研究開発課題名：ターゲット適応型セキュリティ基盤の実現
研究開発代表者：五十部　孝典　（大阪大学・大学院情報科学研究科・教授）
主たる共同研究者：上野　嶺（京都大学）

グランドチャレンジへの挑戦・研究開発課題での達成目標：

処理負荷と強度をターゲットに応じて適応可能な暗号により圧倒的低コスト化を実現し、あらゆる情報を負担なく守る暗号コストフリー社会を構築することで、すべての通信がセキュアな次世代サーバーインフラを実現する

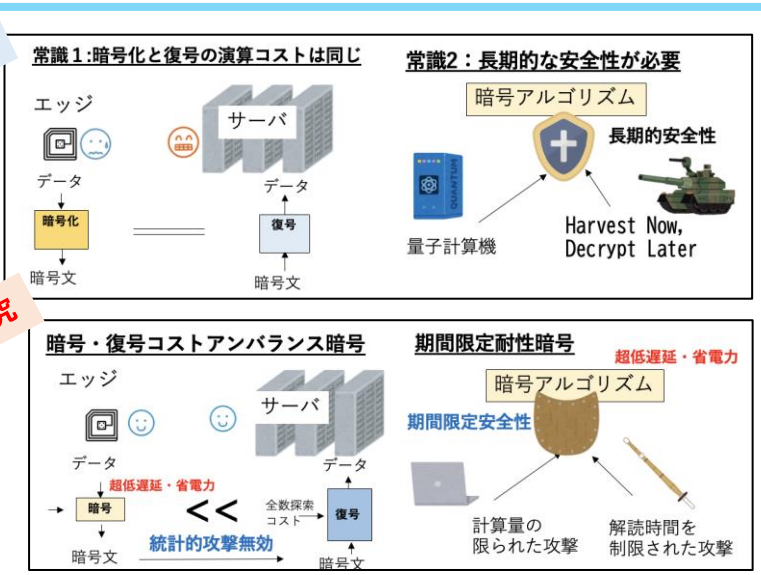
研究概要：

暗号設計の常識を破り、圧倒的な演算の低コスト化を実現する

- **常識 1：暗号化と復号のコストはデバイスの性能に依らず同じ**
  →暗号化と復号の演算コストをハードウェアリソース応じて非対称にする「アンバランス暗号」の開発
- **常識 2：長期的安全性が必須**
  →求められる安全性に応じた「期間限定暗号」の理論構築

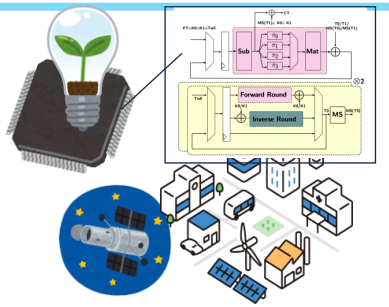
独創性・優位性：

✓ 暗号の常識を打破した、革新的暗号設計の手法を開拓
✓ 既存技術の10倍以上の低コスト化を実現し、暗号コストをフリーへ



想定する社会的インパクト：

- 計算コストを1/10以下に削減し、暗号による消費電力や通信遅延をほぼゼロに
- 超低遅延・超低消費電力により、Beyond 5G/6G時代の大規模IoTを安全に
- 医療・交通・宇宙などミッションクリティカル分野におけるセキュリティリスクを低減
- 国産暗号IPの国際標準化とOSS公開を通じて、産業競争力および経済安全保障を強化



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）

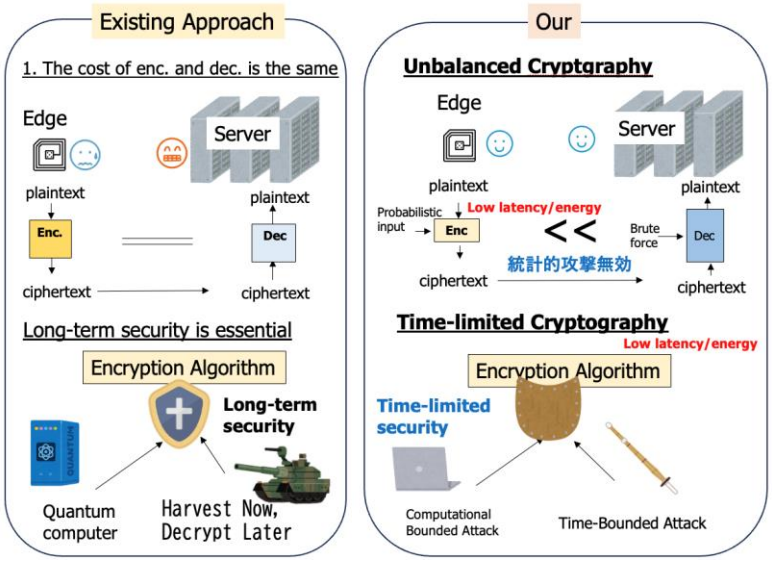
Grand Challenge and Goal：By designing cryptographic functions that can adapt performance and security levels according to the target, we aim to achieve significant cost reductions and create a world where encryption incurs virtually no cost, thereby enabling a next-generation server and network infrastructure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