

Copyright Protection of  
Multimedia Contents for Digital  
Rights Management

디지털 권한 관리를 위한 멀티미디어  
콘텐츠의 저작권 보호

Advisor : Prof. Kyung-Hyune Kwee



A thesis submitted in partial fulfillment of the requirements  
for the degree of

Doctor of Engineering

in Interdisciplinary Program of Information Security,  
Graduate School,  
Pukyong National University

August 2005

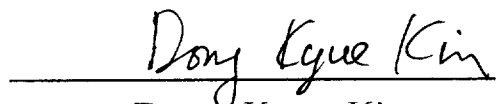
Copyright Protection of Multimedia Contents  
for Digital Rights Management

A Dissertation  
by  
Jae-Gwi Choi

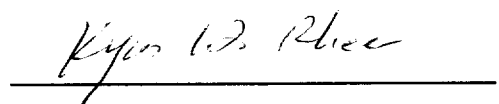
Approved as to style and content by :

  
Chairman Chang Soo Kim

  
Member Ki-Ryong Kwon

  
Member Dong Kyue Kim

  
Member Sang Uk Shin

  
Member Kyung Hyune Rhee

June 17, 2005

# Contents

Lists of Tables .....	iii
Lists of Figures .....	iv
<b>Abstract</b> .....	v
<b>Chapter I. Introduction</b>	
1.1 Background .....	1
1.2 Problem Definition .....	2
1.3 Contributions of This Thesis .....	5
1.4 Structure .....	7
<b>Chapter II. Preliminaries</b>	
2.1 Overview of DRM .....	8
2.2 Watermarking-based Contents Protection .....	11
2.3 Digital Fingerprinting .....	14
2.4 Related Areas .....	22
<b>Chapter III. Design of a Copyright Protection Scheme</b>	
3.1 Introduction .....	25
3.2 Related Works .....	26
3.3 Analysis of Domingo-Ferrer's Scheme .....	29
3.4 Analysis of Sadeghi's Scheme .....	35
3.5 Analysis of Ju et al.'s Scheme .....	40
3.6 Analysis of Goi et al.'s Scheme .....	49
3.7 Our Proposal .....	60
3.8 Open Problems .....	74
3.9 Chapter Summary .....	78
<b>Chapter IV. A Copyright Protection Scheme for Multi-Purchase</b>	
4.1 Introduction .....	80
4.2 Our Proposal .....	82

4.3 Features and Analysis .....	88
4.3 Chapter Summary .....	91
<b>Chapter V. A Copyright Protection Scheme for Broadcast Media</b>	
5.1 Introduction .....	93
5.2 Related Works .....	94
5.3 Analysis of Emmanuel et al.'s Scheme .....	96
5.4 Our Proposal .....	102
5.5 Comparison and Security Analysis .....	109
5.6 Chapter Summary .....	112
<b>Chapter VI. An Application to Mobile Communications</b>	
6.1 Introduction .....	114
6.2 Our Methodology .....	115
6.3 Our Proposal .....	119
6.4 Analysis of Security and Efficiency .....	129
6.5 Chapter Summary .....	132
<b>Chapter VII. Conclusions</b> .....	134
<b>References</b> .....	137

# Lists of Tables

Table 1. Possible word substitutions in example text .....	17
Table 2. The experiment results of Case 1 .....	58
Table 3. The experiment results of Case 2 .....	60
Table 4. Comparison of our proposal with previous schemes ....	72
Table 5. Comparison of our proposal with extended Ju et al.'s scheme .....	91
Table 6. Comparison of our proposal with Emmuanuel et al.'s scheme .....	110
Table 7. Comparison of our proposal with previous methods .....	132

# Lists of Figures

Figure 1.	The DRM pillar model .....	9
Figure 2.	The text of the vector 1111 .....	17
Figure 3.	Fingerprinting and identification steps of asymmetric fingerprinting .....	19
Figure 4.	Conspiracy attack by attackers A, B .....	39
Figure 5.	Watermark generation of Goi et al.'s scheme .....	51
Figure 6.	Each image in our Case 1 attack against Goi et al.'s scheme .....	57
Figure 7.	Each image in our Case 2 attack against Goi et al.'s scheme .....	59
Figure 8.	Buyer registration step of our first proposal .....	65
Figure 9.	Fingerprinting step of our first proposal .....	66
Figure 10.	Watermark generation of our second proposal .....	84
Figure 11.	Mask-blending, Join, and Unmasking steps of our third proposal .....	104
Figure 12.	Buyer blinding with a proxy certificate .....	123
Figure 13.	Signature verification with proxy certificate .....	123
Figure 14.	Fingerprints generation step of our fourth proposal .....	124

# 디지털 권한 관리를 위한 멀티미디어 콘텐츠의 저작권 보호

최 재 귀

부경대학교 일반대학원  
정보보호(학)협동과정

## 요 약

인터넷을 통한 전자 상거래가 활발해짐에 따라 음악 파일이나 교육, 영화 등 각종 콘텐츠 산업이 급속하게 디지털화 되고 있다. 이러한 디지털 콘텐츠는 아날로그 데이터와 달리 사본과 원본의 차이가 전혀 나지 않고, 네트워크를 통한 대량 배포가 가능하기 때문에 역으로 콘텐츠 산업 활성화에 걸림돌이 되고 있다. 따라서 불법 복제와 같은 행위로부터 저작권자의 권리를 보호하기 위해 정보 보호의 중요성이 한층 증대되고 있다.

지금까지 정보보호를 위한 방법으로 이용되어 온 데이터의 암호화는 디지털 데이터에 대한 접근은 어느 정도 제한할 수 있었으나, 적법한 구매자가 불법적인 의도를 가지고 콘텐츠를 복호한 후 이것을 재배포할 경우, 즉 불법 배포로 인한 저작권 침해는 해결할 수 없었다. 실제로 음악 파일이나 동영상 같은 멀티미디어 콘텐츠의 경우 복호된 상태 혹은 콘텐츠의 재생 시 다시 캡처(capture) 되어 암호화되지 않고 배포되는 경우가 대부분이다. 이러한 제한적인 암호화 방식을 보완하기 위하여 콘텐츠 자체에 구매자가 인지할 수 없도록 저작권 정보를 삽입하는 디지털 워터마킹(digital watermarking)이 연구되어 졌다. 디지털 워터마킹 기법은 인간의 의식 체계 또는 감지 능력으로는 검출할

수 없게 저작권자 또는 판매자의 정보를 멀티미디어 콘텐츠 내에 삽입해 줌으로써 이후에 발생하게 될 지적 재산권 분쟁에서 정당함을 증명하는 데 사용되어진다. 그러나, 만약 불법적으로 배포되고 있는 디지털 콘텐츠를 발견하였을 때, 디지털 워터마킹 기법을 사용한 콘텐츠의 저작권자나 판매자는 누구인 지 알 수 있지만, 누가 불법적으로 배포하였는지는 알 수 없다. 그래서 새롭게 연구된 분야가 디지털 핑거프린팅이다. 디지털 핑거프린팅은 기밀 정보를 디지털 콘텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하다고 볼 수 있으나, 삽입 정보의 내용에 있어서는 다르다. 디지털 워터마킹이 저작권자나 판매권자의 정보를 삽입하는 반면, 핑거프린팅은 디지털 콘텐츠를 구매한 사용자의 정보를 삽입하는 것이다. 즉 디지털 워터마킹을 사용하였을 때는 판매되는 모든 콘텐츠에 삽입되는 정보가 동일한 반면, 핑거프린팅을 사용하였을 때는 판매되는 콘텐츠가 구매한 사용자들마다 조금씩 다른 정보를 가지게 된다. 따라서 만약 콘텐츠가 불법적으로 재배포된다면, 해당 콘텐츠 내에서 핑거프린팅된 정보를 추출하여 어떤 구매자에게 판매된 콘텐츠임을 식별할 수 있게 되어, 해당 구매자에게 법적인 조치를 가할 수 있게 된다.

본 논문에서는 이러한 디지털 핑거프린팅 (부정자 추적 기법)에 관해 다루고자 한다.

디지털 핑거프린팅에 관한 연구는 공모에 대한 방지를 효과적으로 구현하는 공모 보안 코드와 프로토콜의 효율성과 안전성을 높이는 연구에 중점을 두고 진행되고 있다. 그러나 지금까지 제안된 연구는 비효율적인 계산량으로 인해 구현 가능성이 떨어지거나, 실현 가능성이 있다 하더라도 그 안전성에 문제가 있는 단점이 있다. 또한 방송 환경하의 핑거프린팅에 관한 연구도 일부에서 진행되어 왔으나 그 안전성과 효율성에 관한 분석은 해결되지 않은 채 남아 있다. 뿐만 아니라, 다중 구매와 무선 환경하의 디지털 핑거프린팅 설계에 관한 것은 지금까지 거의 연구되고 있지 않다.

따라서 본 논문에서는 단일 구매, 다중 구매, 방송 환경, 그리고 무선 환경

의 4가지 환경에 적합한 디지털 핑거프린팅 기법들을 각각 제안하고자 한다. 제안 방식은 다음과 같이 크게 4가지로 나눌 수 있다. 첫째, 핑거프린팅 방식을 이용한 기존의 부정자 추적 기법들에 대한 안전성과 효율성 분석을 통해, 단일 구매 (판매자와 구매자가 1:1인 환경에서, 구매자가 하나의 콘텐츠를 구매할 경우)에 적합한 안전하고 효율적인 디지털 핑거프린팅 기법을 제안하고자 한다. 둘째, 판매자와 구매자가 1:1인 환경이나, 구매자가 다수의 콘텐츠를 구매할 경우인 다중 구매에 적합한 디지털 핑거프린팅 기법을, 셋째, 제한된 컴퓨팅 환경과 메모리를 가진 구매자의 이동 단말기 상에서 적용할 수 있는 디지털 핑거프린팅 기법을 제안하고자 한다. 그리고 마지막으로 방송환경에 초점을 맞춘 디지털 핑거프린팅 기법을 제안하고자 한다.

# Chapter I . Introduction

## 1.1 Background

In a very short time, E-commerce has become a huge business and a driving factor in the development of the Internet. With the proliferation of the Internet, exchange or delivery of digital contents such as MP3 audio and video is very easy and popular. Moreover it is very difficult to distinguish original contents from their copies in digital domain. It has caused unlimited copying, and has made the entertainment industry nervous because their contents might be pirated much more than happens with analogue home taping. Illegal copying threatens intellectual property rights and is becoming more and more critical.

This work deals with the problem of managing illegal copying of digital contents. To put it more concretely, the use of user-unique marking of the contents, fingerprints, is taken up for the purpose of tracking the origin of a discovered illegal copy of the contents.

The scenario is the following. Somebody, the owner of contents(or the seller), has digital contents and wants to sell them to a number of buyers. He embeds an unique mark per buyer (i. e. an ID) into copies

of a digital content using watermarking techniques in order to control the redistribution of contents. Suppose that one of the buyers redistributed the contents illegally and the owner discovered it, that the owner(or the seller) can retrieve the unique mark from the copy for identifying the buyer who used the content for unintended purpose. Finally he can trace the origin of the copy, so-called a traitor, through the unique mark.

It cannot prevent copying, but it can at least help identify the source of pirated copies, and thus enables a legal action. This is the goal of topics in this thesis.

## **1.2 Problem Definition**

What is important in designing fingerprinting schemes is to make it more practical and efficient. However, the complexity of existing schemes is too high to be implementable. Recently, several digital fingerprinting schemes to consider practicality were proposed. These are significant in the sense that there are completely specified from a computation point of view and are thus readily implementable. But these schemes have the serious problems that they cannot offer the security of sellers and buyers. Thus it is necessary to design practical and secure digital fingerprinting that all computations are performed effi-

ciently and the security degree is strengthened.

In general, e-commerce system consists of a set of contents such as image, audio, a set of sellers and a set of buyers. Each buyer wants to buy some contents from a set of sellers. Then the sellers encrypt them with buyer's public key. Anonymous schemes have to offer anonymity of buyers and unlinkability of the contents. Thus each content must be bought with different pseudonyms, because the same anonymous key implies that the buyer's purchases are linkable. But, if we apply existing schemes to this case, a buyer must go through the registration or watermark generation step several times in order to obtain several different pseudonyms. The buyer also must store public keys as many as the number of contents to be purchased, because each content must be encrypted with different key separately. That is, existing schemes have the problem that the number of keys held by buyer's devices should increase in proportion to that of contents purchased, if we apply them to multi-purchase. Moreover, the research on multi-purchase has never been studied so far. This is the reason we are concerned with an efficient fingerprinting scheme for multi-purchases.

It must be a very powerful tool to trace traitors in a broadcast environment. But it is hard to design an efficient fingerprinting scheme for broadcast media. Because each subscriber must receive a slightly different version of a content in order to be identified, it is contrary to

the bandwidth saving of being able to distribute the same content efficiently to many subscribers. Several digital fingerprinting-based schemes have been proposed as a technique to provide copyright protection for broadcast media. But most of them are symmetric, where the broadcaster knows each subscribers' unique mark. Therefore the result of tracing is no real evidence that could unambiguously convince a third party. There is an asymmetric scheme, but its security analysis remains unsettled. Thus the security analysis of the previous scheme must be examined and it is necessary to propose secure fingerprinting scheme for broadcast media.

The demand for mobile communication service is accelerating and mobile communication industries are growing rapidly all over the world. Moreover, they are expected to provide higher quality of multimedia services for users in mobile communication. Thus copyright protection of multimedia contents being provided must be solved along with them. In general, the watermarked contents can be made in off-line, because every sold copy is the same. On the contrary, the fingerprinted contents can be made in on-line, because every sold copy must be slightly different from the original contents. Still less, buyer's memory and computation power in mobile communications is smaller than those of wire ones. There has been no study that tried to make digital fingerprinting schemes for mobile environments. Thus it is necessary to design practical fingerprinting scheme for mobile environ-

ments in order to ensure the success of copyright protection under mobile environments.

### **1.3 Contributions of This Thesis**

Our proposals in this thesis are divided into three main parts and one application: Design of a fingerprinting scheme, a fingerprinting scheme for multi-purchase, a fingerprinting scheme for broadcast media, and its application to mobile communications.

#### **1.3.1 Design of a Fingerprinting Scheme**

We propose a novel digital fingerprinting scheme based on oblivious transfer protocol, which is secure against the dishonesty of a seller and a buyer. That is, the case that one buyer purchases a content is dealt with. We also analyze the existing fingerprinting schemes and show how to break the schemes.

One of contributions of our first proposal is to show the drawbacks of existing schemes. Another contribution is to suggest secure copyright protection schemes, where all computations are performed efficiently and the security degree is strengthened than the previous schemes.

### **1.3.2 Design of a Fingerprinting Scheme for multi-purchase**

We describe a fingerprinting scheme, which is suitable for multi-purchase. The case that one buyer purchases many contents is dealt with.

Our second proposal is significant in the sense that (1) our scheme is the first one which considers multi-purchase case, (2) the number of keys held by a buyer is constant regardless of that of contents purchased, (3) even if the buyer holds one key, unlinkability of contents is provided.

### **1.3.3 Design of a Fingerprinting Scheme for Broadcast Media**

We propose a fingerprinting scheme focused on broadcast environments such as Pay-TV, where multimedia contents are distributed over a network. The case that there is a number of subscribers and one broadcaster is dealt with.

One contribution of our third proposal is to show the serious faults of previous schemes which considered broadcast environments. Other contributions of our third proposal is secure without a trusted third party. (The previous schemes introduced a trusted third party for their security) and provide subscribers' anonymity, which is one of important requirement for electronic marketplaces.

### **1.3.4 Application to Mobile Communications**

We extend fingerprinting schemes to mobile communications.

Our fourth proposal is significant in the sense that (1) it is the first trial which considers mobile communications, (2) it reduces amount of buyers' computations to the minimum.

## **1.4 Structure**

This thesis is organized as follows. Chapter II gives a general introduction to digital contents protection technologies. This is followed by a description of related researches and the area we are concerned with.

The following Chapters present our proposals. Design of a fingerprinting scheme is described in Chapter III, and a fingerprinting scheme for multi-purchase in Chapter IV. Then the proposed fingerprinting scheme for broadcast media is described in Chapter V, and its application to mobile communications is shown in Chapter VI. Finally, we conclude in Chapter VII.

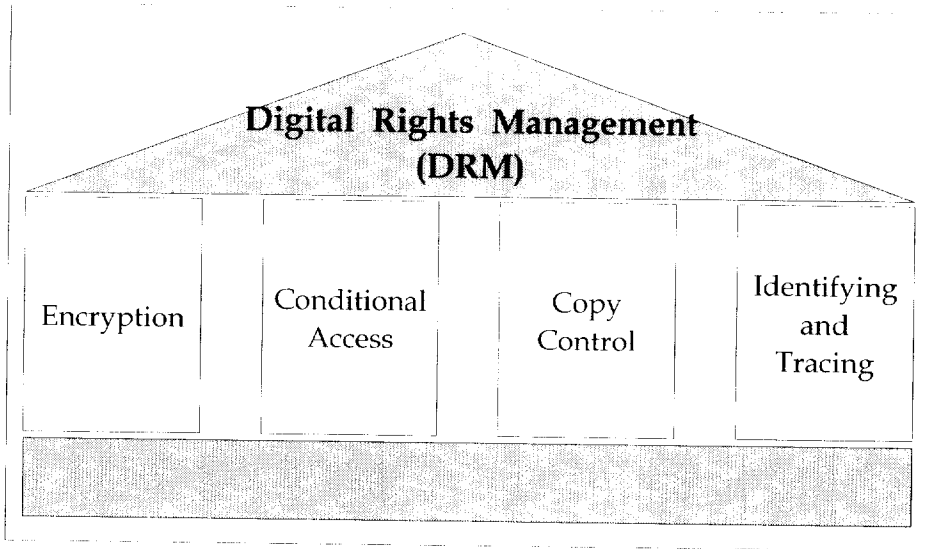
# Chapter II. Preliminaries

## 2.1 Overview of DRM

A major obstacle for digital media distribution and associated business is the possibility of unlimited consecutive copying in the digital domain, which threatens intellectual property rights. The problem of digital content piracy is becoming more and more critical, and major content producers are threatened by observing that their business are drastically reduced because the digital contents can be easily copied and distributed. This is the reason why digital rights management (DRM) is currently garnering much attention from industry and research.

Generally speaking, a DRM system enables the secure exchange of intellectual property, such as copyright protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks. DRM allows contents owners to distribute securely to authorized recipients and gives them control over the whole distribution chains.

The framework of DRM consists of technical, business, social, and legal components. The business aspect of DRM involves new business models such as a free evaluation copy for few days followed by a full permission or a downloadable stream for immediate use followed by a



**Figure 1.** The DRM pillar model.

digital versatile disk(DVD) copy in the mail. The social angle of DRM is governed by societal norms concerning fair use, privacy management, and the education of consumers so as to inform them of the risks associated with using pirated content. The legal aspect deals with the laws of the license jurisdiction and includes legislation, compliance, investigation, and enforcement. The technical DRM perspective deals with the technical standards and infrastructure, which consists of protection mechanisms, trading protocols, and rights language. Here, we will describe the technical aspects of DRM in detail. Figure 1 shows the main components of a DRM system.

This includes:

- *Encryption* of the contents or parts in order to disallow uncon-

trolled access.

- *Access control (conditional access)* according to flexible usage rules. A strength of modern DRM systems is that the usage rules can be adapted to the business models. For example, access can be restricted to certain users, a limited time, or a limited number of accesses. The access right can also be traded, for example, against customer information or the agreement of the customer to receive advertisements. Initial access to the data may even be free, while subsequent access has to be paid for.
- *Copy control* or copy prevention. Depending on the usage rules, no/one/several/unlimited copies of the multimedia data are allowed, with or without the right to produce copies of the copies. The DRM system enforces those copy restrictions. For some usage rules, copy control is difficult to achieve and requires a sophisticated technology like watermarking.
- Decryption key management
- Interface to billing systems of mechanisms. Since most business models for media distribution involve monetary transactions, the DRM system must be able to trigger those transaction.

- *Identification and tracing* of multimedia data. Since authorized users of multimedia usually have access at least to an analog version of the data, they could at least produce copies from that analog output. Thus, analog copies in general can hardly be prevented. For some applications it is necessary to identify and trace back analog and digital copies of distributed media. This can be done by individual digital watermarking of the distributed data and is then also part of the DRM system.

In the next section, we will discuss this part more closely.

## **2.2 Watermarking-based Contents Protection**

Most solutions for content protection are based on a few core technologies, such as cryptography and watermarking. While cryptography is only applicable in the digital domain, watermarking is more effective for contents protection in the analog domain. Cryptography behaves as a protective envelope that prevents unauthorized access, but once the contents are decrypted, the protection is completely destroyed. In contrast to this, detectable remnants of watermarks are more likely to remain after decryption. That is, watermarking technology allows the embedding of hidden data, e. g., copyright information, in the digital content.

DRM technology could benefit from watermarking approaches in several ways, as the variety of watermarking-based systems can address DRM problems. In the following, we will present the various aspects of watermarking approaches to the development of DRM systems [1].

### **2.2.1 Proof of Ownership**

This is the most classical scenario served by watermarking: the author of contents wishes to prove that she is the only legitimate owner of the contents. To do so, as soon as she creates the content, she embeds a watermark to it for identifying her unambiguously. In the sequel, watermark extraction can be used to verify her ownership over the content since, due to the impossibility of removing the watermark, all the copies of the content will contain the watermark, thus linking them to her.

### **2.2.2 Copyright Protection**

Copyright protection is probably the most prominent application of watermarking today. The objective is to embed information about the source, and typically the copyright owner, of the content in order to prevent other parties from claiming the copyright on the content. Thus, the watermarks are used to resolve rightful ownership, and this application requires a very high level of robustness. The driving force for

this application is the Web which contains millions of freely available images that the rightful owners want to protect. Additional issues besides robustness have to be considered. For example, the watermark must be unambiguous and still resolve rightful ownership if other parties embed additional watermarks. Hence, additional design requirements besides mere robustness are applied.

### **2.2.3 Copy Control**

A desirable feature in multimedia distribution systems is the existence of a copy protection mechanism that disallows unauthorized copying of the media. Copy control is very difficult to achieve in open systems; in closed or proprietary systems, however, it is feasible. In such systems it is possible to use watermarks indicating the copy status of the content. An example is the DVD system where the content contains copy information embedded as a watermark. A compliant DVD player is not allowed to playback or copy data that carry a "copy never" watermark. Contents that carry a "copy once" watermark may be copied, but no further consecutive copies are allowed to be made from the copy [2,3].

### **2.2.4 Copy Deterrence; Fingerprinting**

Copy deterrence mechanism is adopted to discourage unauthorized

duplication and distribution. Copy deterrence is achieved by providing a mechanism to trace unauthorized copies to the original owner of the contents or, more generally, to track the author of the infringement. In the most common case, tracing is made possible by letting the seller insert a distinct watermark, which in this case is called a fingerprint, identifying the buyer, or any other addressee of the contents, within any copy of data that is distributed. (The term "fingerprinting" has been recently used for another type of technology aimed at extracting from digital contents a distinctive set of unique characteristics that can be later used for identifying it.) If, later on, an unauthorized copy of the protected contents is found, then its origin can be recovered by retrieving the unique watermark contained in it.

As it is the objective of this thesis, we will discuss it a little further in the next section.

## **2.3 Digital Fingerprinting**

### **2.3.1 The Idea of Fingerprinting**

The idea of fingerprinting is to mark each copy uniquely, so that every distributed copy is a little different from each other. In this way it is possible to distinguish among all legal copies [4]. Thus, if we distrib-

ute copies only to persons who identify themselves, it might be possible, if an illegal copy is found, to identify the person who bought the legal copy from which the illegal copy was made.

Doing so, we hope, will deter users from making illegal copies, since if they redistributed the copy to somebody else, they will lose control over it, and it is possible that the copy will arrive at somebody who will identify and prosecute the user for creating and spreading the copy. Thus the greater risk of being identified ought to make it less popular to spread illegal copies.

### 2.3.2 Examples of Fingerprinting

Fingerprinting has been used for centuries and we may find several classical examples of it. We list examples of fingerprinting before and after the computer era. These examples will provide inspiration about what fingerprinting is and why it is needed [1].

- *Fired Bullet*: Each weapon has its own type of fired bullet depending on both the manufacturer and the type of weapon. Typewriters are similar; each typewriter has its own typesets.
- *Serial Number*: Serial numbers on manufactured products are unique for each product and can be used to distinguish between them.

- *Maps*: Sometimes maps have been drawn with slight deliberate variations from reality to identify copies. Since fingerprints on digital data are easy and inexpensive means of copyright protection, the demand on fingerprinting in computers and communication is getting stronger.
- *Prefix of E-mail Address*: On mailing systems supporting IETF RFC 754, it is possible to add a prefix to usual e-mail address [5]. This can be useful when registering with an on-line services. For example, Bob (Bob@foo.org) can register Mallory+Bob@foo.org at Mallory's site. Then if he receives all unsolicited message to this address, he can infer that Mallory passed the address to some bulk mailer.
- *Digital Audio/Video*: It has been suggested to use fingerprints to check out piracy of video data. In a pay-TV broadcast system, fingerprinting is applied to trace illegal subscribers.
- *Documents*: As copyright protection means, fingerprinting is used in documents to discourage copying. Here, we will give an example where many of the concepts are illustrated [6].

Assume that we have a short text that we want to fingerprint. Our goal might be that somebody inside our organization is leaking infor-

**Table 1.** Possible word substitutions in example text.

Original "0"	fantastic	discovered	profound	new	cars
Variant "1"	amazing	invented	great	future	automobiles

The amazing new technology that we in New Technology Inc. have invented is of great importance to future generations of automobiles.

**Figure 2.** The text of the vector 11111.

mation about our next generation products to the Internet, and we want to find out who it is. The original text looks like:

*The fantastic new technology that we in New Technology Inc. have discovered is of profound importance to new generations of cars.*

As authors of this text we think that the word substitutions in Table 1 can be made without the meaning being lost. The list of possible substitutions must, of course, be kept secret from the users.

Should the users which words could be exchanged for which other words, it would be simple for users leaking the information to remove any traces of their fingerprints from the illegal copy they create.

Each of these substitutions can be made independently of the others, which means that we have five places in which we can choose freely

between two different words. if we present the original word with a '0' and the variant with a '1', we can describe any version of the text with a five-bit binary vector.

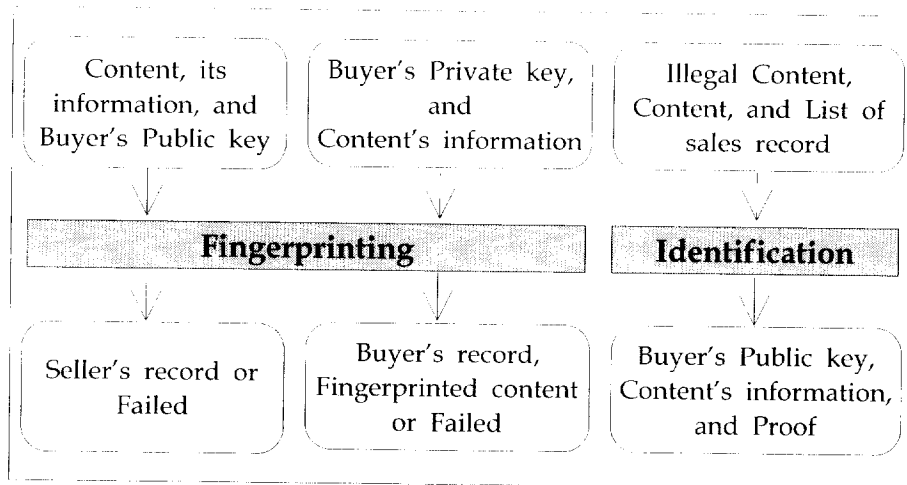
The original text corresponds to the vector (00000), the text, "The amazing new technology that we in New Technology Inc. have discovered is of profound importance to future generations of cars" corresponds to the vector (10010), and the vector (01001) corresponds to the next "The fantastic new technology that we in New Technology Inc. have invented is of profound importance to new generations of automobiles".

If we think that our leak works alone, we can distribute this text in  $2^5 = 32$  different versions to as many different people. If we remember who receives which version, we can find the leak if we happen to find the text somewhere on the Internet. This is the simplest possible way to use fingerprints.

### **2.3.3 History of Fingerprinting**

Researches on fingerprinting can be classified into three main groups: fingerprinting protocol, collusion secure code, and embedding techniques. As the purpose of this chapter is concerned, we will not take up embedding techniques so-called watermarking technology.

The following three types (symmetric, asymmetric, and anonymous schemes) are grouped into same field, fingerprinting protocol. The oth-



**Figure 3.** Fingerprinting and identification steps of asymmetric fingerprinting.

er is the study that tried to develop collusion secure code.

- **Symmetric Schemes:** Classical fingerprinting schemes are symmetrical in the sense that the content owner knows the watermarks uniquely linked with the buyer [7,8]. Thus, if another copy with this watermark turns up, the buyer can claim that the seller redistributed it. Because this could be done for example, by a malicious seller who may want to gain money by wrongly claiming that there are illegal copies around. Thus, one cannot really assign responsibility about redistribution to one of them.
- **Asymmetric Schemes:** This problem is overcome by asymmetric schemes [9,10]. Here, because only the buyer can obtain the exact fingerprinted copy, he/she cannot claim that an unauthorized

copy may have originated from the seller. Hence, if an unauthorized copy is found, the seller can obtain a means to prove to a third party that the buyer redistributed it and he/she can identify a traitor/copyright violator. Figure 3 shows fingerprinting and identifications steps of asymmetric schemes. However the drawback of these solutions is that it did not provide a buyer's anonymity.

- *Anonymous Schemes:* To protect buyer's privacy two anonymous schemes have been suggested by Pfitzman et al. [11] and Ju et al. [12]. The idea is that the seller can know neither the watermarked content nor the buyer's real identity. Nevertheless the seller can identify the copyright violator later. This possibility of identification will only exist for a copyright violator, whereas honest buyers will remain anonymous.
- *Collusion Secure Schemes:* The fingerprinting has a critical issue on how to obtain resilience against a collusion attack, in which the attackers compare two or more fingerprinted copies to find and alter the marks. For collusion secure fingerprinting,  $c$ -frameproof code [13] is introduced to guarantee that no coalition consisting of at most  $c$  traitors can generate a codeword that is not contained in the coalition. Also,  $c$ -secure frameproof code [14] is shown

with the extended property: no two disjoint coalitions consisting of at most  $c$  traitors can generate the same word. These two codes prevent attackers from "framing" innocent user. It is very important to design secure fingerprinting schemes, but it is not our present concern. Thus we will not take up collusion secure schemes in detail.

### 2.3.4 Requirements of Fingerprinting

Requirements of fingerprinting schemes can be listed as follows.

- *Anonymity*: A buyer should be able to purchase digital contents anonymously.
- *Unlinkability*: Given two digital contents, nobody can decide whether or not these two contents were purchased by the same buyer.
- *Traceability*: The buyer who has distributed digital contents illegally can be traced.
- *No Framing (Buyer's security)*: An honest buyer should not be falsely accused by a malicious seller or other buyers.
- *No Repudiation (Seller's security)*: The buyer accused of redistribut-

ing an unauthorized copy should not be able to claim that the copy was created by the seller.

- *Collusion Tolerance*: Attacker should not be able to find, generate, or delete the fingerprint by comparing the copies, even if they have access to a certain number of copies.
- *Practicality*: All computations should be performed efficiently so that it can be readily implementable.

## 2.4 Related Areas

### 2.4.1 Steganography

Steganography is about embedding a secret message in a cover message so that it is not visible and cannot be found [14]. While cryptography is about protecting the content of messages, steganography is about concealing their existence. The embedding can be parameterized by a key that is used when retrieving the secret message may be encrypted for added security, but the encryption can not do what steganography does, which is hide the existence of the secret message.

## 2.4.2 Digital Watermarking

Both steganography and watermarking describe techniques that are used to imperceptibly convey information by embedding it into the content. Of course, watermarks do not always need to be hidden, as some systems use visible digital watermarks, but most of the literature has focussed on imperceptible digital watermarks which have wider applications.

Steganography typically relates to covert point-to-point communication between two parties [15]. Thus, steganography methods are usually not robust against modification of the content, or have only limited robustness and protect the embedded information against technical modifications that may occur during transmission and storage, like format conversion, compression, or digital-to-analog conversion. Watermarking is much like steganography, only that the scheme should be robust against active attackers, even if they know not only that a content contains a watermark, but also if they know the algorithmic principle of the method. A popular application of watermarking is to give proof of digital data by embedding copyright statements.

## 2.4.3 Traitor Tracing

Traitor tracing is the equivalent of fingerprinting for cryptologic keys. It was introduced by Chor et al. for broadcast encryption [16]. When

the data (e.g., a pay-TV movie) is broadcasted in encrypted form, and only the decryption keys are sold, a different key is sold to each pay-TV subscriber. Furthermore, the encryption scheme is adapted so that all keys can be used to decrypt the same ciphertext. Since the decryption key is different from each subscriber, the pay-TV company can trace the user who made illegal copies of his key.

# Chapter III. Design of a Copyright Protection Scheme

## 3.1 Introduction

This chapter gives a copyright protection scheme. More accurately, a tracing traitors (or copyright violators) scheme will be presented.

In the beginning, we will define some terminologies on fingerprinting scheme.

- An *object* is a collection of digital data. Digitally stored texts, images or audio files are examples of such objects.
- An *original* is an object that somebody, who has the legal right wants to distribute. There is exactly one original in the fingerprinting system.
- A *copy* is an object close to the original. A copy in this meaning is not an exact digital copy by digit. Instead it is an object that is so similar to the original that it for all purposes serves just as well.

- A *mark* is a portion of an object and has a set of several possible states; fingerprint is a collection of marks.
- A *distributor* is an authorized provider of fingerprinted objects. For example, if the original is a book, the distributor can be the publisher of that book, that is, the person/company which has the right to distribute the book.
- An *authorized user* is an individual who is authorized to gain access to fingerprinted object.
- A *traitor (copyright violator)* is an authorized user who distributes fingerprinted objects illegally.
- *Illegal distribution* is the distribution of copies by somebody else except the legal distributor.

## 3.2 Related Works

Conventional fingerprinting schemes work as follows: The seller prepares a slightly different "copy" of the data item for each buyer. If he finds a redistributed data item, he finds out to which of the copies sold it corresponds. This concept was introduced in [8]. One problem

with this technique is that the fingerprint is inserted solely by the seller. A buyer whose fingerprint has been found on unauthorized copies can claim that the unauthorized copy was created by the seller. Because the buyer and the seller know the fingerprinted copy. Even if the seller succeeds in identifying a dishonest buyer, his previous knowledge of the fingerprinted copies prevents him from using them as a proof of redistribution in front of third parties.

In [9], asymmetric fingerprinting was proposed to solve this problem of symmetric fingerprinting schemes. In asymmetric fingerprinting schemes, the seller obtains a proof of the treachery. For this, fingerprinting must be an interactive protocol between the buyer and the seller where the buyer also inputs a secret and the seller does not see the fingerprinted copy that this buyer obtains.

In buyer-seller watermarking protocols, a buyer supplies the seller with an encrypted version of a unique watermark (fingerprints) in order to solve this problem. Then the seller embeds the encrypted version of watermarks into a content using an invisible watermarking algorithm. This watermarked copy is then transmitted to the buyer. Since only the buyer knows the decryption key, he can prove to a third party the legitimate ownership of the copy in his possession.

But asymmetric schemes have the drawback that the seller knows the buyer's identity even if the buyer is honest. Later, the concept of anonymous fingerprinting (buyer-seller watermarking) was introduced [11]. The idea is that the seller knows neither the fingerprinted copy nor the

buyer's identity. The most important point of designing anonymous fingerprinting scheme is to make it more practical and efficient. But, Pfitzman and Waidner's scheme [11] is inefficient and impractical because it is based on secure two-party computations without presenting explicit protocols [17]. That is, the two-party computations use general theorems like "every NP-language has a zero-knowledge proof systems". So it has high complexity. Later, Pfitzman and Sadeghi suggested an efficient method without secure two party computations [18]. The first proposals to pay attention to practical fingerprinting scheme were Domingo-Ferrer and Joancomarti's scheme and Domingo-Ferrer's scheme [19,20]. Domingo-Ferrer and Joancomarti's scheme [19] is based on 1-out-of-2 oblivious transfer protocol. However, this approach also relies on an unspecified general zero-knowledge proof. On the contrary, Domingo-Ferrer's scheme [20] is based on committed oblivious transfer (COT) that is completely specified from a computational point of view and is thus readily implementable. But it allows the seller to cheat honest buyers. Later, Sadeghi made several constructive proposals to repair some flaws of [20] scheme and Pfitzman and Sadeghi suggested an efficient method without secure two party computations, which is based on the principle of digital coins [18], [21]. But Sadeghi's scheme [21] also has security problem that buyers and sellers cheat each other and Pfitzman and Sadeghi's scheme [18] is impractical because it used Boneh and Shaw' scheme [13] as a building block for collusion resistance. In [13], their code needed for embedding is so long

that the overall system cannot be practical. Ju et al.'s scheme [12] is the scheme using Cox's invisible watermarking algorithm [22] instead of Boneh and Shaw's scheme. It is a significant model in the sense that it offered the anonymity of a buyer to watermarking protocol. But it cannot provide security of sellers and buyers. We analyze several anonymous schemes clearly in the next section.

### 3.3 Analysis of Domingo-Ferrer's Scheme [20]

What is important in designing fingerprinting scheme is to make it more practical and efficient. Recently, Domingo-Ferrer first proposed committed oblivious transfer protocol-based digital fingerprinting to consider practicality. In this section, we analyze this scheme.

#### 3.3.1 Overview

##### ■ Step 1. System Setup

The digital contents  $item$  is assumed to be  $n$  bit long. There are two possible versions of each contents, a marked version and an unmarked version. For each bit  $item_i (i = 1, 2, \dots, n)$  the seller creates two versions  $item_i^0, item_i^1$  of  $i$ -th bit  $item_i$ . For  $i = 1$  to  $n$ , the seller commits, using BCXs (bit commitment with XOR), to  $item_i^0$  and to  $item_i^1$  to get

**Note 3.1** Oblivious transfer was originally invented by Rabin [23]. The following explains its conception.

Mary has one secret; the protocol allows Bob to learn the secret with probability  $1/2$ ; whatever they do, Mary and Bob cannot modify the probability of Bob learning the secret; moreover, Mary cannot infer from the protocol whether Bob learned the secret or not. A slight variation of the above yields Rabin's one out of two oblivious transfer, whereby Mary has two secrets and the protocol allows Bob to learn one of them; the probability of Bob learning either secret is  $1/2$ ; whatever they do, Mary and Bob cannot modify that probability; moreover, Mary cannot infer from the protocol which was the secret learned by Bob.

In a one-out-of-two oblivious transfer, Bob has to choose between learning bit  $a_0$  or  $a_1$  prepared by Mary but she does not learn his choice  $b$ . Now let us turn to committed oblivious transfer (COT). Suppose that Mary is committed to bits  $\overline{a_0}, \overline{a_1}$  and Bob is committed to bit  $\overline{b}$ . After running  $\text{COT}(\overline{a_0}, \overline{a_1}), (\overline{b})$  Bob knows  $a_b$  and is committed to  $\overline{a_b}$ . Mary, whatever she does, cannot use the protocol to learn information on  $a_{\overline{b}}$ .

$com_i^0, com_i^1$ . The seller sends to the registration center a signed and time-stamped message containing a short *item* description of *item* as well as a list of the  $l < n$  bit positions in containing a mark.

### ■ Step 2. Buyer Registration

1. Registration center chooses a random nonce  $x_r \in Z_p$  and sends  $y_r = g^{x_r}$  to buyer.
2. Then buyer chooses secret random  $s_1$  and  $s_2$  in  $Z_p$  such that  $s_1 + s_2 = x_B \pmod{p}$  and sends  $S_1 = y_r^{s_1}$  and  $S_2 = y_r^{s_2}$  to registration center. In here,  $x_B$  is the private key of the buyer and  $y_B = g^{x_B} \pmod{p}$  is the public key corresponding with it. The buyer convinces the registration center in zero-knowledge of possession of  $s_1$  and  $s_2$ . The buyer computes an El-Gamal public key  $y_1 = g^{s_1}$  and sends it to registration center.
3. Next, the registration center checks that  $S_1 S_2 = y_B^{x_r}$  and  $y_1^{x_r} = S_1$ . If they are verified, the registration center returns to the buyer a certificate  $Cert(y_1)$ . The certificate states the correctness of  $y_1$ .

### ■ Step 3. Fingerprinting

The following steps are executed for  $i = 1, 2, \dots, n$ .

1. The seller permutes the pairs,  $item_i^0, item_i^1$ , and stores the result  $item_i^{(0)}, item_i^{(1)}$  in his purchase record.
2. The seller and the buyer run a Committed Oblivious Transfer Protocol (COT) from [24]. At the beginning of this protocol the seller inputs commitments  $com(item_i^{(0)}), com(item_i^{(1)})$  of his two secret bits  $item_i^{(0)}, item_i^{(1)}$  and the buyer inputs the commitment  $com(b_i)$  to a bit  $b_i$  which indicates the secret she wants to learn. The protocol should not reveal any information on the other secret to the buyer. It also should not leak any information on  $b_i$  to the seller. The output of the protocol to the buyer is the fingerprinted sub-item  $item_i^* := item_i^{(b_i)}$  and its commitment  $com_i^* = com(item_i^*)$ .
3. The buyer signs  $com_i^*$  using  $s_1$  and sends it together with the certificate  $Cert(y_1)$  to the seller who verifies them.

#### ■ Step 4. Identification

After finding a redistributed copy  $item^{red}$ ,

1. The seller retrieves all signed commitments corresponding to the sale contents that is similar enough to  $item^{red}$ .
2. The seller sends a signed copy of  $item^{red}$  to registration center and to all pseudonymous buyers who have bought a copy of this

contents.

3. All suspected pseudonymous buyers execute the following until he finds a traitor

(1) Using a coin-flipping protocol the seller and the pseudonymous buyer agree on  $l_1 \leq i \leq n$  bit positions. The agreement protocol is repeated until the resulting positions contain  $l_3$  marks with  $l_2 \leq l_3 \leq l_1^*$ .

(2) The pseudonymous buyer opens her commitments corresponding to  $l_1$  bit positions agreed upon. If all  $l_3$  opened commitments match with the corresponding bit values in  $item^{red}$ , the seller takes this as proof of redistribution. Otherwise the buyer is declared innocent and gets new fingerprinted contents.

4. The seller presents the opened signed commitments to the registration center requesting for identification. The proof of redistribution consists of opened commitments, the signed  $item^{red}$  sent to the registration center in step 2 and the mark positions sent the registration center in system setup.

\*  $l_2$  is the minimal number of marks to be opened by a suspect buyer in the identification protocol. Thus the probability that the seller identifies an honest buyer who correctly followed fingerprinting protocol correctly is upper-bounded by  $2^{-l_2}$ . The seller can choose  $l_2$  depending on the probability. If  $l_2$  is tuned properly, the risk of unjustly accusing a buyer is sufficiently low not to deter suspect buyers from proving their innocence.

### 3.3.2 Observation on Security and Efficiency

Domingo-Ferrer's scheme [20] is significant in the sense that it presented the first construction for anonymous fingerprinting which is completely specified from a computational point of view and is thus readily implementable. But the most undesirable issue of the scheme is that it did not offer the security of buyers and sellers, because the seller knows the buyer's fingerprinted contents if he abuses flows of COT in [20].

#### ■ Observation on Security

The fingerprinting step of Domingo-Ferrer's scheme is insecure because the seller can always cheat the buyer by inputting the same version of the  $item_i$  (e.g.  $item_i^0$ ) to the COT-protocol for each  $i$ . Thus the seller will always know the output of COT, i.e., he knows which fingerprinted contents is assigned to which buyer. This allows a dishonest seller to wrongly accuse an honest buyer of treachery. Hence Domingo-Ferrer's scheme does not satisfy the security of buyers and sellers in Chapter 2, because an honest buyer is falsely accused by a malicious seller and the buyer accused of reselling an unauthorized copy can also claim that the copy was created by the seller.

#### ■ Observation on Efficiency

One of the requirements for anonymous fingerprinting is to reduce

the computational complexity. However it has complexity of  $O(nm)$  plain oblivious transfer and  $O(nm^2)$  plain bit commitments (digital contents consist of  $n$  bits and  $m$  is a security parameter) in the fingerprinting step [24]. It is unrealistic, because its round complexity is linear in the square number of bit-length of contents.

It also has 5 exponent, 1 zero-knowledge proof, and 4-pass number in the registration protocol. A further critical issue is that the seller must contact all pseudonymous buyers during the identification step.

### **3.4 Analysis of Sadeghi's Scheme [21]**

Sadeghi's scheme made several constructive proposals to repair some flaws of Domingo-Ferrer's scheme. This scheme is very similar to Domingo's one except for the buyer registration and fingerprinting (dispute) steps.

#### **3.4.1 Overview**

##### **■ Step 1. Buyer Registration**

In general, if sellers can collude with a registration center, she can easily know the real identity of honest buyers. Since the pseudonym of buyers is provided by a registration center in anonymous fingerprinting schemes. Sadeghi suggested a  $k$  out of  $m$  trust model in order

to reduce the chance of a dishonest seller to identify the buyer (real identity of the buyer). It means that  $k$  out of  $m$  registration centers perform the registration of the buyer. So the seller must collude with  $k$  out of  $m$  registration centers in order to succeed in revealing the honest buyer's real identity. The case  $k = m$  is trivial and similar to the case with a single registration center, since one can simply establish a certificate chain among the registration center.

## ■ Step 2. Fingerprinting

Fingerprinting step of Sadeghi's scheme [21] is the same that of Domingo-Ferrer [20] except adding the following process.

During the fingerprinting (or a dispute) step the buyer requests the seller to open some pairs of commitments input to COT in a cut and choose manner and verifies whether the seller has behaved properly or not. However not all pairs can be opened and the identification-relevant parameters such as  $l_3$  must be adapted accordingly.

## ■ Step 3. Identification

After finding a redistributed copy  $item^{red}$ ,

1. The seller retrieves all signed commitments corresponding to the sales contents that is similar enough to  $item^{red}$ .
2. The seller sends a signed copy of  $item^{red}$  to registration center and to all pseudonymous buyers who have bought a copy of this

contents.

3. All suspected pseudonymous buyers execute the following until he finds a traitor
  - (1) Using a coin-flipping protocol the seller and the pseudonymous buyer agree on  $l_1 \leq i < n$  bit positions. The agreement protocol is repeated until the resulting positions contain  $l_3$  marks with  $l_2 \leq l_3 \leq l_1$ .
  - (2) The pseudonymous buyer opens her commitments corresponding to  $l_1$  bit positions agreed upon. If all  $l_3$  opened commitments match with the corresponding bit values in  $item^{red}$ , the seller takes this as proof of redistribution. Otherwise the buyer is declared innocent and gets new fingerprinted contents.
4. The seller presents the opened signed commitments to the registration center requesting for identification. The proof of redistribution consists of opened commitments, the signed  $item^{red}$  sent to the registration center in step 1 and the mark positions sent to the registration center in system setup.

### 3.4.2 Observation on Security and Efficiency

It is significant since it raised the efficiency and security of Domingo-Ferrer's scheme. But undesirable issue is that it did not offer the security of buyers and sellers, because buyers can know both ver-

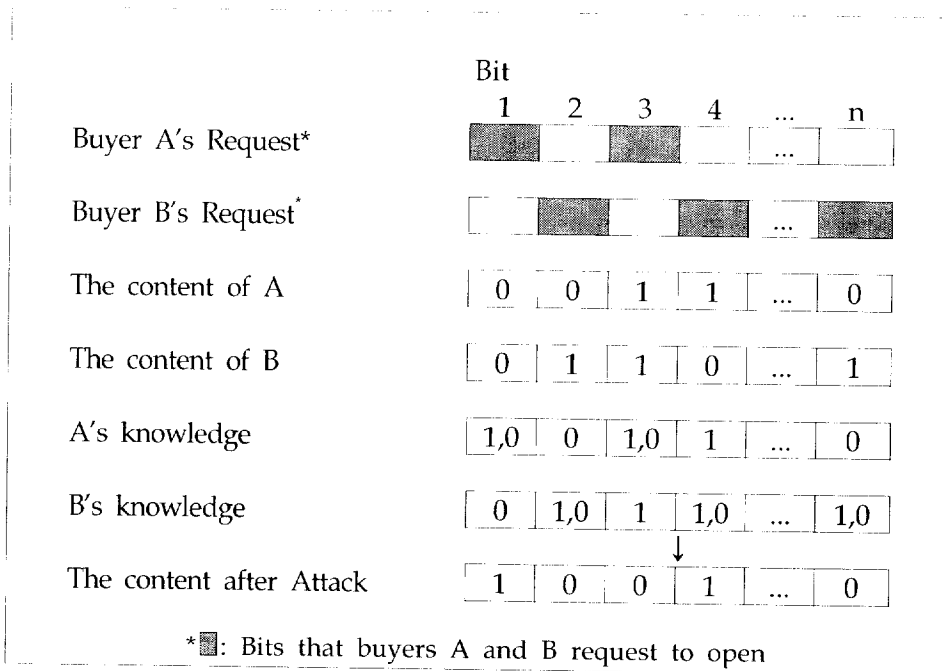
sions of contents' each bits in Sadeghi's scheme [21], [25,26].

### ■ Observation on Security

Sadeghi insisted that his scheme solved security problem of Domingo-Ferrer's scheme to open some pairs of commitments inputs to COT in the fingerprinting step or a dispute one.

Let's consider the following case. The buyer (Alice) will request to open special bits (for example even bits) and the buyer (Bob) will also request to open special bits (for example odd bits). The seller cannot know that Alice and Bob is the same buyer (of course, two buyers (Alice and Bob) can collude. The seller cannot also know they will collude in this case.) because buyers use the different anonymous identity using one-time registration in the anonymous schemes. Then the buyer can obtain two versions of all bits and can create another contents that are not assigned to her/him. Of course the collusion of over two buyers makes it possible.

On the other hand, there is the case that the seller can know all bits to be opened in advance. In the case, the buyer and the seller agree on open bits before oblivious transfer protocol execution. Then the seller inputs not two versions of  $item_i$  but a version of  $item_i$  to the bits positions not requested. In other words, he cheats buyers by inputting same value at the specific location. Thus the seller can know the buyer's some fingerprint and can combine it with the other buyers' some



**Figure 4.** Conspiracy attack by attackers A, B.

fingerprint. In the result, the seller can obtain a complete content that is mixed some buyer's fingerprint. Although the seller redistributed it for his own gain, it is possible that traitors turned out honest buyers. There is not a certain method to verify whether the seller has behaved properly. Of course the buyer can request the seller to open all pairs of commitments input in order to verify whether the seller has behaved properly. In this case, the buyer can obtain the other fingerprinted contents because the buyer knows all information (two versions) about the fingerprinted contents.

After all, it is weak against our attack and did not offer the security of buyer and seller. Figure 4 shows our attack method against

Sadeghi's scheme.

### ■ Observation on Efficiency

This scheme has complexity of  $O(nm)$  plain oblivious transfers and  $O(nm^2)$  plain bit commitments (digital contents consist of  $n$  bits and  $m$  is a security parameter) in the fingerprinting step [24] (Let see [20]). Sadeghi's scheme has to use cut and choose manner additional for opening bits (Cut and choose protocol needs much computation and many pass numbers). Thus it is unrealistic, because its round complexity is linear in the square number of bit-length of contents like Domingo-Ferrer's scheme.

A further critical issue is that the seller must contact all pseudonymous buyers during the identification step. This is again an unrealistic approach that all other proposals on anonymous fingerprinting try to avoid.

## 3.5 Analysis of Ju et al.'s Scheme [12]

Buyer-seller watermarking protocol is a combination of traditional watermarking and fingerprinting techniques. It is very similar to fingerprinting schemes. For example, in applications where multimedia content is electronically distributed over a network, the content owner can embed a distinct watermark (fingerprint), in each copy of the data

that is distributed. If unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the unique watermark corresponding to each buyer.

Ju et al. proposed an anonymous buyer-seller watermarking protocol, where a buyer can purchase contents anonymously, but the anonymity can be controlled. They used two trusted parties: the watermark certification authority and the judge. The significance of this protocol is that it offered anonymity to watermarking protocol.

In the following, we describe and analyze this scheme.

### 3.5.1 Overview

#### ■ Preprocessing

All participants have a pair of a private key and a public key  $(x, y)$  certificated by certificate authority (CA).

#### ■ Step 1. Watermark Generation

1. A buyer generates an anonymous key pair of a private key and a public key  $(\overline{x}_B, \overline{y}_B)$ . A buyer generates  $C = E_{y_j}(\overline{x}_B)$  and *cert* proving that  $\overline{x}_B$  is a discrete logarithm or e-th root of a given  $\overline{y}_B$  without disclosing  $\overline{x}_B$  using a verifiable encryption scheme. In here,  $y_j$  is the public key of the judge. After the buyer transmits

$C, \overline{y_B}, \text{sign}_{x_B}(\overline{y_B})$ : signature of  $\overline{y_B}$  and the certificate *cert* to the watermark certification authority.

2. The authority verifies the certificate. If it is verified, the watermark certification authority is convinced that  $C$  is indeed the encryption of  $\overline{x_B}$ . Then, the watermark certification authority generates a watermark  $W = \{w_0, w_2, \dots, w_{n-1}\}$  randomly and sends to the buyer the anonymous public key  $\overline{y_B}$  and the watermark encrypted with the buyer's anonymous public key  $ew = E_{\overline{y_B}}(W)$  along with  $s = \text{sign}_{x_W}(ew \parallel \overline{y_B})$ , which certifies the validity of the watermark and also ensures that  $\overline{y_B}$  was used to encrypt  $W$  as public key. The watermark certification authority stores  $B, ew, s, \overline{y_B}, \text{sign}_{x_B}(\overline{y_B})$  and  $(C, \text{cert})$  in his secret database,  $Table_W$ . Here  $\parallel$  denotes a concatenation and the used encryption algorithm is homomorphic.

**Definition 3.1** The idea of the verifiable encryption scheme is that if A and B wish to exchange their signatures on some message, they will first exchange verifiable encryption of them, using  $E$  as the public key of some trusted third party. If this was successful, it will be safe for A to just reveal his signature to B. Even if B never answers, A can get B's signature by having the trusted party decrypt it [27].

**Definition 3.2** Encryption function  $E: G \rightarrow R$  defined on a group  $(G, \cdot)$  is said to be homomorphic if  $E$  forms a homomorphism. That is, given  $E(x)$  and  $E(y)$  for some unknown  $x, y \in G$ , anyone can compute  $E(x \cdot y)$  without any need for the secret key. In other words, by privacy homomorphism with respect to  $\otimes$ , it means it has the property that  $E_k(x \otimes y) = E_k(x) \otimes E_k(y)$ .

## ■ Step 2. Watermark Insertion

1. A buyer sends  $\overline{y_B}, E_{y_B}^-(W), s$  to the seller to obtain a watermarked content.
2. By verifying the signature with the watermark certification authority's public key, the seller is convinced of the watermark's validity. If the verification holds, the seller generates a unique watermark  $V$  and embeds it into multimedia content  $X$ . Let  $X'$  be the watermarked content with  $V$ . To embed the second watermark  $W$  generated by the watermark certification authority into  $X'$  without decrypting  $E_{y_B}^-(W)$ , the seller encrypts the watermarked content  $X'$  with  $\overline{y_B}$  and finds the permutation  $\sigma$  satisfying  $\sigma(E_{y_B}^-(W)) = E_{y_B}^-(\sigma(W))$ . Because of the homomorphic property of the encryption algorithm  $E$  used by the watermark certification authority, the seller can compute watermarked content  $E_{y_B}^-(X'')$ . Where  $\otimes$  denotes the embedding operation. The seller transmits the computed  $E_{y_B}^-(X'')$  to the buyer and stores  $\overline{y_B}, ew, s, \sigma$  and  $V$  in his/her table  $Table_B$ .

$$\begin{aligned}
 E_{y_B}^-(X'') &= E_{y_B}^-(X') \otimes \sigma(E_{y_B}^-(X)) = E_{y_B}^-(X \otimes V) \otimes E_{y_B}^-(\sigma(W)) \\
 &= E_{y_B}^-(X \otimes V \otimes \sigma(W))
 \end{aligned}$$

### ■ Step 3. Copyright Violator Identification

When an illegal copy  $Y$  of an original content  $X$  is discovered, the seller extracts the unique watermark  $U$  in  $Y$  using detection algorithm. Then, he/she finds the buyer's information  $\overline{y_B}, ew, s, \sigma$  stored with  $V$  with the highest correlation by examining the correlations of extracted watermark  $U$  and all  $V$ 's in the  $Table_B$ . And the seller sends them with  $X, Y$  to the judge. The judge verifies  $sign_{x_B}(\overline{y_B})$  and  $cert$  with the help of the watermark certification authority, and recovers the buyer's anonymous private key  $\overline{x_B}$ . If the verification succeed, judge computes  $\sigma(W)$  and checks the existence of  $\sigma(W)$  in  $Y$  by extracting the watermark from  $Y$  and estimating its correlations with  $\sigma(W)$ . If there exists  $\sigma(W)$ , the buyer is guilty and the buyer's ID is revealed to the seller.

### 3.5.2 Observation on Security and Efficiency

#### ■ Observation on Security

This scheme is very efficient in the sense that identification protocol is carried out without any help of the accused buyer. But the most undesirable issue of Ju et al.'s scheme [12] is that the seller can recreate the buyer's copy if he colludes with the watermark certification authority and the judge. Thus the seller can cheat an honest buyer in this

**Definition 3.3** 'Conspiracy attack' means that a seller colludes with the watermark certification authority or the judge in order to recreate buyer's copy for his gain or a buyer colludes with these two parts in order to remove his/her fingerprint from recreated copies for their bad purposes.

scheme. In the following, we describe our two attack methods [28-30].

■ **Conspiracy Attack I: *Collusion of the Seller, the Watermark Certification Authority and the Judge***

To forge illegal copy,  $Y$  with the special watermark  $W$ , first the seller sends  $\overline{y_B}$ ,  $s$  received from a buyer to the watermark certification authority. The watermark certification authority searches for the buyer's information,  $ew = E_{y_B}^-(W)$ ,  $C = E_{y_j}(\overline{x_B}, \overline{y_B})$ , corresponding with  $\overline{y_B}$ ,  $s$  in  $Table_W$  and sends them,  $C$ , to the judge. The judge decrypts  $C$  and sends  $\overline{x_B}$  to watermark certification authority. The watermark certification authority decrypts  $ew$  using  $\overline{x_B}$  received from the judge and sends it to the seller. Then, the seller can recreate the buyer's copy because he/she knows the buyer's unique watermark,  $W$ .

### ■ Conspiracy Attack II: Collusion of the Seller and the Judge

Ju et al., insists that only the buyer can decrypt the watermarked contents, because the watermarked content  $E_{y_B}^-(X'')$  encrypted with the buyer's anonymous public key  $\overline{y_B}$ . However in this protocol, a seller can obtain  $C = E_{y_j}(\overline{x_B}), \overline{y_B}$  transmitted through insecure channel in the watermark generation protocol. If a seller obtains  $C, \overline{y_B}$ , she/he searches the buyer's record corresponding with  $\overline{y_B}$  at  $Table_B$  and sends  $C, E_{y_B}^-(X'')$  to the judge. These are just plain texts in the view of the judge. Thus the seller (or the judge) can decrypt the buyer's copy  $X''$ .

In this scheme, the seller cannot obtain proof of treachery, because the accused buyer can claim that the unauthorized copy was created by the seller. After all, Ju et al.'s scheme is weak against conspiracy attack. Of course, Ju et al.'s scheme assumes that the watermark certification authority and the judge are TTP and do not collude with a seller. But in principle, in the model for anonymous protocol the trust in the authority should be minimal. Note that when talking about attackers we also mean collusion of sellers and watermark certification authority and the judge. In other words, the seller must be able to execute all processes securely without compromising her private key even if the attacker is a trust center.

## ■ Observation on Efficiency

Ju et al.'s scheme is based on public key encryption schemes with homomorphic property and a verifiable encryption schemes [27]. It presupposes an additional condition such as existence of the secure verifiable encryption scheme compared with Memon and Wong's scheme [10] (Memon and Wong's scheme is based on the public key encryption schemes with homomorphic property and Cox's algorithm [22]). In [12], a verifiable encryption scheme is used in order to carry out identification protocol without any help of the accused buyer. But, a verifiable encryption scheme must take some care needs such as the secure hash function etc., to avoid that one party falsely accuses the other of cheating [27].

The next undesirable point is protection of the buyer's anonymity. Most of anonymous protocols minimize the possibility of a buyer's real ID's exposure: the pseudonym of a buyer is only known to an authority (normally registration center - watermark certification authority in [12]). But in this protocol, both the watermark certification authority and the judge can know the buyer's real ID corresponding with the buyer's anonymous public key. Besides, the judge of Ju et al.'s scheme should be restricted. The judge that buyers chose in the watermark generation protocol must take part in identification protocol in order to identify a copyright violator. In comparison with other anonymous protocols (Whoever is honest can be an arbiter), Ju et al.'s scheme is inefficient in this aspect.

## 3.6 Analysis of Goi et al.'s Scheme [31]

Recently, Goi et al. proposed a new anonymous buyer-seller watermarking protocol where the buyer is allowed to generate his own secret watermark. The authors insisted that their scheme protected the buyer's security from conspiracy attack. However their scheme is also insecure. In the following, we will review and analyze it.

### 3.6.1 Overview

#### [Notations]

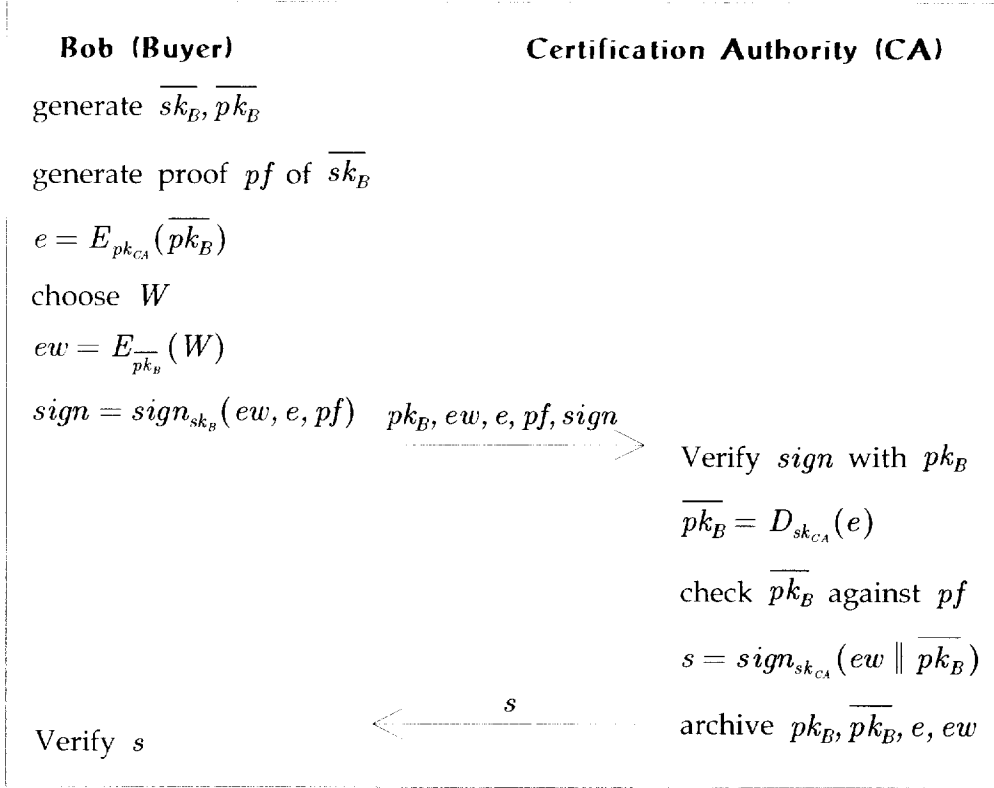
- $A$  Alice, the seller who sells the digital multimedia content
- $B$  Bob, the buyer who can buy contents anonymously
- $CA$  Certification authority who can issue the certificate and a pair of keys  $(pk, sk)$  for every agent in the PKI
- $X$  Original content with  $m$  elements  $x_1, x_2, \dots, x_m$
- $W$  Watermark with  $n$  elements  $w_1, w_2, \dots, w_n$
- $X', X''$  Watermarked content
- $X \otimes W$  Embed  $W$  into  $X$  with the embedding operation  $\otimes$
- $\sigma$  Random permutation function chosen by Alice
- $cert$  A certificate computed by Bob
- $E(.) / D(.)$  Encryption/Decryption algorithm of a public-key with homomorphic property

## ■ Step 1. Watermark Generation

The buyer, Bob enlists the help of a certification authority, CA to certify his chosen anonymous public key,  $\overline{pk_B}$ . In this way, only CA knows where  $\overline{pk_B}$  came from. CA is the one who issues public key certificates containing public and private key-pairs of all agents (including Alice, Bob and Carol) in a public key infrastructure (PKI) and hence is definitely trustable, otherwise PKI would be secure and no public and private key-pairs would be binding or confidential. There is no need for a separate watermark certification authority. The watermark generation phase is given in Figure 5.

## ■ Step 2. Watermark Insertion

1. B sends  $\overline{pk_B}$ ,  $ew$ ,  $s$  to A to obtain a watermarked content.
2. By verifying the signature with CA's public key, A is convinced of the watermark's validity. If the verification holds, A generates a unique watermark  $V$  and embeds it into multimedia content  $X$ . B uses Cox's scheme as the embedding algorithm [22]. To embed the second watermark  $W$  into  $X'$  without decrypting  $E_{\overline{pk_B}}(W)$ , A encrypts the watermarked content  $X'$  with  $\overline{pk_B}$  and finds the permutation  $\sigma$  satisfying  $\sigma(E_{\overline{pk_B}}(W)) = E_{\overline{pk_B}}(\sigma(W))$ . Because of the homomorphic property of the encryption algorithm  $E$ , A can com-



**Figure 5.** Watermark generation of Goi et al.'s scheme [31].

pute watermarked content  $E_{\overline{pk_B}}(X'')$ . A transmits the computed  $E_{\overline{pk_B}}(X'')$  to the buyer and stores  $\overline{pk_B}, ew, s, \sigma$  and  $V$  in his table  $Table_B$ .

$$\begin{aligned}
 E_{\overline{pk_B}}(X'') &= E_{\overline{pk_B}}(X') \otimes \sigma(E_{\overline{pk_B}}(X)) \\
 &= E_{\overline{pk_B}}(X \otimes V) \otimes E_{\overline{pk_B}}(\sigma(W)) \\
 &= E_{\overline{pk_B}}(X \otimes V \otimes \sigma(W))
 \end{aligned}$$

### ■ Step 3. Copyright Violator Identification

When Bob is suspected, the judge will request by law for him to disclose the unique self-generated watermark,  $W$  and then compute the deterministic encryption  $E_{pk_B}^d(W)$ . The result is compared with the stored  $ew$  in the CA's database, whose integrity can be validated by using  $s$ : (1) if they are not the same, B will be guilty because of giving a fraudulent watermark, (2) if yes, then, the judge will proceed to extract the embedded watermark in multimedia content. Finally, the extracted watermark is compared with  $\sigma(W)$ . If they match, then B is guilty, otherwise B is innocent. Alice is not able to recreate  $X''$  because she does not know the unique watermark  $W$ .

### 3.6.2 Observation on Security

The scheme is meaningful in the sense that it provides true anonymity. The previous schemes only provide "partial" anonymity. That is, the buyer's anonymity is guaranteed only if watermark certification authority is honest. But Goi et al.'s scheme is insecure if buyers are collude. In the following, we prove it.

The authors insisted that their scheme removed possibility of conspiracy attack between a seller and a watermark certification authority by means that the buyer generates his own secret watermark. But their means causes collusion attack among buyers. We conducted an experi-

ment in order to prove insecurity of Goi et al.'s scheme as follows.

Suppose that two buyers, Bob and Carol, intend to collude in order to recreate another content that is not assigned to them. They use average attack for their successful attack.

### ■ Bob

1. Bob generates  $\overline{sk_B}, \overline{pk_B}$  and generates proof  $pf_1$  of  $\overline{sk_B}$ . He computes  $e_1$  and chooses watermark,  $W_1 = \{w_1, w_2, \dots, w_n\}$ .

$$e_1 = E_{pk_{CA}}(\overline{pk_B}), \quad ew_1 = E_{pk_B}(W_1)$$

$$sign_1 = sign_{sk_B}(ew_1, e_1, pf_1)$$

He sends  $pk_B, ew_1, e_1, pf_1, sign_1$  to CA.

2. CA verifies  $sign_1$  with  $pk_B$ , and checks  $\overline{pk_B}$  against  $pf_1$ . If they are verified, CA computes  $s_1$  and sends it to Bob.

$$s_1 = sign_{sk_{CA}}(ew_1 \parallel \overline{pk_B})$$

CA stores  $pk_B, \overline{pk_B}, e_1, ew_1$ .

3. Bob verifies  $s_1$ .
4. Bob sends  $\overline{pk_B}, ew_1, s_1$  to a seller to obtain a watermarked content.
5. By verifying the signature with CA's public key, the seller is convinced of the watermark's validity. If the verification holds, the seller generates a unique watermark  $V_1$  and embeds it into multi-

media content  $X$ . To embed the second watermark  $W_1$  into  $X'$ , the seller encrypts the watermarked content  $X'$  with  $\overline{pk_B}$  and computes  $\sigma_1(E_{\overline{pk_B}}(W_1))$ . The seller transmits the computed  $E_{\overline{pk_B}}(X'')$  to Bob and stores  $\overline{pk_B}, ew_1, s_1, \sigma_1$  and  $V_1$  in his table  $Table_B$ .

$$E_{\overline{pk_B}}(X'') = E_{\overline{pk_B}}(X \otimes V_1 \otimes \sigma_1(W_1))$$

6. Bob decrypts it.  $D_{\overline{sk_B}}(E_{\overline{pk_B}}(X'')) = X \otimes V_1 \otimes \sigma_1(W_1)$ .

## ■ Carol

1. Carol generates  $\overline{sk_C}, \overline{pk_C}$  and generates proof  $pf_2$  of  $\overline{sk_C}$ . He computes  $e_2$  and chooses watermark,  $W_2$ .

$$W_2 = -W_1 = \{-w_1, -w_2, \dots, -w_n\}.$$

$$e_2 = E_{\overline{pk_{CA}}}(\overline{pk_C}), \quad ew_2 = E_{\overline{pk_C}}(W_2)$$

$$sign_2 = sign_{\overline{sk_A}}(ew_2, e_2, pf_2)$$

He sends  $\overline{pk_C}, ew_2, e_2, pf_2, sign_2$  to CA.

2. CA verifies  $sign_2$  with  $\overline{pk_C}$ , and checks  $\overline{pk_C}$  against  $pf_2$ . If they are verified, CA computes  $s_2$  and sends it to Carol.

$$s_2 = sign_{\overline{sk_{CA}}}(ew_2 \parallel \overline{pk_C})$$

CA stores  $\overline{pk_C}, \overline{pk_C}, e_2, ew_2$ .

3. Carol verifies  $s_2$ .
4. Carol sends  $\overline{pk_C}, ew_2, s_2$  to a seller to obtain a watermarked content.
5. By verifying the signature with CA's public key, the seller is convinced of the watermark's validity. If the verification holds, the seller generates a unique watermark  $V_2$  and embeds it into multimedia content  $X$ . To embed the second watermark  $W_2$  into  $X'$ , the seller encrypts the watermarked content  $X'$  with  $\overline{pk_C}$  and computes  $\sigma_2(E_{\overline{pk_A}}(W_2))$ . The seller transmits the computed  $E_{\overline{pk_A}}(X'')$  to Alice and stores  $\overline{pk_A}, ew_1, s_1, \sigma_2$  and  $V_1$  in his table  $Table_B$ .  

$$E_{\overline{pk_C}}(X'') = E_{\overline{pk_C}}(X \otimes V_2 \otimes \sigma_2(W_2))$$
6. Carol decrypts it.  $D_{sk_C}(E_{\overline{pk_C}}(X'')) = X \otimes V_2 \otimes \sigma_2(W_2)$ .

### ■ Bob and Carol

Bob and Carol recreates another content,  $X^{red}$ , by averaging their each content.

$$X^{red} = \frac{X \otimes V_1 \otimes \sigma_1(W_1) \otimes X \otimes V_2 \otimes \sigma_2(-W_1)}{2}$$

The content,  $X^{red}$ , can be presented in two cases according to  $\sigma$  that the seller chose.

**Case 1.  $\sigma_1 = \sigma_2$ :** In this case, the buyers, Bob and Carol, can remove their unique watermarks in the recreated content,  $X^{red}$ .

$$X^{red} = \frac{X \otimes V_1 \otimes \sigma_1(W_1) \otimes X \otimes V_2 \otimes \sigma_1(-W_1)}{2} = X \otimes \frac{V_1 \otimes V_2}{2}.$$

Thus, even if the seller finds illegal copy  $X^{red}$  after, he can not identify Bob or Carol as a copyright violator. Because  $X^{red}$  does not contain  $W_1, W_2$ . In addition, because  $V_1$  and  $V_2$  are known to both Bob(Carol) and the seller, it is insufficient to prove that either Bob or Carol distributed  $X^{red}$  illegally. The simulation result is shown in Table. 2. In order to evaluate the proposed attack, we take the "lena" of Figure 6-(a) and produce the watermarked image of Figure 6-(d) by averaging two watermarked images of Figure 6-(b) and 6-(c). If  $W^{red}$  extracted from  $X^{red}$  differs from  $W_1$  or  $W_2$ , it is highly unlikely that  $W^{red}$  will be identical to the buyers' watermark,  $W_1, W_2$ .



(a) Original image.



(b) Bob's watermarked image.



(c) Carol's watermarked image.



(d) Watermarked image  $X^{red}$ .

**Figure 6.** Each image in our Case 1 attack against Goi et al.'s scheme.

We measure the similarity of  $W$  and  $W'$  by  $sim(W, W') = \frac{X \cdot X'}{\sqrt{X' \cdot X'}}$ . If the similarity is greater than 6, it has corresponding watermark with illegal content.

**Table 2.** The experiment results of Case 1.

Similarity		Ju et al.,'s Scheme [12]	Goi et al.,'s Scheme [31]
$W_1$ from Bob's image	$W_1$	33.288	33.288
	$W_2$	0.6	0.6
$W_2$ from Carol's image	$W_1$	0.56	0.56
	$W_2$	33.288	33.288
$W^{red}$ from $X^{red}$	$W_1$	24.041	<b>1.67</b>
	$W_2$	21.445	<b>-1.67</b>

**Case 2.**  $\sigma_1 \neq \sigma_2$ : In this case, the buyers, Bob and Carol, generate their unique watermarks under the condition,  $0.9 \leq |w_i| \leq 1$  to make correlation between  $W_1, W_2$  and the extracted information from  $X^{red}$  to be low.

$$X^{red} = \frac{X \otimes V_1 \otimes \sigma_1(W_1) \otimes X \otimes V_2 \otimes \sigma_1(-W_1)}{2}.$$

Our experiment shows that there has no correlation between  $W_1, W_2$  and the extracted information from  $X^{red}$ . Basically, the watermark,  $W_1, W_2$ , must consist of a pseudo-random sequence of length  $n$ , each value is a random real number with a normal distribution having mean 0 and variance 1. But, because the watermark is encrypted and the encrypted watermark is sent to CA and the seller, they cannot check the validity of the watermark. Thus two buyers abuse this point

and can make another content that is not assigned to them. The simulation result of case 2 is shown in Table. 3. Likewise of the case 1, we take the "lena" of Figure 6-(a) and produce the watermarked image of Figure 7-(c) by averaging two watermarked images of Figure 7-(a) and 7-(b). If the similarity is greater than 6, it has corresponding watermark with illegal content.



(a) Bob's watermarked image. (b) Carol's watermarked image.



(c) Watermarked image  $X^{red}$ .

**Figure 7.** Each image in our Case 2 attack against Goi et al.'s scheme.

**Table 3.** The experiment results of Case 2.

Similarity		Goi et al.,’s Scheme [31]
$W_1$ from Bob’s image	$W_1$	29.658
	$W_2$	0.6
$W_2$ from Carol’s image	$W_1$	0.54
	$W_2$	29.658
$W^{red}$ from $X^{red}$	$W_1$	<b>3.443</b>
	$W_2$	<b>3.443</b>

It was found from the results that Goi et al.,’s scheme did not prove security of sellers and buyers. Thus Goi et al.,’s scheme is insecure contrary to the designers’ original claim.

### 3.7 Our Proposal

In this section, we solve the previous schemes’ problems mentioned in the previous section. That is, we suggest how to make secure fingerprinting schemes against the dishonesty of sellers and buyers [25,26],[32].

#### 3.7.1 Our Methodology

##### ■ Oblivious Transfer using Two-lock Cryptosystem

We introduce oblivious transfer using two-lock cryptosystem in order to prevent the dishonesty of buyers or sellers. The  $t$ -out-of- $n$  oblivious

transfer of Qian-Hong Wu et al. is applied to the fingerprinting step of our scheme. To our best knowledge, a more efficient protocol for OT was presented as "Oblivious Transfer Using Two-Lock Cryptosystem" in [33]. We assume that this protocol is secure, and the security proof is given in the same paper.

Let Alice possess  $n$  (string) secret  $m_1, m_2, \dots, m_n$  and be willing to reveal  $t$  secret of them to Bob. Suppose Bob is interested in secrets  $m_{i_1}, m_{i_2}, \dots, m_{i_t}$ . Assume that Alice chooses her random secret key  $k$  and Bob chooses secret keys  $s_1, s_2, \dots, s_t$ . It is convenient to implement  $t$ -out-of- $n$  OT using two-lock cryptosystem as follows.

1. Alice sends Bob:  $Y_1 = A_k(m_1), \dots, Y_n = A_k(m_n)$ .
2. Bob sends Alice:  $Z_1 = B_{s_1}(Y_{i_1}), \dots, Z_t = B_{s_t}(Y_{i_t})$ .
3. Alice sends Bob:  $C_1 = A_k^{-1}(Z_1), \dots, C_t = A_k^{-1}(Z_t)$ .
4. Bob decrypts:  $m_{i_1} = B_{s_1}^{-1}(C_{i_1}), \dots, m_{i_t} = B_{s_t}^{-1}(C_{i_t})$ .

Here,  $A_k(\cdot), B_s(\cdot)$  are the different encryption algorithm and  $A_k^{-1}(\cdot)$  denotes the decryption of  $A_k(\cdot)$ . Bob can decrypt the cipher text  $C$  and reveal the message  $m = B_k^{-1}(C)$ . In case that  $A = B$ , it is also known as commutative encryption [34]. To achieve sending

privacy, Alice's encryption algorithm should meet the security requirements: given  $C_1, Z_1, \dots, C_t, S_{i'}$  it is infeasible to find  $k'$  satisfying  $C_1 = A_{k'}^{-1}(Z_1), \dots, C_t = A_{k'}^{-1}(Z_t)$ . In our protocol, we use this protocol based on discrete logarithm, which is secure unless an adversary could compute discrete logarithm. Also we assume that  $A_k(\cdot), B_s(\cdot)$  are deterministic mappings. It should be noticed that in [34], there are two variants of two-lock encryption based on the discrete logarithm problem, and one of these scheme is deterministic.

### ■ Watermarking algorithm

The second idea is that we use Cox's algorithm [22] which has high resistant against collusion attack instead of Boneh and Shaw's code as a building block for collusion tolerance in order for efficient identification process. In [22], watermark  $W = \{w_1, \dots, w_m\}$  consists of a pseudo-random sequence of length  $m$ , each value  $w_i$  is a random real number with a normal distribution having mean 0 and variance 1. In order to place a length  $m$  watermark into an  $N \times N$  image, they computed the  $N \times N$  DCT of the image. Then they placed the watermark into the  $m$  highest magnitude coefficients of the transform matrix, excluding the DC component. That is, the watermark  $W$  is inserted into the largest  $m$  AC coefficients  $\{h_1, \dots, h_m\}$ . The watermarked sequence  $H' = \{h'_1, \dots, h'_m\}$  is obtained according to

$h'_i = h_i \cdot (1 + \alpha w_i)$ ,  $i = 1, 2, \dots, m$ . Where  $\alpha$  is the scaling parameter.

To determine if a given image  $Y$  contains the watermark  $W$ , the decoder extracts  $T = \{t_1, \dots, t_m\}$  from  $Y$  by taking the largest  $m$  DCT AC coefficients of  $Y$  and subtracting their values from  $h_i$ . That is  $t_i = h_i - y_i$ . The confidence measure on the presence of the watermark  $W$  in  $Y$  is taken to be the correlation between  $W$  and  $T$ .

Results reported using the largest 1000 AC coefficients show the technique to be remarkably robust against various image processing operations, and also after printing and rescanning [35]. If we use this algorithm, sellers can identify the traitor by estimating watermark's correlations between the redistributed copy and assigned watermark without the help of buyers. Of course, if any watermarking algorithm is secure against collusion attack, the algorithms can also be used in our scheme.

### 3.7.2 Proposed Scheme

#### [Outline]

The proposed scheme consists of the following steps: Buyer registration step for buyer's pseudonym, fingerprinting step for making a fingerprinted contents and identification step for identification of the traitor.

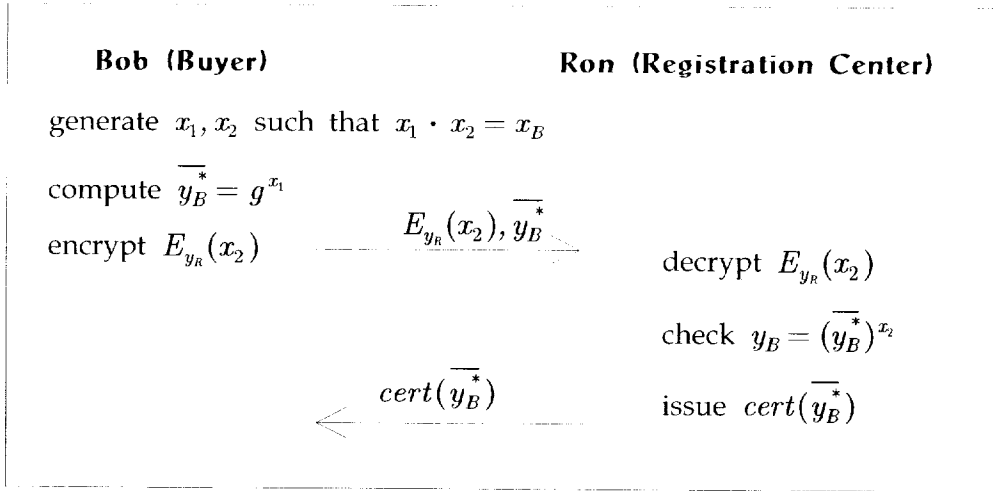
### [Preprocessing]

Let  $p \leq n$  (*bits*) be a large prime such that  $q = (p - 1)/2$  is also a prime. Let  $G$  be a group of order  $p - 1$  and let  $g$  be a generator of  $G$  such that computing discrete logarithms to the base  $g$  is difficult.

### [Notations]

We assume that the content being sold is a still image, though in general the protocol is also applicable to audio and video contents for ease of exposition. We establish some notation as follows.

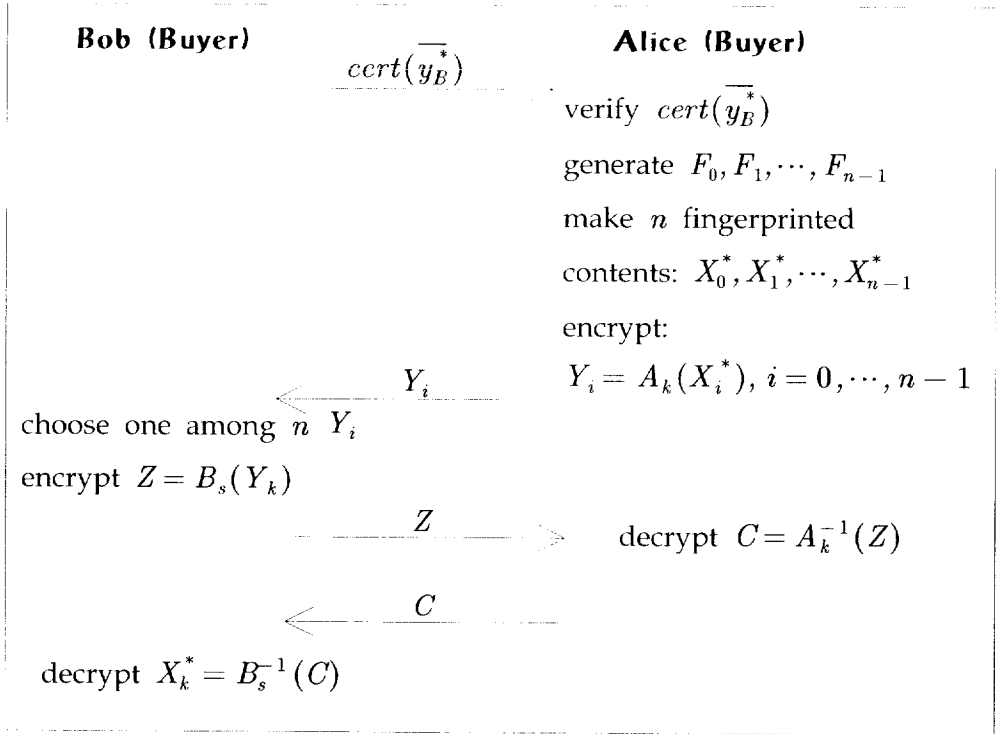
- Alice                      The seller who sells the digital multimedia content
- Bob                        The buyer who can buy contents anonymously
- Ron                        A registration center
- $x_A/y_A$                   Private key/Public key corresponding with  $x_A$  of Alice
- $x_B/y_B$                   Private key/Public key corresponding with  $x_B$  of Bob
- $x_R/y_R$                   Private key/Public key corresponding with  $x_R$  of Ron
- CA                        Certification authority who can issue the certificate and a pair of keys  $(x, y)$  for every agent in the PKI
- $X$                         Original content with  $m$  elements  $x_1, x_2, \dots, x_m$
- $E_a(\cdot)/E_a^{-1}(\cdot)$     Encryption/Decryption algorithm with secret key  $a$ .
- $Sign_a(\cdot)$               Signature algorithm with private key  $a$ .



**Figure 8.** Buyer registration step of our first proposal.

### ■ STEP 1. Buyer Registration

1. The buyer (Bob) chooses secret random  $x_1, x_2$  in  $Z_p$  such that  $x_1 \cdot x_2 = x_B \in Z_p$ . Bob sends  $y_B, \overline{y_B^*}$  ( $\overline{y_B^*} = g^{x_1}$ ) and  $x_2 (E_{y_R}(x_2))$  encrypted by using the Registration Center's (Ron) public key  $y_R$ . Bob convinces Ron of zero-knowledge of possession of  $x_1$ . The proof given in [36] for showing possession of discrete logarithms may be used here.
2. Ron decrypts  $E_{y_R}(x_2)$  and checks that  $y_B = (\overline{y_B^*})^{x_2}$ . If it is verified, Ron returns to Bob a certificate  $cert(\overline{y_B^*})$ . The certificate states the correctness of  $\overline{y_B^*}$ .



**Figure 9.** Fingerprinting step of our first protocol.

## ■ STEP 2. Fingerprinting

Bob sends  $cert(\overline{y_B^*})$  to a seller (Alice). If it is verified, Alice generates valid  $n$  fingerprints,  $F_0, F_1, \dots, F_{n-1}$ , randomly. She must generate different  $n$  fingerprints to all buyers. Each fingerprint  $F_i$  of our protocol and  $W$  of Cox's scheme have the same property. Then she makes  $n$  copies to embed each fingerprint  $F_i$ . All copies have different embedding information (fingerprint). Alice stores records  $cert(\overline{y_B^*}), \overline{y_B^*}, F_0, \dots, F_{n-1}$  at her table  $Table_A$ . Next, Alice and Bob execute OT with two-lock cryptosystem as follows.

1. Alice encrypts  $n^*$  copies (fingerprinted contents) with her secret key  $k$  and sends Bob:

$$Y_0 = A_k(X_0^*), \dots, Y_{n-1} = A_k(X_{n-1}^*)$$

2. Bob chooses one among them. Suppose Bob chose  $Y_2$ . Then he re-encrypts it with his secret key  $s$  and sends it back to Alice:  $Z = B_s(Y_2)$ . Now Bob cannot know the hidden fingerprint because they are encrypted with Alice's key but he can verify that Alice did not encrypt the same contents (that is embedded same fingerprint into original contents).
3. Alice stores records  $Z$  at her table  $Table_A$  and sends Bob:  $C = A_k^{-1}(Z)$ . Alice also cannot know which fingerprinted contents Bob chose because it is encrypted with Bob's secret key.
4. Bob decrypts and uses:  $X_2^* = B_s^{-1}(C)$ .

### ■ STEP 3. Traitor Identification

After finding a redistributed copy  $X^{red}$ , Alice extracts the unique fingerprint  $G$  in  $X^{red}$ . For robust fingerprint embedding algorithm, by computing correlations of extracted fingerprint  $G$  and every fingerprint stored in  $Table_A$ , Alice finds  $F_i$  with the highest correlation and ob-

\* Here, Alice generates  $n (\geq 2)$  fingerprints, where Bob would choose one out of  $n$  fingerprinted contents. The choice of  $n$  implies a trade off between correctness and efficiency. In such case, probability of Alice knowing which fingerprinted contents Bob chose would be equal to  $1/n$ .

tains the transaction information involving  $F_i$  from the table. The information consists of  $\text{cert}(\overline{y_B^*}), \overline{y_B^*}, Z$ . Alice sends them and the redistributed copy to an arbiter. The arbiter verifies the presence of  $F_i$  in the  $X^{\text{red}}$ , if it is checked, he asks the real identity of the traitor to Ron. Thus the seller can identify the traitor.

If the accused buyer cannot agree with the arbiter's decision, he sends his own contents to arbiter (or the arbiter asks the buyer  $Z$  and the buyer must open  $Z$ ). If the same  $F_i$  indeed presents in the accused buyer's contents or  $Z$ , he is found guilty otherwise he is innocent.

### 3.7.3 Features and Security Analysis

We discuss and analyze features and security of the proposed scheme according to the list of requirements (Chapter 2). We assume that all of the underlying primitives are secure. Security of our scheme relies on that of the underlying watermarking algorithm and cryptosystem.

- **Anonymity:** We assume that the registration center does not reveal the buyer's real ID if the buyer is honest. In fingerprinting step, the seller knows  $\overline{y_B^*}$ . Finding  $y_B$  would require knowledge of  $x_2$ . However, if the encryption algorithm is secure, the only way for

the seller to find  $x_2$  is to compute  $\log_g \overline{y_B^*}$ . But polynomial algorithm proving discrete logarithm problem does not exist, so attacker (seller) does not compute  $x_2$ . Thus buyer anonymity is guaranteed.

- **Unlinkability:** Because our scheme executes one-time registration generation protocol whenever the buyer buys a content (By going through the registration step several times, the buyer can obtain several different certified keys  $\overline{y_B^*}$ ). This implies that the buyer's purchases are unlinkable.
- **Traceability:** Due to the properties of the underlying encryption, we can assume that a malicious buyer cannot change or substitute a fingerprint generated by the seller. Further a detecting function in the fingerprint detection must guarantee that the seller can extract the unique fingerprint  $F_i$  that belong to a traitor. Besides, the buyer cannot remove the fingerprint  $F_i$  because he does not know  $F_i$ . Thus the buyer who has distributed digital contents illegally can be traced in our scheme.
- **No Framing:** Since, to forge  $Y$  with the special fingerprint  $F_i$ , the seller must know either the buyer's private key  $s$ . In our pro-

posal, only the buyer knows his secret key  $s$  if computing discrete logarithm is hard and encryption algorithm (underlying primitives) is secure. Since we use secure oblivious transfer with two-lock cryptosystem in the fingerprinting step, the seller cannot know which fingerprinted contents buyers selected. And the seller cannot input the same values in the execution of OT because all inputs are received to the buyer and the buyer checks them. Thus an honest buyer should not be wrongly identified as a traitor, because the others cannot recreate the buyer's copy with specific fingerprint.

- **No Repudiation:** The buyer accused of reselling an unauthorized copy cannot claim that the copy was created by the seller or a security breach of the seller's system. Since only the buyer knows his secret key  $s$  and his unique fingerprinted contents  $X_i^*$ , the others cannot recreate the buyer's copy.
- **Collusion Tolerance:** Our scheme has used Cox's algorithm as a building block. We assumed that this algorithm is secure. And this algorithm is estimated to be highly resistant to collusion attacks [35]. Our protocol is secure only as much as the underlying watermarking techniques are secure and robust.

- *Practicality*: While computation complexity of both schemes [20,21] of fingerprinting step is  $O(nm)$  plain oblivious transfers and  $O(nm^2)$  plain bit commitments, that of our protocol is just  $t + 1$  encryptions and 2 decryptions, where  $t$  is the number of contents to be copied/fingerprinted for a content. It is not liner in the length of contents. Doing this in sequence is unrealistic in [20] and [21] schemes, because the round complexity of the algorithm is linear in the bit-length  $n$  of the contents (one should think of the size of an image). And Domingo-Ferrer's scheme [20] has 5 exponentiations, a zero knowledge proof and 4-pass number in the registration step, but our protocol has just 4 exponentiations, a zero knowledge proof and 2-pass. Besides all buyers must take part in the identification step in [20,21]. On the contrary, the seller can identify the traitor without the help of buyer in our protocol. In addition, Ju et al.'s scheme [12] needs a watermark authority as a TTP, but our scheme need not any trusted party except a judge. In the event, our scheme first reduces the round complexity and computational complexity from [20] and [21] schemes. Furthermore we improve the identification step to remove the participation of the buyers (all buyers). We design anonymous fingerprinting scheme that removes interaction property between buyers and sellers in the fingerprinting step (embedding procedure).

**Table 4.** Comparison of our proposal with the previous schemes.

Features	Our Proposal	[12] scheme	[20] scheme	[21] scheme	[31] scheme
Anonymity	○	○	○	○	○
No Framing	○	×	×	×	×
No Repudiation	○	×	×	×	×
Collusion Tolerance	○	○	×	×	○
Participators of the Identification	Seller, RC	WCA, Seller	All buyers, Seller, RC	All buyers, Seller, RC	Buyer, Seller, RC

### 3.7.4 Comparison with Previous Schemes

We compare the features of our proposal with the previous schemes in Table 4.

The most undesirable issue of the previous schemes is that they do not offer the security of buyer and seller (No Framing and No Repudiation) because the seller can know the buyer’s fingerprint if he abuses flows of COT in [20] scheme, or buyers can know both versions of contents’ each bit in [21] scheme. Ju et al.’s scheme [12] must assume that the watermark certification authority does not collude with a seller or a buyer for their protocols, and also must assume honesty of the judge. Because a buyer’s private key is encrypted with the judge’s public key, and is used for decryption of content and anonymity offer-

ing in Ju et al.'s scheme, it must not be revealed. Since we consider conspiracy attack, we described that two schemes [12],[31] did not provide security of sellers and buyers. On the contrary, our proposal offers the security of buyer and seller even if it is based on OT protocol.

Domingo-Ferrer's scheme does not offer collusion-tolerance that is an important property a fingerprinting scheme should possess and Sadeghi's scheme [21] also does not solve this problem. In fact, Domingo-Ferrer's scheme introduced the approach to use tamper-proof device such as smart card to provide collusion-tolerance. But Domingo-Ferrer's scheme just sketched it and leaves some problems such that the buyer and the seller have complete trust in the smart card and this is difficult to justify because the tamper-resistance of smart cards provides only limited security [21]. Sadeghi's scheme [21] just pointed out problems of [20] scheme and did not suggest any solutions. So we describe that collusion-tolerance in the two schemes was not offered. A further critical problem in [20] is that during the identification step the seller must contact all buyers (This problem has reported in [21] scheme, but [21] scheme has not suggested its solution).

Pfitzman and Sadeghi's scheme [18] and our scheme offer collusion-tolerance but [18] scheme has the problem that the length of code used is too long (the code needed for embedding is so long that the overall system cannot be called practical). On the other hand, our scheme uses Cox's scheme [22] for collusion-tolerance that is estimated

to be highly resistant to collusion attacks [35]. The most meaningful feature of our scheme is practicality. Since we remove interaction between the buyer and the seller in the fingerprinting step and exclude the buyer's participation from identification step.

### **3.8 Open Problems on Buyer-Seller Watermarking Protocols**

In this section, we discuss the security of previous asymmetry buyer-seller watermarking protocols. Specially, we analyze the security of protocols against chosen ciphertext attack (CCA). It is essential in designing protocols that are secure against active adversaries and is correct security definition for a cryptosystem. We show that all known asymmetry schemes based on homomorphic encryption are insecure against chosen ciphertext attacks (CCA). Our result shows that the seller can obtain the buyer's unique watermark even if it is encrypted with buyer's public key in these schemes.

Homomorphic encryption is used as a useful tool to provide buyer-seller watermarking with asymmetry property. In these protocols [10],[12],[30],[31], they embed two watermarks,  $W, V$  into one image. One is generated by the WCA for buyer's right (false-implication concern), and the other is generated by a seller for his copyright. In fact,

a buyer generates his own unique watermark  $W$  instead of the WCA, a seller generates the other watermark  $V$  in [31]. But what is important is not who does generate the watermark  $W$  but they use homomorphic encryption algorithm for embedding two watermarks in this research. Here, the seller needs to embed the encrypted watermark  $E_{y_B}(W)$  into  $X$  embedded the second watermark  $V$  without decrypting it, because the seller must not know the first watermark  $W$  for asymmetry. Thus, the purpose of  $V$  is to enable the seller to identify the specific buyer an illegal copy has potentially arisen from.

That is,  $V$  is not the watermark the seller will use to prove that the buyer has made illegal copies of an image. This is a role of the watermark  $W$ . In order to offer asymmetry, they introduced encryption scheme with asymmetry property [37,38].

Let us discuss the security of these schemes against chosen cipher attacks in detail. The most undesirable issue of previous asymmetry schemes is that they do not satisfy asymmetry requirement because of used homomorphic encryption. Thus the seller or the others (except the buyer) can cheat an honest buyer in these schemes.

To forge illegal copy  $X^{red}$  with the special watermark  $W$ , first the seller (the others except the buyer, the owner of  $W$ ) selects random number  $r$ . The others can also obtain  $E_{y_B}(W)$  are transmitted through insecure channel. Then, he computes  $r \cdot E_{y_B}(W)$  with the help of en

**Security Against Adaptive CCA:** We briefly describe it introduced by Racoff and Simon [39]. Security is defined via the following game played by the adversary.

First, the encryption scheme's key generation algorithm is run, with a security parameter as input. Next, the adversary makes arbitrary queries to a "decryption oracle", decrypting ciphertexts of his choice.

Next, the adversary choose two message,  $m_0, m_1$  and sends these to an "encryption oracle". The encryption oracle choose a bit 0, 1 at random, and encrypts  $m_b$ . The corresponding ciphertext is given to the adversary. After receiving the ciphertext from the encryption oracle, the adversary continues to query the decryption oracle, subject only to the restriction that the query must be different from the output of the encryption oracle. At the end of the game, the adversary outputs  $b'$  in 0 or 1, which is supposed to be the adversary's guess of the value  $b$ . If the probability that  $b' = b$  is  $1/2 + \epsilon$ , then the adversary's advantage is defined to be  $\epsilon$ . The cryptosystem is said to be secure against chosen ciphertext attack if the advantage of any polynomial-time adversary is negligible.

encryption oracle, and sends it decryption oracle. Decryption oracle give him its reply,  $r \cdot E_{y_B}(W)$ . Finally, he can know  $W$  using  $\frac{r \cdot W}{r}$  easily. Because these protocols used RSA scheme [37] as follows.

$$E_{y_B}(W) = W^{y_B} \rightarrow r \cdot E_{y_B}(W) = r \cdot W^{y_B}$$

$$D(r \cdot W^{y_B}) = r \cdot W \rightarrow \frac{r \cdot W}{r} = W$$

Now the seller (adversary) can recreate the buyer's copy. Thus, in these schemes, the seller cannot obtain proof of treachery, because the accused buyer can claim that the unauthorized  $X^{red}$  was created by the seller or the adversary. After all, previous asymmetry protocols used RSA scheme are weak against CCA.

In [10] scheme, they suggested that the El-Gamal cryptosystem with homomorphic property [38] can be used instead. But this scheme is also weak against CCA. We can use different homomorphic encryption algorithms instead of [37] and [38] schemes.

But, unfortunately, there are not secure homomorphic encryption schemes to be applied to watermarking protocols. Of course, there are some schemes with homomorphic property secure against chosen ciphertext attack [40-43]. [41],[42], and [43] schemes are based on factorization problem, and [40] scheme is based on the Diffie-Hellman decision problem. [40] and [42] schemes were specially suggested for threshold cryptosystems and [42] and [43] schemes considered just one

bit as message space. Thus they cannot be applied to watermarking algorithm of pixel by pixel. Because we take the two-dimensional DCT of an image and the watermark is inserted into the largest coefficients for collusion attacks. And [41] scheme keeps the homomorphic property, but the result will no longer be a ciphertext that withstands CCA. Thus we can conclude that the existing schemes with homomorphic property based on factorization problem can not be applied to asymmetry buyer-seller watermarking protocols.

### **3.9 Chapter Summary**

In this chapter, we describe secure digital fingerprinting scheme.

First, we showed some problems of the previous anonymous schemes. Then we described how to make secure fingerprinting schemes against the dishonesty of sellers and buyers in section 3.7. Here, we used oblivious transfer protocol with two lock cryptosystem to make it practical and secure.

Next, we discussed the security of buyer-seller watermarking schemes used homomorphic encryption. Most protocols used homomorphic encryption in order to provide a watermarking protocol with asymmetry property. In a buyer-seller watermarking protocol, asymmetry property is very important. Because a seller cannot prove the fact to a third party that dishonest buyers distributed content illegally if it

does not offer asymmetry property.

Though homomorphic encryption holds a key point in buyer-seller watermarking schemes, this topic has never been studied so far. Thus we dealt with this topic and pointed out that used homomorphic encryption is not secure against chosen ciphertext attacks. Our result showed that the existing schemes cannot provide asymmetry property despite of their claim. That is, because a seller can know the buyers' unique watermark, honest buyers can be found as guilty in these schemes. Design of secure digital fingerprinting scheme against CCA remains to be solved as an open problem.

# Chapter IV. A Copyright Protection Scheme for Multi-Purchase

## 4.1 Introduction

In this chapter, our concern is to generalize a buyer-seller watermarking protocol to multi-purchase environments.

### ■ Contents Sales in E-commerce

In general, E-commerce system consists of a set of contents such as image and audio, a set of sellers and a set of buyers. Each buyer wants to buy some contents from a set of sellers. If their transaction is concluded, then the sellers encrypt them with buyer's public key and send them to the buyer in a general buyer-seller watermarking protocol. When the buyer receives the encrypted contents, he has to decrypt them with his private key to use them.

### ■ Why we need novel scheme for multi-purchase

What is important in anonymous schemes is to offer anonymity of buyers and unlinkability of the contents.

Anonymity means that a buyer can buy contents anonymously, and

unlinkability means that anyone cannot determine whether the contents were purchased by the same buyer. Consider the case that the anonymity holds and the unlinkability does not hold. Then, if a party can trace the buyer from a transcript by any other means, the party can also trace all transcripts of the buyer. It facilitates de-anonymization [44]. That is, given the history of linkable transcripts of an anonymous buyer, a party may compare the history with the seller's information about when, what, and how many contents each person purchase, and thus may trace the buyer. Thus each content must be bought with different pseudonyms, because the same anonymous key implies that the buyer's purchases are linkable.

If a buyer wants to buy over two contents, he must go through the registration or watermark generation step several times in order to obtain several different pseudonyms in the previous schemes [11],[12],[18],[20]. The buyer must store private keys as many as the number of contents to be purchased, because each content must be encrypted with different key separately [12]. It is very inefficient. Still less, a typical buyer's device holds a very limited memory and computation power. That is the reason we propose an efficient protocol for multi-purchase.

we present more efficient buyer-seller watermarking scheme suitable to multi-purchase in next section [45-47].

## 4.2 Our Proposal

### [Preprocessing]

Let  $p (\leq n \text{ bits})$  be a large prime such that  $q = (p - 1)/2$  is also prime. Let  $G$  be a group of order  $p - 1$ , and let  $g$  be a generator of  $G$  such that computing of the discrete logarithms to the base  $g$  is difficult.

### [Notations]

For ease of exposition we assume that the content being sold is a still image, though in general the protocol is also applicable to audio and video data like Memon and Wong's scheme [10]. We also assume that all of the underlying primitives are secure.

The watermarking insertion step can be represented as  $X' = X \otimes W$ , where

- Alice      The seller who sells the digital multimedia content
- Bob        The buyer who can buy contents anonymously
- Wendy     A watermark certification authority (WCA)
- Ron        A registration center (RC)
- $x_A/y_A$    Private key/Public key corresponding with  $x_A$  of Alice
- $x_W/y_W$    Private key/Public key corresponding with  $x_W$  of Wendy
- $x_R/y_R$    Private key/Public key corresponding with  $x_R$  of Ron
- $X$          Original image to be a vector of "features".
- $W$          Watermarks as a vector of "watermark elements".

- $X$   $X \otimes W$ , watermarked image embedded into  $W$ .
- $E/D$  Encryption/Decryption with homomorphic property.
- $sign_a(\cdot)$  Signature algorithm with private key  $a$ .
- $total$  The number of contents to be purchased.

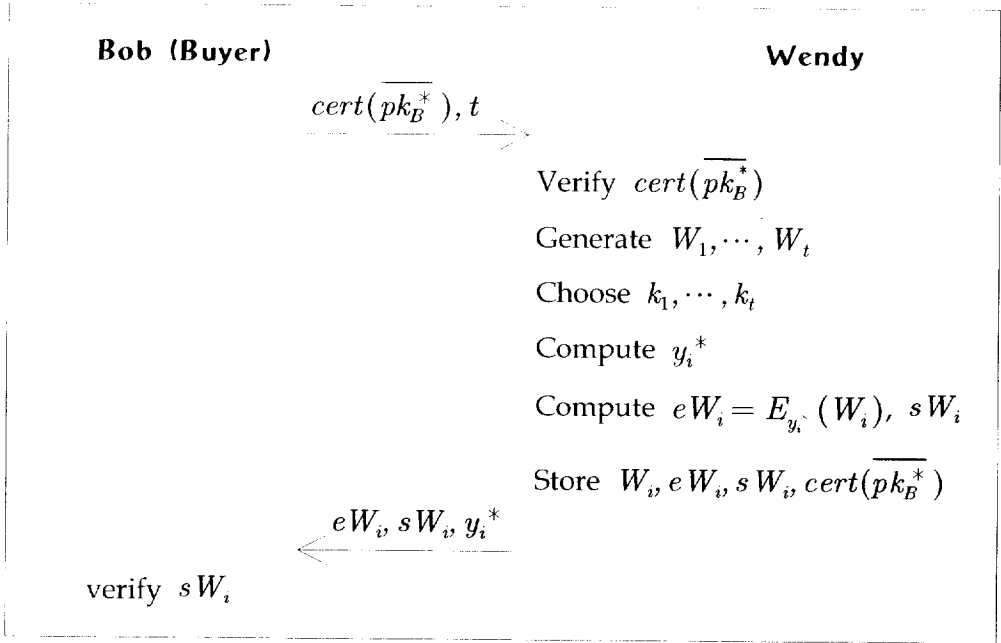
### ■ STEP 1. Registration

1. The buyer (Bob) chooses secret random  $x_1, x_2$  in  $Z_p$  such that  $x_1 \cdot x_2 = x_B \in Z_p$ . Bob sends  $y_B, \overline{y_B^*}$  ( $\overline{y_B^*} = g^{x_1}$ ) and  $x_2 (E_{y_R}(x_2))$  encrypted by using the Registration Center's (Ron) public key  $y_R$ . Bob convinces Ron of zero-knowledge of possession of  $x_1$ .
2. Ron decrypts  $E_{y_R}(x_2)$  and checks that  $y_B = (\overline{y_B^*})^{x_2}$ . If it is verified, Ron returns to Bob a certificate  $cert(\overline{y_B^*})$ . The certificate states the correctness of  $\overline{y_B^*}$ . Ron keeps  $y_B, x_2, cert(\overline{y_B^*})$  secretly.

### ■ STEP 2. Watermark Generation

This protocol is performed between WCA (Wendy) and Bob.

1. The buyer sends  $cert(\overline{y_B^*})$  and  $total$  to the WCA.
2. WCA first verifies  $cert(\overline{y_B^*})$  and if it holds, he generates  $t = total$  watermarks  $W_0, W_1, \dots, W_{t-1}$  randomly. Note that each  $W_i = \{w_{i_0}, w_{i_1}, \dots, w_{i_{n-1}}\}$ ,  $0 \leq i \leq t-1$ .



**Figure 10.** Watermark generation of our second protocol.

3. WCA chooses  $s$  and  $t$  keys  $k_0, k_1, \dots, k_{t-1}$  ( $k_i \in Z_p$ ) randomly and computes  $y_0^*, y_1^*, \dots, y_{t-1}^*$  where  $y_i^* = ((\overline{y_B^*})^{k_i}, g^{k_i})$ . Next, WCA encrypts each watermarks  $W_i$  with  $y_i^*$  and  $s$  such that  $eW_i = E_{y_i^*}(W_i) = ((g^{k_i})^s, W_i \cdot (y_i^{k_i})^s)$ . Then he computes signature  $sW_i = \text{Sign}_{x_w}(eW_i \parallel y_i^*)$ , which certifies the validity of the watermark and also ensures that  $y_i^*$  was used to encrypt  $W_i$  as a public key. Here  $\parallel$  denotes a concatenation and the encryption algorithm is homomorphic.
4. The WCA stores  $W_i, eW_i, sW_i, \text{cert}(\overline{y_B^*})$  secretly in the buyer's

fields of his DataBase  $Table_W$ . Then he sends  $eW_i, sW_i, y_i^*$  to Bob.

5. The buyer verifies  $sW_i$  using the Wendy's public key. If it holds, he obtains the valid watermarks that can decrypt with his own secret key  $x_1$ .

As mentioned before, the buyer can use the same  $\overline{cert(y_B^*)}$ , if he wants to obtain valid watermarks from Wendy continuously.

### ■ STEP 3. Watermark Insertion

This is an interactive protocol between a seller(sellers) and the buyer.

1. The buyer sends  $eW_i, sW_i, text_i$  and  $st_i = Sign_{x_1}(text_i)$  to Alice, the seller (It does not matter the sellers are different persons or not).
2. Alice verifies  $sW_i, y_i^*$  using Wendy's public key and  $st_i$  using  $y_i^*$ . If the two aforementioned checks succeed, the next step proceeds.
3. Let  $X_i$  denote the original images which the buyer wants to purchase. The seller generates unique  $V_i$  randomly and embeds a unique watermark into contents  $X_i$ . Let  $X_i'$  be the watermarked image with  $V_i$ . When an unauthorized copy  $X_i'$  is generated, this unique watermark  $V_i$  is used for identifying the original buyer of

$X_i'$ . To embed the second watermark  $W_i$  generated by Wendy into  $X_i'$  without decrypting  $E_{y_i^*}(W_i)$ , Alice encrypts the watermarked content  $X_i'$  with  $y_i^*$  and finds the permutation  $\sigma_i$  satisfying  $\sigma_i(E_{y_i^*}(W_i)) = E_{y_i^*}(\sigma_i(W_i))$ . Because of the homomorphic property of the encryption algorithm  $E$  used by Wendy, the seller can compute watermarked content  $E_{y_i^*}(X'')$  by the following process.  $s'$  is chosen randomly by the seller for encryption the content.

$$\begin{aligned}
E_{y_i^*}(X'') &= E_{y_i^*}(X_i') \otimes \sigma_i(E_{y_i^*}(W_i)) \\
&= E_{y_i^*}(X_i') \otimes E_{y_i^*}(\sigma_i(W_i)) \\
&= \{E_{y_i^*}(x_{i_1}'), \dots, E_{y_i^*}(x_{i_m}')\} \otimes \{E_{y_i^*}(w_{i_{\sigma_i(1)}}), \dots, E_{y_i^*}(w_{i_{\sigma_i(n)}})\} \\
&= \{E_{y_i^*}(x_{i_1} \otimes w_{i_{\sigma_i(1)}}), \dots, E_{y_i^*}(x_{i_n} \otimes w_{i_{\sigma_i(n)}}), \dots, E_{y_i^*}(x_{i_m}')\} \\
&= E_{y_i^*}(X_i \otimes V_i \otimes \sigma_i(W_i))
\end{aligned}$$

$$E_{y_i^*}(X'') = (g^{k_i})^s \cdot (g^{k_i})^{s'}, X'' \cdot (y_i^*)^s \cdot (y_i^*)^{s'}$$

4. Alice transmits  $E_{y_i^*}(X'')$  to Bob and stores  $eW_i, sW_i, st_i, y_i^*, V_i, \sigma_i$  in her DataBase  $Table_S$ .  $Table_S$  is a table of records maintained by seller for image  $X$  containing one entry for each copy of  $X$  that she sells.
5. The buyer decrypts the encrypted image  $E_{y_i^*}(X'')$  and obtains the watermarked image  $X_i''$ . Note that, buyers can decrypt the watermarked image encrypted with her own private key  $x_1$  such that

$$\begin{aligned}
D_{x_1}(E_{y_i^*}(X_i'')) &= \frac{(X_i \otimes V_i \otimes \sigma_i(W_i)) \cdot (y_i^*)^{s+s'}}{\{(g^{k_i})^{s+s'}\}_{x_1}} \\
&= X_i \otimes V_i \otimes \sigma_i(W_i)
\end{aligned}$$

#### ■ STEP 4. Copyright Violator Identification

When an illegal copy  $Y$  of an original image  $X$  is discovered,

1. The seller extracts the unique watermark  $U$  in  $Y$  using detection algorithm. Then, he finds  $V_j$  ( $j \geq 0$ ) with the highest correlation and obtains the transaction information involving  $V_j$  from the table by computing correlations of extracted watermark  $V_j$  and every watermark stored in  $Table_s$ . The information consists of  $eW_i, sW_i, st_i, y_i^*, V_i, \sigma_i$ . And the seller sends them with  $X, Y$  to an arbiter.
2. The arbiter verifies  $sW_i$  with the Wendy's public key  $y_W$ . If the verification holds, the arbiter sends  $y_i^*$  to Wendy. Then the Wendy sends  $W_i$  back to the arbiter.
3. The arbiter computes  $\sigma_i(W_i)$  and checks the existence of  $\sigma_i(W_i)$  in  $Y$  by extracting the watermark from  $Y$  and estimating its correlations with  $\sigma_i(W_i)$ . If there exists  $\sigma_i(W_i)$ , she asks the real identity of the violator to Ron and reveals the buyer's ID to the seller. Otherwise, the buyer is innocent.

### 4.3 Features and Analysis

- *Anonymity*: We assumed that the registration center does not reveal the buyer's real identity if he is honest. Even if the seller knows a pseudonym  $y_i^*$ , they cannot know  $y_B$ . Because finding  $y_B$  would require knowledge of  $x_2$ . It is known to only the buyer (except RC). Thus buyer's anonymity is provided if the seller and the mobile agent cannot compute discrete logarithms.
- *Unlinkability*: In multi-purchase, not  $\overline{y_B^*}$  but  $t$  different keys  $y_0^*, y_1^*, \dots, y_{t-1}^*$  are transmitted to the sellers. And each watermarked image sold to a buyer must be encrypted with each different key for unlinkability of digital contents. Thus given two digital contents, nobody can decide whether these two contents were purchased by the same buyer or not.
- *Traceability*: Due to the properties of the underlying encryption and digital signature techniques, we can assume that a malicious buyer cannot change or substitute watermarks generated by the watermark certificate center. The security of traceability is the same as that of [10] and [12] schemes. Sellers should insert a watermark  $V_i$  and  $\sigma_i(W_i)$  in the right manner for her own interest.

If she does not correctly insert  $V_i$  or  $\sigma_i(W_i)$ , she would not be able to identify the original buyer of an illegal copy. Further a detecting function in the watermark detection must guarantee that the seller can extract the unique watermark  $V_i$  that belongs to a copyright violator. Besides, buyers cannot remove  $\sigma_i(W_i)$  from  $X_i$  even though he and his mobile agent know  $W_i$ . Because they do not know permutation function  $\sigma_i$ . Thus the copyright violator can be traced in our scheme.

- **No Framing:** Since, to forge  $Y$  with the special watermark  $W_i$ , the seller must know either the buyer's private key  $x_1$  or the buyer's unique watermark  $W_i$ . In our proposal, only the buyer knows his private key  $x_1$  and his unique watermark if computing discrete logarithm is hard and used encryption algorithm (underlying primitives) is secure.
- **No Repudiation:** Since only the buyer can decrypt encrypted watermarked contents, the others (except watermark certification center) cannot recreate the buyer's copy. Only the buyer can obtain the watermarked contents even though the mobile agent executes its computations instead of him. Since the watermarked contents encrypted with buyer's public key are transmitted. Thus the buyer

accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or other buyers.

- *Collusion tolerance:* Our scheme has used robust watermarking algorithms against collusion attacks. We assumed that used algorithms are secure. And these algorithms are estimated to be highly resistant at collusion attacks. Our protocol is secure only as much as the underlying watermarking techniques are secure and robust.
- *Practical Possibility:* In previous scheme [11],[12],[18], the buyer has to carry out the registration and watermark insertion step. On the contrary, the buyer executes the one-time registration step and delegation step in our scheme. Our scheme reduces buyers' necessary key and computations amounts to minimum. Thus our scheme can be practically realized in real applications.
- *Efficient extension:* In our scheme, the buyer executes the registration step just one time regardless of a number of contents purchased. Besides, buyers can decrypt contents with one decryption key even if each content (watermarked image) is encrypted with each different key. If the previous schemes are applied to multi-purchase protocol, the number of registration step execution and decryption keys increase in proportion to those of

**Table 5.** Comparison of our proposal with extended Ju et al.'s scheme [12].

Features	Our Proposal	Extended [12] scheme
The number of execution of Watermark generation step	1	n
The number of encryption key	n	n
The number of decryption key	1	n

contents to be purchased in order to keep unlinkability. But the number of private key stored in the buyer's device is constant independent of the number of contents purchased in our proposal.

#### 4.4 Chapter Summary

To protect the privacy of buyers, buyers' purchase should be done anonymously, and unlinkability of purchased contents should be satisfied. If we apply the previous scheme to multi-purchase case, the problem is that the number of keys held by buyer's devices increases in proportion to those of purchased contents. Otherwise, they cannot provide unlinkability. To improve this inefficiency, we first proposed an anonymous buyer-seller watermarking protocol to multi-purchase environment in this Chapter.

Our proposal satisfied anonymity and unlinkability, where a buyer executes registration step one time and the number of buyer's necessary key is also one regardless of that of contents.

In result, our proposal reduced the number of buyer's necessary key and the amount of buyers' computations to the minimum.

Our proposal is significant in the sense that it is the first scheme applied to multi-purchase environments efficiently. We expect that our scheme will be applicable to the customer-centered commercial transaction.

# Chapter V. A Copyright Protection Scheme for Broadcast Media

## 5.1 Introduction

Over the past few years, a considerable number of studies have been made on protecting broadcast media. Typically, in broadcast networks, cryptographic techniques such as broadcast encryption are sufficient to give a enough level of protection against dishonest reception. Here, digital contents are encrypted to ensure that only privileged users can recover the content from the encrypted broadcast. It often deals with the tracing mechanism, which enables providers to trace the source of keys used by an illegal device such as pirate decoders: Legitimate users illegally selling their keys to others.

However it does not consider the illegal distribution of the decrypted contents by legitimate users. So, if illegal copies are found, it is difficult to determine which subscriber was the source of those copies. It is therefore necessary to provide a means for tracing illegal copies, to deter a copyright violator. Traceability schemes based on digital watermarking(fingerprinting) techniques have been proposed as the important class of these techniques. For example, in applications such as pay-per-view video where multimedia content is distributed over a net-

work, the broadcaster can embed a distinct watermark, in each copy of the content that is distributed. If illegally redistributed copies of the content are found, then the origin of the copy can be determined by retrieving the unique watermark corresponding to each subscriber. It must be a very powerful tool to protect copyright in a broadcast environment. But it is hard to design an efficient watermarking-based copyright protection scheme for broadcast media. Because each subscriber must receive a slightly different content in order to be identified, it is contrary to the bandwidth saving of being able to distribute the same data efficiently to multiple subscribers.

In this chapter, we are concerned with a secure and efficient integrated solution to trace traitors and broadcast, and limit the discussion to digital watermarking-based copyright protection scheme.

## **5.2 Related Works**

### **5.2.1 Symmetric Schemes**

Watermarking-based protocol for broadcast environments was first formally studied by Anderson and Manifavas [48]. But it is extremely vulnerable to collusion among subscribers: Five or more subscribers can together produce plaintext or keys for installation in pirate decoder that cannot be traced. Besides, the multicaster would need huge com-

puting resources in this scheme. After, for the lightweight network components, Brown et al.'s scheme [49] was proposed. It is also inefficient in the sense that the network bandwidth requirement is high because it transmits copies, where is greater than the depth of the multicast group tree. In addition, each sender must trust the chain of network routers and honesty of network providers is required in this scheme.

After, Judge and Ammar proposed a multicast video watermarking protocol with a hierarchy of intermediaries [50]. It places a hierarchy of intermediaries as end systems in the network and forms an overlay network between them. Like [49] scheme, it also requires that each sender must trust the chain of active network intermediaries and network providers. After, Chu et al.'s scheme has suggested, which is the centralized approach that needed a trusted group leader [51]. They creates two watermarked streams, and assigns a unique random binary sequence to each subscriber. But, it must transmit two copies of the stream, and requires the significant amount of key message. After, two schemes [52,53] considered on-line feedback from the pirate subscribers have suggested. By introducing time dimension, [52] scheme considered the dynamic tracing scenario in which the number of transmitted watermarked copies in a segment depends on the feedback from the previous segment. But it is vulnerable to the delayed rebroadcast attack. This problem was solved in [53] scheme. However it requires higher bandwidth for sending each segment, and needs to know the

user group size in advance to decide how many copies to generate.

### **5.2.2 Asymmetric Schemes**

The most serious problem of the previous schemes [48-53] is that these are symmetric. That is, the watermark generation and embedding is performed or controlled by the broadcaster. Therefore, a broadcaster with malicious intentions could falsely implicate an innocent subscriber in tracing a copyright violator.

This problem is first overcome by Emmanuel et al.'s scheme [54]. It is a significant model in the sense that it first offered asymmetric property to broadcast video watermarking protocol and the number of transmitted copy is just one. Here, because only a subscriber can obtain the exact watermarked copy, the broadcaster cannot frame an honest subscriber as a traitor. Asymmetry is based on the existence of a trusted third party (a watermark generation authority) and public key algorithms with homomorphic property in this scheme. But this scheme is insecure and inefficient. In addition, it does not provide subscriber's anonymity. We describe it in detail in the next section.

## **5.3 Analysis of Emmanuel et al.'s Scheme [54]**

In this section, we briefly review the construction proposed in [54]. It

involves the broadcaster B, the receiver  $R_i$ , and a watermark generation authority WGA known and trusted by B and  $R_i$ .

### 5.3.1 Overview of Emmanuel et al.'s Scheme

#### ■ Step 1. Mask-Blending

Each frame  $x_n(k, l)$  is scrambled with a mask frame  $v(k, l)$ , using  $x_n^m(k, l) = \alpha x_n(k, l) + \beta v(k, l)$ . Where  $x_n^m(k, l)$  is the  $n$ th masked video frame and  $\alpha$  and  $\beta$  are scaling factors. Then the B broadcasts  $x_n^m(k, l)$ .

#### ■ Step 2. Mutual Authentication

##### [Notations]

- $A \rightarrow B: M$                       M is transferred from A to B
- $sign_X$                               Signature done using  $X$ 's private key
- $Rqst\_proof$                         Request on  $proof\_msg$
- $cert_X$                                 Digital certificate of  $X$
- $t_X$                                        $X$ 's timestamp containing a generation time and an expiration time
- $r_X$                                        $X$ 's nonce to prevent reply attack
- $proof\_msg$                           Proof of ownership or distributorship of digital contents
- $k_i$                                         $R_i$ 's public key in the homomorphic public key cryptosystem
- $E_{k_i}(\alpha W_i(k, l))$               The scaled encrypted watermark with  $k_i$

- *Pay<sub>Info</sub>*                      Payment information

Msg.1.  $R_i \rightarrow B$ :  $sign_{R_i}(t_{R_i}, r_{R_i}, Rqst\_proof), cert_{R_i}$

Msg.2.  $B \rightarrow R_i$ :  $sign_B(t_B, r_B, R_i, r_{R_i}, \alpha, proof\_msg), cert_B$

Msg.3.  $R_i \rightarrow WGA$ :  $sign_{R_i}(t_{R_i, WGA}, r_{R_i, WGA}, WGA, r_B, k_i, \alpha), cert_{R_i}$

Msg.4.  $WGA \rightarrow R_i$ :  
 $cert_{WGA}, sign_{WGA}(E_{k_i}(\alpha W_i(k, l))),$   
 $sign_{WGA}(t_{WGA}, r_{WGA}, R_i, r_B, E_{k_i}(\alpha W_i(k, l)))$

Msg.5.  $R_i \rightarrow B$ :  
 $sign_{R_i}(r_B, k_i, E_{k_i}(\alpha W_i(k, l)), order_{Info}, Pay),$   
 $cert_{WGA}$

Msg.6.  $B \rightarrow R_i$ :  $sign_B(E_{k_i}(v_i(k, l)), r_B)$

### ■ Step 3. Unmasking Frame Process

1. B generates invisible watermark  $W_{b_i}(k, l)$  specifically for  $R_i$ . Then B creates an unmasking frame  $v_{b_i}(k, l)$  for the using  $v_{b_i}(k, l) = \beta v(k, l) - \alpha W_{b_i}(k, l)$ . The frame  $v_{b_i}(k, l)$  is then encrypted with the public key  $k_i$  to obtain  $E_{k_i}(v_{b_i}(k, l))$ . A random permutation  $\sigma$  is generated and is used to permute the elements of the encrypted watermark  $E_{k_i}(\alpha W_i(k, l))$  received from  $R_i$ . Let  $\sigma(\alpha W_i(k, l)) = W_i^\sigma(k, l)$ . B then computes the following equation  $E_{k_i}(W_i^\sigma(k, l))$  from  $E_{k_i}(v_i(k, l))$ . Here Emmanuel et al. used

Niederreiter's public key cryptosystem [55] as encryption algorithm:

$$\begin{aligned} E_{k_i}(v_i(k, l)) &= E_{k_i}(v_{b_i}(k, l)) - E_{k_i}(W_i^\sigma(k, l)) \\ &= E_{k_i}(v_{b_i}(k, l) - W_i^\sigma(k, l)) \end{aligned}$$

2. To view the channel without any obscurity, the  $R_i$  decrypts  $E_{k_i}(v_i(k, l))$  using the  $R_i$ 's private key  $k_i'$  to obtain  $v_i(k, l)$ . The frame  $v_i(k, l)$  is then used to unmask the obscured video. The following equation defines the unmasking process, where  $x_n^{W_i}(k, l)$  is the watermarked frame for the  $R_i$ :

$$\begin{aligned} x_n^{W_i}(k, l) &= \frac{1}{\alpha} (x_n^m(k, l) - v_i(k, l)) \\ &= x_n(k, l) + W_{b_i}(k, l) + \sigma(W_i(k, l)) \end{aligned}$$

Here,  $W_{b_i}(k, l)$  and  $W_i(k, l)$  are used for copyright violator detection and  $\sigma(W_i(k, l))$  is used for addressing asymmetric property.

### 5.3.2 Analysis of Emmanuel et al.'s Scheme

#### ■ Observation on Security

In this protocol, they embed two watermarks into one unmasking frame. One is generated by a watermark generation authority, and the other is generated by a broadcaster. The broadcaster needs to embed the encrypted first watermark  $E_{k_i}(\alpha W_i(k, l))$  into unmasking frame

embedded the second watermark without decrypting it, because the broadcaster must not know the first watermark for asymmetry. In order to offer asymmetry, Emmanuel et al. used Niederreiter's scheme [55] based on generalized reed-solomon codes. Niederreiter's scheme possesses privacy homomorphism with respect to addition and subtraction. Here, privacy homomorphism means that  $E_{k_i}(x_1) \pm E_{k_i}(X_2) = E_{k_i}(X_1 \pm X_2)$ . The security of this protocol lies in the private key  $k_i'$  (Niederreiter's scheme) of the subscriber and that of the watermark generation authority, subscriber and broadcaster used while signing. But, unfortunately Niederreiter's scheme [55] was broken by [56] scheme. In [56], they proved that the work function of breaking is just  $O(n^3)$ . This means that private key in the Niederreiter's algorithm can be revealed in  $O(n^3)$ . Here,  $n$  is the length of code. Emmanuel et al. also claimed that McEliece public key cryptosystem [57] instead of Niederreiter's scheme can be used in their scheme. But, Gobson showed that if the attacker knows not only the public key but also the ordering, then [57] scheme can be broken very easily [58]. After, Heiman and Shamir showed that a Generalized Reed-Solomon code used in [57] can be extracted from their equation [59]. Although there is no efficient method known for accomplishing this, [57] scheme suffers from the drawback that the size of public key is very large. For this reasons, [57] scheme receives little attention in practice. In addition, other secure homomorphic public key cryptosys-

tem with respect to addition and subtraction to be combined with watermarking protocol are unknown till now.

Thus we can know that Emmanuel et al.'s scheme is also insecure and impractical because of the cryptographic algorithm with homomorphic property.

### ■ Observation on Efficiency

In [54] scheme, if a broadcaster colludes with the watermark generation authority, they can recreate the subscriber's copy. Because the watermark generation authority knows one unique watermark  $W_i(k, l)$  the broadcaster knows the other watermark  $W_b(k, l)$  of all subscribers. Thus if they collude, they can produce the same unmasking frame as a certain honest subscriber. Therefore Emmanuel et al.'s scheme must assume that the watermark generation authority is honest.

The next shortcoming is that it has many passes in the mutual authentication step and does not provide subscriber's anonymity. Because the certificate containing the public key and identity of the subscribers should be sent to the broadcaster in this protocol, the broadcaster knows the real identity of all subscribers. It is also desirable that anonymity of honest subscribers should be protected.

## 5.4 Our Proposal

In this section, we describe digital watermarking-based traceability scheme without a watermark generation authority and homomorphic encryption algorithms. The watermarking algorithm (embedding and detection algorithms) of our scheme is based on Emmanuel et al.'s scheme.

### [Preprocessing]

Let  $p (\geq n \text{ bits})$  be a large prime such that  $q|p-1$  is also prime.

Let  $G$  be a group of order  $p-1$ , and let  $G$  be a generator of  $g$  such that computing discrete logarithms to the base  $g$  is difficult.

### [Notations]

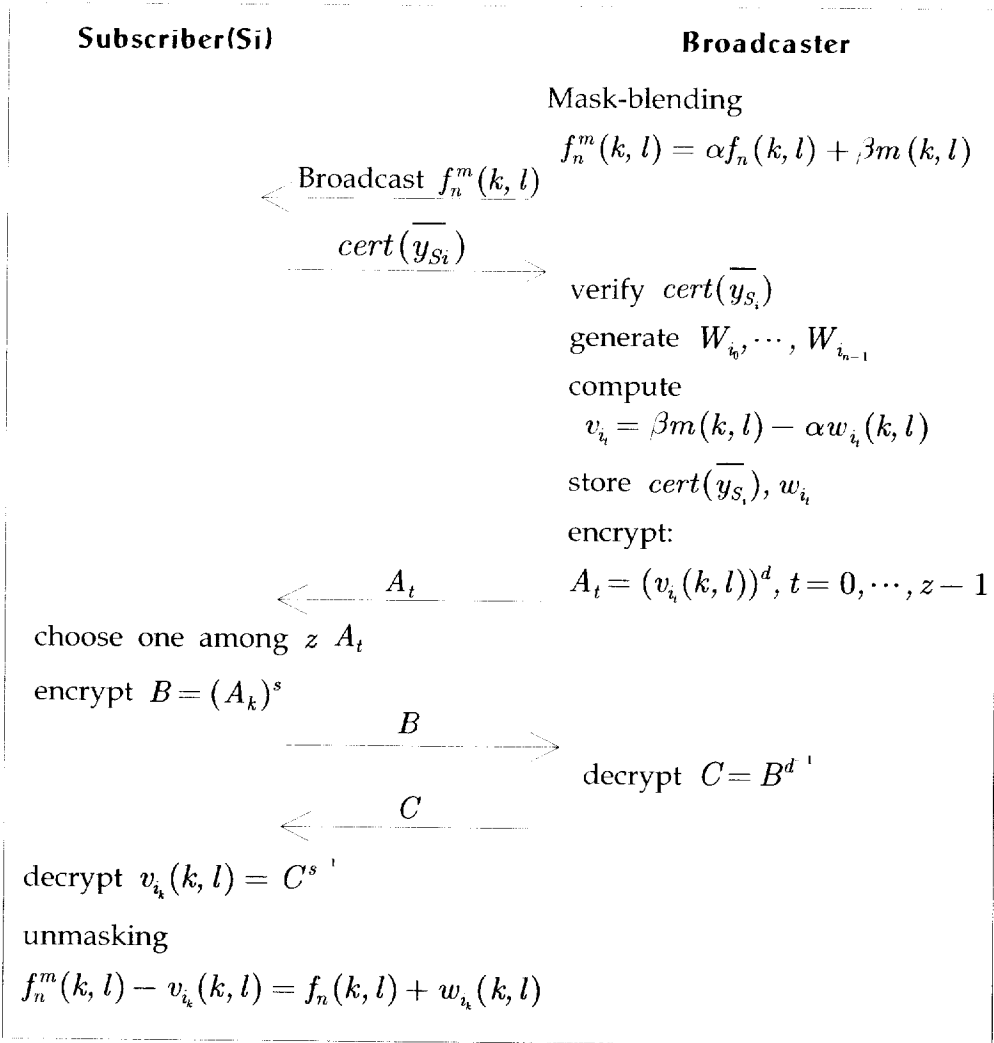
- $x_{S_i}/y_{S_i}$  Private key/public key corresponding with  $x_{S_i}$  of a subscriber  $S_i$
- $x_B/y_B$  Private key/public key corresponding with  $x_B$  of a broadcaster
- $x_R/y_R$  Private key/public key corresponding with  $x_R$  of a registration center
- $f_n(k, l)$   $n$ th frame of broadcast video of dimension  $K \times L$
- $m(k, l)$  Mask frame of dimension  $K \times L$
- $f_n^m(k, l)$   $n$ th masked video frame
- $\alpha, \beta$  scaling factors such that  $\alpha + \beta = 1$

## [Key Setup]

All participants (subscriber  $s_i$ , a broadcaster and a registration center) have a pair of a private key and a public key  $x, y$  such that  $y = g^x \pmod{p}$ , all of which have been registered with appropriate certificate authority.

### ■ STEP 1. Registration

1. A subscriber,  $S_i$ , chooses secret random  $x_{i_1}, x_{i_2}$  such that  $x_{i_1} \cdot x_{i_2} = x_{S_i} \in Z_q$ . The subscriber computes  $\overline{y_{S_i}}$  and encrypts  $x_{i_2}$  with the registration center's public key such that  $\overline{y_{S_i}} = g^{x_{i_1}} \pmod{p}, E_{y_R}(x_{i_2})$ . Then he sends them to the registration center. The subscriber convinces the registration center of zero-knowledge of possession of  $x_{i_1}$ . The proof given in [36] for showing possession of discrete logarithms may be used here.
2. The registration center decrypts  $E_{y_R}(x_{i_2})$  and checks that  $y_{S_i} = (\overline{y_{S_i}})^{x_{i_2}}$ . If it is verified, the registration center returns a certificate  $cert(\overline{y_{S_i}})$  to the subscriber. The certificate states the correctness of  $\overline{y_{S_i}}$ .



**Figure 11.** Mask-blending, Join, and Unmasking step of our third proposal.

### ■ STEP 2. Mask-Blending Process

Let us denote the  $n$ th frame of broadcast video as  $f_n(k, l)$ . Each frame consists of  $K \times L$  pixels. The broadcaster constructs a mask frame  $m(k, l)$  of dimension  $K \times L$  with the view that the video

frames are obscured after masking blending. The mask  $m(k, l)$  is blended with the video, frame by frame using the following equation:

$$f_n^m(k, l) = \alpha f_n(k, l) + \beta m(k, l)$$

The masking process simulates the scrambling effect. The scaling factors are necessary to adjust the strength of the mask, and are assumed to be public. The masked frame is then broadcast. The receivers who are non-subscribers would be able to view  $f_n^m(k, l)$  which is obscured.

### ■ STEP 3. Join

1. A subscriber  $S_i$  sends  $cert(\overline{y_{S_i}})$  to the broadcaster. If  $cert(\overline{y_{S_i}})$  is verified,  $S_i$  and the broadcaster execute oblivious transfer protocol.
2. The broadcaster generates  $k (\geq 2)$  watermarks  $w_{i_0}, \dots, w_{i_{k-1}}$  with  $K \times L$  pixels randomly for the  $S_i$  and computes  $k$  unmasking frames as follows.

$$v_{i_t} = \beta m(k, l) - \alpha w_{i_t}(k, l), 0 \leq t \leq z - 1$$

The broadcaster stores  $cert(\overline{y_{S_i}}), w_{i_0}, \dots, w_{i_{z-1}}$  at his table  $Table_B$ .

The broadcaster encrypts  $z^*$  frames with his secret key  $d$  and sends the subscriber:

\* Here, the broadcaster issues  $z$  watermarks, where the subscriber would choose one out of  $z$  unmasking frames. The choice of  $z$  implies a trade-off between correctness and efficiency. In such case, probability that the broadcaster can know the unmasking frame (watermark) that a subscriber chose would be equal to  $1/z$ .

$$A_0 = (v_{i_0}(k, l))^d, \dots, A_{z-1} = (v_{i_{z-1}}(k, l))^d$$

3. The subscriber chooses one among them. Suppose the subscriber chose  $A_1 = (v_{i_1}(k, l))^d$ . Then he re-encrypts it with his secret key  $s$  and sends it back to the broadcaster:  $B = (A_1)^s$ . Now the subscriber cannot know the hidden watermark because it is encrypted with the broadcaster's key, but it can verify that the broadcaster did not encrypt the same unmasking frames. (If the broadcaster encrypts and sends same unmasking frames ( $z$  frames), he can produce the subscriber's unique unmask frame.)
4. The broadcaster sends the  $C = B^{d^{-1}}$  and stores  $A_0, \dots, A_{z-1}$  at *Table\_B*. The broadcaster also cannot know which unmasking frame (watermark) the subscriber chose because it is encrypted with the subscriber's secret key. The subscriber decrypts and uses:  $v_{i_1}(k, l) = C^{s^{-1}}$ .

It is not clear whether  $v_{i_i}(k, l) \in G_q$  or not. If  $v_{i_i}(k, l) \notin G_q$ , we use the following method from the third pass of this step.

- The broadcaster selects  $z$  random values  $u_0, \dots, u_{z-1} \in G_{q'}$ , encrypts them with his secret key  $d$  and sends the subscriber. Here we use the following encryption algorithm:

$$A_0 = u_0^d, \dots, A_{k-1} = u_{k-1}^d.$$

- The subscriber chooses one among them. Suppose the subscriber chose  $A_1 = u_1^d$ . Then he re-encrypts it with his secret key  $s$  and sends it back to the broadcaster:  $B = A_1^s$ .
- The broadcaster sends the subscriber:  $C = B^{d^{-1}}$  and stores  $C$  at  $Table_B$ .
- The broadcaster generates  $z$  unmasking frames and computes:
$$u_0' = H(u_0), \dots, u_{z-1}' = H(u_{z-1}),$$

$$E_{u_0'}(v_{i_0}(k, l)), \dots, E_{u_{z-1}'}(v_{i_{z-1}}(k, l)),$$
 where  $H$  is a hash function. He sends them to the  $S_i$ . Here,  $E_a()$ ,  $D_a()$  is an encryption/decryption algorithm with secret key  $a$ .
- The subscriber computes  $u_1 = C^{S^{-1}}$ ,  $u_1' = H(u_1)$  and decrypts  $D_{u_1'}(E_{u_1'}(v_{i_1}(k, l)))$ . Thus a subscriber can obtain only one unmasking frame among  $E_{u_0'}(v_{i_0}(k, l)), \dots, E_{u_{z-1}'}(v_{i_{z-1}}(k, l))$ , and a broadcaster cannot know which frame the subscriber chose. In this case, the broadcaster must verify that she inputs not the same values but  $z$  different unmasking frames when a traitor disputes that the illegal copy has originated from the broadcaster. Thus the broadcaster stores them:

$$u_0', \dots, u_{z-1}', E_{u_0'}(v_{i_0}(k, l)), \dots, E_{u_{z-1}'}(v_{i_{z-1}}(k, l))$$

#### ■ STEP 4. Unmasking Process

To view the channel without any obscurity, the  $S_i$  first uses his own unmasking frame  $v_i(k, l)$  obtained in the join step. The following equation defines the unmasking process.

$$\begin{aligned}
 f_n^{w_i} &= (f_n^m(k, l) - v_i(k, l)) \times \frac{1}{\alpha} \\
 &= (\alpha f_n(k, l) + \beta m(k, l) - v_i(k, l)) \times \frac{1}{\alpha} \\
 &= (\alpha f_n(k, l) + \beta m(k, l) - \beta m(k, l) + \alpha w_i(k, l)) \times \frac{1}{\alpha} \\
 &= f_n(k, l) + w_i(k, l)
 \end{aligned}$$

Here,  $f_n^{w_i}(k, l)$  is the watermarked frame for a subscriber  $S_i$ . Note that  $f_n^{w_i}(k, l)$  contains the robust invisible watermark  $w_i(k, l)$  for copyright violator detection.

#### ■ STEP 5. Copyright Violator Identification

After finding a re-broadcasted copy  $f_n^{w_i}(k, l)^{red}$ , the broadcaster extracts the unique watermark  $w_i'(k, l)$ . For robust watermarking algorithm, by computing correlation of extracted watermark  $w_i'(k, l)$  and every watermarks stored in  $Table_B$ , the broadcaster finds  $w_i'(k, l)$  with the highest correlation and obtains the transaction information involving  $w_i(k, l)$  from the table. The information contains  $cert(\overline{y_{S_i}})$ . The

broadcaster sends it and  $f_n^{w_i}(k, l)^{red}$  to an arbiter. The arbiter verifies the presence of  $w_i(k, l)$  in the  $f_n^{w_i}(k, l)^{red}$ , if it is checked, he asks the real identity of the traitor to the registration center. Thus the broadcaster can identify the traitor. If the correlation value is smaller than the minimum threshold, he declares that the watermark is not found. Thus the accused subscriber turns out to be honest.

## 5.5 Comparison and Security Analysis

We compare and discuss features and security of our proposal with Emmuanuel et al.'s scheme [54] in Table 6.

- **Confidentiality:** In both schemes, only authorized subscribers can access broadcast information and can view it without any obscurity. Because non-subscribers cannot obtain an unmasking frame  $v_i(k, l)$  they would only be able to view  $f_n^{w_i}(k, l)$ , which is obscured. Thus our scheme provides confidentiality.
- **Asymmetry:** Since, to forge  $f_n^{w_i}(k, l)$  with the special watermark  $w_i(k, l)$ , the broadcaster must know either the subscriber's private keys or the unique watermark  $w_i(k, l)$ . We used OT with two

**Table 6.** Comparison of our proposal with Emmanuel et al.'s scheme [54].

Features	Our Proposal	[54] scheme
Confidentiality	○	○
Asymmetry	○	×
Anonymity	○	×
Security	Secure	Insecure
Pass number in the Join	4	6

-lock cryptosystem for asymmetry. Thus, if this cryptosystem is secure, the broadcaster cannot know which unmasking frame subscribers selected. Here, because only the subscriber knows his secret key  $s$  (if computing discrete logarithm is hard and encryption algorithm is secure), the others cannot recreate the subscriber's unmasking frame with specific watermark. Thus an honest subscriber should not be wrongly identified as a traitor. Added to this, the subscriber accused of re-broadcasting an unauthorized frame also cannot claim that the frame was created by the broadcaster or a security breach of the broadcaster's system. Thus we provide watermarking protocol with asymmetry property without homomorphic encryption and a trusted third party. On the contrary, it is possible that the broadcaster can know the subscriber's watermark if he colludes with the watermark generation authority in [54]. Although, they assumed that honesty of a watermark generation authority, the private key of subscribers can be revealed

because of insecurity of [57] scheme they used. Thus [54] scheme cannot provide asymmetry with broadcast video watermarking protocol. But, our scheme offers asymmetric property without a trusted third party (watermark generation authority).

- **Anonymity:** We assume that the registration center does not reveal the subscriber's real identity if the subscriber is honest. In the join step, the broadcaster knows  $\overline{y_{S_i}}$ . Finding  $y_{S_i}$  would require knowledge of  $x_{S_i}$ . However, if the encryption algorithm is secure, the only way for the broadcaster to find  $x_{S_i}$ ,  $x_{S_i}$  is to compute  $\log_g \overline{y_{S_i}}$  and decrypt  $E_{y_R}(x_{i_2})$ . But polynomial algorithm proving discrete logarithm problem does not exist, attacker (the broadcaster) does not compute  $x_{S_i}$ . Thus subscribers' anonymity is guaranteed in our scheme.
- **Traceability:** Our scheme has used Emmuanuel et al.'s scheme as a watermarking algorithm for video (specially MPEG-2 compressed video). Due to the properties of embedding and detecting method of [54] scheme, we can assume that a malicious subscriber cannot change or substitute a watermark generated by the broadcaster. Further a detecting function in the identification step guarantees that the broadcaster can extract the unique watermark  $w_i(k, l)$

that belong to a traitor. Thus the subscriber who has re-broadcasted frames illegally can be traced in our scheme. Our protocol is secure only as much as the underlying watermarking algorithm techniques are secure and robust. Of course, Emmuanuel et al.'s scheme can also identify a copyright violator. But Emmuanuel et al.'s scheme needs a trusted third party (watermark generation authority) for the real evidence on the illegal redistribution of dishonest subscriber.

- *Other Advantages:* Emmuanuel et al.'s scheme requires 6-pass number, while our scheme just requires 4-pass number in order to obtain unmasking frame.

## 5.6 Chapter Summary

Several digital watermarking-based traceability schemes have been proposed as a technique to provide copyright protection for broadcast media. But, most of them are symmetric, where the broadcaster knows each subscribers' unique watermark. Thus redistributed copy is found, it could just as well have been produced by the broadcaster or someone with illegal access to the broadcaster's equipment. Therefore, the result of tracing is no real evidence that could unambiguously convince a third party.

For offering symmetry, Emmanuel et al. proposed a digital rights management scheme recently. They used public key cryptosystems with homomorphic property and a trusted third party so-called watermark generation authority. But this scheme is insecure because of the used cryptographic algorithm. They must also assume honesty of the watermark generation authority for its security.

In this Chapter, we first showed the insecurity and inefficiency of Emmanuel et al.'s protocol and then suggested a secure and efficient watermarking-based protocol for broadcast video. Our scheme is secure and provides asymmetry without a watermark generation authority. Another meaningful feature of our scheme is to consider a subscriber's anonymity, which is one of important requirement for electronic marketplaces.

# Chapter VI. An Application to Mobile Communications

## 6.1 Introduction

Mobile communication has already been recognized to be an essential means for realizing the information society because of its capabilities of connecting 'anybody', 'anytime', 'anywhere'. The demand for mobile communication service is accelerating and mobile communication industries are growing rapidly all over the world. Moreover, they are expected to provide higher quality of multimedia services for users than today's systems. Thus copyright protection of multimedia contents being provided must be solved along with them.

In general, the fingerprinted contents can be made in on-line, because every sold copy is slightly different from the original contents and unique to its buyer. Thus fingerprinting schemes with high complexity are not suited for the real application and, what is more, cannot be implemented in mobile communication. But most of known fingerprinting schemes are based on computationally unspecified black boxes without presenting explicit protocols such as secure multiparty computation or general zero-knowledge proof [17]. These protocols are embodied by

difficult problems with much computation such as discrete logarithm problem or graph isomorphic problem. Their complexity is much too high to be materialized even in wire communication. Still less, buyer's memory and computation power is very small in mobile communication. There is an efficient method without secure two party computations [18], [20]. But this method is also impractical because it uses Cox's algorithm [13] as a building block for collusion resistance. In [13], their code needed for embedding is so long that the overall system cannot be practical.

To address this problem, we will propose a digital fingerprinting scheme for mobile communication using mobile agent who has more computational power than buyer [32], [46], [60-62].

## **6.2 Our Methodology**

The basic primitives of our proposal is proxy certificates. In this section, we explain the concept of proxy certificates briefly.

Security issues related to the usage of mobile agents in performing operations to which their owners have to be bound, such as payments, are of utmost importance if these kinds of agents are to be used in electronic commerce. If this binding is achieved by means of digital signature techniques, this means agents have to carry the owner's pri-

vate key to the host where they sign documents. This exposes the key to attackers because it is copied outside protected environments. In our scheme, we used a mechanism, called proxy certificates, that avoids the need for the agent to have access to the user's private key for digitally signing documents, but still binds the owner to the contents of those documents. We briefly review the construction proposed in [63].

### [Notations]

- $CA$  The identity of a certification authority
  - $A(X)$  The identity of a mobile agent belonging to  $X$
  - $pk_X$  The public key of  $X$
  - $sk_X$  The private key of  $X$
  - $\{M\}$  A message with contents  $M$
  - $\{M\}_{sk_X}$  A message with contents  $M$  signed by  $X$
  - $cert\{X, pk_X\}_{sk_Y}$  The digital certificate of  $X$  issued by  $Y$
  - $cert\{X, pk_{A()}, [D]\}_{sk_X}$  The proxy certificate of a mobile agent belonging to  $X$ , with additional data  $D$
- 
- Signature verification of  $\{M\}_{sk_X}$ : Verification is successful iff  $M$  equals  $M_1$ ,  $sig\_ver(M, X)$
  - Verification of  $cert\_ver(X, Y) = Z, pk_Z$ : Verification is successful iff  $sig\_ver(cert\{X, pk_X\}_{sk_Y}, Y)$  is successful, in which case it has  $Z = X$  and  $pk_Z = pk_X$ .

## ■ Issuing Proxy Certificates

A proxy certificate is issued and signed by the owner of an agent. Obviously, there is an associated key pair that is also generated by the agent's owner.

The certificate contains a validity period, the identity of the agent's owner, and a set of constraints indicating the valid operations that the agent is allowed to perform while using that certificate.

The buyer is bound to the actions performed (i.e., documents signed) by the agent through the owner's identity and signature in the proxy certificate. For this purpose, the identity in the proxy certificate must be the same as the identity in the buyer's signature certificate. Thus a proxy certificate for an agent belonging to buyer B is denoted as  $cert\{B, pk_{A(B)}, [constraints]\}_{sk_B}$

## ■ Using Proxy Certificates

When migrating to an external server the agent will carry its proxy certificates, which can be part of the data that composes the agent's specific code. The agent will also carry the buyer's signature certificate, as before. The secret data includes the agent's private signature key, along with the usual secret data, but now excluding the buyer's signature key. i.e., the agent carries, among other elements:

$$\{cert\{B, pk_B\}_{sk_{CA}}, cert\{B, pk_{A(B)}, [constraints]\}_{sk_B}, sk_{A(B)}\}$$

When the agent decides to purchase some good of service, it must check the details of the purchase against the constraints in its proxy certificate, and only proceeds if all of the constraints are satisfied. In order to make a payment and purchase, the agent sends its proxy certificates and the buyer's certificate to the seller:

$$\{cert\{B, pk_B\}_{sk_{CA}}, cert\{B, pk_{A(B)}, [constraints]\}_{sk_B}\}$$

Besides the verification of signatures, discussed below, the seller should check the constraints in the certificate in order to ensure that the agent is allowed to make the purchase. Even though the agent has already performed this check, the seller should do it again to prevent possible malfunctions on the agent's behaviors.

### ■ Signature Verification

The act of verifying a signature made by the agent on some message  $\{M\}$  represents more than simply binding the agent to the signed data. The buyer has to be bound to the data, as well. Therefore, when verifying a signature, the seller will first validate the buyer's signature certificate, i.e., performs

$$cert\_ver(cert\{B, pk_B\}_{sk_{CA}}, CA) \text{ and obtains } B \text{ and } pk_B.$$

Next, the seller validates the proxy certificate which  $cert\_ver(cert\{B, pk_B\}_{sk_{CA}}, [constraints]\}_{sk_B}, B)$  and obtains  $A(B)$  and  $pk_{A(B)}$ . This ensures that the buyer has delegated powers to the agent. Finally, the signature on the data is verified by doing

$sig\_ver(M, A(B))$ .

### 6.3 Our Proposal

#### [Assumptions]

For ease of exposition we assume that the content being sold is a still image, though in general the protocol is also applicable to audio and video data like [10] and [12] schemes. We also assume that all of the underlying primitives are secure.

#### [System Set Up]

Let  $p (\leq nbits)$  be a large prime such that  $q = (p - 1)/2$  is also prime. Let  $G$  be a group of order  $p - 1$ , and let  $g$  be a generator of  $G$  such that computing of discrete logarithms to the base  $g$  is difficult. That all participants have a pair of a private key and a public key  $(x, y)$  such that  $y = g^x \pmod{p}$ , all of which have been registered with appropriate certificate authority.

#### [Notations]

The fingerprinting insertion step can be represented as  $X' = X \otimes F$ , where

- $X$  Original image to be a vector of "features",  $X = \{x_1, \dots, x_m\}$
- $F$  Watermarks as a vector of "fingerprint elements",  $F = \{f_1, \dots, f_n\}$ ,  $m \geq n$ .
- $\otimes$  Fingerprints insertion operation
- $X', X''$  Fingerprinted image
- $E/D$  Encryption/Decryption algorithm with homomorphic property.
- $sign_{sk_X}(M)$  Signature of  $X$  on the message  $M$
- $cert\{pk_X\}_{sk_Y}$  The digital certificate of  $X$  issued by  $Y$
- $cert\{pk_{MA}, [D]\}_{sk_X}$  The proxy certificate of a mobile agent, with additional data  $D$

### [Roles of each entity]

The entities of our scheme consist of the fingerprint certificate center(FC), a mobile agent, a buyer, and a seller. The role of each entity is as follows:

#### *Fingerprint Certificate Center*

- ✓ He generates random fingerprints in the required manner and issues them to any user (mobile agent) upon request.
- ✓ He is in charge of the registration process and has secret database to keep secret user information.
- ✓ He has to take part in identification protocol in order to reveal the user's real identity who distributed digital contents illegally

when a seller request.

- ✓ He has private  $y_F$  and public key  $y_F = g^{x_F} \pmod{p}$ .
- ✓ He is the trusted third party.

### *Mobile agent*

- ✓ He carries out fingerprints generation protocol and fingerprints insertion protocol instead of buyers.
- ✓ He is able to sign messages about purchasing on behalf of the buyer after execution delegation protocol.
- ✓ He has private  $x_M$  and public key  $y_M = g^{x_M} \pmod{p}$ .

### *Buyer*

- ✓ She has to register to FC to obtain her own anonymous public key.
- ✓ She delegates the power of signing and protocol execution to a mobile agent who will execute protocols instead of herself.
- ✓ She issues the proxy certificates to mobile agent.
- ✓ She has private key  $x_B$  and public key  $y_B = g^{x_B} \pmod{p}$ .

### *Seller*

- ✓ He is an agent selling digital contents.
- ✓ He has database to record anonymous buyers and their information.

- ✓ He has to embed the anonymous buyer's information into digital contents without revealing it (decrypting it).

### 6.3.2 Proposed Scheme

The proposed anonymous fingerprinting scheme consists of the following 5 steps.

#### ■ Step 1. Registration

A buyer registers to FC as follows:

1. A buyer chooses secret random  $x_1$  and  $x_2$  in  $Z_p$ .

$$x_1 \cdot x_2 = x_B \in Z_p$$

2. He sends  $\overline{y_B^*} = g^{x_1} \pmod{p}$  and encrypting  $x_2$  using FC's public key  $y_F$  such as  $E_{y_F}(x_2)$  to FC.  $\overline{y_B^*}$  is anonymous public key of the buyer. The buyer convinces the FC of zero-knowledge of possession of  $x_1$ .
3. The FC first decrypts  $E_{y_F}(x_2)$  using his private key  $sk_F$  and checks that  $(\overline{y_B^*})^{x_2} = y_B \pmod{p}$ . If it is verified, FC returns to the buyer certificates,  $cert\{\overline{y_B^*}\}_{x_F}$  that state the correctness of  $\overline{y_B^*}$ .
4. FC keeps them  $y_B, cert\{\overline{y_B^*}\}_{x_F}, \overline{y_B^*}$  secretly in his secure user information DataBase  $Table_{FC}$ .

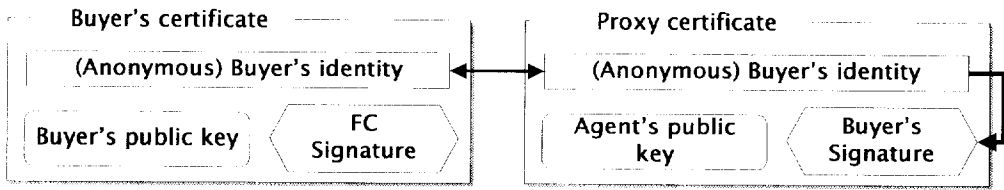


Figure 12. Buyer binding with a proxy certificate.

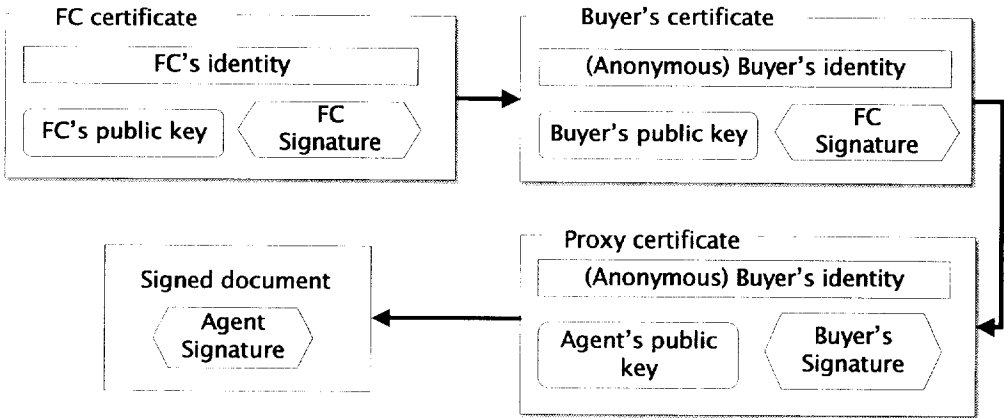


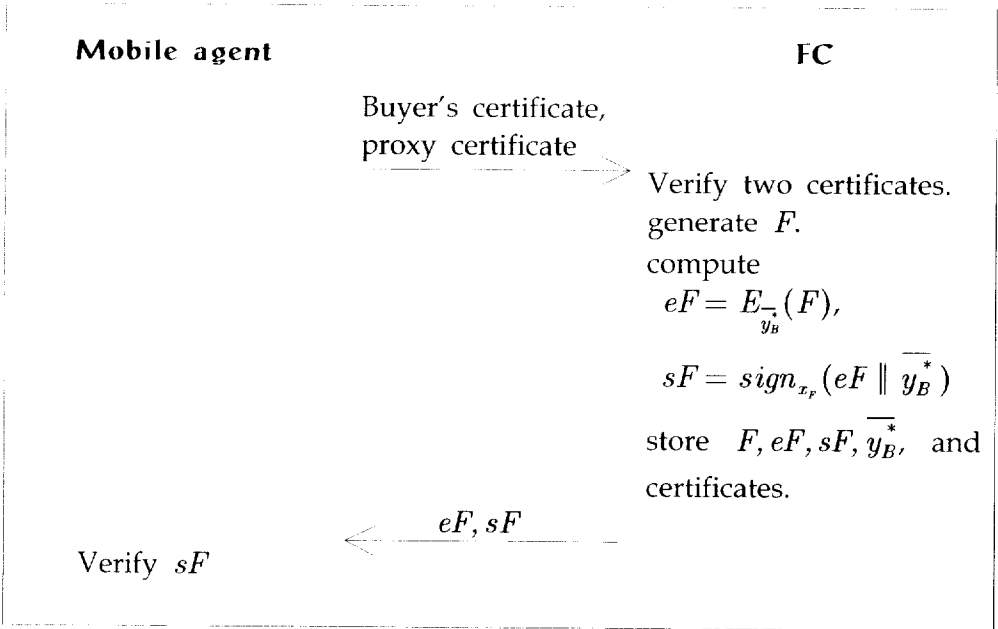
Figure 13. Signature verification with proxy certificate.

## ■ Step 2. Delegation

Now, an anonymous buyer and a mobile agent execute delegation step. Here, an anonymous buyer delegates the power of signing (purchase contents) to the mobile agent. After this step, the mobile agent is able to perform the rest of fingerprinting protocol on behalf of the buyer.

We use proxy certificates for secure delegation in here.

1. The (anonymous) buyer issues the proxy certificate,  $cert\{y_M, [text]\}_{x_1}$  to the agent. The certificate contains his own



**Figure 14.** Fingerprints generation step of our fourth proposal.

identity (anonymous identity) and a set of text indicating the valid operations that the agent is allowed to perform while using that certificate and contents to will be purchased (see Figure 12, 13 for illustration).

2. The buyer sends  $\text{cert}\{\overline{y_B^*}\}_{x_f}$  and  $\text{cert}\{y_M, [text]\}_{x_1}$  to agent.

### ■ Step 3. Fingerprints Generation

This protocol is performed between FC and the mobile agent.

1. The mobile agent sends the buyer's certificate and proxy certificate to the FC.

2. FC first verifies the buyer's certificate using his private key  $x_F$  and then, confirms whether  $\overline{y_B^*}$  exists in his own DataBase  $Table_{FC}$  or not.
3. If it exists, FC checks validity of a proxy certificate using the buyer's anonymous public key.
4. If it holds, FC generates fingerprints  $F$  randomly. Note that  $F = \{f_0, \dots, f_{n-1}\}$ . In here, we use a specific construction which introduced a spread-spectrum watermarking techniques proposed by Cox et al [22]. Cox et al. embed a set of independent real numbers  $F = \{f_0, \dots, f_{m-1}\}$  drawn from a zero mean, variance 1, Gaussian distribution into the  $m$  largest DCT AC coefficients of an image. Results reported using the largest 1000 AC coefficients show the technique to be remarkably robust against various image processing operations, and after printing and rescanning and multiple-document (collusion) attack. It is pointed out to be highly resistant at collusion attacks [35].
5. FC encrypts fingerprints  $F$  with the buyer's anonymous public key  $\overline{y_B^*}$ .

$$eF = E_{\overline{y_B^*}}(F), \quad sF = sign_{x_F}(eF \parallel \overline{y_B^*})$$

Then, he computes signature  $sign_{x_F}(eF \parallel \overline{y_B^*})$ , which certifies the

validity of the fingerprint and also ensure that  $\overline{y_B^*}$  was used to encrypt  $F$  as a public key. The FC stores  $F, eF, sF, cert\{y_M, [text]\}_{x_1}$  secretly in the buyer's fields of his DataBase  $Table_{FC}$ .  $y_B, cert\{\overline{y_B^*}\}_{x_p}, \overline{y_B^*}$  have already stored in the buyer's fields of  $Table_{FC}$ . Here  $\parallel$  denotes a concatenation and the used encryption algorithm is homomorphic.

6. FC sends  $eF, sF$  to the mobile agent.
7. The mobile agent verifies  $sF$  using the FC's public key. If it holds, he obtains the valid fingerprints encrypted with the buyer's anonymous public key.

#### ■ Step 4. Fingerprints Insertion

This is an interactive protocol between a seller and the mobile agent who must buy digital image instead of the buyer who wants to purchase fingerprinted image.

1. A mobile agent sends  $cert\{\overline{y_B^*}\}_{x_p}, cert\{y_M, [text]\}_{x_1}, eF, sF$  and  $\overline{y_B^*}, y_M, sM$  to the Seller.

$$sM = sign_{x_M}(text)$$

2. A seller verifies two certificates and  $sM$  (see Figure 13). If the verification holds, the next step proceeds.
3. Let  $X$  denote the original image which the buyer (the mobile

agent) wants to purchase. The seller generates unique  $W$  randomly and embeds a unique fingerprint into content  $X$ . Let  $X'$  be the fingerprinted image with  $W$ . When an unauthorized copy  $X'$  generated from, this unique fingerprint  $W$  is used for identifying the original buyer of  $X'$ . To embed the second fingerprint  $F$  generated by the FC into  $X'$  without decrypting  $E_{y_B}^{\rightarrow}(F)$ , the seller encrypts the watermarked content  $X'$  with  $\overline{y_B^*}$  and finds the permutation  $\sigma$  satisfying  $\sigma(E_{y_B}^{\rightarrow}(F)) = E_{y_B}^{\rightarrow}(\sigma(F))$ . Because of the homomorphic property of the encryption algorithm  $E$  used by the FC, the seller can compute fingerprinted content  $E_{y_B}^{\rightarrow}(X'')$ .

4. The seller transmits  $E_{y_B}^{\rightarrow}(X'')$  to the mobile agent and stores  $y_M, \overline{y_B^*}, F, \sigma, eF, sF, sM$  and two certificates  $cert\{\overline{y_B^*}\}_{x_{FC}}$ ,  $cert\{y_M, [text]\}_{x_i}$  in his DataBase  $Table_S$ .  $Table_S$  is a table of records maintained by Seller for image  $X$  containing one entry for each copy of  $X$  that he sells.
5. The mobile agent sends  $E_{y_B}^{\rightarrow}(X'')$  to the buyer. The buyer decrypts the encrypted image  $E_{y_B}^{\rightarrow}(X'')$  and obtains the fingerprinted image  $X''$ .

Note that, buyers can decrypt the fingerprinted image encrypted with her own private key  $x_1$ .

In our protocol, the buyer does not know  $\sigma$ , she cannot remove  $\sigma(F)$  from  $X''$ .

### ■ Step 5. Traitor Identification

When an illegal copy  $X^{red}$  of an original image  $X$  is discovered,

1. The seller extracts the unique watermark  $U$  in  $X^{red}$  using detection algorithm. Then, she finds  $F$  with the highest correlation and obtains the transaction information involving  $W$  from the table by computing correlations of extracted watermark  $F$  and every watermark stored in  $Table_s$ . The information consists of  $y_M, \overline{y_B^*}, F, \sigma, eF, sF, sM$  and  $F$ . And the seller sends them with  $X, X^{red}$  to an arbiter.
2. The arbiter verifies  $sF$  with the FC's public key  $y_F$ . If the verification holds, the arbiter performs the next step.
3. The arbiter sends  $\overline{y_B^*}, cert\{\overline{y_B^*}\}_{x_F}, cert\{y_M, [text]\}_{x_1}$  to FC. Then the FC sends  $F$  back to the arbiter.
4. The arbiter computes  $\sigma(F)$  and checks the existence of  $\sigma(F)$  in  $X^{red}$  by extracting the fingerprint from  $X^{red}$  and estimating its correlations with  $\sigma(F)$ . If there exists  $\sigma(F)$ , the buyer is guilty

and the buyer's ID is revealed to the seller.

## 6.4 Analysis of Security and Efficiency

### 6.4.1 Security Analysis

- *Anonymity*: We assume that the fingerprint certificate center does not reveal the buyer's real identity if she is honest. Even if the seller and the mobile agent know a pseudonym  $\overline{y_B^*}$ , which is related to  $y_B$ , it is unknown to the seller and the mobile agent because  $x_2$  is encrypted with FC's public key. Thus buyer's anonymity is provided if the seller and the mobile agent cannot compute discrete logarithms. Therefore buyers should be able to purchase digital image anonymously in our scheme.
- *Unlinkability*: In our protocol, fingerprinted images sold to a buyer must be encrypted with each different key for unlinkability of digital contents. Also these different keys are transmitted to the seller. Thus given two digital contents, nobody can decide whether these two images (contents) were purchased by the same buyer or not.
- *Traceability*: Due to the properties of the underlying encryption

and digital signature techniques, we can assume that a malicious buyer cannot change or substitute a fingerprint generated by the fingerprints certificate center. Sellers should insert a fingerprint  $F$  and  $\sigma(F)$  in the right manner for her own interest. If she does not correctly insert  $F$  or  $\sigma(F)$ , she would not be able to identify the original buyer of an illegal copy. Further a detecting function in the fingerprint detection must guarantees that the seller can extract the unique watermark (fingerprint)  $F$  that belongs to a traitor. Thus the buyer who has distributed digital contents illegally (traitor) can be traced in our scheme.

- **No Framing:** Since, to forge  $X^{red}$  with the special watermark,  $F$ , the seller must know either the buyer's private key  $x_1$  or the buyer's unique watermark  $F$ . In our proposal, only the buyer knows his private key  $x_1$  and his unique watermark if computing discrete logarithm is hard and used encryption algorithm (underlying primitives) is secure. Because the seller cannot recreate the buyer's copy with specific watermark, an honest buyer should not be wrongly identified as a traitor in our protocol.
- **No Repudiation:** Since only the buyer can decrypt encrypted fingerprinted contents (Only the buyer knows his own secret key  $x_1$ ),

the others cannot recreate the buyer's copy. Thus the buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or a security breach of the seller's system.

- *Collusion Tolerance*: Our scheme have used Cox's algorithm [22] as a building block. The protocol is secure only as much as the underlying watermarking techniques are secure and robust. We assumed that the underlying watermarking algorithm is secure and this algorithm is pointed out to be highly resistant to collusion attacks [35].

#### 6.4.2 Efficiency Analysis

In our scheme, the buyer has to execute the registration step and delegation step, and the mobile agent does buyer's computation instead of him.

In previous schemes, the buyer has to carry out the registration step, fingerprints generation step, and fingerprints insertion step. There is no comparison between computational cost of fingerprinting step with very high complexity (based on secure multi-party protocols) and that of delegation step. Thus, it is enough to prove that our protocol is more efficient than the other previous schemes [11], [18] from the view of buyers. Our scheme is practicable and efficient scheme from the

**Table 7.** Comparison of our proposal with previous methods.

Sub-Protocol	Our Proposal	Previous Schemes
Registration	Buyer-TTP	Buyer-TTP
Delegation	Buyer, MA <sup>1</sup>	.
Fingerprint Generation	MA-TTP	Buyer-TTP <sup>2</sup> Buyer-Seller <sup>3</sup>
Fingerprints Insertion	MA-Seller	Buyer-Seller
Identification	Seller, TTP, Arbiter	Seller, TTP, Arbiter

\*1: Mobile Agent

\*2: In case of [12] scheme

\*3: In case of [11] and [20] schemes

view of buyers, because it reduces amounts of buyers' computations and memory to minimum. We briefly show the comparison between our method and the previous methods about participators of each step in the Table 7.

## 6.5 Chapter Summary

In this Chapter, we presented an anonymous fingerprinting scheme for mobile communications using mobile agent, which is efficient and feasible from a practical view. A proxy certificates are used as the basic primitive.

Utilization of mobile agents to facilitate electronic commerce oper-

ations is an appealing concept, especially when those operations are tedious or very difficult to perform by human users. But, in distributed environment, it is very difficult to assume the trust of mobile agent and the delegation key issuing protocol. The delegation to others can be risky because this means have to carry the buyer's private information to the mobile agent. This exposes the information to attacks because it is copied outside a protected environment.

To address this problem, we used proxy certificates, which avoid the need for the mobile agent to have access to the buyer's private information, but still bind the owner to the contents of an order sheet.

We used homomorphic encryption scheme to remove interactive between a mobile agent and the seller in a digital fingerprints embedding step and proxy certificates to remove risk about exposure of the buyer's private information. Our proposal satisfies all properties of anonymous fingerprinting scheme; (1) only the buyer can know the fingerprinted copy, however the buyer delegated his/her power to the mobile agent, (2) the buyer can perform fingerprinting protocol in safety. In other words, the honest buyer can not be identified as a traitor even if the mobile agent does dishonest things such as collusion with the seller, and (3) it is practical and efficient because it reduces amount of the buyer's computations to the minimum. Thus our approach is suited for the customer-centered commercial transaction and mobile communications that the client has a small memory and computation power.

## Chapter VII. Conclusions

This thesis has discussed copyright protection system using combination of watermarking and fingerprinting for preventing an illegal redistribution of digital contents.

In Chapter II, we have introduced an overview of DRM, digital watermarking, digital fingerprinting, and related areas of research which are generally referred to as "copyright protection".

In Chapter III, we have suggested secure copyright protection scheme and have discussed secure buyer-seller watermarking protocol against chosen ciphertext attack.

First, we have showed some problems of the previous copyright protection schemes. Then we have presented how to make secure fingerprinting schemes using oblivious transfer protocol. Next, we have discussed the security of buyer-seller watermarking schemes used homomorphic encryption. Here, we have showed that homomorphic encryption algorithms which the existing schemes used is not secure against chosen ciphertext attack.

In Chapter IV, we first proposed an anonymous buyer-seller watermarking protocol to multi-purchase environment. If we apply the pre-

vious scheme to multi-purchase case, the number of keys held by buyer's devices increases in proportion to that of contents purchased. To solve this inefficiency, we have suggested a scheme that satisfied anonymity and unlinkability, where a buyer executes registration step one time and the number of buyer's necessary key is also one regardless of that of contents. Our proposal is significant in the sense that it is the first scheme applied to multi-purchase environments efficiently.

In Chapter V, we have suggested a secure and efficient watermarking-based protocol for broadcast video. First we have showed the insecurity and inefficiency of the previous scheme. Compared with the previous scheme, our scheme is secure and provides asymmetry without a watermark generation authority. Another meaningful feature of our scheme is to consider a subscriber's anonymity, which is one of important requirement for electronic marketplaces.

In Chapter VI, we first have proposed an anonymous fingerprinting scheme for mobile communications using mobile agent, which is efficient and feasible from a practical view. Here, we introduced a concept of mobile agent with proxy certificates, which removes risk about exposure of the buyer's private information. Our proposal satisfies all properties of anonymous fingerprinting scheme. Our approach is suited for the customer-centered commercial transaction and mobile communications that the client has a small memory and computation power.

In conclusion, we have suggested secure copyright protection schemes applied to most environments such as single-purchase, multiple-purchase, broadcast, and mobile communications in this thesis.

# References

- [1] S. Katzenbeisser and F. Petitcolas, *Information hiding: techniques for steganography and digital watermarking*, Artech House, ISBN 1-58053-035-4.
- [2] J. A. Bloom, I. J. Cox, T. Kalker, J. P. Linnartz, M. L. Miller, and C. B. S. Traw, "Copy protection for DVD video," *Proc. IEEE*, vol. 87, pp. 1267-1276, July 1999.
- [3] J. P. Linnartz and G. Maes, "The 'ticket' concept for copy control based on embedded signalling," *5th Computer Security European Symposium on Research in Computer Security*, J. J. Quisquater et al., Eds. Springer-Verlag, vol 1485, pp. 257-274, 1998.
- [4] G. R. Blakely, C. Meadows, and G. B. Purdy, "Fingerprinting long forgiving messages," *Advances in cryptology Crypto'85*, Hugh C Williams, Ed. Springer-Verlag, vol. 218, pp. 180-189, 1986.
- [5] J. Löfvenberg, *Codes for digital*, Linköping Studies in Science and Technology Dissertation No. 722.
- [6] J. Postel, "Out-of-Net host address for mail," *IETF RFC 754*, The Internet Engineering Task Force, Apr. 1979.
- [7] L. Qian and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *Journal of Visual Commun. Image Represent*, vol. 9, pp. 194-210, Sep. 1998.
- [8] N. R. Wanger, "Fingerprinting," *Proc. IEEE Symposium on Security and*

*Privacy*, pp. 18-22, 1983.

- [9] B. Pfitzman and M. Schunter, "Asymmetric fingerprinting," *Advances in cryptology-Eurocrypt'96*, U. Maurer Ed. Springer-Verlag, vol. 1070, pp. 84-95, 1996.
- [10] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Processing*, vol. 10, no. 4, pp. 643-649, April 2001.
- [11] B. Pfitzman and W. Waidner, "Anonymous fingerprinting," *Advances in cryptology-Eurocrypt'97*, W. Fumy Ed. Springer-Verlag, vol. 1233, pp. 88-102, 1997.
- [12] H. S. Ju, H. J. Kim, D. H. Lee, and J. I. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," *5th international conference on information security and cryptology*, P. J. Lee and C. H. Lim Eds. Springer-Verlag, vol 2587, pp. 421-432, 2002.
- [13] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *Advances in cryptology Crypto'95*, Ivan Damgard et al., Eds. Springer-Verlag, vol. 963, pp. 452-465, 1995.
- [14] D. R. Stinson, T. van Trung, and R. Wei, "Secure frameproof codes, key distribution patterns, group testing algorithms and related structures," *Journal of Statistical Planning and Inference*, vol. 86, no 2, pp. 595-617, 2000.
- [15] D. Kahn, *The codebreakers-the story of secret writing*, NewYork, NewYork, USA: Scribner, 1996.
- [16] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," *IEEE Trans. Information theory*, vol. 46, pp. 893-910, May 2000.

- [17] D. Chaum, I. Damgard, and J. van de Graaf, "Multiparty computation ensuring privacy of each party's input and correctness of the result," *Advances in cryptology Crypto'87*, C. Pomerance Ed. Springer-Verlag, vol. 293, pp. 86-119, 1995.
- [18] B. Pfitzman and A. R. Sadeghi, "Coin-based anonymous fingerprinting," *Advances in cryptology-Eurocrypt'99*, J. Stern Ed. Springer-Verlag, vol. 1592, pp. 150-164, 2000.
- [19] J. Domingo-Ferrer and J. H. Joancomarti, "Efficient smart-card based anonymous fingerprinting," *Smart card research and applications 1998*, J. J. Quisquaater and B. Schneier Eds. Springer-Verlag, vol 1820, pp. 221-228, 2000.
- [20] J. Domingo-Ferrer, "Anonymous fingerprinting based on committed oblivious transfer," *International workshop on practice and theory in public key cryptography'99*, H. Imai and Y. Zheng Eds. Springer-Verlag, vol 1560, pp. 43-52, 1999.
- [21] A. R. Sadeghi, "How to break a semi-anonymous fingerprinting scheme," *4th international workshop on information hiding*, I. S. Moskowitz Ed. Springer-Verlag, vol. 2137, pp. 384-394, 2001.
- [22] I. J. Cox, J. Kilian, T. Leighton, and T. Shamnon, "Secure spread spectrum watermarking for image, audio and video," *IEEE Trans. Image Processing*, vol.6, no 12, pp. 1673-1678, Dec. 1997.
- [23] M. Rabin, "How to exchange secrets by oblivious transfer," *Technical Report, Tech. Memo. TR-81*, Aiken Computation Laboratory, Harvard University, 1981.

- [24] C. Crupeau, J. van de Graaf, and A. Tapp, "Committed oblivious transfer and private multi-party computation," *Advances in cryptology Crypto'95*, Ivan Damgard et al., Eds. Springer-Verlag, vol. 963, pp. 110-123, 1995.
- [25] J. G. Choi, K. R. Kwon, and J. H. Park, "Analysis of COT-based fingerprinting schemes: new approach to design practical and secure fingerprinting scheme," *7th International workshop on information hiding*, J. Fridrich Ed. Springer-Verlag, vol. 3200, pp. 265-279, 2004.
- [26] J. G. Choi, J. H. Park, and T. S. Kim, "Secure oblivious transfer protocol-based digital fingerprinting against conspiracy attack," *Journal of Korea Institute of Information Security and Cryptology*, vol. 14, no 3, pp. 146-153, 2004.
- [27] J. Camenisch and I. Damgard, *Verifiable encryption and applications to group signatures and signatures sharing*, Technical Report RS 98-32, Brics, Department of Computer Science, University of Aarhus, Dec. 1998.
- [28] J. G. Choi, K. Sakurai, and J. H. Park, "An anonymous buyer-seller watermarking without trust assumptions," *Proc. Computer Security Symposium 2003*, pp. 71-76, 2003.
- [29] J. G. Choi, K. Sakurai, and J. H. Park, "Secure anonymous buyer-seller watermarking protocol against conspiracy attack," *Proc. ISEC, IEICE 1003-196*, pp. 75-82, 2003.
- [30] J. G. Choi, K. Sakurai, and J. H. Park, "Does it need trusted third party? design of buyer-seller watermarking protocol without trusted

- third party," *Applied cryptography and network security 2003*, J. Zhou et al., Eds. Springer-Verlag, vol. 2846, pp. 265-279, 2003.
- [31] B. M. Goi, R. C. W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi, "Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity," *2nd Applied cryptography and network security*, Jakobsson et al., Eds. Springer-Verlag, vol. 3089, pp. 369-382, 2004.
- [32] J. G. Choi and J. H. Park, "New anonymous fingerprinting scheme based on the proxy signature and committed oblivious transfer," *SK Telecommunications Review*, vol. 12, no 5, pp. 711-719, 2002.
- [33] Q. H. Wu, J. H. Zhang, and Y. M. Wang, "Practical t-out-n oblivious transfer and its applications," *5th international conference on information and communications security-ICICS2003*, S. Qing et al., Eds. Springer-Verlag, vol. 2836, pp.226-237, 2003.
- [34] F. Bao, R. Deng, and P. Feng, "An efficient and practical scheme for privacy protection in e-commerce of digital goods," *International conference on information and communications security 2000*, Dongho Won, Ed. Springer-Verlag, vol. 2836, pp. 167-170, 2000.
- [35] J. Killian, F. T. Leighton, L. R. Matheson, T. G. Shannon, R. E. Tarjan, and F. Zane, "Resistance of digital watermarks to collusive attacks," *Proc. IEEE ISIT*, pp. 271, 1998.
- [36] D. Chaum, J. H. Evertse, and J. van de Graaf, "An improved protocol for demonstrating possession of discrete logarithms and some generalization," *Advances in cryptology Eurocrypt'87*, D. Chaum and W.

- L. Price Eds. Springer-Verlag, vol. 304, pp. 87-119, 1987.
- [37] R. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.
- [38] J. D. Cohen and M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," *Proc. IEEE, 26th Annu Symp. Foundations Computer Science*, pp. 372-382, July 1985.
- [39] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge of knowledge and chosen ciphertext attack," *Advances in cryptology-crypt'91*, J. Feigenbaum Ed. Springer-Verlag, vol. 576, pp. 433-444, 1992.
- [45] J. G. Choi, J. H. Park, and K. Sakurai, "Fingerprinting scheme suitable to multi-purchase," *Proc. Computer Security Symposium*, vol 16, pp. 29-34, Oct. 2002.
- [40] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in cryptology Crypto'98*, H. Krawczyk Ed. Springer-Verlag, vol. 1462, pp. 13-25, 1998.
- [41] P. A. Fouque and D. Pointcheval, "Threshold cryptosystems secure against chosen-ciphertext attacks," *Advances in cryptology-Asiacrypt 2001*, C. Boyd Ed. Springer-Verlag, vol. 2248, pp. 351-368, 2001.
- [42] J. Katz and M. Yung, "Threshold cryptosystems based on factoring," *Advances in cryptology-Asiacrypt 2002*, Y. Zheng Ed. Springer-Verlag, vol. 2501, pp. 192-205, 2002.

- [43] M. Naor and M. Yung, "Public key cryptosystems provably secure against chosen ciphertext attacks," *Proc. 22nd ACM Symposium on theory*, pp. 427-437, 1990.
- [44] T. Nakanish, N. Haruna, and Y. Sugiyama, "Unlinkable electronic coupon protocol with anonymity control," *2nd international workshop on information security-ISW'99*, M. Mambo and Y. Zheng Eds. Springer-Verlag, vol. 1729, pp. 37-46, 1999.
- [46] J. G. Choi and J. H. Park, "A generalization of an anonymous buyer-seller watermarking protocol and its application to mobile communications," *3rd International workshop on digital watermarking*, I. J. Cox et al., Eds. Springer-Verlag, vol. 3304, pp. 232-243, 2004.
- [47] J. G. Choi and K. H. Rhee, "Design of digital fingerprinting for multi-purchase," *Journal of Korea Multimedia Society*, vol 7, no 12, pp. 1708-1718, 2004.
- [48] R. Anderson and C. Manifivas, "Chameleon-A new kind of stream cipher," *4th international workshop on fast software encryption*, Eli Biham, Ed. Springer-Verlag, vol. 1267, pp. 107-113, 1997.
- [49] I. Brown, C. Perkins, and J. Crowcroft, "Watercasting: distributed watermarking of multicast media," *First international workshop on networked group communication*, L. Rizzo and S. Fdida Eds. Springer-Verlag, vol. 1736, pp. 286-300, 1999.
- [50] P. Judge and M. Ammar, "WHIM: watermarking multicast video with a hierarchy of intermediaries," *International Journal of Computer*

- and Telecommunications Networking*, vol. 39, issue 6, pp. 699-712, 2000.
- [51] H. H. Chu, L. Qiao, and K. Nahrstedt, "A secure multicast protocol with copyright protection," *Proc. SPIE Symposium on Electronic Imaging, ACM SIGCOMM Computer Communication Review*, vol. 32, no. 2, pp. 42-60, 2002.
- [52] A. Fiat and T. Tassa, "Dynamic traitor tracing," *Journal of cryptology*, vol. 14, no. 3, pp. 211-223, 2001.
- [53] R. S. Naini and Y. Wang, "Sequential traitor tracing," *IEEE Trans. Information Theory*, vol. 49, no. 5, pp. 1319-1326, 2003.
- [54] S. Emmanuel and M. S. Kankanhalli, "A digital rights management scheme for broadcast video," *Journal of Multimedia System*, vol. 8, no. 6, Springer-Verlag, pp. 444-458, 2003.
- [55] H. Niederreither, "Knapsack-type cryptosystem based on algebraic coding theory," *DSN Progress, Report 42-44*, pp. 114-116, 1978.
- [56] V. M. Sidelnikov and S. O. Shestakov, "On the insecurity of cryptosystems based on generalized reed-solomon codes," *Discrete Mathematics and applications*, vol. 1, no. 4, pp. 439-444, 1992.
- [57] R. J. McEliece, "A public key cryptosystem based on algebraic coding theory," *JPL DSN Progress Rep.*, pp.114-116, 1978.
- [58] J. K. Gibson, "Equivalent goppa codes and trapdoors to McEliece's public key cryptosystem," *Advances in cryptology Eurocrypto'91*, D. W. Daview Ed. Springer-Verlag, vol. 547, pp. 517-521, 1992.
- [59] R. Heiman and A. Shamir, *On the security of cryptosystems based on linear error correcting codes*, Applied Mathematics, Weizmann Institute

of Science , Rehovot, Israel, 1987.

- [60] J. G. Choi, K. Sakurai, and J. H. Park, "An efficient fingerprinting scheme with proxy signature," *Proc. Symposium on Cryptography and Information Security 2003*, pp. 1151-1156, Jan. 2003.
- [61] J. G. Choi, K. Sakurai, and J. H. Park, "An approach to materialize digital fingerprinting based on proxy signature schemes," *Proc. 12th International World Wide Web 2003*, pp. 197, May 2003.
- [62] J. G. Choi, K. Sakurai, and J. H. Park, "Proxy certificates based digital fingerprinting scheme for mobile communication," *Proc. 37th IEEE International Carnahan Conference on Security Technology*, pp. 587-594, Oct. 2003.
- [63] A. Romao and M. M da Silva, "Secure mobile agent digital signatures with proxy certificates," *E-Commerce Agents*, J. Liu and Y. Ye Eds. Springer-Verlag, vol 2033, pp. 206-220, 2001.

# Curriculum Vitae

## Personal Data

- Name Jae-Gwi Choi
- Gender Female
- Date of Birth Apr. 10. 1972.

## Education

- Feb. 1998. B.E. in Dept. of Computer Science, Pukyong National Univ, South of Korea.
- Aug. 2001. M.E. in Dept. of Computer Science Education, Pukyong National Univ.
- Oct. 2002~Aug. 2003. A Short-term Exchange student, in Dept. of Computer and Communication Engineering, Kyushu Univ. Japan. (Support by Japan Society for the Promotion of Science)
- Apr. 2004~Sep. 2004. Internship, Institute of Industrial Science, Tokyo Univ. Japan. (Support by Korea Science and Engineering Foundation)
- Aug. 2005. Ph.D. in Dept. of Information Security, Pukyong National Univ.

## Employment

- Apr. 1999~Mar. 2001. An Assistant Teacher, in Div. of Electronic Computer Information Communication, Pykyong National Univ.
- 2001~2003, 2005. A part-time Teacher, in Div. of Electronic Computer Information Communication, Pykyong National Univ.

## Publications

### ● International Papers

#### Journal paper

- [1] J. G. Choi, Goichiro Hanaoka, K. H. Rhee, and Hideki Imai, "How to break COT-based fingerprinting schemes and design new one," *IEICE Trans. Fundamentals*, Oct. 2005.

#### Conference papers

- [1] J. G. Choi and J. H. Park, "A generalization of an anonymous buyer-seller watermarking protocol and its application to mobile communications," *IWDW2004, LNCS 3304, Springer-Verlag*. pp.232-243, Oct. 2004.
- [2] J. G. Choi, J. H. Park, and K. R. Kwon, "Analysis of COT-based fingerprinting schemes: new approach to design practical and secure fingerprinting scheme," *IHW2004, LNCS3200, Springer-Verlag*. pp.253-265, May. 2004.
- [3] J. G. Choi, K. Sakurai, and J. H. Park, "Does it need trusted party? Design of buyer-seller watermarking protocol without trusted third party," *ACNS2003, LNCS 2846, Springer-Verlag*. pp.265-279, Oct. 2003.
- [4] J. G. Choi and J. H. Park, "Unforgeable RFID variable ID

- scheme with efficient identification," *International Conference on Computing, Communications and Control Technologies*, Volume 2, pp.34-38, Aug. 2004.
- [5] J. G. Choi, K. Sakurai, and J. H. Park, "Proxy certificates based digital fingerprinting scheme for mobile communication," *Proc of 37th IEEE Int'l Carnahan Conf. on Security Technology*, pp.587-594, Oct. 2003.
- [6] J. G. Choi and J. H. Park, "An efficient anonymous fingerprinting scheme based on COT," *Proc. of The 2002 Korea-Japan Joint Symposium on Advanced Engineering & Science*, pp.118-123, Aug.2003.
- [7] J. G. Choi, K. Sakurai, and J. H. Park, "Secure anonymous buyer-seller watermarking protocol against conspiracy attack," *Proc. of ISEC, IEICE*, Vol. 1003, No 196, pp.75-82, Jul. 2003.
- [8] J. G. Choi, K. Sakurai, and J. H. Park, "An approach to materialize digital fingerprinting based on proxy signature schemes," *Proc. of the 12<sup>th</sup> International World Wide Web 2003*, pp.197, May. 2003.
- [9] J. G. Choi, K. Sakurai, and J. H. Park, "An anonymous buyer-seller watermarking without trust assumptions," *Computer Security Symposium 2003*, Vol 2003, No. 45, pp.71-76, May. 2003.
- [10] J. G. Choi, K. Sakurai, and J. H. Park, "Anonymous fingerprinting with a robust asymmetry," *Proc. of 2003 International Conference on Multimedia Technology and Its Application*, pp.422-429, Jan. 2003.
- [11] J. G. Choi, K. Sakurai, and J. H. Park, "An efficient fingerprinting scheme with proxy signature," *Proc. of the*

- Symposium on Cryptography and Information Security 2003*, pp.1151-1156, Jan. 2003.
- [12] J. G. Choi, K. Sakurai, and J. H. Park, "An anonymous fingerprinting scheme with a strong anonymous and a True asymmetry," *Proc. of the Symposium on Cryptography and Information Security 2003*, pp.1157-1162, Jan. 2003.
- [13] J. G. Choi, J. H. Park, and K. Sakurai, "Fingerprinting scheme suitable to multi-Purchase," *Computer Security Symposium 2002*, Vol 2002, No.16, pp.29-34, Oct. 2002.
- [14] J. G. Choi and J. H. Park, "A study on undeniable multi-signature scheme verified with partial", *Proc. of East-Asian Language Processing and Internet Information Technology*, pp.93-96. Jan, 2002.

## ● Domestic Papers

### Journal papers

- [1] J. G. Choi, and K. H. Rhee, "Design of digital fingerprinting for multi-purchase," *Journal of Korea Multimedia Society*, Vol 7, No 12, pp.1708-1718, Dec. 2004.
- [2] J. G. Choi, and J. H. Park, "Unforgeable RFID tag variable ID scheme with efficient identification," *Journal of Korea Information Processing Society*, Vol 14, No 3, pp.146-153, Aug. 2004.
- [3] J. G. Choi, T. S. Kim, and J. H. Park, "Secure oblivious transfer protocol-based digital fingerprinting against conspiracy attack," *Journal of Korea Institute of Information Security and Cryptography*, Vol 11-C, No 4, pp.447-454, Jun. 2004.
- [4] J. G. Choi, J. H. Park, and Kouichi Sakurai, "An anonymous fingerprinting scheme with a robust asymmetry," *Journal of Korea Multimedia Society*, Vol 6, No 4, pp.620-629, Jul. 2003.

- [5] J. G. Choi, and J. H. Park, "New anonymous fingerprinting scheme based on the proxy signature and committed oblivious transfer," *SK Telecommunication Review*, Vol 12, No 5, pp.711-719, Oct. 2003.

### **Conference papers**

- [1] J. G. Choi, and K. H. Rhee, "Is secure buyer-seller watermarking protocols against conspiracy attack," *Proc. of Korea Multimedia Society*, Vol 11, No 1, pp.110, May. 2005.
- [2] J. G. Choi, S. H. Lim, and J. H. Park, "Secure oblivious transfer protocol-based digital fingerprinting against conspiracy attack," *Proc. of Korea Institute of Information Security and Cryptology*. pp. 45-53, Feb. 2004.
- [3] B. M. Seo, S. J. Kim, J. G. Choi, and J. H. Park, "Contents protection system model for digital broadcasting using traitor tracing scheme," *Proc. of Korea Information Processing Society*, pp.1831-1834, Nov. 2003.
- [4] J. G. Choi, J. H. Park, and Kouichi Sakurai, "An efficient anonymous digital fingerprinting scheme for multiple purchases using message recovery signature," *Proc. of Korea Institute of Information Security and Cryptology*, pp.79-89, Feb. 2003.
- [5] S. J. Kim, J. G. Choi, and J. H. Park, "One-time proxy signature with efficiency," *Proc. of Korea Institute of Information Security and Cryptology*, pp.24-28, Feb. 2003.
- [6] J. G. Choi, and J. H. Park, "An anonymous fingerprinting scheme with redistribution after tracing a traitor," *Proc. of Korea Multimedia Society*, pp.229-233, Nov, 2002.
- [7] S. J. Kim, J. G. Choi, and J. H. Park, "Efficient license download with anonymity," *Proc. of Korea Multimedia Society*, pp.945-948,

Nov. 2002.

- [8] S. J. Kim, J. G. Choi, and J. H. Park, "Efficient one-time proxy signature with anonymity," *Proc. of Korea Information Processing Society*, pp.224-228, Nov. 2002.
- [9] S. J. Kim, M. H. Lee, J. G. Choi, and J. H. Park, "An extension of proxy signature and its application," *Proc. of Korea Multimedia Society*, pp.844-848, May. 2002.

# Acknowledgments

Facing the conferment of a doctor's degree gives me a lot of thoughts. It has been already 3 and half years since I came here. Even though the first day at graduate school has started just like any other day, each and every day made me understand why they often say that writing a good paper is as painful as women's giving a birth. I believe that, for those years, I tried to learn more and study more with every possible effort, even more than when I was in Mater's course. But yet, to finish my degree with this dissatisfied thesis puts me to shame rather than to joy. For me to have this moment, there has been many people who stood by me and encouraged me continuously over the time. I wish to give my thanks to those people through this short note.

First I'd like to thank my adviser, Prof. KyungHyune Rhee, as I could finish my degree only with his concerns and considerations for me. It wasn't that long but the time in the Lab, which I started with many concerns and worries at first, has been comfortable and enjoyable because of him. I will remember all his wisdom for life and learning and try to live up to them in my everyday's life.

And then I'd like to thank Prof. ChangSoo Kim and SangUk Shin, who were in the thesis committee and willingly advised me a lot for my thesis. There are also professors in Dept. of Information Security and professors in Dept. of Computer Science, who I'd like to extend my thanks to, too. Especially I thank Prof. SungJin Cho, who gave us wonderful and also instructive lectures in every semester. I will

try to measure up to their expectation for me.

There are also Prof. KiRyong Kwon and DongKyue Kim, who took the examiner's job even while they were so busy and gave me a lot of good advice for my thesis as well as my career afterwards. Their warm encouragement and earnest advice gave me a courage to go through all this hardship and helped me to develop a new vision for my study. Once again, I express my thanks to them.

Next, I'd like to say thanks to Prof. Hideki Imai and Prof. Kouichi Sakurai, who have been watching me since my days in Japan and given me a lot of help and information. I also want to say thanks to Prof. DukHong Moon, Prof. JunHyo Kim, Prof. SungYong Bae, YongSuk Hur, KyueSung, WonGeun, EunKyeong, JunHo, SangKyun, and JuYoung, all of whom made my life abroad rich rather than harsh and rough.

And here I want to show gratitude and respect for the late Prof. JiHwan Park who lead me to the right path of learning as well as of life sometimes as a strong teacher would do and sometimes like a warm and affectionate father. From time to time I couldn't help myself thinking that it is too hard to meet his high expectation, but now I realize that without his trust and support, there wouldn't be me as I am. Now he's gone and all I could do is just to miss his strict instruction. But his teachings will live in my heart, which will prevent me getting lazy but only push me to try even harder. I know I will keep on working hard to make him proud of me even from the heaven. Once again I give my thanks and respects to him from the bottom of my heart.

There is also colleagues in Multimedia security & applications Lab and Information security & Internet applications Lab, who I want to thank. The time spent in Multimedia security & applications Lab, laughing and shedding tears with colleagues became the most precious experience and memory of my life. Now the Lab, which connected us together, disappeared. But I believe that the time we had with the late Prof. JiHwan Park and his teachings will always be there to keep us close continuously. I thank them for their concerns and affections toward me over the time. Also I have to say thanks to colleagues in Information security & Internet applications Lab, who constantly supported me for last one year while I was having a difficulty to fit into a new environment.

To my family, who have endured me while I was neglecting them with an excuse of studying, I say "Thank you and I'm sorry". My sisters and brothers in law have been there all the time to watch and support me whenever I felt exhausted and dismayed. And my mother, with her endless capacity of love for me, she shared all my joys and tears with me together. Thanks for her love and support from the bottom of my heart.

I dedicate this thesis, the final result of my work and efforts for years, to my parents.

## 감사의 글 (in Korean)

박사 학위를 앞둔 지금, 많은 생각들이 스쳐 지나갑니다. 3년 6개월이라는 박사과정, 시작은 작았지만, 한 편의 좋은 논문을 만든다는 것이 말로 표현 못할 산고(産苦)에 비유되는 것이 이해되는 날들이었습니다. 석사때보다 더 많이 배우고, 더 많이 공부하며, 부족하나마 노력을 다해 지낸 시간이었지만, 이렇게 모자란 논문으로 결실을 맺으니 기쁨보다는 부끄러운 마음이 앞섭니다. 지금까지 저를 옆에서 지켜봐 주시며 끊임 없이 힘을 주신 많은 분들께 이 지면을 통해 감사의 말을 전하고자 합니다.

지도교수인 이경현 교수님께 감사드립니다. 교수님의 아낌없는 관심과 배려 덕분에 무사히 학위를 마칠 수 있었습니다. 그리 길지 않은 시간이었지만, 많은 고민과 걱정으로 시작했던 연구실 생활도 교수님 덕분에 편안하고 즐거운 마음으로 지낼 수 있었습니다. 학문과 삶에 대한 교수님의 말씀 하나 하나 새겨가며 최선을 다해 살아가겠습니다.

그리고 논문 심사를 맡아 주셔서 많은 지도를 해 주신 김창수 교수님과 신상욱 교수님께도 감사드리며, 항상 가까이서 편안한 마음으로 공부를 할 수 있게 해 주신 정보보호학과 교수님과 전자계산학과 여러 교수님들께도 감사를 드립니다. 특히 매학기 마다 유익한 강의를 해 주신 조성진 교수님께 감사의 말을 전하고 싶습니다. 교수님들의 기대에 어긋나지 않도록 열심히 살아가겠습니다.

또한 바쁘신 가운데 학위논문 심사를 맡아주시고 논문뿐만 아니라 진로에 대해서도 많은 조언을 해 주신 권기룡 교수님과 김동규 교수님께도 감사드립니다. 교수님들의 따뜻한 격려와 진심어린 충고는 저에게 큰 힘이 되었을 뿐만 아니라, 연구에 대한 새로운 시야를 가지게 해 주

었습니다. 감사드립니다.

그리고 일본 유학생활동부터 저를 지켜봐 주시며 많은 정보와 도움을 주신 Hideki Imai 교수님과 Kouichi Sakurai 교수님께도 감사드리며, 자칫 메마를 뻔했던 유학생활동을 풍요롭게 해 준 문덕홍 교수님, 김준효 교수님, 배성용 교수님과 허용석 선생님, 규성이, 원근이, 은경이, 준호, 상균이, 주영이에게도 감사의 마음을 전합니다.

그리고 엄한 스승의 모습으로, 때로는 따뜻한 아버지의 모습으로 학문적으로는 물론 삶의 바른 길을 지도해 주신 故 박지환 교수님께 깊은 존경과 감사를 드립니다. 때로는 교수님의 지나친 기대에 힘들어하기도 했지만, 교수님의 신뢰와 격려가 없었더라면 지금의 저도 없었을 것입니다. 이젠 교수님의 무서운 훈계마저 그렇지만, 교수님이 저에게 준 가르침과 용기를 가슴에 새기며 교수님의 제자라는 사실에 누가 되지 않도록 열심히 살아가겠습니다. 다시 한번 진심으로 존경과 감사의 말을 올립니다.

그리고 멀티미디어 보호 및 응용 연구실과 정보 보호 및 인터넷 응용 연구실의 선배님, 동기, 그리고 후배님에게도 감사드립니다. 멀티미디어 보호 및 응용 연구실에서 함께 울고 웃으며 보낸 시간들은 그 무엇과도 바꿀 수 없는 소중한 경험이고 추억입니다. 비록 우리를 하나로 묶어준 연구실은 사라졌지만, 故 박지환 교수님의 가르침과 함께 했던 지난 시간이 계속해서 우리를 한 울타리로 묶어줄 것이라 믿으며, 그동안 보여준 관심과 애정에 감사의 뜻을 전합니다. 또한 새로운 환경에 적응하지 못해서 힘들었던 지난 1년간, 끊임없이 힘이 되어 준 정보 보호 및 인터넷 응용 연구실 가족들에게도 깊은 감사를 드립니다.

그리고 공부한다는 핑계로 너무나 오랫동안 소홀하게 대했던 나의 가족에게 미안하다는 말과 함께 고맙다는 말을 전합니다. 늘 옆에서 지켜

보며 힘들고 지친 나에게 힘이 되어 준 언니와 형부, 제부, 그리고 동생에게 고마움을 전합니다. 마지막으로 내가 힘들 때나 기쁠 때, 같이 힘들어하고, 기뻐해 주신 나의 어머니, 어머니의 헌신적인 사랑에 감사드리며, 이 논문을 사랑하는 나의 어머니와 아버님에게 바칩니다.