Journal of Computational and Applied Mathematics 259 (2014) 586–591

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Anonymous trace and revoke☆

Murat Ak[a,*], Serdar Pehlivanoğlu[b], Ali Aydın Selçuk[c]

[a] Department of Computer Engineering, Akdeniz University, Antalya, Turkey
[b] Department of Computer Engineering, Zirve University, Gaziantep, Turkey
[c] Department of Computer Engineering, TOBB University of Economics and Technology, Ankara, Turkey

ARTICLE INFO

Article history:
Received 15 February 2013
Received in revised form 11 September 2013

Keywords:
Digital content distribution
Digital rights management
Broadcast encryption
Trace and revoke
Anonymity
Privacy

ABSTRACT

A broadcast encryption (BE) scheme is a method for encrypting messages in a way that only a set of privileged users can decrypt it. Anonymity in a BE system is to hide any information on the privileged set. This problem has very recently had some attention and some constructions are proposed to achieve anonymity. However, anonymity in a trace and revoke (TR) scheme has not been studied yet, and to the best of our knowledge there is no construction for an anonymous TR system. In this paper, we present a generic transformation from an anonymous BE scheme into an anonymous TR scheme.

1. Introduction

Broadcast encryption (BE) is introduced in [1] and later studied in [2,3].[1] With such systems it is possible to encrypt to any chosen set of *privileged* users while the others (called *revoked users*) are precluded from the reception of the message.

A coalition of malicious users (called traitors) may use their legitimate keys to produce a pirate decryption box (called the pirate decoder) that is made available to unintended parties. Traitor tracing (TT) systems are employed [4,5] to deter users from involving in this type of piracy.

It is desired to integrate both revocation and tracing functionalities in a single system. However, combining these two features is not always easy as pointed in [6–8]. A non-trivial construction, called a trace and revoke scheme (TR), is proposed by Naor and Pinkas in [9]. Later, Naor et al. [6] proposed a TR scheme which employs a weaker tracing strategy that focuses on disabling the pirate decoder rather than identifying traitors. Yet this strategy has been shown to have its own weakness, called pirate evolution [10]. Other successful TR systems proposed so far include [7,11].

A common shortcoming of all the systems above is that the anonymity of the privileged set is not preserved in the ciphertext. Despite its importance, anonymity for BE schemes has not been considered until [12–15].

Barth et al. [12] construct an anonymous BE scheme that is secure in the random oracle model by employing a *key-private* (i.e., ciphertexts do not leak public key information) IND-CCA2 secure public key encryption scheme. Fazio and Perera [13] propose an *outsider anonymous* BE scheme where the identities are hidden only from unauthorized users (outsiders).

☆ This work was supported in part by the Turkish Scientific and Technological Research Agency (TÜBİTAK), under grant number 111E213.
* Corresponding author. Tel.: +90 5366057644.
E-mail addresses: muratakcs@gmail.com, muratak@akdeniz.edu.tr (M. Ak), serdar.pehlivanoglu@zirve.edu.tr (S. Pehlivanoğlu), aliaydinselcuk@gmail.com (A.A. Selçuk).

[1] In this manuscript, we put a very dense list of references due to the lack of space.

0377-0427/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cam.2013.10.019

A recent work by Libert et al. [15] achieves IND-CCA2 anonymity. A lower bound due to the size of the description of the privileged set is also provided. Kiayias and Samari [14] later improved this lower bound by showing that the number of encryptions in an anonymous BE scheme has to be at least linear in the length of the privileged set.

Anonymity of a TR scheme has not been studied yet, and to the best of our knowledge there is no anonymous TR system. In this paper, we present a generic transformation of an anonymous BE scheme into an anonymous TR scheme. The transformation preserves the public and private key sizes of the underlying scheme and expands the ciphertext length by a factor of two in the worst case.

When we apply our transformation to the anonymous BE schemes of Libert et al. [15] (which are in fact IND-CCA2 secure), we obtain a fully anonymous TR scheme with the same efficiency performance of [15] but our transformation inherits IND-CCA1 security rather than IND-CCA2. Another instantiation with [13] leads to a TR scheme with a weaker type of anonymity, called outsider-anonymity, while achieving a ciphertext length of $O(s)$ where s is the size of the privileged set.

2. Preliminaries

2.1. Anonymous broadcast encryption

A BE scheme consists of three algorithms: (1) $\texttt{KeyDist}(1^n)$ generates private keys $sk_i : i \in [n]$ (throughout the paper we will denote the set $\{1, 2, \ldots, n\}$ by $[n]$) and a public key PK. (2) $\texttt{Encrypt}(PK, S, m)$, on input message m and a set S, prepares a ciphertext c. (3) $\texttt{Decrypt}(PK, sk_i, c)$ responds with m if and only if $i \in S$. Those users in S are called privileged users while the rest are called revoked users.

In such schemes, even if all revoked users in $[n]\backslash S$ collude to decrypt a ciphertext intended for the set S, they should not be able to get any useful information about the message. This confidentiality feature is formalized below in Game 1 (see [2,3]).

Game 1 IND-CCA1 confidentiality game for BE schemes.

1: *Initialize.* The challenger $\mathcal{C}$ runs $(\{sk_i\}_{i\in[n]}, PK) \leftarrow \texttt{KeyDist}(1^n)$ and sends PK to a probabilistic polynomial time (PPT) adversary $\mathcal{A}$.
2: *Query Phase.* $\mathcal{A}$ can corrupt polynomially many users, denoted by set R, and capture the keys $\{sk_i\}_{i\in R}$. A CCA1 adversary can also make polynomially many decryption queries (i, c) to which the challenger $\mathcal{C}$ responds with $\texttt{Decrypt}(PK, sk_i, c)$.
3: *Challenge.* The adversary provides a set S^* which satisfies $S^* \cap R = \emptyset$, and two messages m_0, m_1. $\mathcal{C}$ chooses $b \in_R \{0, 1\}$ and prepares $c^* \leftarrow \texttt{Encrypt}(PK, S^*, m_b)$ and sends c^* to $\mathcal{A}$.
4: *Guess.* $\mathcal{A}$ guesses b' for b.

Throughout the paper, we say an adversary playing a security game (e.g. Game 1 above) wins if it guesses correctly, i.e. if $b' = b$ holds. In general, we define the advantage of an adversary in a security game as $\text{Adv}_{\mathcal{A}} = |\Pr[\mathcal{A} \text{ wins}] - 1/2|$.

Definition 1. A BE scheme B is IND-CCA1 secure if $\text{Adv}_{\mathcal{A}}$ is negligible for any PPT adversary $\mathcal{A}$ playing Game 1.

In an anonymous broadcast encryption scheme, the adversary should be unable to distinguish between any two equal-sized sets of privileged users as long as the corrupted users do not cover the symmetric difference of the two sets. Following the terminology of [14], we define ANO-CCA1 anonymity via the following Game 2.

Game 2 ANO-CCA1 anonymity game for BE schemes.

1: *Initialize.* The challenger $\mathcal{C}$ runs $(\{sk_i\}_{i\in[n]}, PK) \leftarrow \texttt{KeyDist}(1^n)$ and sends PK to a PPT adversary $\mathcal{A}$.
2: *Query Phase.* $\mathcal{A}$ can corrupt polynomially many users, denoted by set R, and captures the keys $\{sk_i\}_{i\in R}$. A CCA1 adversary can also make polynomially many decryption queries (i, c) to which the challenger $\mathcal{C}$ responds with $\texttt{Decrypt}(PK, sk_i, c)$.
3: *Challenge.* $\mathcal{A}$ provides a message m and two equal-sized sets S_0, S_1 which satisfy $(S_0 \Delta S_1) \cap R = \emptyset$, where $S_0 \Delta S_1 = (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$. $\mathcal{C}$ chooses $b \in_R \{0, 1\}$ and prepares $c^* \leftarrow \texttt{Encrypt}(PK, S_b, m)$ and sends c^* to $\mathcal{A}$.
4: *Guess.* $\mathcal{A}$ guesses b' for b.

Definition 2. A BE scheme B is *priv-eq* ANO-CCA1 secure if $\text{Adv}_{\mathcal{A}}$ is negligible for any PPT adversary $\mathcal{A}$ playing Game 2.

More generally, we define a BE scheme B to be *priv-full* ANO-CCA1 secure if the challenge sets can be any two subsets of $[n]$.

2.2. Trace and revoke scheme

A trace and revoke (TR) scheme is a multiuser encryption system that supports both revocation (as in BE) and piracy detection (as in traitor tracing schemes). In this paper, we consider an adversarial setting where the adversary corrupts a number of user keys (that we call traitor keys) and produces a pirate decoder which succeeds in decrypting ciphertexts