

Cryptology ePrint Archive: Report 2013/069

Hardness of SIS and LWE with Small Parameters

Daniele Micciancio and Chris Peikert

Abstract: 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. A 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 $q \geq \beta \cdot \sqrt{n \log n}$, and is essentially 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.

Category / Keywords: foundations / complexity theory, foundations, lattice techniques

Date: received 13 Feb 2013

Contact author: daniele at cs.ucsd.edu

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20130220:093644 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]