Brief Announcement: Secret Handshakes from CA-Oblivious Encryption *

Claude Castelluccia, Stanisław Jarecki, and Gene Tsudik
School of Information and Computer Science
UC Irvine, CA 92697, USA
{ccastell, stasio, gts}@ics.uci.edu

ABSTRACT

Secret handshake protocols were recently introduced Balfanz, et al. [1] to allow members of the same group to authenticate each other *secretly*, in the sense that someone who is *not* a group member cannot tell, by engaging some party in the handshake protocol, whether that party is a member of the group. On the other hand, any two parties who *are* members of the same group will recognize each other as members. Thus, secret handshakes can be used in any scenario where group members need to identify each other without revealing their group affiliations to outsiders. The secret handshake protocol of [1] relies on a *Bilinear Diffie-Hellman* assumption on certain elliptic curves. We show how to build secret handshake protocols secure under more standard cryptographic assumptions, like the RSA or the Diffie Hellman (DH) assumption, using a novel tool of *CA-oblivious* public key encryption, i.e. an encryption scheme where neither the public key nor the ciphertext reveal any information about the Certification Authority which certified the public key.

Categories and Subject Descriptors

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

General Terms

Algorithms, Security, Theory

Keywords

authentication, privacy, anonymity, encryption

Problem Exposition: A secret handshake scheme, introduced by Balfanz et al. [1], allows group members to authenticate each other *secretly* in the following sense. If A is a member of group G_a and B is a member of G_b, a secret handshake scheme guarantees that: (1) They authenticate each other if and only if $G_a = G_b$; and (2) if $G_a \neq G_b$ then the only thing that either party learns is *the sole fact* that $G_a \neq G_b$.

To enable practical group management, including revocation of group members, a secret-handshake scheme should be similar to a PKI system. Namely, each member should have a (random) ID on which the group manager issues a group-specific *trapdoor*. Thus a secret handshake amounts to the following task: For a given CA, Alice wants to prove to Bob that she holds a trapdoor t_A issued by this CA on her ID_A, but only if Bob holds a trapdoor t_B issued by the same CA on his ID_B. Moreover, the protocol must be "CA-oblivious" in the sense that if a cheating Bob does not hold a valid (ID,trapdoor) pair (ID_B, t_B), his interaction with Alice must not help him in guessing if Alice belongs to this group or not.

Previous solution vs. ours: The protocol of [1] is based on a Bilinear Diffie-Hellman (BDH) assumption on certain elliptic curves. As in the identity-based encryption of Boneh and Franklin, A and B can compute each other's public keys PK_A, PK_B from their ID's and from the public key of the CA. Alice and Bob can then non-interactively compute a session key from either (t_A, PK_B) or (t_B, PK_A). The two parties can verify if they computed the same key via a standard MAC-based challenge - response protocol. Under the BDH assumption in the Random Oracle Model, an attacker cannot compute the session key without a valid trapdoor, and without the key he cannot learn anything from the MAC-based challenge-response protocol. Thus, the "CA-obliviousness" property of this protocol follows from two properties of cryptosystems built on bilinear maps: (1) that a public key can be computed without any certificate-like information which reveals CA affiliation; and (2) that a session key can be computed non-interactively, and thus again that no CA-specific information is exchanged.

We show that one does not need the BDH assumption (and associated expensive Weil-pairing computation) to achieve these properties. We show that a CA-oblivious encryption scheme can be based either on the RSA or on the DH problems. In both cases, unlike in the BDH-based solution above, the public-keys are computed by (CA-oblivious) interaction with the key owner. The resulting authentication protocol has lower or comparable computational cost and its round complexity stays at 3 rounds (DH) or requires one extra round (RSA).

References:

[1] Balfanz, Durfee, Shankar, Smetters, Staddon, Wong, "Secret handshakes from pairing-based key agreements," in *IEEE Symposium on Security and Privacy*, 2003.

*Full version at `http://eprint.iacr.org/2004/133/`

PODC'04, July 25–28, 2004, St. John's, Newfoundland, Canada.
ACM 1-58113-802-4/04/0007.