Peikert, Chris

Public-key cryptosystems from the worst-case shortest vector problem (extended abstract).

(English) Zbl 1304.94079
Proceedings of the 41st annual ACM symposium on theory of computing, STOC '09. Bethesda, MD, USA, May 31 – June 2, 2009. New York, NY: Association for Computing Machinery (ACM) (ISBN 978-1-60558-613-7). 333-342 (2009).

MSC:

94A60 Cryptography
68W25 Approximation algorithms

Keywords:

cryptography; lattices

Full Text: DOI