CRYPTOGRAPHIC PROCESSORS

Security in reconfigurability

IEEE J. Solid-State Circuits https://doi.org/10.1109/JSSC.2017.2776302 (2018)

The potential to intercept sensitive data from the Internet of Things (IoT), combined with the pervasiveness of the IoT, has stimulated efforts to improve the security of these highly networked devices. Cryptographic algorithms are typically employed to ensure secure communication through the use of authentication for trustworthiness, data encryption for confidentiality and integrity, and fault tolerance to defend against attacks. Implementing these algorithms using software, though simple, tends to be energy inefficient and slow. Application-specific integrated circuits are fast but limited to a single purpose. Alternatively, cryptographic coprocessors offer a level of flexibility but at the cost of a high area and power overhead.

Yiqun Zhang and colleagues at the University of Michigan, Ann Arbor have now developed a reconfigurable cryptographic processor, termed Recryptor, capable of running multiple cryptographic functions at the same time. They implement a custom-designed crypto-SRAM (static random access memory) bank that can operate normal memory and support in-memory and near-memory computing capable of large vector calculations for cryptographic algorithms. The Recryptor's versatility is demonstrated by running cryptographic primitives of various public/secret key cryptographies and hash functions. Moreover, the Recryptor operates with an average speedup of 6.8 times, and average energy improvements of 12.8 times, compared to the state-of-the-art software-accelerated and hardware-accelerated implementations.

Michael Lee

Published online: 9 March 2018
https://doi.org/10.1038/s41928-018-0049-5