DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

Linear Zero-Knowledge
A Note on Efficient Zero-Knowledge Proofs and Arguments

Ivan Damgård
Department of Computer Science
University of Aarhus

Tuesday, April 23, 1996, at 2:15 PM
The Seminar Room

Abstract: We present a zero-knowledge proof system for any NP language L, which allows showing that $x \in L$ with error probability less than 2^{-k} using communication corresponding to $O(|x|^c) + k$ *bit commitments*, where c is a constant depending only on L. The proof can be based on any bit commitment scheme with a particular set of properties. We suggest an efficient implementation based on factoring.

In fact, our protocol can show that a Boolean Circuit of size n is satisfiable with error probability 2^{-n} using $O(n)$ commitments. This is the first protocol to achieve "linear zero-knowledge" in this sense (the best earlier result used $\Omega(n \cdot \text{poly-}\log n)$).

We also present a 4-move perfect zero-knowledge interactive argument for any NP-language L. On input $x \in L$, the communication complexity is $O(|x|^c) \cdot max(k, l)$ *bits*, where l is the security parameter for the prover (the meaning of l is that if the prover is unable to solve an instance of a hard problem of size l before the protocol is finished, he can cheat with probability at most 2^{-k}).

Again, the protocol can be based on any bit commitment scheme with a particular set of properties. We suggest efficient implementations based on discrete logarithms or factoring.

We present an application of our techniques to multiparty computations, allowing for example t committed oblivious transfers with error probability 2^{-k} to be done simultaneously using $O(t + k)$ commitments. Results for general computations follow from this.

As a function of the security parameters, our protocols have the smallest known asymptotic communication complexity among general proofs or arguments for NP. Moreover, the constants involved are small enough for the protocols to be practical in a realistic situation: both protocols are based on a Boolean formula Φ containing and-, or- and not-operators which verifies an NP-witness of membership in L. Let n be the number of times this formula reads an input variable. Then the communication complexity of the protocols when using our concrete commitment schemes can be more precisely stated as at most $4n + k + 1$ commitments for the interactive proof and at most $5nl + 5l$ bits for the argument (assuming $k \leq l$).

Joan F. Boyar