A Compact Signature Scheme with Ideal Lattice (Extended Abstract)

Keita Xagawa * Keisuke Tanaka *

Keywords: lattice-based cryptography, ideal lattices, signature scheme.

Since the seminal work of Ajtai [1], lattice-based cryptography has attracted many researchers. As fruitful results, there are one-way and collision-resistant hash functions (e.g., [1, 6]) and public-key cryptosystems, which are secure based on the *worst-case* hardness of lattice problems. However, the primitives have drawbacks; The size of a public key and that of an index of hash functions is large, say $\tilde{O}(n^2)$.

Hence, to obtain compactness, Micciancio proposed one-way hash functions based on the worst-case hardness of *cyclic* lattice problems [5]. Along the way, Lyubashevsky and Micciancio, and Peikert and Rosen proposed collision-resistant hash functions based on the worst-case hardness of *cyclic/ideal* lattice problems [4, 7]. The assumptions used in them are not weaker than the assumptions that general lattice problems are hard in the worst case. Compensating for security, they enjoy lightness in weight of the key and the index, say $\tilde{O}(n)$.

Recently, Gentry, Peikert, and Vaikuntanathan proposed new lattice-based trapdoor functions [3]. Their functions are many-to-one and the trapdoor information is used for sampling from the preimages under certain distribution. The collision-resistance or one-wayness are based on the worst-case hardness of general lattice problems. Using the functions, they construct several cryptographic primitives, such as a digital signature scheme, a universally composable oblivious transfer, and an identity-based encryption scheme.

The collection of the functions is a tuple of algorithms, a key-generation algorithm, a sampling algorithm from a domain, and a sampling algorithm from the preimages. They used Ajtai's algorithm [2] as the key-generation algorithm in their collection, where Ajtai's algorithm outputs an index of the Micciancio-Regev hash functions [6] and a short basis of a lattice relative to the hash function.

Our Results: In this paper, we propose a variant of Ajtai's algorithm which outputs an index of the Lyubashevsky-Micciancio hash functions [4] and a short basis of a lattice relative to the hash function. Combining our algorithm with the sampling algorithms by Gentry et al., we obtain the collection of trapdoor collision-resistant functions. The security of the collection is proved by combining the arguments of Gentry et al. and of Lyubashevsky and Micciancio [4]. By the construction of the Lyubashevsky-Micciancio hash functions, the size of an index is $\tilde{O}(n)$.

Along the argument of Gentry et al. we obtain a signature scheme which is strongly existential unforgeable under chosen message attacks in the random oracle model if certain ideal lattice problems is hard in the worst case.

References

[1] Ajtai, M. Generating hard instances of lattice problems (extended abstract). In *STOC '96*, pp. 99–108, 1996.

[2] Ajtai, M. Generating hard instances of the short basis problem. In *ICALP '99*, pp. 1–9, 1999.

[3] Gentry, C., Peikert, C., and Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. To appear, *STOC 2008*.

[4] Lyubashevsky, V., and Micciancio, D. Generalized compact knapsacks are collision resistant. In *ICALP 2006, Part II*, pp. 144-155, 2006.

[5] Micciancio, D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity 16*, 4 (2007), 365–411.

[6] Micciancio, D., and Regev, O. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing 37*, 1 (2007), 267–302.

[7] Peikert, C., and Rosen, A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC 2006*, pp. 145–166, 2006.

* Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. {xagawa5, keisuke}@is.titech.ac.jp. Supported in part by JSPS Global COE program "Computationism as a Foundation for the Sciences", Grant-in-Aid for JSPS Fellows, NTT Information Sharing Platform Laboratories, and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 16092206