Title:

Key Recovery Attacks on Approximate Homomorphic Encryption with Non-Worst-Case Noise Flooding Countermeasures

Abstract:

We present novel key-recovery attacks on Approximate Homomorphic Encryption schemes, such as CKKS, when employing noise-flooding countermeasures based on non-worst-case noise estimation. Our attacks build upon and enhance the seminal work by Li and Micciancio at EUROCRYPT 2021. We demonstrate that relying on average-case noise estimation undermines noise-flooding countermeasures, even if the secure noise bounds derived from differential privacy as published by Li et al. at CRYPTO 2022 are implemented. This study emphasizes the necessity of adopting worst-case noise estimation in Approximate Homomorphic Encryption when sharing decryption results. We perform the proposed attacks on OpenFHE, an emerging open-source FHE library garnering increased attention. We experimentally demonstrate the ability to recover the secret key using just one shared decryption output. Furthermore, we investigate the implications of our findings for other libraries, such as IBM's HElib library, which allows experimental estimation of the noise bounds. Finally, we reveal that deterministic noise generation utilizing a pseudorandom generator fails to provide supplementary protection.

Authors:

Qian Guo - Lund University
Denis Nabokov - Lund University
Elias Suvanto - ENS Lyon
Thomas Johansson - Lund University