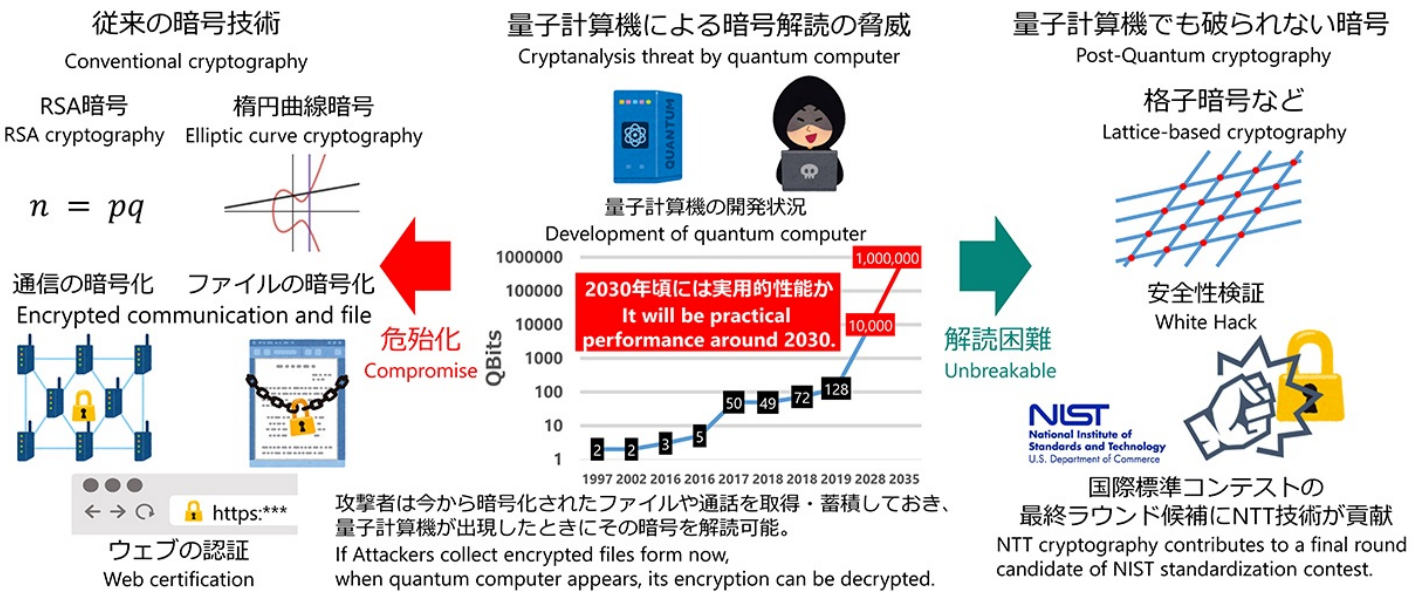
S05 NTT耐量子計算機暗号

量子計算機でも破ることができないNTT次世代暗号です

概　要

膨大な情報を超高速に処理できる量子計算機の実現が近づいています。それにより、量子計算機によって、現在利用されている一部の暗号技術は危殆化します。NTTでは量子計算機でも破ることが不可能な暗号技術の研究・開発を実施し、高い安全性と効率性をみたす耐量子計算機暗号の実用化をめざします。



出展社

日本電信電話株式会社

特　徴

- 国際標準化コンテストの最終選考に残っている公開鍵暗号基本技術の開発
- 大学との共同研究による厳密な安全性検証と高速化検討を通じたバランスのよい暗号方式

利用シーン

- 長期的な機密性が必要な通信の保護のために、既存暗号を耐量子計算機暗号への置換え
- 量子計算機の実現によって脅威となる従来の認証システムに対するマイグレーション

今後の展開

- 国際標準採択へ向けNTT耐量子計算機暗号技術のさらなる安全性と効率化を研究します。また、既存のNTT暗号サービスを量子計算機でも破れないような開発を実施します。

コラボレーションパートナー

- さまざまな組織と共同でコンテストに参加し、安全性検証などを大学と実施しています。

問い合わせ先：
rdforum-sv-ml@hco.ntt.co.jp