A Decade of Lattice Cryptography

Chris Peikert
Computer Science and Engineering
University of Michigan, United States
Editorial Scope

Topics

Foundations and Trends® in Theoretical Computer Science publishes surveys and tutorials on the foundations of computer science. The scope of the series is broad. Articles in this series focus on mathematical approaches to topics revolving around the theme of efficiency in computing. The list of topics below is meant to illustrate some of the coverage, and is not intended to be an exhaustive list.

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations research
- Parallel algorithms
- Quantum computation
- Randomness in computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2014, Volume 10, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.
A Decade of Lattice Cryptography

Chris Peikert
Computer Science and Engineering
University of Michigan, United States
# Contents

1 Introduction 2  
  1.1 Scope and Organization 4  
  1.2 Other Resources 6  

2 Background 7  
  2.1 Notation 7  
  2.2 Lattices 8  
  2.3 (Discrete) Gaussians and Subgaussians 12  
  2.4 Cryptographic Background 14  

3 Early Results 18  
  3.1 Ajtai’s Function and Ajtai-Dwork Encryption 18  
  3.2 NTRU 21  
  3.3 Goldreich-Goldwasser-Halevi Encryption and Signatures 22  
  3.4 Micciancio’s Compact One-Way Function 24  
  3.5 Regev’s Improvements to Ajtai-Dwork 25  

4 Modern Foundations 26  
  4.1 Short Integer Solution (SIS) 26  
  4.2 Learning With Errors (LWE) 33  
  4.3 Ring-SIS 41  
  4.4 Ring-LWE 47
5 Essential Cryptographic Constructions 54
  5.1 Collision-Resistant Hash Functions 55
  5.2 Passively Secure Encryption 55
  5.3 Actively Secure Encryption 68
  5.4 Lattice Trapdoors 70
  5.5 Trapdoor Applications: Signatures, ID-Based Encryption 86
  5.6 Signatures Without Trapdoors 93
  5.7 Pseudorandom Functions 99

6 Advanced Constructions 104
  6.1 Fully Homomorphic Encryption 104
  6.2 Attribute-Based Encryption 114

7 Open Questions 122
  7.1 Foundations 122
  7.2 Cryptographic Applications 125

References 129
Abstract

Lattice-based cryptography is the use of conjectured hard problems on point lattices in \( \mathbb{R}^n \) as the foundation for secure cryptographic systems. Attractive features of lattice cryptography include apparent resistance to quantum attacks (in contrast with most number-theoretic cryptography), high asymptotic efficiency and parallelism, security under worst-case intractability assumptions, and solutions to long-standing open problems in cryptography.

This work surveys most of the major developments in lattice cryptography over the past ten years. The main focus is on the foundational short integer solution (SIS) and learning with errors (LWE) problems (and their more efficient ring-based variants), their provable hardness assuming the worst-case intractability of standard lattice problems, and their many cryptographic applications.

DOI: 10.1561/0400000074.
1

Introduction

This survey provides an overview of lattice-based cryptography, the use of apparently hard problems on point lattices in $\mathbb{R}^n$ as the foundation for secure cryptographic constructions. Lattice cryptography has many attractive features, some of which we now describe.

Conjectured security against quantum attacks. Most number-theoretic cryptography, such as the Diffie-Hellman protocol [62] and RSA cryptosystem [173], relies on the conjectured hardness of integer factorization or the discrete logarithm problem in certain groups. However, Shor [178] gave efficient quantum algorithms for all these problems, which would render number-theoretic systems insecure in a future where large-scale quantum computers are available. By contrast, no efficient quantum algorithms are known for the problems typically used in lattice cryptography; indeed, generic (and relatively modest) quantum speedups provide the only known advantage over non-quantum algorithms.

Algorithmic simplicity, efficiency, and parallelism. Lattice-based cryptosystems are often algorithmically simple and highly parallelizable,
consisting mainly of linear operations on vectors and matrices modulo relatively small integers. Moreover, constructions based on “algebraic” lattices over certain rings (e.g., the NTRU cryptosystem [105]) can be especially efficient, and in some cases even outperform more traditional systems by a significant margin.

**Strong security guarantees from worst-case hardness.** Cryptography inherently requires average-case intractability, i.e., problems for which random instances (drawn from a specified probability distribution) are hard to solve. This is qualitatively different from the worst-case notion of hardness usually considered in the theory of algorithms and NP-completeness, where a problem is considered hard if there merely exist some intractable instances. Problems that appear hard in the worst case often turn out to be easier on the average, especially for distributions that produce instances having some extra “structure,” e.g., the existence of a secret key for decryption.

In a seminal work, Ajtai [7] gave a remarkable connection between the worst case and the average case for lattices: he proved that certain problems are hard on the average (for cryptographically useful distributions), as long as some related lattice problems are hard in the worst case. Using results of this kind, one can design cryptographic constructions and prove that they are infeasible to break, unless all instances of certain lattice problems are easy to solve.¹

**Constructions of versatile and powerful cryptographic objects.** Historically, cryptography was mainly about sending secret messages. Yet over the past few decades, the field has blossomed into a discipline having much broader and richer goals, encompassing almost any scenario involving communication or computation in the presence of potentially

¹Note that many number-theoretic problems used in cryptography, such as discrete logarithm and quadratic residuosity, also admit (comparatively simple) worst-case/average-case reductions, but only within a fixed group. Such a reduction gives us a distribution over a group which is as hard as the worst case for the same group, but says nothing about whether the group itself is hard, or which groups are hardest. Indeed, the complexity of these problems appears to vary quite widely depending on the type of group (e.g., multiplicative groups of integers modulo a prime or of other finite fields, elliptic curve groups, etc.).
malicious behavior. For example, the powerful notion of fully homomorphic encryption (FHE), first envisioned by Rivest et al. [172], allows an untrusted worker to perform arbitrary computations on encrypted data, without learning anything about that data. For three decades FHE remained an elusive “holy grail” goal, until Gentry [80, 79] proposed the first candidate construction of FHE, which was based on lattices (as were all subsequent constructions). More recently, lattices have provided the only known realizations of other versatile and powerful cryptographic notions, such as attribute-based encryption for arbitrary access policies [97, 36] and general-purpose code obfuscation [78].

1.1 Scope and Organization

This work surveys most of the major developments in lattice cryptography over the past decade (since around 2005). The main focus is on two foundational average-case problems, called the short integer solution (SIS) and learning with errors (LWE) problems; their provable hardness assuming the worst-case intractability of lattice problems; and the plethora of cryptographic constructions that they enable.

Most of this survey should be generally accessible to early-stage graduate students in theoretical computer science, or even to advanced undergraduates. However, understanding the finer details of the cryptographic constructions—especially the outlines of their security proofs, which we have deliberately left informal so as to highlight the main ideas—may require familiarity with basic cryptographic definitions and paradigms, which can be obtained from any graduate-level course or the textbooks by, e.g., Katz and Lindell [110] or Goldreich [91]. The reader who lacks such background is encouraged to focus on the essential ideas and mechanics of the cryptosystems, and may safely skip over the proof summaries.

The survey is organized as follows:

- Chapter 2 recalls the necessary mathematical and cryptographic background.
- Chapter 3 gives a high-level conceptual overview of the seminal works in the area and their significance.
1.1. Scope and Organization

- Chapter 4 covers the modern foundations of the area, which have largely subsumed the earlier works. Here we formally define the SIS and LWE problems and recall the theorems which say that these problems are at least as hard to solve as certain worst-case lattice problems. We also cover their more compact and efficient ring-based analogues, ring-SIS and ring-LWE.

- Chapter 5 describes a wide variety of essential lattice-based cryptographic constructions, ranging from basic encryption and digital signatures to more powerful objects like identity-based encryption. These schemes are presented within a unified framework, using just a handful of concepts and technical tools that are developed throughout the chapter.

- Chapter 6 describes a few more advanced cryptographic constructions, with a focus on fully homomorphic encryption and attribute-based encryption.

- Chapter 7 concludes with a discussion of some important open questions in the area.

While we have aimed to convey a wide variety of lattice-based cryptographic constructions and their associated techniques, our coverage of such a large and fast-growing area is necessarily incomplete. For one, we do not discuss cryptanalysis or concrete parameters (key sizes etc.) of lattice-based cryptosystems; representative works on these topics include [75, 146, 76, 118, 51, 120]. We also do not include any material on the recent seminal constructions of candidate multilinear maps [77, 58, 83, 59] and their many exciting applications, such as general-purpose code obfuscation [78, 175]. While all multilinear map constructions to date are related to lattices, their conjectured security relies on new, ad-hoc problems that are much less well-understood than SIS/LWE. In particular, it is not known whether any of the proposed constructions can be proved secure under worst-case hardness assumptions, and some candidates have even been broken in certain ways (see, e.g., [53, 107, 54, 57]). Note that early constructions of fully homomorphic encryption also relied on ad-hoc assumptions, but constructions
based on more standard assumptions like (ring-)LWE soon followed; the same may yet occur for multilinear maps and their applications.

1.2 Other Resources

There are several other resources on modern lattice cryptography, or specialized subtopics thereof. (However, due to the rapid development of the field over the past few years, these surveys are already a bit dated in their coverage of advanced cryptographic constructions and associated techniques.) Some excellent options include:

- The 2007 survey by Micciancio [138] on cryptographic functions from worst-case complexity assumptions, including ring-based functions;
- the 2009 survey by Micciancio and Regev [146] on lattice-based cryptographic constructions and their cryptanalysis;
- the 2010 survey by Regev [171] on the learning with errors (LWE) problem, its worst-case hardness, and some early applications;
- the overviews of fully homomorphic encryption by Gentry [81] and Vaikuntanathan [182];
- videos from the 2012 Bar-Ilan Winter School on Lattice Cryptography and Applications [28];
- other surveys, books, and course notes [155, 141, 168, 140] on computational aspects of lattices, including cryptanalysis.
References


References

[26] Abhishek Banerjee and Chris Peikert. New and improved key-


References


References


References


References


References


References


for obtaining digital signatures and public-key cryptosystems. Commun. 

[174] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In 

[175] Amit Sahai and Brent Waters. How to use indistinguishability ob-
fuscation: deniable encryption, and more. In STOC, pages 475–484, 
2014.

[176] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduc-

[177] Claus-Peter Schnorr. Efficient signature generation by smart cards. J. 

[178] Peter W. Shor. Polynomial-time algorithms for prime factorization 
and discrete logarithms on a quantum computer. SIAM J. Comput., 

[179] Nigel P. Smart and Frederik Vercauteren. Fully homomorphic SIMD 

[180] Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case 

Efficient public key encryption based on ideal lattices. In ASIACRYPT, 


Fully homomorphic encryption over the integers. In EUROCRYPT, 

[184] Roman Vershynin. Compressed Sensing, Theory and Applica-
tions, chapter 5, pages 210–268. Cambridge University Press, 
2012. Available at http://www-personal.umich.edu/~romanv/
papers/non-asymptotic-rmt-plain.pdf

Columbia University, 2010.
References
