J. Cryptology (2007) 20: 1
10.1007/s00145-007-5001-1

Journal of
CRYPTOLOGY

Editor's Note

This issue contains a paper by Neal Koblitz and Alfred Menezes which takes a critical look at how the term "provable security" is used in cryptography. This paper is different from the papers appearing traditionally in the *Journal of Cryptology*; it falls into a new category which can be called "position papers." While it is a technical paper, it contains no theorems and its main goal is to present views on how the significance of security proofs in cryptography can be evaluated.

The paper is discussed controversially in the cryptographic research community, and some members expressed the opinion that such a paper is not suitable for the *Journal of Cryptology*. It is my conscious decision to allow for such position papers to be published, provided they satisfy certain criteria. Some of the criteria that will be applied when evaluating a position paper for publication are that it must be technically interesting, very well-written, of interest to large parts of the community, and it must distinguish clearly between opinions and technical statements. The style must be primarily technical rather than philosophical and it must not be offensive. I encourange submissions of such position papers, but with a warning that the editorial board will be very selective for this category of papers.

UELI MAURER