

Contents

1	The History of the LLL-Algorithm	1
	Ionica Smeets	
2	Hermite's Constant and Lattice Algorithms	19
	Phong Q. Nguyen	
3	Probabilistic Analyses of Lattice Reduction Algorithms	71
	Brigitte Vallée and Antonio Vera	
4	Progress on LLL and Lattice Reduction	145
	Claus Peter Schnorr	
5	Floating-Point LLL: Theoretical and Practical Aspects	179
	Damien Stehlé	
6	LLL: A Tool for Effective Diophantine Approximation	215
	Guillaume Hanrot	
7	Selected Applications of LLL in Number Theory	265
	Denis Simon	
8	The van Hoeij Algorithm for Factoring Polynomials	283
	Jürgen Klüners	
9	The LLL Algorithm and Integer Programming	293
	Karen Aardal and Friedrich Eisenbrand	
10	Using LLL-Reduction for Solving RSA and Factorization Problems	315
	Alexander May	

11	Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign	349
	Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, and William Whyte	
12	The Geometry of Provable Security: Some Proofs of Security in Which Lattices Make a Surprise Appearance	391
	Craig Gentry	
13	Cryptographic Functions from Worst-Case Complexity Assumptions	427
	Daniele Micciancio	
14	Inapproximability Results for Computational Problems on Lattices	453
	Subhash Khot	
15	On the Complexity of Lattice Problems with Polynomial Approximation Factors	475
	Oded Regev	