Investigation of ABE for HW/SW Codesign

Classical public-key cryptography is based on an all-or-nothing approach, i.e. if a user is in possession of a secret key, he can fully decrypt a ciphertext that is encrypted with a corresponding public key. However, it is not possible to decrypt only parts of data. Attribute-Based Encryption (ABE) [1], however, is a branch of Functional Encryption (FE) that allows for such fine grained access control. ABE systems include a trusted authority, which can distribute secret sub-keys. A user can thus authenticate itself towards the trusted authority to obtain a certain secret key. This key is then used to decrypt a corresponding subset of the data depending on the user's permissions.

PALISADE [2] is a library, that implements several Homomorphic Encryption (HE) schemes as well as an ABE scheme. In this work, your goal is to integrate such a scheme on a HW/SW Platform using PALISADE. The next step is then a detailed analysis of performance and cost metrics to estimate the requirements for constrained devices.


If you are interested in the work and want to get further details, please contact me via email, attach a CV and grading report.

Prerequisites

- C/C++ programming skills
- Ideally experience using microcontrollers or FPGAs

Contact

E-mail: patrick.karl@tum.de

Advisors

Patrick Karl