報道関係各位

ものづくり　ひとづくり　未来づくり
国立大学法人
名古屋工業大学

電波を暗号化する、より安全で高品質な無線通信方式を開発
世界初！暗号化機能を損ねないまま伝送誤り率を 100 分の 1 以下に

名古屋工業大学 情報工学専攻　岡本英二准教授らが、カオス信号を用いて無線電波を暗号化し、同時に伝送ビット誤りが大幅に減少する安全・高品質な通信方式を開発しました。

無線電波を暗号化する手法の一つとしてこれまでカオス通信（注1）というものが提案されていましたが、安全性は向上するものの伝送ビット誤りが 2 倍以上に増加し、通信品質が低下してしまうことが問題でした。岡本准教授らのグループはターボ符号化（注2）という手法をカオス通信に適用することで，世界で初めて暗号化機能を損ねないまま伝送ビット誤り率をこれまでの 1/100 以下にすることに成功しました。スマートフォンや車両無線など様々な無線通信に適用されることが期待されます。

無線通信はコンテンツの大容量化により常に高速化が求められています。2020 年に実用化開始が計画されている第 5 世代移動通信システム（5G）では、これまでの 1000 倍の高速化が必要とされております。5G ではスマートフォンだけでなく、自販機、IT 機器、医療機器、自動車などのモノからモノ（M2M – Machine to Machine）への通信も収容することが検討されています。このときに必要なことは無線が高品質で安全であることです。現在でもスマートフォンを用いたオンライン決済や位置情報の活用のように無線での重要情報の伝送は増加しており、更なる安全性確保が求められています。しかし現在の通信秘匿は図1 に示すように上位層プロトコルによってなされており、伝送信号そのものは秘匿されない状態でした。このような背景においては物理層、つまり電波からの秘匿性確保を行うことも必要であると考えられておりました。

アプリケーション層	SSLに基づくサービス，パスワード	現在の方式
セッション層	SSL（公開鍵暗号方式）	
ネットワーク層	IDに基づく共通鍵生成，IPsec	
物理層	0,1の復号不能，同期不能	

図１　現在の通信プロトコルにおける秘匿性の確保

今回開発したカオスを用いたターボ符号化電波暗号化通信方式は、物理層の暗号化を実現するだけでなく、一般的な無線通信方式に比べて 1/100 以下のビット誤り率を達成しました。本手法の暗号化は 1024bit RSA 暗号以上の計算量的安全性を持っているため、安全・高品質化を両立させた方式を実現しました。物理層において安全性と高品質化を両立した方式はこれまでに無かったものです。

本手法を上位層暗号化と併用することでスマートフォンの更なる安全性を確保でき、高品質化によって省電力化が図れるため電池の待ち受け時間長期化にも寄与します。一方で、上位層の暗号化方式は信号処理に時間がかかるため低遅延伝送への適用は不向きですが、開発した手法を用いることで上位層の暗号化を省略することも可能であり、即時性が必要な自動運転の制御無線などへの応用が期待されます。本成果は 8 月の電子情報通信学会英文論文誌 5G 小特集号に掲載されます。

（注1 ）カオス通信

カオス信号は決定論的な非線形の規則にしたがって、予測不可能・不規則な振る舞いをする信号のことである．この信号を通信信号に加算や乗算することで，カオスの初期値を知らない受信者は正常に復号ができなくなるため，秘匿性が保持される．共通鍵暗号システムの一種として用いられる．

（注２ ）ターボ符号

ターボ符号は誤り訂正符号の一つで，強力な誤り訂正能力を持つ．無線通信では受信信号に雑音が重畳されることから，ビット誤りが生じて通信品質が低下してしまう．そこで送信側で予め情報ビットに加えて，符号化規則に則った冗長ビット（パリティビット）を付加して送信し，受信側で受信情報ビットとパリティビットを符号化規則に対応する復号化規則に則り演算することで，雑音によって生じたビット誤りを訂正することができる．この受信側の演算を繰り返すことで誤り訂正能力を向上させる符号化方式がターボ符号である．

本件へのお問い合わせ　国立大学法人名古屋工業大学 大学院工学研究科情報工学専攻
TEL：052-735-5452　090-3456-2661　mail:okamoto@nitech.ac.jp　担当：岡本英二