Chair for Embedded Systems
Prof. Dr. J. Henkel

Bachelor/Master Thesis

Homomorphic Encryption Accelerator for Reconfigurable Systems

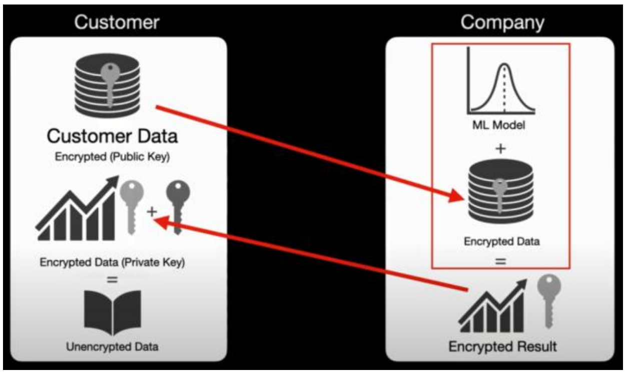

Image Source: https://www.youtube.com/watch?v=nlsd2LO-S50

With the ever growing popularity of cloud computing, the problem of trusting the Cloud Service Provider (CSP) with regards to the sensitive data has risen. Data could leak from CSP, get hacked or CSP might not be trusted.

Homomorphic Encryption (HE) is a revolutionary concept. It uses the homomorphism from algebra (hence the name homomorphic) as the encryption and decryption are mapping the data between plaintext and ciphertext spaces. Therefore, it allows untrusted third parties (e.g, CSP) to process data while being encrypted. Thus, the untrusted third party will not have access to the data unencrypted in any phase of the processing. Only the owner of the sensitive data with the secret key can access the result and decrypt it.

The main disadvantage of HE is its latency overhead. It can take several hundred milliseconds to complete a simple addition or multiplication. Therefore, they can significantly benefit from hardware acceleration.

Reconfigurable Systems such as FPGAs are very practical systems for using custom accelerators. One can prototype the accelerator, use it and change the accelerator type during runtime.

In this thesis we tackle the possibility of accelerating HE using FPGAs. We intend to build accelerators for processing homomorphic data. Either for the whole process or the bottlenecks of homomorphic processing.

Tasks of the student

Tasks will vary according to the thesis topic and scope (master or bachelor). Mainly hardware development will be performed. However, software development is also possible. Especially when working on the encryption or decryption part or the comparison between software/hardware performance.

Skills beneficial for the thesis

- Programming Skills (C, C++, Python)
- Knowledge of VHDL

Skills acquired with the Thesis

- Work in a research environment
- Hands-on experience in Hardware and Software development
- In depth knowledge of Hardware Security

Contact

- Hassan Nassar, M.Sc., hassan.nassar@kit.edu
  http://ces.itec.kit.edu/~nassar
- Dr.-Ing. Lars Bauer, lars.bauer@kit.edu
  http://ces.itec.kit.edu/~bauer