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. Our former members are active not only in engineering field but also business and consulting communities.

1. Cryptography and Network Security

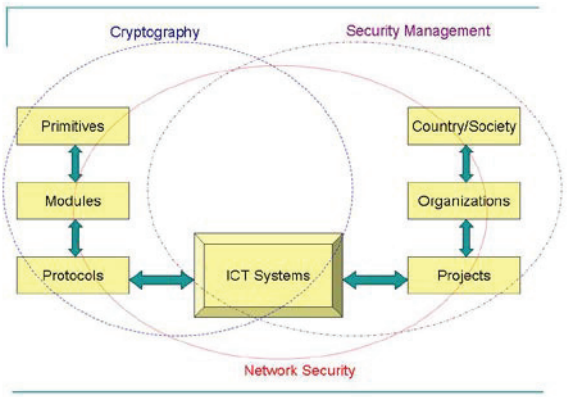
Both in theory and practice, correct sense of security evaluation is the first. All of our members first study the correct sense from the theory of cryptography, and then start one's own particular research topics.

Therefore, each member can introduce our most theoretical framework to visitors: relations among security notions (the proof of the equivalence between the notion "the security property P holds against the attack model Q under the assumption R" and the notion "the security property S holds against the attack model T under the assumption U"), for example. Based on this approach called provable-security, 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 DoS (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 competitions.

2. Security Management

Financial issues are important factors in dispute settlement related to information security. Also, many systems fail not for technical reasons so much as from misplaced economic incentives. Motivated by these observations, we are pioneering security economics and psychology. For example, we provided the most advanced empirical analyses of the effects of information-security investment. The financial theory we proposed in 2001 provides an abstracted model of virtual currencies such as Bitcoin. We also study a wider range of virtual currencies such as loyalty programs. This is a field where we can pioneer new research areas.



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)