Complexity Of Lattice Problems A Cryptographic Perspective The Springer International Series In Engineering And Computer Science

[Book] Complexity Of Lattice Problems A Cryptographic Perspective The Springer International Series In Engineering And Computer Science

Yeah, reviewing a books **Complexity Of Lattice Problems A Cryptographic Perspective The Springer International Series In Engineering And Computer Science** could ensue your close contacts listings. This is just one of the solutions for you to be successful. As understood, triumph does not suggest that you have fantastic points.

Comprehending as competently as concord even more than supplementary will have the funds for each success. adjacent to, the pronouncement as capably as perception of this Complexity Of Lattice Problems A Cryptographic Perspective The Springer International Series In Engineering And Computer Science can be taken as capably as picked to act.

Complexity Of Lattice Problems A

On the Complexity of Lattice Problems with Polynomial ...
n, lattice problems are known to be in complexity classes such as NP\coNP and are hence unlikely to be NP-hard Here we survey known results in this area We also discuss some related zero-knowledge protocols for lattice problems 1 Introduction A lattice is the set of all integer combinations of n linearly independent vectors v1;:::;vn in Rn

On the Complexity of Lattice Puzzles
2012ACMSubjectClassification Theoryofcomputation→Problems,reductionsandcompleteness lattice puzzle If the puzzle has a hint of the order of each set of plates by, for example, one/twosided operations #depths rule complexity note

Computational complexity of lattice problems and cyclic ...
Complexity of lattice problems SVP and SIVP are both known to be NP-hard In fact, even the problem of nding the rst successive minimum 1 (respectively, all successive minima 1;:::; n) of a given lattice is NP-hard: it is as hard as SVP (respectively, SIVP) Moreover {Theorem 1 (SIVP to SVP reduction)

The Complexity of the Covering Radius Problem on Lattices ...

these applications, attention to the covering radius problem, specifically from a computational complexity point of view, has been recently brought by Micciancio [26] who showed that this problem can be used to get tighter connections between the average and worst case complexity of lattice problems

Lattice-based Cryptography

complexity aspects of lattice problems Figure 1: A two-dimensional lattice and two possible bases So what is a lattice? A lattice is a set of points in n-dimensional space with a periodic structure, such as the one illustrated in Figure 1

A Deterministic Single Exponential Time Algorithm for Most ...

The complexity of lattice problems has been investigated intensively All three problems mentioned above have been shown to be NP-hard both to solve exactly [54, 3, 13], or even approximate within small (constant or sub-polynomial in n) approximation factors [13, 8, ...

Complex Lattice Reduction Algorithm for Low-Complexity ...

(MIMO), complexity reduction, complex-valued algorithm I INTRODUCTION BY exploiting the linearity of a communication chan-nel and the lattice structure of the modulation, many detection problems can be interpreted as the problem of finding the closest lattice point This lattice viewpoint of detection problems [1]–[3] forms the foundation

Noninteractive Statistical Zero-Knowledge Proofs for ...

characterizing the complexity of lattice problems Proof systems have provided an excellent means of making progress in this endeavor We review some recent results below, after introducing the basic notions An n-dimensional lattice in Rn is a periodic \grid" of points consisting of all integer linear

Trapdoors for Hard Lattices and New Cryptographic ...

exceedingly useful in studying the computational complexity of lattice problems [AR03, AR05, Pei07], particularly their worst-case/average-case connections (eg, [Reg04, MR07, Reg05]) Up to this point, however, discrete Gaussians have been used primarily as an ...

Generalized compact knapsacks, cyclic lattices, and ...

Keywords: Knapsack problem, cyclic lattices, average-case complexity, one-way functions 1 Introduction Few problems in the theory of computational complexity and its application to the foundations of cryptog-raphy have been as controversial as the knapsack problem and its many variants, including the notorious NP-hard subset-sum problem [31]

On the Lattice Smoothing Parameter Problem

reductions for lattice problems, a wealth of lattice-based cryptographic constructions, and (implicitly) the tightest known transference theorems for fundamental lattice quantities In this work we initiate a study of the complexity of approximating the smoothing parameter to within a factor , denoted -GapSPP We show that (for "= 1=poly(n)):

Post-quantum Lattice-based Cryptography Implementations: ...

computational problems on lattices to within polynomial factors [9] This is the basis for security of lattice-based cryptography schemes The fastest algorithm to solve the SVP problem has the time and memory complexity of 2O(n)[10–12] We take the below definitions from [13]: ACM Computing Surveys, Vol 1, No 1, Article 1

A Deterministic Single Exponential Time Algorithm for Most ...

The complexity of lattice problems has been investigated intensively All three problems mentioned above have been shown to be NP-hard (possibly under randomized reductions) both to solve exactly [vEB81, Ajt98, BS99], or even approximately within small …

A Decade of Lattice Cryptography

standard lattice problems, and their many cryptographic applications Contents Indeed, the complexity of these problems appears to vary quite widely depending on the type of group (eg, multiplicative groups of integers modulo a prime or of other finite fields, elliptic curve groups, etc)

How to Use a Short Basis: Trapdoors for Hard Lattices and …

discrete Gaussian probability distribution over an arbitrary lattice, given an appropriate basis The sampling algorithm also enables simpler and (slightly) tighter worst-case/average-case connections for lattice problems, and may have additional applications in complexity theory and cryptography 111 Gaussian Sampling Algorithm

On the Quantum Complexity of the Continuous Hidden …

groups are very interesting as well and have fascinating connections with lattice problems [30]; however, no polynomial time algorithm is known for those cases, and the best known algorithm has sub-exponential complexity [20], using very di erent techniques The simplest version of the Hidden Subgroup Problem consists of nding a

On the Lattice Isomorphism Problem

science including algorithms, computational complexity and cryptography One of the most fundamental lattice problems is the Shortest Vector Problem (SVP), where given a lattice basis the goal is to find a shortest nonzero vector in the lattice This problem is known to be NP-hard (underrandomized reductions) for approximation factors which

THE COMPLEXITY OF THE COVERING RADIUS PROBLEM

problem, speci cally from a computational complexity point of view, has been recently brought by Micciancio (2004) who showed that this problem can be used to get tighter connections between the average- and worst-case complexity of lattice problems In the covering radius problem, given a lattice (or a code) and some value r,

A CCA-Secure Cryptosystem Using Massive MIMO Channels

lattice problems Hence, this complexity is conjectured to be exponentially hard in the number of transmitter antennas Alice uses In particular, no existing algorithms, including those of a quantum computer, have been shown to solve such problems in sub-exponential time