Necessary and Sufficient Assumptions for Non-Interactive Zero-Knowledge Proofs of Knowledge for all NP Relations

Alfredo De Santis* Giovanni Di Crescenzo† Giuseppe Persiano‡

Presenting Author: Giovanni Di Crescenzo
Suggested Duration of Talk: 5 minutes

Abstract

Establishing relationships between primitives has been an important area in the foundations of Cryptography, since the first days of modern Cryptography. In some cases, researchers have been successful in presenting necessary and sufficient conditions for the existence of primitives. For instance, it is known that the existence of one-way functions is necessary and sufficient for the construction of other primitives as pseudo-random generators, commitment schemes, pseudo-random functions, signatures schemes, zero-knowledge proofs of membership for all languages in NP and zero-knowledge proofs of knowledge for all NP relations. Moreover, some other primitives, such as public-key cryptosystems, are known to exist under the necessary and sufficient assumption of the existence of one-way functions with trapdoors. In this paper we consider the primitive of *non-interactive zero-knowledge proofs of knowledge,* namely, methods for writing a proof that on input x the prover knows y such that relation $R(x, y)$ holds. These proofs have important applications for the construction of cryptographic protocols, as cryptosystems and signatures that are secure under strong types of attacks. They were first defined in [1], where a sufficient condition for the existence of such proofs for all NP relations was given. In this paper we show, perhaps unexpectedly, that such condition, based on a variant of public-key cryptosystems, is also necessary. Moreover, we present an alternative and natural condition, based on a variant of commitment schemes, which we show to be necessary and sufficient as well for the construction of such proofs. Such equivalence also allows us to improve known results on the construction of such proofs under the hardness of specific computational problems. Specifically, we show that assuming the hardness of factoring Blum integers is sufficient for such constructions. This paper is scheduled to appear as [2].

References

[1] A. De Santis and G. Persiano, *Zero-Knowledge Proofs of Knowledge without Interaction*, in Proceedings of FOCS 1992.

[2] A. De Santis, G. Di Crescenzo, and G. Persiano, *Necessary and Sufficient Assumptions for Non-Interactive Zero-Knowledge Proofs of Knowledge for NP relations*, in Proceedings of ICALP 2000, to appear.

*Dipartimento di Informatica ed Applicazioni, Università di Salerno, Baronissi (SA), Italy. E-mail: ads@dia.unisa.it.
†Telcordia Technologies, Inc., Morristown, NJ, USA. E-mail: giovanni@research.telcordia.com.
‡Dipartimento di Informatica ed Applicazioni, Università di Salerno, Baronissi (SA), Italy. E-mail: giuper@dia.unisa.it