Micciancio, Daniele; Peikert, Chris

Hardness of SIS and LWE with small parameters. (English) Zbl 1310.94161

Canetti, Ran (ed.) et al., Advances in cryptology – CRYPTO 2013. 33rd annual cryptology conference, Santa Barbara, CA, USA, August 18–22, 2013. Proceedings, Part I. Berlin: Springer (ISBN 978-3-642-40040-7/pbk). Lecture Notes in Computer Science 8042, 21-39 (2013).

Summary: The short integer solution (SIS) and learning with errors (LWE) problems are the foundations for countless applications in lattice-based cryptography, and are provably as hard as approximate lattice problems in the worst case. An important question from both a practical and theoretical perspective is how small their parameters can be made, while preserving their hardness.

We prove two main results on SIS and LWE with small parameters. For SIS, we show that the problem retains its hardness for moduli $q \geq \beta \cdot n^\delta$ for any constant $\delta > 0$, where β is the bound on the Euclidean norm of the solution. This improves upon prior results which required $q > \beta \cdot \sqrt{n \log n}$, and is close to optimal since the problem is trivially easy for $q \leq \beta$. For LWE, we show that it remains hard even when the errors are small (e.g., uniformly random from $\{0, 1\}$), provided that the number of samples is small enough (e.g., linear in the dimension n of the LWE secret). Prior results required the errors to have magnitude at least $\sqrt{n}$ and to come from a Gaussian-like distribution.

For the entire collection see [Zbl 1270.94007].

MSC:

94A60	Cryptography
68P25	Data encryption (aspects in computer science)

Cited in **1** Review
Cited in **16** Documents

Keywords:

lattice cryptography; computational hardness; SIS; LWE

Software:

BKZ

Full Text: DOI