Lattice Based Cryptography

Daniele Micciancio, University of California, San Diego

`daniele@cs.ucsd.edu`

Revised August 12, 2003

Cryptographic applications of lattices include both cryptanalysis and the design of (provably secure) cryptographic functions. Cryptanalysis applications are usually based on lattice reduction techniques. The name “lattice based cryptography” typically refers to the second kind of applications: using lattices as a source of computational hardness in the construction of cryptographic functions which are at least as hard to break as solving some underlying lattice problem.

The study of lattice based cryptography has been largely stimulated by Ajtai’s discovery in 1996 [1] that certain variants of the knapsack problem are at least as hard to break on the average as the worst case instance of certain lattice problems, e.g., solving the Shortest Vector Problem (SVP) approximately within polynomial factors. Specifically, assuming that there is no efficient algorithm to approximate SVP within a factor $g = n^c$ in the worst case (where n is the dimension of the lattice, and c is an arbitrary constant independent of n), one can build knapsack-like cryptographic (one-way) functions that are almost certainly hard to break (when the key is chosen at random). In 1997 Ajtai and Dwork [2] also proposed a cryptosystem with similar average-case/worst-case connection properties: decrypting random challenges is at least as hard as solving the worst-case instance of a variant of the shortest vector problem, called the *unique* SVP (uSVP). Since finding approximate solutions to lattice problems gets easier and easier as the approximation factor grows, an important question in the area is to determine the smallest factor g such that one can build cryptographic functions that are as hard to break as finding g -approximate solutions to lattice problems. At the time of this writing, the strongest known results are Micciancio’s collision resistant hash functions [5] based on the inapproximability of the covering

radius problem within $g \approx n^{2.5}$, and Regev's cryptosystem [7] based on the inapproximability of uSVP within $g \approx n^{1.5}$.

All these results about lattice based cryptography are mostly interesting from a theoretical viewpoint, as they are the only known cryptographic constructions that can be proved secure based on a worst case complexity assumption (see the entry computational complexity for further discussion on complexity assumptions). In practice, most lattice based cryptographic functions need extremely large keys in order to avoid known cryptanalytic attacks. The reason is that the storage typically required by an n -dimensional lattice grows at least as the square of the security parameter n . So, even if the security parameter is set to a few hundreds, the resulting key can easily exceeds hundreds of thousands of bits. However, practical lattice based cryptographic constructions may be possible. The main practical lattice based cryptosystem is NTRU, proposed by Hoffstein, Pipher and Silverman in 1996 [3]. NTRU achieves small key size using a special class of lattices (convolutional modular lattices) that allow for very compact representation. Unfortunately, NTRU is not known to be provably secure based on any worst case complexity assumptions, so the security of this system relies on traditional cryptanalytic methods.

Lattice based cryptography is still a young and very active research area, and work is being done toward the design of cryptosystems that are both very efficient, and have provable security guarantees similar to Ajtai's original construction. A recent result pointing in this direction, is the discovery by Micciancio [4] that certain generalized compact knapsacks are at least as hard to break as solving the worst case instance of some lattice problems. These compact knapsacks achieve very small key size using a class of lattices different, but related to those used by NTRU. However, they do not provide an encryption scheme because they lack the trapdoor (secret key) necessary for decryption. Other recent results that may lead to provably secure practical constructions are the lattice based identification schemes of Micciancio and Vadhan [6], where the same lattice can be shared by all users, and the public key consists of a single vector (with secret key given by the lattice point closest to the public vector).

For a detailed study of lattice based cryptographic functions with provable security properties and an expository overview of the main lattice based cryptosystems, the reader is referred to [5]. See also lattice reduction for information about the use of lattices in cryptanalysis.

References

- [1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing - STOC '96*, pages 99–108, Philadelphia, Pennsylvania, USA, May 1996. ACM.
- [2] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on theory of computing - STOC '97*, pages 284–293, El Paso, Texas, USA, May 1997. ACM.
- [3] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem. In J. Buhler, editor, *Algorithmic Number Theory: Third International Symposium - ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288, Portland, OR, USA, June 1998. Springer.
- [4] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science - FOCS 2002*, pages 356–365, Vancouver, BC, Canada, Nov. 2002. IEEE.
- [5] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.
- [6] D. Micciancio and S. Vadhan. Statistical zero-knowledge proofs with efficient provers: lattice problems and more. In D. Boneh, editor, *Advances in cryptology - CRYPTO 2003, proceedings of the 23rd annual international cryptology conference*, volume 2729 of *Lecture Notes in Computer Science*, pages 282–298, Santa Barbara, California, USA, Aug. 2003. Springer-Verlag.
- [7] O. Regev. New lattice based cryptographic constructions. In *Proceedings of the thirty-fifth annual ACM symposium on theory of computing - STOC 2003*, pages 407–426, San Diego, CA, USA, June 2003. ACM.