RUHR-UNIVERSITÄT BOCHUM

Side-Channel Attacks on Implementations of Lattice-based Cryptosystems

Julian Speith, Felix Haarmann

Exposé
May 7, 2016
Embedded Security Group - Prof. Dr.-Ing. Christof Paar

Exposé

Despite the rapid progress in the developement of quantum computers and the hereby increasingly urgent need for post-quantum cryptographic algorithms, no such algorithms has yet been standardised [CJL$^+$16].
Our paper will give an overview over some selected lattice-based algorithms and their implementation in respect to their resistance to various side-channel attack techniques.
A short introduction to the topic of lattice-based cryptography and its advantages in prospect to quantum computers, as well as the importance of implementations of such algorithms being resistant to side-channel attacks will be given in Section 1 of our paper.
Section 2 will explain our notation and give an overview over the mathematic background information needed to understand this paper. This includes introducing the reader to the concept of *(ideal) lattices*, the *learning with errors problem (LWE)* (both described in [LPR12]), *Discrete Gaussion Distributions*, the *ring-LWE Encryption Scheme* and the *BLISS Signature Scheme*. Additionally we will give a short explanation of the side-channel attack terminology used throughout this paper, which will be similar to the one used in [KJJ99], [KJJR11], [PRB10] and [PM10].
Section 3 will deal the ring-LWE encryption scheme and will be split in two parts, starting with the description of a masked implementation of the decryption function, including a masked decoder build upon a masked table lookup (as described in [RRVV15]). As *masking* is a technique used to prevent an attacker from gaining intermediate information through side-channels while the algorithm is being executed, the second part of this section will be an evaluation of the proposed implementation in respect to its soundness to first- and second-order side-channel attacks.
A different approach to masking of the ring-LWE encryption scheme [RdCR$^+$16] will be presented in Section 4 of our paper, which will as well be split into a description of the proposed scheme and an evaluation. Furthermore, the second masking scheme will be compared to the first one in respect to efficiency and complexity.

Finally, in Section 6 we will be presenting two measures used for blinding polynomial multiplication and Gaussian sampling [Saa16], which might help against the attacks described in Section 5. As both, polynomial multiplication and Gaussian sampling, are generic operations used in most lattice based cryptosystems, those countermeasures can be used in a much broader way, than the masking approaches detailed in Section 3 and 4.

RingLWE Implementation: [PG14]
Bliss introduction: [DDLL13]
Flush, Gauss and Reload: [BHLY16]

Bibliography

[BHLY16] Leon Groot Bruinderink, Andreas Hlsing, Tanja Lange, and Yuval Yarom. Flush, gauss, and reload – a cache attack on the bliss lattice-based signature scheme. Cryptology ePrint Archive, Report 2016/300, 2016.

[CJL+16] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. Technical Report NIST IR 8105, National Institute of Standards and Technology (NIST), February 2016.

[DDLL13] Lo Ducas, Alain Durmus, Tancrde Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. Cryptology ePrint Archive, Report 2013/383, 2013.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 388–397, 1999.

[KJJR11] Paul C. Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011.

[LPR12] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. Cryptology ePrint Archive, Report 2012/230, 2012.

[PG14] Thomas Pöppelmann and Tim Güneysu. *Selected Areas in Cryptography – SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, chapter Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware, pages 68–85. Springer Berlin Heidelberg, 2014.

[PM10] Emmanuel Prouff and Robert McEvoy. First-order side-channel attacks on the permutation tables countermeasure extended version. Cryptology ePrint Archive, Report 2010/385, 2010.

[PRB10] Emmanuel Prouff, Matthieu Rivain, and Rgis Bvan. Statistical analysis of second order differential power analysis. Cryptology ePrint Archive, Report 2010/646, 2010.

[RdCR+16] Oscar Reparaz, Ruan de Clercq, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, chapter Additively Homomorphic Ring-LWE Masking, pages 233–244. Springer International Publishing, 2016.

[RRVV15] Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. A masked ring-lwe implementation. Cryptology ePrint Archive, Report 2015/724, 2015.

[Saa16] Markku-Juhani O. Saarinen. Arithmetic coding and blinding countermeasures for ring-lwe. Cryptology ePrint Archive, Report 2016/276, 2016.