Abstract: FHE for hardware, hardware for FHE and beyond

Anisha Mukherjee
Graz University of Technology, Graz, Austria[1]

The modern digital world is quite asymmetric: devices like cell phones are compact but computationally challenged, which is why we often need access to large off-site 'cloud' servers with greater computing power. However, trust is a major issue with such 'outsourced' computations. Fully Homomorphic Encryption (FHE) introduced the possibility of performing arbitrary computations on encrypted data without needing to decrypt it. Our group[1] explores FHE under a lens to answer diverse questions about its design and implementational aspects.

Hardware for FHE: Homomorphic operations incur a computational overhead of around 10^4 to 10^6 when compared with the same operations on plaintexts/unencrypted data. Thus, software implementations of FHE schemes fail to be usable in real-world privacy preserving computations. Instead, hardware accelerators are required to bridge the gap between algorithmic design and real-world feasibility of FHE schemes. We focus on two works [KMM$^+$24, AMK$^+$] that explore two new directions for FHE acceleration.

The lattice hard problem of Learning with Errors (LWE) is a popular choice for designing FHE schemes. Polynomial multiplication forms the backbone of all homomorphic operations in a Ring/Module-LWE-based FHE scheme. In this talk we cover two new directions for FHE acceleration. In [KMM$^+$24], we design a *multiplier-less* number theoretic transform (NTT) using a Fermat number as an auxiliary modulus and apply a multivariate ring transformation to achieve seamless scalability. Using this technique, our hardware accelerator achieves around thousand times speed-up compared to software implementations.

All prior Application-Specific Integrated Circuit (ASIC) FHE accelerators works propose to put every component needed for FHE onto one chip (monolithic). In [AMK$^+$], Aikata et al. take a different route and present the first-of-its-kind multi-chiplet-based FHE accelerator 'REED'. Chiplets are considered pivotal in future directions in semiconductor technology as they improve yield, scalability and reduce manufacturing costs. Their work achieves around three thousand times speed-up compared to a CPU (24-core 2×Intel X5690).

FHE for hardware: After studying hardware acceleration works, we see that they start with the mathematical representation of a given homomorphic encryption scheme and make hardware-based building blocks to speed up these algorithms in the scheme. Contrasting the typical hardware accelerator development cycle, we take the opposite direction design a Module-LWE based 'modular' HE scheme that offers hardware reusability as well as a stronger security assumption [MAM$^+$].

Beyond theoretical security: While FHE offers resistance from data breaches in outsourced computations, it suffers from substantial computational and communication overheads. The Hybrid Homomorphic Encryption (HHE) protocol was developed to mitigate these issues. Aikata et al. [ADSR] introduce a novel fault attack which is the first generalized analysis of HHE under Differential Fault Analysis (DFA) without requiring any strong assumptions like nonce reuse. They present a complete key recovery procedure by introducing only a single fault in not only for the standard scheme like AES but also for the new HHE-tailored Symmetric Encryption (SE) schemes.

[1] CryptEng: `https://www.iaik.tugraz.at/research-area/securesystems/`

References

[ADSR] Aikata Aikata, Ahaan Dabholkar, Dhiman Saha, and Sujoy Sinha Roy. SASTA: Ambushing hybrid homomorphic encryption schemes with a single fault. `https://eprint.iacr.org/2024/041`.

[AMK+] Aikata Aikata, Ahmet Can Mert, Sunmin Kwon, Maxim Deryabin, and Sujoy Sinha Roy. REED: Chiplet-based accelerator for fully homomorphic encryption. `https://eprint.iacr.org/2023/1190`.

[KMM+24] Andrey Kim, Ahmet Can Mert, Anisha Mukherjee, Aikata Aikata, Maxim Deryabin, Sunmin Kwon, HyungChul Kang, and Sujoy Sinha Roy. Exploring the advantages and challenges of fermat NTT in FHE acceleration. CRYPTO, 2024. `https://eprint.iacr.org/2024/314`.

[MAM+] Anisha Mukherjee, Aikata, Ahmet Can Mert, Yongwoo Lee, Sunmin Kwon, Maxim Deryabin, and Sujoy Sinha Roy. Modhe: Modular homomorphic encryption using module lattices potentials and limitations. *TCHES*, 2024(1). `https://eprint.iacr.org/2023/895`.

Biography

Anisha Mukherjee obtained her bachelor's and master's degree in Mathematics from Delhi University, India. She is currently a PhD student under Prof. Sujoy Sinha Roy at Institute for Applied Information Processing and Communications, Graz University of Technology, Austria. Her research interests include design and analysis of homomorphic encryption schemes and isogeny-based post-quantum cryptography.