別紙２

令和４年度　防衛装備庁
安全保障技術研究推進制度

研究成果報告書
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

令和５年５月

学校法人玉川学園

本報告書は、防衛装備庁の安全保障技術研究推進制度による委託業務として、学校法人玉川学園が実施した令和４年度「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」の成果を取りまとめたものです。

１．委託業務の目的

１．１　研究課題の最終目標

本委託業務では、共通鍵暗号方式の物理暗号通信システムの安全性向上を目的として、量子雑音ランダム化ストリーム暗号(注1)に関する研究を実施する。特に、従来暗号の枠組みの範疇では超越できない暗号学のシャノン限界(注2)を超越できる安全性を目指す。このためにまず、量子乱数を用いた量子ランダム化拡張技術の検討を行い、量子雑音駆動型DSR（Deliberate signal randomization）(注3)を開発し、これを量子雑音ランダム化ストリーム暗号の暗号化部に組み込んだ暗号システム(注4)を実証することを目標とする。次に、安全性向上の評価理論を構築し、今回提案する量子雑音ランダム化ストリーム暗号による暗号通信システム(注5)の安全性向上の検証を目標とする。実験検証はオフライン方式で実施する。

量子雑音駆動型DSRを組み込んだ量子雑音ランダム化ストリーム暗号が有すべき性能･機能は以下の通りである。

- 暗号信号の盗聴されにくさを表すひとつの指標である暗号信号拡散率を実験測定し、いずれかの主要な変調方式（位相変調、強度変調、直交振幅変調など）においては80%以上の性能を目指す。
- 暗号通信システムに応じて量子ランダム化拡張量を最適化する機能を目指す。
- 量子ランダム化拡張量を最適化した暗号信号を実現し、暗号システムでビット誤りを測定し、ビット誤り率が1.8%未満になる性能を目指す。

暗号通信システムにおいて安全性向上の実験検証で達成すべき性能・機能は以下の通りである。

- 実験測定可能な物理パラメータで表せる評価式を導き、実験評価結果の意味を正しく説明でき、シャノン限界超越との関係を明確にできる理論の構築を目指す。
- ディジタルコヒーレント検波技術を応用し、暗号信号光を受光し、判別距離(注6)を推定する評価式の実測評価を可能とする測定系を構築する。
- シャノン限界超越として、暗号システムにおいて、オフライン方式で実験測定により推定される判別距離が鍵長(例えば、256ビット)よりも大きくなる機能(性能)を目指す。
- 暗号通信システムにおいて、オフライン方式での評価手法で、理論推定できる判別距離が鍵長(例えば、256ビット)よりも大きくなる機能(性能)の実験実証を目指す。暗号通信システムの構成は、暗号信号光波長Cバンド帯(1530～1565nm)、通信容量10Gb/s以上で、都市部をカバーするメトロネットワークに適用できる程度の通信距離100km以上とし、ビット誤り率は1.8%未満の性能を目指す。

注釈

(注1) 量子雑音ランダム化ストリーム暗号
光信号受信時に不変・不可避に付加される量子雑音によるランダム性により、盗聴者に暗号文を正しく読み取らせない手法で安全性を高めることを特徴とするストリーム暗号。ストリーム暗号とは、データをビット毎に暗号化する暗号のこと。

(注2) 暗号学のシャノン限界
情報理論的安全性を達成できるデータの量の限界であり、盗聴者が暗号文を正しく読み取れることを前提とする暗号理論体系においては、暗号鍵の長さと等しい。

(注3) 量子雑音駆動型DSR
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。

(注4) 暗号システム
量子雑音ランダム化ストリーム暗号の基本システムは暗号化部と復号化部からなる。暗号システムは、暗号化部と復号化部が直接結合された構成のシステムで、暗号化部でデータを暗号に変換し、復号化部でその暗号を復号し元のデータに変換する。

(注5) 暗号通信システム
暗号システムに通信回線（光ファイバ回線など）が加わったシステム。暗号化部、通信回線、及び復号化部がこの順番で接続されたシステムで、通信回線を介して遠隔地にいる正規通信者同士の暗号通信を可能とする。量子雑音ランダム化ストリーム暗号を通信システムとして見た場合には、暗号化部と復号化部はそれぞれ送信機と受信機となる。
(注6) 判別距離
安全性の指標であり、定められたある長さの鍵が与えられている条件下で、暗号文を得たときにデータに対する曖昧さがなくなるデータの長さ。

１．２　最終目標を実現するために克服又は解明すべき要素課題

最終目標を実現するために克服すべき要素課題は以下の通りである。

(1) 暗号用乱数発生の検証
量子雑音ランダム化ストリーム暗号の安全性向上に寄与する本質的な技術は量子雑音に基づく乱数発生機構を有する量子ランダム化拡張技術と見込んでいる。そこで最終目標の達成に不可欠な当該技術を実現するために、量子ランダム化拡張に組み込む量子乱数発生機構の提案及び解析を行い、特に当該機構から発せられる乱数系列の検証が必要である。

(2) 量子ランダム化拡張技術開発
従来の共通鍵暗号の安全性を超えるための技術として、新たなランダム化拡張機構の開発が必須となる。量子ランダム化拡張技術は判別距離を大きくするための技術で、シャノン限界超越（判別距離＞鍵長）の実現に不可欠である。暗号化部内で量子雑音を意図的に付加することにより暗号信号のランダム性を高めるために、量子雑音からディジタル的あるいはアナログ的な手法により得られる量子乱数発生機構をランダム化拡張技術に組み込み、DSRを量子雑音で駆動するランダム化拡張の手法を解明し、新たな量子ランダム化拡張理論を構築する必要がある。加えて、当該理論の検証のために、量子ランダム化拡張回路を設計し、暗号システムとしての動作を検証する必要がある。また、検証において判別距離を同定するために、測定可能な物理量で表せる判別距離を推定して評価する理論を構築し、評価に必要な物理量を測定する実験系を構築する必要がある。

(3) 暗号通信システム評価
一般に暗号通信システムでは、盗聴者に対しては情報を秘匿にし、通信回線の先にいる正規通信者は情報を正しく受信できることが要件となる。量子ランダム化拡張技術を組み込んだ本要素課題で対象とする暗号通信システムでは、信号レベル数対雑音マスキング比率が大きくなり盗聴防止効果が高まるが、一方で、正規通信者の信号対雑音比の劣化が生じ通信性能に悪影響を及ぼす。そのため、正規通信者が正しく通信でき同時に安全性を向上できる量子雑音ランダム化ストリーム暗号を用いた暗号通信システムを解明し、この暗号通信システムの回線のいかなる位置においても推定できる判別距離が鍵長よりも長くなるという、最終目標である安全性向上を検証する必要がある。

１．３　要素課題に対する実施項目及び体制

前述の要素課題を克服するために、(1)から(7)の実施項目を設定し、(8)のプロジェクトの総合的推進を図り実施する。実施において、まず、(1)量子乱数発生の機構を(2)量子ランダム化拡張に組み込み実装する。次に、量子ランダム化拡張を組み込んだ暗号化部と復号化部を結合し(3)暗号システムを実装する。その後、暗号システムで(4)量子ランダム化拡張量の最適化を実施する。併せて、暗号システムの判別距離を推定するために、(5)判別距離測定系を構築する。最終的に、暗号システムと通信回線を結合し、(6)暗号通信システムを評価する実験系を構築し、安全性向上を実験評価する。評価には、(7)安全性向上の評価理論を適用する。以下に、各実施項目の内容を示す。

(1) 量子乱数発生

要素課題(1)の克服に向け、量子雑音のランダム性を利用した乱数発生を実現する。いくつか実現手法が考えられる。光信号受信時に発生するボルン効果による量子雑音を高速アナログ・ディジタル変換器により取り込みディジタル化する手法を本実施項目の第一候補とする。別の手法として、アナログ処理を特徴とする光源の位相雑音を直接的に制御する手法なども有効性を含めて検討する。具体的な実施内容は、まず、暗号利用に適した乱数発生手法を選定するために、一般的な量子乱数発生に関する先行技術を調査する。次に、先行技術調査に基づき、実施項目(2)の量子ランダム化拡張技術に組み込むために適した発生手法を検討する。続いて、発生手法を実現するための実験系を電子部品や光部品などを用いて構築し、構築した実験系で乱数データを生成し、そのランダム性を解析する。解析では、既存の乱数発生手法との比較も実施する。

本実施項目の終了までに達成すべき目標は、第一に、量子雑音ランダム化ストリーム暗号の量子ランダム化拡張技術に利用可能な量子乱数発生機構を提案する。第二に、提案手法により生成される乱数のランダム性を実験により評価し、実施項目(2)の量子ランダム化拡張技術に組み込んで利用できる形態とする。量子乱数発生は、10Gb/s以上の通信容量での暗号通信システムを可能とするものを目指す。

(2) 量子ランダム化拡張実装

要素課題(2)の量子ランダム化拡張技術を実現するために、ディジタル的あるいはアナログ的な手法の量子乱数発生とDSRを含む量子ランダム化拡張技術を連結する。そのために本実施項目では、既存のDSRと異なり量子乱数での駆動を可能とする量子雑音駆動型DSRについて理論的な検討を実施する。次に、理論検討結果から得られた量子雑音駆動型DSRを高速で動作させるための方策を考案する。その上で、まず、量子雑音駆動型DSRのアルゴリズム的な核となるプログラムを設計・作成する。実施項目(1)において量子乱数発生を達成するまでの間は、量子乱数を模擬する擬似乱数など代替乱数を用いてオフライン方式で量子雑音駆動型DSRを模倣させ、任意波形発生器を用いてランダム化性能を実験評価する。代替乱数での動作を検証した後、最終的には、実施項目(1)の量子乱数発生で得られる量子乱数を用いて量子雑音駆動型DSRを駆動し、実施項目(3)、(4)及び(6)の達成に用いる。

本実施項目の終了までに達成すべき目標は、第一に、量子雑音駆動型DSRを構成し、量子乱数の代わりに擬似乱数を用いてオフライン方式でランダム化性能を実験評価する。第二に、実施項目(1)で得られる量子乱数を組み込んだ量子雑音駆動型DSRを評価し、暗号信号拡散率80%以上を目指す。第三に、量子雑音駆動型DSRは、実施項目(3)の暗号システムに組み込めるようにする。量子雑音駆動型DSRは、通信容量10Gb/s以上の暗号通信システムを可能とするものを目指す。

(3) 暗号システム実装

正規通信者同士が暗号通信できるよう、実施項目(2)で実現する量子雑音駆動型DSRを組み込んだ暗号化部と復号化部が同期して動作する暗号システムが、要素課題(2)の克服に求められる。そのために、本実施項目では、まず、実施項目(2)の量子雑音駆動型DSRを量子雑音ランダム化ストリーム暗号の暗号化部に組み込むために、量子雑音駆動型DSRの出力を接続し、通信データを入力し暗号信号を出力する既存の不規則マッピングを含む暗号化部を設計し、それを実現するプログラムを作成する。なお、暗号信号は位相変調、強度変調、直交振幅変調方式などが用いられるが、第一候補として位相変調方式を採用する。次に、暗号化部から出力される暗号信号を入力し、通信データを出力する復号化部と暗号化部の同期がとれるプロトコルを考案しプログラム作成する。最終的に、動作検証として擬似乱数系列で構成される模擬的な通信データを用いて復号化部から出力される通信データのビット誤り率評価試験を実施する。本試験は、不具合発生時に効率的に原因を解明できるように二段階のステップとする。まず電気領域で電気信号のビット誤り率測定を実施する。次に、電気信号で駆動する光変調器にレーザ光を入力して得られる光信号を用いた光領域での評価を実施する。

本実施項目の終了までに達成すべき目標は、第一に、量子雑音駆動型DSR及び不規則マッピングを組み込んだ暗号化部を駆動するプログラムを作成する。第二に、暗号化部と復号化部を同期させるプロトコルを考案し、暗号システムを実現する。第三に、暗号システムの動作試験を電気信

号で実施し動作検証する。第四に、光ファイバ通信の一般的な波長帯であるCバンド帯(1530～1565nm)の光信号で動作試験を実施し動作検証する。動作検証は、電気信号、光信号共にビット誤り率が誤り訂正符号で訂正可能な1.8%未満になることを目指す。

(4) 量子ランダム化拡張量の最適化

量子ランダム化拡張の導入により、正規通信者の通信性能劣化は避けられないが、適切な設計を行いある程度のビット誤りを許容する方法で最適化し、要素課題(3)の正規通信者への悪影響を小さく抑える。そのために、本実施項目では、まず、実施項目(2)で付加する量子ランダム化拡張量とビット誤り率の関係を分析し、正規通信者の通信品質を保証し、かつ、量子ランダム化拡張量を可能な限り大きくする手法を考案する。次に、考案した手法に基づき量子ランダム化拡張量の最適化を実施する。その上で、最適化した量子ランダム化拡張量を暗号信号に付加し、ビット誤り率を評価指標として、実験により最適化の評価を行う。最終目標を達成するために最適な量子ランダム化拡張量を付加した暗号信号ではビット誤りが多すぎて正規通信者同士さえも通信ができないことを避けるために、既存技術の誤り訂正符号の導入を検討し、正規通信者にとって十分な通信品質を確保する。

本実施項目の終了までに達成すべき目標は、第一に、量子ランダム化拡張量とビット誤り率の関係を分析する手法を考案する。第二に、考案した手法に基づき最適化設定を行い、ビット誤りを測定し、ビット誤り率が誤り訂正符号で訂正可能な1.8%未満になることを目指す。

(5) 判別距離測定系構築

シャノン限界超越の検証には要素課題(2)の判別距離推定の実験を通じた同定が求められる。そのために、実験測定可能な物理量で表すことができる評価理論に基づく判別距離推定の実験測定系を構築する。量子雑音駆動型DSRを組み込んだ従来にない暗号信号光を測定するため、ディジタルコヒーレント検波技術を軸に光ディテクタ、光ハイブリッドなど光部品・光学装置、電子回路部品・装置を用いて設計・構築する。本実施項目では、まず、実施項目(4)で得られる量子ランダム化拡張量を最適化した暗号信号を受光し、実施項目(7)で得られる判別距離推定の評価式に必要な物理量の測定を可能とする測定系を設計する。次に、設計した測定系を実際に構築し、暗号信号光の判別距離を推定・評価する。本測定系により、要素課題(3)の暗号通信システムにおける判別距離の評価が可能となる。

本実施項目の終了までに達成すべき目標は、第一に、評価式に必要な物理量を実験測定する系を設計する。第二に、設計した測定系を実現するための部材・装置を選定し、新たな測定系を構築する。第三に、構築した測定系をシャノン限界超越の評価試験に適用する。

(6) 暗号通信システム評価

要素課題(3)を克服するために、実施項目(3)の暗号システムを暗号通信システムに適用することが求められる。そのため、本実施項目では、まず、ディジタルコヒーレント受信技術を用いた光ファイバ通信システムを対象とした数値解析用のシミュレーションモデルを構築し、暗号信号光の通信特性を数値解析する。次に、通信特性の実験評価のために光ファイバ伝送路を通信回線とする光ファイバ通信システムを構築する。続いて、暗号信号光の波形解析や光スペクトル解析を行い、オフライン方式で通信性能を実験評価する。最終的に、実施項目(7)で得られる安全性向上の理論を適用し、暗号通信システムの安全性を実験評価する。

本実施項目の終了までに達成すべき目標は、第一に、数値解析手法を用いて通信特性を解析する。第二に、通信特性の実験評価に必要な光ファイバ通信システムを構築する。第三に、オフライン方式で通信距離やビット誤り率を評価する。この際、信号光波長Cバンド帯(1530～1565nm)、通信容量10Gb/s以上で、都市部をカバーするメトロネットワークに適用できる程度の通信距離100km以上の構成で、ビット誤り率は誤り訂正符号で訂正可能な1.8%未満を目指す。第四に、実施項目(7)の安全性向上の評価理論を適用し安全性向上を実験検証する。

(7) 安全性向上の評価理論

本実施項目を遂行することで、実施項目(6)の暗号通信システム評価が可能となり、要素課題

(3)の克服を目論んでいる。現時点では、シャノン限界超越と判別距離の厳密な関係が未解明である。そこで、判別距離推定の実験評価に向け、判別距離や雑音マスキングなどと安全性評価に関する先行技術を調査することから始める。平行して、GPUアクセラレータを本学既存設備（ワークステーション）と組み合わせ、盗聴者能力を量子信号検出理論の観点から推定するための計算環境を整える。次に、実験測定可能な物理パラメータで表せる評価式の導出に取り組む。最終的に、導出された評価式を実験評価に適用した場合の意味を正しく説明でき、シャノン限界超越との関係を明確にできる理論の構築を目指す。

本実施項目の終了までに達成すべき目標は、第一に、盗聴者能力を量子信号検出理論の観点から推定するための計算環境を構築する。第二に、安全性向上評価理論として測定可能物理量で表せる判別距離の評価式を導出する。第三に、実施項目(6)の暗号通信システム評価実験に当該理論を適用して、安全性向上を理論的に裏付ける。

(8) プロジェクトの総合的推進

本委託業務は研究代表者及び研究分担者２名により適切に分担・連携して実施する。また、研究代表者により各要素課題に関する研究の進捗を適切に管理し、必要に応じて研究手法の合理化を検討し、プロジェクトの推進を図る。

２．研究開始時に設定した研究目標の達成度

本研究では、量子雑音駆動型DSR（以下、QDSR）を組み込んだ量子雑音ランダム化ストリーム暗号を実現し、これを暗号通信システムに適用し、通信システムの安全性を向上することを目標とした。初めに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提案し、オフライン信号処理方式を用いて発生速度100Gb/sの高速乱数発生に成功した。更に、実運用での評価に適したリアルタイム信号処理方式にも取り組み、発生速度50Gb/sの乱数発生を実証という計画を超える成果を得た。なお、本成果は、量子雑音揺らぎに基づく乱数発生手法の発生速度の中で世界最速である。次に、本手法で発生させ乱数を用いて駆動したQDSRを実証し、位相変調方式の信号に対して、80%以上の暗号信号拡散率を実現した。このQDSRを量子雑音ランダム化ストリーム暗号の暗号化部に実装した暗号システムを構築し、ビット誤り率が1%未満での暗号通信に成功すると共に、安全性が桁違いに高くなることを検証した。更に、この暗号システムを光ファイバ通信システムに適用し、通信容量10Gb/sで通信距離362kmの無中継光ファイバ暗号通信を実施し、高い通信性能と安全性を同時に実証した。また、計画を超える取り組みとして、敷設光ファイバ回線において光増幅器を用いて暗号信号を中継する光ファイバ増幅中継暗号通信システム実験を行い、通信容量10Gb/sで400kmの通信に成功し、光ファイバ通信システム全体において桁違いに高い安全性を実証した。安全性向上評価理論に関しては、マスキング数、盗聴者のシンボル誤り率の指標が有効であることを理論的に明らかにし、本指標を用いて安全性向上の実験検証を実施した。以上のように、当初の目標を達成した。

３．委託業務における研究の方法及び成果

３．１　量子乱数発生

QDSRを実現するために、高速で乱数を発生可能な手法として、量子雑音測定に基づく乱数発生手法を提案し、実証した。本手法は、量子雑音を測定しそのランダム性を利用して乱数を発生する。量子雑音は、光ファイバ通信で利用されているコヒーレント検波をもちいると測定できる。光ファイバ通信向けに要素技術は開発済で、測定に必要な部品は市販されており、実装に向けても優れた手法であり、乱数生成速度がGb/sを越える特徴がある。図1に、本手法を実現する具体的なブロック図を示す。

レーザ（LASER）出力はコヒーレント状態にある光と見做せる。複素振幅α’を持つコヒーレント状態は記号$|\alpha\rangle$で表すことにする。コヒーレント状態光$|\alpha\rangle$はビームスプリッタ等で構成される光分岐部でM個の光に分割することができ、コヒーレント状態の基本的な性質から$|\alpha_1\rangle\otimes|\alpha_2\rangle\otimes\cdots\otimes|\alpha_M\rangle$と書ける。それぞれの$|\alpha_m\rangle$もまたコヒーレント状態である。各分岐光$|\alpha_m\rangle$は測定部において測定される。分岐光$|\alpha_m\rangle$はさらに（ほぼ等分配の）ビームスプリッタで$|\alpha_m^{(A)}\rangle$と$|\alpha_m^{(B)}\rangle$に2分割された後、それぞれをフォトダイオードで光電流$I_m^{(A)}$または$I_m^{(B)}$に変換する。そこで、$I_m = I_m^{(A)} - I_m^{(B)}$とす

れば、測定結果μ_mはショット雑音によって揺らぐ電流I_mとなる。この場合、揺らぎは平均$|\alpha_m^{(A)}|^2 - |\alpha_m^{(B)}|^2 \approx 0$, 分散$|\alpha_m^{(A)}|^2+|\alpha_m^{(B)}|^2$を持つスケラム分布に従う。各測定結果$\mu_m$は合成する処理部に送られる。処理部ではまず、測定結果μ_mを適当な方法でビット値$b_m \in \{0,1\}$に変換する。例えば最も簡単な方法は、電流Imの正負を以て変換することである。処理部ではさらに$r = b_1 \oplus b_2 \oplus \cdots \oplus b_M$を計算する。このrが最終的な出力値（RND）になる。最終出力ビット値r の偏りP(r=0)とP(r=1)の差は M に応じて指数的に小さくなることが明らかになっている。例えば、$M = 8$ の場合、$\max_m |P(b_m = 0) - P(b_m = 1)| = 0.1$のとき、$|P(r = 0) - P(r = 1)| \leq 10^{-8}$ となる。

別の乱数発生手法として、真空場揺らぎを利用する方法も考えられる。CWレーザから出力される光をビームスプリッタで二等分に分岐し、バランスホモダイン方式で測定すると真空場揺らぎを観測できる。この測定結果を取得したエントロピー源をもちい、ハッシング処理により乱数を抽出する。エントロピー源のランダム性が厳密に保証されていることや、光ファイバ通信向けの部品を転用することで高速動作可能である点で優位性がある。高速性については、光ファイバ通信の通信速度程度の駆動が理論上可能で、具体的には、10Gb/s程度の発生速度が期待できる。更に、並列処理による高速化が可能である。図1の構成を基本構成として図2のように拡張することで、並列化を容易に実現できる。並列的に生成された乱数群を並列度に応じた倍速クロックで出力することでさらなる高速化が期待できる。例えば、基本構成を速度10Gbpsで駆動し、並列度8とすると、速度80Gbpsの乱数生成を見込める。この優位性に着目し、本研究では後者の手法で実験検証を実施した。

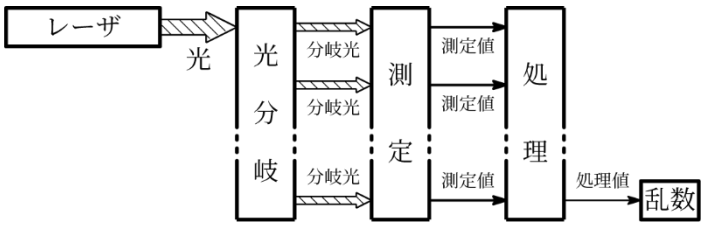


図1：量子雑音測定に基づく乱数発生のブロック図

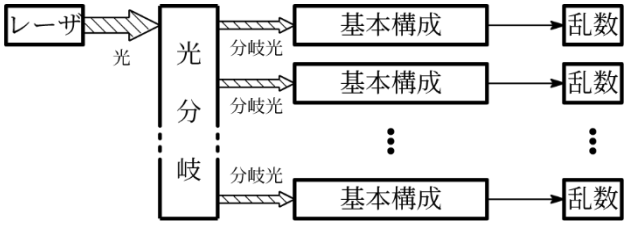


図2：基本構成の並列化

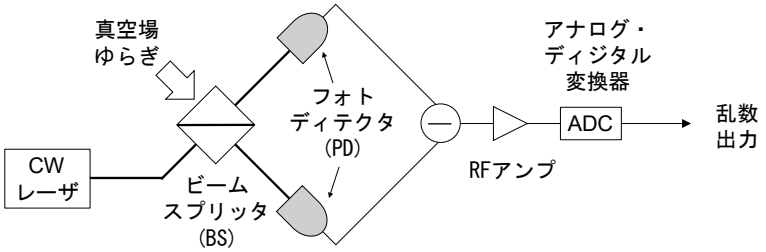


図3：提案する量子乱数発生機構を具現化するための回路構成例

量子雑音測定方式の乱数発生手法を具現化するための回路構成例を図3に示す。簡単のために、並列度は1とした。光ファイバ通信で利用されているホモダイン検波方式で真空場の揺らぎを観測する。この揺らぎが量子雑音となり量子雑音に基づく乱数の生成が可能となる。CWレーザ(レーザ光源)、光を分岐するビームスプリッタ(BS)、光を受光するフォトディテクタ(PD)、電気増幅器(RFア

ンプ)及びアナログ・ディジタル変換器(ADC)で構成される。CWレーザから出力される連続光をBSで分岐してバランスホモダイン受信する。受信信号をRFアンプで増幅し、ADCでディジタル化する。1サンプルからADCのビット分解能分の乱数を得られる。ADCの後段で、ディジタル的に後処理し古典雑音を取り除き、量子雑音のみによる乱数を得ることができる。

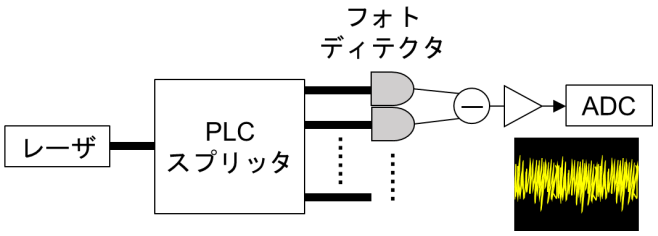


図4：並列化による高速化を実現するための構成例

更に、基本構成の並列化するための実験構成についても検討した。図4に示すように、一つの入力ポートに対して複数の出力ポートがあるPLCスプリッタを利用して並列化する。平面導波路型(PLC)スプリッタをもちいるとコンパクトに並列化を構成できる。並列化可能数は、レーザから出力される光パワー、PLCスプリッタの挿入損失及び分岐数に基づく損失で決定される。量子雑音を測定するためにPDに必要な光パワーが下限となり、PLCスプリッタの損失と分岐比に基づく損失の和をレーザ出力光パワーから差し引いた値が、PD所要パワーを下回ると量子乱数が得られなくなる。レーザ出力パワーP_{LD}、並列数N_{pall}、PLCスプリッタの過剰挿入損失L_{PLC}、PDでの光パワーP_{PD}とすると、次の関係式が導かれる。

$$P_{LD} = \frac{N_{pall} \times P_{PD}}{L_{PLC}} \tag{1}$$

この式より、並列数の最大数N_{MAX}は、PDでの所要最低光パワーをP_{PD_MIN}とすると、次式で表せる。

$$N_{MAX} = \frac{P_{LD} \times L_{PLC}}{P_{PD_{MIN}}} \tag{2}$$

本式を利用して、高速乱数として発生速度を100Gb/sと設定し、光分岐比の検討や部品選定を実施した。その結果、4並列化により発生速度100Gb/sの量子乱数を発生できる見通しを得た。4並列化のために1対8の光スプリッタが必要なので、低損失かつ損失の出力ポート依存性の小さな石英ベースのプレーナ光回路を採用した。光源には出力パワーが70mWを越える低雑音・高出力レーザ装置が必要との検討結果に基づき、図5に示すように、光スプリッタで分岐した局発光を4つのバランス・フォトディテクタ(BPD)で受光し、それぞれのBPDの出力を分解能12bit、帯域4GHzのリアルタイムオシロスコープの入力チャネルに接続し、12.5Gsample/sのサンプリングレートで雑音波形を取り込んだ。取り込んだ雑音は、オフライン信号処理で4Gsample/sにリサンプリングした。レーザ光パワーと雑音の分散量の関係は線形で、取り込んだ雑音は量子雑音が主であることを裏付けていた。図6は、各チャネルの雑音分布を示している。測定範囲の調整のため、分解能12bits中の10bitsを使用した。いずれのチャネルもガウス分布であることを確認した。

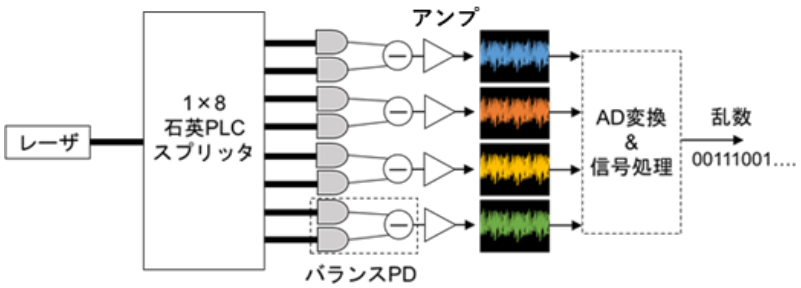


図5：並列化をもちいた乱数発生の構成図（オフライン信号処理）

次に、このガウス分布から一様な乱数を引き出す後処理として、次の三つの手法を比較した。

・テプリッツ行列によるハッシング（4000×2000）→　効率：50%
・テプリッツ行列によるハッシング（4000×2500）→　効率：62.5%
・2系列のXOR（RMSB, LMSB処理）→　効率：50%

次に、エントロピー源としての評価として、NIST SP800-90Bの検定を実施した。検定結果をまとめて図7に示す。市販の乱数発生器のエントロピー（平均7.8757）とほぼ同等性能を実現した。最大出力レートは、4チャネル×4Gsample/s×10bits×0.625(効率)より、100Gb/sと設定通りとなった。更なる高速化には、光源の出力パワーと並列数の増大、ADCの高分解能化などが必要になる。

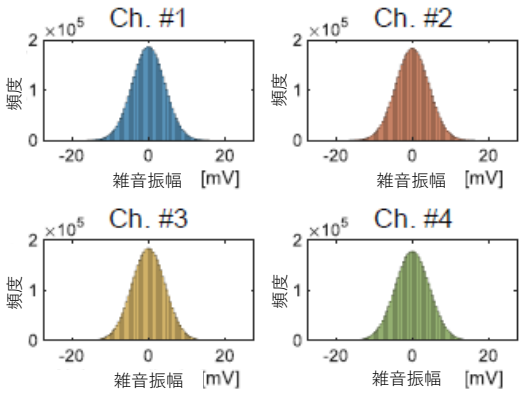


図6：4チャネルの雑音分布

	Hashing Matrix size: 4000×2500	Hashing Matrix size: 4000×2000	XOR
Efficiency	62.5%	50%	50%
Aggregated gen. rate (potential)	100 Gbps	80 Gbps	80 Gbps
NIST test	passed	passed	passed
Entropy (average of four channels)	7.8735	7.8779	7.8704

図7：NIST SP800-90Bによる検定結果

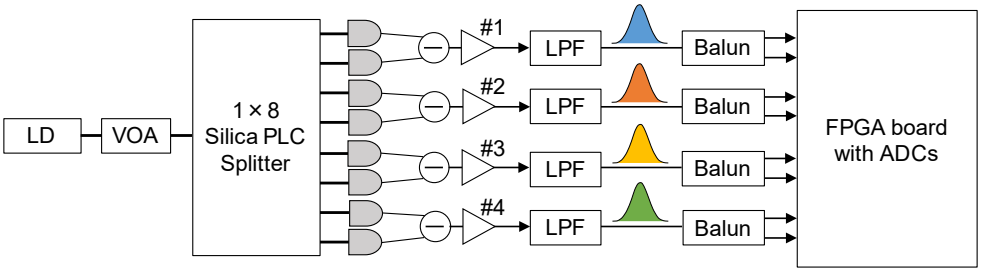


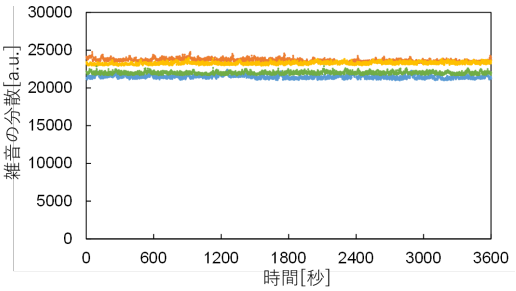
図8：リアルタイムでの乱数発生の構成

オフライン信号処理手法は、データをメモリーに一旦保存した後、保存したデータを処理するので安価で効率的に動作検証が可能である。一方、処理できるデータ量はメモリー容量に限られる。暗号通信のデータ評価には適当な手法であるが、乱数自体の特性評価にはより長い時間のデータが求められることが、研究を進めた結果分かった。そこで、当初の計画ではオフライン信号処理としたが、リアルタイム化を行い、その検証を実施した。図8にリアルタイム信号

処理方式での乱数発生の構成を示す。図5と同様の構成であるが、信号処理部は高速信号処理が可能なFPGA(Field Programmable Gate Array)を用いた。並列数と各チャネルの帯域を適切に設計することにより、4チャネル並列で各チャネル2GHzの帯域のエントロピー源を実現した。リアルタイム化のためには、大規模な行列演算である乱数抽出処理を高スループットで実装する必要があるため、本抽出処理を並列にFPGAに実装した。その結果、12.5Gbit/s × 4channel = 50Gbit/sの乱数発生速度を達成した。これまでの最高速度の約2.6倍となる。さらなる高速化に向けては、光源パワーの増大と並列数の増加が必要となる。また、光集積技術を用いた空間多重エントロピー源の小型化が期待できる。光スプリッタとBPDは、コヒーレント受信フロントエンド光回路で実証されているように、ハイブリッドまたはヘテロジーニアスに集積化が可能である。

	Ch. 1	Ch. 2	Ch. 3	Ch. 4
Entropy [bits/byte]	7.8727	7.8698	7.8736	7.8764
Chi square test	✓	✓	✓	✓
Length of LRS test	✓	✓	✓	✓
IID permutation test	✓	✓	✓	✓
Restart test	✓	✓	✓	✓

(a)



(b)

図9：リアルタイムで発生させた乱数の評価結果。(a)NIST SP800-90Bによる検定結果、(b)乱数の分散の時間変動。

3．2　量子ランダム化拡張実装

量子ランダム化拡張は、暗号鍵に基づき暗号信号に付加されるランダム性に加えて、量子乱数で駆動されたQDSRによるランダム性を暗号信号に付加する。これにより、暗号信号のランダム性が拡張され、暗号強度が高まる。送受信者がQDSR用の鍵を共有する必要がない、つまりキーレスなので組み込みが容易という特徴がある。一方、キーレスのため、正規受信者でも量子乱数に基づくランダム性を取り除くことができず、原理的に正規受信者の通信特性は劣化する。図10に、BPSK信号を一例に用いて量子ランダム化拡張の概要を示す。暗号鍵に基づき生成される基底信号に応じた位相回転($\theta_{basis}(i)$)に、量子乱数で駆動されたQDSRによるランダムな位相回転($\theta_{QDSR}(i)$)を付加し、位相回転のランダム性を増大する。QDSRによる位相の変調度(QDSR変調度)をγ_{QDSR}($0 \leq \gamma_{QDSR} \leq 1$)とすると、量子ランダム化拡張により、$\pi\gamma_{QDSR}$だけ位相に揺らぎが加えられる。$\gamma_{QDSR}$は暗号信号拡散率に対応する。同図(iii)は正規受信者が復号後に得られるコンスタレーションを表している。量子ランダム化拡張で付加された位相揺らぎは、正規受信者でも取り除くことができず、正規受信者のビット誤りを引き起こす原因となり得る。

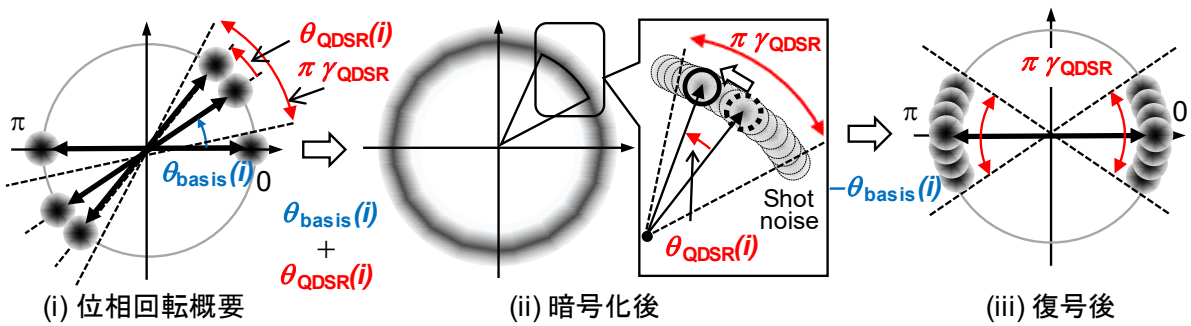


図10：量子ランダム化拡張の概要

本手法は、強度変調方式、位相変調方式、直交振幅変調方式など様々な変調方式に適用できるが、本研究では位相変調方式で検証実験を実施した。まず、量子ランダム化拡張の実装に向け、量子乱

数発生器で発生した量子乱数でDSRを駆動するプログラム作成しQDSRを実現した。次に、送受信者が共有する共通鍵を用いて発生させた擬似乱数に基づくランダム性を付加された暗号信号に、QDSRによる位相揺らぎを追加した。安全性評価は、安全性評価指標のひとつであるマスキング数を用いた。マスキング数とは、ある暗号信号の量子雑音が覆い隠す暗号信号レベルの数を表す。マスキング数が大きいほど、正しい暗号信号レベルを正しく識別することが困難になる。この安全性評価指標の妥当性は3．3節で説明する。

QDSRを組み込まない場合、2値PSK(BPSK)方式のマスキング数は、量子雑音を隣接信号の位相差で割ることにより、次式で表される。

$$\Gamma_{PSK} = \frac{2^{m+1}}{2\pi}\sqrt{\frac{2h\nu_0 B}{\eta_q P_0}} \tag{3}$$

ここで、mは多値変調度、Bは信号帯域、P_0は信号光パワー、hはプランク定数、υ_0は信号周波数、η_qはフォトディテクタの量子効率を表している。多値変調度、信号帯域が大きいほどマスキング数は大きくなり安全性は向上する。一方、信号光パワーが大きいほどマスキング数は小さくなり安全性が低下する。通常、光ファイバ通信システムでは信号光パワーは、伝送損失により小さくなったり、光増幅器により大きくなったり変動する。そのため、安全性が信号光パワーに依存することは、通信システム全体の安全性を高める上で望ましくない。

次に、QDSRを組み込んだ場合のマスキング数を解析した。QDSRは一様に分布し実効的にQDSR変調度分のマスキング効果が増えているものとして解析を行い、次式を得た。

$$\Gamma_{QDSR} = \frac{2^{m+1}}{2\pi}\left(\sqrt{\frac{2h\nu_0 B}{\eta_q P_0}} + \pi\gamma_{QDSR}\right) \tag{4}$$

第1項は式(3)と同じで、従来のマスキング効果を表している。第二項はQDSRにより追加されるマスキング効果で、信号光パワーには依存せずにQDSR変調度γ_{QDSR}により決定される。第2項が第1項に比べて十分大きくなる条件下では、マスキング数は信号光パワーに無依存となる。すなわち、QDSRにより、光ファイバ通信システム全体のマスキング数を大きな値に維持することができ、システム全体を安全にすることが可能となるという新たな知見が得られた。

前述の通り、QDSRにより正規受信者にもランダム性が残留する。そのため、マスキング数を大きくすれば安全性は高くなるが、一方で、正規通信者間での通信品質が低下してしまう。そこで、QDSRが正規受信者に及ぼすビット誤り率を解析した。解析のモデルを図11に示す。解析では、信号光はBPSK、正規受信者はホモダイン検波で信号光を受信するものとした。また、QDSRは一様に分布し実効的にQDSR変調度分だけマスキング効果が増えているものとした。

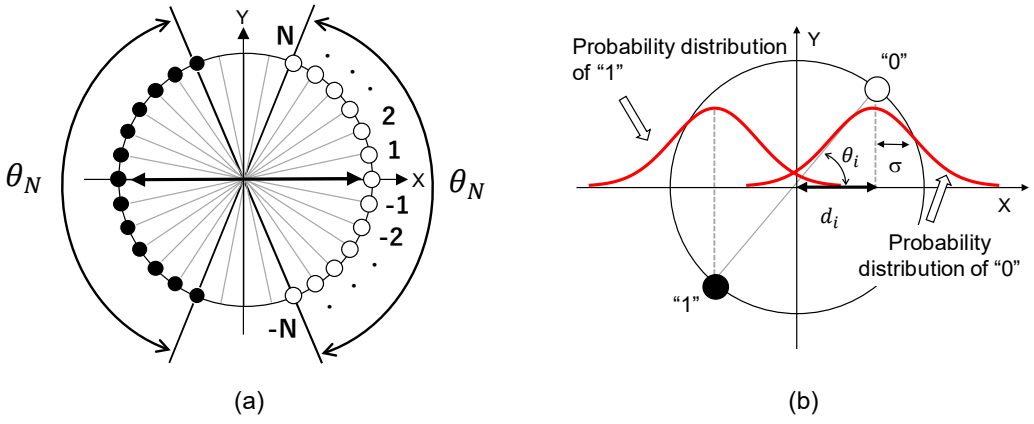


図11：QDSRが正規受信者のビット誤り率に及ぼす影響の解析モデル(BPSK信号)。(a)QDSR変調度を表すコンスタレーション。(b)正規受信者が測定する雑音分布

基底数をMとすると信号元数は2Mとなり、QDSRによる位相変調量は$\theta_N = \pi N/M$となる。NはQDSR量で、$0 \le N \le M/2-1$を満たす整数である。Nが小さいとQDSRによる位相変調量は小さくなり、逆にNが大きいとQDSRによる位相変調量は大きくなる。“0”を“1”と誤る確率P^B_0、“1”を“0”と誤る確率P^B_1を送出し、データ“0”と“1”の発生頻度が等しいとすると、正規受信者のビット誤り率(BER)は、

$$\mathrm{BER} = \frac{1}{2}P_0^B + \frac{1}{2}P_1^B = \frac{1}{2(2N+1)}\sum_{i=-N}^{N}\mathrm{erfc}\left(\frac{d_i}{\sqrt{2}\sigma}\right) \tag{5}$$

となる。ここで、$d_i = \sqrt{n_S}\cos(i\pi/M)$で、$n_S$はフォトン数を表す。本式に各値を代入するとビット誤り率が求められる。一例として、基底数M = 2^{11}の場合のビット誤り率を計算した結果を図12に示す。フォトン数は100、1,000、10,000とした。B=10Gb/sとすると、光パワーは、それぞれ約-49dBm、-39dBm、-29dBmとなる。-49dBmという小さな値であっても、$\gamma_{QDSR} \le 0.85$(暗号信号拡散率 < 85%)ではビット誤り率は10^{-9}よりも小さくなり、QDSRの影響はほぼ無視できることが分かった。ただし、本解析では量子雑音のみを考慮したが、実際のシステムでは受信回路の熱雑音や光増幅器で発生する自然放出光雑音など付加雑音も雑音に含まれることに注意する必要がある。

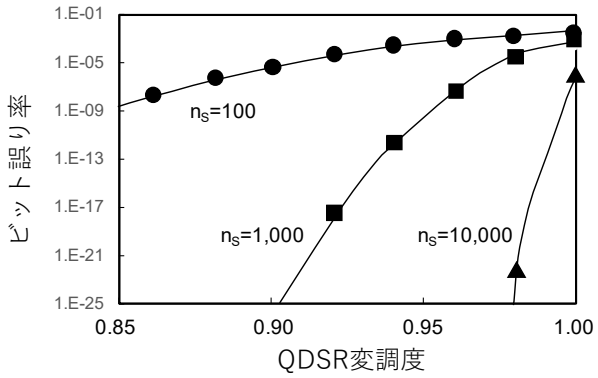


図12：量子雑音のみを考慮した場合の正規受信者のビット誤り率のQDSR変調度依存性。

次に、QDSRを組み込んだ暗号信号を測定し、量子ランダム化拡張を実験検証した結果をまとめる。暗号信号は、B = 5Gb/s、基底数M = 2^{15}、光パワーP = 1mWのBPSK信号とした。ディジタルコヒーレント通信で用いられるイントラダイン受信機を用いて測定したコンスタレーションを図13に示す。QDSR変調度を大きくすると、位相はよりランダムになった。コンスタレーションの各位相の頻度分布を算出し、頻度が半分になる位相量を求め、暗号信号拡散率を評価した。理論値と評価値はほぼ一致しており、例えば、γ_{QDSR} = 0.80に設定したとき、測定した位相揺らぎの全幅は2.6(rad)で、QDSR変調度は0.83、暗号信号拡散率は83%を達成していた。以上の結果より、QDSRはほぼ設計通り実装されたことが分かった。

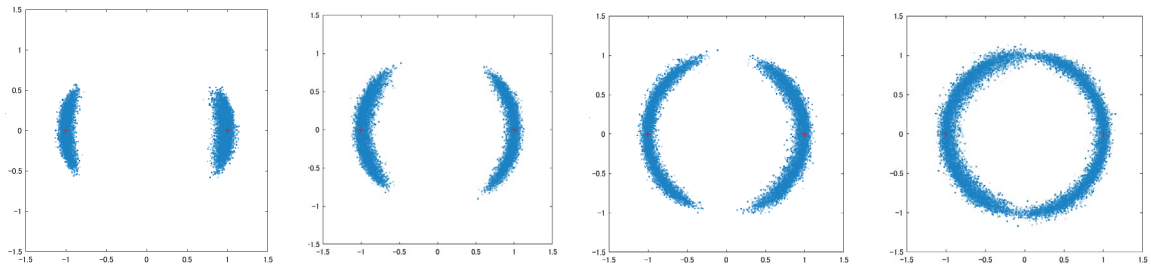


図13：QDSRを駆動して発生させたBPSK信号のコンスタレーション。(a) γ_{QDSR} = 0.2、(b) γ_{QDSR} = 0.4、(c) γ_{QDSR} = 0.6、(d) γ_{QDSR} = 0.8。

次に、この位相揺らぎにより発生するマスキング数の評価結果を示す。マスキング数の測定では、まず、位相揺らぎの分布と発生頻度を測定し、発生頻度が半分になる位相揺らぎ幅を求めた。次に、その値を隣接BPSK信号位相差$0.96\times10^{-5}(=\pi/2^{15})$で割った。QDSR変調度に対するマスキング数を図14に示す。QDSRがない場合($\gamma_{QDSR}=0$のとき)と比較して、2桁以上も大きくなっており、安全性が飛躍的に高まることが分かる。以上の実験結果から、ランダム化拡張としてQDSRを組み込んだ暗号送信部が所望の通りの動作をしていることを検証できた。

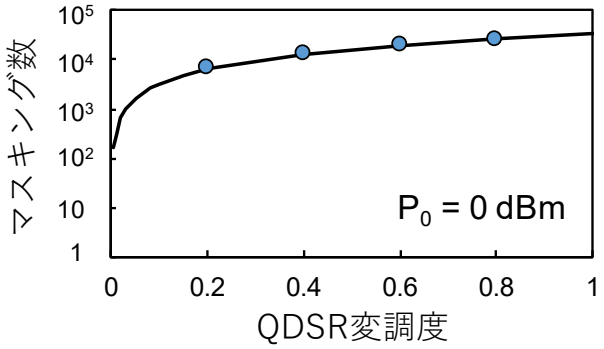


図14：マスキング数のQDSR変調度依存性。

次に、暗号通信システムの基盤となる、暗号化部と復号部を直接結合した暗号システムを実装した。図15に示すように、暗号化部は、暗号鍵と擬似乱数発生器により発生させる基底選択信号に、QDSRによるランダム性を加えて生成した電気信号で光変調器を駆動する。信号光波長は、光ファイバ通信の一般的な波長帯であるCバンド帯(1530～1565nm)の1550.1nmに設定した。復号部は、光信号を電気信号に変換するイントラダイン検波、及び暗号化部と同じ暗号基底信号発生部で構成される。QDSRによりランダム化された多値信号光の直交振幅を測定し、暗号鍵に基づき生成される基底信号に応じた位相回転量($\theta_{basis}(i)$)の逆の位相回転を施すことで、元の2値信号に復号される。復号後の信号のビット誤り率を測定し、暗号システムを評価した。ビット誤り率は、受信した信号光をメモリーに保存した後に信号処理を実施するオフライン信号処理手法を用いて求めた。図16(a)に、ビット誤り率のQDSR変調度依存性をまとめて示す。光パワーが0dBmと比較的大きい場合、QDSR変調度を大きくしても$\gamma_{QDSR}=0.6$ 程度までは、BER $<10^{-5}$と本評価の測定限界以下の十分に小さなビット誤り率だった。$\gamma_{QDSR}=0.8$ 程度になるとビット誤りが大きくなるが、それでもビット誤り率が1%を下回っていた。光パワーが-30dBmと小さい場合、受信回路で発生する熱雑音の影響が大きく、QDSR変調度が低い領域においてもビット誤り率は10^{-3}台であるものの、誤り訂正符号によりエラーフリーを実現できるとされるビット誤り率よりも十分に小さな値を達成できた。以上のように、高品質の暗号通信が可能なことを検証できた。

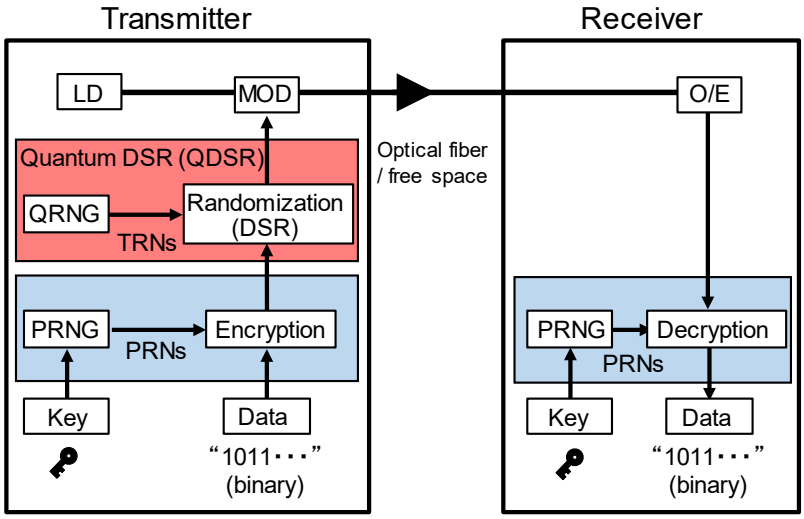


図15：構築した暗号システムの構成。

続いて、安全性評価のためにマスキング数の信号光パワー依存性を評価した。図16(b)にマスキング数の信号光パワー依存性を示す。黒い線は、QDSRを組み込まない場合のマスキング数を表している。信号光パワーが100倍になると、マスキング数は1/10になる。例えば、信号光パワーが0dBmの時、マスキング数は10程度になっている。これは、信号光が強いと安全性が低下することを示している。一方、QDSRを導入すると、信号光パワーに依存せずに大きなマスキング数を実現できることが分かる。同じ信号光パワーでは、QDSR変調度に比例してマスキング数は大きくなっている。信号光パワーとは無関係に大きなマスキング数、すなわち、高い安全性を実現できる意義は実用上極めて大きい。一般に光通信システムの信号光パワーは、通信システムの条件（伝送路の損失や受信端での所望の信号対雑音比など）により決まる。例えば、暗号通信システムの途中で光増幅器を使用しない無中継光通信システムでは、通信距離に応じて送信機出力パワーを大きな値に設定する必要がある。QDSRがない場合は、光パワーが大きいと所望の安全性を達成できなくなることがあり得る。しかし、このような場合においても、QDSRを導入することによりマスキング数を大きくすることができ、所望の安全性を達成できる。以上のように、QDSR導入により、暗号システムの安全性の向上を実験検証できた。

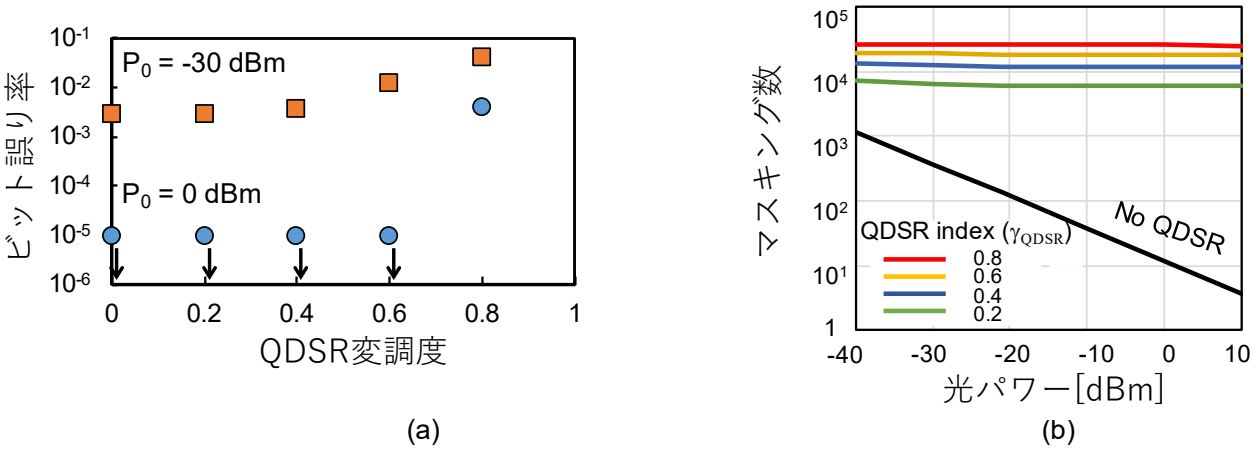


図16：(a) ビット誤り率特性のQDSR変調度依存性。■は暗号信号光パワーが−30dBm、●は0dBm。
(b) QDSRの有無による雑音マスキング数と暗号光パワーとの関係。

別の安全性評価として、盗聴者の暗号信号識別率の理論解析を行った。図11(a)のPSK信号のモデルで、信号振幅が量子雑音よりも十分大きいとした。暗号信号の電界強度をA、量子雑音量をσ、信号対量子雑音比を$\gamma = A^2/\sigma^2$とすると、盗聴者の暗号信号識別確率は、誤差関数(erf)を用いて

$$P_{EVE} = \frac{1}{2N+1} erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2N+1}{2M/\pi}\right)\right] \tag{6}$$

と表せることを導いた。基底数Mに比較してQDSR変調度が小さいとき、$(2N+1)\pi/2M \ll 1$となり、式(6)は次式のように近似でき、暗号信号識別確率がマスキング数(Γ_{BPSK})とQDSR量(N)を用いて表記できる。

$$P_{EVE} = \frac{1}{2N+1} erf\left(\frac{2N+1}{\sqrt{2}\Gamma_{BPSK}}\right) \tag{7}$$

本式より、マスキング数が大きくなると誤差関数の値が0に近づき、QDSR量が大きくなると誤差関数の係数が0に近づき、暗号信号識別確率は小さくなり盗聴者は暗号信号を正しく識別することが困難になることが分かる。数値計算例を図17に示す。QDSR量を大きくすると、盗聴者の暗号信号識別確率は小さくなり、安全性が高まる(同図(a))。QDSR量が小さい領域では、式(7)の誤差関数が支配的になり、暗号信号識別確率はマスキング数に応じた値になっている。一方、QDSRが大きくなると、誤差関数は1に近づくため、誤差関数の係数が支配的になり、盗聴者の暗号信号識別確率はマスキング数に依存しなくなる。横軸を信号光パワーにした識別確率を同図(b)に示す。QDSRを導入すると信号光パワーに依存しなくなることが見てとれる。更に、信号光パワーが−20dBmと小さい時であって

も桁違いに、信号光パワーが0dBmときは2桁以上も識別確率が小さくなり、安全性が飛躍的に高くなっている。

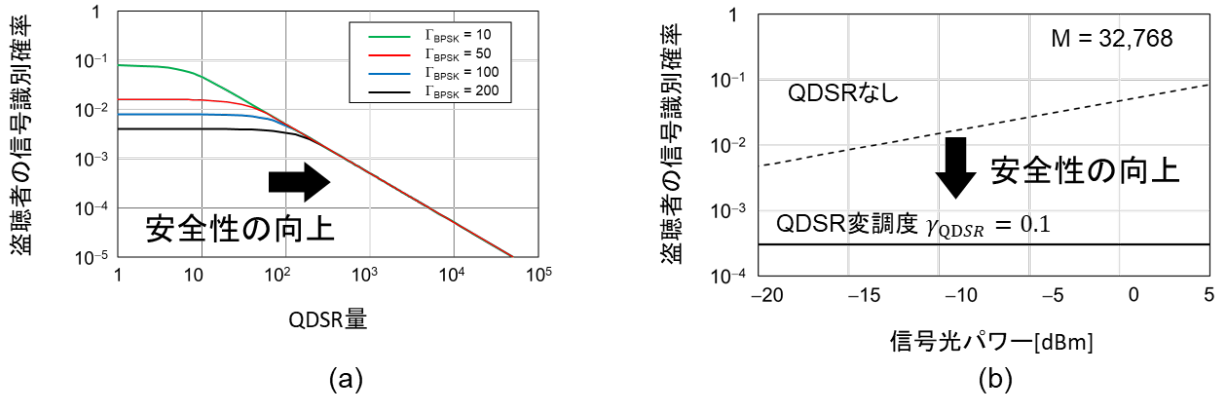


図17：盗聴者の暗号信号識別確率。(a)QDSR依存性、(b)信号光パワー依存性。

以上をまとめると、QDSRを組み込んだ量子雑音ランダム化ストリーム暗号を実現し、その安全性評価を実施し、位相変調方式の信号に対してQDSRにより80%以上の暗号信号拡散率を検証した。更に、QDSRを組み込んだ量子雑音ランダム化ストリーム暗号を実装した暗号システムを構築し、ビット誤り率が1%未満になると共に、安全性が桁違いに高くなることを実証した。

３．３　暗号通信システム評価

一般に暗号通信システムでは、盗聴者に対してデータを秘匿にし、光ファイバ回線などの通信回線で結ばれた他端にいる正規通信者に正しいデータを伝えることが要件となる。QDSRを組み込んだ暗号通信システムでは、マスキング数が大きくなると盗聴防止効果が高まるが、一方で、正規通信者の信号対雑音比の劣化を招き通信特性に悪影響を及ぼす。そのため、正規通信者が誤りなくデータ通信でき同時に安全性を向上できることを、量子雑音ランダム化ストリーム暗号を用いた暗号通信システムで検証しなければならない。そこで、QDSRを組み込んだ量子雑音ランダム化ストリーム暗号をもちいた光ファイバ暗号通信システム実験を実施した。最初に、送受信機間には光ファイバのみを接続し、途中で光増幅器を用いない無中継伝送を実施した。次に、長距離光ファイバ通信システムで一般に用いられる伝送路、すなわち、光ファイバ伝送により発生する光信号パワーの減衰を光増幅器で補償する光ファイバ増幅中継システムで実験評価を行った。以下にこれらの二つの実験結果を示す。その後、安全性向上に関して実施した理論研究結果をまとめる。

(1)無中継暗号通信システム

無中継伝送システムの構成を図18に示す。送信器と受信機の構成要素は、前述の暗号システムと同様である。レーザ光源(LD)から出力される波長1550.1nmの光が第一の変調器(MZI)で5Gb/sのBPSKデータで位相変調され、二つ目の変調器(PM)でQDSRを含めて暗号化回路で用意された基底信号で位相変調される。変調器(PM)出力は単一偏波でデータ容量5Gb/sのBPSK信号光で、多値数は2^{16}(基底数：2^{15} = 32,678)。これを偏波多重器(PolMUX)で偏波多重し、容量10Gb/sの暗号信号を用意した。光ファイバ伝送路に入力する信号光パワー(P_0)は、可変光減衰器(VOA)の減衰量で調整した。図18の送信機出力箇所に示すように暗号信号のコンスタレーションはドーナッツ状になっている。光ファイバ伝送路は、60.4kmの長さの光ファイバ(伝送損失が0.147dB/km)がボビンに巻かれた状態の光ファイバボビン6個で構成され、全長は362.4km。この光ファイバ伝送路内を伝送後、暗号信号光は受信機に入力される。受信機では、まず信号光パワーを光増幅器(EDFA)で増幅した。次に、コヒーレント受信フロントエンドとBPDでイントラダイン検波し、リアルタイムオシロスコープでAD変換しメモリーに保存した。保存したデータをオフライン方式で信号処理し、偏波分離、光ファイバ伝送路の分散補償、共通鍵を用いた復号などを行い、多値の暗号信号からBPSKデータを得た。得られたデータと送信データを比較してビット誤りを検出し、ビット誤り率を算出した。

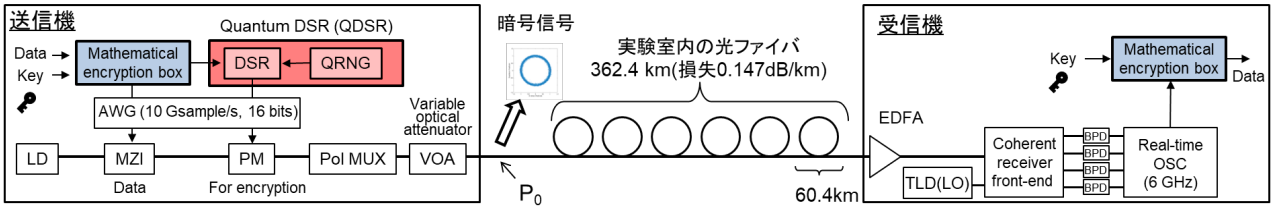


図18：QDSRを導入した光ファイバ暗号通信システム(光増幅器を用いない無中継伝送)の実験構成図

図19に、QDSRがない場合(γ_{QDSR} = 0)、QDSRがγ_{QDSR} = 0.2と0.4の場合のビット誤り率の信号光パワー依存性を示す。暗号化しない場合のBPSK信号のビット誤り率も参考に示している。グラフ内に伝送後で復号前の暗号信号のコンスタレーションと復号後のBPSK信号のコンスタレーションを示す。ドーナツ状の暗号信号からBPSK信号が復号されていることが分かる。QDSRの有無、変調度にかかわらず、信号光パワーを大きくすると、例えば、誤り訂正符号UFEC(Ultra Forward Error Correction)の閾値を下回り、362.4km無中継伝送後に十分な通信品質が得られた。暗号化・復号のないBPSK信号のビット誤り率とQDSRなしで暗号化・復号した場合のビット誤り率を比較すると、後者にわずかなパワーペナルティが生じている。暗号信号光とBPSK信号の伝送特性に本質的な違いはないので、このパワーペナルティは暗号化と復号の信号処理過程により発生しているものと考えられる。同じ信号光パワーの時、QDSR変調度を大きくするとビット誤り率が劣化しているが、正規受信者でも除去できない揺らぎがQDSRで付加されるためである。

次に、盗聴者のシンボル誤り率(SER)を評価し、本暗号通信システムの安全性を調査した。シンボル誤り率は、暗号信号レベルを正しく識別できない確率を表す。マスキング効果が全くない暗号信号は、すべての暗号信号レベルを正しく識別できるので、シンボル誤り率は0になる。一方、マスキング効果が作用すると、盗聴者は暗号信号を正しく識別できなくなり、シンボルの識別の誤りが生じる。SER = 1 になると、全ての暗号信号を正しく識別できないことになる。図19(b)に、無中継暗号通信システムの盗聴による盗聴ポイントでのシンボル誤り率を示す。通常の量子雑音ランダム化ストリーム暗号をもちいたシステムでは、シンボル誤り率は送信機の出力直後が一番小さく安全性が低く、伝送するにつれてシンボル誤り率は大きくなり安全性が高まる。これは、式(3)で示したように、伝送路を暗号信号が伝搬するにつれて信号光パワーが小さくなり、その結果、マスキング数が大きくなるからである。送信端付近では、シンボル誤り率は0.9を下回っている。すなわち、暗号通信システムの安全性の上限が、送信端直後の安全性で決定される。一方、QDSRを組み込むと、図19(b)に示すように送信機直後でもシンボル誤り率はほぼ1となり、暗号通信システムの送信端から受信端までのいずれの箇所において、シンボル誤り率はほぼ1となり、暗号通信システム全体の安全性を大幅に向上できた。

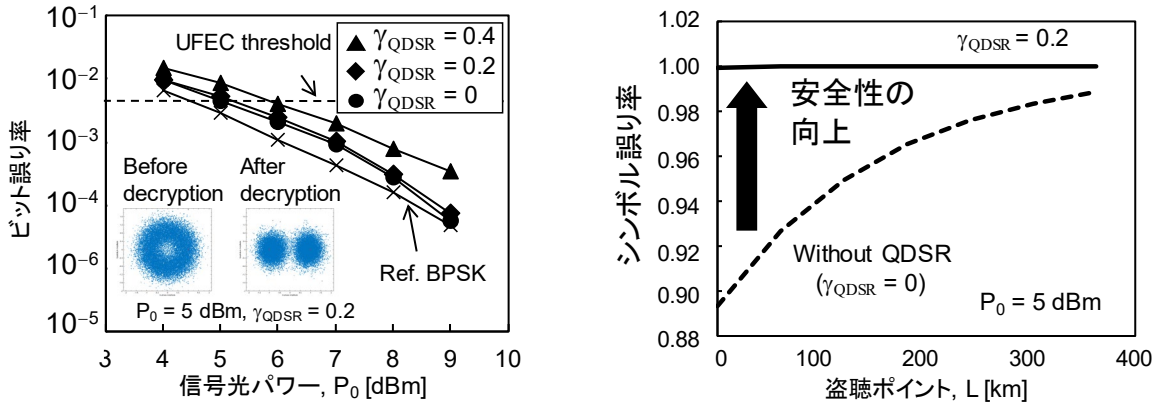


図19：QDSRを組み込んだ光ファイバ暗号通信システム(光増幅器を用いない無中継伝送)の評価結果。(a)ビット誤り率の伝送路入力光パワー依存性。(b)伝送路の盗聴場所におけるシンボル誤り率。

(2)光ファイバ増幅中継暗号通信システム

信号光が光ファイバ内を伝送すると、レイリー散乱による損失などの光ファイバ固有の損失や光ファイバの曲げ損失などのシステム組み込みによる損失を受け、信号光パワーは減衰する。典型的な減衰量は0.2dB/kmで、光ファイバを15km伝送すると光パワーが半減する。そのため、長距離通信システムでは、弱くなった光を光のまま増幅する光増幅器を用いて信号光を中継する。前述の通り、無中継暗号通信システムで360km以上の暗号通信に成功した。本研究で対象としている量子雑音ランダム化ストリーム暗号の特徴のひとつは、量子技術を使っているにもかかわらず光増幅中継が可能なことで、光増幅中継により長距離通信することができる。最長の通信距離は、我々が2021年に発表した、約50km毎に光増幅器で中継するシステムで日米間の太平洋横断距離に相当する1万km強である。

本研究では、QDSRを導入した量子雑音ランダム化ストリーム暗号でも、光増幅中継器を用いて、増幅中継ができることを世界で初めて検証した。当初の計画では、実験室内の光ファイバボビンを伝送路とした検証実験を計画していたが、構築した暗号信号の送受信機動作の安定性が予想以上に高かったので、目標以上の計画に変更し、より高い通信性能と耐環境特性などが求められる屋外敷設光ファイバ回線で通信実験を行った。

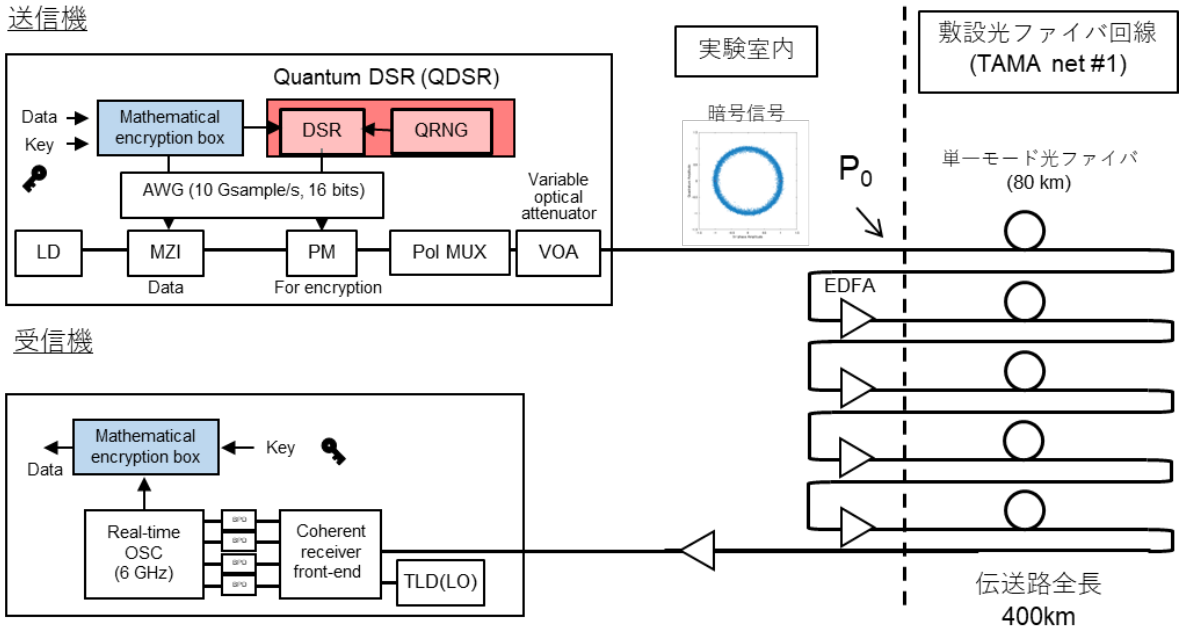


図20：光ファイバ増幅中継暗号通信システムにおけるQDSRを組み込んだ量子雑音ランダム化ストリーム暗号の通信実験構成の概要

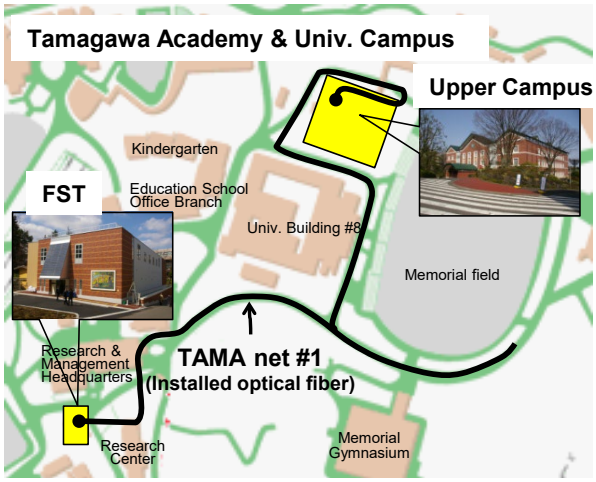


図21：屋外敷設光ファイバ回線(TAMA net #1)

表1：光増幅中継伝送システムの伝送実験条件

変調方式	BPSK
通信容量	10Gb/s（偏波多重）
基底数	2^{15}（=32,768）
QDSR変調度	0.2
通信距離 （中継間隔）	400km （80km）
伝送路入力パワー	-19dBm

実験系構成を図20に示す。伝送路の光ファイバ回線(単一モード光ファイバ)は、図21に示すように本学キャンパス内の地下に敷設されている。主な実験条件を表1にまとめて示す。送受信機構成は前述の無中継暗号通信システムの構成と同じで、送信端では5Gb/sで単一偏波のBPSK信号を10Gb/sに偏波多重し、受信端ではイントラダイン検波とオフライン信号処理で暗号信号からBPSK信号を復号・復調した。伝送路は、敷設光ファイバ回線で80km伝送毎に光増幅器(EDFA)で信号光を増幅中継した。合計5回増幅中継する構成にし、通信距離は400km。

図22(a)の左側に400km伝送後の暗号信号のコンスタレーションを示す。伝送前のコンスタレーションは図20の伝送路入力付近に示してあるように雑音が少ないが、増幅中継伝送により信号対雑音比が劣化している。正規受信者は鍵を用いて、この暗号信号から2値信号を復号できる。同図(a)の右側に、暗号鍵を用いて復号したBPSK信号のコンスタレーションを示す。2値にきれいに復号されていることが見てとれる。若干縦長になっているが、これはQDSRの影響である。復号したBPSKから算出されたビット誤り率は8.1×10^{-5}と小さく、光増幅器を用いた光増幅中継システムでも、QDSRを導入した量子雑音ランダム化ストリーム暗号による暗号通信が可能なことを検証できた。

安全性の評価も実施した。マスキング数を図22(b)に黒線で示す。400kmの光ファイバ回線全域においてマスキング数は6,000以上の大きな値に保つことができた。これは、盗聴者の暗号信号識別確率に換算すると、10^{-4}程度と十分小さく、全回線において高い安全性を実現できた。比較のために、QDSRを導入していない量子雑音ランダム化ストリーム暗号の場合のマスキング数を青線で示しているが、本手法は桁違いに安全性が高くなっていることが分かる。

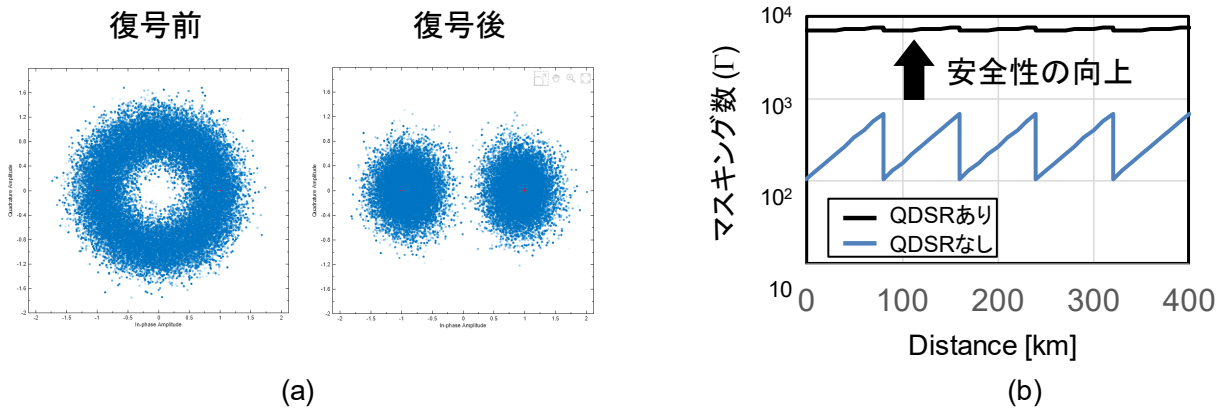


図22：QDSRを組み込んだ光ファイバ暗号通信システム(光増幅器を用いた中継伝送)の評価結果。(a)400km伝送後の復号前後のコンスタレーション、(b)伝送路の各地点でのマスキング数。

以上の実験検証により、QDSRを組み込んだ量子雑音ランダム化ストリーム暗号は、光増幅器を中継に利用した光ファイバ通信システムに応用可能であり、通信容量10Gb/sで400km伝送することに成功した。この実験結果から、本研究の所期の目標が達成されたと結論づけられる。屋外敷設光ファイバ回線で検証できたことは、当初の目標を上回る成果である。

(3)安全性向上の評価理論

以上の暗号通信システムの安全性の評価にはマスキング数，シンボル誤り率，ビット誤り率が利用される。評価理論の検討結果から導かれるこれらの意味と有効性を以下にまとめる。

当初、実験を通じて測定可能な物理パラメータによる安全性評価式の導出を目論み、本研究の主題である量子雑音ランダム化ストリーム暗号の安全性解析における適切なアプローチとそこでの諸原理の役割について考察した。情報理論における情報の取り扱いから解き始めることで、本研究で扱う暗号通信システムの解析においてはシャノンの通信モデルにおける通信路行列を分岐点として、量子信号検出理論を主体として物理を通じた解析が主となる部分と、暗号解読アルゴリズムのような論理的な解析が主となる部分とに分離したアプローチによってシステム全体の解析と評価を進めることが基本方針として適切であるとの考えに至った。マスキング数とシンボル誤り率は物理が主

となる部分の解析の中での解析対象物であり、ビット誤り率は論理が主となる部分の中での中心的な解析対象物である。両者の関係を論じるためには通信路行列の適切な見積もりが必要であり、このことから物理と論理を分離したアプローチを取る場合、物理が主となる部分を論理が主となる部分に先行して解析する必要があることを明らかにした。物理が主となる解析ではいくつかの基本原理（レーザ光の非直交性、減衰通信路通過後の光の状態、量子非複製定理、光増幅器の基本定理、量子信号識別限界、など）から、QDSRのような量子ランダム化拡張技術を付与する前のシステムにおけるマスキング数及びシンボル誤り率が付与した後のシステムのそれらより劣化しないことが導かれる。

そこで、量子信号検出理論に基づいて盗聴者能力を推定するための計算を実施した。量子信号検出理論における準最適な受信機におけるエラープロファイルを計算し、それに基づき量子雑音由来のマスキング数とシンボル誤り確率を計算した。同等の計算はホモダイン／ヘテロダイン測定でも実行できる。こうした計算を通じて量子雑音ランダム化ストリーム暗号の根源的な安全性は準備された信号間の量子力学的非直交性に起因することが示唆されていることから、多値光信号の非直交性を定量的に把握するための指標（非直交度，NOI）を定義するに至った。これは、すべての光信号が量子力学的に直交する場合に0となり、反対にどの信号を受信しているかの識別が全くできないほどに非直交性が強くなるにつれて1に近い値を返す指標となっている。本研究では専ら位相変調方式（PSK）の信号系を用いているため、その場合の非直交度を図23に示す。この図が示すように、光パワーが通常の光通信システムで用いられている程度に大きくても、換言すると、平均光子数が非常に多くても、信号の数が増えるにつれて非直交度は1に近づいていくことが分かった。

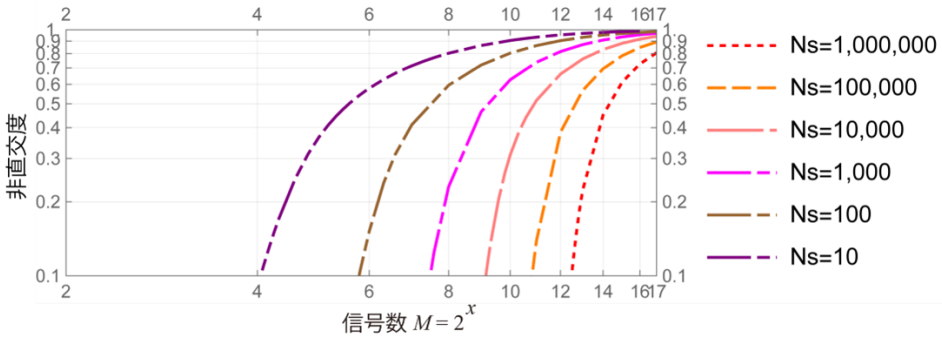


図23：非直交度の多値度依存性。

また、同じ状況で非直交度が1に近づくにつれて量子通信路容量が減少することも確認した。このことは、判別距離による評価と関係している。判別距離を大きくするには盗聴者にもたらされる情報量を小さくする必要がある。したがって、信号数の適切な設定によってもたらされる量子通信路容量の減少によって判別距離が増加することが見込まれる。さらに、QDSRのような量子ランダム化拡張技術はそれが付与されていない場合に比べて、盗聴後に追加の情報処理を強制することから量子通信路容量がさらに減少し、それゆえに判別距離はより大きくなることが見込まれる。しかしながら、先行研究で導出されている判別距離の下界はQDSRが組み込まれた場合も含めて本研究で現れる状況に対して形式的に適用可能であるものの、その導出過程を考慮すれば粗い評価量である。また、より厳密な判別距離を導出するためには、鍵のある状況での情報量最大化問題を解決する必要があるが、量子信号検出理論における情報量最大化問題は難問として知られている。そこで、判別距離に代わるより直接的で厳密な評価を目指して最適量子受信機で盗聴した際の情報ビット検出確率を数値計算によって評価した。ここでの最適量子受信機は誤り率を基準として理論物理学上許容される最高性能を持つ受信機であり、実験評価で用いられるホモダイン受信機よりも当然ながら信号検出能力は高い。また、情報ビット検出確率は、盗聴者のビット誤り率と表裏一体の関係にある。図24(a)に、正検出確率P(0|0) が1 から、そして誤検出確率P(1|0) が0 から，Mの増加に伴いそれぞれ1/2へ収束する様子を示す。同図(b)に正誤の検出確率の差Δ = |P(0|0)−P(1|0)| がMの増加に伴い単調に減少する様子を示す。図24の各図で(i)盗聴信号の平均光子数n = 100、(ii)1,000、(iii)10,000、(iv)100,000、(v)1,000,000。全体の傾向として、盗聴信号の平均光子数nが一桁上がると同じ検出確率をもたらすMはおよそ3.1 倍になる。十分大きなM（つまり十分大きな暗号化基底

数M）を設計時に選択すれば，盗聴信号の平均光子数nが非常に大きく、しかも盗聴者が最適量子受信機を利用してもΔ ≈ 0，P(0|0) ≈ P(1|0) ≈ 1/2 となることが示された。つまり、信号元数の増加で確実に盗聴者を全数探索の状況に追い込める。これらの結果をQDSRが組み込まれた量子雑音ランダム化ストリーム暗号の通信システム評価実験に当てはめると、QDSRは正規受信者の復号性能を担保しながら，盗聴者のビット誤り率特性を劣化させる効果があると言える。

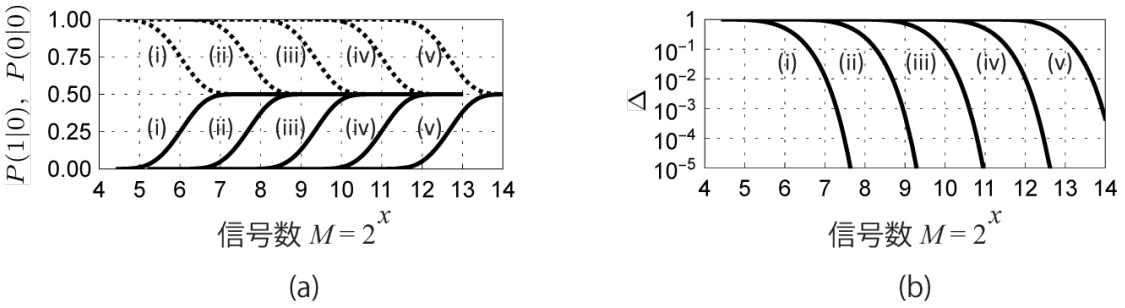


図24：最適量子受信機による(a)情報ビット正検出確率P(0|0)と誤検出確率P(1|0)、(b)両者の検出確率の差。

以上の安全性向上に関する理論検討をまとめると、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の整理をし、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。

４．委託業務全体の成果

４．１　計画時に想定していなかった成果（副次的成果）や、目標を超える成果

目標を超える成果がふたつ得られた。ひとつは、屋外に敷設してある光ファイバ回線で暗号通信システムの検証に成功したこと。目標では、実験室内のボビンに巻かれた光ファイバ素線を用いて、暗号通信のシステム実験を行う計画だった。実験室内の光ファイバ素線は環境変化がないので安定で均一な伝送路になる。しかし実利用されている通信システムは屋外に敷設されている光ファイバ回線を利用する。屋外敷設光ファイバ回線の安定性は、温度変化、道路沿いに敷設されている場合は自動車などの走行に係る不規則な振動など様々な環境変化により、大きく変動する。そのため、このような変動があっても通信できることが実用化には不可欠である。今回構築した暗号システムの安定性は当初の予想を大きく上回っていたので、目標を変更し屋外敷設光ファイバ回線で実験するという高い目標に挑戦し、通信容量10Gb/sで400kmの暗号通信に成功した。ふたつ目は、量子乱数をリアルタイムで発生できたこと。当初の計画では、オフライン方式での動作検証だったが、研究を進めた結果、発生する乱数のランダム性の時間依存性が極めて重要な評価指標になることが分かった。そこで、大規模な行列演算である乱数抽出処理を高スループットで実現する並列処理などを設計・実装し、発生速度50Gb/sという高速で乱数のリアルタイム発生に成功した。

４．２　研究課題の発展性（間接的成果を含む）

本研究では、QDSRをもちいることにより、通信データを守る量子雑音ランダム化ストリーム暗号の安全性を高められると同時に、光信号パワーに依存せずに暗号通信システム全体の安全性を高い状態に保てることを明らかにした。その過程で、リアルタイムで50Gb/sという高速発生可能な量子乱数発生器を実証した。本研究では、量子乱数発生器は量子雑音ランダム化ストリーム暗号の安全性向上に利用したが、サイバーセキュリティを中心に様々な用途が期待される。更に、現状、バルク部品で構成されているので、光集積回路技術などによる小型化も期待される。暗号通信システムの検証は、限られた経費で多くの成果が得られるように、安価で実証できるオフライン方式で実施した。実利用に向けて、リアルタイム方式での動作検証が期待される。本研究では光ファイバ通信に限定したが、空間光通信への応用も期待できる。

４．３　研究成果の発表・発信に関する活動

研究成果等の状況に記載の通り、国内外での学会発表、和文論文誌や英文論文誌で発表、プレス発表の他、本学HPに研究成果を掲載し、本研究の成果発信に努めた。

５．プロジェクトの総合的推進

５．１　研究実施体制とマネジメント

本プロジェクトに参画する全ての研究者が出席する定例会議を毎月開催し、研究進捗の共有、研究計画の効率化、研究手法の合理化などを検討し、目標達成までのロードマップを更新しながらプロジェクトを推進した。

５．２　経費の効率的執行

通信装置、光部品、電子部品など既に所有しているもので代用できるものは流用した。光ファイバ通信実験では、光ファイバを購入せず国内ファイバメーカから借用した。学会出張・発表は、光通信関連でトップレベルの会議のみに限定した。

６．まとめ、今後の予定

本研究では、予測不可能性の高い乱数を高速で発生する量子乱数発生手法を提案し、オフライン信号処理方式で発生速度 100Gb/s、リアルタイム信号処理方式で発生速度 50Gb/s の乱数発生を実証した。量子雑音揺らぎを利用した乱数発生では世界最速の発生速度である。次に、通信データの安全性向上を目的に、本手法で発生させた乱数を用いて予測不可能性の高い揺らぎを付加した、量子雑音駆動型 DSR（QDSR）付きの新たな量子雑音ランダム化ストリーム暗号を実現した。更に、通信容量 10Gb/s で通信距離 362km の無中継光ファイバ暗号通信システムに本暗号を適用し、高い通信性能と安全性が同時に実現されること検証した。また、屋外敷設光ファイバ回線を用いて光増幅器で暗号信号を中継する光ファイバ増幅中継暗号通信システム実験にも適用し、通信容量 10Gb/s で 400km の通信に成功すると同時に、光ファイバ通信システムの送信端から受信端までのすべてにおいて桁違いに安全性が高められていることを検証した。安全性向上評価理論研究も実施し、マスキング数や盗聴者のシンボル誤り率が評価指標として有効であることを明らかにし、実験検証の安全性向上を本指標で評価した。

量子乱数発生は、量子雑音ランダム化ストリーム暗号の安全性向上に利用したが、今後、サイバーセキュリティを中心に様々な用途が考えられる。現状はバルク部品で構成されているので、光集積回路技術などによる小型化、また高速化は今後の課題である。QDSR 付き量子雑音ランダム化ストリーム暗号は、本研究では限られた経費で多くの成果が得られるように、全てオフライン信号処理方式で検証したが、実利用に向けてリアルタイムでの動作検証が課題である。また、量子計算機でも解読できない耐量子計算機暗号による認証・鍵交換と本暗号によるデータ通信を統合した高安全な暗号通信システムの開発も考えられる。加えて、本研究では光ファイバ通信システムへの適用のみ実証したが、空間光通信への適用も考えられる。

７．研究発表、知的財産権等の状況

（１）研究発表等の状況

種別	件数
学術論文	6件
学会発表	12件
展示・講演	該当なし
雑誌・図書	該当なし
プレス	1件
その他	該当なし

（２）知的財産権等の状況

発明の名称	発明者	出願登録区分	出願番号 （出願日）	出願区分	出願国	登録番号 （登録日）
乱数発生装置	加藤研太郎、二見史生、谷澤健	出願	特　願　2021-26425(P2021-26425)(2021年2月22日)	国内	日本	

（３）その他特記事項

該当なし