Anonymous Identification and Designated-Verifiers Signatures from Insecure Batch Verification

Sherman S.M. Chow[1] and Duncan S. Wong[2]

[1] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu
[2] Department of Computer Science
City University of Hong Kong
Hong Kong, China
duncan@cs.cityu.edu.hk

Abstract. Versatility in cryptography is interesting. Instead of building a secure scheme from another secure one, this paper presents an oxymoron making use of the insecurity of a scheme to give useful feature in another context. We show the insecurity of the batch verification algorithms in Cui *et al.*'s work about an identity-based (ID-based) signature scheme. Following Chow *et al.*'s idea in EuroPKI 2005, we turn such attack into a secure ID-based ring signature scheme. We also show how to add linkability. We present two applications of our scheme, which are a short ID-based strong designated verifier signature scheme and an ID-based ad-hoc anonymous identification scheme, with an extension secure against a concurrent man-in-the-middle attack.

Keywords: Identity-based, ad hoc anonymous identification, strong designated verifier signatures, ring signatures, linkability, bilinear pairings.

1 Introduction

Versatility in cryptography is interesting. One central line of research is to identify which cryptographic primitive can help achieving what security function, often in an inconceivable way. An example in the cryptographic scheme level is using multi-trapdoor commitment scheme [16] to transform any proof of knowledge (or identification) protocol into one which is secure against a concurrent man-in-the-middle attack. From application level, we see electronic voting schemes [21,25] based on ring signature schemes with linkability [21].

Instead of building a secure scheme from another secure one, this paper turns the insecurity of a scheme into an useful feature in another context.

1.1 Linkable Ring Signatures

Ring signature scheme is a group-oriented signature scheme with 1-out-of-n signer anonymity and spontaneous signer group formation. As observed in [9],

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 203–219, 2007.

identity-based (ID-based) ring signature is better than its counterpart in traditional public key infrastructure, in terms of spontaneity. One can even involve members who have not requested for their private key from the key generation centre (KGC).

In Chow *et al.*'s survey of ring signatures [9], one of the major paradigms of ID-based ring signature schemes can be seen as derived from the failure to batch verify the underlying ID-based signatures. Indeed, a recent scheme in [2] can be regarded as a work exploiting the aggregate verification of the standard ID-based signature in [23], although the authors gave no discussion about this issue. Here we use the same methodology to transform our attack on the batch verification of ID-based signatures proposed recently by Cui *et al.* [12] into a secure ring signature scheme, with further modification to remove all unnecessary components from straightforward transformation.

Following the recent trends of providing different level of anonymity in group-oriented signatures (e.g. [1,8,21,25]), we show how to add linkability into the resulting scheme. A detailed comparison of the efficiency with existing schemes will also be made. We remark the recent generic approach to build ID-based signature schemes with special properties [15] is not applicable to ring signatures.

A recent application of ring signature is concurrent signature, which partially solves the fair exchange problem without the help of trusted third party. Our ring signature also fits in the generic construction of concurrent signature in [10].

1.2 Strong Designated Verifier Signatures

The first application of our scheme is identity-based strong designated verifier signature. Similar to ring signature, designated verifier signature (DVS) scheme is a privacy-oriented one in which the signature produced can only be verified by a specific user, but no one else. Its interactive version, designated verifier proof, is introduced in [18]. Apart from providing the apparent restricted-verifiability, it also helps to solve other problems in secure two-party computations.

Ring signature gives a simple method to give DVS. By involving the intended recipient of the signed message as the second member of a 2-persons group, only the recipient can ascertain the message's authenticity, but no one else.

The idea of *strong* designated verifier signature has also been considered in [18]. Informally, *strong* here means the use of the verifier's private key is essential to perform verification. The strong property can be implemented by a chosen-ciphertext-secure (CCA2) encryption [20,24]. However, such approach gives inefficient construction as CCA2 encryption needs more computation than a semantic-secure one in general. Considering the signature size, a ciphertext and possibly a validity check tag are appended to the signature. Two proposals without explicit encryption step are presented in [24]. One is a generic construction based on chameleon hash and the other is a concrete scheme with encryption step integrated with the signing step. Their concrete scheme follows Boneh-Franklin paradigm [5], thus an expensive $MapToPoint$ encoding function [5] is required.

Recently, a short ID-based strong DVS scheme is proposed in [17]. In their scheme, given a signature on a message m that an adversary wants to learn the