Removing Complexity Assumptions from Concurrent Zero-Knowledge Proofs*

Giovanni Di Crescenzo†

Presenting author: Giovanni Di Crescenzo

Suggested presentation time: 4 minutes

Abstract

Zero-knowledge proofs are a powerful tool for the construction of several types of cryptographic protocols. Due to their importance, considerable attention has been given to the study of which adversarial settings and complexity assumptions are necessary for implementing zero-knowledge protocols, the ultimate goal being that of achieving the most adversarial possible setting together with the minimal possible assumptions or none at all. In particular, recently, such protocols have been investigated in a concurrent and asynchronous distributed model, where protocols have been proposed relying on various synchronization assumptions and unproven complexity assumptions.

In this paper we present the first constructions of proof systems and arguments that are concurrent zero-knowledge *without relying on unproven complexity assumptions*. Our techniques transform a non-concurrent zero-knowledge protocol into a concurrent zero-knowledge one. They apply to large classes of languages and preserve the type of zero-knowledge: if the original protocol is computational, statistical or perfect zero-knowledge, then so is the transformed one. On the other hand, our synchronization assumptions are probably stronger than previous proposals.

In the fully asynchronous model, we show some relationship between the problem of obtaining concurrent zk proofs and the well studied problem of reducing the soundness error of non-concurrent zk proofs. This relationship allows to derive, under some assumptions, lower bounds on the round complexity of concurrent zk proofs, and gives some evidence of round-optimality of our techniques.

This paper is scheduled to appear as [1].

References

[1] G. Di Crescenzo, *Removing Complexity Assumptions from Concurrent Zero-Knowledge Proofs*, in Proceedings of COCOON 2000, to appear.

†Telcordia Technologies Inc., 445 South Street, Morristown, NJ, 07960. E-mail: giovanni@research.telcordia.com.