Constant-Size Dynamic k-TAA*

Man Ho Au, Willy Susilo, and Yi Mu

Center for Information Security Research
School of Information Technology and Computer Science
University of Wollongong, Wollongong 2522, Australia
{mhaa456, wsusilo, ymu}@uow.edu.au

Abstract. k-times anonymous authentication (k-TAA) schemes allow members of a group to be authenticated anonymously by application providers for a bounded number of times. Dynamic k-TAA allows application providers to independently grant or revoke users from their own access group so as to provide better control over their clients. In terms of time and space complexity, existing dynamic k-TAA schemes are of complexities $\mathrm{O}(k)$, where k is the allowed number of authentication. In this paper, we construct a dynamic k-TAA scheme with space and time complexities of $O(\log(k))$. We also outline how to construct dynamic k-TAA scheme with a constant proving effort. Public key size of this variant, however, is $O(k)$.

We then construct an ordinary k-TAA scheme from the dynamic scheme. We also describe a trade-off between efficiency and setup freeness of AP, in which AP does not need to hold any secret while maintaining control over their clients.

To build our system, we modify the short group signature scheme into a signature scheme and provide efficient protocols that allow one to prove in zero-knowledge the knowledge of a signature and to obtain a signature on a committed block of messages. We prove that the signature scheme is secure in the standard model under the q-SDH assumption.

Finally, we show that our dynamic k-TAA scheme, constructed from bilinear pairing, is secure in the random oracle model.

Keywords: k-TAA, dynamic k-TAA.

1 Introduction

Teranisi *et al.* [18] proposed k-times anonymous authentication (k-TAA) so that users of a group can access applications anonymously while application providers (AP) can decide the number of times users can access their applications. In k-TAA, there are three entities, namely, group manager (GM), application providers (AP) and users. Users first register to GM and each AP announce independently the allowable number of access to its application. A registered user can then authenticate himself to the AP's anonymously, up to the allowed number of times. Anyone can trace a dishonest user who tries to access an application for more than the allowable number of times.

* This work is partially supported by ARC Linkage Project Grant LP0667899.

R. De Prisco and M. Yung (Eds.): SCN 2006, LNCS 4116, pp. 111–125, 2006.

In k-TAA, AP's have no control over the group of users accessing their applications. In actual scenarios, AP's may wish to select their own group of users. Dynamic k-TAA, proposed by Nguyen *et al.* [15], has added this flexibility over ordinary k-TAA systems. In a dynamic k-TAA, the role of AP's is more active and they can select their user groups, granting and revoking access of registered users independently.

Many existing k-TAA schemes (and dynamic k-TAA schemes) [18,15] are quite efficient, with time and space complexities independent of the total number of users. However, size of the public key of AP's, together with the communication cost between users and AP's, are both of order $O(k)$. The computational cost of the user for an authentication protocol is also of order $O(k)$. In this paper, we construct k-TAA and dynamic k-TAA scheme with complexity of $O(\log(k))$. We also outline how to reduce the proving cost to $O(1)$ at the cost of public key size of AP.

In constructing our scheme, we modify the short group signature from Boneh *et al.* [2] into a signature scheme, which we shall referred to as BBS+ signature, with two protocols, similar to [8,10] (referred to as CL, CL+ respectively hereafter). We do not claim originality of this modification as it has been outlined in [10]. However, we supply the details of the modification, together with the protocols and analyze its security. In particular, the protocol of showing possession of a signature is different from [2] in which the modified protocol achieve perfect zero-knowledge while the original protocol is computational. We prove that BBS+ signature is secure in the standard model under the q-SDH assumption. This BBS+ signature could be used as building blocks for other cryptographic systems. It has similar properties to CL (based on Strong RSA) and CL+ signatures (based on LRSW). To sign a block of messages, the signature scheme outperforms the existings schemes in the literature (signature size of CL+ is linear to number of messages in the block to be signed, CL is 1346 bits while BBS+ is only 511 bits).

The recently proposed group signature from [5] can also be modified into signature scheme with efficient protocol secured in the stand model. However, the signing of a message have to be done in a bit-by-bit manner.

1.1 Related Works

Very recently, Teranishi and Sako [19] proposed an ordinary k-TAA scheme with constant proving cost. We shall refer to it as TS06 hereafter. Our ordinary k-TAA scheme, constructed from the dynamic one following the outline of [15], is very similar to TS06. Our construction can be thought of as an extension of TS06 to dynamic k-TAA to give AP more control over their clients. This is achieved by the use of dynamic accumulator and the idea of using dynamic accumulator for access control was introduced in [9]. Finally, as pointed out in [19], k-TAA shares certain similarities with compact e-cash schemes, introduced in [7]. The main difference being in k-TAA schemes, each provider may chooses its only k and a user could authenticated himself k_1 times to provider-1, k_2 times to provider-2, etc., while in a compact e-cash scheme, the user can only