Chapter XII

Secure Trust Transfer Using Chain Signatures

Amitabh Saxena, La Trobe University, Australia
Ben Soh, La Trobe University, Australia

Abstract

In this chapter, we discuss the concept of “trust transfer” using chain signatures. Informally, transferring trust involves creating a trust (or liability) relationship between two entities such that both parties are liable in the event of a dispute. If such a relationship involves more than two users, we say they are connected in a chained trust relationship. The members of a chained trust relationship are simultaneously bound to an agreement with the property that additional members can be added to the chain but once added, members cannot be removed thereafter. This allows members to be incrementally and noninteractively added to the chain. We coin the term “chained signatures” to denote signatures created in this incremental way. An important application of chained signatures is in e-commerce transactions involving many users. We present a practical construction of such a scheme that is secure under the Diffie-Hellman assumption in bilinear groups.
Introduction

An aggregate signature [introduced by Boneh, Gentry, Lynn, & Shacham (2003) in Eurocrypt’03] is a novel cryptographic primitive constructed using bilinear maps based on the hardness of the Computational Diffie-Hellman problem (CDHP). In addition to the necessary properties of signature aggregation and batch verification, the aggregate signatures of Boneh et al. (2003) possess another interesting property, namely; the inability to extract any individual signatures just from the aggregation. This was demonstrated in Boneh et al. (2003) using the example of verifiably encrypted signatures (VES). The security of the VES scheme relies on the hardness of the k-element aggregate extraction problem (k-EAEP). It was shown in Coron and Naccache (2003) that the k-EAEP is as hard as the CDHP.

In this chapter, we introduce the idea of chain signatures as another novel application of the k-EAEP. At the conclusion of this chapter, it will be evident that a chain signature is a more general case of the VES scheme of Boneh et al. (2003). The rest of the chapter is organized as follows. We give an overview of the problems addressed by our chapter in section 2 and formalize the notion of chain signatures in section 3. We give a brief overview of bilinear pairings (the cryptographic primitives of the scheme) in section 4. Finally, in section 5 we present the scheme and show, as an application, a novel method to prevent spam in section 8. Our intention is to summarize the work of Saxena and Soh (2005c).

Motivation

Before going into the details of chain signatures, we give some motivation for the need of such a definition. A real-life example will only be given in section 8 (spammer tracing). For now, we assume a hypothetical contract-signing scenario between n distinct users ID_1, ID_2, ..., ID_n such that any user ID_i wants to commit to a contract only if the (i-1) users ID_1, ID_2, ..., ID_{i-1} have committed. At the same time, ID_i does not want to be liable for (or is unaware of) the rest of the n-i users ID_{i+1}, ID_{i+2}, ..., ID_n.

As a second requirement, once ID_i commits to the contract, he/she wants to ensure that the next (unknown) user ID_{i+1} cannot convince a court of ID_i’s commitment independent of the commitments of the rest of the users ID_1, ID_2, ..., ID_{i-1}. That is, it must not be possible to remove any user ID_j’s commitment (1 ≤ j ≤ i) without removing the rest of the (i-1) commitments assuming that users cannot interact.

To make this scenario meaningful, we additionally require that each user ID_i cannot interact (or collude) with any of the past users ID_1, ID_2, ..., ID_{i-1} once they have committed to the contract. If two or more users collude, then we require that at least one member from the coalition is in this chain.

We propose a model to address this type of issue. Essentially, the aim of our model is to be able to arbitrarily connect many entities in a nonrepudiable chained trust relationship. Using our commitment scheme, trust (and liability) can be sequentially transferred from user ID_i to ID_n via the chain of users. Although chain signatures resemble