Prof.	Kanta Matsuura	Campus	Komaba (IIS)	Field	Information Security

Comprehensive Information Security

——Crypto, Network, and Management——

【 General Description 】 Our research purpose is to contribute to the quality of life by enhancing information security. We study all the three areas of security: cryptography, network security, and security management.

【Research】 Our philosophy is based on cryptography and its rigorous approach for evaluation. In addition to cryptography, our activities include pioneering efforts in the following topics. In recent years, fundamental cryptology and security management (e.g. security economics) made remarkable progresses.

1. Cryptography and Network Security

Both in theory and practice, correct sense of security evaluation is the first. All of our members are recommended to first study the correct sense from the theory of cryptography, and then start one's own particular research topics.

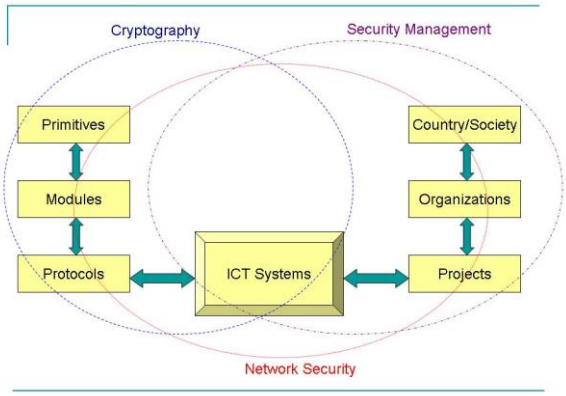
We emphasize an approach called provable security which realizes mathematical proofs of security. Based on this approach, we solve real-world problems rigorously by functional encryptions (e.g. Resplittable threshold encryption). **This is a field where we can create new applications by deep theories.**

In network security, we face a wide variety of threats such as Denial-of-Service, malware, and malicious use of anonymous communication tools. We study countermeasures against them and recorded several world-class performances. **This is a field where we can experience world-class actual competitions.**

2. Security Management

Financial issues are important factors in dispute settlement related to information security. Many systems fail not for technical reasons so much as from misplaced economic incentives. Digital-evidence technologies such as blockchain can make big impacts on the society (e.g. by cryptocurrencies). Motivated by these observations, we are pioneering security economics, psychology, and their related technologies.

For example, we provided the most advanced empirical analysis of security investment. The financial theory we proposed in 2001 provides an abstracted token model of cryptocurrencies. Many cryptocurrencies are based on blockchain, and before the launch of Bitcoin in 2009, we published pioneering papers on key ideas deployed by blockchain (e.g. Proof-of-Work for security in 1998, completely digital timestamp in 2003). **This is a field where we can pioneer new paradigms.**



Laboratory (E-block of IIS, 4th floor, Room Ew-401): (ext.: 56286)
Prof. Office (Room Ee-403):
kanta@iis.u-tokyo.ac.jp (ext.: 56284)