

# W4 無線・通信

## Beyond 5G無線通信プロトコルにおけるセキュリティ評価

### 概要

Beyond 5Gでの超高速・大容量化へ対応し、かつ量子計算機でも破られないような、高速かつ強固な暗号技術・セキュリティ技術の開発が求められています。ATRでは、Beyond 5G時代に対応した暗号・セキュリティ技術無線通信プロトコルに適用した際の評価を実施しています。

### 特徴

- 量子計算機を使っても解読できない暗号技術をBeyond 5Gの無線プロトコルに導入した場合の、性能と安全性を評価するシステムを開発しています。
- 評価を通じて、性能面・セキュリティ面での課題を整理し、Beyond 5G時代に求められる暗号・セキュリティ技術を検討・提案します。
- 現在広く利用されている暗号アルゴリズムAES(Advanced Encryption Standard)で、量子計算機でも解読が困難なセキュリティレベル(鍵長256ビット)に上げると、通信性能(スループット・レイテンシ)への影響は限定的であることを確認しました。

### 今後の展開

- Beyond 5G無線通信プロトコルのセキュリティ評価を通して、安心・安全な移動通信インフラの実現に貢献します。

### テーマ「ともに究め、明日の社会を拓く」との関連

- 産・学の研究機関と連携し、安心・安全な次世代移動通信インフラの実現に貢献します。

### Beyond 5Gセキュリティ評価システム



5G-RANを模擬した環境



新たな暗号・セキュリティ技術を実装



通信性能・安全性を評価・検証

### 通信性能の評価結果

