R&D Project Title: Target-Adaptive Security Infrastructure

Principal Investigator：Takanori Isobe（Professor, Graduate School of Information Science and Technology, The University of Osaka）
Co-PI：Rei Ueno (Kyoto University)

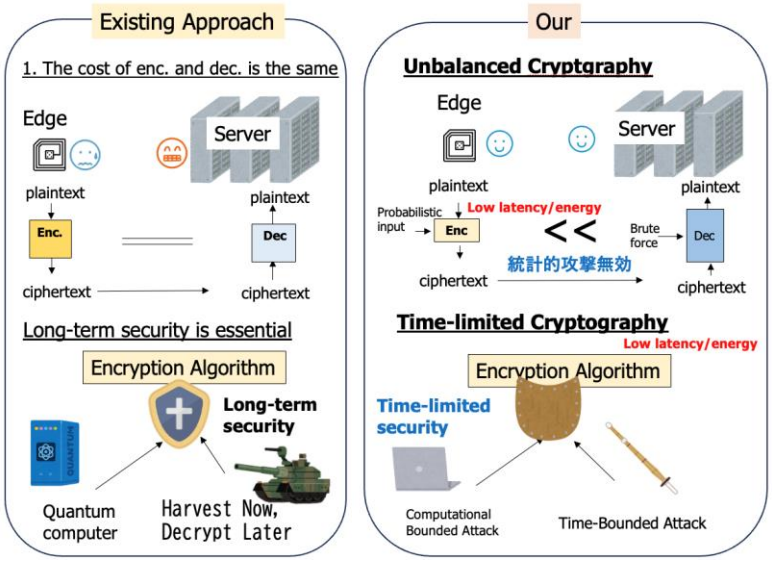
Grand Challenge and Goal：By designing cryptographic functions that can adapt performance and security levels according to the target, we aim to achieve significant cost reductions and create a world where encryption incurs virtually no cost, thereby enabling a next-generation server and network infrastructure in which all communications are fully secure

Summary：

Breaking the conventional principle of cryptographic design to achieve overwhelming cost reduction

1. The cost of encryption and decryption is the same regardless of device
   → Develop “Unbalanced Cryptography,” where encryption and decryption costs are made asymmetric according to available hardware resources
2. Long-term security is essential
   → Construct the theory of “Time-Limited Cryptography,” which adapts to the required level of security

✓ Pioneering a novel methodology for cryptographic design
✓ Achieving more than 10x cost reduction compared to existing technologies, making cryptographic costs virtually negligible



Social Impact：

- Cut computation costs, reducing cryptographic power use and delay to near zero
- Secure large-scale IoT in the Beyond 5G/6G era with ultra-low latency and power
- Lower risks in mission-critical fields like healthcare, transport, and space
- Boost industrial competitiveness and economic security via global standards