Lattices and Factoring
(Invited Talk)

Léo Ducas[1]

Cryptology Group,
Centrum Wiskunde & Informatica,
Amsterdam, The Netherlands

Abstract. In this talk, I would like to re-popularize two dual ideas that relate Lattices and Factoring. Such a connection may appear surprising at first, but is only one logarithm away: after all, factoring is nothing more than a *multiplicative* knapsack problem, i.e. a subset product problem, where the weights are given by the set of small enough primes.
The first of the two ideas, we owe to Schnorr (1991) and to Adleman (1995). It consists in finding close or short vectors in a carefully crafted lattice, in the hope that they will provide so-called factoring relations. While this idea does not appear to lead to faster factoring algorithms, it remains fascinating and has in fact lead to other major results. Indeed, the Schnorr-Adleman lattice plays a key role in the proof by Ajtai (1998) of the NP-hardness of the shortest vector problem.
The second idea, due to Chor and Rivest (1988) shows a reverse connection: constructing the lattice this time using *discrete* logarithms, they instead solve the bounded distance decoding (BDD) problem through easy factoring instances. Revisiting their idea, Pierrot and I (2018) showed that this was a quite close to an optimal construction for solving BDD in polynomial time. It was in fact the best known such construction until some recent work by Peikert and Mook (2020).
I wish to conclude with an invitation to explore the cryptographic potential of other lattices than the random q-ary lattices —the lattices underlying the Learning with Error problem (LWE) and the Short Integer Solution problem (SIS). While SIS and LWE have shown to be very convenient for constructing the most advanced schemes and protocols, I believe that more general lattices have a yet untapped potential for cryptography.