Lattice problems whose average-case complexity is connected to worst-case assumptions are appealing foundations for provably secure cryptosystems. A sharper understanding of their inherent hardness would enable more precise security analyses, thus resulting in more efficient cryptographic primitives.

We review the landscape of the average-case complexity of lattice problems, sketch some of the technical tools employed in their analysis, and discuss ongoing efforts to assess their generic-case complexity.