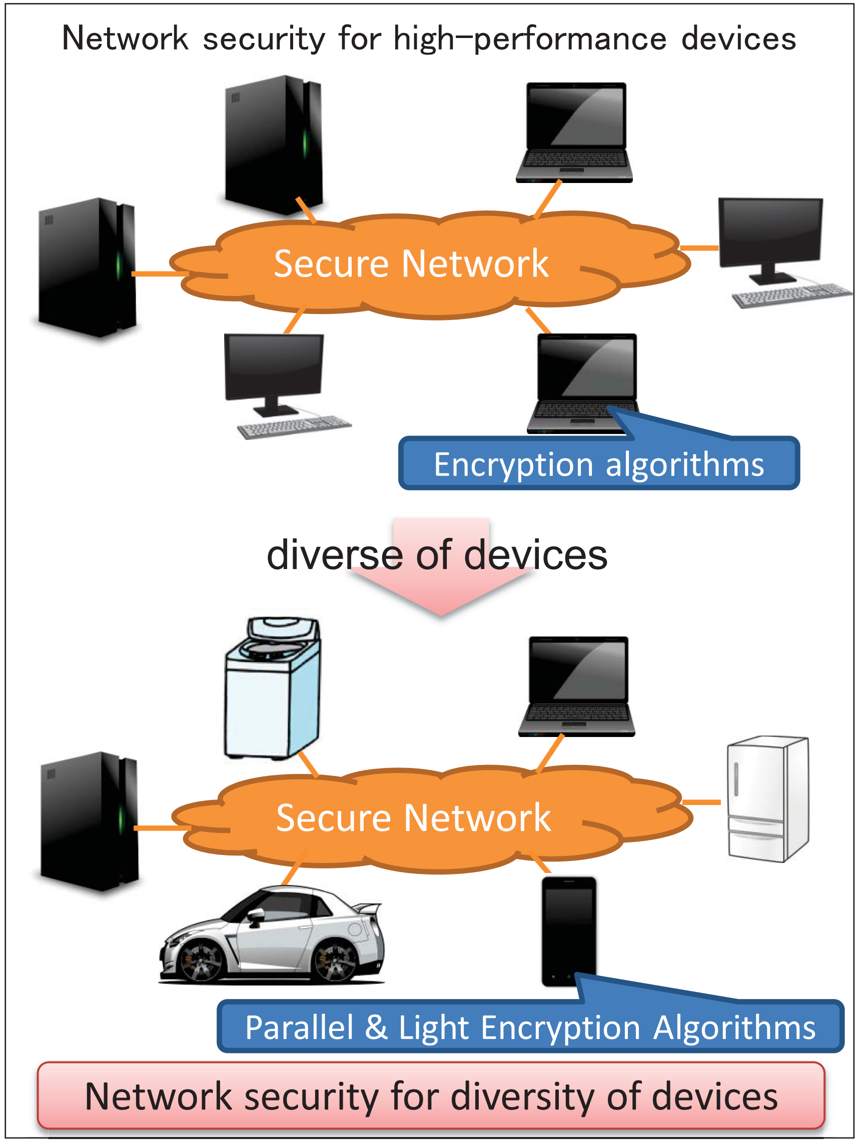
Faculty of Engineering
Tokushima University

Cryptography for Parallelized & Low-performance Devices

Associate Professor Akinori Kawachi


Network security for high-performance devices
Secure Network
Encryption algorithms
diverse of devices
Secure Network
Parallel & Light Encryption Algorithms
Network security for diversity of devices

The information communication technology, which gave deep impacts to modern society, such as the Internet is entering a new phase. Most of devices in networks were supposed as devices which have high performance with sufficient memory. Nowadays, devices in networks are being diversified, and a lot of lower-performance devices such as smartphones, home electrical appliances, etc., are connected with the networks. Moreover, even such small devices utilize multi-core processors inside them.

It is inevitable for the next-generation network technology to develop cryptographic systems that are available for low-performance devices and suitable for multi-core processors.

In this research project, we aim at constructing new fundamental cryptographic systems, such as public-key encryptions, digital signature schemes, and interactive identification schemes, that enable us to perform basic operations (e.g., encryption) with much less memory and parallelize the operations easily. For the constructions, we mathematically analyze security of the systems by techniques of mathematical sciences. We also aim at revealing theoretical limitations in term of possibility and performance of the constructions.

Keywords: Cryptography, Parallelization, Light-weight

E-mail: kawachi@is.tokushima-u.ac.jp
Tel. +81-88-656-9446>
HP : https://sites.google.com/site/akinorikawachi