Challenges in Hardware Implementations of FHE Algorithms

Çetin Kaya Koç
cetinkoc@ucsb.edu
Iğdır University, NUAA, and UC Santa Barbara
https://koclab.net/koc.html

Encryption functions with additive and multiplicative homomorphisms are called Fully Homomorphic Encryption (FHE) functions and they allow us in principle to compute any function homomorphically. Applications are found in national security, finance, and healthcare, where privacy of great concern. Since the groundbreaking work of Craig Gentry [4], there have been several FHE algorithm proposals, however, their time and space requirements do not give way to acceptably efficient implementations in real-world scenarios. While the encryption, decryption and homomorphic operations are simple arithmetic operations in polynomial rings and fields, the sizes of operands are beyond the usual operand sizes that we have been used to in standard public-key cryptography.

Several functions with fully-homomorphic properties work with polynomial rings of the form $\mathbb{Z}_q[t]/(t^n+1)$. These rings are applied to the FHE algorithms such as, the CKKS and the RLWE BGV [3][1]. For the RLWE BGV, the moduli can take values in the intervals $q \in [2^{15}, 2^{500}]$ and $n \in [2^{10}, 2^{15}]$. The CKKS works with polynomial rings of the form $\mathbb{Z}[t]/\phi(t)_m$ for which the defining polynomial $\phi(t)_m$ is the m-th cyclotomic polynomial for $m \in \mathbb{Z}^+$ and a power of 2. It also works with a ring $\mathbb{Z}_p[t]/\phi(x)_m$.

For example, the polynomial operands (representing ciphertexts) used in the BGV algorithm [2] are supposed to have up to 16k terms, with each term up to 1k bits. About 1024-bit message is encrypted into two ciphertexts each of which requires 32 million bits. Design of hardware to accommodate keeping the public and private keys, and ciphertexts require memory and arithmetic-logic technologies beyond current practice of public-key cryptography. Several US, European, Chinese, and Japanese funding and research organizations have taken the challenge and working on practical FHE implementations. Unfortunately there has not been satisfactory results, since the problem has both algorithmic and technological challenges. This talk is an introduction to the operand types and sizes of FHE, and also arithmetic in large polynomials rings useful for implementing FHE.

References

[1] Z. Brakerski, S. Garg, and R. Tsabary. FHE-based bootstrapping of designated-prover NIZK. IACR ePrint Archive, 1168, 2020.

[2] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) Fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory*, 6(3), 2014.

[3] J. H. Cheon, A. Kim, M. Kim, and Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In T. Takagi and T. Peyrin, editors, *ASIACRYPT*, pages 409–437. Springer, LNCS Nr. 10624, 2017.

[4] C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.