Schneider, Tobias; **Paglialonga, Clara**; **Oder, Tobias**; **Güneysu, Tim**

Efficiently masking binomial sampling at arbitrary orders for lattice-based crypto. (English)

Zbl 07159417

Lin, Dongdai (ed.) et al., Public-key cryptography – PKC 2019. 22nd IACR international conference on practice and theory of public-key cryptography, Beijing, China, April 14–17, 2019. Proceedings. Part II. Cham: Springer (ISBN 978-3-030-17258-9/pbk; 978-3-030-17259-6/ebook). Lecture Notes in Computer Science 11443, 534-564 (2019).

Summary: With the rising popularity of lattice-based cryptography, the Learning with Errors (LWE) problem has emerged as a fundamental core of numerous encryption and key exchange schemes. Many LWE-based schemes have in common that they require sampling from a discrete Gaussian distribution which comes with a number of challenges for the practical instantiation of those schemes. One of these is the inclusion of countermeasures against a physical side-channel adversary. While several works discuss the protection of samplers against timing leaks, only few publications explore resistance against other side-channels, e.g., power. The most recent example of a protected binomial sampler (as used in key encapsulation mechanisms to sufficiently approximate Gaussian distributions) from CHES 2018 is restricted to a first-order adversary and cannot be easily extended to higher protection orders.

In this work, we present the first protected binomial sampler which provides provable security against a side-channel adversary at arbitrary orders. Our construction relies on a new conversion between Boolean and arithmetic (B2A) masking schemes for prime moduli which outperforms previous algorithms significantly for the relevant parameters, and is paired with a new masked bitsliced sampler allowing secure and efficient sampling even at larger protection orders. Since our proposed solution supports arbitrary moduli, it can be utilized in a large variety of lattice-based constructions, like NewHope, LIMA, Saber, Kyber, HILA5, or Ding Key Exchange.

For the entire collection see [Zbl 1408.94007].

MSC:

94A60 Cryptography

Full Text: DOI