Formidable Challenges in Hardware Implementations of Fully Homomorphic Encryption Functions for Applications in Machine Learning

Çetin Kaya Koç
University of California Santa Barbara
Santa Barbara, California
cetinkoc@ucsb.edu

ABSTRACT

The concept of homomorphic encryption was introduced almost exactly same time as the first public-key cryptographic algorithm RSA, which was multiplicatively homomorphic. Encryption functions with additive and multiplicative homomorphisms allow us (at least in principle) to compute any function homomorphically, and thus are highly desired. Such encryption functions have applications in healthcare, machine learning and national security. Since the work of Craig Gentry [1], there have been several fully homomorphic encryption proposals, however, their time and space requirements do not give way to acceptably efficient implementations in real-world scenarios. The challenge comes from the fact that, while the encryption, decryption and homomorphic operations are simple arithmetic operations (such as polynomial addition and multiplication), the sizes of operands are beyond the usual operand sizes we have been used to in the standard public-key cryptography. 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 one ciphertext that requires several million bits. In this talk, I will present some of formidable algorithmic and architectural challenges facing FHE implementors.

CCS Concepts/ACM Classifiers

• **Security and privacy~Management and querying of encrypted data** • Security and privacy~Public key encryption • **Theory of computation~Computational complexity and cryptography** • Information systems~Data encryption • Hardware~Hardware accelerators

Author Keywords

FHE, Leveled FHE, BGV, CKKS, key switching, modulus switching, linearization, scaling.

ASHES '20, November 13, 2020, Virtual Event, USA.

ACM ISBN 978-1-4503-8090-4/20/11.
https://doi.org/10.1145/3411504.3421208

BIOGRAPHY

Çetin Kaya Koç received the PhD degree in electrical & computer engineering from the University of California Santa Barbara in 1988. His research interests are in cryptographic hardware and embedded systems, algorithms and architectures for computer arithmetic and finite fields. He is the cofounder of the *Cryptographic Hardware and Embedded Systems Conference*, and the founding editor-in-chief of the *Journal of Cryptographic Engineering*. Koç is the co-author of the 4 books in cryptography, published by Springer. He was elected as an IEEE Fellow in 2007 for his contributions to cryptographic engineering.

REFERENCES

[1] C. Gentry. "A Fully Homomorphic Encryption Function." PhD Dissertation, Stanford University, 2009.

[2] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "(Leveled) Fully Homomorphic Encryption without Bootstrapping." ACM Trans. on Comp.Theory, Vol. 6, No. 3, 2014.