T-79.511 Special Course on Cryptology / Zero Knowledge: Comments on "Resettable Zero Knowledge"

Petteri Kaski

November 14, 2001

1 Introduction

The purpose of this document is to give comments and constructive criticism on the manuscript [2] on resettable zero knowledge.

Some general comments on the survey. The survey is clearly organized and well-written. The introduction explains the relevance of the new notion (of RZK) and illustrates its nontriviality with respect to earlier ZK proof systems. Section two of the manuscript contains the formal definitions of RZK and RWI under the sequential and interleaved adversarial models, which are then shown to be equivalent. The third section presents a protocol framework whose protocols can be transformed to RZK/RWI protocols if their security has been established in a specific hybrid model. The fourth and fifth sections focus on deriving an RZK proof system for languages in NP via a transformation from an RWI proof system. The last section outlines the public key model and its significance in reducing the number of rounds in an RZK proof system.

All in all, the survey provides an intuitive introduction to the topic for the reader familiar with the standard definitions and terminology related to ZK. Several pointers to recent literature are provided for the reader interested to know more.

2 Specific comments and suggestions

This section contains some miscellanous comments on the survey. Some of the comments are formulated as questions as the reviewer is on somewhat unfamiliar territory here.

RZK and RWI definitions. The reader is required to supply a lot of the missing detail, but this is all right assuming the reader has sufficient background in ZK.

Definition 5. The final bullet of the definition is somewhat unclear; is the intention that it is hard for the verifier to "break" the authenticator system. Why is only oracle access allowed?

Construction 6. Why are the subsequent messages *independent* of r_1? Could it not be the case that the verifier's reply to the prover's first message (which usually depends on r_1) also depends on r_1, so that this dependence induces a dependence between r_2 and r_1, which results in a dependence in the subsequent prover messages?

Definition 7. Is the first assumption regarding the initiation of at most one session with each incarnation redundant, given the following assumption?

Theorem 8. Two minor suggestions. The statement of the theorem could be clarified to indicate that the things which are indistinguishable are probability ensembles indexed over x, y from suitable sets. Furthermore, in the spirit of Theorem 3 and Corollary 4, a corollary could be formulated that explicitly states that Theorem 3 implies RWI and RZK, respectively, for admissible proofs systems which are WI and ZK, respectively, in the hybrid model.

Proposition 9. Both perfectly hiding and perfectly binding commitment schemes are used in the proof, yet it only suffices to assume the existence of two-round perfectly hiding commitment schemes in the statement of the theorem? Furthermore, would for example a three-round commitment scheme suffice, or is it (e.g.) insufficient to guarantee admissibility?

Is there a reason (possibly relating to the soundness of the underlying interactive proof system) why the prover's commitments are perfectly binding whereas the verifier's commitments are perfectly hiding?

The public key model. The survey does not explicitly state where the public key(s) are used in the construction. This would assist comprehension. Furthermore, what if the prover is powerful enough to break the public-key scheme?

Grammar and spelling. Some minor grammatical errors exist (mainly subject/verb disagreement) in the manuscript. Also many closed compounds appear hyphenated and vice versa (e.g. "pseudorandom", "two-round", "3-coloring", "nonconstant"). A standard spelling and punctuation reference (e.g. [1]) should provide helpful in this respect.

References

[1] *The Chicago Manual of Style*, 14th Edition. University of Chicago Press, Chicago, 1993.

[2] J. Wallén. T-79.511 Special Course on Cryptology / Zero Knowledge: Resettable zero knowledge. Draft, November 19, 2001.