Anonymous k-Show Credentials

Mohamed Layouni and Hans Vangheluwe

School of Computer Science, McGill University,
3480 University Street, Montreal, H3A 2A7, Quebec, Canada

Abstract. Privacy-preserving digital credentials are cryptographic tools that allow a user to prove a predicate about his/her identity or qualifications, without the verifying party learning additional information beyond the status of that predicate. The Identity Mixer (Idemix) [CL01] is a framework providing such credentials. In Idemix, we can distinguish two types of credentials: (1) one-time show credentials which can be shown only once before unveiling the identity of their holder, and (2) multi-show credentials which can be shown infinitely many times without the showings being linked to each other, or to the identity of their holder. In this paper, we bridge the gap between the two previous types of credentials, and extend Idemix to k-show credentials (for $k > 1$.) The k-show credentials we propose can be shown anonymously, but linkably, up to k times.

Keywords: Privacy-preserving digital credentials, anonymity, multiple-show credentials.

1 Introduction

With the increasing digitization of society, and the continuous migration of day-to-day services from the paper world to the digital world, digital credentials have become a very important tool. Similar to their paper counterparts, digital credentials are special documents, issued by a certification authority, that may contain a variety of information about their holder (e.g., identity attributes, qualifications, privileges, etc.) In addition, digital credentials have attractive features, that make them superior to their paper counterparts, such as searchability, large-scale data-mining, and knowledge discovery, just to name a few. With the latter features, comes also the disadvantage that credential holders are now a lot easier to monitor, and to have their privacy violated. Furthermore, digital credentials – by their very nature – are easy to clone and copy, and using them without proper safeguards could lead to serious security problems. To address this set of conflicting requirements, namely privacy and security requirements, privacy-preserving credentials have been invented [Cha85, CP92, Bra94, Bra00, CL01, CL04]. In a privacy-preserving digital credential system, one can generally distinguish three types of players: a certification authority, a user, and a verifier. In some cases, the certification authority and the verifier are controlled by the same entity. The certification authority issues a credential to a user who fulfills certain conditions. In exchange for goods and services, the user may be required to prove,

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 181–192, 2007.

to a service provider (the verifier), possession of a valid credential from the certification authority. The user may also be required to prove a predicate on the attributes encoded in his credential. The service provider may later decide to deposit a transcript of the interaction it had with the user, to the certification authority. The main requirements the credential system should satisfy are: (1) Non-forgeability: the user should not be able to succeed in proving the validity of forged credentials, or in proving predicates that are not satisfied by the attributes encoded on his CA-issued credential, and (2) Privacy: the verifier should not be able to learn any information about the user's credentials beyond what can be naturally inferred from the status of the proven predicate. The latter requirement can be refined even further, by adding constraints on the number of times a credential can be used. Based on this last criterion, we can distinguish three types of credentials:

1. Multiple-show credentials: they can be shown infinitely-many times without the showings being linked to each other, or to the issuing protocol instance where they were generated.
2. One-show credentials: they can be shown anonymously only once, before the identity of their holder is unveiled.
3. Limited- or k-show credentials, for ($k > 1$): they can be shown anonymously up to k times, after which the identity of the holder is revealed.

Privacy-preserving credential systems are becoming increasingly popular, and there is a growing interest in concrete implementations [Ide07, UPr07, Hig07]. The Identity Mixer [Ide07] is based on Camenisch and Lysyanskaya's credentials [CL01], and is one of today's most complete credential systems. Idemix provides a framework supporting only the first two types of credentials, namely multi-show credentials, and one-time show credentials.

Our Contribution: In this paper, we bridge the gap between the two first types of credentials, and extend the Idemix framework to k-show credentials (for $k > 1$.) A naive way to construct k-show credentials is by issuing k separate copies of one-show credentials, but this option obviously lacks efficiency. The solution we propose in this paper extends the one-time show credentials of [CL01] to k-show credentials without a significant increase in complexity. Compared to the protocols of [CL01], we only add 2 extra exponentiations and 1 proof of discrete logarithm knowledge to the user in the pseudonym creation protocol. For the issuing protocol, the user performs 3 more exponentiantions and a proof of knowledge for each additional showing allowed. Finally, the complexity of the showing protocol can be made very close to that of one-time show credentials [CL01] by using precomputations and fast exponentitation methods [Gor98].

Anonymous k-show credentials may be used in a variety of applications. They can be used for instance to build public transit passes, where a user is allowed to make up to k rides anonymously, after which the pass serial number will be uncovered, revoked, and added to a black list. In order to count the number of times a credential is shown, the issuing organization is able to link different showings of the same credential to each other, but not to the identity of the