Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 29 (2007) 229–237
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

A lightweight and anonymous copyright-protection protocol

Tzung-Her Chen [a,*], Gwoboa Horng [b]

[a] *Department of Computer Science and Information Engineering, National Chiayi University, 300 University Rd., Chia-Yi City, Taiwan 600, ROC*
[b] *Department of Computer Science, National Chung-Hsing University, Taiwan, ROC*

Received 15 November 2005; accepted 25 March 2006
Available online 30 May 2006

Abstract

Gradually, copyright-protection protocols have attracted much attention in that they provide effective copyright protection mechanisms. Asymmetric copyright-protection protocols allow the buyer to know and possess the protected content yet the seller has no idea about it. Subsequently, if an illegal copy is found, the seller can identify the buyer by cooperating with a trusted third party. Most copyright-protection protocols adopt public-key cryptosystems to achieve asymmetry. However, both encryption and decryption of multimedia based on public-key cryptosystems have the drawbacks of requiring high computational complexity and suffering from the burden of maintaining Public Key Infrastructure. Hence, enhancement and further development of these protocols are both necessary and central to the development of future e-commerce. In this paper, a lightweight copyright-protection protocol, benefiting from combining secret-key cryptosystems and a tamper-resistant device, is proposed to provide not only asymmetry of the protocol but also transaction anonymity of the buyer. Since the tamper-resistant device, generally speaking, provides a higher security level and is more and more commonly used, the schemes based on a tamper-resistant device are more practical than before. Moreover, the proposed protocol is computationally efficient and the key management is simple.

Keywords: Anonymous; Asymmetry; Copyright-protection protocol; Watermarking; Fingerprinting; Tamper-resistant machine

1. Introduction

Copyright protection, aimed to encourage the creator of contents to promote the societal and cultural evolution, has been a well-known policy for several centuries now. Due to the rapid growth of broadband networks, distribution of digital contents, such as online video, audio and e-books, over the Internet is a must way to go. Digital content is easier and faster to be duplicated, modified and redistributed than before. Hence, digital content protection has become one of the most important and urgent issues.

Traitor tracing is a cryptographic system which can be used to trace an adversary for illegal redistribution by tracking the individual decryption key [1,2]. When a pirate decoder is confiscated, the pirate decryption key is exposed. Therefore, the content provider can identify the traitor and thus the traitor is found guilty. The major drawback is that once the decoder decrypts and outputs the decrypted contents in the customer end, the customer is able to duplicate and redistribute the contents without being identified. This implies that traitor tracing schemes lack the capability of copyright protection.

Recently, digital watermarking techniques, a complement to cryptography, are growing at an exponential rate. Watermarking based on steganographic systems can embed information directly into digital contents. Basically, there are two classes of robust digital watermarking: copyright watermarking and fingerprint watermarking.

Copyright watermarking embeds an *identical copyright message*, so-called *watermark*, which indicates the owner's or creator's identification, into each copy of the digital content. Copyright watermarking is used to declare the copyright. Therefore, this technique cannot be used to trace the person who distributes illegal copies.

Fingerprint watermarking (also called fingerprinting) embeds a *unique fingerprint message*, so-called *fingerprint*, into an individual copy. Therefore, it can be used to track illegal customers. It's noteworthy that fingerprinting can be quite expensive in order to resist collusion attacks. Nevertheless there are researches that claimed to have successfully addressed collusion attacks [3]. Furthermore, the essential challenge of both

* Corresponding author.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

0920-5489/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2006.03.010

copyright watermarking and fingerprinting is that robustness to digital watermarking is still an open problem.

Most fingerprinting schemes suffer from that there is no lawful basis for content suppliers to sue the illegal customers. This is because almost all proposed fingerprinting schemes assume that the owners themselves, who embed fingerprints into digital contents, are trustworthy. Unfortunately, this is not always true. Because both the seller and the buyer know the same fingerprinted content, there is no way, from the technical aspect, to distinguish who actually distributes the fingerprinted copy illegally. That is, they fail in solving the dispute of copyright protection. Therefore, copyright watermarking or fingerprint watermarking alone is not sufficient to resolve the rightful copyright of the digital content.

Thus, a copyright-protection protocol relying on the well-defined cryptographic tools is necessary. From the application point of view, copyright-protection protocols could be further classified as follows:

1. *Symmetry*: The seller knows the embedded fingerprint which is uniquely linked with the buyer. That is, the seller knows the protected contents sold to the buyer. Therefore, the judge cannot determine who is guilty of illegal distribution due to ambiguity.
2. *Asymmetry*: In an asymmetric copyright-protection protocol, only the buyer knows and possesses the protected content. Subsequently, if an illegal copy found by the seller, the seller can identify the buyer and prove to the judge that the buyer is guilty for illegal distribution.
3. *Anonymous asymmetry*: Other than having the advantage of asymmetric schemes, an anonymous scheme can further guarantee the buyer's privacy. Nevertheless if his subsequent illegal distribution is found then his identity will be revealed according to the clue embedded in the distributed copy.

In 1998, Qian and Nahrstedt [4] proposed an owner–customer copyright-protection protocol. In their scheme, the owner or seller still possesses the exact protected copy that the buyer received. Hence, the buyer can still claim that the found unauthorized copy is distributed by the owner or the seller. Memon and Wong [5] proposed an asymmetric buyer–seller copyright-protection protocol in which the seller does not know the exact protected copy that the buyer received. Unfortunately, as pointed out in [6] the Memon–Wong scheme suffers from unbinding problems, failing to provide the mechanism on binding a chosen watermark to a specific digital content or a specific transaction. Thus, when the seller finds a pirated copy, it is possible for the seller to transplant the watermarks embedded in the pirated copy into another copy of a higher-priced content to form piracy in such a way he/she illegally profits more. With the anonymity of the buyer in addition, Lei et al., not only provide a fix to the Memon–Wong scheme but also form a new one. Inspired by [5], Chen et al. recently proposed an anonymous buyer–reseller watermarking protocol to address the digital contents redistribution in the second-hand markets [7]. Tomsich and Katzenbeisser also proposed another asymmetric copyright-protection protocol using a trusted tamper-proof hardware [8].

Unfortunately, the major common drawback of [4–8] is that encryption or decryption of the whole content based on a public-key cryptosystem gives rise to the drawback of high computation complexity. Moreover, since each entity including the seller and the buyer owns a pair of keys, a private key and a corresponding public key, their schemes suffer from the expensive complexity of public-key infrastructure (**PKI**) [9].

It's worthwhile to note that in the field of security more and more researches show that tamper-resistant machine (hereafter **TRM** for short) hardware provides higher security level than software technique [8,10]. **TRM** has been studied for many years and used in realistic applications, such as Cable **TV** box, **DVD** and applications with smart cards, etc.

Since tamper-resistant hardware is claimed to be the most obvious solution to the digital rights management (**DRM**) problem [10], how to benefit from combining a copyright-protection protocol with **TRM** with low overhead is the main focus of this chapter. An anonymous and asymmetric copyright-protection protocol will be proposed. The protected content received from the seller contains both a watermark, indicating the copyright, and a fingerprint, indicating the unique serial number of the **TRM** which is registered to a trusted registration authority and bound to the individual buyer. Cooperating with a trusted third party, the identity of the buyer with the **TRM** will be revealed and accused of his illegal redistribution.

With asymmetry, the seller has no idea about any sold fingerprinted content associated with the buyer. Hence, the seller cannot profit from reselling the content sold to the buyer and subsequently accuse the buyer of illegal redistribution. On the other hand, the buyer has no excuse to deny his illegal redistribution.

Furthermore, the proposed protocol enables anonymous transactions between a buyer and a seller in order to further protect the privacy of the buyer. Compared with [4–8], encrypting or decrypting the content with secret-key cryptosystems [9] clearly makes the proposed protocol efficient. Since the tamper-resistant device, generally speaking, provides a higher security level and is more and more common, the scheme is more practical than before. Moreover, the burden of maintaining **PKI** is removed, i.e., the key management is simple.

The rest of this paper is organized as follows. The proposed protocol is described in the next section. Security analysis and further discussions are given in Sections 3 and 4, respectively. Finally, conclusions are presented in Section 5.

2. The proposed new copyright protection protocol

2.1. Framework and definitions

In this section, the infrastructure of the proposed anonymous and asymmetric protocol for copyright protection is defined.

For simplicity, a scenario with the following participants is defined:

1. *Tamper-Resistant Machine* (**TRM**): The **TRM** conducts decryption and determines a fingerprinted content in which the embedded fingerprint message indicates the serial number of