Theme: Hardware Security

- Sub Theme: Enhanced Chip Security by Blockchain

Blockchain is a decentralized public ledger that provides a way for information to be recorded and shared. Blockchain-powered transaction has shown a new paradigm of trust building mechanism without third-party intermediaries. All participants in blockchain can quickly prove authorship of information by exploiting advanced cryptography with public/private keys. However, in spite of advantage of blockchain trust, as the connections of small internet of things (IoT) devices increase, the entry points for hackers also increase and hackers can penetrate through a weak leaf node in blockchain. Therefore, we have to address an issue on security vulnerabilities of small IoT devices as a leaf node.

We are aiming to find a feasibility proof of new schemes to enhance the embedded hardware security by applying blockchain technology to IoT infrastructure. Through innovative ideas, we would like to achieve the secured data transaction with resilience to malicious attacks, while satisfying a limitation of hardware complexity and transaction latency.

- Runnable on an ultra-low power processor for a leaf node (< 1 uW/MHz)
- New hardware wallet architect robust to a transaction validation delay
- New cryptography algorithm incorporated with blockchain and embedded hardware security considering IoT layered architecture

※ The topics are not limited to the above examples and the participants are encouraged to propose original idea.

※ Funding : Up to USD $150,000 per year