Hardware Accelerator for Secure Cloud Computing

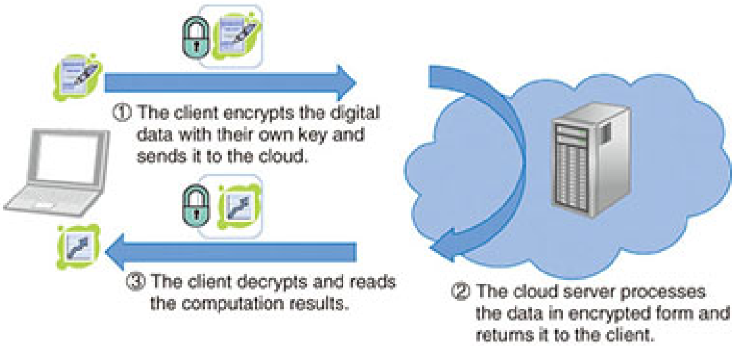
① The client encrypts the digital data with their own key and sends it to the cloud.
② The cloud server processes the data in encrypted form and returns it to the client.
③ The client decrypts and reads the computation results.

*Image Source: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html

Homomorphic encryption enables computation on encrypted data, opening a door to privacy-preserving cloud computing. When it is used, the cloud operators (datacenters) receive encrypted inputs but not the secret key to decrypt them. The computation takes place on the encrypted data, yielding an encrypted result. Only the users can decrypt the result with their secret key when they download it to their local computer. As a result, the cloud operator does not get any information about the sensitive data. Homomorphic encryption has numerous applications, e.g. in healthcare industry where data is protected by privacy laws.

Though this is conceptually amazing, the data is encrypted into large polynomials, and even simple operations require significant computing effort. As a result, general purpose computers are slow to execute them. On the other hand, hardware acceleration with a domain-specific architecture could offer many-fold acceleration in the cloud. In its recent call, DARPA announced 33M USD anticipated funding for accelerating Homomorphic Computation [1]. This thesis topic allows students to help design this accelerator, and work on securing data that is processed in the cloud domain.

We look for students motivated to design custom hardware for fast execution of homomorphic computations. The student could explore various algorithms which promise fast execution, optimising them for a chosen word-length. Furthermore, the student can investigate near-memory architectures, which could bring polynomial storage and homomorphic computation together. For this project, we specifically look for a student who has a VLSI background, and is interested in designing an ASIC.

[1] - `https://www.darpa.mil/news-events/2020-03-02`

Practicalities

Promoter:	Ingrid Verbauwhede		
Daily supervisor:	Furkan Turan	furkan.turan@esat.kuleuven.be	office 01.23
	Jose Maria Bermudo Mera	jose.bermudo@esat.kuleuven.be	office 01.19
	Michiel Van Beirendonck	michiel.vanbeirendonck@esat.kuleuven.be	office 01.16
	Angshuman Karmakar	angshuman.karmakar@esat.kuleuven.be	office 01.16
Nature of the work:	20% literature, 20% theoretical work, 60% implementation		
Number of students:	1 or 2		