook is derived and multiple-access interference is quantified. Then the generic result is utilized for specific fingerprint codebooks. Orthogonal, simplex and Gaussian fingerprints are considered and exact bit error probabilities are computed as special cases of the generic result. For these codebooks multiple-access interference at the output of the matched filter

is also analyzed. Subsequently, collusion resistance of each fingerprint is investigated. Note that bit error probability is used as the cost function for collusion resistance derivation. Afterwards asymptotic behavior of bit error probability expression of each codebook is analyzed with respect to signal length, noise power and number of users. Finally we examine the error exponent of bit error probability which gives insight into its asymptotic behavior.

2. NOTATION AND PROBLEM SETUP

2.1. Notation

Bold lowercase letters denote vectors and bold uppercase letters denote matrices. Bold lowercase letters with a subscript represent a specific vector e.g. $\mathbf{q}_j$ is the fingerprint vector of jth user. $\mathbb{R}$ stands for the set of real numbers and $\mathbb{R}^N$ for the N dimensional real space spanned by length N vectors. Transpose of a vector or matrix is represented by a superscript T. Euclidean inner product of two vectors $\mathbf{q}_i, \mathbf{q}_j \in \mathbb{R}^N$ is $\langle \mathbf{q}_i, \mathbf{q}_j \rangle$ and L_2 norm of a vector is $\|\mathbf{q}_j\|$. Hamming weight of vector $\mathbf{b}$ is denoted by $\omega(\mathbf{b})$. $C(n,k)$ represents size k combinations from a set of size n.

$Pr(.)$ denotes a probability, $E(.)$ denotes expectation. Subscript letters under expectation operator represent the random variable whose probability distribution is used for expectation. '$\sim$' is used to indicate that random variable on the left of this operator comes from the distribution given in the right, e.g. if x is Gaussian with 0 mean and σ^2 variance we denote it by $x \sim \mathcal{N}(0, \sigma^2)$. Q function represents the Gaussian tail probability and it is given by $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$. The abbreviation "i.i.d." stands for independent and identically distributed. $\log(x)$ is the natural logarithm of x and $\exp(x)$ is the exponential e^x.

2.2. Signal Model

In this setup, employed embedding method is additive watermarking. The signal model described in this section and the bit error probability expressions derived in Section 3 are valid for any additive fingerprint codebook. The attack channel is linear averaging and additive noise is i.i.d. Gaussian. Note that both embedder and attack channel obey distortion constraints introduced in Section 2.3. There are a total of M users and K of them join the collusion clique independent of each other. At the detector side correlation detector is used. Correlation detector computes correlation between colluded signal and individual users' fingerprints and it is also named as the

focused detector. It is assumed that number of colluders is known at the detector. Hard thresholding is applied to the outputs of the focused detector and decisions are made according to the thresholded decision statistics.

Considering additive code embedding, fingerprinted data for kth user, $\mathbf{x}_k$, is given by

$$\mathbf{x}_k = \mathbf{s} + \mathbf{q}_k \tag{2.1}$$

where $\mathbf{s}$ and $\mathbf{q}_k$ are the original content and kth user's fingerprinting code, respectively. $\mathbf{x_k}$, $\mathbf{s}$ and $\mathbf{q}_k$ are all length N column vectors. Linear averaging Gaussian attack averages copies of K users and add *additive white Gaussian noise* (AWGN) to the averaged signal. Colluded copy that is available to the decoder, $\mathbf{y}$, is given by

$$\mathbf{y} = \mathbf{s} + \frac{1}{K}\sum_{j \in SC} \mathbf{q}_j + \mathbf{n} \tag{2.2}$$

where SC is the set of colluders and $\mathbf{n}$ is the length N AWGN vector with zero mean and $\sigma^2\mathbf{I}_N$ covariance matrix. It is safe to assume that the original signal $\mathbf{s}$ is available at the decoder. Therefore, from now on, the colluded signal is going to be simply written as

$$\mathbf{y} = \frac{1}{K}\sum_{j \in SC} \mathbf{q}_j + \mathbf{n} \tag{2.3}$$

Quantifying each user's presence in the collusion clique as a binary random variable leads to the following equivalent expression for the colluded signal $\mathbf{y}$

$$\mathbf{y} = \frac{1}{K}\sum_{j=1}^{M} \mathbf{q}_j b_j + \mathbf{n} \tag{2.4}$$

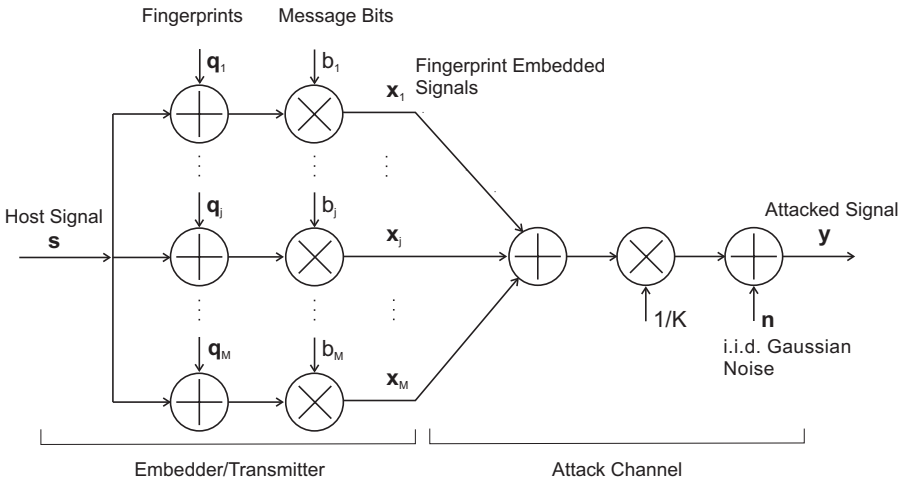

Figure 2.1. Signal model for the fingerprinting problem.

where

$$b_j = \begin{cases} 1 & \text{if user j is in the collusion set } SC, \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Above representation of the colluded signal leads to two important observations. First, users send binary messages that are modulated by signature waveforms to the detector. Second, modulated waveforms are received as a single superposed waveform on top of which AWGN is added. In other words first observation states that collusion activity is in effect transmission of a message to a receiver. Second observation, on the other hand, characterizes the channel that this transmission takes place; a multiple access channel with AWGN. In the light of these observations it can be concluded that fingerprinting problem with averaging attack is equivalent to a communication problem with a multiple-access AWGN channel. In Figure 2.1 the described signal model is depicted.

2.3. Distortion Constraints

Distortion constraints are imposed on both the fingerprint embedder and colluders in order to preserve the perceptual quality of the original multimedia content. In particular, it can be assumed that L_2 norms of additive signals on the original content

are bounded by $\sqrt{D_E}$ and $\sqrt{D_A}$, respectively in the fingerprinted copy and attacked copy . From fingerprint embedder's point of view codewords degrade the multimedia quality hence distortion constraint on the embedder is given by

$$\|\mathbf{q}_j\|^2 \leq ND_E, \quad j \in \{1, 2, \ldots, M\} \tag{2.6}$$

Here note that this constraint is valid for deterministic fingerprint codewords. For fingerprints that are generated in a stochastic fashion, e.g. Gaussian fingerprints, expected value of the L_2 norm is an appropriate qualifier as given below

$$E\left[\|\mathbf{q}_j\|^2\right] \leq ND_E, \quad j \in \{1, 2, \ldots, M\} \tag{2.7}$$

On the other hand, the attack channel degrades the perceptual quality of the content by deciding on the collusion clique size and adding noise. Since the noise introduced by the attack channel is a stochastic process, distortion constraint on the attack channel can be quantified by expected value of the L_2 norm as follows

$$E\left[\|\frac{1}{K}\sum_{j=1}^{M}\mathbf{q}_j b_j + \mathbf{n}\|^2\right] \leq ND_A, \quad \text{s.t. } \omega(b) = K \tag{2.8}$$

Exact expressions of distortion constraints for specific codebooks are going to be derived in the following sections.

2.4. Focused Detector

Focused detector, also named as correlation detector, is the conventional detector structure for fingerprint decoding. It bases on the correlation between the colluded copy and fingerprint codes of users. Specifically, it focuses on user k and computes the decision statistic v_k by computing the correlation between the kth fingerprint and

received signal. Output of the correlation detector for user k is given by

$$\begin{aligned} v_k &= \mathbf{q}_k^T \mathbf{y} \\ &= \frac{1}{K} \sum_{j \in SC} \mathbf{q}_k^T \mathbf{q}_j + \mathbf{q}_k^T \mathbf{n} \end{aligned} \tag{2.9}$$

Decision on user k is made by thresholding the correlator output v_k with respect to the threshold τ

$$\left\{ \begin{array}{ll} \text{user k is in SC} & \text{if} \quad v_k \geq \tau \\ \text{user k is not in SC} & \text{if} \quad v_k < \tau \end{array} \right\} \tag{2.10}$$

As stated before fingerprinting problem with an averaging attack channel is in effect a communication problem with a multiple-access channel. With this analogy in mind, it is also easy to see that the described decoding and decision strategy is equivalent to matched filtering used in communications [12]: Colluded copy is passed through the filter that is matched to the kth user's fingerprint code and a decision is made on kth user's binary message b_k. Hence colluder detection problem is transformed into detection of independent binary messages, b_k's, modulated by signature waveforms, $\mathbf{q}_k$'s. Output of the matched filter, i.e. the decision statistic, for user k is therefore

$$\begin{aligned} v_k &= \mathbf{q}_k^T \mathbf{y} \\ &= \frac{1}{K} \sum_{j=1}^{M} \mathbf{q}_k^T \mathbf{q}_j b_j + \mathbf{q}_k^T \mathbf{n} \\ &= \frac{1}{K} \sum_{j=1}^{M} \mathbf{q}_k^T \mathbf{q}_j b_j + n_k \end{aligned} \tag{2.11}$$

where $n_k = \mathbf{q}_k^T \mathbf{n}$ is the Gaussian noise with 0 mean and $\sigma^2 \mathbf{q}_k^T \mathbf{q}_k$ variance, i.e.

$$n_k \sim \mathcal{N}\left(0, \sigma^2 \|\mathbf{q}_k\|^2\right) \tag{2.12}$$

which follows from the fact that vector product in $\mathbf{q}_k^T \mathbf{n}$ linearly combines N independent

Gaussian random variables. The decision method for matched filtering is given by

$$\left\{ \begin{array}{lll} \hat{b}_k = 1 & \text{if} & v_k \geq \tau \\ \hat{b}_k = 0 & \text{if} & v_k < \tau \end{array} \right\} \tag{2.13}$$

Here, an important observation is that the decision statistic of user k, v_k, includes information on both its own bit and other users' bits. Dividing the summation in (2.11) into two parts we get

$$\begin{aligned} v_k &= \frac{1}{K}\mathbf{q}_k^T\mathbf{q}_k b_k + \sum_{\substack{1\leq j\leq M \\ j\neq k}} \mathbf{q}_k^T\mathbf{q}_j b_j + n_k \\ &= \frac{1}{K}\|\mathbf{q}_k\|^2 b_k + \gamma_k + n_k \end{aligned} \tag{2.14}$$

where

$$\gamma_k = \sum_{\substack{1\leq j\leq M \\ j\neq k}} \mathbf{q}_k^T\mathbf{q}_j b_j \tag{2.15}$$

In (2.14) the first term is the information on user k's own bit whereas the second term, γ_k, is the undesirable information from other colluders' bits resulting from their presence in the collusion clique. This second term is analogous to *Multiple Access Interference* (MAI) arising in a multiple-access channel as defined in wireless communications literature [12]. In wireless communications, MAI results from the simultaneous transmissions of more than one user over the same channel. It acts as an additive noise term and degrades the performance of the receiver unless codewords of users are orthogonal to each other in L_2 sense. Consequently, remembering that matched filtering is the optimum detection strategy under AWGN channel; focused detector turns out to be a suboptimum detector structure for non-orthogonal codebooks. Explicitly; outputs of filters matched to different users become correlated and v_k reveals not to be a sufficient statistic for a decision on b_k.

In order to represent the decision statistics of all users in a single expression and to see explicitly the relations between correlation detectors' outputs, and hence MAI, we rewrite the colluded signal at the detector as

$$\mathbf{y} = \frac{1}{K}\mathbf{Q}\mathbf{b} + \mathbf{n} \tag{2.16}$$

where $\mathbf{b} = [b_1 \dots b_M]^T$ is the length M vector representing the presence of all users in the clique, and $\mathbf{Q} = [\mathbf{q}_1 \dots \mathbf{q}_M]$ is the NxM matrix whose jth column is the fingerprint for the jth user. Then, output of a filter matched to user k's fingerprint is given by

$$\begin{aligned} v_k &= \mathbf{q}_k^T \mathbf{y} \\ &= \frac{1}{K}\mathbf{q}_k^T \mathbf{Q}\mathbf{b} + \mathbf{q}_k^T \mathbf{n} \end{aligned} \tag{2.17}$$

Defining $\mathbf{v} = [v_1 \dots v_M]^T$ as the length M vector representing the decision statistics of all users, outputs of the matched filters can be written as

$$\begin{aligned} \mathbf{v} &= \mathbf{Q}^T \mathbf{y} \\ &= \frac{1}{K}\mathbf{Q}^T \mathbf{Q}\mathbf{b} + \mathbf{Q}^T \mathbf{n} \end{aligned} \tag{2.18}$$

For a given $\mathbf{b}$, first and second order statistics of the vector output of the matched filter, $\mathbf{v}$, are respectively given by

$$\begin{aligned} E[\mathbf{v}|\mathbf{b}] &= E\left[\frac{1}{K}\mathbf{Q}^T \mathbf{Q}\mathbf{b} + \mathbf{Q}^T \mathbf{n}\right] \\ &= \frac{1}{K}\mathbf{Q}^T \mathbf{Q}\mathbf{b} + E\left[\mathbf{Q}^T \mathbf{n}\right] \\ &= \frac{1}{K}\mathbf{Q}^T \mathbf{Q}\mathbf{b} \end{aligned} \tag{2.19}$$

$$
\begin{aligned}
E\left[\mathbf{v}\mathbf{v}^T|\mathbf{b}\right] &= E\left[\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}+\mathbf{Q}^T\mathbf{n}\right)\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}+\mathbf{Q}^T\mathbf{n}\right)^T\right] \\
&= E\left[\frac{1}{K^2}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\mathbf{b}^T\mathbf{Q}^T\mathbf{Q}\right]+E\left[\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\mathbf{n}^T\mathbf{Q}\right] \\
&+ E\left[\frac{1}{K}\mathbf{Q}^T\mathbf{n}\mathbf{b}^T\mathbf{Q}^T\mathbf{Q}\right]+E\left[\mathbf{Q}^T\mathbf{n}\mathbf{n}^T\mathbf{Q}\right] \\
&= \frac{1}{K^2}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\mathbf{b}^T\mathbf{Q}^T\mathbf{Q}+\mathbf{Q}^TE\left[\mathbf{n}\mathbf{n}^T\right]\mathbf{Q} \qquad (2.20) \\
&= \frac{1}{K^2}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\mathbf{b}^T\mathbf{Q}^T\mathbf{Q}+\sigma^2\mathbf{Q}^T\mathbf{Q} \qquad (2.21)
\end{aligned}
$$

where equations (2.19) and (2.20) follow from $E\left[\mathbf{n}\right]=\mathbf{0}$ and equation (2.21) follows from $E\left[\mathbf{n}\mathbf{n}^T\right]=\sigma^2\mathbf{I}_N$ since $\mathbf{n}\sim\mathcal{N}\left(\sigma^2,\mathbf{I}_N\right)$. Because of the linearity of the matched filter $\mathbf{v}$ is a Gaussian random vector and its covariance matrix is

$$
\begin{aligned}
\mathbf{\Sigma}_{\mathbf{v}|\mathbf{b}} &= E\left[\mathbf{v}\mathbf{v}^T|\mathbf{b}\right]-E\left[\mathbf{v}|\mathbf{b}\right]E\left[\mathbf{v}|\mathbf{b}\right]^T \\
&= \frac{1}{K^2}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\mathbf{b}^T\mathbf{Q}^T\mathbf{Q}+\sigma^2\mathbf{Q}^T\mathbf{Q}-\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\right)\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}\right)^T \\
&= \sigma^2\mathbf{Q}^T\mathbf{Q} \qquad (2.22)
\end{aligned}
$$

Therefore output of the matched filter is a Gaussian random vector with mean $\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}$ and covariance matrix $\sigma^2\mathbf{Q}^T\mathbf{Q}$, i.e.

$$
\mathbf{v}\mid\mathbf{b}\sim\mathcal{N}\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b},\sigma^2\mathbf{Q}^T\mathbf{Q}\right) \qquad (2.23)
$$

Considering a single matched filter's output, we observe $v_j\sim\mathcal{N}\left(\frac{1}{K}\mathbf{q}_j^T\mathbf{Q}\mathbf{b},\sigma^2\mathbf{q}_j^T\mathbf{q}_j\right)$. Here note that $\mathbf{Q}^T\mathbf{Q}$ term in the preceding equations is the cross-correlation matrix for any given codebook. The matrix entry at ith row and jth column is $\mathbf{q}_i^T\mathbf{q}_j$, the correlation value between ith and jth users' fingerprints. Consequently the cross-correlation matrix of the codebook characterizes the MAI in the attack channel such that the off-diagonal elements of the cross-correlation matrix appear in γ_k and make the decision statistics of different users correlated.

3. PERFORMANCE OF FOCUSED DETECTOR FOR GENERIC CODEBOOKS

Decision strategy for the focused detector, as given in equation (2.13), depends on thresholding each user's matched filter output with respect to a given threshold τ. However, vector of decision statistics were found to be $\mathbf{v} \sim \mathcal{N}\left(\frac{1}{K}\mathbf{Q}^T\mathbf{Q}\mathbf{b}, \sigma^2\mathbf{Q}^T\mathbf{Q}\right)$ where $\mathbf{Q}^T\mathbf{Q}$ is not necessarily an identity matrix. In the most general case $\mathbf{v}$ vector is made up of v_j's that are correlated Gaussian random variables. As a result, decision statistic of a user contains interference from other users' fingerprints, named as MAI in the previous sections and quantified through the entries of $\mathbf{Q}^T\mathbf{Q}$. Noting that the $\mathbf{Q}^T\mathbf{Q}$ matrix is the cross-correlation matrix of a codebook it can be concluded that the codebook structure is the main factor that affects the performance of the detector.

At this point it is worth mentioning that codebooks with non-zero cross-correlations between their fingerprints, hence resulting correlated decision statistics, will eventually cause cumbersome error probability calculations. However we obtain the probability of error expression for the most general case without confining ourselves to a specific codebook structure. Consequently the sought-after error probability expression is a generic one and holds true with no dependency on the codebook. Probability of error expressions and other performance measures for specific codebooks are going to be investigated separately as special cases of the generic structure.

Without putting any restrictions on the fingerprint codebook, we start with the following assumptions for our correlation detector structure and error probability calculations:

1. Codebook is known at the detector side.
2. The number of the colluders in the collusion clique is known at the detector and it is given by K.
3. Each user decides on whether to join the collusion clique or not independently, i.e. b_j's are independent such that $\forall j,\ 1 \leq j \leq M$ and $b_j \in \{0, 1\},\ Pr[b_j = 1] = \theta_j$.

Here note that these are mild assumptions for our setup and they are frequently taken into account in the literature [1].

3.1. Bit Error Probability

Bit error probability of user k is the probability of falsely deciding on the presence of user k in the collusion clique. It can be also named as bit error probability of communications theory since it is the error probability for detecting a binary variable. Defining the focused error probability of user k as P_e^k, it can be formulated as follows

$$\begin{aligned}
P_e^k &= Pr\left[\hat{b}_k \neq b_k \mid \omega(\mathbf{b}) = K\right] \\
&= Pr\left[\hat{b}_k = 1 \mid b_k = 0, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \\
&+ Pr\left[\hat{b}_k = 1 \mid b_k = 1, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \\
&= Pr\left[v_k \geq \tau \mid b_k = 0, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \\
&+ Pr\left[v_k \leq \tau \mid b_k = 1, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \qquad (3.1)
\end{aligned}$$

Recalling the statistical characteristics of matched filter outputs, given in (2.23), and considering the assumptions discussed in the previous section exact expression for P_e^k is found to be

$$\begin{aligned}
P_e^k = \frac{1}{d_k(\theta)} \Bigg\{ & (1-\theta_k) \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. \omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right) a_k(\mathbf{b}) \right] \\
& + \theta_k \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. \omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right) a_k(\mathbf{b}) \right] \Bigg\} \qquad (3.2)
\end{aligned}$$

where

$$a_k(\mathbf{b}) = \prod_{\substack{1\le i\le M\\ i\neq k}} \theta_i^{b_i}\,(1-\theta_i)^{1-b_i}$$

$$d_k(\theta) = (1-\theta_k)c_{0,k} + \theta_k c_{1,k}$$

$$c_{0,k} = \sum_{\substack{\mathbf{b}\in\{0,1\}^M\\ s.t.\,\omega(\mathbf{b})=K, b_k=0}} a_k(\mathbf{b})$$

$$c_{1,k} = \sum_{\substack{\mathbf{b}\in\{0,1\}^M\\ s.t.\,\omega(\mathbf{b})=K, b_k=1}} a_k(\mathbf{b})$$

For a detailed calculation of P_e^k refer to Appendix A.

Again note that P_e^k given in (3.2) is valid for any codebook structure because we did not make any assumptions on fingerprints and their cross-correlation values. In the following section we present bounds on bit error probability P_e^k and also obtain simplified expressions by employing some mild constraints on the codebook.

3.2. Bounds on Bit Error Probability

Using the definition of $a_k(\mathbf{b})$ given in equation (A.17), we clearly have the following bounds on it:

1. The case where $\omega(\mathbf{b}) = K$ and $b_k = 0$:

$$\left(\min_i \theta_i\right)^K \left[1 - \max_{i\neq k}\theta_i\right]^{M-K-1} \le a_k(\mathbf{b}) \le \left(\max_i \theta_i\right)^K \left[1 - \min_{i\neq k}\theta_i\right]^{M-K-1} \tag{3.3}$$

   for $\mathbf{b} \in \{0,1\}^M$.

2. The case where $\omega(\mathbf{b}) = K$ and $b_k = 1$:

$$\left(\min_{i\neq k} \theta_i\right)^{K-1} \left[1 - \max_i \theta_i\right]^{M-K} \le a_k(\mathbf{b}) \le \left(\max_{i\neq k} \theta_i\right)^{K-1} \left[1 - \min_i \theta_i\right]^{M-K} \tag{3.4}$$

for $\mathbf{b} \in \{0,1\}^M$.

Then the upper and lower bounds for P_e^k are given by

1. Upper bound on P_e^k: Using the right hand sides of (3.3) and (3.4) in (3.2)

$$P_e^k \leq \frac{1}{d_k(\theta)} \left\{ (1-\theta_k) \left(\max_i \theta_i \right)^K \left[1 - \min_{i \neq k} \theta_i \right]^{M-K-1} \left[\sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 0}} Q\left(\frac{\tau - \gamma_k}{\sigma \|\mathbf{q}_k\|} \right) \right] \right.$$
$$\left. + (\theta_k) \left(\max_{i \neq k} \theta_i \right)^{K-1} \left[1 - \min_i \theta_i \right]^{M-K} \left[\sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau - \gamma_k}{\sigma \|\mathbf{q}_k\|} \right) \right] \right\} \tag{3.5}$$

2. Lower bound on P_e^k: Using the left hand sides of (3.3) and (3.4) in (3.2)

$$P_e^k \geq \frac{1}{d_k(\theta)} \left\{ (1-\theta_k) \left(\min_i \theta_i \right)^K \left[1 - \max_{i \neq k} \theta_i \right]^{M-K-1} \left[\sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 0}} Q\left(\frac{\tau - \gamma_k}{\sigma \|\mathbf{q}_k\|} \right) \right] \right.$$
$$\left. + (\theta_k) \left(\min_{i \neq k} \theta_i \right)^{K-1} \left[1 - \max_i \theta_i \right]^{M-K} \left[\sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau - \gamma_k}{\sigma \|\mathbf{q}_k\|} \right) \right] \right\} \tag{3.6}$$

A special case is where all users join equiprobably to the collusion clique which means $\{b_k\}$ are i.i.d. random variables i.e. $\forall k, \theta_k = \theta$. In this case following are observed

1.

$$d_k(\theta) = C(M,K) \theta^K (1-\theta)^{M-K} \tag{3.7}$$

2.

$$(1-\theta_k)\left(\max_i \theta_i\right)^K \left[1-\min_{i\neq k}\theta_i\right]^{M-K-1} = (1-\theta_k)\left(\min_i \theta_i\right)^K \left[1-\max_{i\neq k}\theta_i\right]^{M-K-1} = \theta^K (1-\theta)^{M-K} \tag{3.8}$$

3.

$$(\theta_k)\left(\max_{i\neq k} \theta_i\right)^{K-1} \left[1-\min_i \theta_i\right]^{M-K} = (\theta_k)\left(\min_{i\neq k} \theta_i\right)^{K-1} \left[1-\max_i \theta_i\right]^{M-K} = \theta^K (1-\theta)^{M-K} \tag{3.9}$$

Hence the upper bound (3.5) is equal to the lower bound (3.6). Then using (3.7), (3.8) and (3.9) in (3.5) or (3.6) we obtain the exact expression of P_e^k for equiprobable colluders as

$$P_e^k = \frac{1}{C(M,K)} \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right) + \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right) \right] \tag{3.10}$$

Here some remarks are worth to mention. First of all probability of error expression doesn't depend on the choice of θ. Furthermore prior probabilities of being in the collusion clique or not are equal for all users and they are given by $Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] = \frac{M-K}{M}$ and $Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] = \frac{K}{M}$. It is also important to emphasize that (3.10) is an exact expression for focused error probability. Here, the case of equiprobable colluders is a fair assumption and is widely considered to be the frequent situation in the literature. Therefore we are going to proceed further with this assumption and find upper and lower bounds on P_e^k.

A brief observation on (3.10) reveals that γ_k's are the only variables that depend on $\mathbf{b}$'s; hence on the summations. Remembering that γ_k's are functions of correlations

between fingerprint codewords we define the following

$$\alpha \stackrel{\triangle}{=} \max_{i \neq j} \langle \mathbf{q}_i, \mathbf{q}_j \rangle = \max_{i \neq j} \mathbf{q}_i^T \mathbf{q}_j \tag{3.11}$$

$$\beta \stackrel{\triangle}{=} \min_{i \neq j} \langle \mathbf{q}_i, \mathbf{q}_j \rangle = \min_{i \neq j} \mathbf{q}_i^T \mathbf{q}_j \tag{3.12}$$

as the maximum and minimum values of correlations. Using (3.11) and (3.12) in the definition of γ_k, (2.15), we get

$$\frac{1}{K} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} \beta b_j \leq \gamma_k \leq \frac{1}{K} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} \alpha b_j \tag{3.13}$$

$$\frac{\beta}{K} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j \leq \gamma_k \leq \frac{\alpha}{K} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j \tag{3.14}$$

Considering the conditions on $\mathbf{b}$ we clearly have the following conditional bounds on γ_k:

1. The case where $\omega(\mathbf{b}) = K$ and $b_k = 0$:

$$\frac{\beta}{K} \leq \gamma_k \leq \frac{\alpha}{K} \tag{3.15}$$

2. The case where $\omega(\mathbf{b}) = K$ and $b_k = 1$:

$$\frac{K-1}{K} \beta \leq \gamma_k \leq \frac{K-1}{K} \alpha \tag{3.16}$$

(3.15) follows from the fact that K of b_j's are 1 for $\omega(\mathbf{b}) = K$ and $b_k = 0$ and (3.16) follows from the fact that $K-1$ of b_j's are 1 for $\omega(\mathbf{b}) = K$ and $b_k = 1$. Then the upper and lower bounds for P_e^k of equiprobable colluders case, (3.10), are given by:

1. Upper bound on P_e^k: In (3.10), using the right hand side of (3.15) in the first

term and left hand side of (3.16) in the second term gives

$$P_e^k \leq \frac{1}{C(M,K)} \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\alpha}{\sigma\|\mathbf{q}_k\|}\right) + \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\beta}{\sigma\|\mathbf{q}_k\|}\right) \right] \tag{3.17}$$

$$= \frac{C(M-1,K)}{C(M,K)} Q\left(\frac{\tau-\alpha}{\sigma\|\mathbf{q}_k\|}\right) + \frac{C(M-1,K-1)}{C(M,K)} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\beta}{\sigma\|\mathbf{q}_k\|}\right) \tag{3.18}$$

$$= \frac{M-K}{M} Q\left(\frac{\tau-\alpha}{\sigma\|\mathbf{q}_k\|}\right) + \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\beta}{\sigma\|\mathbf{q}_k\|}\right) \tag{3.19}$$

2. Lower bound on P_e^k: In (3.10), using the left hand side of (3.15) in the first term and right hand side of (3.16) in the second term gives

$$P_e^k \geq \frac{1}{C(M,K)} \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\beta}{\sigma\|\mathbf{q}_k\|}\right) + \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\alpha}{\sigma\|\mathbf{q}_k\|}\right) \right] \tag{3.20}$$

$$= \frac{C(M-1,K)}{C(M,K)} Q\left(\frac{\tau-\beta}{\sigma\|\mathbf{q}_k\|}\right) + \frac{C(M-1,K-1)}{C(M,K)} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\alpha}{\sigma\|\mathbf{q}_k\|}\right) \tag{3.21}$$

$$= \frac{M-K}{M} Q\left(\frac{\tau-\beta}{\sigma\|\mathbf{q}_k\|}\right) + \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\frac{K-1}{K}\alpha}{\sigma\|\mathbf{q}_k\|}\right) \tag{3.22}$$

Note that (3.18) and (3.21) follow from the fact that according to the conditions on the summations; number of terms in the first summations of (3.17) and (3.20) is $C(M-1,K)$, number of terms in the second summations of (3.17) and (3.20) is $C(M-1,K-1)$.

At this point we have not started to investigate the exact expressions or bounds of bit error probability in terms of convexity, optimality or asymptotic analysis. However expressions similar to the upper and lower bounds, given in (3.19) and (3.22) respectively, are going to arise frequently in this work for different codebooks, so we propose

the following theorem which defines a structure for bit error probability and presents statements on its convexity.

Theorem 3.2.1. *Define* $f(\tau)$ *as*

$$f(\tau) \triangleq aQ\left(\frac{\tau-\alpha}{\sigma_f}\right) + bQ\left(\frac{\beta-\tau}{\sigma_f}\right) \tag{3.23}$$

where $a, b, \sigma_f \in (0,\infty)$, $\alpha, \beta \in \mathbb{R}$ *and* $\alpha \neq \beta$. $f(\tau)$ *has an extremum point at*

$$\tau^* = \frac{\sigma_f^2}{\beta-\alpha}\log\left(\frac{a}{b}\right) + \frac{\alpha+\beta}{2} \tag{3.24}$$

Furthermore τ^* *is a global minimizer if* $\beta > \alpha$ *and a global maximizer if* $\beta < \alpha$.

Proof. See Appendix B □

Note that applying the results of Theorem 3.2.1 on upper and lower bounds gives expressions that are conditioned on α and β. On the other hand these variables, which are codebook dependent, are going to be defined and evaluated for specific codebooks and we are going to be able to present meaningful results for each codebook. Therefore we are leaving our analysis on bit error probability to subsequent sections.

Up to now we have focused on the probability of error on deciding a specific user's presence in the collusion clique, i.e. bit error probability for user k. Exact expression is found in equation (3.2) and employing the equiprobable colluders assumption, i.e. for $1 \leq j \leq M$, $b_j \in \{0,1\}$ are i.i.d. with $Pr[b_j = 1] = \theta$, a greatly simplified expression is obtained in (3.10). It is important to note that in (3.10) there are no assumptions on fingerprint codebook structure and these results hold for any fingerprint scheme. After this point we started putting constraints on the codebook by defining the maximum and minimum values of cross-correlations between fingerprints; respectively α in (3.11) and β in (3.12). By using these definitions we derived the upper and lower bounds on the probability of bit error as in equations (3.19) and (3.22).

From now on we concentrate on specific codebook structures under equiprobable colluders assumption. The general results found in this section will be basis for our derivations for different codebooks. Generally speaking, exact expression in equation (3.10) will guide us for stochastic codebooks. On the other hand bounds in (3.19) and (3.22) will be useful for deterministic codebook structures, because we can make clear distinctions between different codebooks by means of cross-correlation values of codebooks. For instance, orthogonal fingerprints impose zero cross-correlation whereas simplex fingerprints have non-zero but equal cross-correlation values between codewords.

In the subsequent sections we consider both deterministic and stochastic fingerprint classes that have been widely used in the literature. Namely, we consider orthogonal, simplex and Gaussian fingerprints in Chapters 4, 5, 6 respectively. For each codebook structure we derive bit error probability, optimum threshold for minimum probability of error and collusion resistance. We also make asymptotic analysis on signal length and noise power of the attack channel. Moreover we utilize appropriate distortion constraints on codebooks and attack channel during our calculations.

4. ORTHOGONAL FINGERPRINTS

Orthogonal fingerprints, as the name suggests, have zero cross-correlation values between codewords, i.e. for $1 \leq i, j \leq M$ and $i \neq j$, $\mathbf{q}_i^T \mathbf{q}_j = 0$. In this case, from equation (2.14), output of the matched filter focused on user k is given by

$$v_k = \frac{1}{K} \|\mathbf{q}_k\|^2 b_k + n_k \tag{4.1}$$

Furthermore, noting that the cross-correlation matrix of orthogonal codewords is simply a diagonal matrix whose jth diagonal element is $\rho_{jj} = \mathbf{q}_j^T \mathbf{q}_j$ and denoting it by $\mathbf{\Sigma}$; it easily follows from equation (2.23) that the output vector for matched filters has the distribution

$$\mathbf{v} \sim \mathcal{N}\left(\frac{1}{K}\mathbf{\Sigma}\mathbf{b}, \sigma^2 \mathbf{\Sigma}\right) \tag{4.2}$$

Inspecting (4.1) and (4.2) brings out two observations. First, no multiple access interference appears in the output of the detector matched to user k. Second, outputs of the correlation detector are uncorrelated Gaussian random variables which are also independent. Therefore the only undesired signal at matched filter outputs is the independent Gaussian noise process. In the light of these observations single user matched filter turns out to be the optimal detector for detecting fingerprints under averaging attack with Gaussian noise. From another point of view zero cross-correlation between fingerprints of different users implies that γ_k's, as defined in (2.15), are equal to zero. Remembering that γ_k represents the MAI in user k's decision statistic it can be easily seen that MAI disappears from matched filters' outputs. With γ_k equal to

zero exact expression for kth user's bit error probability in equation (3.10) reduces to

$$P_e^{O,k} = \frac{1}{C(M,K)} \left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau}{\sigma\|\mathbf{q}_k\|}\right) + \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau}{\sigma\|\mathbf{q}_k\|}\right) \right]$$
$$= \frac{M-K}{M} Q\left(\frac{\tau}{\sigma\|\mathbf{q}_k\|}\right) + \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau}{\sigma\|\mathbf{q}_k\|}\right) \tag{4.3}$$

Note that above expression can also be validated by remembering that the maximum and minimum values for cross-correlations between different fingerprints, α and β respectively, are zero and in that case upper and lower bounds in (3.19) and (3.22) become equal to each other.

4.1. Optimum Threshold and Minimum Probability of Error

With the exact probability of error expression in hand we can define the optimum value of the threshold τ that gives the minimum probability of error for focused detector as

$$\tau_{opt}^{O} \stackrel{\triangle}{=} \underset{\tau}{\operatorname{argmin}}\, P_e^{O,k} \tag{4.4}$$

With the above definition optimum value for τ is given by

$$\tau_{opt}^{O} = \frac{\|\mathbf{q}_k\|^2}{2K} + K\sigma^2 \log\left(\frac{M-K}{K}\right) \tag{4.5}$$

whose derivation is given in Appendix D.1. As a result, using (4.5) in (4.3) the minimum probability of error is found as

$$P_{e,min}^{O,k} = \frac{M-K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{2K\sigma} + \frac{K\sigma}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right)$$
$$+ \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{2K\sigma} - \frac{K\sigma}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right) \tag{4.6}$$

Note the first term in optimum threshold as given in (4.5) comes from the codeword of user k which is the desired information at matched filter output. On the other hand, the second term is a correction factor related to the noise variance, number of colluders, and prior probabilities of user k's presence in the collusion clique.

4.2. Collusion Resistance

For the derivation of collusion resistance and asymptotic analysis we can impose the distortion constraints on the embedder and attacker to our results with equality. For orthogonal fingerprints distortion constraint on the embedder, (2.6), is given by

$$\|\mathbf{q}_k\|^2 \leq ND_E \tag{4.7}$$

and the distortion constraint on the attackers, from equation (2.8) is given by

$$\sigma^2 \leq D_A - \frac{D_E}{K} \tag{4.8}$$

Employing above constraints in (4.6) with equality we get

$$\begin{aligned} P_{e,min}^{O} = \frac{M-K}{M} Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A - \frac{D_E}{K}}} + \frac{K\sqrt{D_A - \frac{D_E}{K}}}{\sqrt{ND_E}} \log\left(\frac{M-K}{K}\right)\right) \\ + \frac{K}{M} Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A - \frac{D_E}{K}}} - \frac{K\sqrt{D_A - \frac{D_E}{K}}}{\sqrt{ND_E}} \log\left(\frac{M-K}{K}\right)\right) \end{aligned} \tag{4.9}$$

Note that the minimum probability of error doesn't depend on k, index of a specific user. Because embedder constraint with equality implies that fingerprint embedder generates codewords with the highest possible L_2 norm which is given by (4.7). Consequently all codewords have the same L_2 norm getting rid of the dependency on user index k. From another point of view equal L_2 norms for fingerprints is a simple and realistic assumption because after generating a codebook norms can be normalized to a desired value and equal norms for users implies equal expectation for users' possibility

of joining a collusion clique.

Collusion resistance is defined as the maximum number of colluders that can be identified given that the probability of error is below a specified value, i.e.

$$K^O \triangleq \underset{K}{\operatorname{argmax}} P_e \qquad s.t. \quad P_e \leq \epsilon \tag{4.10}$$

However, it is an infeasible approach to try to obtain K^O using $P^O_{e,min}$ given in equation (4.9) because of transcendental functions of K arising in calculations. Consequently we first approximate (4.9) with a much simpler equation. Assuming $\sqrt{N} \gg K, M$ minimum probability of error becomes

$$P^O_{e,min} \approx Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A - \frac{D_E}{K}}}\right) \tag{4.11}$$

which is monotonic increasing in K. Using the approximate value for $P^O_{e,min}$ in the definition of collusion resistance, (4.10), we obtain the collusion resistance for orthogonal fingerprints as

$$K^O = \frac{D_E + \sqrt{D_E^2 + \frac{ND_AD_E}{(Q^{-1}(\epsilon))^2}}}{2D_A} \tag{4.12}$$

whose derivation is given in Appendix E.1. The collusion resistance expression obtained is monotonic increasing in D_E and monotonic decreasing in D_A: The maximum number of colluders that can be caught increases by embedding fingerprints with greater L_2 norms, and by restricting the attackers to lower noise power. Moreover, as the signal and fingerprint length increases collusion resistance increases which also makes sense.

4.3. Error Exponent and Asymptotic Analysis

As noise becomes vanishingly small, i.e. $\sigma \to 0$, second terms in Q-functions of equation (4.6) approach to zero such that minimum probability of error becomes

$$P_{e,min}^{O} \approx Q\left(\frac{\|\mathbf{q}_k\|}{2K\sigma}\right) \tag{4.13}$$

Also noting that Q-function monotonically decreases with its argument we have

$$\lim_{\sigma \to 0} P_{e,min}^{O} = 0 \tag{4.14}$$

which implies that in the absence of noise error-free detection is possible for orthogonal fingerprints. In fact, remembering that there is no MAI but just AWGN interference at matched filter outputs, L_2 norm of the matched codeword is the only remaining signal in the absence of noise. In that case optimum threshold becomes $\tau_{opt}^{O} = \frac{\|\mathbf{q}_k\|^2}{2K}$ which just depends on the L_2 norm of the codeword and number of colluders. Note that τ_{opt}^{O}'s dependency on prior probabilities also vanishes.

In the case that signal length becomes large, i.e. as $N \to \infty$, we get

$$\lim_{N \to \infty} P_{e,min}^{O} = 0 \tag{4.15}$$

applying the same reasoning as we used in small noise case. Explanation of this result lies in the fact that as the signal length increases number of samples for matched filter outputs increases and decision making on more samples becomes more accurate.

Another meaningful situation is where total number of users and number of colluding users approach to infinity while the ratio between the two is preserved. Explicitly we are investigating

$$\lim_{K,M \to \infty} P_{e,min}^{O} \quad s.t.\ \pi_1 = \frac{K}{M} \text{ and } \pi_0 = \frac{M-K}{M} \tag{4.16}$$

where π_0 and π_1 are in fact prior probabilities of being in the collusion clique or not, respectively. Noticing that $\frac{M-K}{K}$ is greater than zero when $\pi_1 = \frac{K}{M} \leq \frac{1}{2}$, from (4.9)

$$\lim_{K,M\to\infty} P_{e,min}^{O} = \begin{cases} \frac{K}{M} & \text{if } \pi_1 \leq \frac{1}{2} \\ \frac{M-K}{M} & \text{if } \pi_1 \geq \frac{1}{2} \end{cases} \tag{4.17}$$

which means as the total number of users and number of colluders increase prior probabilities π_0 and π_1, which depend on the knowledge on the number of users, become much more reliable and hence detection solely depends on prior knowledge. In other words information from colluders' fingerprints almost vanishes if the total number of users and number of colluders become sufficiently large. Inspecting equation (4.5) we observe that τ_{opt}^{O} approaches to infinity if $\frac{K}{M} \leq \frac{1}{2}$ and in that case detector always identifies users as innocent, i.e. $\forall k\ \hat{b}_k = 0$, and probability of error becomes $\frac{K}{M}$.

Upto now we have investigated the asymptotic behavior of probability of error with respect to noise power, number of users and signal length. However we have not taken the rate of variation in bit error probability into consideration. For instance; as signal length becomes larger error probability decreases eventually to zero but we don't know how fast it decreases. In order to examine the rate of variation we define error exponent w.r.t. signal length N as follows

$$e^{O} \triangleq \lim_{N\to\infty} -\frac{1}{N} \log\left(P_{e,min}^{O}\right) \tag{4.18}$$

As signal length N increases arguments of Q-functions in (4.9) also increase. Using the upper bound for Q-function, $Q\left(x\right) \leq \frac{1}{2}\exp\left(-\frac{x^2}{2}\right)$, we can approximate the probability of error in (4.9) as

$$P_{e,min}^{O} \approx \frac{1}{2}\exp\left(-\frac{ND_E}{8K^2\left(D_A - \frac{D_E}{K}\right)}\right) \tag{4.19}$$

Applying the definition of error exponent we have

$$e^O = \frac{D_E}{8K^2\left(D_A - \frac{D_E}{K}\right)} \tag{4.20}$$

Notice that error exponent is monotonic increasing in D_E and monotonic decreasing in D_A and K.

5. SIMPLEX FINGERPRINTS

Simplex fingerprints as proposed in [22] have maximal resistance to Gaussian averaging attack channels. They maximize the minimum distance between all possible collusion sets and non-collusion sets involving a specific user and it is shown that minimum distance primarily governs error probability [22]. In this section exact expression for probability of bit error and asymptotic analysis along with the collusion resistance are given.

Without loss of generality setting the L_2 norms of all codewords equal to ρ, i.e. $\forall k,\ \|\mathbf{q}_k\|^2 = \rho$, simplex fingerprints have the following relation between its codewords

$$\mathbf{q}_i^T \mathbf{q}_j = \begin{cases} -\frac{\rho}{M-1} & \text{if } i \neq j \\ \rho & \text{if } i = j \end{cases} \tag{5.1}$$

which means fingerprints are equally correlated. In this case, recalling equation (2.14) and the assumption that number of colluders K is known at the detector, we can write the output of the matched filter focused on user k as follows

$$v_k = \frac{\rho}{K} b_k - \frac{\rho}{K(M-1)} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j + n_k \tag{5.2}$$

It is obvious that output of the kth matched filter contains interference from other users' presence in the collusion clique, thus MAI term γ_k in (2.14) doesn't vanish as it does for orthogonal codes. In (5.2) γ_k is quantified conditionally on b_k as follows

$$\begin{aligned} \gamma_k &= -\frac{\rho}{K(M-1)} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j \\ &= \begin{cases} -\frac{\rho}{M-1} & \text{if } b_k = 0 \\ -\frac{\rho(K-1)}{K(M-1)} & \text{if } b_k = 1 \end{cases} \end{aligned}$$

It is important to note that γ_k doesn't depend on the collusion set, i.e. $\mathbf{b}$, hence interference can be mitigated at the detector outputs with the knowledge on the number of colluders.

Probability of bit error for simplex codebooks can be derived either from the exact expression in (3.10) by noting that γ_k's are independent of $\mathbf{b}$ vectors or from the bounds in (3.19) and (3.22) by noting that maximum and minimum values for cross-correlations between codewords are equal. In both ways we obtain the following expression for bit error probability

$$P_e^S = \frac{M-K}{M} Q\left(\frac{(M-1)\tau+\rho}{\sigma(M-1)\sqrt{\rho}}\right) + \frac{K}{M} Q\left(\frac{(M-K)\rho - K(M-1)\tau}{\sigma K(M-1)\sqrt{\rho}}\right) \tag{5.3}$$

Notice that bit error probability of simplex codes is equal for all users.

5.1. Optimum Threshold and Minimum Probability of Error

Optimum threshold that minimizes the bit error probability in (5.3) is defined as

$$\tau_{opt}^S \stackrel{\triangle}{=} \underset{\tau}{\operatorname{argmin}}\, P_e^S \tag{5.4}$$

and its solution is given by

$$\tau_{opt}^S = \frac{\rho(M-2K)}{2K(M-1)} + \frac{\sigma^2 K(M-1)}{M} \log\left(\frac{M-K}{K}\right) \tag{5.5}$$

Refer to Appendix D.2 for derivation of τ_{opt}^S. Minimum probability of error is found by putting τ_{opt}^S in 5.3 and is given by

$$\begin{aligned} P_{e,min}^S = {} & \frac{M-K}{M} Q\left(\frac{M\sqrt{\rho}}{2\sigma K(M-1)} + \frac{\sigma K(M-1)}{M\sqrt{\rho}} \log\left(\frac{M-K}{K}\right)\right) \\ & + \frac{K}{M} Q\left(\frac{M\sqrt{\rho}}{2\sigma K(M-1)} - \frac{\sigma K(M-1)}{M\sqrt{\rho}} \log\left(\frac{M-K}{K}\right)\right) \end{aligned} \tag{5.6}$$

5.2. Collusion Resistance

Now we can impose the distortion constraints on embedder and attacker with equality into our results for asymptotic analysis and collusion resistance calculations. Distortion constraint on the fingerprint embedder is the same as orthogonal codes

$$\rho \leq N D_E \tag{5.7}$$

However attacker constraint changes a bit such that

$$\sigma^2 \leq D_A - D_E \frac{M-K}{K(M-1)} \tag{5.8}$$

Using these distortion constraints in the equation (5.6) with equality we get

$$\begin{aligned} P_{e,min}^S = \frac{M-K}{M} Q \Bigg(& \frac{M\sqrt{ND_E}}{2\sqrt{K(M-1)}\sqrt{D_A K(M-1) - D_E(M-K)}} \\ & + \frac{\sqrt{K(M-1)}\sqrt{D_A K(M-1) - D_E(M-K)}}{M\sqrt{ND_E}} \log\left(\frac{M-K}{K}\right) \Bigg) \\ + \frac{K}{M} Q \Bigg(& \frac{M\sqrt{ND_E}}{2\sqrt{K(M-1)}\sqrt{D_A K(M-1) - D_E(M-K)}} \\ & - \frac{\sqrt{K(M-1)}\sqrt{D_A K(M-1) - D_E(M-K)}}{M\sqrt{ND_E}} \log\left(\frac{M-K}{K}\right) \Bigg) \end{aligned} \tag{5.9}$$

Assuming $\sqrt{N} \gg K, M$ minimum bit error probability, given in (5.9), can be approximated as

$$P_{e,min}^S \approx Q\left(\frac{M\sqrt{ND_E}}{2\sqrt{K(M-1)}\sqrt{D_A K(M-1) - D_E(M-K)}} \right) \tag{5.10}$$

which is monotonic increasing in K. Using above approximation and the definition in

(4.10) collusion resistance is found as

$$K^S = \frac{D_E + \sqrt{D_E^2 + \frac{ND_E(MD_A - D_A + D_E)}{(M-1)(Q^{-1}(\epsilon))^2}}}{\frac{2(MD_A - D_A + D_E)}{M}} \tag{5.11}$$

whose detailed derivation is given in Appendix E.2.

5.3. Error Exponent and Asymptotic Analysis

As noise variance decreases second terms of Q-functions vanish and we can approximate the bit error probability as

$$P_{e,min}^S \approx Q\left(\frac{M\sqrt{\rho}}{2\sigma K(M-1)}\right) \tag{5.12}$$

which approaches to zero as its argument increases with decreasing σ, s.t.

$$\lim_{\sigma \to 0} P_{e,min}^S = 0 \tag{5.13}$$

Therefore error-free detection is possible with simplex fingerprints in the absence of additive noise, just like orthogonal fingerprints. As it is mentioned before MAI interference from simplex fingerprints can be removed from detector outputs.

Following the same analysis we made for orthogonal fingerprints we also have

$$\lim_{N \to \infty} P_{e,min}^S = 0 \tag{5.14}$$

which applies that number of samples available at the focused detector improves its performance.

Considering the case where $K, M \to \infty$ while $\pi_1 = \frac{K}{M}$ is a constant we observe

that

$$\lim_{K,M\to\infty} P_{e,min}^{S} = \begin{cases} \frac{K}{M} & \text{if } \pi_1 \leq \frac{1}{2} \\ \frac{M-K}{M} & \text{if } \pi_1 \geq \frac{1}{2} \end{cases} \tag{5.15}$$

which means sufficiently large number of users wipes out the information coming from the codewords of colluders and the detector bases its decisions on the prior probabilities of users on being in the collusion set or not.

In order to evaluate the error exponent for simplex fingerprints we need to consider $N \to \infty$ for which bit error probability in (5.9) can be approximated by utilizing the bound $Q(x) \leq \frac{1}{2}\exp\left(-\frac{x^2}{2}\right)$ as

$$P_{e,min}^{S} \approx \frac{1}{2}\exp\left(-\frac{NM^2D_E}{8K(M-1)(D_AK(M-1)-D_E(M-K))}\right) \tag{5.16}$$

Then from the definition of error exponent given in (4.18) we have

$$\begin{aligned} e^S &= \lim_{N\to\infty} -\frac{1}{N}\log\left(\frac{1}{2}\exp\left(-\frac{NM^2D_E}{8K(M-1)(D_AK(M-1)-D_E(M-K))}\right)\right) \\ &= \frac{M^2D_E}{8K(M-1)(D_AK(M-1)-D_E(M-K))} \end{aligned} \tag{5.17}$$

which is monotonic increasing in D_E and monotonic decreasing in D_A and K.

6. GAUSSIAN FINGERPRINTS

In a communication setup with AWGN channel Gaussian distributed codewords make up the capacity achieving codebook structure. High capacity in a communication channel intuitively causes expectations for high collusion resistance. In fact, optimality of Gaussian fingerprints in terms of collusion resistance is shown in [7]. However exact bit error probability for Gaussian fingerprints is not studied in the literature. In this section bit error probability expression for Gaussian fingerprints is derived and asymptotic analysis is presented.

Samples of a Gaussian fingerprint are drawn from a stochastic process and stochastic codebook generation implies that cross-correlation values between codewords are not deterministic anymore. Especially interference term γ_k given in (2.15) is a random variable whose distribution should be identified before beginning performance analysis. Since the detector focuses on a specific user k and outputs a decision statistic based on the correlation between the kth user's fingerprint and the colluded copy we derive our results conditioned on the fingerprint of user k, $\mathbf{q}_k$. In this section any calculation focused on user k is conditioned on $\mathbf{q}_k$ if it is not stated otherwise.

In this work we are dealing with unbounded Gaussian fingerprints. Codeword for user k, $\mathbf{q}_k$, is generated as a sequence of i.i.d. random samples such that jth element of $\mathbf{q}_k$ is a Gaussian with 0 mean and σ_g^2 variance, i.e.

$$\mathbf{q}_k \sim \mathcal{N}\left(0, \sigma_g^2 \mathbf{I}_N\right) \tag{6.1}$$

For convenience we rewrite the expression given in (2.14) for matched filter output, v_k:

$$v_k = \frac{1}{K}\|\mathbf{q}_k\|^2 b_k + \gamma_k + n_k \tag{6.2}$$

First observation on γ_k is that, conditioned on $\mathbf{q}_k$, γ_k is a Gaussian random variable

because it is a linear combination of $N \times \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j$ i.i.d. Gaussian random variables. Therefore its distribution can be characterized by identifying its mean and variance. Expected value of γ_k is

$$E\left[\gamma_k \mid \mathbf{b}\right] = \frac{1}{K} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} \mathbf{q}_k^T E\left[\mathbf{q}_j\right] b_j = 0 \tag{6.3}$$

Variance of γ_k is given by

$$E\left[\gamma_k^2 \mid \mathbf{b}\right] = \frac{1}{K^2} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} \sum_{\substack{1 \leq i \leq M \\ i \neq k}} \mathbf{q}_k^T E\left[\mathbf{q}_j \mathbf{q}_i^T\right] \mathbf{q}_k b_j b_i \tag{6.4}$$

$$= \frac{1}{K^2} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} \mathbf{q}_k^T E\left[\mathbf{q}_j \mathbf{q}_j^T\right] \mathbf{q}_k b_j \tag{6.5}$$

$$= \frac{\sigma_g^2 \|\mathbf{q}_k\|^2}{K^2} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j \tag{6.6}$$

where (6.5) comes from the fact that $E\left[\mathbf{q}_j \mathbf{q}_i^T\right] = \mathbf{0}$ for $i \neq j$ and (6.6) follows by using the distribution given in (6.1). Hence we have

$$\gamma_{k|\mathbf{b}} \sim \mathcal{N}\left(0, \frac{\sigma_g^2 \|\mathbf{q}_k\|^2}{K^2} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j\right) \tag{6.7}$$

Moreover, n_k is also shown to be Gaussian in (2.12) with mean 0 and variance $\sigma^2 \|\mathbf{q}_k\|^2$. Knowing that γ_k and n_k are independent Gaussian random variables we can conclude that their sum is also Gaussian and v_k has the following Gaussian distribution:

$$v_{k|\mathbf{b}} \sim \mathcal{N}\left(\frac{\|\mathbf{q}_k\|^2}{K} b_k, \|\mathbf{q}_k\|^2 \left(\sigma^2 + \frac{\sigma_g^2}{K^2} \sum_{\substack{1 \leq j \leq M \\ j \neq k}} b_j\right)\right) \tag{6.8}$$

Again, we want to emphasize that the preceding result, distribution of v_k, is conditioned on $\mathbf{q}_k$ and all the remaining derivations in this section assume the same if it is not stated

otherwise.

We also investigate the sufficiency of v_k for decision on b_k, at the same time optimality of the matched filter, for Gaussian fingerprints. For this purpose we evaluate the covariance of v_k and v_l, σ_{kl} as follows

$$\begin{aligned}
\sigma_{kl|\mathbf{b}} &= E\left[v_k v_l \mid \mathbf{b}\right] - E\left[v_k \mid \mathbf{b}\right] E\left[v_l \mid \mathbf{b}\right] \\
&= E\left[\gamma_k \gamma_l \mid \mathbf{b}\right] + E\left[n_k n_l \mid \mathbf{b}\right] && (6.9) \\
&= \frac{1}{K^2} \sum_{\substack{1\le j\le M \\ j\neq k}} \sum_{\substack{1\le i\le M \\ i\neq l}} \mathbf{q}_k^T E\left[\mathbf{q}_j \mathbf{q}_i^T\right] \mathbf{q}_l^T b_j b_i + \sigma^2 \mathbf{q}_k^T \mathbf{q}_l && (6.10) \\
&= \frac{\sigma_g^2 \mathbf{q}_k^T \mathbf{q}_l}{K^2} \sum_{\substack{1\le j\le M \\ j\neq k,\ j\neq l}} b_j + \sigma^2 \mathbf{q}_k^T \mathbf{q}_l && (6.11)
\end{aligned}$$

Non-zero covariance between matched filters' outputs means that making decision for a specific user k by just observing the filter output v_k is suboptimal.

6.1. Optimum Threshold and Minimum Probability of Error

Recall that bit error probability expression in (3.10) is valid for any given codebook and it is a function of all possible collusion sets of size K. Dependency on the collusion sets is through γ_k whose definition is given in (2.15). For orthogonal and simplex codebooks γ_k's were quantified independent of the collusion clique and as a result we obtained error probability expressions free of collusion clique structure. On the other hand, for the case of stochastic codebooks the interference term is also stochastic and it can be characterized by its probability distribution. Therefore we can get rid of the dependency on the collusion clique by evaluating the expected value of bit error probability with respect to γ_k.

Taking the expected value of bit error probability expression given in (3.10) with

respect to γ_k we have

$$P_e^{G,k} \triangleq E_{\gamma_k}\left[P_e^k\right] = \frac{1}{C(M,K)}\left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} E\left[Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\right] + \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} E\left[Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma}-\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\right]\right] \tag{6.12}$$

Noting that γ_k is Gaussian; we need the expression for the expectation of Q-function with respect to a Gaussian random variable which is given in the following proposition:

Claim 6.1.1. *Let $a, b \in \mathbb{R}$ and $x \sim \mathcal{N}(0,\sigma^2)$. Expected value of $Q(ax+b)$ with respect to x is given by*

$$E_x\left[Q\left(ax+b\right)\right] = Q\left(\frac{b}{\sqrt{1+a^2\sigma^2}}\right) \tag{6.13}$$

Proof. See Appendix C. □

In (6.12) the distribution of γ_k for the first summation where $b_k = 0$ is given by

$$\gamma_{k|b_k=0,\omega(\mathbf{b})=K} \sim \mathcal{N}\left(0, \frac{\sigma_g^2\|\mathbf{q}_k\|^2}{K}\right) \tag{6.14}$$

which follows from the distribution conditioned on $\mathbf{b}$ given in (6.7). Applying Claim 6.1.1 we have

$$E\left[Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\right] = Q\left(\frac{\tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2+\frac{\sigma_g^2}{K}}}\right) \tag{6.15}$$

Next, in (6.12) the distribution of γ_k for the second summation where $b_k = 1$ is

given by

$$\gamma_{k|b_k=1,\omega(\mathbf{b})=K} \sim \mathcal{N}\left(0, \frac{\sigma_g^2\|\mathbf{q}_k\|^2(K-1)}{K^2}\right) \tag{6.16}$$

Again using Claim 6.1.1 we get

$$E\left[Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\right] = Q\left(\frac{\frac{\|\mathbf{q}_k\|^2}{K} - \tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{(K-1)\sigma_g^2}{K^2}}}\right) \tag{6.17}$$

Now using (6.15) and (6.17) in (6.12) we obtain the bit error probability expression for user k conditioned on codeword $\mathbf{q}_k$ for Gaussian fingerprints as follows:

$$P_e^{G,k} = \frac{M-K}{M}Q\left(\frac{\tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{\sigma_g^2}{K}}}\right) + \frac{K}{M}Q\left(\frac{\frac{\|\mathbf{q}_k\|^2}{K} - \tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{(K-1)\sigma_g^2}{K^2}}}\right) \tag{6.18}$$

An approximate value for the optimum threshold minimizing the bit error probability expression of (6.18) is given by

$$\tau_{opt}^G = \frac{\|\mathbf{q}_k\|^2}{2K} + \left(K\sigma^2 + \sigma_g^2\right)\log\left(\frac{M-K}{K}\right) \tag{6.19}$$

where it is assumed that $K \gg 1$. For detailed derivation refer to Appendix D.3. With the optimum threshold given in (6.19) an approximate value, $\tilde{P}_{e,min}^G$, for minimum probability of error can be written as follows

$$\begin{aligned}\tilde{P}_{e,min}^G = &\frac{M-K}{M}Q\left(\frac{\|\mathbf{q}_k\|}{2\sqrt{K^2\sigma^2 + K\sigma_g^2}} + \frac{\sqrt{K^2\sigma^2 + K\sigma_g^2}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right) \\ &+ \frac{K}{M}Q\left(\frac{\|\mathbf{q}_k\|}{2\sqrt{K^2\sigma^2 + K\sigma_g^2}} - \frac{\sqrt{K^2\sigma^2 + K\sigma_g^2}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right)\end{aligned} \tag{6.20}$$

Remark: As mentioned before all the derivations in this section are condition on $\mathbf{q}_k$, kth user's codeword. However we can find generalized expressions that are independent of users' codewords. In order to find such an expression we should calculate the

expected value of bit error probability with respect to the distribution of the norm of the kth user's codeword, $\|\mathbf{q}_k\|$. First we define $\rho_g \triangleq \frac{\|\mathbf{q}_k\|}{\sigma_g^2}$ whose distribution is a chi-square distribution with N degrees of freedom which is given by

$$f_{\rho_g}(\rho_g) = \frac{1}{2^{N/2}\Gamma\left(N/2\right)} \rho_g^{N/2-1} \exp\left(-N/2\right) \tag{6.21}$$

Using $\|\mathbf{q}_k\| = \sigma_g^2 \rho_g$ in (6.18) and taking expectation with respect to ρ_g we obtain the bit error probability, which is independent of users, as follows

$$\begin{aligned} P_e^G = \frac{M-K}{M} \int_0^\infty \frac{1}{2^{N/2}\Gamma\left(N/2\right)} \rho_g^{N/2-1} \exp\left(-N/2\right) Q\left(\frac{\tau}{\sigma_g \sqrt{\sigma^2 \rho_g + \frac{\sigma_g^2 \rho_g}{K}}}\right) d\rho_g \\ + \frac{K}{M} \int_0^\infty \frac{1}{2^{N/2}\Gamma\left(N/2\right)} \rho_g^{N/2-1} \exp\left(-N/2\right) Q\left(\frac{\frac{\sigma_g^2 \rho_g}{K} - \tau}{\sigma_g^2 \sqrt{\sigma^2 \rho_g + \frac{(K-1)\sigma_g^2 \rho_g}{K^2}}}\right) d\rho_g \end{aligned} \tag{6.22}$$

However these integrals are not tractable so we are proceeding with conditioning our result on kth user's codeword $\mathbf{q}_k$.

6.2. Collusion Resistance

First we write the distortion constraints on the embedder and attacker for Gaussian fingerprints. Distortion constraint on the fingerprint embedder is given by

$$\sigma_g^2 \leq D_E \tag{6.23}$$

and attacker constraint is given by

$$\sigma^2 \leq D_A - \frac{D_E}{K} \tag{6.24}$$

Using these constraints with equality in (6.20) we get

$$\tilde{P}_{e,min}^{G} = \frac{M-K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{2K\sqrt{D_A}} + \frac{K\sqrt{D_A}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right) + \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|}{2K\sqrt{D_A}} - \frac{K\sqrt{D_A}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right) \tag{6.25}$$

Here note that an embedder constraint is obtained on the variance of the distribution from which codewords are drawn. However we should also control the value of $\|\mathbf{q}_k\|$ which is assumed to be given in all our derivations although it is stochastically generated. Therefore we impose the following constraint on $\|\mathbf{q}_k\|$

$$\|\mathbf{q}_k\|^2 \approx N D_E \tag{6.26}$$

Note that the above constraint is given approximately since we can not have a strict restraint on a stochastically generated codeword. Using the constraint (6.26) in (6.25) we have

$$\tilde{P}_{e,min}^{G} \approx \frac{M-K}{M} Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A}} + \frac{K\sqrt{D_A}}{\sqrt{ND_E}}\log\left(\frac{M-K}{K}\right)\right) + \frac{K}{M} Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A}} - \frac{K\sqrt{D_A}}{\sqrt{ND_E}}\log\left(\frac{M-K}{K}\right)\right) \tag{6.27}$$

which can be simplified more by assuming $\sqrt{N} \gg K$ as follows

$$\tilde{P}_{e,min}^{G} \approx Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A}}\right) \tag{6.28}$$

Using this approximate expression, which is monotonic increasing in K, collusion resistance is found to be

$$K^G = \frac{\sqrt{ND_E}}{2Q^{-1}(\epsilon)\sqrt{D_A}} \tag{6.29}$$

whose derivation is given in Appendix E.3. Here notice that K^G is monotonic increasing in D_E and ϵ and monotonic decreasing in D_A.

6.3. Error Exponent and Asymptotic Analysis

When noise variance becomes sufficiently small we have

$$\lim_{\sigma\to 0}\tilde{P}_{e,min}^{G}=\frac{M-K}{M}Q\left(\frac{\|\mathbf{q}_k\|}{2\sqrt{K\sigma_g^2}}+\frac{\sqrt{K\sigma_g^2}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right)+\frac{K}{M}Q\left(\frac{\|\mathbf{q}_k\|}{2\sqrt{K\sigma_g^2}}-\frac{\sqrt{K\sigma_g^2}}{\|\mathbf{q}_k\|}\log\left(\frac{M-K}{K}\right)\right) \tag{6.30}$$

Consequently as noise becomes vanishingly small bit error probability for Gaussian fingerprints doesn't approach zero contrary to orthogonal and simplex fingerprints. Expression given in (6.30) is the error floor faced by Gaussian codebooks.

In the large signal length case we have

$$\lim_{N\to\infty}\tilde{P}_{e,min}^{G}=0 \tag{6.31}$$

which follows from evaluating (6.27) for large N.

Now we examine the case where $K, M\to\infty$ while $\pi_1=\frac{K}{M}$ is a constant. Using $\tilde{P}_{e,min}^{G}$ given in 6.27 we observe that

$$\lim_{K,M\to\infty}P_{e,min}^{G}=\begin{cases}\frac{K}{M} & \text{if } \pi_1\leq\frac{1}{2}\\ \frac{M-K}{M} & \text{if } \pi_1\geq\frac{1}{2}\end{cases} \tag{6.32}$$

which means for sufficiently large total number of users and large number of colluders prior probabilities of users on being in the collusion set dominate the information coming from the codewords of colluders.

As N goes to infinity bit error probability given in (6.27) can be approximated

by

$$\tilde{P}^{G}_{e,min} \approx \frac{1}{2} \exp\left(-\frac{ND_E}{8K^2 D_A}\right) \tag{6.33}$$

Therefore error exponent for Gaussian fingerprints is given by

$$e^G = \lim_{N\to\infty} -\frac{1}{N} \log\left(\tilde{P}^{G}_{e,min}\right) = \frac{D_E}{8K^2 D_A} \tag{6.34}$$

which is monotonic increasing in D_E and monotonic decreasing in D_A and K.

7. NUMERICAL RESULTS AND DISCUSSION

Inspecting the approximate minimum bit error probability expressions of orthogonal, simplex and Gaussian fingerprints given in (4.19), (5.16), (6.33) respectively, we see that

$$P_{e,min}^{S} < P_{e,min}^{O} < P_{e,min}^{G} \tag{7.1}$$

for large values of signal length N or small noise power σ. The same trend can also be observed in Figure 7.1-7.5 which plot the exact bit error probabilities for orthogonal and simplex fingerprints and approximate expression for Gaussian codes. Simplex codes exhibit lower error probability than orthogonal codes because of the negative cross-correlations between simplex codes. Moreover, in Figure 7.1-7.3 differences between codewords in terms of error probability is small and it diminishes more as K increases. As K approaches to total number of users M probability of error of all codebooks converges to the same value. Figure 7.1-7.3 also show the variation of bit error probability with respect to signal length N and distortion constraints D_E, D_A as discussed in the previous sections.

In Figure 7.4 and 7.5 bit error probability is plotted with respect to *watermark to noise ratio* (WNR) which is given by

$$WNR = \frac{\|\mathbf{q}_k\|^2}{\|n\|^2} \tag{7.2}$$

Considering the distortion constraints satisfied with equality WNR becomes

$$WNR = \frac{D_E}{\sigma^2} \tag{7.3}$$

for all three codebooks. Here note that Gaussian fingerprints satisfy (7.3) approximately because of their stochastic nature. In Figure 7.4 we see that minimum probability of bit error decreases and difference between Gaussian fingerprints and the other

two fingerprints increases with increasing WNR. Furthermore the noise floor for Gaussian codebooks quantified in (6.30) can be observed in Figure 7.5.

Collusion resistance expressions given in (4.12), (5.11) and (6.29), for orthogonal, simplex and Gaussian fingerprints respectively, reveals that

$$K^S > K^O > K^G \tag{7.4}$$

Theoric collusion resistance expressions and exact numerical results are also plotted in Figure 7.6. Note that collusion resistance for all three codebooks are almost identical. It is obvious from collusion resistance expressions that as N increases collusion resistance of the three codebooks gets much closer. In Figure 7.7 collusion resistance with respect to total number of users is plotted where probability of error is 0.1. It is observed that as M increases collusion resistance also increases one-to-one with M upto some point and continuues increasing after that point with a decreased rate.

Error exponents for the three codebooks are plotted in Figure 7.8 with respect to number of colluders. From the figures

$$e^S > e^O > e^G \tag{7.5}$$

and as the number of colluder increases the gap between Gaussian fingerprints and the other two diminishes. As mentioned before rrror exponent indicates the rate of decay for error probability and the decay rate for the three codebooks can be observed in Figure 7.9.

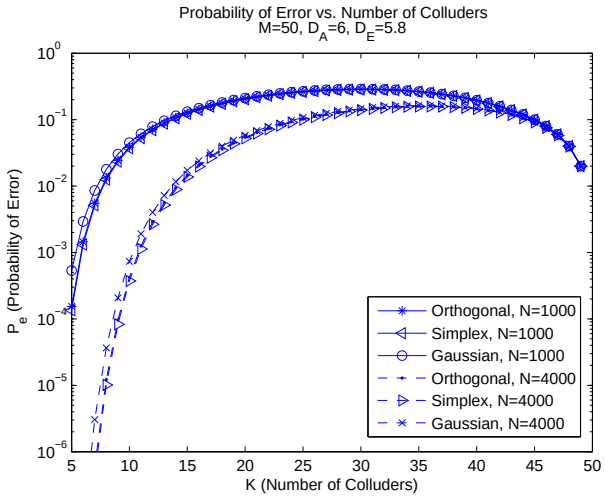

Figure 7.1. Probability of error vs. number of colluders for various values of signal length N.

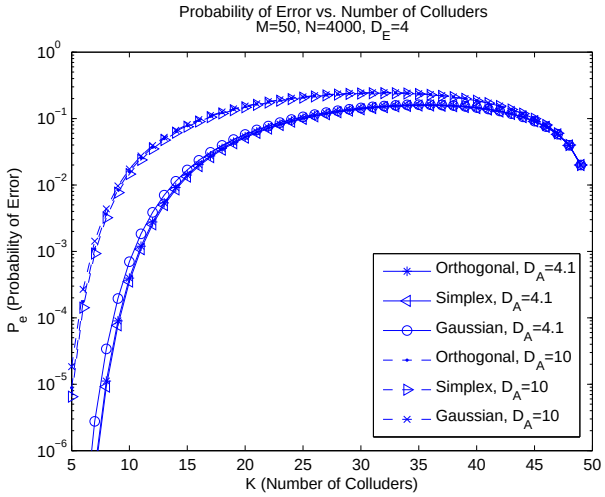

Figure 7.2. Probability of error vs. number of colluders for various values of attacker distortion constraint D_A.

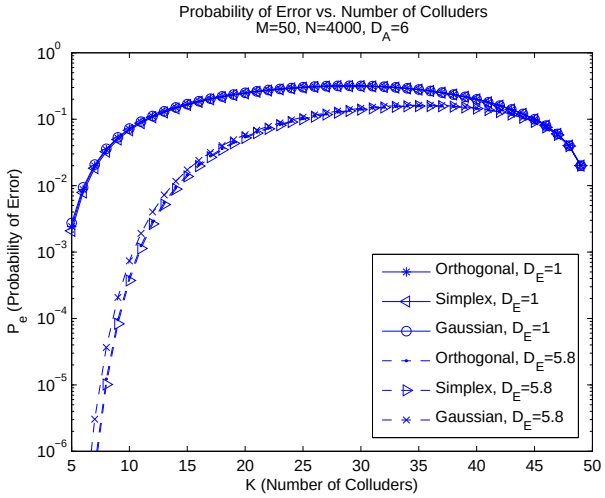

Figure 7.3. Probability of error vs. number of colluders for various values of embedder distortion constraint D_E.

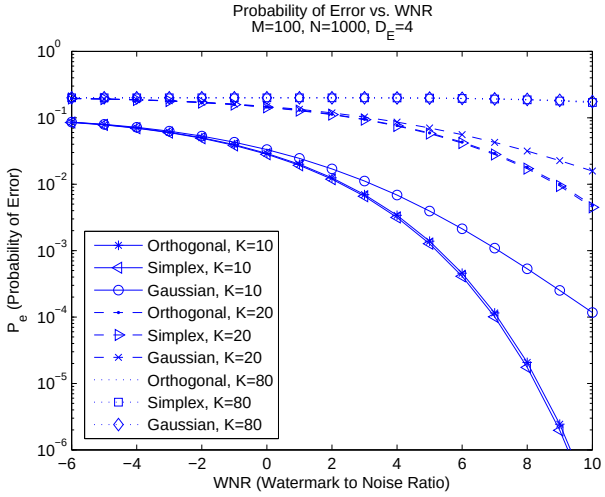

Figure 7.4. Probability of error vs. watermark to noise ratio for various values of colluder number K.

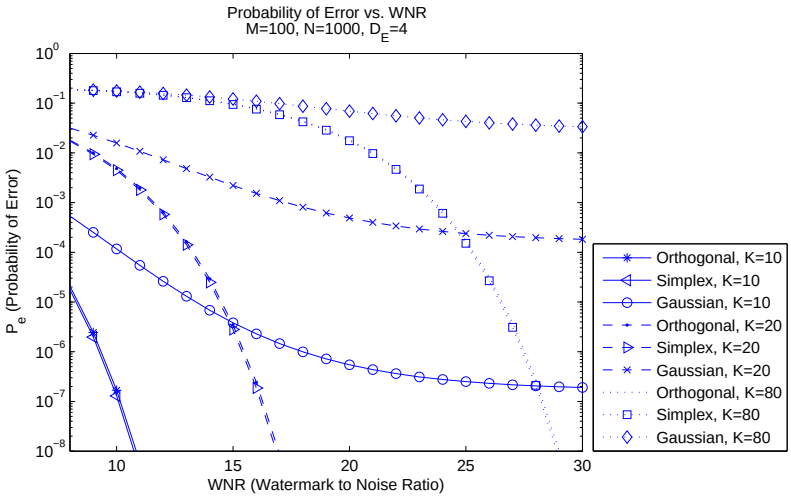

Figure 7.5. Probability of error vs. high watermark to noise ratio for various values of colluder number K.

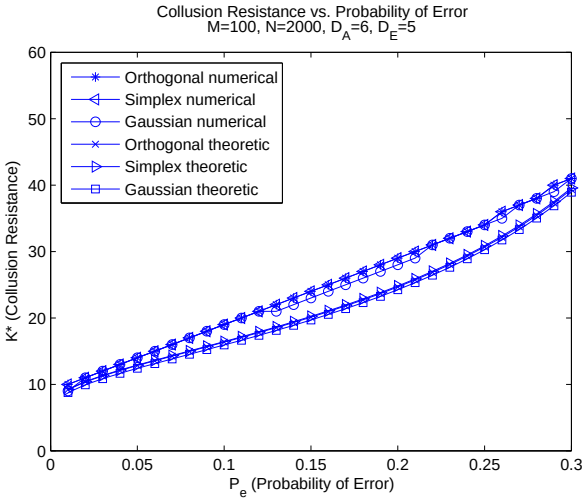

Figure 7.6. Collusion resistance vs. probability of error.

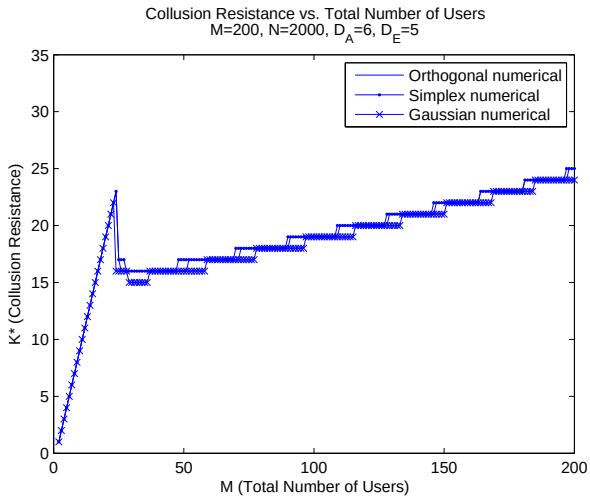

Figure 7.7. Collusion resistance vs. total number of users.

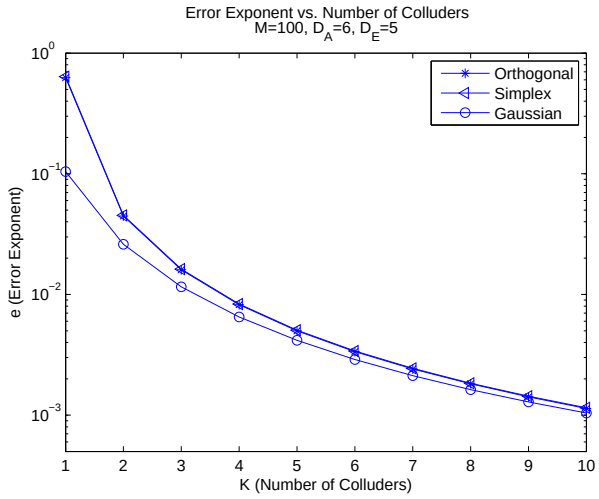

Figure 7.8. Error exponent vs. number of colluders.

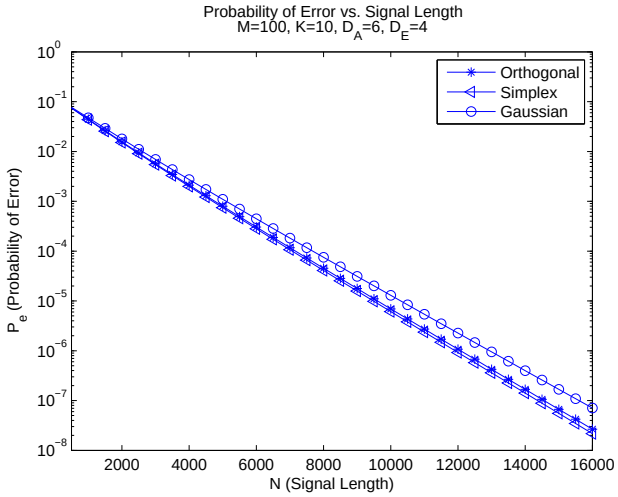

Figure 7.9. Probability of error vs. signal length.

8. CONCLUSIONS

In this work a communication theoretic modeling and performance analysis of the fingerprinting problem is presented from the detector point of view. As the problem setup additive fingerprint embedding under Gaussian averaging attack and correlation detector is considered. It is assumed that colluders join the collusion clique independent of each other and the number of colluders is available at the detector.

Embodying the presence of a user in the collusion by a binary random variable is the first step through modeling fingerprinting as a communication system. Each user practically sends his/her message bit modulated by the fingerprint code. Transmitted signals are passed through an AWGN channel and a superposed waveform is seen at the receiver. Here the communication channel is a multiple-access channel as seen from the receiver side and it actually corresponds to linear averaging collusion attack. Furthermore focused detector is the analogue of the well known matched filter which is the optimum receiver for single-user AWGN channel. It is shown that decision statistics from matched filter are correlated random variables unless the fingerprint codes are orthogonal to each other and the correlation results from multiple-access interference. MAI, which degrades the matched filter performance by rendering it suboptimal, is also explicitly quantified for specific codebooks.

With the motivation of focused detection and decision method at the receiver side, bit error probability is employed as the basic performance measure and collusion resistance derivations along with the asymptotic analysis are presented. A generic bit error probability expression is obtained which is valid for all additive codebooks; bit error probabilities of orthogonal, simplex and Gaussian fingerprints are derived from this generic result. For these codebooks minimum achievable bit error probability is found and its asymptotic behavior is investigated with respect to signal length, number of users and noise power. The concept of error exponents is utilized and the rate of change for bit error probability at asymptotes is examined.

It is obvious that work on fingerprint detectors can be broadened further by designing improved receivers and analyzing their performances. Communications literature which is a pretty mature field recommends high-performance receivers especially for multiple-access channels. For instance, optimum and suboptimum multi-user receivers which are dramatically superior to matched filter in terms of performance are proposed in [26].

APPENDIX A: DERIVATION OF BIT ERROR PROBABILITY FOR GENERIC CODEBOOKS

Putting the expression for v_k from equation (2.11) into equation (3.1) we get

$$\begin{aligned}
P_e^k &= Pr\left[\frac{1}{K}\sum_{j=1}^{M}\mathbf{q}_k^T\mathbf{q}_j b_j + n_k \geq \tau \mid b_k = 0, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \\
&+ Pr\left[\frac{1}{K}\sum_{j=1}^{M}\mathbf{q}_k^T\mathbf{q}_j b_j + n_k \leq \tau \mid b_k = 1, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \\
&= Pr\left[n_k \geq \tau - \frac{1}{K}\sum_{\substack{1\leq j\leq M \\ j\neq k}}\mathbf{q}_k^T\mathbf{q}_j b_j \mid b_k = 0, \omega(\mathbf{b}) = K\right] \\
&\times Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \\
&+ Pr\left[n_k \leq \tau - \frac{1}{K}\|\mathbf{q}_k\|^2 - \frac{1}{K}\sum_{\substack{1\leq j\leq M \\ j\neq k}}\mathbf{q}_k^T\mathbf{q}_j b_j \mid b_k = 1, \omega(\mathbf{b}) = K\right] \\
&\times Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \qquad \text{(A.1)}
\end{aligned}$$

where the last equation follows from the fact that conditions on the probabilities force $\mathbf{q}_k^T\mathbf{q}_j b_k = 0$ for $j = k$, $b_k = 0$ and $\mathbf{q}_k^T\mathbf{q}_j b_k = \|\mathbf{q}_k\|^2$ for $j = k$, $b_k = 1$. Using the definition of γ_k from (2.15) equation (A.1) becomes

$$\begin{aligned}
P_e^k &= Pr\left[n_k \geq \tau - \gamma_k \mid b_k = 0, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \\
&+ Pr\left[n_k \leq \tau - \frac{1}{K}\|\mathbf{q}_k\|^2 - \gamma_k \mid b_k = 1, \omega(\mathbf{b}) = K\right] Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \qquad \text{(A.2)}
\end{aligned}$$

conditioning P_e^k on all possible message vectors, i.e. $\mathbf{b}$'s,

$$P_e^k = \Bigg[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Pr\left[n_k \geq \tau - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 0\right] Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 0\right] \Bigg] Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right]$$
$$+ \Bigg[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Pr\left[n_k \geq \tau - \frac{1}{K}\|\mathbf{q}_k\|^2 - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 1\right] Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 1\right] \Bigg] Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \tag{A.3}$$

In equation (A.3) the following terms are going to be calculated separately

$$Pr\left[n_k \geq \tau - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 0\right] \tag{A.4}$$
$$Pr\left[n_k \geq \tau - \frac{1}{K}\|\mathbf{q}_k\|^2 - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 1\right] \tag{A.5}$$
$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 0\right] \tag{A.6}$$
$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 1\right] \tag{A.7}$$
$$Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] \tag{A.8}$$
$$Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] \tag{A.9}$$

Since $n_k \sim \mathcal{N}\left(0, \sigma^2\|\mathbf{q}_k\|^2\right)$ it is straightforward for equations (A.4) and (A.5) to

write

$$Pr\left[n_k \geq \tau - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 0\right] = Q\left(\frac{\tau - \gamma_k}{\sigma\|\mathbf{q}_k\|}\right) \tag{A.10}$$

$$Pr\left[n_k \geq \tau - \frac{1}{K}\|\mathbf{q}_k\|^2 - \gamma_k \mid \mathbf{b}, \omega(\mathbf{b}) = K, b_k = 1\right] = Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma} - \frac{\tau - \gamma_k}{\sigma\|\mathbf{q}_k\|}\right) \tag{A.11}$$

Using Bayes rule for equation (A.6) we have

$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 0\right] = \frac{Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 0\right] Pr\left[\mathbf{b} \mid b_k = 0\right]}{Pr\left[\omega(\mathbf{b}) = K \mid b_k = 0\right]} \tag{A.12}$$

Note that, here

$$Pr\left[\mathbf{b} \mid b_k = 0\right] = \prod_{\substack{1 \leq i \leq M \\ i \neq k}} \theta_i^{b_i} \left(1 - \theta_i\right)^{1 - b_i} \tag{A.13}$$

$$Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 0\right] = \begin{cases} 1 & \text{if } \omega(\mathbf{b}) = K \text{ where } b_k = 0 \\ 0 & \text{else} \end{cases} \tag{A.14}$$

$$\begin{aligned} Pr\left[\omega(\mathbf{b}) = K \mid b_k = 0\right] &= \sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. b_k = 0}} Pr\left[\omega(\mathbf{b}) = K, \mathbf{b} \mid b_k = 0\right] \\ &= \sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. b_k = 0}} Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 0\right] Pr\left[\mathbf{b} \mid b_k = 0\right] \\ &= \sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. b_k = 0}} Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 0\right] \left(\prod_{\substack{1 \leq i \leq M \\ i \neq k}} \theta_i^{b_i} \left(1 - \theta_i\right)^{1 - b_i} \right) \end{aligned} \tag{A.15}$$

$$= \sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 0}} \left(\prod_{\substack{1 \leq i \leq M \\ i \neq k}} \theta_i^{b_i} \left(1 - \theta_i\right)^{1 - b_i} \right) \tag{A.16}$$

where (A.15) follows from using (A.13), (A.16) follows from using (A.14). Next we

define

$$a_k(\mathbf{b}) = \prod_{\substack{1 \le i \le M \\ i \neq k}} \theta_i^{b_i} \left(1 - \theta_i\right)^{1 - b_i} \tag{A.17}$$

and

$$c_{0,k} = \sum_{\substack{\mathbf{b} \in \{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 0}} a_k(\mathbf{b}) \tag{A.18}$$

Using these definitions, (A.13) and (A.16) can be rewritten as

$$Pr\left[\mathbf{b} \mid b_k = 0\right] = a_k(\mathbf{b}) \tag{A.19}$$

and

$$Pr\left[\omega(\mathbf{b}) = K \mid b_k = 0\right] = c_{0,k} \tag{A.20}$$

respectively. Using (A.14), (A.19) and (A.20) in (A.12), we get

$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 0\right] = \frac{a_k(\mathbf{b})}{c_{0,k}} \tag{A.21}$$

for all $k \in \{1, 2, \ldots, M\}$.

Proceeding with (A.7) and applying Bayes rule

$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 1\right] = \frac{Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 1\right] Pr\left[\mathbf{b} \mid b_k = 1\right]}{Pr\left[\omega(\mathbf{b}) = K \mid b_k = 1\right]} \tag{A.22}$$

Note that, here

$$Pr\left[\mathbf{b} \mid b_k = 0\right] = \prod_{\substack{1 \le i \le M \\ i \neq k}} \theta_i^{b_i} \left(1 - \theta_i\right)^{1 - b_i} = a_k(\mathbf{b}) \tag{A.23}$$

where (A.23) follows from using (A.17). Furthermore

$$Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 1\right] = \begin{cases} 1 & \text{if } \omega(\mathbf{b}) = K \text{ where } b_k = 1 \\ 0 & \text{else} \end{cases} \tag{A.24}$$

Then a straightforward analysis reveals that

$$\begin{aligned} Pr\left[\omega(\mathbf{b}) = K \mid b_k = 1\right] &= \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. b_k = 1}} Pr\left[\omega(\mathbf{b}) = K, \mathbf{b} \mid b_k = 1\right] \\ &= \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. b_k = 1}} Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 1\right] Pr\left[\mathbf{b} \mid b_k = 1\right] \\ &= \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. b_k = 1}} Pr\left[\omega(\mathbf{b}) = K \mid \mathbf{b}, b_k = 1\right] a_k(\mathbf{b}) \qquad \text{(A.25)} \\ &= \sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t. \omega(\mathbf{b}) = K, b_k = 1}} a_k(\mathbf{b}) \qquad \text{(A.26)} \\ &= c_{1,k} \qquad \text{(A.27)} \end{aligned}$$

where (A.25) follows from using (A.23), (A.26) follows from using (A.24). Next, using (A.23), (A.24) and (A.27) in (A.22), we get

$$Pr\left[\mathbf{b} \mid \omega(\mathbf{b}) = K, b_k = 1\right] = \frac{a_k(\mathbf{b})}{c_{1,k}} \tag{A.28}$$

for all $k \in \{1, 2, \ldots, M\}$.

Applying Bayes rule to equation (A.8) we have

$$Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] = \frac{Pr\left[\omega(\mathbf{b}) = K \mid b_k = 0\right] Pr\left[b_k = 0\right]}{Pr\left[\omega(\mathbf{b}) = K\right]} \tag{A.29}$$

Now, note that,

$$\begin{aligned} Pr\left[\omega(\mathbf{b}) = K\right] &= Pr\left[\omega(\mathbf{b}) = K \mid b_k = 0\right].Pr\left[b_k = 0\right] + Pr\left[\omega(\mathbf{b}) = K \mid b_k = 1\right].Pr\left[b_k = 1\right] \\ &= c_{0,k}(1-\theta_k) + c_{1,k}\theta_k \end{aligned} \tag{A.30}$$

where (A.30) follows from using (A.18), (A.27) and recalling the fact that

$$Pr\left[b_k = 1\right] = \theta_k \quad \text{and} \quad Pr\left[b_k = 0\right] = 1 - \theta_k \tag{A.31}$$

Next, using (A.18), (A.30) and (A.31) in (A.29), we get

$$Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] = \frac{(1-\theta_k)c_{0,k}}{(1-\theta_k)c_{0,k} + \theta_k c_{1,k}} \tag{A.32}$$

Proceeding with (A.9) and applying Bayes rule, we have

$$\begin{aligned} Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] &= \frac{Pr\left[\omega(\mathbf{b}) = K \mid b_k = 1\right] Pr\left[b_k = 1\right]}{Pr\left[\omega(\mathbf{b}) = K\right]} \\ &= \frac{\theta_k c_{1,k}}{(1-\theta_k)c_{0,k} + \theta_k c_{1,k}} \end{aligned} \tag{A.33}$$

where (A.33) follows from (A.27), (A.30) and (A.31).

Furthermore, upon defining

$$d_k(\theta) = Pr\left[\omega(\mathbf{b}) = K\right] = (1-\theta_k)c_{0,k} + \theta_k c_{1,k} \tag{A.34}$$

equations (A.32) and (A.33) can be rewritten as

$$Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right] = (1-\theta_k)\frac{c_{0,k}}{d_k(\theta)} \tag{A.35}$$

$$Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right] = \theta_k \frac{c_{1,k}}{d_k(\theta)} \tag{A.36}$$

Here note that $Pr\left[b_k = 0 \mid \omega(\mathbf{b}) = K\right]$ and $Pr\left[b_k = 1 \mid \omega(\mathbf{b}) = K\right]$ are the prior prob-

abilities of user k's presence in the collusion clique given that the number of colluders is known at the detector side.

Finally, using (A.10), (A.11), (A.21), (A.28), (A.35) and (A.36) in (A.3), we obtain

$$\begin{aligned} P_e^k &= (1-\theta_k)\frac{c_{0,k}}{d_k(\theta)}\left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\frac{a_k(\mathbf{b})}{c_{0,k}}\right] \\ &\quad + \theta_k\frac{c_{1,k}}{d_k(\theta)}\left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma}-\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)\frac{a_k(\mathbf{b})}{c_{1,k}}\right] \\ &= \frac{1}{d_k(\theta)}\left\{(1-\theta_k)\left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=0}} Q\left(\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)a_k(\mathbf{b})\right]\right. \\ &\quad \left.+\theta_k\left[\sum_{\substack{\mathbf{b}\in\{0,1\}^M \\ s.t.\omega(\mathbf{b})=K, b_k=1}} Q\left(\frac{\|\mathbf{q}_k\|}{K\sigma}-\frac{\tau-\gamma_k}{\sigma\|\mathbf{q}_k\|}\right)a_k(\mathbf{b})\right]\right\} \end{aligned} \tag{A.37}$$

APPENDIX B: PROOF OF THEOREM 3.2.1

Taking the first derivative of $f(\tau)$, defined in (3.23), with respect to τ we get

$$\frac{\partial f(\tau)}{\partial \tau} = \frac{1}{\sigma_f \sqrt{2\pi}} \left[-a \exp\left(-\frac{1}{2} \left(\frac{\tau - \alpha}{\sigma_f} \right)^2 \right) + b \exp\left(-\frac{1}{2} \left(\frac{\beta - \tau}{\sigma_f} \right)^2 \right) \right] \tag{B.1}$$

Following the fact that first order derivative evaluated at extremum points equals to 0 we have

$$\begin{aligned} &\frac{\partial f(\tau)}{\partial \tau} \mid_{\tau=\tau^*} = 0 \\ &\iff a \exp\left(-\frac{1}{2} \left(\frac{\tau^* - \alpha}{\sigma_f} \right)^2 \right) = b \exp\left(-\frac{1}{2} \left(\frac{\beta - \tau^*}{\sigma_f} \right)^2 \right) \end{aligned} \tag{B.2}$$

whose solution is given by

$$\tau^* = \frac{\sigma_f^2}{\beta - \alpha} \log\left(\frac{a}{b} \right) + \frac{\alpha + \beta}{2} \tag{B.3}$$

Here note that τ^* given in above equation is the unique extremum point of $f(\tau)$. Now, second order derivative test can be used to determine whether τ^* is a minimizer or maximizer of $f(\tau)$. Second order derivative test is based on evaluating the second derivative at the extremum point of interest and examining the sign of the result. Taking the derivative of (B.1) and after some basic algebra we get the second order derivative of $f(\tau)$ as follows

$$\frac{\partial^2 f(\tau)}{\partial \tau^2} = \frac{1}{\sigma_f^3 \sqrt{2\pi}} \left[a(\tau - \alpha) \exp\left(-\frac{1}{2} \left(\frac{\tau - \alpha}{\sigma_f} \right)^2 \right) + b(\beta - \tau) \exp\left(-\frac{1}{2} \left(\frac{\beta - \tau}{\sigma_f} \right)^2 \right) \right] \tag{B.4}$$

Using (B.3) in (B.4) we have

$$\begin{aligned}\frac{\partial^2 f(\tau)}{\partial \tau^2}\,|_{\tau=\tau^*} &= \frac{1}{\sigma_f^3\sqrt{2\pi}}\left[a(x+y)\exp\left(-\frac{1}{2}(x+y)^2\right)+b(x-y)\exp\left(-\frac{1}{2}(x-y)^2\right)\right]\\ &= \frac{1}{\sigma_f^3\sqrt{2\pi}}\exp\left(-\frac{x^2+y^2}{2}\right)\left[a(x+y)\exp\left(-xy\right)+b(x-y)\exp\left(xy\right)\right]\\ &= \frac{\sqrt{ab}}{\sigma_f^4\sqrt{2\pi}}\exp\left(-\frac{x^2+y^2}{2}\right)(\beta-\alpha) \qquad \text{(B.5)}\end{aligned}$$

where

$$x \stackrel{\triangle}{=} \frac{\beta-\alpha}{2\sigma_f} \qquad \text{and} \qquad y \stackrel{\triangle}{=} \frac{\sigma_f}{\beta-\alpha}\log\left(\frac{a}{b}\right) \qquad \text{(B.6)}$$

Recalling that $a, b, \sigma_f \in (0, \infty)$ is given in the proposition of the theorem, all of the terms in (B.5) except $\beta - \alpha$ reveal to be positive. Hence second derivative evaluated at τ^* is positive if $\beta - \alpha > 0$ which means around τ^* $f(\tau)$ is convex, and vice versa. As a result τ^* is a minimizer if $\beta > \alpha$ and a maximizer if $\beta < \alpha$. However we still don't know whether τ^* is a global extremum or not. For this purpose we should inspect $f(\tau)$ at the left and right boundaries of the set containing all possible τ values. Noting that $\tau \in (-\infty, \infty)$ we have

$$\lim_{\tau\to\infty} f(\tau) = b \qquad \text{and} \qquad \lim_{\tau\to-\infty} f(\tau) = a$$

which means τ^* is the global extremum point of $f(\tau)$. To sum up; any function in the form of (3.23) has an extremum point given by (3.24) which is a minimizer if $\beta > \alpha$ and a maximizer if $\beta < \alpha$.

APPENDIX C: PROOF OF CLAIM 6.1.1

Given $a, b \in \mathbb{R}$ and $x \sim \mathcal{N}(0, \sigma^2)$ we are looking for

$$E_x\left[Q\left(ax+b\right)\right] = \frac{1}{2\pi\sigma}\int_{-\infty}^{\infty}\int_{ax+b}^{\infty}\exp\left(-\frac{u^2}{2}\right)\exp\left(-\frac{x^2}{2\sigma^2}\right)dudx \tag{C.1}$$

With a change of variables by defining $v \stackrel{\triangle}{=} -u + ax$ we obtain

$$\begin{aligned} E_x\left[Q\left(ax+b\right)\right] &= \frac{1}{2\pi\sigma}\int_{-\infty}^{\infty}\int_{b}^{\infty}\exp\left(-\frac{(v+ax)^2}{2}\right)\exp\left(-\frac{x^2}{2\sigma^2}\right)dvdx \\ &= \frac{1}{\sqrt{2\pi}\sqrt{1+a^2\sigma^2}}\int_{b}^{\infty}\exp\left(-\frac{v^2}{2}\right) \\ &\times \int_{-\infty}^{\infty}\frac{1}{\frac{\sqrt{2\pi}\sigma^2}{\sqrt{1+a^2\sigma^2}}}\exp\left(-\frac{x^2}{\frac{2\sigma^2}{1+a^2\sigma^2}}\right)\exp\left((-va)x\right)dxdv \end{aligned} \tag{C.2}$$

where second integral over x is trivially given by

$$\exp\left(\frac{a^2\sigma^2v^2}{2\left(1+a^2\sigma^2\right)}\right) \tag{C.3}$$

Using (C.3) in (C.2) and after straightforward algebra we get

$$E_x\left[Q\left(ax+b\right)\right] = \frac{1}{\sqrt{2\pi}\sqrt{1+a^2\sigma^2}}\int_{b}^{\infty}-\frac{v^2}{2\left(1+a^2\sigma^2\right)}dv \tag{C.4}$$

which is the tail probability of a Gaussian random variable $v \sim \mathcal{N}(0, 1+a^2\sigma^2)$. As a result we obviously have

$$E_x\left[Q\left(ax+b\right)\right] = Q\left(\frac{b}{\sqrt{1+a^2\sigma^2}}\right) \tag{C.5}$$

APPENDIX D: DERIVATION OF OPTIMUM THRESHOLDS

Derivations of optimum thresholds minimizing the bit error probability expressions of different codebooks follow similar plots. Specifically they are given as corollaries to Theorem 3.2.1.

D.1. Orthogonal Fingerprints

Rewriting the bit error probability expression given in (4.3) we get

$$P_e^{O,k} = \frac{M-K}{M} Q\left(\frac{\tau}{\sigma\|\mathbf{q}_k\|}\right) + \frac{K}{M} Q\left(\frac{\|\mathbf{q}_k\|^2/K - \tau}{\sigma\|\mathbf{q}_k\|}\right) \tag{D.1}$$

Defining

$$\begin{aligned} \sigma_f &= \sigma\|\mathbf{q}_k\| \\ \beta &= \|\mathbf{q}_k\|^2/K \\ \alpha &= 0 \end{aligned}$$

we have an identical expression to $f(\tau)$ given in Theorem 3.2.1 with $a = (M-K)/M$ and $b = K/M$. Noticing that $\|\mathbf{q}_k\|^2/K > 0$ optimum threshold that minimizes the bit error probability for orthogonal fingerprints is given by

$$\tau_{opt}^{O} = \frac{\|\mathbf{q}_k\|^2}{2K} + K\sigma^2 \log\left(\frac{M-K}{K}\right) \tag{D.2}$$

which is a corollary to Theorem 3.2.1

D.2. Simplex Fingerprints

If we rewrite the bit error probability expression given in (5.3) we get

$$P_e^S = \frac{M-K}{M} Q\left(\frac{\tau + \frac{\rho}{(M-1)}}{\sigma\sqrt{\rho}}\right) + \frac{K}{M} Q\left(\frac{\frac{(M-K)\rho}{K(M-1)}\rho - \tau}{\sigma\sqrt{\rho}}\right) \tag{D.3}$$

Next we define

$$\begin{aligned} \sigma_f &= \sigma\sqrt{\rho} \\ \beta &= \frac{M-K}{K(M-1)} \\ \alpha &= -\frac{\rho}{(M-1)} \end{aligned}$$

Furthermore, with $a = (M-K)/M$ and $b = K/M$, bit error probability expression for simplex codes is identical to $f(\tau)$ given in (3.23). Noting that $\frac{(M-K)\rho}{K(M-1)} > -\frac{\rho}{(M-1)}$, we obtain the optimum threshold for simplex codes from Theorem 3.2.1 as follows

$$\tau_{opt}^S = \frac{\rho(M-2K)}{2K(M-1)} + \frac{\sigma^2 K(M-1)}{M} \log\left(\frac{M-K}{K}\right) \tag{D.4}$$

D.3. Gaussian Fingerprints

For $K \gg 1$ bit error probability expression given in (6.18) can be approximated by

$$P_e^{G,k} \approx \frac{M-K}{M} Q\left(\frac{\tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{\sigma_g^2}{K}}}\right) + \frac{K}{M} Q\left(\frac{\frac{\|\mathbf{q}_k\|^2}{K} - \tau}{\|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{\sigma_g^2}{K}}}\right) \tag{D.5}$$

Defining

$$\sigma_f = \|\mathbf{q}_k\|\sqrt{\sigma^2 + \frac{\sigma_g^2}{K}}$$
$$\beta = \frac{\|\mathbf{q}_k\|^2}{K}$$
$$\alpha = 0$$

With $a = (M-K)/M$ and $b = K/M$ approximate expression in (D.5) is identical to (3.23). Also noting that $\frac{\|\mathbf{q}_k\|^2}{K} > 0$ Theorem 3.2.1 gives the optimum threshold for Gaussian fingerprints as follows

$$\tau_{opt}^{G} = \frac{\|\mathbf{q}_k\|^2}{2K} + \left(K\sigma^2 + \sigma_g^2\right)\log\left(\frac{M-K}{K}\right) \tag{D.6}$$

APPENDIX E: DERIVATION OF COLLUSION RESISTANCES

E.1. Orthogonal Fingerprints

Using the approximate expression for $P_{e,min}$ given in (4.11), we are looking for the maximum value of K satisfying the following inequality

$$\frac{\sqrt{ND_E}}{2K\sqrt{D_A - \frac{D_E}{K}}} \geq Q^{-1}(\epsilon) \tag{E.1}$$

since Q function is monotonic decreasing in its argument. Here note that if $\epsilon \geq \frac{1}{2}$, $Q^{-1}(\epsilon)$ falls in $(-\infty, 0]$. In that case, since the left hand side of the inequality (E.1) is always positive, all possible K's satisfy the $P_{e,min} \leq \epsilon$ condition and collusion resistance turns out to be M, total number of fingerprinted users. Thus proceeding with $\epsilon \leq \frac{1}{2}$ we can write

$$\begin{aligned}
&\frac{ND_E}{4K^2\left(D_A - \frac{D_E}{K}\right)} \geq \left(Q^{-1}(\epsilon)\right)^2 \\
&\iff \frac{4\left(Q^{-1}(\epsilon)\right)^2 D_A K^2 - 4\left(Q^{-1}(\epsilon)\right)^2 D_E K - ND_E}{4K^2\left(D_A - \frac{D_E}{K}\right)} \leq 0 \\
&\iff 4\left(Q^{-1}(\epsilon)\right)^2 D_A K^2 - 4\left(Q^{-1}(\epsilon)\right)^2 D_E K - ND_E \leq 0
\end{aligned} \tag{E.2}$$

which is a convex function of K and has the roots

$$K_{1,2} = \frac{D_E \pm \sqrt{D_E^2 + \frac{ND_AD_E}{\left(Q^{-1}(\epsilon)\right)^2}}}{2D_A} \tag{E.3}$$

Observing that

$$\sqrt{D_E^2 + \frac{ND_AD_E}{\left(Q^{-1}(\epsilon)\right)^2}} = D_E\sqrt{1 + \frac{ND_A}{\left(Q^{-1}(\epsilon)\right)^2 D_E}} \geq D_E \tag{E.4}$$

one of the roots turns out to be negative and the other positive. Recalling that E.2 is convex, maximum value of K satisfying E.1, i.e. collusion resistance, is found as

$$K^O = \frac{D_E + \sqrt{D_E^2 + \frac{ND_AD_E}{(Q^{-1}(\epsilon))^2}}}{2D_A} \tag{E.5}$$

E.2. Simplex Fingerprints

As stated in the definition of collusion resistance, equation (4.10), and considering the approximate value for bit error probability given in (5.10) we look for the maximum value of K satisfying

$$\begin{aligned} & Q\left(\frac{M\sqrt{ND_E}}{2\sqrt{K(M-1)}\sqrt{D_AK(M-1)-D_E(M-K)}}\right) \leq \epsilon \\ \iff & \frac{M^2ND_E}{4K(M-1)(D_AK(M-1)-D_E(M-K))} \geq \left(Q^{-1}(\epsilon)\right)^2 \end{aligned} \tag{E.6}$$

where the second equation comes from the fact that argument of Q-function in the first equation and $Q^{-1}(\epsilon)$ is always positive. Latter observation is the result of sticking to the same reasoning we made during the derivation of orthogonal codes' collusion resistance, thus considering the case where $\epsilon \leq \frac{1}{2}$. Working a bit on equation (E.6) results in the following inequality

$$\begin{aligned} & 4\left(Q^{-1}(\epsilon)\right)^2(M-1)(MD_A-D_A+D_E)K^2 \\ & -4\left(Q^{-1}(\epsilon)\right)^2M(M-1)D_EK - M^2ND_E \leq 0 \end{aligned} \tag{E.7}$$

whose left hand side is convex in K and has the roots

$$K_{1,2} = \frac{D_E \pm \sqrt{D_E^2 + \frac{ND_E(MD_A-D_A+D_E)}{(M-1)(Q^{-1}(\epsilon))^2}}}{\frac{2(MD_A-D_A+D_E)}{M}} \tag{E.8}$$

Noticing that one of the roots is negative collusion resistance is found to be

$$K^S = \frac{D_E + \sqrt{D_E^2 + \frac{ND_E(MD_A - D_A + D_E)}{(M-1)(Q^{-1}(\epsilon))^2}}}{\frac{2(MD_A - D_A + D_E)}{M}} \tag{E.9}$$

E.3. Gaussian Fingerprints

Using the approximate bit error probability expression given in (6.28) collusion resistance is defined as the maximum value of K satisfying

$$\begin{aligned} & Q\left(\frac{\sqrt{ND_E}}{2K\sqrt{D_A}}\right) \leq \epsilon \\ \iff & \frac{ND_E}{4K^2(D_A)} \geq Q^{-1}(\epsilon) \end{aligned} \tag{E.10}$$

Here we used the reasoning which we utilized for both orthogonal and simplex fingerprints in the preceding sections. Rearranging the terms of inequality (E.10) we have

$$4\left(Q^{-1}(\epsilon)\right)^2 D_A K^2 - ND_E \leq 0 \tag{E.11}$$

whose roots are given by

$$K_{1,2} = \pm \frac{\sqrt{ND_E}}{2\sqrt{D_A\left(Q^{-1}(\epsilon)\right)^2}} \tag{E.12}$$

Noting that one of the roots is negative and right hand side of the inequality (E.11) is convex collusion resistance for Gaussian fingerprints is given by

$$K^G = \frac{\sqrt{ND_E}}{2\sqrt{D_A\left(Q^{-1}(\epsilon)\right)^2}} \tag{E.13}$$

REFERENCES

1. Wu, M., W. Trappe, O. Wang, and K. J. R. Liu, "Collusion-Resistant Fingerprinting for Multimedia", *IEEE Signal Processing Magazine*, Vol. 21, No. 2, pp. 15–27, March 2004.

2. Boneh, D. and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data", *IEEE Transactions on Information Theory*, Vol. 44, No. 5, pp. 1897–1905, September 1998.

3. Kiyavash, N. and P. Moulin, "A framework for optimizing nonlinear collusion attacks on fingerprinting systems", *Proceedings of 40th Annual Allerton Conference on Information Sciences and Systems*, pp. 1170–1175, March 2006.

4. Kiyavash, N. and P. Moulin, "On optimal collusion strategies for fingerprinting", *Proceedings of ICASSP*, Vol. 5, pp. V–V, May 2006.

5. Zhao, H. V., M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting", *IEEE Transactions on Image Processing*, Vol. 14, No. 5, pp. 646–661, May 2005.

6. Stone, H., *Analysis of Attacks on Image Watermarks With Randomized Coefficients*, NEC Research Institute, Princeton, NJ, 1996.

7. Ergun, F., J. Kilian, and R. Kumar, "A Note on the Limits of Collusion-Resistant Watermarks", *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*, pp. 140–149, Prague, Czech Republic, May 1999.

8. Tanaka, K., Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image", *Proceedings of IEEE Military Communications*, p. 216220, 1990.

9. Swanson, M. D., B. Zhu, and A. H. Tewfik, "Data hiding for video-in-video", *Proceedings of IEEE International Conference on Image Processing*, Vol. 2, p. 676679, 1997.

10. Cox, I., J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673–1687, December 1997.

11. Bender, W., D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, Vol. 35, No. 3-4, pp. 313–336, 1996.

12. Proakis, J. G., *Digital Communications*, New York: McGraw-Hill, 1995.

13. Kilian, J., T. Leighton, L. Matheson, T. Shamoon, R. Tarjan, and F. Zane, "Resistance of Digital Watermarks to Collusive Attacks", *Proceedings of IEEE International Symposium on Information Theory*, p. 271, August 1998.

14. Chen, B. and G. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", *IEEE Transactions on Information Theory*, Vol. 47, p. 14231443, May 2001.

15. Yacobi, Y., "Improved Boneh-Shaw Content Fingerprinting", *Proceedings of RSA Conference*, pp. 378–391, San Francisco, CA, USA, April 2001.

16. Pfitzmann, B. and M. Waidner, "Asymmetric fingerprinting for larger collusions", *Proceedings of 4th ACM Conference on Coumputer and Communications Security*, pp. 151–160, 1997.

17. Chu, H., L. Qiao, and K. Nahrstedt, "A secure multicast protocol with copyright protection", *ACM SIGCOMM Computer Communication Review*, Vol. 32, No. 2, pp. 42–60, April 2002.

18. Lin, C., M.Wu, J. Bloom, M. Miller, I. Cox, and Y. Liu, "Rotation, scale, and translation resilient public watermarking for images", *IEEE Transactions on Image*

Processing, Vol. 10, No. 5, p. 767782, May 2001.

19. Wang, Z. J., M. Wu, H. V. Zhao, W. Trappe, and K. J. R. Liu, "Anti-Collusion Forensics of Multimedia Fingerprinting Using Orthogonal Modulation", *IEEE Transactions on Image Processing*, Vol. 14, No. 6, pp. 804–821, June 2005.

20. Zane, F., "Efficient watermark detection and collusion security", *Proceedings of 4th International Conference on Financial Cryptography*, pp. 21–32, February 2000.

21. Trappe, W., M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia", *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, p. 10691087, April 2003.

22. Kiyavash, N. and P. Moulin, "Regular Simplex Fingerprints and Their Optimality Properties", *Proceedings of International Workshop on Digital Watermarking*, pp. 97–109, Siena, Italy, September 2005.

23. Kirovski, D. and M. K. Mihcak, "Bounded Gaussian Fingerprints and the Gradient Collusion Attack", *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005.

24. Somekh-Baruch, A. and N. Merhav, "On the capacity game of private fingerprinting systems under collusion attacks", *IEEE Transactions on Information Theory*, Vol. 51, No. 3, pp. 884– 899, March 2005.

25. Su, J., J. Eggers, and B. Girod, "Capacity of digital watermarks subjected to an optimal collusion attack", *European Signal Processing Conference*, September 2000.

26. Verdu, S., *Multiuser Detection*, New York: Cambridge University Press, 1998.