Complex Zero-Knowledge Proofs of Knowledge Are Easy to Use

Sébastien Canard, Iwen Coisel, and Jacques Traoré

Orange Labs, 42 rue des Coutures, 14000 Caen, France
{sebastien.canard,iwen.coisel,jacques.traore}@orange-ftgroup.com

Abstract. Since 1985 and their introduction by Goldwasser, Micali and Rackoff, followed in 1988 by Feige, Fiat and Shamir, zero-knowledge proofs of knowledge have become a central tool in modern cryptography. Many articles use them as building blocks to construct more complex protocols, for which security is often hard to prove. The aim of this paper is to simplify analysis of many of these protocols, by providing the cryptographers with a theorem which will save them from stating explicit security proofs. Kiayias, Tsiounis and Yung made a first step in this direction at Eurocrypt'04, but they only addressed the case of so-called "triangular set of discrete-log relations". By generalizing their result to any set of discrete-log relations, we greatly extend the range of protocols it can be applied to.

1 Introduction

The main purpose of authentication is to know who is who. More precisely, Alice wants to be convinced that the entity she communicates with is the right one. When using cryptography, this is often achieved by proving knowledge of a particular secret without (provably) revealing it. In 1985, Goldwasser, Micali and Rackoff [19] introduced the concept of zero-knowledge interactive proofs (ZKIP). The idea of using it for purposes of authentication came one year later in the article by Fiat and Shamir [15], followed in 1988 by Feige, Fiat and Shamir [14], who introduced the zero-knowledge proofs of knowledge (ZKPK).

In modern cryptography, these protocols are not only used for authentication but also as building blocks to achieve more complex purposes, such as for example guaranteeing the anonymity of a user [1,5,9] or committing to a secret value without being able to change one's mind [16]. In these schemes, users typically have to compute some public data relying on secret and random values, then prove that these public data are well-formed by using these building blocks. The security of the global construction relies both on the computed data and protocols they are involved in, which consequently have to be proven as being ZKPK.

The aim of this paper is to simplify analysis of many of these protocols, by providing the cryptographers with a theorem which will save them from stating explicit security proofs. Kiayias, Tsiounis and Yung made a first step in this direction at Eurocrypt'04, but they only addressed the case of so-called "triangular set of

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 122–137, 2007.

discrete-log relations". By generalizing their result to any set of discrete-log relations, we greatly extend the range of protocols it can be applied to.

1.1 Related Work

Many ZKPK have been proposed since the article of Feige et al. in 1988 [14]. When based on discrete logarithms, they are often built over a cyclic group $\mathcal{G} = \langle g \rangle$ either of known prime order q (after Schnorr's article [22]) or of unknown order (but in the same range of magnitude as the order of G). In this paper, we will only consider discrete-logarithm based ZKPK in groups of unknown order, since this is the most difficult case. In this setting, the building block is the GPS authentication scheme [18], which allows to prove knowledge of a discrete logarithm in such groups.

The construction of complex cryptographic tools such as group signature schemes, credential schemes or e-cash systems, always requires more than a single proof of knowledge of a single discrete logarithm. Rather, it involves several secret values and several (discrete-log based) relations between these values. The GPS scheme has therefore to be extended in order to obtain first new building blocks as e.g. a proof of knowledge of a representation [16,13], that involves two secret values and one relation, a proof of equality of two known representations [11,7], which requires four secret values and two relations, or the proof that a committed value lies in an interval [4,7,10,3], that necessitates several secret values and relations. Then, these various building blocks are used to construct still more elaborate protocols, the security of which must be demonstrated in detail for each of them, though the proofs are very similar to each other. As a consequence, it would be very useful to design a "general proof" which could apply to a wide range of such protocols, saving the designers from proving them secure.

Kiayias, Tsiounis and Yung [20] use such complex protocols in their construction of traceable signatures and, as an independent interest of the paper, make a first step towards designing such a general proof. They introduce the notion of *Discrete-Log Relation Set* (DLRS), that is a set of relations involving objects (as public keys and parameters) and free variables (as secret elements). For each free variable, there is a corresponding secret known by a prover $\mathcal{P}$. Then they propose a generic 3-move honest verifier zero-knowledge proof that allows $\mathcal{P}$ to prove the knowledge of these values. They also show that their construction is a ZKPK in the particular case of a triangular discrete-log relation set, that is when each relation introduces at most one new free variable w.r.t. the previous ones. They thus solve the above problem only in part, since their security proof only addresses a particular case. The aim of our paper is to solve this problem in general, for any discrete-log relation set.

1.2 Our Contribution

In this paper, we prove the soundness of any discrete-log relation set (DLRS), as defined by Kiayas, Tsiounis and Yung [20], i.e. when G is a (large) subgroup