Cryptology ePrint Archive: Report 2011/188

Physical Turing Machines and the Formalization of Physical Cryptography

Ulrich Rührmair

Abstract: We introduce an extension of the standard Turing machine model, so-called Physical Turing machines, and apply them in a reductionist security proof for a standard scheme from physical cryptography.

Category / Keywords:

Date: received 12 Apr 2011

Contact author: ruehrmair at in tum de

Available formats: PDF | BibTeX Citation

Version: 20110412:194944 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]