Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

Stellingen

behorende bij het proefschrift

"Lattice Cryptography: Isomorphisms & Dual Attacks"

1. Given a lattice Λ, and a set $\mathcal{W}$ obtained by lattice sieving the dual of Λ, then $(f_{\mathbf{w}}(\mathbf{t}))_{\mathbf{w}\in\mathcal{W}}$ are not mutually independent where $f_{\mathbf{w}}(\mathbf{t}) = \cos(2\pi\langle\mathbf{w},\mathbf{t}\rangle)$.

2. By modelling dual vectors in $\mathcal{W}$ as uniform from a ball, one obtains an accurate prediction for the score $\sum_{\mathbf{w}} f_{\mathbf{w}}(\mathbf{t})$, whenever $\mathbf{t}$ follows a Gaussian distribution, or the uniform distribution on a sphere, ball or $\mathbb{R}^n/\Lambda$.

3. HAWK is a lattice-based signature scheme that is one of the simplest to implement, and it can be implemented on a wide range of devices.

4. Given a Hermitian form $\mathbf{Q}$ of the module lattice R^2 where $R = \mathbb{Z}[X]/(X^n+1)$, and a nontrivial automorphism $\mathbf{U} \in \mathrm{GL}_{2n}(\mathbb{Z})$ of the unstructured quadratic form related to $\mathbf{Q}$, one can solve SMLIP for $\mathbf{Q}$ by running BKZ-β with $\beta = n/2+1$ on some sublattice that (1) is constructed in polynomial time from $\mathbf{U}$ and (2) has rank at most n.

5. Every attack against Learning with Errors (LWE) can be phrased more generally as an attack against Bounded Distance Decoding on random lattices. The general analogue is as efficient but easier to understand thanks to geometric intuition.

6. Machine-learning based attacks against sparse-secret LWE are worse than lattice-reduction based attacks.

7. Building further upon the work of other researchers is only sustainable, if the software related to papers is released open-source, and if it is easy to use. Additionally, the software is more reusable when the version control, e.g., Git, history is published.

8. All built-in BibTEX base styles fail to sort by family names. For example, 'Vasco da Gama' is catalogued at 'G', while BibTEX catalogues it incorrectly at 'D'.

9. The lattice isomorphism problem is the easiest to comprehend in terms of an arbitrary rotation. However, in implementations and algorithms, quadratic forms are formally necessary.

10. Large language models not only produce convincing, false statements sometimes, but they are also destructive for the educational system, computer consumer market, electricity net, and climate.

11. Most researchers use *cf.* incorrectly as a synonym for 'see' rather than to compare/relate it to something else.

12. Engaging in recreational activities with co-workers improves productivity and social cohesion.

Ludo N. Pulles

Leiden, 23 September 2026