Information Sciences 378 (2017) 99–108

Contents lists available at ScienceDirect

Information Sciences

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

Secure publicly verifiable and proactive secret sharing schemes with general access structure

Samaneh Mashhadi

Department of Mathematics, Iran University of Science & Technology, Narmak, Tehran, 16846 13114, Iran

ARTICLE INFO

Article history:
Received 6 March 2016
Revised 17 June 2016
Accepted 22 October 2016
Available online 24 October 2016

Keywords:
Publicly verifiable secret sharing
Proactive scheme
Standard model
Bilinear pairing
Monotone span program
Robust

ABSTRACT

A publicly verifiable secret sharing allows anyone to detect the cheating of dealer or participants only from the public information. In this paper, by using bilinear pairings and monotone span programs we propose two practical publicly verifiable secret sharing schemes with general access structure. The first scheme has provable security in the standard model. The other scheme is proactive, robust and secure against mobile attack. These schemes tolerate active and adaptive adversaries and provide great capabilities for many applications.

1. Introduction

A publicly verifiable secret sharing (PVSS) scheme is a special verifiable secret sharing (VSS) scheme with the property that the validity of shares can be verified not only by participants themselves but also by any other party [4,20]. These schemes provide great capabilities for many applications such as, electronic voting, threshold binding ElGamal, threshold revocable electronic cash, threshold software key escrow.

1.1. Related work

Recently, several secret sharing schemes with provable security are proposed [6,8,12,14,15,19,21]. In 2005, a formalization of the intuitive notion of semantic security for a PVSS scheme was first introduced by [19]. Afterwards, Heidarvand and Villar [8] refined the notion for the worst case, i.e. in the presence of an active and adaptive adversary, and proposed two formal definitions of security for a PVSS scheme in the standard model (IND-secrecy and CSA-secrecy). In the weaker notion (IND-secrecy) an adversary cannot tell apart the shared secret from a random value, while in the stronger notion (CSA-secrecy) an adversary is active and changes the secrets. Moreover, they proposed a PVSS scheme [8] and, based on decisional bilinear square assumption (DBS), proved that it has indistinguishability of secrets (IND-secrecy) in the standard model. In 2011, Jhanwar [12] proposed a PVSS scheme and provided a formal proof for the IND-secrecy of his scheme, based on the (t, n)-multi-sequence of exponents Diffie-Hellman assumption ((t, n)-MSE-DDH). Thereafter, in the random oracle model and under the bilinear Diffie–Hellman assumption (BDH), Wu and Tseng [21] proposed a IND-secure PVSS scheme. Recently, Gan et al. [6], based on the decisional bilinear Diffie–Hellman assumption (DBDH), proposed a PVSS scheme that has CSA-secrecy. They used collision-resistant hash function to prove the security of their scheme in the standard model.

E-mail address: smashhadi@iust.ac.ir

http://dx.doi.org/10.1016/j.ins.2016.10.040
0020-0255/

1.2. Motivation

The goal of this paper is to propose two improvements of the previous PVSS schemes. *The first improvement* is intended to increase the effectiveness and flexibility of the previous threshold PVSS schemes. In most PVSS schemes, such as schemes mention above [6,8,12,19,21], (t, n) threshold access structures are considered. That is, any t or more participants can recover the secret, but $t-1$ or fewer participants cannot. These PVSS schemes have the implicit assumption that all participants in the scheme have the same level of power or influence. However, there exists many situations in which all of the participants do not have the same power or the same probability to be dishonest. In these cases, secret sharing based on the general access structure are required [3,5,10,18]. *The second improvement* is motivated from this fact that in long-lived secrets, a mobile adversary may still have enough time to gradually corrupt enough participants and gets the secret. In order to defend against such attack, proactive secret sharing schemes are required [1,17].

1.3. Contribution

To bridge these gaps, in this paper, we propose two improvements. One uses the general access structure, which makes it more flexible than previous threshold PVSS schemes. The other is proactive and secure against mobile attacks. Based on the DBS problem, we prove that the first proposed PVSS scheme enjoys the IND-secrecy. Compared with the previous PVSS schemes [6,8,12,21], this scheme has the following advantages:

- Have general access structure.
- Have simpler phases based on monotone span program.
- Have very fewer public values in general access scenario.
- The security analysis is not based on hash functions.

The second improvement is an extension of the first one and has the same advantages as previous scheme. Moreover, it has the following advantages:

- Are proactive secret sharing with public verifiability.
- Are robust and secure against mobile attack.
- Are practical for long-lived secrets.

1.4. Organization

The reminder of this paper is organized as follows. Section 2 contains some preliminaries. We review the formal model of a PVSS scheme and security requirements of a proactive secret sharing scheme in Section 3. The first PVSS scheme is presented in Section 4, and its security is analyzed in Section 5. We propose proactive PVSS scheme in Section 6. Finally, we give some comparative results in Section 7.

2. Preliminaries

2.1. Access structure

Definition 1. *Given a set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$, a monotone access structure Γ on $\mathcal{P}$ is a set of non-empty subsets of participants which is closed under upward-inclusion (monotone increasing)*

$$(A \in \Gamma, A \subseteq B \subseteq \mathcal{P}) \Rightarrow B \in \Gamma.$$

The sets in Γ are called the authorized sets, and the sets not in Γ are called the unauthorized sets. The set of the unauthorized sets is called an adversary structure Δ, i.e. $\Delta = \Gamma^c$ and is monotone decreasing. The set Γ^- consists of minimal elements in Γ and set Δ^+ consists of maximal elements in Δ .

Definition 2. *For any two monotone decreasing sets Δ_1, Δ_2 operation element-wise union $\uplus$ is defined as follows:*

$$\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}.$$

Definition 3. *An adversary structureΔ is $\mathcal{Q}^2$ if no two sets in Δ cover $\mathcal{P}$, that is*

$$\nexists B_1, B_2 \in \Delta : \quad B_1 \cup B_2 = \mathcal{P}.$$

Definition 4. *The dual of an adversary structure Δ over $\mathcal{P}$ is the collection*

$$\widetilde{\Delta} = \{B \subseteq \mathcal{P} : B^c \notin \Delta\}.$$

It is interesting to note thatΔ is $\mathcal{Q}^2$ iff $\Delta \subseteq \widetilde{\Delta}$.