# 暗号基礎技術

ネットワーク上を流れる通信データやその上で実現される各種サービスの安全性を担保するためのセキュリティ技術として、次世代の安心・安全な暗号基礎技術の研究開発を進めています。特に、次世代の共通鍵暗号アルゴリズムの設計と解析、次世代の公開鍵系暗号技術の研究、耐量子安全性を有する暗号技術の研究などを進めています。

現在のインターネット上では、プライバシ情報やクレジットカード番号等の機密性の高い情報が多くやり取りされています。通信内容を秘匿するために共通鍵暗号や公開鍵暗号が使われていますが、大規模かつ安定して計算が行えるような量子コンピュータが完成すると、現在広く用いられている暗号アルゴリズムは安全でなくなります。そのため、量子コンピュータを用いても解読や偽造ができないような耐量子計算機暗号技術の研究・開発が必要となります。

NTTは、量子コンピュータが苦手とすると考えられている問題を基に、メッセージを秘匿するだけでなく、メッセージの改ざんを防止する等のより強い安全性（CCA安全性*1）を持つ耐量子公開鍵暗号を実現する手法を開発しました。この手法は汎用性が高く、さまざまな既存方式に対しても適用可能で、世界最高水準の耐量子公開鍵暗号方式を高効率に構成できます。この技術に基づく耐量子公開鍵暗号を用いることで、量子コンピュータ実現後の時代においても、既存方法と同程度の負荷で暗号通信が可能になります。

*1 CCA安全性：Chosen Ciphertext Attack（選択的暗号文攻撃)安全性

**●耐量子計算機暗号技術**