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

Qian Guo[1] Denis Nabokov[1] Elias Suvanto[2] Thomas Johansson[1]

August 16, 2024

[1]Dept. of Electrical and Information Technology, Lund University, Lund, Sweden
{qian.guo,denis.nabokov,thomas.johansson}@eit.lth.se

[2]ENS Lyon, France
elias.suvanto@ens-lyon.fr

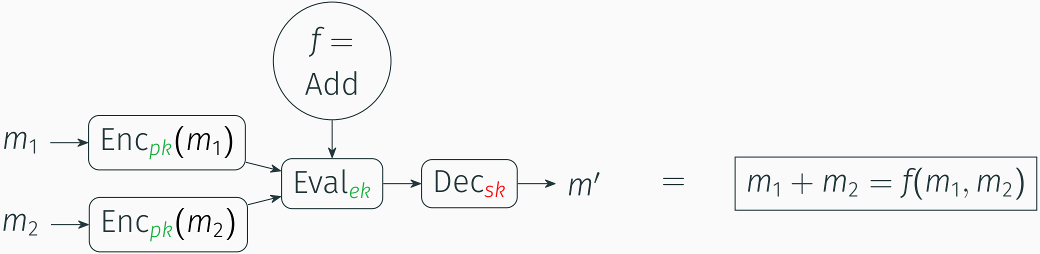
LUND UNIVERSITY

Contribution

- Show that non-worst-case noise estimation for approximate homomorphic computation can lead to key recovery
- Works even for a passive adversary
- Show such an attack for popular library OpenFHE

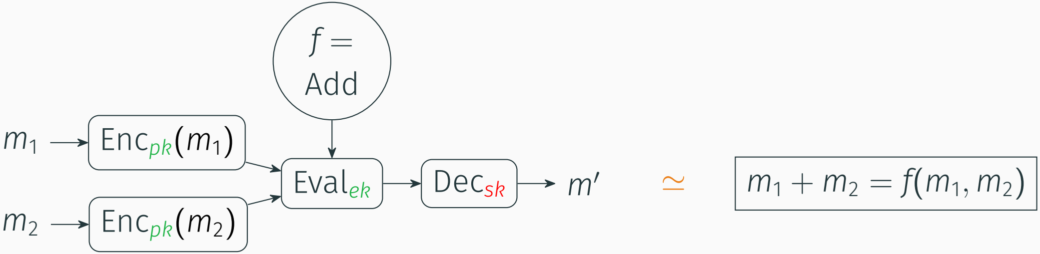
Homomorphic encryption (HE)

- HE scheme = public key encryption with special operations over ciphertexts



- Works for other functions f, such as Multiplication or more general functions
- pk, ek — public keys, sk — secret key

Approximate HE



- Final result m' deviates slightly from desired output

CKKS details

- CKKS — the most used approximate HE scheme

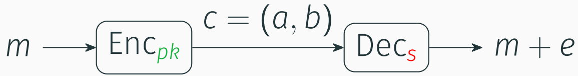
$$b = \underbrace{a \cdot s + e}_{\text{RLWE sample over } \mathbb{Z}_q[x]/(x^n+1)} + m$$

$$c = (a, b)$$

- Decryption of ciphertext c produces

$$\mathrm{Dec}_s(c) = b - a \cdot s = \underbrace{m + e}_{\text{approximate output}}$$

Announcing decryption results [LM21]

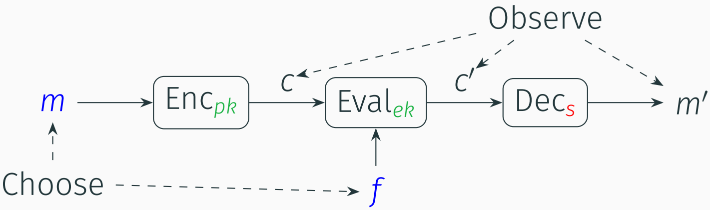


$$\underbrace{b}_{\text{(known) part of ciphertext}} - \underbrace{m + e}_{\text{(known) approx. decryption result}} = a \cdot s \implies \text{leak of } s$$

- Passive adversary can retrieve the secret key

$\mathrm{IND\text{-}CPA}^{\mathsf{D}}$ security model [LM21]

- $\mathrm{IND\text{-}CPA}^{\mathsf{D}}$ is the adaptation of $\mathrm{IND\text{-}CPA}$ to approximate HE



- New decryption function $\mathsf{Dec}^{\mathsf{D}}_{s}((a, b)) = \mathsf{Dec}_{s}((a, b)) + e_{\mathsf{new}}$

$$\underbrace{b - m + e + e_{\mathsf{new}}}_{\text{new approx. decryption result}} = \underbrace{a \cdot s - e_{\mathsf{new}}}_{\text{new RLWE sample}}$$

Noise growth

- During homomorphic operations noise inside ciphertext grows
- Added noise e_{new} have to grow with it
- If e_{new} grows slower, we show that key recovery is possible, i.e. there is no $\text{IND-CPA}^{\text{D}}$
- Specifically, the adversary by choosing an input and function to be evaluated gets

$$b' = a \cdot s + e_{\text{attack}},$$

where e_{attack} depends on ratio between ciphertext and added noise

Real-world noise estimation

- Large e_{new} negatively affects performance
- Thus, HE libraries generally use one of the two approaches:
- Empirical noise estimation
  - Owner of the secret key estimates the expected noise before the real computation
  - Contradicts $\mathrm{IND\text{-}CPA}^{\mathsf{D}}$ since there are assumptions on the input distribution and evaluation function
  - Makes e_{new} to be constant
- Average-case estimation
  - Various heuristics are used when computing the noise bound during homomorphic operations
  - Generally assumes that ciphertexts are independent, e.g. addition produces noise $\sqrt{2}$ times larger, not 2 times

Real-world noise estimation

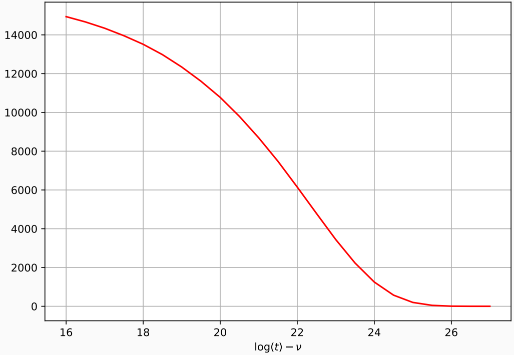
- Large e_{new} negatively affects performance
- Thus, HE libraries generally use one of the two approaches:
- Empirical noise estimation
  - Owner of the secret key estimates the expected noise before the real computation
  - Contradicts $\mathrm{IND\text{-}CPA}^{\mathrm{D}}$ since there are assumptions on the input distribution and evaluation function
  - Makes e_{new} to be constant
- Average-case estimation
  - Various heuristics are used when computing the noise bound during homomorphic operations
  - Generally assumes that ciphertexts are independent, e.g. addition produces noise $\sqrt{2}$ times larger, not 2 times

Noise estimation

- Both specified approaches lead to key recovery when an adversary chooses a big enough function f and special inputs
- We claim that worst-case estimation should be implemented if the decryption result is published

Attack on OpenFHE

- Attack considers average-case estimation
- We take evaluation function $g_t(c_0, \ldots, c_{t-1}) = \sum_{i=0}^{t-1} c_i$
- Submit inputs to compute $g_t(c_0, \ldots, c_0)$
- Using $t = 2^{57}$ it is possible to remove noise completely
- Note: $g_t(c_0, \ldots, c_0)$ can be computed fast by doubling the ciphertext $\log t$ times
- We recover the secret key in about a minute



Weight of e_{attack}; $\nu = 30$

Thank you for your attention

Bibliography

Baiyu Li and Daniele Micciancio, *On the security of homomorphic encryption on approximate numbers*, Advances in Cryptology – EUROCRYPT 2021, Part I (Zagreb, Croatia) (Anne Canteaut and François-Xavier Standaert, eds.), Lecture Notes in Computer Science, vol. 12696, Springer, Cham, Switzerland, October 17–21, 2021, pp. 648–677.