Brief Announcement: A Flexible Framework for Secret Handshakes

Gene Tsudik*
Department of Computer Science
University of California, Irvine
gts@ics.uci.edu

Shouhuai Xu†
Department of Computer Science
University of Texas, San Antonio
shxu@cs.utsa.edu

ABSTRACT

Secret handshakes offer anonymous and unobservable authentication and serve as an important tool in the arsenal of privacy-preserving techniques. Prior research focused on 2-party secret handshakes with one-time credentials. This paper breaks new ground on two accounts: (1) we obtain secure and efficient secret handshakes with reusable credentials, and (2) we provide the first treatment of *multi-party* secret handshakes.

Categories and Subject Descriptors

C.2.4 [**Computer-Communication Networks**]: Distributed Systems

General Terms

Security

Keywords

secret handshakes, privacy-preservation, anonymity, credential systems, unobservability, key management

1. OVERVIEW

We investigate *interactive privacy-preserving mutual authentication*; specifically, *secret handshakes*. A secret handshake scheme allows two or more group members to authenticate each other in an anonymous, unlinkable and unobservable manner such that one's membership is not revealed unless every other party's membership is also ensured. We achieve this by presenting a secret handshake framework – **GCD**. This framework is a *compiler* that transforms three main ingredients – a **G**roup signature scheme, a **C**entralized group key distribution scheme, and a **D**istributed group key agreement scheme – into a secure secret handshake scheme. We formally specify this framework based on desired functionality and security properties.

Existing secret handshake techniques are only able to support 2-party secret handshakes [1], [2, 3]. Our framework represents the first result that supports truly *multi-party* secret handshakes. We present some concrete examples where a handshake participant computes only $O(m)$ modular exponentiations and sends/receives $O(m)$ messages, where m is the number of handshake participants.

¿From the security perspective, our framework has two novel features. First, it can be resolved into concrete schemes that provide the novel and important `self-distinction` property which ensures the uniqueness of each handshake participant. It guarantees that the protocol is a multi-party computation with the exact number of players that claim to be participating. Without `self-distinction`, a malicious insider can easily impersonate any number of group members by simultaneously playing multiple roles in a handshake protocol. Thus, an honest participant may be fooled into making a wrong decision when the number of participating parties is a factor in the decision-making policy. We also note that self-distinction is trivial for 2-party secret handshakes. However, it becomes more challenging for handshakes of three or more, since the parties cannot simply expose their identities; otherwise, anonymity would be lost.

Second, unlike prior work [1, 2] which relies on one-time credentials to achieve `unlinkability`[1] our approach provides `unlinkability` with multi-show (or reusable) credentials. This greatly enhances its usability and practicality. Moreover, our approach does not require users to be aware of other groups, unlike [3].

A full version of this paper can be found in [4].

2. REFERENCES

[1] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H. Wong. Secret Handshakes from Pairing-Based Key Agreements, *IEEE Symposium on Security and Privacy 2003*.

[2] C. Castelluccia, S. Jarecki, and G. Tsudik. Secret Handshakes from CA-Oblivious Encryption, *ASIACRYPT 2004*.

[3] S. Xu and M. Yung. k-anonymous Secret Handshakes with Reusable Credentials, *ACM CCS 2004*.

[4] G. Tsudik and S. Xu, A Flexible Framework for Secret Handshakes, *Cryptology ePrint Archive: Report 2005/034*.

*Supported by the National Science Foundation under award IIS-ITR-0331707.
†Supported by the US Army Research Office under grant W911NF-05-1-0160.

PODC'05, July 17–20, 2005, Las Vegas, Nevada, USA.
ACM 1-58113-994-2/05/0007.

[1] This ensures that multiple handshake sessions involving the same participant(s) cannot be linked by an adversary.