zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Micciancio, Daniele; **Peikert, Chris**

Trapdoors for lattices: simpler, tighter, faster, smaller. (English) Zbl 1297.94090

Pointcheval, David (ed.) et al., Advances in cryptology – EUROCRYPT 2012. 31st annual international conference on the theory and applications of cryptographic techniques, Cambridge, UK, April 15–19, 2012. Proceedings. Berlin: Springer (ISBN 978-3-642-29010-7/pbk). Lecture Notes in Computer Science 7237, 700-718 (2012).

Summary: We give new methods for generating and using "strong trapdoors" in cryptographic lattices, which are simultaneously simple, efficient, easy to implement (even in parallel), and asymptotically optimal with very small hidden constants. Our methods involve a new kind of trapdoor, and include specialized algorithms for inverting LWE, randomly sampling SIS preimages, and securely delegating trapdoors. These tasks were previously the main bottleneck for a wide range of cryptographic schemes, and our techniques substantially improve upon the prior ones, both in terms of practical performance and quality of the produced outputs. Moreover, the simple structure of the new trapdoor and associated algorithms can be exposed in applications, leading to further simplifications and efficiency improvements. We exemplify the applicability of our methods with new digital signature schemes and CCA-secure encryption schemes, which have better efficiency and security than the previously known lattice-based constructions.

For the entire collection see [Zbl 1239.94002].

MSC:

94A60 Cryptography

Cited in **16** Reviews
Cited in **124** Documents

Software:

BKZ; SWIFFT

Full Text: DOI

© 2021 FIZ Karlsruhe GmbH