応用研究

W2　無線・通信

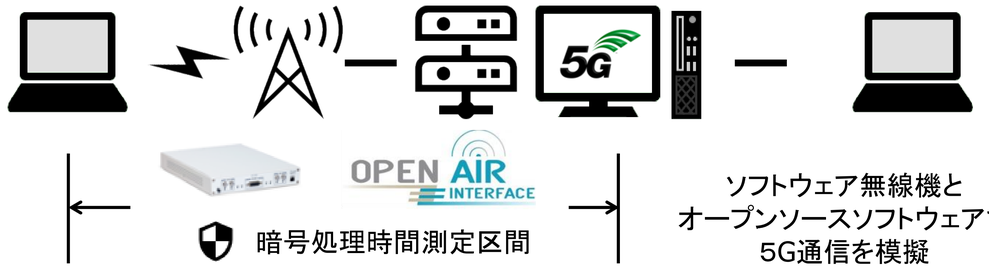
Beyond 5G無線通信プロトコルにおけるセキュリティ評価

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・セキュリティ技術を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）よりも強固で量子計算機でも解読が困難な、鍵長256ビットの認証暗号方式Rocca-Sを5Gの通信プロトコルに実装しました。
- 鍵長128ビットのAESに比べて、Rocca-Sは、暗号処理に要する時間を60%以上削減できることを実証しました。



暗号アルゴリズム	AES-128	AES-256	Rocca-S
暗号処理時間（平均、マイクロ秒）	2.381	2.642	0.870

1.511[us]（63%）減少

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「万博、そしてその先へ ～科学技術が描く未来～」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。

9 産業と技術革新の基盤をつくろう

連絡先：適応コミュニケーション研究所　担当　横山浩之　E-Mail：hr-yokoyama@atr.jp

本研究は、総務省 電波資源拡大のための研究開発「安全な無線通信サービスのための新世代暗号技術に関する研究開発」(JPJ000254) により実施しています。