Minimum Resource Zero-Knowledge Proofs

(Extended Abstract)

Joe Kilian* Silvio Micali† Rafail Ostrovsky‡

Abstract

What are the resources of a zero-knowledge Proof? *Interaction, communication, and envelops.* That interaction, that is the number of rounds of a protocol, is a resource is clear. Actually, it is not a very available one: having someone on the line to answer your questions all the time is quite a luxury. Thus, minimizing the number of rounds in zero-knowledge proofs will make these proofs much more attractive from a practical standpoint. That communication, that is the number of bits exchanged in a protocol, is a resource is also immediately clear. Perhaps, what is less clear is why envelopes are a resource. Let us explain why this is the case.

Zero-knowledge proofs work by hiding data from a verifier. Only some of this data will be later revealed, at the verifier's request: enough to convince him that the statement at end is true, but not enough to give him any knowledge beyond that. Data can be hidden in two ways: physically – e.g. by putting it into an envelope – or digitally – by encrypting it. But why is it important to minimize the number of envelopes? Physically, because a GOOD envelope is expensive – it actually must be a led box or a safe. Digitally, because minimizing the number of envelopes corresponds to reducing the transmitted bits. In fact, to transmit an encrypted message, one needs to send more bits than in the message itself. For instance, to send an encrypted bit, one needs to send at least 60 bits in some probabilistic encryption scheme. Also, to decrypt each ciphertext, one has to send the decryption key. However, many bits may be encrypted and decrypted with the same overhead of a few bits. Thus if one manages to package the data that should be hidden in as few envelopes as possible, while maintaining zero-knowledge, the protocol will require transmitting much less bits.

---

[*] MIT, partially supported by NSF 865727-CCR and ARO DALL03-86-K-017.

[†] MIT, supported in part by NSF grant DCR-84-13577.

[‡] Boston University, supported in part by NSF grant DCR-86-07492.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 545-546, 1990.

MINIMIZING ENVELOPES AND COMMUNICATION

How many envelops are sufficient for any (not a specific) zero-knowledge proof? Certainly 0 is not enough. And 1 alone does not seem to help. Shamir [oral communication] a few years ago presented a zero-knowledge proof for Knapsack problems which required only 3 envelopes. Recently, Levin [oral communication] a few months ago presented a 3-envelope ZK proof for Graph Coloring. Why was this not satisfactory? Because their solution only works for the mentioned specific problems. That is, it is not a technique that applies to any NP problem. Assume that you want to prove in zero-knowledge that a graph is Hamiltonian. You wish to use few envelopes. First you would transform your input to an instance of Knapsack. Then you would prove, using only 3 envelopes, that the resulting Knapsack problem is solvable. However, this transformation DOES NOT PRESERVE THE SIZE OF THE PROBLEM. In fact, if your original problem consisted of n bits, the resulting Knapsack may easily consist of n^2 bits. That is, you may use only 3 envelopes, but these envelopes are enormous, as they have to contain n^2 bits. This defeats the motivation of using few envelopes in the first place.

We present a scheme for proving statements in zero-knowledge that

1. uses only 2 envelopes and
2. works for any NP statement.

That is, you can apply our method to your problem directly, without blowing up its size.

MINIMIZING INTERACTION

Blum, Feldman and Micali, and De Santis, Micali and Persiano have shown that if two parties agree on a common random string, then they can perform zero-knowledge proofs. Their result requires some interaction at the beginning for choosing the common random string. After that, however, the prover, for each theorem that he discovers, may send to the verifier a single message (to which the verifier needs not to respond) that constitutes a zero-knowledge proof of the discovered theorem. Their result, however, assumes that a specific, number theoretic permutation is trap-door. Usually cryptography starts with very specific assumptions and later manages to find solutions that work given any general assumption. This is also the case here.

We succeeded in achieving non-interactive zero-knowledge proofs by using ANY general trap-door permutation (algebraic or not). More specifically, we prove that after a pre-processing stage consisting of $O(k)$ executions of Oblivious Transfer, *any* polynomial number of NP-theorems of any poly-size can be proved non-interactively and in zero-knowledge, based on the existence of *any* one-way function, so that the probability of accepting a false theorem is less then $\frac{1}{2^k}$. The Oblivious transfer may be easily implemented given a trap-door permutation.

AN EXTENDED VERSION OF THIS PAPER APPEARS IN THE PROCEEDINGS OF 30TH ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE