Bellare, Mihir; Goldreich, Oded

Proving computational ability. (English) [Zbl 1343.94041]


Summary: We investigate extending the notion of a proof of knowledge to a proof of the ability to perform some computational task. We provide some definitions and protocols for this purpose.

For the entire collection see [Zbl 1220.68005].

MSC:

- 94A60 Cryptography
- 68Q05 Models of computation (Turing machines, etc.) (MSC2010)
- 68Q25 Analysis of algorithms and problem complexity

Keywords:

- proofs of knowledge
- zero-knowledge
- cryptographic protocols

Full Text: DOI Link

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.