安全保障技術研究推進制度　令和４年度終了課題　終了評価結果

1. 評価対象研究課題

（１）研究課題名：量子雑音ランダム化ストリーム暗号の安全性向上に関する基礎研究

（２）研究代表者：学校法人玉川学園 玉川大学　二見 史生

（３）研究期間　：令和２年度～令和４年度

2. 終了評価の実施概要

日時　　：令和５年１１月９日

場所　　：TKP 秋葉原カンファレンスセンター

評価委員：未来工学研究所　理事長、上席研究員／東京大学　名誉教授
平澤　泠（委員長）

元 三菱ケミカルホールディングス 顧問
岩野 和生

理化学研究所　革新知能統合研究センター　副センター長
上田 修功

情報セキュリティ大学院大学　情報セキュリティ研究科長・教授
大久保 隆夫

玉川大学　脳科学研究所　特別研究員
大森 隆司

兵庫県立大学　大学院情報科学研究科　教授
田中 俊昭

千葉商科大学　総合教育センター長、
東工大　名誉教授、筑波大　名誉教授
寺野 隆雄

産業技術総合研究所　人間拡張研究センター・主任研究員
長谷川 良平

（委員長以外は五十音順・敬称略）

3. 研究と成果の概要

研究の概要

本研究では、共通鍵を用いた光ファイバ暗号通信システムの安全性向上を目的として、量子雑音を発生源とする予測不可能性の高い乱数で駆動されるランダム化拡張技術及びそのランダム性を暗号に組み込み安全性向上を図る技術を開発し、これらの技術を適用した光ファイバ暗号通信システムの通信特性及び安全性を評価した。

成果の概要

量子雑音の揺らぎに基づく予測不可能性の高い乱数で高速発生可能な手法を考案、発生速度 100Gb/s（オフライン信号処理方式）で量子雑音を発生源とする乱数発生に成功し、本乱数で駆動するランダム化拡張技術である量子雑音駆動型 DSR※(Deliberate Signal Randomization)を実現した（80%以上の暗号信号拡散率)。

また、これを組み込んだ新たな量子雑音ランダム化ストリーム暗号の光ファイバ伝送実験を行い、次の暗号通信に成功した。

・伝送路の途中で光増幅器を利用しない無中継光ファイバ暗号通信システム（通信容量 10Gb/s、距離 362km、ビット誤り率 1%未満）
・屋外敷設光ファイバ回線と光増幅器で構成される光増幅中継光ファイバ暗号通信システム（通信容量 10Gb/s、距離 400km）

これらの通信システムの安全性評価として、本研究で安全性向上理論の裏付けした指標（マスキング数、盗聴者のシンボル誤り率）を用いて、送信機から受信機までの間のいずれのポイントにおいても、光信号パワーに依存せずに、桁違いに安全性を高められたことを明らかにした。

加えて、乱数発生技術においては、50Gb/s という高速（論文発表時、量子雑音揺らぎに基づく乱数発生手法の中で世界最速）でリアルタイムに乱数を発生する乱数発生技術を開発した。

さらに、安全性向上の理論検討については、量子雑音ランダム化ストリーム暗号の安全性解析に向けたアプローチと基本諸原理について整理し、量子信号検出理論に基づいた盗聴者能力を推定するため諸量を位相変調の場合で計算し、暗号通信システム評価実験で得られた結果について、より理論的な視点から安全性が向上していることを裏付けた。

※量子雑音駆動型 DSR とは、既存の DSR と異なり、量子雑音に基づくランダム性を強制的に暗号信号に取り込み暗号信号のランダム性を増強する技術の総称で、ディジタル的な実現手法やアナログ的処理を用いて実現する手法がある。

4. 終了評価の評点

S　特筆すべき研究成果をあげた。

5. 総合コメント

タイプ C に相応しい、新規なアイディアによる発想の転換により新たな局面を開いた。基礎から理論を組み立て評価手法まで構築したユニークな研究であり、方式の独創性、創出された成果は極めて顕著といえる。

新しい方式であるため、従来の方式に対する優位性は今後実証する必要があるが、応用次第で発展の可能性が十分にあり、将来性の高い研究である。

情報セキュリティ分野に限らず、様々な産業分野における量子雑音ランダム化ストリーム暗号の社会実装と普及に向けた、今後のさらなる活躍を期待する。

6. 主な個別コメント

- 当初の目標に加え、世界最速の乱数発生手法の開発や、敷設光ファイバー回線を用いた光増幅中継暗号光ファイバー通信システム実験の成功など、目標以上の成果を創出している。
- 自ら基礎理論を作って評価するなど、実用性と理論性を兼ねたユニークな研究である。実用化と普及を期待する。
- 本研究の方式はユニークであり、その考え方の普及が発展性に影響するであろう。
- 特定分野での大規模な実証にはまだまだ時間がかかると思うが、量子暗号発生装置だけでも単体で実用化すればすぐにでも多分野からの引き合いがあると期待できる。
- 新しい暗号方式であるため、安全性の評価のために独自の評価指標で評価しているが、従来方式に対する優位性を主張するには、既存の評価指標での比較（攻撃に対する安全性など）も必要。応用次第では、発展の可能性が十分にある。
- 論文や学会発表の数量も多く、その有用性は国際的にも評価されている。
- これからまだまだ発展の余地がある。インパクトファクターの高い雑誌に載り得るような研究であり、頑張ってもらいたい。
- コンパクトな体制で大きな成果を挙げた。