Final Report for Period: 09/2010 - 08/2011 **Submitted on:** 05/09/2012

Principal Investigator: Peikert, Chris . **Award ID:** 1042585

Organization: Georgia Tech Research Corp

Submitted By:

Peikert, Chris - Principal Investigator

Title:

Collaborative Research: CT-ISG: Efficient Cryptography Based on Lattices

Project Participants

Senior Personnel

Name: Peikert, Chris

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Rosen, Alon

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator and presenter of 'SWIFFT: A Modest Proposal for FFT Hashing,' publication in Fast Software Encryption (FSE) 2008. Collaborator on 'Pseudorandom Functions and Lattices,' Eurocrypt'12.

Name: Regev, Oded

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'learning with errors over rings' project.

Name: Micciancio, Daniele

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller,' Eurocrypt'12.

Post-doc

Name: Lyubashevsky, Vadim

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'learning with errors over rings' project.

Graduate Student

Name: Vaikuntanathan, Vinod

Worked for more than 160 Hours: Yes

Contribution to Project:

Graduate student summer 2007 intern at SRI; collaborator on recent papers.

Name: Wan, Andrew

Worked for more than 160 Hours: Yes

Contribution to Project:

Summer student intern at SRI. Worked on cryptanalysis of lattice-based signature schemes. Supported for about 12 weeks.

Name: Cash, David

Worked for more than 160 Hours: No

Contribution to Project:

Collaborated in research project on circular and key-dependent message security. No financial support.

Name: O'Neill, Adam

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on deniable encryption project, Fall 2009-Fall 2010.

Name: Banerjee, Abhishek

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'Pseudorandom Functions and Lattices,' Eurocrypt'12.

Name: Lindner, Richard

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator or 'Better Key Sizes (and Attacks) on LWE-Based Encryption,' CT-RSA'11.

Name: Alperin-Sheriff, Jacob

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'Circular and KDM Security for Identity-Based Encryption,' PKC'12.

Name: Krehbiel, Sara

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'How to Share a Lattice Trapdoor,' submitted manuscript.

Name: Bendlin, Rikke

Worked for more than 160 Hours: Yes

Contribution to Project:

Collaborator on 'How to Share a Lattice Trapdoor,' submitted manuscript.

Undergraduate Student

Technician, Programmer

Other Participant

Research Experience for Undergraduates

Organizational Partners

The Interdisciplinary Center Herzliya

Alon Rosen was a collaborator and presenter of 'SWIFFT: A Modest Proposal for FFT Hashing,' appearing at Fast Software Encryption 2008.

Columbia University

Collaborated with Columbia faculty on a cryptanalysis project.

Tel Aviv University

Aarhus University

Graduate student Rikke Bendlin visited Georgia Tech to collaborate with PI and his graduate students.

Other Collaborators or Contacts

I have also collaborated with the following people on research topics related to this project:

Rocco Servedio and Tal Malkin, professors of computer science at Columbia University

Amit Sahai, professor of computer science at UCLA

Benny Applebaum, postdoc in computer science at Princeton University

Dennis Hofheinz of Karlsruher Institut f?r Technologie, Germany

Eike Kiltz of Centrum Wiskunde & Informatica, Netherlands

Mihir Bellare of UC San Diego

Brent Waters of U Texas, Austin

Activities and Findings

Research and Education Activities:

Major research activities include several new lattice-based cryptographic schemes, algorithms, and complexity-theoretic results that have appeared (or will appear) in highly selective conferences (STOC, CRYPTO, EUROCRYPT, FSE) and journals (Computational Complexity, SICOMP, J Cryptology). A specific list of publications is given separately in this report.

Educational activities include collaborations with summer PhD student interns (at SRI) and other graduate and undergraduate students and postdocs (at Georgia Tech) on topics in lattice-based cryptography, including the design and analysis of new schemes, devising attacks on proposed schemes from the literature, and implementations. Other educational activities include running a lattice cryptography reading group at Georgia Tech, and supervising several undergraduate students in implementing many of the cryptographic schemes designed under this project.

Educational activities also include presentations of specific research results and broader surveys at the following institutions, conferences, and workshops, in most cases including significant attendance by graduate students:

* Invited plenary talk at Security and Cryptography for Networks, Sep 2010

* Invited tutorial at Lattice Crypto Day, Paris, May 2010

* Invited tutorials at Workshop on Public-Key Cryptography and
  Geometry of Numbers, Leiden University, Amsterdam, May 2010

* Invited plenary talk at Theory of Cryptography Conference (TCC) 2009

* Workshop on Barriers in Computational Complexity II, Princeton

* Workshop on Computer Security and Cryptography, University of Montreal

* UC Berkeley

* University of Maryland

* Penn State University

* Georgia Institute of Technology

* Massachusetts Institute of Technology

* UC San Diego

* Columbia University

* McGill University

* Microsoft Research, Silicon Valley and Redmond

* STOC 2008 and 2009 conferences

* EUROCRYPT 2010 conference

* CRYPTO 2008, 2009, 2010 conferences

Findings:

Our main findings include (asymptotically efficient) secure lattice-based constructions of the cryptographic primitives and applications listed below. According to the state of the art, all of these schemes are resistant to quantum computing-based attacks, are highly parallelizable, and are secure assuming only the worst-case hardness of standard lattice problems.

* Pseudorandom functions and permutations (also known as block ciphers)

* Public-key encryption based (for the first time) on the standard decisional shortest vector problem on arbitrary lattices.

* Simple and efficient chosen ciphertext-secure public key encryption schemes.

* 'Hash-and-sign' unforgeable signature schemes, in both the random oracle and standard models.

* Identity-based encryption, both 'single-level' and 'hierarchical,' in both the random oracle and standard models.

* Efficient and fully parallelizable algorithms for implementing all of the above applications, and preliminary reference implementations for some.

* A highly efficient ring-based public key encryption scheme.

* Encryption schemes that are resilient to partial leakage of the secret key.

* A 'deniable' encryption scheme that is secure under coercion of both the sender and receiver simultaneously.

* Simple 'universally composable' oblivious transfer and multiparty computation protocols.

* Noninteractive zero-knowledge proofs for various lattice problems.

* 'Circular-secure' public-key and identity-based encryption that is secure for key-dependent messages.

* 'Threshold' versions of many of the above applications, which distribute trust and increase robustness by distributing privileged information and operations across several parties (some of which may be malicious).

* A fast, practical cryptographic hash function that has been accepted as a first-round candidate to the NIST SHA-3 competition.

Our research has also strengthened the foundations in the use of lattices in cryptography and complexity theory. Findings include a method for generating computationally 'hard' lattices together with optimally short trapdoor bases, new and improved attack methods on lattice-based cryptoschemes, and limits on the hardness of certain lattice problems in norms other than the standard Euclidean (l2) norm.

In addition, our research has defined and constructed, based on lattices and other mathematical foundations, new cryptographic concepts and abstractions that have had significant additional applications across cryptography more broadly. These include:

* 'Lossy' trapdoor functions.

* 'Preimage sampleable' functions.

* Dual-mode and 'lossy' encryption schemes.

Training and Development:

The project has included participation by a three PhD student summer interns (at SRI) who had little to no prior research experience in lattice-based cryptography: Vinod Vaikuntanathan, Andrew Wan, and Joel Alwen. From these interactions, Vaikuntanthan is a co-author on three publications (1 in STOC, 2 in CRYPTO); Wan is a co-author on a paper under submission, and Alwen is the co-author on a paper that appeared in STACS 2009 and (by invitiation) in the journal Theory of Computing Systems.

At Georgia Tech, the project includes ongoing participation by PhD students Daniel Dadush, Abhishek Banerjee, Sara Krehbiel, and Jacob Alperin-Sheriff; former PhD student Adam O'Neill (now graduated); and undergraduate students William Rorabaugh and Sam Kim.

Outreach Activities:

Journal Publications

Chris Peikert, "Limits on the Hardness of Lattice Problems in l_p Norms", Computational Complexity, p. 300, vol. 17, (2008). Published, 10.1007/s00037-008-0251-3

Chris Peikert and Brent Waters, "Lossy Trapdoors Functions and Their Applications", SIAM Journal on Computing, p. , vol. , (2010). Accepted,

David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert, "Bonsai Trees, or How to Delegate a Lattice Basis", Journal of Cryptology, p. , vol. , (2010). Submitted,

Joel Alwen and Chris Peikert, "Generating Shorter Bases for Hard Random Lattices", Theory of Computing Systems, p. , vol. , (2011). Accepted,

Books or Other One-time Publications

Chris Peikert, Brent Waters, "Lossy Trapdoor Functions and Their Applications", (2008). Conference proceedings, Published
Editor(s): Cynthia Dwork
Collection: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008
Bibliography: ISBN 978-1-60558-047-0

Craig Gentry, Chris Peikert, Vinod Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions", (2008). Conference proceedings, Published
Editor(s): Cynthia Dwork
Collection: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008
Bibliography: ISBN 978-1-60558-047-0

Chris Peikert, "Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem", (2009). Conference proceedings, Published
Editor(s): Michael Mitzenmacher
Collection: Symposium on Theory of Computing (STOC)
Bibliography: ISBN:978-1-60558-506-2

Benny Applebaum, David Cash, Chris Peikert, Amit Sahai, "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems", (2009). Conference proceedings, Accepted
Editor(s): Shai Halevi
Collection: CRYPTO
Bibliography: None available yet

Joel Alwen, Chris Peikert, "Generating Shorter Bases for Hard Random Lattices", (2009). Conference proceedings, Published
Editor(s): Susanne Albers, Jean-Yves Marion
Collection: Symposium on Theoretical Aspects of Computer Science
Bibliography: Published by Schloss Dagstuhl; available at http://drops.dagstuhl.de/opus/volltexte/2009/1832

Yuriy Arbitman, Gil Dogon, Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, Alon Rosen, "SWIFFTX: A Proposal for the SHA-3 Standard", (2008). NIST Proposal, Submitted to NIST, published on Internet
Bibliography: None available yet

Chris Peikert, "An ef&#64257;cient and parallel Gaussian sampler for lattices", (2010). Conference proceedings, Published
Editor(s): Tal Rabin
Collection: Proceedings of CRYPTO 2010
Bibliography: pages 80-97

David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert, "Bonsai trees, or how to delegate a lattice
basis", (2010). C, Published
Editor(s): Henri Gilbert
Collection: Proceedings of EUROCRYPT 2010
Bibliography: pages 523?552

Vadim Lyubashevsky, Chris Peikert, and Oded Regev, "On ideal lattices and learning with errors over rings", (2010). Conference proceedings, Published
Editor(s): Henri Gilbert
Collection: Proceedings of EUROCRYPT 2010
Bibliography: pages 1-23

Yevgeniy Dodis, Sha&#64257; Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan, "Public-key encryption schemes with auxiliary inputs", (2010). Conference proceedings, Published
Collection: Proceedings of TCC 2010
Bibliography: pages 361?381

Sha&#64257; Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan, "Robustness of the learning with errors assumption", (2010). Conference proceedings, Published
Collection: Proceedings of ICS 2010 (Symposium on Innovations in Computer Science)
Bibliography: Unknown page numbers.

Richard Lindner, Chris Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption", (2011). Book, Published
Editor(s): Aggelos Kiayias
Collection: Proceedings of CT-RSA'11 (Cryptographer's Track)
Bibliography: N/A

Abhishek Banerjee, Chris Peikert, Alon Rosen, "Pseudorandom Functions and Lattices", (2012). Book, Published
Editor(s): David Pointcheval, Thomas Johansson
Collection: Proceedings of Eurocrypt'12
Bibliography: N/A

Daniele Micciancio, Chris Peikert, "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller", (2012). Book, Published
Editor(s): David Pointcheval, Thomas Johansson
Collection: Proceedings of Eurocrypt'12
Bibliography: N/A

Jacob Alperin-Sheriff, Chris Peikert, "Circular and KDM Security for Identity-Based Encryption", (2012). Book, Published
Collection: Proceedings of PKC'12
Bibliography: N/A

Adam O'Neill, Chris Peikert, Brent Waters, "Bi-Deniable Public-Key Encryption", (2011). Book, Published
Editor(s): Phillip Rogaway, Rei Safavi-Naini
Collection: Proceedings of Crypto'11
Bibliography: N/A

Web/Internet Site

Other Specific Products

Contributions

Contributions within Discipline:

Findings from the project have provided fundamental conceptual contributions, analytical techniques, and new concrete constructions to the discipline of cryptography. In particular, our findings have greatly advanced the state of the art of 'lattice-based' cryptography, which provides schemes that are highly parallelizable, efficient, and apparently secure even against quantum computers.

Conceptual contributions include:

* The notion of 'lossy functions,' and in particular 'lossy trapdoor functions' (lossy TDFs). We show that lossy TDFs can be used as the foundation for simple and efficient constructions of several important and powerful cryptographic tools, including collision-resistant hash functions, chosen ciphertext-secure encryption, oblivious transfer, and more.

* The notion of 'preimage sampleable functions' (PSFs), which generalize the long-standing notion of trapdoor permutations (TDPs). Our research shows that PSFs can act as a secure replacement for TDPs in many common cryptographic applications (e.g., signature schemes and identity-based encryption).

* The notion of a 'bonsai tree,' which is a hierarchy of trapdoor functions supporting expressive and selective control and delegation of its trapdoors for applications such as digital signatures and (hierarchical) identity-based encryption.

Specific contributions include:

* The first public-key encryption scheme whose security can provably be based on the standard 'shortest vector problem' on lattices. This work resolves a long-standing open problem, and was awarded Best Paper at STOC 2009.

* Constructions of identity-based encryption (IBE) and hierarchical IBE in both the 'random oracle' model, and the standard model. These works appeared in STOC 2008 and Eurocrypt 2010, and were awarded Best Paper at the latter conference.

* Highly efficient and compact public-key encryption schemes based on lattices arising from rings and number fields.

* Simple and modular algorithms for generating a 'hard' lattice together with an optimally short basis (or 'strong trapdoor') for that lattice. These algorithms are crucial components for generating keys in many lattice-based cryptographic schemes.

* Simple and efficient public-key and identity-based encryption schemes that remain secure even when encrypting their own secret keys, or the secret keys of others. Until recently, achieving such 'key-dependent security' was a long-shanding goal with many applications in credential schemes, homomorphic encryption, formal analysis of protocols, etc.

* New and very general analyses of 'discrete Gaussian distributions,' which play an essential role in the study of lattices in mathematics and computer science. Our analysis shows that discrete Gaussians behave very 'nicely' under commonly-used metrics called l_p norms,

and under operations such as convolution.
The new analysis applies broadly to the study of lattices in computer science, and in particular, it improves upon the known security of essentially all lattice-based cryptographic schemes.

* Algorithms that sample from a discrete Gaussian distribution over a lattice, given any set of sufficiently short vectors in the lattice. These algorithms have numerous applications both in cryptographic schemes based on lattices, and within the study of the complexity of lattice problems. The most recent algorithm for this task is also efficient and fully parallelizable, making it suitable for implementation in real cryptosystems.

* Noninteractive zero-knowledge proofs for various lattice problems of cryptographic importance.

Contributions to Other Disciplines:

Contributions to Human Resource Development:

The project has involved the mentoring of several graduate and undergraduate students, many of whom continue to work on topics in lattices and cryptography.

Contributions to Resources for Research and Education:

The project has supported the creation of public educational resources such as lecture notes and presentations (slides, video) that are widely consulted by other students and researchers.

Contributions Beyond Science and Engineering:

Conference Proceedings

Peikert, C, Some Recent Progress in Lattice-Based Cryptography, "MAR 15-17, 2009", THEORY OF CRYPTOGRAPHY, 6TH THEORY OF CRYPTOGRAPHY CONFERENCE, TCC 2009, 5444: 72-72 2009

Lyubashevsky, V;Micciancio, D;Peikert, C;Rosen, A, SWIFFT: A Modest Proposal for FFT Hashing, "FEB 10-13, 2008", FAST SOFTWARE ENCRYPTION, 5086: 54-72 2008

Peikert, C;Vaikuntanathan, V, Noninteractive statistical zero-knowledge proofs for lattice problems, "AUG 17-21, 2008", ADVANCES IN CRYPTOLOGY - CRYPTO 2008, PROCEEDINGS, 5157: 536-553 2008

Peikert, C;Vaikuntanathan, V;Waters, B, A framework for efficient and composable oblivious transfer, "AUG 17-21, 2008", ADVANCES IN CRYPTOLOGY - CRYPTO 2008, PROCEEDINGS, 5157: 554-571 2008

Peikert, C, Limits on the hardness of lattice problems in l(p) norms, "JUN 13-16, 2007", COMPUTATIONAL COMPLEXITY, 17 (2): 300-351 2008

Peikert, C, Limits on the hardness of lattice problems in l(p) norms, "JUN 13-16, 2007", Twenty-Second Annual IEEE Conference on Computational Complexity, Proceedings, : 333-346 2007

Categories for which nothing is reported:

Activities and Findings: Any Outreach Activities

Any Web/Internet Site

Any Product

Contributions: To Any Other Disciplines

Contributions: To Any Beyond Science and Engineering