Efficient IBE using Lattice Trapdoors

Lucas Prabel

Univ Rennes, CNRS, IRISA

Abstract

Lattice-based cryptography is a promising area for constructing advanced cryptographic primitives that are potentially secure even in the presence of quantum computers. Among those primitives, identity-based encryption (IBE) is a well-known cryptographic scheme and constructing both efficient and provable secure schemes in the sandard model is still a challenging task with regard to the current NIST post-quantum competition.

This work tackles these problems by proposing two different lattice-based constructions, going along with their respective implementations, of identity-based encryption schemes based on classical IBE schemes ([ABB10]) mixed with the efficient trapdoors of Micciancio and Peikert ([MP12]). To gain in efficiency compared to existing IBE, we consider two different approaches, relying on recent results and in particular on the approximate trapdoors of [CGM19], with two different hardness assumptions.

The first approach is based on the IBE of Agrawal, Boneh, Boyen, but using gadget-based trapdoors and efficient sampling techniques in the module setting. We study the possibility of using approximate trapdoors, with SIS/LWE assumptions, rather than the exact trapdoors of [MP12], in order to obtain a more efficient scheme, without drastically reducing the intrinsic security. The use of approximate trapdoors leads to the appearance of error terms which must be taken care of in the decryption phase of the scheme. The resulting scheme is IND-sID-CPA secure in the standard model and resulted in an implementation showing that it is more efficient than the counterpart IBE using exact trapdoors.

The second approach consists in using the NTRU hardness assumption with gadget-based trapdoors in order to obtain a more efficient IBE in terms of timings and parameter sizes. This novel approach is not straightforwardly compatible with NTRU lattices and to achieve that, we use a variant of the NTRU hardness assumption, called iNTRU (for inhomogeneous NTRU), which was first defined in [GGH$^+$19]. This new scheme also resulted in an implementation, making it possible to assess its timings performance and comparing it with our previous IBE and with the diffent existing IBE of the litterature.

Therefore, this work provides different solutions in order to obtain schemes that can be used in practice, by reducing the size of their parameters (keys and ciphers) and the execution time of their different algorithms. Finally, we hope these new constructions and implementations will pave the way for more practical advanced trapdoor-based constructions.

References

[ABB10] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.

[CGM19] Y. Chen, N. Genise, and P. Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. In *ASIACRYPT (3)*, volume 11923 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2019.

[GGH$^+$19] N. Genise, C. Gentry, S. Halevi, B. Li, and D. Micciancio. Homomorphic encryption for finite automata. In *ASIACRYPT (2)*, volume 11922 of *Lecture Notes in Computer Science*, pages 473–502. Springer, 2019.

[MP12] D. Micciancio and C. Peikert. Trapdoors for lattices: simpler, tighter, faster, smaller. In *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.