3　量子光ネットワーク技術
3-1　量子鍵配送ネットワーク研究開発の現状

藤原幹生　佐々木雅英

将来の暗号解読の脅威のない安全な通信を実現できる量子鍵配送（QKD）技術を紹介する。QKDの安全性は物理法則により担保され、世界各国で開発が進められている。QKDは基本的には1対1での使用が原則であるが、QKDによるネットワークを構築し、より利便性の高いシステムとして提供できるネットワークアーキテクチャをNICTを中心として開発を進めている。本稿ではQKDの原理、実装の概要とネットワークアーキテクチャを紹介する。

1　まえがき

近年、パソコン、家電、自動車、ロボット、スマートメーター等のあらゆる物がインターネットに接続され、様々な情報がビッグデータとして蓄積され誰でもアクセスできる環境、いわゆるIoT（Internet of Things）が急速に普及しはじめている。IoTにより実空間とサイバー空間の融合が高度に深化した社会では利便性の反面、攻撃者が容易に悪意のあるソフトウェア（いわゆるマルウェア）によるサイバー攻撃を仕掛けられる状況にあり、実際、国家の関与が疑われるような組織的かつ高度な攻撃手法の登場が、国民生活・経済・社会活動に重大な被害を生じさせ、我が国の安全保障に対する脅威も年々高まってきている。現在、我々が日常のネットサービスでも使用している公開鍵暗号や共通鍵暗号は、解くのが難しい数学問題に基づいて安全性保証を行っている。このような数理暗号は、計算技術の進展に比例し安全性の危殆化の懸念が増大する。特に、元になる暗号鍵が破られると、それに基づくすべての暗号機能の安全性が瓦解してしまう。例えば、最も標準的に使われている公開鍵暗号のRSA暗号の安全性は、素因数分解問題の困難さに基づいているが、鍵長1024 bitの仕様は既に解読の危険域に達し、鍵長2048 bitへの移行が進んでいる[1]。ここで感取すべきことは、暗号システムの更新作業にはハードウェアへの負担の増加が伴うという点である。例えば、1024 bitと2048 bitを比較した際、5～30倍の処理能力が必要になり、一般ユーザの環境ではパフォーマンスが低下する恐れがある。また、たとえ2048 bitへの更新を完了したとしても、暗号アルゴリズムの解読に関する数学的新発見があれば、その暗号方式は機能しなくなる。最悪、既に解読されている方式を使い続けている可能性も否定できない。

また、盗聴者は、今は解読できなくても、通信路を行きかうデータをコピーし入手後いったん保存しておき、将来、何らかの方法で暗号化に使われた鍵を入手したり、新しい解読技術を手にした時点で、保存していた暗号化データを解読して重要情報を知る可能性もある。例えば、Edward Snowdenが暴露した、いわゆるスノーデンファイルでは、アメリカの諜報機関がインターネット上の暗号化されたデータを将来の解読に備えて記録しているとしている。実際、欧米の諜報機関が光ファイバー網上で大規模な盗聴を長期間にわたって行っていたことが知られている（2013年、ガーディアン紙やワシントン・ポスト紙）。そこで用いられた技術は、光スイッチや光ファイバーの診断を行う際に使われるタッピング装置である。現在では、小型のタッピング装置が市販されており、そのまま光盗聴器として転用できるものである。実は、わざわざ特殊な装置でタッピングしなくても、最新の光子検出器を用いると光ファイバー内を行きかう信号の様子が見えてしまうことも分かってきた[2]。光ケーブルをある程度曲げるだけで、ケーブル内の隣り合う光ファイバーの間で光信号が漏れてしまう、いわゆる光ファイバー間クロストークという現象である。これらの事実は、将来にわたって担保できる秘匿性、いわゆる『フォワードシークラシー』（Forward secrecy）を持った暗号技術の必要性を強く示唆している。

それらの眼前の危機に対し、量子鍵配送（Quantum Key Distribution: QKD）は、理論上、いかなる能力をもった第三者（盗聴者）にも情報を決して漏らすことなく暗号鍵を離れた2地点間で共有する方法であり、ベネット（C. H. Bennett）とブラサール（G. Brassard）によって1984年に提案された[3]。この方式はBB84プロトコルと呼ばれている。提案から約10年程はあまり大きな関心を集めなかったが、1994年に素因数

分解問題や離散対数問題を効率的に解く量子計算アルゴリズムが発見され[2]、現在インターネット上で使われている鍵交換方式や暗号化方式に対する新たな脅威が現れたことで、一躍脚光を浴びることとなった。

QKDの安全性は、解くのが難しい数学的問題に基づくものではなく、搬送信号が従う量子力学という普遍の物理法則に基づくものである。QKDでは0、1の乱数列の情報を、量子力学的性質を適切に制御した信号へ符号化して送信、通信路上での測定（いわゆる盗聴）行為はそのような信号状態に必ず痕跡を残すという性質（不確定性原理）と、量子状態は誤りなくコピーを作ることができないというno-cloning（コピー不可能）定理を利用して、共有した乱数列から盗聴可能性のあるビットデータを排除することで、盗聴の恐れのない安全な乱数列を共有することができる。実際、『物理法則上許されるどんな技術でQKDの通信を盗聴したとしても、適切な信号処理（鍵蒸留処理）によって盗聴者への漏洩情報量を幾らでも小さくすることができる』ということを情報理論的手法によって証明することができる。盗聴者の能力に対する一切の仮定が無いという意味で、QKDは『無条件安全』な鍵配送であると言われる。このようにして共有した暗号鍵を、送信したい平文と同じデータサイズだけ用意し、平文のビットデータと排他的論理和を取って暗号文を生成して送信、一度使った暗号鍵は二度と使いまわさないように運用することで（所謂Vernam’s one-time pad: OTP）、いかなる能力の計算機や将来の技術でさえも解読できない暗号化通信を実現することができる。

これまで様々な機関によって研究開発が行われ、BB84プロトコル以外にも新しいプロトコルが次々と発案されるとともに[4][5]、安全性証明や理論解析手法が進展し装置性能も向上してきた。2000年代後半から欧米で幾つかのベンチャー企業が誕生し、QKD装置の商用化に成功している[6]–[8]。2005年には、アメリカ国防総省・国防高等研究計画局（DARPA）の支援を受けたプロジェクト（The DARPA Quantum Network）が世界初の都市圏QKDネットワークをボストン地区に構築した。3地点を結ぶリング型のネットワークで、鍵生成レートは約10 kmの敷設ファイバー上で毎秒1,000 bit（1 k bits per second:1 kbps）程度であった[9]。2008年には、欧州連合の研究開発プロジェクトSECOQC（Secure Communication based on Quantum Cryptography）がウィーン市内に6地点を結んだ都市圏QKDネットワークを構築し、様々な異なる方式のQKD装置の相互接続の実証デモに成功した。典型的な鍵生成レートは、約30 kmの敷設ファイバー上で1 kbps程度であり、音声の暗号化通信などが実証された[10]。その後、欧州ではSECOQCの成果を核にして、欧州電気通信標準化機関（ETSI）においてQKDの標準化に向けた取組を進めている[11]。

我が国では、2001年から総務省とNICTが産学官連携プロジェクトを推進し、それまでのQKD装置の鍵生成レートを一気に100倍向上させ、2010年には産学官連携チームが東京圏に6つのノードからなる鍵交換網のテストベッド『Tokyo QKD Network』を構築し、世界で初めてQKDによる動画の秘匿伝送の実証に成功した[12]。

2011年度から2015年度の5年間はNICT委託研究「セキュアフォトニックネットワーク技術の研究開発」（No.157）というプロジェクトの下で、QKDシステムの試験運用と安全性評価技術の研究開発が行われた[13]。また、QKDネットワークから供給される暗号鍵を用いた新しいアプリケーションの開発も行われており、これまでにネットワークスイッチ[14] [15]、スマートフォン[16]、ドローン[17][18]など様々な情報通信機器へのアプリケーションインターフェースが開発されている。鍵配送機能と鍵管理機能のほかに、様々なアプリケーションインターフェースを搭載したネットワークソリューションのことをQKDプラットフォームと呼んでおり、既にTokyo QKD Network上で試験運用されている。ユーザはその詳細な中身を知らなくても、ニーズに応じた規模のQKDプラットフォームをブラックボックスとして導入しアプリケーションインターフェースを情報通信機器にインストールすることで、既存のセキュリティシステムの機能はそのまま維持しつつ、いかなる能力の計算機や将来の技術でさえも盗聴・解読できない暗号鍵を様々な情報通信端末間で交換できるようになり、システム全体のセキュリティを強化することができる。

2015年には、テストベッド環境下での評価試験を経たQKD装置をユーザ環境下に移設し、実用レベルでの評価実験が始まっている。例えば、日本電気（株）（NEC）は都内某所にあるサイバーセキュリティ対策の中核拠点「サイバーセキュリティ・ファクトリー」でサイバー脅威情報の暗号化通信に向けた評価実験を2015年7月から行っており[19]、2016年度末まで継続したのち、ImPACTプロジェクトの量子セキュアフォトニックネットワークチームに引継がれ、研究開発を行っている。

（株）東芝は仙台市の東芝ライフサイエンス解析センターと東北大学東北メディカル・メガバンク機構間の7 kmの回線でゲノム解析データの暗号化通信実験を2015年8月から行っており[20]、2017年8月まで継続中である。これらのQKD装置は、海外のベンチャー企業の製品より鍵生成レートにおいて50倍以上高速であり、光損失率0.2 dB/kmの標準的な光ファ

イバーでは伝送距離 50 km で約 1 Mbps、東京圏の実際の敷設環境での商用ファイバー（平均光損失率 0.5 dB/km 程度）では伝送距離 50 km で数 100 kbps である。一方、近年、中国では中国科学技術大学が主導する国家プロジェクトが北京市、済南市、合肥市、上海市にそれぞれ 50 ノード規模の都市圏 QKD ネットワークを構築し、さらにそれらを計 32 個の中継ノードでリレーにより結ぶ総延長 2,000 km の QKD バックボーンを構築し、国家スケールの超高秘匿通信インフラを完成させつつある [21]。またアメリカでは、バテル（Battelle）社がスイスのベンチャー企業 id Quantique 社と共同で 700 km に及ぶ都市間 QKD ネットワークを構築し、非営利団体にオープンテストベッドとして開放する計画を発表している [22]。

このように QKD 技術は、都市圏や都市間スケールの実環境で試験運用される段階に達している。今後、実環境での QKD プラットフォームの運用実績と安全性評価に関する知見を蓄積しながら、超高秘匿通信インフラとしての実用性を高めてゆく必要がある。本稿では QKD の簡単な説明と、NICT が中心となって開発を進めている QKD ネットワークアーキテクチャを紹介する。

2　QKD の動作原理

2.1　QKD プロトコルと原理

QKD では、送信者は乱数列のビット情報 0、1 を適切な量子信号に符号化して送り、受信者は適切な測定法を用いて量子信号を受信する。量子信号は、少なくとも 2 つ以上の非直交状態を含んでいなければならない。以下、本稿では、代表的な QKD プロトコルである BB84 を例にとって説明する。プロトコルの概要を図 1 に示す。暗号分野においては、慣習的に、正規の送信者を Alice（アリス）、受信者を Bob（ボブ）、盗聴者を Eve（イブ）と呼ぶ。以下では、この慣習に従う。また、量子信号として単一光子の偏光状態を用いる場合を例にとって BB84 プロトコルの概要を説明する。

BB84 プロトコルでは、2 種類の偏光状態のセット、つまり、水平、垂直偏光の Z 基底 {|H⟩, |V⟩}、右斜、左斜偏光の X 基底 {|45°⟩, |−45°⟩} を用意する。{|H⟩, |V⟩} は {|Z0⟩, |Z1⟩} と、{|45°⟩, |−45°⟩} は {|X0⟩ , |X1⟩} と表記してプロトコルの記述を行う。送信者（アリス）は、乱数表の各ビット情報 0、1 を光子に符号化する際、Z 基底、X 基底の中からどちらか 1 つをランダムに選択して、0、1 をそれぞれ対応する偏光状態へ符号化する。したがって、送信する量子信号は、{|Z0⟩ , |Z1⟩, |X0⟩, |X1⟩} の 4 つの成分からなる。それぞれの基底内での状態ベクトルは互いに直交するが、Z、X の基底間での状態ベクトルは非直交状態となる。実際、その内積は

$$\langle Z0|X0\rangle = \langle Z0|X1\rangle = \frac{1}{\sqrt{2}} \tag{1}$$

$$\langle Z1|X0\rangle = \langle Z1|X1\rangle = \frac{1}{\sqrt{2}} \tag{2}$$

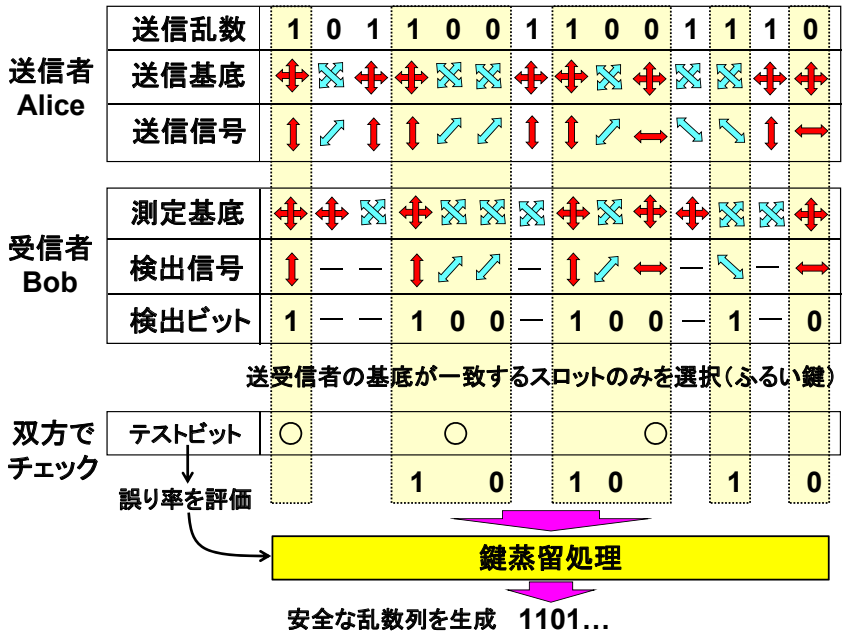

図 1　偏光を用いた場合の BB84 プロトコルの概要（送受信者間でのビット情報や基底情報の対応表）

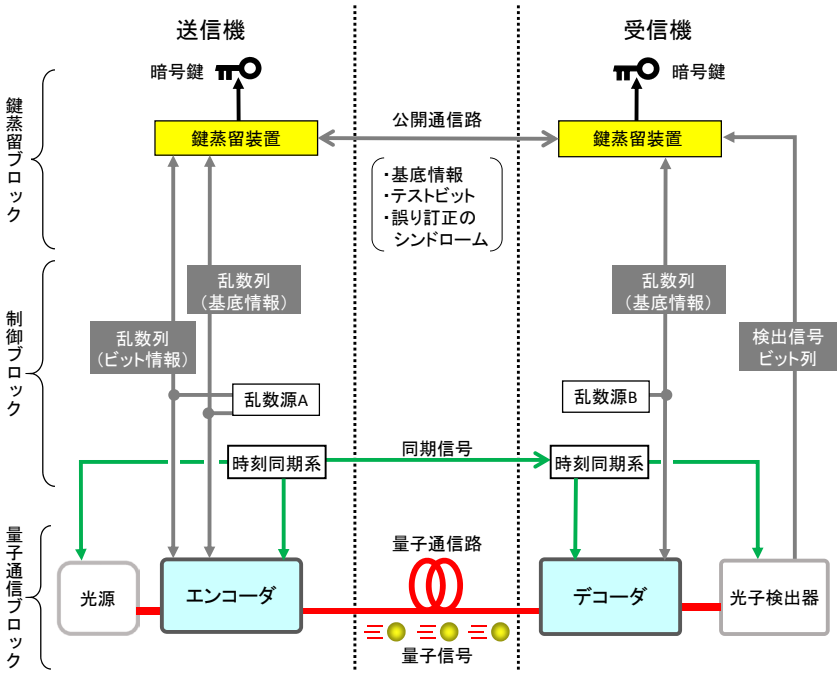

図２　QKD リンクのブロック構成図

となる。図２に送受信者間でのビット情報や基底情報の対応表の簡単な例を示す。

受信者（ボブ）は、Z 基底、X 基底の中からどちらか１つを（送信者とは独立に）ランダムに選択し、光子を測定する。量子通信路内での光損失のため、光子が検出されない時間スロットも出てくる。なお、量子通信路内では雑音も存在し、送信状態とは異なる状態で検出される場合もあるが、図１中では、そのような場合は省略している。

この量子信号の伝送後に、アリスとボブはビット情報が０だったか１だったかは伏せておき、実際に用いた基底が Z だったか X だったか（基底情報）のみを、公開通信路を介して交換し合い、アリスとボブの基底が一致するスロットのみを選択する（基底照合）。これによって残るビット列のことをふるい鍵という。次に、ふるい鍵の一部をテストビットして抜き出してアリスとボブの間で突合せ、ビット誤り率を評価する。

もし、量子通信路への盗聴があれば、それはビット誤り率の上昇となって現れる。それは、イブがどんなに盗聴法を工夫して量子通信路を流れる非直交状態の系列をコピーし、情報を得ようとしても、非識別性定理やコピー不可能定理のために、ボブへ再送した系列には必ず誤りが生じてしまうためである。アリスとボブは、それをふるい鍵からランダムに選んだテストビットを突き合わせることによって盗聴を見抜く仕組みとなっている。

実際にはイブが居なかったとしても、量子通信路に雑音がある場合には、やはりビット誤り率が高くなるが、これがイブによるものか雑音によるものか区別する方法は無いので、量子通信路の雑音はすべてイブによる効果であると考える。

アリスとボブはテストビットのビット誤り率の結果を基に盗聴可能性の有無を判定し、盗聴可能性が無いと判断した場合、さらに、ビット誤り率の値に応じた適切な鍵蒸留処理を行うことにより、最終的に安全な乱数列を抽出して暗号鍵とする。

2.2　QKD リンクの構成

QKD リンクは、光子を介して乱数のデータを共有するための『量子通信ブロック』、共有した乱数データから安全な暗号鍵を取り出す『鍵蒸留ブロック』及びこれらを制御する『制御ブロック』からなる。制御ブロックは、量子通信ブロックと鍵蒸留ブロックに乱数列を供給するとともに、量子通信ブロックに同期信号を供給して時刻同期をとる。その大まかなシステム構成を図２に示す。同期信号は、物理的にはアリスが量子信号とうまく多重化してから量子通信路内を経由してボブに送る場合が多い。以下に、量子通信ブロックと鍵蒸留ブロックの詳細について説明する。

・量子通信ブロック

量子通信ブロックは、光源、エンコーダ、量子通信路、デコーダ、光子検出器からなり、同期信号を介して時刻同期しながら量子信号の伝送を行う。

光源としては、単一光子源ではなくレーザ光源を使うことが多い。実際、レーザ光パルスでも、以下で述

べるような制御を行うことで長距離の QKD を実現できる。まず、送信側での制御として、以下の 4 つの処置を施す。

(i) 微弱レーザ光：レーザ光を減衰させ、パルスあたり 2 光子以上含まれる確率が充分小さい微弱なパルスにしてから通信路に入れる。

(ii) 位相乱雑化：各ビットの状態間に位相相関が生じないよう光源あるいは変調器を制御する。

(iii) デコイ法 (Decoy method)：どうしても消しきれない複数光子成分による伝送性能の劣化を防ぐため、鍵生成に使う信号パルスの他にそれとは異なるレーザ光強度のパルス (おとりパルス、あるいはデコイパルス) をランダムに入れ込む。

(iv) タイムビン信号 (Time-bin signal)：2 つのパルスのペア (タイムビン) [23] を生成し、そのペアにビット情報と基底情報を符号化する。

(i) は単一光子を主成分とする状態を作るための要件である。(ii)、(iii) は伝送性能を伸ばすための要件である。(iv) は、量子通信路が光ファイバーの場合に考慮すべき要件である。タイムビン信号は偏光信号よりも光ファイバー内で起こる擾乱の影響をより効果的に抑制することができる。実際、2 つのパルスがほぼ同じ擾乱を受けるため、受信側で 2 つのパルスをうまく干渉させてから光子検出することで、擾乱の影響を消し去ることができる。以下、これらの点について実際のエンコーダの装置構成の例 (図 3) に基づいて説明する。

レーザ光を減衰させるのはエンコーダから出射する直前に減衰器を用いて行う。したがって、要件 (i)「微弱レーザ光」はエンコーダ内で最後に行われる。それまでは十分な強度を持ったレーザ光 (古典信号) のまま符号化を行う。レーザ光は位相の揃ったコヒーレント状態であるが、BB84 プロトコルの伝送性能を上げるためには異なる入力パルス間の位相には相関が存在してはならない (要件 (ii)「位相乱雑化」)。

もし、パルス間に位相相関があると、イブはパルス列から位相を推定しデコイ法の効果を打ち消すような量子測定を行うことができるため安全性が劣化する。典型的な高速 QKD 装置の実装例では、1.244 GHz の繰り返しレートでこのような位相相関の無いレーザ光パルスを生成する。時間幅は 50 ピコ秒 (5×10^{-12} 秒, 50 ps) 程度である。レーザ光パルスは 800 ps の間隔でエンコーダに次々に入力される。これらのパルス系列を $|\alpha 1\rangle$、$|\alpha 2\rangle$、$|\alpha 3\rangle$、…、ここで振幅が $\alpha 1 = |\alpha|e^{i\theta 1}$、$\alpha 2 = |\alpha|e^{i\theta 2}$、$\alpha 3 = |\alpha|e^{i\theta 3}$、… とすると、位相 θ_1、θ_2、θ_3、… が互いに相関なくランダムに変化していなくてはならない。ここでは、ある位相のレーザ光パルスがエンコーダに入力されたとして、それがどのようにビット情報と基底情報を符号化され要件 (iv) を満たす「タイムビン信号」として出力されるかを説明する。

レーザ光パルスは、いったん分岐し長さの異なる 2 つの光路を通過させてから合波する (非対称干渉計を通過させる) ことにより、時間にして 400 ps の遅延を持つパルスペアに変換される。このパルスペアは $|\alpha\rangle_F \otimes |\alpha\rangle_S$ と記述される。ここで、添え字 F、S は、時間的に前にある第 1 パルス (First)、後ろにある第 2 パルス (Second) というパルス位置モードを表す添え字である。その後、パルスペアは 2 つの電極を持った 2 重駆動型の光変調器に入力される。そして、図 2

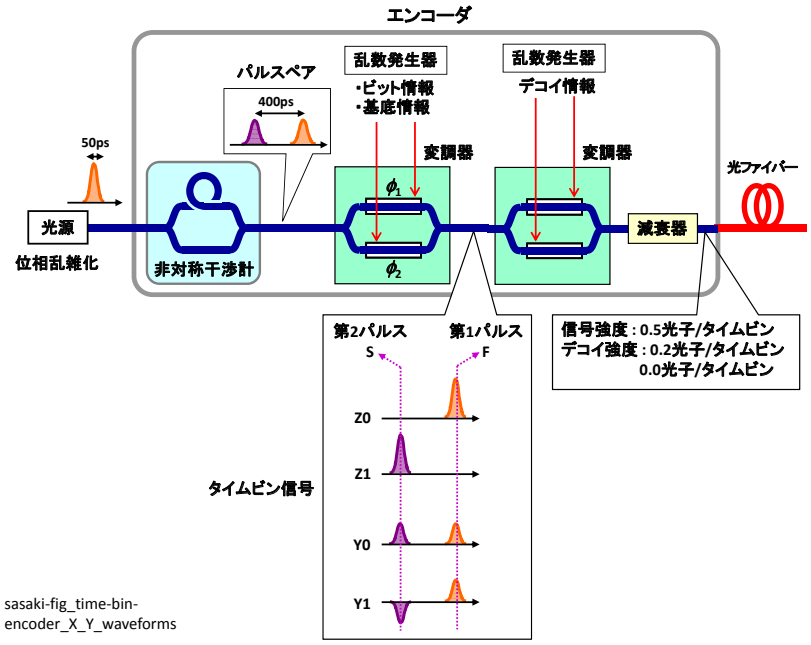

図 3　BB84 プロトコルを光ファイバー伝送用途で実際に装置実装する際に使われるエンコーダの構成とタイムビン信号の概要

の制御ブロックの乱数源 A から提供される乱数列に応じて、それぞれの電極でビット情報と基底情報に対応する位相 φ1、φ2 の変調を受けてから合波されタイムビン信号となって出力される。下記に状態を式にて記述する。

$$|\Psi_{Z0}\rangle = |\alpha\rangle_F \otimes |0\rangle_S \quad (3)$$

$$|\Psi_{Z1}\rangle = |0\rangle_F \otimes |\alpha\rangle_S \quad (4)$$

$$|\Psi_{Y0}\rangle = \left|\frac{\alpha e^{-i\pi/4}}{\sqrt{2}}\right\rangle_F \otimes \left|\frac{\alpha e^{i\pi/4}}{\sqrt{2}}\right\rangle_S \quad (5)$$

$$|\Psi_{Y0}\rangle = \left|\frac{\alpha e^{i\pi/4}}{\sqrt{2}}\right\rangle_F \otimes \left|\frac{\alpha e^{-i\pi/4}}{\sqrt{2}}\right\rangle_S \quad (6)$$

ここで、$|\Psi_{Z0}\rangle$、$|\Psi_{Z1}\rangle$ は Z 基底、$|\Psi_{Y0}\rangle$、$|\Psi_{Y1}\rangle$ は Y 基底に対応する状態である。これらの 4 つの状態は、先に説明した偏光モードでの Z 基底、X 基底と QKD に関する機能上、全く等価な効果を持っている。基底に Y と命名している理由は変調器を構成する際の印加電圧の便宜上の表現によるためである。

その後、タイムビン信号は 2 つめの 2 重駆動型光変調器に入力され、要件 (iii)「デコイ法」に従って複数種類の強度のどれかにランダムに変調されてから、次に減衰器を通り微弱な光パルスに成形され、最後に量子通信路の光ファイバーへ入力される。デコイ法の一例として、信号強度を $|\alpha|^2$ =0.5 光子／タイムビン、デコイ強度を $|\alpha|^2$ =0.2 光子／タイムビンと $|\alpha|^2$ =0 光子／タイムビン（真空状態）の 2 種類に設定する例などがある。現実のレーザ光では 2 光子以上がパルス内に含まれる確率を完全に消し去ることはできない。したがって、タイムビンパルス内に 2 光子以上を含む状態もわずかながら残ってしまう。そうすると、イブが光子を 1 個抜き取り、残りの光子をボブへそのままの状態で送るという、いわゆる光子数分離攻撃が可能になる。この場合、基底とビットの内容は変化しないのでビット誤りは全く生じない。したがって、盗聴も検知できなくなる。デコイ法はこのような攻撃への耐性を高め、伝送距離を伸延する効果がある。光源の光子数分布が既知である場合、異なる信号強度が混ざった信号の検出率、誤り率は伝送路のロスにより一意に決まるが、先に述べた多光子状態を抜き取る攻撃があった場合、その比率が変化し、盗聴者に漏れた情報量を推定することができる。詳細は文献に譲る [24][25]。

・鍵蒸留ブロック

鍵蒸留ブロックは、送受信者の鍵蒸留装置とそれらをつなぐ公開通信路からなる。制御ブロックの乱数源 A、B からは、エンコーダとデコーダに提供したものと同じ乱数列が、それぞれアリスとボブの鍵蒸留装置に提供される。また、光子検出器からの検出信号が制御ブロックを経由してボブの鍵蒸留装置に提供される。ボブの検出信号とそれに対応するアリスの乱数列のデータを突き合わせて並べたものを『生鍵』と呼ぶ。乱数列、検出信号のやり取りの際にも同期信号により時刻同期を行う。このようにして共有された生鍵に、これから述べるような鍵蒸留処理を施して最終的な暗号鍵を抽出する。

図 4 に、鍵蒸留処理の大まかな流れをまとめる（BB84 プロトコルの例に準拠している）。光子伝送の後、アリスとボブには膨大な生鍵のデータが蓄積される。そのデータをできるだけ大きなブロック、例えば、百万ビット程度のブロックにまとめ、そのブロック単位で図 4 の鍵蒸留処理を行う。

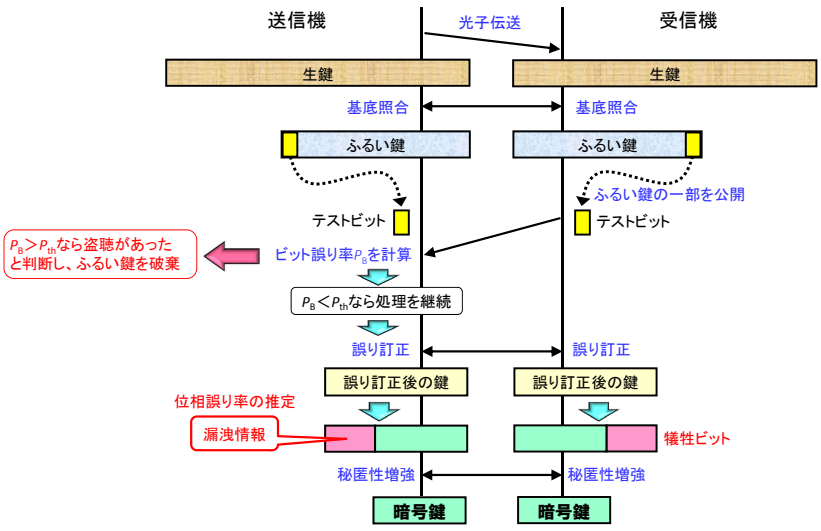

図 4　鍵蒸留処理の流れ

(i) 最初に公開通信路を介して基底照合を行って、同じ基底だったビット列を『ふるい鍵』として抽出する。

(ii) ふるい鍵の一部をテストビットとして切出し、公開通信路を介して送受信者間で共有し、Z 基底のビットの食い違いの割合、いわゆるビット誤り率 P_B を計算する。

(iii) この値がある閾値 P_{th} より大きければ ($P_B \geq P_{th}$)、盗聴があったと判し、このブロック全体を破棄して鍵蒸留は中止する。

(iv) もし閾値より小さければ ($P_B < P_{th}$)、ふるい鍵に誤り訂正処理を施す。

(v) さらに位相誤り率というものを推定し、この値に応じて、『犠牲ビット』の割合を決め、それに応じた秘匿性増強処理を行って最終的に安全な暗号鍵を抽出する。

たとえ、イブが盗聴を行っていても、ビット誤り率が閾値より小さければ ($P_B < P_{th}$)、秘匿性増強によって「誤り訂正後の鍵」から更にある割合のビットを「犠牲ビット」としてランダムに選んで捨てることで、イブに漏れる情報量を実効的にゼロにすることができる。例えば、標準的な BB84 プロトコルの場合、閾値は P_{th} ～ 11 % 程度である。

なお、QKD におけるビット誤りは、現実的には盗聴以外にも、量子通信路上での伝送エラー、変調・復調時の装置エラー、光子検出器の雑音からも生じる。このような装置不完全性によるビット誤りを盗聴に起因するビット誤りと完全に切り分けることは不可能なので、すべて盗聴に起因するもの、つまり、送受信者にとって最も不利な条件として考える。

最新の QKD 装置では、数 10 km の敷設ダークファイバー上でのビット誤り率 P_{th} を数 % 程度まで抑えることができるようになっている。ビット誤り率がこの値から上昇すれば、盗聴があったと判断される。従来の光通信路の診断技術では、光子を通信路から抜き取って測定した後、通信路へ戻して再送するという攻撃を検出することはできないが、QKD 装置ではこのような巧妙な中間者攻撃でも検知することができる。さらに、将来開発されるもっと巧妙な盗聴攻撃でも、光通信路からの情報漏洩につながるあらゆる盗聴攻撃はすべて検知することができる。これは従来の暗号技術にはない大きなメリットであり、光通信インフラへの盗聴が現実化する中で極めて重要な意味を持つ特徴である。一方で、無条件安全性を保証するために、距離や速度といった通信性能はある程度犠牲にならざるを得ない。QKD リンクで直接配送できる性能としては、敷設ファイバー 50 km 圏で暗号鍵生成レートが毎秒 20 万～ 30 万ビット (200 ～ 300 kbps) 程度である。つまり、リアルタイムでワンタイムパッド暗号化できる速度は、まだ高々 MPEG–4 の動画データである。これに対して、すでに欧米や中国のベンチャー企業によって製品化されている装置の性能は、更に低く都市圏で 1 kbps 程度に止まっている。

3 QKD プラットフォーム

QKD の直接伝送の距離・速度にはまだ限界があるものの、『信頼できるノード (トラステッドノード)』を介した『鍵のカプセルリレー (鍵リレー)』を行うことで、QKD をネットワーク化し広域で安全な鍵交換を行うことが可能である。複数の QKD リンクを接続してネットワーク化し、鍵カプセルリレーなどに必要な鍵管理機能を搭載したシステムを一般に『QKD ネットワーク』と呼ぶ。

QKD ネットワークの構築にはまだ高いコストがかかるものの、いったん生成された暗号鍵は、正しく蓄積し管理・運用することによって、様々な通信機器や制御機器に供給しセキュリティ強化に活用することができる。また、十分な鍵サイズがあれば、暗号化は平文と鍵の『単純な』論理和なので、暗号方式の大幅な簡素化が可能になる。そのため、処理遅延はほとんど解消されるとともに、通信機器間の暗号化方式も統一化しやすくなる。したがって、鍵 ID を適切に管理し鍵データをリレーすることによって、セキュリティシステムの仕様や方式の違いを超えた、組織をまたぐ暗号通信の互換性確保が可能になる。実際、特殊な重要通信用途では、広く普及しているインターネット等とは切り分けられた専用の暗号ネットワークシステムが、その暗号仕様は非公開であることが多く、関係する組織間で相互接続しようと思っても、簡単には相互乗り入れができないという問題が潜在的に存在する。QKD ネットワークの導入はこのような問題の解消にも役立つ可能性があり、相互接続性の向上に有効であると期待される。

このような新しい付加価値の実現に必要となる効率的な鍵管理機能と、様々なアプリケーションをサポートするインターフェースを QKD ネットワークに搭載し、ユーザがブラックボックスとして使えるようなネットワークソリューションの形に仕上げたシステムをここでは特に『QKD プラットフォーム』と呼ぶ。それは図 5 に示すとおり、量子レイヤと鍵管理レイヤ及び鍵供給レイヤという 3 つのレイヤから構成される。

量子レイヤでは光子を使って QKD により暗号鍵の配送を行う。QKD そのものは、光ファイバーあるいは光空間通信などの光通信路を介して 1 対 1 のリンクで行う。

ネットワーク化は、信頼できるノードを設けそこに

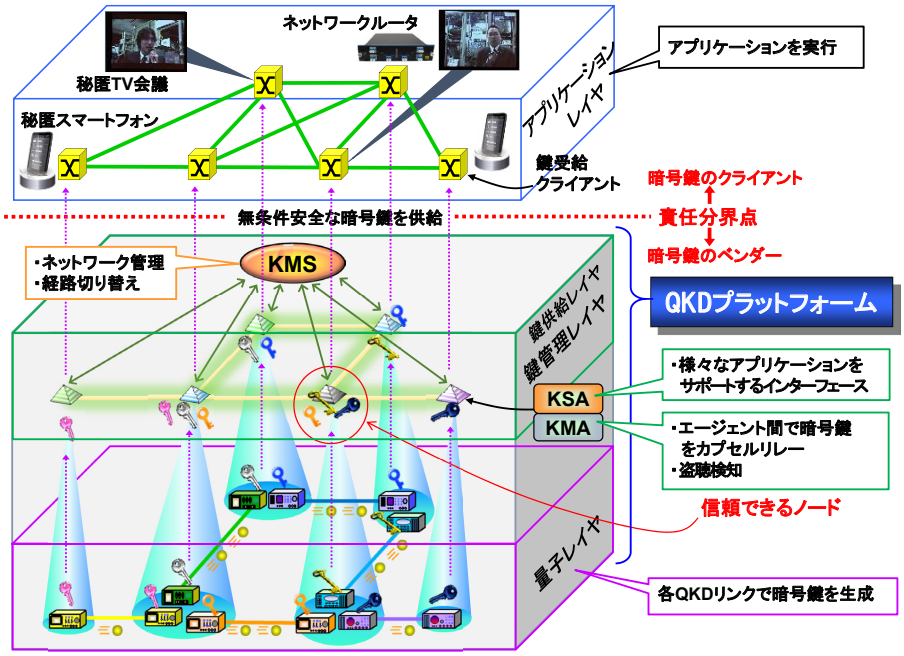

図 5　QKD プラットフォームの概念図。QKD そのものを行う量子レイヤ、暗号鍵の管理・運用を行う鍵管理レイヤ、アプリケーションインターフェースを搭載した鍵供給レイヤから構成される。KMS: 鍵管理サーバ、KMA: 鍵管理エージェント、KSA: 鍵供給エージェント

2 つの QKD リンクの端点を引き込んで、一方の QKD リンクからの暗号鍵を他方のリンクの暗号鍵でカプセル化（鍵のビット値の排他的論理和）し、バケツリレーのように行うことで実現する。この鍵リレーを行うのが鍵管理レイヤである。つまり、各 QKD リンクで生成した暗号鍵は、上にある鍵管理レイヤに吸い上げて管理・運用する。鍵管理レイヤでは、各ノードに鍵管理エージェント（KMA）という装置があり、正規のユーザ以外に誤って暗号鍵をリレーしてしまわないように、認証技術と組み合わせながら、安全な鍵リレーを実現する。そこで用いる認証方式としては、計算量的安全性ではなく情報理論的安全性に基づく Wegman-Carter 認証方式を用いる [26]。

また、鍵管理サーバ（KMS）がネットワーク全体での暗号鍵の蓄積状況、消費状況、盗聴の有無などを集中管理し、盗聴攻撃があった際の経路切替えを行う。

対象とするアプリケーションやそれを実装している機器によって、暗号鍵の要求やその受け渡し作業の仕様は一般的に異なる。様々なアプリケーションへ暗号鍵を自在に供給するために、鍵管理エージェントの直上に鍵供給エージェント（KSA）を定義し、その中に必要となるアプリケーションインターフェースを組み込んでいる。この鍵供給エージェントからなるレイヤを鍵供給レイヤと呼ぶ。鍵供給レイヤを定義することによって、鍵供給ベンダー側と鍵受給クライアント側でのインターフェース設計作業や責任分界を明確化できる。物理的には、鍵管理エージェントも鍵供給エージェントも同一装置（パソコンなど）内に実装されるため、鍵管理レイヤと鍵供給レイヤは縮退している。

このように、QKD そのものを行う量子レイヤ、暗号鍵の管理･運用を行う鍵管理レイヤ､アプリケーションインターフェースを搭載した鍵供給レイヤによって QKD プラットフォームというシステムが構成されている。

これを既存のネットワークに導入することで、従来のセキュリティ機能はそのまま維持しつつ、フォワードシークラシーを持つ暗号鍵によって様々なアプリケーションのセキュリティ強化が可能となる。図 5 の中にあるアプリケーションレイヤは、QKD プラットフォームの説明において暗号鍵を利用したプロトコルを総称するものであり、一般にネットワーク設計で広く使われる「OSI（Open Systems Interconnection）参照モデル」における第 7 層の「アプリケーションレイヤ」とは別の意味で使っている。つまり、OSI モデルのどの層にあっても、QKD プラットフォームから暗号鍵を供給されるアプリケーションは全て図 4 のアプリケーションレイヤにひとくくりに含めている。

アプリケーションレイヤのユーザ（クライアント）は、QKD プラットフォームに対して暗号鍵を共有したい相手を伝えて必要な量の暗号鍵を要求する。QKD プラットフォームは､この要求に対してフォワードシークラシーを持った暗号鍵を所定のフォーマットで供給する。いったん、QKD プラットフォームから供給された暗号鍵は、ユーザの責任において利用する。

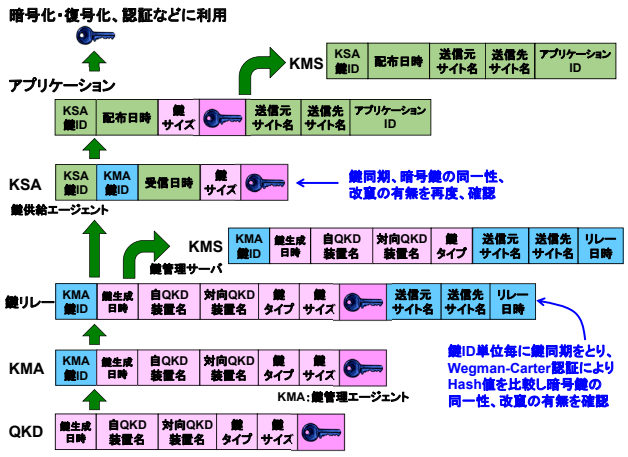

図 6　QKD プラットフォームでの鍵管理概要

このように責任分界点は、QKD プラットフォームとアプリケーションレイヤの境界にある。この境界では、共通インターフェースを用いて暗号鍵の要求と供給、受給が行われることが重要である。このようにすることで、アプリケーションの開発者は共通インターフェースに対応した鍵受給クライアントをアプリケーション内に作るだけで鍵供給を受けることができ、QKD プラットフォーム内部での処理の詳細を知る必要がない。一方で、鍵が供給された後の管理責任は、アプリケーションレイヤのユーザが負うことになる。逆に、QKD プラットフォームの側では、アプリケーションの内容を知る必要はない。

万が一、アプリケーションレイヤ上のどこかで、ヒューマンエラーによる暗号鍵の漏洩など、不測の事態や不審なインシデントがあった場合には、ユーザは保管していた暗号鍵のブロックをいったん破棄し、QKD プラットフォームから新しい暗号鍵を受け取ることで、堅牢なセキュリティをネットワーク上で維持することが可能になる。図 6 に QKD プラットフォームの鍵管理層で行われている鍵管理用データフォーマット（概略）を示す。

4　まとめ

本稿において QKD リンクの原理の紹介と QKD ネットワークの安全な運用を可能とする QKD プラットフォームを紹介した。これらの技術は伝送路の安全性を高めることに加え、秘密分散などの現代暗号技術と融合させることによりゲノムデータなど超長期に安全性を担保する必要があるデータの安全な保存にも応用が可能である [27]。QKD は各国で理論・技術とも、現在もなお精力的に研究が進められており、コストをかけてでも守らなければならない情報に対して適用することに障害がなくなりつつある。NICT は世界最高性能の技術を維持・発展させ、暗号解読技術が突如現れても矢庭に安全な通信を確保できるソリューションを提供できるよう技術レベルの向上に努めていきたい。

謝辞

本稿の成果は 2011 年度から 2015 年度の NICT 委託研究「セキュアフォトニックネットワーク技術の研究開発」（No.157）及び ImPACT プロジェクト「量子セキュアフォトニックネットワーク」での成果が中心であり、量子 ICT 先端開発センターのメンバーと当該プロジェクトに参加いただいているメンバー全員の努力の結晶である。研究開発を共に進めていただけることに心より感謝いたします。また JGN、情報通信システム室、セキュリティ基盤研究室の方々からも日々ご支援を頂いており、この場をお借りしてお礼申し上げます。

【参考文献】

1　Recommendation for Key Management: Part 1 : General. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.
2　M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, “Photon level crosstalk between parallel fibers installed in urban area” Opt. Express, 18 (21) pp.22199–22207, 2010.
3　C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin. Tossing,” In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp.175–179. IEEE, New York, 1984.
4　N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74 (1), pp.145–195 2002.
5　V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, and M. P. Norbert Lütkenhaus, “The Security of Practical Quantum Key Distribution,” Review of Modern Physics 81 :1301-1353 2009.
6　id Quantique SA. http://www.idquantique.com/
7　MagiQ Technologies, Inc. http://www.magiqtech.com/Home.html.
8　QuintessenceLabs Pty Ltd. http://www.quintessencelabs.com/
9　C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. Current status of thDARPA Quantum Network (Invited Paper). In Quantum Information and Computation III, Proc. SPIE, vol.5815, pp.138{149, Orlando, Florida, March 2005.
10　M. Peev, C. Pacher, R. Alleaume, C. Barreiro, W. Boxleitner, J. Bouda, R.Tualle-Brouri, E. Diamanti, M. Dianati, T. Debuisschert, J. F. Dynes, S.Fasel, S. Fossier, M. Fuerst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentchel, H. Hübel, G. Humer, T. Länger, M.Legre, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, E. Querasser, G. Ribordy, A. Poppe, L. Salvail, S. Robyr, M. Suda, A. W. Sharpe, A. J. Shields, D. Stucki, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in Vienna,” New J. Phys. 11(7), 075001/1-37 (2009).
11　Quantum Key Distribution - Industry Specification Group (QKD-ISG), European Telecommunications Standards Institute. http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.
12　M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer,

M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express, 19 (11), pp.10387–10409 2011.
13 The Project UQCC (Updating Quantum Cryptography and Communications). http://www.uqcc.org/
14 M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki, “Highly secure network switches with quantum key distribution systems,” Int. J. Network security 17, pp.34–39 2015.
15 特許第 5791112 号「通信方法及び通信システム」藤原幹生、佐々木雅英.（2015 年 8 月 14 日登録）
16 M. Sasaki. QKD Platform and its Applications. Presentation in Part II Fiber Network, The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video is available in http://2015.uqcc.org/program/index.html
17 NICT プレスリリース 2015 年 9 月 28 日．ドローンの通信の安全性を強化する技術を開発．http://www.nict.go.jp/press/2015/09/28-1.html
18 M. Sasaki. Tokyo Free Space Optical Testbed. Presentation in Part III Space Network, The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video is available in http://2015.uqcc.org/program/index.html
19 NEC プレスリリース 2015 年 9 月 28 日．NEC、量子暗号システムの実用化に向けた評価実験をサイバーセキュリティ・ファクトリーで開始. http://jpn.nec.com/press/201509/20150928_03.html.
20 東芝プレスリリース 2015 年 6 月 18 日．盗聴が理論上不可能な量子暗号通信システムの実証試験の開始について．http://www.toshiba.co.jp/about/press/2015_ 06/pr_j1801.htm.
21 Q. Zhang. Quantum Network in China. Presentation in Part V Relay Talk and Discussion, The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video and slide are available in http://2015.uqcc.org/program/index.html
22 N. Walenta, D. Caselunghe, S. Chuard, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legr e, T. McCandlish, L. Monat, A. Morrow, G. Ribordy, D. Stucki, M. Tourville, P. Trinkler, and R. Wolterman. Towards a North American QKD Backbone with Certifiable Security. Contributed talk in the afternoon session on Sept. 28, The Fifth International Conference on Quantum Cryptography (QCrypt2015), Tokyo, Sept. 28 {-Oct. 2, 2015, http://2015.qcrypt.net/scientfic-program/
23 W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum cryptography using entangled photons in energy-time Bell states,” Phys. Rev. Lett. 84 (29), pp.4737–4740 2000.
24 H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett. 94 (23), 230504 2005.
25 X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A72 (1), 012326 2005.
26 L. Carter and M. Wegman. New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci, 22 :265–279 1981.
27 M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, “Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing,” Sci. Reports, 6, 28988-1-8 2016.

藤原幹生　（ふじわら　みきお）
未来 ICT 研究所
量子 ICT 先端開発センター
研究マネージャー
博士 (理学)
量子鍵配送、光子検出技術、極低温エレクトロニクス

佐々木雅英　（ささき　まさひで）
未来 ICT 研究所
主管研究員
理学博士
量子通信、量子暗号