A Novel Direct Anonymous Attestation Scheme Using Secure Two-Party Computation

Xiaohan Yue[1] and Fucai Zhou[2]

[1] College of information science and engineering, Shenyang University of Technology
Shenyang, China
xhyuer@gmail.com
[2] College of information science and engineering, Northeastern University
Shenyang, China
fczhou@mail.neu.edu.cn

Abstract. Direct Anonymous Attestation (DAA) is a cryptographic scheme which enables the remote authentication of a trusted platform whilst preserving privacy under the user's control. In term of construction of DAA, due to the limited computational and storage capability of trusted platform module (TPM), in this paper, we propose a novel approach for constructing an efficient DAA scheme: we design a secure two-party computation protocol for the Join/Issue protocol of DAA, and construct the DAA scheme concretely under the q-SDH assumption and XDH assumption. Based on the DAA security model, we prove that our DAA scheme meets user-controlled anonymity, user-controlled traceability in the random oracle model. Finally compared with other existing DAA schemes, our DAA scheme has better performance.

Keywords: Trusted Computing, direct anonymous attestation, secure two-party computation, security proof.

1 Introduction

Trusted Computing [1] is a hardware-based security guarantee mechanism, which allows commodity computers to provide cryptographic assurances about their behavior. The core of this architecture is a device called Trusted Platform Module [2] (TPM). TPM is a hardware chip embedded in platforms that can carry out various cryptographic functions. One important function of TPM is integrity reporting, and the process of reporting the integrity of a platform is known as remote attestation. To achieve the goals of remote attestation and ensure the user privacy, Trusted Computing Group (TCG) has introduced two ways as follows:

One way to preserve user privacy is to employ a trusted third party to manage the relationship between a platform's true unique identity, and one or more pseudonyms that can be employed to generate attestations for different purposes. TCG initially adopted this approach in the TPM specification 1.1[3], dubbing the trusted third party a Privacy CA and associating the pseudonyms with Attestation Identity Keys (AIKs). A TPM's true unique identity is represented by the Endorsement Key (EK) embedded

J. Su et al. (Eds.): ICoC 2013, CCIS 401, pp. 218–235, 2013.

in the TPM. However, the Privacy CA architecture has met with some real-world limitations as described in [4].

To address the limitations of Privacy CA, another way called Direct Anonymous Attestation (DAA) [4] was developed and incorporated into the latest TPM specification 1.2 [2] and the Mobile Trusted Module specification [5]. DAA is a remote authentication mechanism for trusted computing platform, and mainly consists of the Join/Issue protocol and the Sign protocol. The participants in a DAA scheme have three types: the issuer, the signer and the verifier. The issuer is in charge of verifying the legitimating of signers and of issuing a signing key to each signer. The signer, which consists of a TPM and a host where the TPM is attached, can convince a verifier that the DAA signatures generated by the signer are valid. The verifier can verify the membership of the signer from the DAA signatures but it cannot learn the identity of the signer. The DAA scheme is completely decentralized and achieves anonymity by combining research on group signatures and credential systems. Unlike the group signatures, the issuer in DAA is not a privileged group manager, so anonymity can never be revoked, i.e., a DAA signature cannot be opened by anyone including the issuer to reveal the identity of the signer. Instead of full-anonymity and traceability as held in group signatures[6], DAA has user-controlled anonymity and traceability, that means the DAA signer (user) and verifier are able to decide whether the verifier enables to determine if any two signatures have been produced by the same signer.

Related works. DAA has drawn a lot of attention from both industry and cryptographic researchers after the concept and a concrete scheme of DAA were first introduced by Brickell, Camenisch, and Chen [4]. Durahim et al.[7] constructed a privacy-preserving mutual authentication and key agreement protocol using DAA scheme for ensuring privacy. Bichsel et al. [8] made use of a variant DAA scheme to build an anonymous credential system on a standard Java card. Bella et al. [9] utilized a DAA scheme to enforce privacy in e-commerce and proposed a self-enforcing privacy protocol. Gummadi et al. [10] developed a NAB ("Not-A-Bot") system which can preserve the current privacy semantics of web and email by extending the DAA service. Many other DAA-based works have been presented in literatures [11, 12, 13].

However the performance of original DAA scheme is inefficient, hence many other DAA schemes were proposed from the view of performance. Recently, researchers have been working on how to create DAA schemes with elliptic curves and pairings, since ECC-based DAA is more efficient in both computation and communication than RSA-based DAA. The first ECC-based DAA scheme was proposed by Brickell et al.[14] This scheme is based on symmetric pairings. Chen et al. [15,16] improved the above scheme [14] and proposed two extended DAA schemes by using asymmetric pairings for the purpose of increasing implementation flexibility and efficiency. To further improve the performance of the scheme [16], Chen et al. [17] modified the scheme, and compared with the original DAA scheme via a concrete implementation. Recently, Chen [18] introduced a more efficient DAA scheme by making use of batch proof and verification technique. But the efficient scheme [18] has some security drawbacks, Brickell et al [31] then fix these drawbacks by proposing a new batch proof and verification protocol. These DAA schemes are based on the LRSW assumption and DDH assumption. Other DAA schemes were proposed by Chen and