情報セキュリティ分野における

量子技術

日本銀行金融研究所
情報技術研究センター
田村裕子

量子技術とは

- 「二重性」、「重ね合わせ」、「量子もつれ」といった量子の性質を積極的に操作・制御し、活用するもの。量子の性質を工学的に実装できるようになったことで、量子コンピューター、量子通信や量子センサなど、これまでになかった先端的な技術が登場

（引用）文部科学省、「一家に1枚　量子技術」

代表例は量子コンピュータ

- これまでの計算機では解くことが難しかった(計算に膨大な時間がかかる)問題のうち、量子コンピュータであれば現実的な時間で解けるものがある
- 量子コンピュータによる計算手順＝量子アルゴリズム

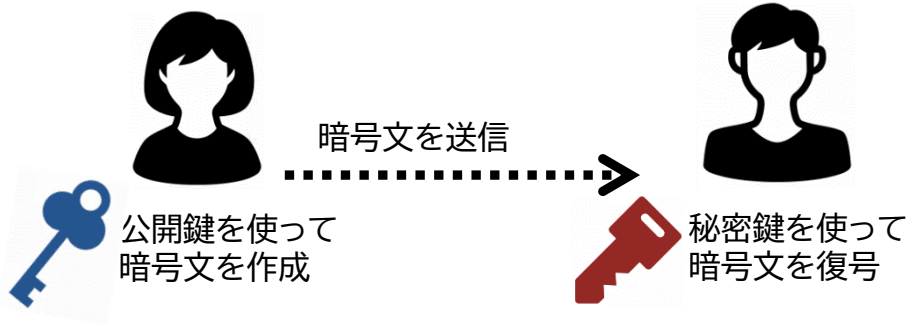
  ✓ Shorのアルゴリズム　＝素因数分解問題と離散対数問題を効率的に解く
  ✓ Groverのアルゴリズム
  ✓ Dutsch-Jozsaのアルゴリズム
  ✓ Simonのアルゴリズム
  ✓ ・・・

現在広く利用されている
公開鍵暗号系の安全性が低下

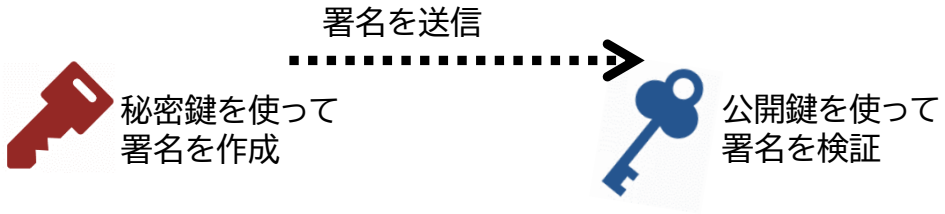
（参考） 國廣昇、「量子コンピュータによる暗号解読アルゴリズム：隠れ部分群問題から見た素因数分解問題と離散対数問題」、DPS2026-J-1

公開鍵暗号系の主な用途

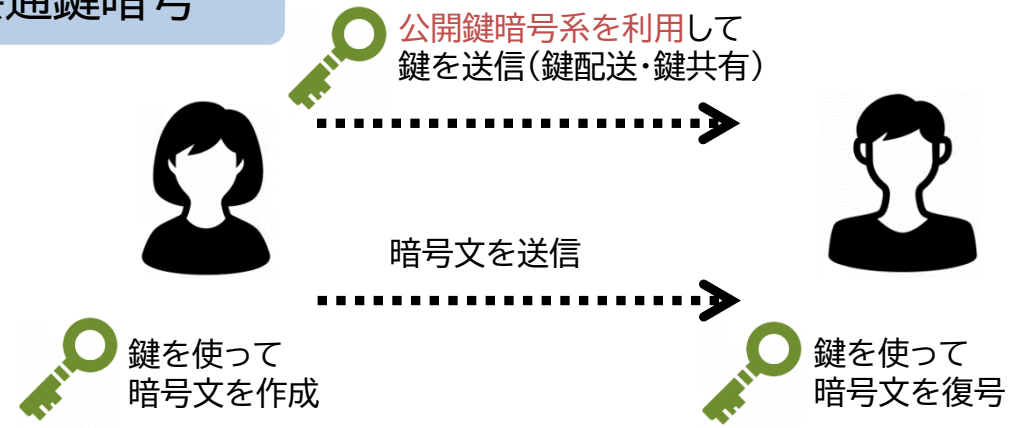
公開鍵暗号



デジタル署名



共通鍵暗号



量子コンピュータに耐性をもつ暗号方式

① 量子鍵配送 （QKD: Quantum Key Distribution）

- 量子力学の原理を利用した通信チャネル（量子通信路）を形成して鍵の配送を行う方式
- 量子通信路の利用が前提

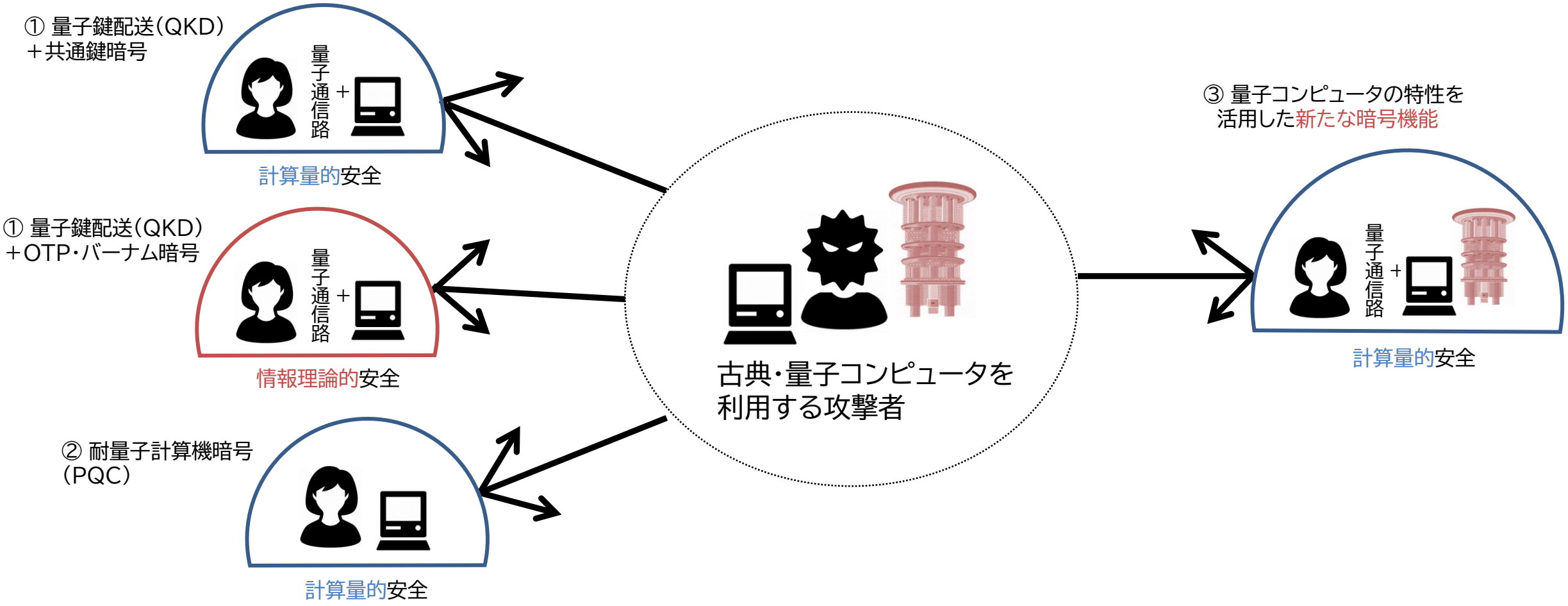
② 耐量子計算機暗号 （PQC: Post-Quantum Cryptography）

- 量子コンピュータであっても計算が難しい問題に安全性の根拠を置く暗号方式
- 古典コンピュータの利用が前提

- 超特異楕円曲線同種写像問題
- 多変数二次連立方程式問題
- 最短ベクトル問題

- 誤り訂正符号に基づくランダムな線形符号の復号問題

量子コンピュータに耐性をもつ暗号方式



本日のプログラム

① 量子コンピュータの仕組みと開発動向
② 超長期秘匿性実現を目指して：量子鍵配送・量子セキュアクラウド
③ 金融分野における耐量子計算機暗号への移行・・・パネルディスカッション
④ 量子コンピュータの特性を活用した新たな暗号機能