Journal of Computer and System Sciences 82 (2016) 466–476

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Solutions to the anti-piracy problem in oblivious transfer

Lingling Xu [a], Fangguo Zhang [b,*], Willy Susilo [c], Yamin Wen [d]

[a] School of Computer Science and Engineering, South China University of Technology, Guangzhou, China
[b] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China
[c] Center for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, Australia
[d] School of Mathematics and Statistics, Guangdong University of Finance & Economics, Guangzhou, China

ARTICLE INFO

Article history:
Received 3 June 2013
Accepted 12 July 2015
Available online 27 November 2015

Keywords:
Oblivious transfer
Access control
Fingerprinting
Anti-piracy
Group signature

ABSTRACT

In this paper, we consider the applications of digital fingerprinting in oblivious transfer (OT) and present the solutions to the anti-piracy problem in OT protocols. OT protocols can be applied to goods purchasing, pay-per-view TV and sensitive database access while maintaining the users' privacy. In these applications, if the users redistribute the messages that they acquired from the server's database or sell them to others, then both of the server's privacy and benefits will be damaged. Prior to this work, such an anti-piracy problem has never been considered in the OT protocols, even though it is an essential problem to make OT protocols adoptable in practice. In this work, we consider this problem for the first time and present practical solutions, by combining a digital fingerprinting scheme into OT, to provide the pirate-tracing in OT protocols. By performance analysis, our solutions turn out to be practical.

1. Introduction

The diversity of the current Internet applications, such as pay-per-view movie streaming and electronic commerce, has been the greatest enabler for the need of the 'ubiquitous Internet'. The advent of ubiquitous Internet has induced the privacy protection of users, which is considered to be a primary concern to enable a success adoption of the latest technologies. In the database access over the Internet scenario, the database log reveals much information that exposes the user's privacy, as the access will often represent what the user is looking for, or the relevant search pattern. To circumvent this problem, Rabin presented the notion of oblivious transfer (OT) in [27] as a remedy to this situation. In OT, the user privacy is preserved in such a way that a user makes requests to a server, and finally obtains the chosen messages *without* requiring the server to learn anything about the choice. To date, there are many OT protocols that have been proposed in the literature to ensure user privacy, including basic OT in [10,12,14–17,20–23] and many variants of OT such as priced OT in [1], restricted OT in [18], and OT with access control (AC-OT) in [6,8,30,31].

These OT protocols can be applied in confidential database access such as electronic health records, private health records, electronic commerce and online banking. Nevertheless, in all of these schemes, the users are provided with the liberty of disseminating information that may disadvantage the server. Consider an example where OT is used in digital goods purchase. If the user redistributes the information (or sells the information to others) that he has obtained from the

* Corresponding author.
E-mail addresses: xulingling810710@163.com (L. Xu), isszhfg@mail.sysu.edu.cn (F. Zhang), wsusilo@uow.edu.au (W. Susilo), yamin.wen@gmail.com (Y. Wen).

http://dx.doi.org/10.1016/j.jcss.2015.11.003
0022-0000/© 2015 Elsevier Inc. All rights reserved.

server, then the server will be disadvantaged in particular when the goods are very valuable. Thus, it is clear that there is a need to provide an anti-piracy solution to the OT protocols. Nevertheless, there exists no work that considered this problem in the literature.

1.1. Our contributions

The goal of this work is to solve the problems of anti-piracy in OT protocols. Respectively for basic OT and OT with access control, we present practical solutions to the anti-piracy problem. The main contributions of this paper are summarized as follows:

- For the first time, we consider the anti-piracy protection in OT protocols. Prior to this work, no researchers have been concerned about this problem although it is essential to make OT protocols adoptable in practice. Due to the privacy property of users in OT, the problem of solving the piracy in OT seems to be an elusive issue. Nonetheless, we present two solutions to this problem by combining digital fingerprinting into basic OT and OT with access control respectively.
- Firstly, in order to provide the anti-piracy protection in basic OT, a digital signature and an asymmetric fingerprinting, derived from the scheme in [11], are combined to achieve the desired functionality. In this solution, three parties, say the server, user, and arbiter, are included. The solution consists of three subprotocols: FingerprintData, ObtainData, TraitorRecovery. Here FingerprintData and ObtainData are both interactive protocols between the user and server. After ObtainData is finished, the user can obtain fingerprinted messages without the server learning which fingerprinted copies of which messages the user has obtained. Later, if the server finds an illegal redistributed copy, by executing TraitorRecovery with the arbiter, the identity of the user who redistributed the copy can be revealed and punished. In addition, we analyze the security of the solution including server security and user security. Since it aims to provide the anti-piracy protection in basic OT, in this solution, the user is authenticated to the server.
- Besides the solution to the anti-piracy protection in basic OT, we also provide a solution to the problem in the OT with access control (AC-OT). Since in AC-OT, the users can obtain chosen messages from the server obliviously and anonymously, it seems to be more elusive to trace a pirate user who illegally redistributes a message. Whereas, we make a simple modification of the solution to anti-piracy in basic OT above, by integrating the group signature into it, to obtain a solution to achieve the pirate tracing in AC-OT.
- We analyze the performance of the solutions with regard to computation complexity, communication overhead and round complexity in detail. By the analysis, the solutions can be practical by properly selecting efficient building blocks including signature and group signature schemes.

1.2. Related works

When considering anti-piracy, there exist many related work in the literature, such as fingerprinting and traitor tracing. Fingerprinting schemes deter people from illegal copying of digital data by enabling the merchant of the data to identify the original buyer of a copy that was redistributed illegally. Fingerprinting was first presented in [29], and then further extended subsequently in [2,4,7,11,13,25,26]. In his seminal paper, Wager presented a symmetric fingerprinting scheme in which two parties know the data with the fingerprint: the buyer of the original copy and the merchant. Thus, on one hand, if the dishonest buyer redistributes the copy with this fingerprint, the merchant can provide an evidence to any third party that the buyer has violated the term of sale. On the other hand, a dishonest merchant may also redistribute the copy to gain some extra money by wrongly claiming that there are illegal copies around. To alleviate this problem, the asymmetric fingerprinting in [7,25] has been proposed. In this scheme, only the buyer knows the fingerprinted copy, but not the merchant. Hence, the merchant cannot provide any evidence to any third party if the copy of the item is actually found. To further provide buyer's privacy, anonymous fingerprinting in [11,26] has been proposed. In the works by [7,11,13,19,28], fingerprinting schemes were presented by using OT as a building block to protect against illegal copying of digital data. However, they didn't present solutions to provide the pirate tracing in OT.

In the existing fingerprinting schemes, when a buyer purchases digital data from a merchant, even if the user is anonymous, the merchant can still link the data with a pseudonym. When the merchant finds a copy of the data, the merchant can first find the pseudonym linked with the data and then open the identity of the buyer with the pseudonym (maybe with the help of a registration center). Nevertheless, in OT, since the database server cannot learn which messages a user has requested, or even who is the user (in OT with access control), then the merchant cannot link an illegal copy of data with any user. Therefore, the problem of solving the piracy in OT seems to be an elusive issue.

To the best of our knowledge, our paper considers the anti-piracy protection to OT protocols for the first time, and provide solutions for respectively the basic OT and OT with access control. In this way, a user cannot arbitrarily redistribute any data which is obviously obtained from the database server.

1.3. Organization of the paper

The rest of the paper is organized as follows. In Section 2, we will review oblivious transfer protocols including basic OT and OT with access control. Subsequently, we will present our solution to anti-piracy problem for the basic OT and analyze