DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

And God said, "let there be light",...
and Man said, "can I have some dice as well?"

René Peralta
Electrical Engineering and Computer Science Department
University of Wisconsin at Milwaukee

Tuesday, May 21, 1996, at 2:15 PM
Room 22

Abstract: We show how to produce short proofs of theorems such that a distrusting Verifier can be convinced that the theorem is true yet obtains no information about the proof itself. The paper makes use of what we have called "set certification", which consists of proving that a vector of bit commitments encodes a vector of bits in a given set without revealing the bit-vector itself. We have high hopes for what useful results this technique might eventually yield. Since our shortest proofs don't exactly fit any of the published categories of zero-knowledge proofs, we have named them "discreet proofs". As an example of the power of these techniques, we show discreet proofs of knowledge of RSA and DES keys which fit on a floppy disk.

This is joint work with Joan Boyar.

Joan F. Boyar