Research Topics

Efficient Implementation of ECC

- Article: FourQ on Embedded Devices with Strong Countermeasures against Side-channel attacks, Preliminary version in *CHES 2017* and extended version in *IEEE Transactions on Dependable Computing and Secure Computing, 2018*
- Authors: Z Liu, P Longa, G Pereira, O Reparaz, and H Seo
- Comments: This paper presents an excellent ECC implementation on 8/16/32-bit microcontrollers (MCUs): the first implementations of FourQ-based scalar multiplication and ECDH key exchange and ECDSA on 8, 16, and 32-bit microcontrollers (MCUs), and demonstrate that this curve can deliver the fastest curve-based computations on embedded IoT devices, potentially helping to achieve stringent design goals in terms of response time and energy

Efficient Implementation of PQCrypto

- Article: Efficient Ring-LWE Encryption on 8-bit AVR processors. *CHES 2015*
- Authors: Zhe Liu, Hwajeong Seo, Sujoy Sinha Roy, Johann Grossschädl, Howon Kim, Ingrid Verbauwhede
- Comments: This paper presents an excellent Ring-LWE implementation on resource constraint 8/16/32-bit IoT devices: For the first time, this paper several novel optimizations for speeding up the execution time and reducing the memory consumption of Ring-LWE encryption for 8/16/32-bit processors. The results presented in CHES2015 and IEEE TC set new speed records for ring-LWE encryption on an 8/16/32-bit processor and outperform related RSA and ECC implementations by an order of magnitude.