【特別寄稿】

量子コンピュータ時代に対応する情報セキュリティ

― 量子雑音ストリーム暗号 Y-00（Yuen2000 プロトコル）―

原澤 克嘉

はじめに

近年、世界各国で量子技術の研究開発に国家レベルでの巨額な投資がおこなわれ、急速な進化を遂げだしている。特に中国では、量子技術開発だけで年間 1 兆円を超える規模の研究投資がおこなわれている。

量子関連技術の中でも「量子コンピュータ」、「量子センサー」、「量子暗号」の分野においては、早期実現化に向けた開発競争が激化し、各国から様々な成果が論文やメディアで報告されている。その様な中でも特に量子コンピュータの開発が著しい進化を遂げ出している[1]。

量子コンピュータの実用化は新材料や創薬開発などの化学計算や各種シミュレーション等、現在のスーパーコンピュータでは膨大な計算量(計算時間)を要する課題に対しては非常に有効であり期待されているが、同時に計算量を安全性の根拠としている現代暗号においては、解読の脅威にさらされることになる。

現代の情報化社会においてライフラインをコントロールする IoT や AI、経済活動の中心となるキャッシュレス決算や仮想通貨など情報通信の役割は非常に重要であり、安心・安全な国家を安定に維持するための生命線となる。そのため情報通信のインフラは、強靭なセキュリティで確実に守ることが必須になる。本稿では、量子技術の動向および将来の量子コンピュータ時代に向けた情報セキュリティを構築できる量子雑音ストリーム暗号の実用化について述べる。

1　量子技術の動向

現在、量子技術は、各国で盛んに研究されている。この量子技術を先行して実現することにより、国間関係における安全保障の面において、

[1] Frank Arute et al. “Quantum supremacy using a programmable superconducting processor,” https://www.nature.com/articles/s41586-019-1666-5.pdf.

より優位な立場で展開することが可能になる。表 1 は、中国、米国、日本で実用化に向けて開発の進む主な量子技術について開発状況を比較したものである[2]。今までは米国、日本が先行して研究開発を行ってきたが、ここ数年で中国が驚異的な勢いで急成長してきている。

表 1　主な量子技術の比較

	量子コンピュータ(ゲート型)	量子センシング(量子レーダー)	量子暗号(Y-00)
中国	①中国科学院、中国科学技術大学 12 Q-bit ②Alibaba、中国科学院 11 Q-bit クラウドサービス開始	①CETC (China Electronics Technology Group Corporation) 検出範囲：100km 検出技術：量子相関	①College of Communication Engineering, Army Engineering University of PLA ■ Y-00(強度変調：ISK) 2.5Gbps, 100km(古典雑音)
	トピックス ■量子鍵配送：QKD BB-84プロトコル 中国科学院,中国科学技術大学, etc. . ①China/Austria間伝送　145kbps, 7600km（衛星移動きょりを含む）、128bitAES[インターネット]+QKD[衛星通信] ②北京/上海間伝送　1kbps, 2000km 32拠点中継 ■量子通信（テレポーテーション）：青海省と雲南省間約1200km衛星通信　量子もつれ状態の光子ペア伝送		
米国	①IBM 53 Q-bit クラウドサービス開始 ②Google 53 Q-bit 量子超越性（？） ③Intel 49 Q-bit	①米国陸軍研究所 検出範囲 数m 検出技術 古典相関、量子相関	①ノースウェスタン大学（Y-00 位相変調：PSK） 2.5Gbps,200km ②MIT、オクラホマ大学 Y-00の応用研究を開始
日本	現在、日本国内では、量子ゲート型の開発期間はなく、量子アニーリングが主流になっている	①玉川大学 距離性能 数百m（計算値） 検出範囲 古典相関、量子相関	①日立（Y-00 ISK） 1.25Gbps～10Gbps、500km ②玉川大学(Y-00：PSK) 28Gbps、1000km ③東北大学(Y-00:直角位相振幅変調：QAM) 70Gbps、100km

[2] Frank Arute et al. “Quantum supremacy using a programmable superconducting processor”;　Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan1,　“Secure quantum key distribution with realistic devices” https://arxiv.org/pdf/1903.09051.pdf; Haisong Jiao, Tao Pu, Jilin Zheng, Hua Zhou, Lin Lu, Peng Xiang, Jiyong Zhao, and Weiwei Wang “Semi-quantum noise randomized data encryption based on an amplified spontaneous emission light source,” https://www.osapublishing.org/oe/abstract.cfm?uri=oe-26-9-11587; *MIT Technology Review* 「兵器としての「量子技術」 激化する米中開発競争の行方」 https://www.technologyreview.jp/s/123739/the-us-and-china-are-in-a-quantum-arms-race-that-will-transform-warfare/; M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, "QAM quantum stream cipher using digital coherent optical transmission," *Opt. Express* Vol. 22, No. 4, pp. 4098-4107, February (2014); Ken Tanizawa and Fumio Futami, “Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels”, Vol. 27, No. 2, 21 Jan 2019, *OPTICS EXPRESS* 1071; K.Harasawa, “New Quantum Cipher Optical Communication: Y-00”, 2012, *Optical Communication*, Intech open, https://www.intechopen.com/books/optical-communication/new-quantum-cipher-optical-communication-y-00.

特に、量子コンピュータは、クラウド利用できる実用段階に入ってきており、多くの研究機関が新たな計算アルゴリズムの開発やアプリケーションの開発に利用を始めている。このような計算能力が高い量子コンピュータ時代における情報通信のセキュリティ（特に暗号）を改めて考えなおし、先行して対策していくことが重要である。

2　量子コンピュータ時代の暗号

（1）現代暗号

数学的根拠に基づく計算量を安全性の根拠にする現代暗号は、現在、最高性能のスーパーコンピュータを用いたとしても暗号解読には、膨大な計算量を必要とするため、天文学的な時間が必要となる。しかし、この計算量は、コンピュータの性能に大きく依存する。日本の CRYPTREC（Cryptography Research and Evaluation Committees）からは、スーパーコンピュータの性能の進化と、現代暗号に対する脅威が報告されている[3]。

この報告では、一般的に公開鍵暗号として利用されている RSA（1024 ビット）暗号は、現存のスーパーコンピュータである「京」でも 1 年以内に解読可能である。このため暗号の安全性を強化する必要があり、より複雑な（2048 ビット等）RSA へ移行されてきている。このような安全性強化は、進化し続けるスーパーコンピュータの進化の状況に合わせてアップデート継続しなければならない。更に量子コンピュータ（超電導量子ビット型やイオントラップ型）の出現と、その実用化により、予測を遥かに超えた計算能力の進化が始まろうとしている。

量子コンピュータの性能予測については、様々な意見があるが、現在の開発状況から最速の進化予測（ビット数が 4 年で 14 倍の予想）をすると、ショアのアルゴリズムを用いることで因数分解計算が容易になり RSA 暗号は、2030 年代に容易に解読されるようになり、2040 年代には、Grover のアルゴリズム（総当たり攻撃に適したアルゴリズム）を使うことにより、現在一般的に利用されている共通鍵暗号である AES の解読時間も大幅に

[3] “CRYPTREC Report 2018,”
https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2018.pdf

短縮される。また新たに最適なアルゴリズムが開発されると時間軸は大幅に縮まることになる[4]。

そのため、現在では、耐量子コンピュータ暗号として数学的により複雑な暗号方式として格子暗号や多変数多項式暗号などの研究が盛んに行われてきている。しかし、暗号化、復号化を行うために、より複雑な計算処理が必要となるため、公開鍵暗号や認証に期待ができるが、AES やストリーム暗号の代替としては非常に困難である。しかし、前述のように暗号化、復号化に必要な計算量が大きいため、高速・大容量のリアルタイムに伝送に適応するのは困難である。

（2）量子暗号

ア　[BB84]

一般的に量子暗号と言うと、光の最小単位である単一光子の伝送を利用し、鍵の共有化をおこなう Quantum Key Distribution（QKD） を想像する人が多い。この方式は、情報理論的安全性が証明されている暗号プロトコルである「One Time Pad（OTP）」を実現するための条件の一つ(絶対的に安全な鍵の配送)を実行するための手段である。OTP を実現する条件には、「鍵の長さ≧データの長さ」、「鍵は 1 回ごとに使い捨てる」、「同じ鍵は繰り返し使用ができない」、「絶対に安全な鍵の配送」などがある。この中で、「絶対に安全な鍵の配送」に QKD を用いて、OTP を実現する技術（この暗号プロトコルを BB84 と呼ばれている）である。しかし、単一光子伝送では、平均送信パワーが光子 1 個の最小単位なので、伝送路（光ファイバ）損失の影響等を受け、確率的に受信端に到達できる光子の数は非常に少なくなる。このため伝送速度（伝送容量）と伝送距離が大きく制限されてしまい、長距離化、大容量化が進む現在の情報通信ネットワークへの直接的な適用は不向きになる。

BB84 を大容量伝送に適用する考え方としては、中国で実験されているように、AES（128 ビット）の共通鍵の共有に BB84 を組合せ、ビデオ会議を実施している例がある。しかし、これは OTP を実現するわけではなく、単に安全な鍵配送を実現しているだけにすぎないため、データ伝送の安全性は従来通りの AES の計算量で決定する。この伝送は中国科学アカデミー(北京)とオーストリア科学アカデミー(ウィーン)の間の約 7600km

[4] “イノベーションジャパン 2019　JST 事業セミナー”　講演資料より
https://www.jst.go.jp/crds/sympo/20190829/pdf/02.pdf.

の距離を人口衛星の利用で実施されたが、QKD は地上の拠点と衛星間のアップ・ダウンの空間通信で使用し、中国－オーストリア間の移動は人口衛星で行われている[5]。

鍵の伝送速度は 128bps であり、総量が「約 560 キロビット」の鍵伝送を行っている。その時のビデオ会議のための伝送されたデータの総容量は「約 2 ギガバイト」であり OTP の条件である「鍵の長さ(量)≧データの長さ(量)」は満たせていないことになる。
また、同じく中国では、北京―上海間で約 2000km の伝送試験を実施している[6]。

この伝送区間には 32 の中継拠点があり、各拠点では復号化/暗号化を繰り返し、従属的に繋ぎ合わせ距離を稼いでいる。鍵の伝送速度は 1kbps であり、OTP を実施しているとすれば暗号化されたデータ伝送速度は 1kbps 以下となる（ちなみに ISDN での電話 1 回線の伝送速度は 64kbps である）。

イ　[Y-00]

Y-00 暗号は、唯一物理レイヤーを直接守れるセキュリティ技術であり、共通鍵暗号であるが、高速・大容量のリアルタイム伝送に対応できる量子雑音効果を利用したストリーム暗号である[7]。

表 2 に ISO（International Organization for Standardization）の通信ネットワークを 7 階層に分割した OSI（Open Systems Interconnection model standardized）参照モデルを示す。

---

[5] "Real-world intercontinental quantum communications enabled by the Micius satellite," psy. org, https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html.

[6] J. Qiu, "Quantum communications leap out of the lab," *Nature* 508(7497), 441–442 (2014).

[7] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme," *Phys. Rev. A*, Vol. 72, p. 022335, 2005; K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, T. Hosoi, Y. Doi, K.Ohhata, T. Katayama, T. Shimizu, "Consideration of the Implementation Circuit of Randomization for Physical Cipher by Yuen 2000 protocol", *The Transactions of the IEICE C*, Vol. J91-C, No8, p1-10, 2008; K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, and Y. Doi, "Quantum encryption communication over a 192 Km, 2. 5 Gbit/sec line with optical transceivers employing Yuen-2000 protocol based intensity modulation", IEEE/OSA. *Journal of Light Wave Technology*, vol-29, No. 3, p316-323, 2011.

ネットワークを構築する７つのレイヤーの機能の内、レイヤー１の物理層だけ、現在、対応できるセキュリティ技術がない。今までは、上位レイヤーのセキュリティ技術だけでも何とか安全性を保つことができたが、光通信の周辺技術の進歩と共に、コンピュータ性能も進化して、特別な技術や設備がなくとも誰でも簡単に光ファイバーからの盗聴を行うことが可能になった（後節参照）。情報戦が重要視される現在の安全保障活動において、情報ネットワークのレイヤー１を直接守ることは非常に重要であり、Y-00 は、レイヤー１を守ることのできる唯一のセキュリティ技術と考えている。

表 2　国際標準化機構（ISO）の OSI 参照モデルの 7 階層

Layer	通信機能階層	セキュリティ技術
L7	アプリケーション層	XML, S/MIME(e-mail), PGP, SET(credit card), SSH(remote)
L6	プレゼンテーション層	
L5	セッション層	
L4	トランスポート層	SSL/TLS, Socks
L3	ネットワーク層	IPSec
L2	データリンク層	PPTP, WEP, AES
L1	物理層（伝送路）	**無 ⇒ (Y-00)**

図１に示すように、IoT やクラウドコンピューティングが進む現在、ユーザーアプリケーションでのデータは増え、光通信、無線通信は、それぞれの技術開発に伴い通信速度も増大している。レイヤー１のセキュリティ技術を、通信ネットワークに適用するためには、光通信やモバイル無線通信などの技術的な進化や利用されるアプリケーションを無視することはできず、高速・大容量伝送およびリアルタイム伝送への対応が必須である。特に海に囲まれた日本においては、離島間や国間の伝送には、海底ケーブルを利用した長距伝送も不可欠であり、長距離化への対応も必須となる。

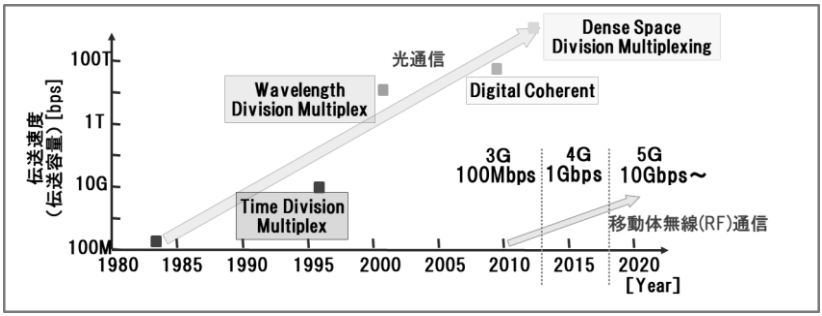


図１　通信の大容量化

3　光ファイバーの盗聴

「自社のネットワークは、インターネットとは切り離したクローズド環境であり、専用線を使っているから安全」という考えがある。しかし拠点や施設が特定できると、そこへ出入りする専用の通信線路は比較的簡単に見つけることができる。

現在は、様々なサイバーセキュリティ対策が開発されており、クラウド内やデータセンタ内を強固に守ることが可能になってきている。入退管理システム等で拠点内を強固に守ることはできるが、データがその守られた拠点から一歩外へ出ると、全伝送線路を設備的に守り抜くことは経済的に不可能であり現実的でない。盗聴ターゲットのビルの周辺の通信マンホールや、遠隔地などのターゲット施設から出てくる専用線は、簡単に特定しやすく、通信事業者の保守員やケーブルテレビの工事者装うことで、疑われることなく誰でも簡単に伝送路にアクセスすることが可能になる（図２）。

更に量子コンピュータのクラウド利用が始まれば、誰でも簡単に高度な解析計算も可能になる。

次に光ファイバーの脆弱性について説明する。未だに「光ファイバーは盗聴できない」と言う光ファイバー安全神話を信じている人も多い。光ファイバーのタッピングは非常に簡単である。図３のように光ファイバーは、コア部とクラッド部を屈折率の違う石英ガラスで構成している。光信号は

その境界面にできるミラー効果を利用し、コア内を全反射しながら進行していく。光ファイバーを鋭角に曲げると、屈折率と光の入射角の関係で一部の光信号がクラッドを通過し、光ファイバーの外へ漏れ出す。この原理を利用して光信号を抜取ることができる光ファイバー検査治具がインターネットの通信販売で（＄1000 程度）されており、誰でも入手することが可能である。

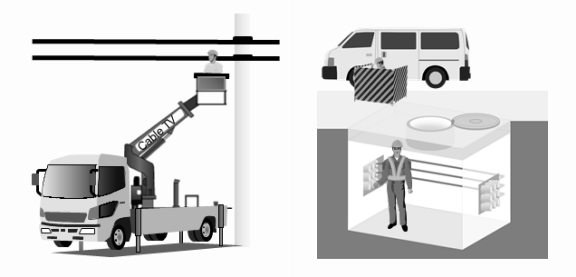


図２　光ファイバーのタッピング（１）

実際の盗聴は、光ファイバーの被覆をカッターで剥き、芯線を露出させ、曲げることで漏れ出した光をレンズで集光し取り出す（治具を使えば光ファイバーを挟むだけで良い）。この抜き出した光を光ファイバーアンプで増幅することにより伝送中の光信号と同様な信号を生成することができる。これには特別な技術はいらず、誰でも簡単に行える。抜取ったデータは、量子コンピュータのクラウド利用で解読可能になる。

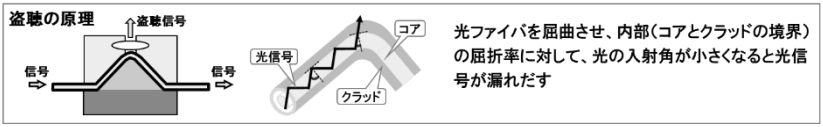


図３　光ファイバーのタッピング（２）

4　Y-00 の概要

（1）量子雑音と信号検出

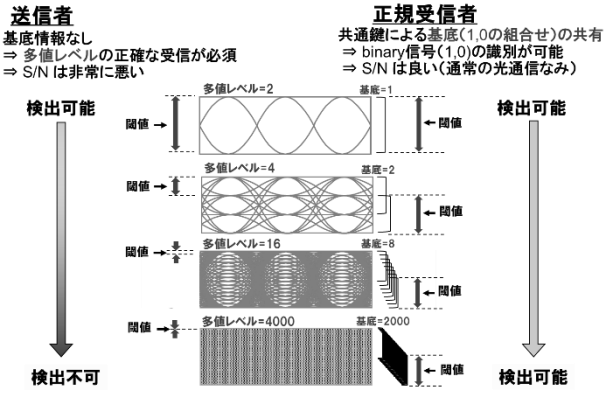
前述のように現在光ファイバーで伝送するデータは、殆どの場合レイヤー2 以上の階層で暗号（現在暗号）化されている。現代暗号で暗号化されたデータは数学的に複雑な処理を施されているが、光ファイバーに流れる信号は、“１”、“０”のデジタル（バイナリ）信号である。前節で説明した

ように、盗聴者は簡単にこの“１”、“０”の暗号化された信号を正確に抜き盗ることができ、後は計算機の処理能力次第で解読できるため、計算処理能力の非常に高い量子コンピュータの実用化は脅威となる。

Y-00 の暗号化は、光の特殊な多値変調方式と量子雑音を利用した秘匿効果を利用することで“1”、“0”のデジタル信号ではない多値変調信号を生成し、盗聴者には物理的な量子雑音効果（不確定性原理）を顕著に与え完全ランダムに誤ったデータしか取得することができないようにする新たな暗号方式である。基本的に、規則性のないランダムに誤るエラーを持ったデータを用いた計算で正しい解を導き出すことはできない。

一方、正規の受信者は共通鍵の情報により量子雑音の影響を受けることなく正しいバイナリ情報（“１”、“０”）を直接導き出すことができる。図 4 を用いてこの仕組みを説明する。この図は、光ファイバー内の伝送信号を 1 ビットごとに時間軸（X 軸）をずらして波形を重ね合わせたもの（アイパターン）である。

信号が 2 値の場合、“1”、“0”は、視覚的にもはっきりと判別でき、そのスペースの中心に閾値を置くことで、受信者は“１”、“０”の信号識別が可能になる。波形中心部のスペースが広いほど受信側で正しく信号を識別できる。図のように多値数を 4 値、16 値と増やしていくと、スペースは狭くなり、受信側で多値レベルの識別誤り発生確率は高くなる。多値数が 4000 値にもなると、各々のレベルの持つ雑音が隣接する複数のレベル値まで覆うようになり、正しいレベルの識別は不可能になる。ここで影響する雑音が量子雑音（実際には古典の影響も付加され安全性は、より強化されるが設計上は量子雑音の効果のみで安全性を考える）であり、Y-00 の暗号化には、この量子雑音効果を利用する。盗聴者は、



この雑音を量子力学の理論上除去することができないため、その影響を直接受けることになる[8]。

図４　Y-00 の量子雑音効果(強度変調)-

（2）基本的な Y-00 の暗号化、復号化の考え方）

Y-00 の送信者は、多値の信号レベル配置の中に基底（2 値の組合せ）を論理的に埋め込み、共通（秘密）鍵で 1 ビットごとに基底を選択し、そこに“１”または“０”の情報を載せた信号レベルを伝送する。送受信者間では共通鍵を利用することにより選択している基底を共有できている。

受信者は、送られてくる基底がわかっているので“１”、“０”の中心レベルに信号の識別のため閾値を移動させることで量子雑音の影響を受けることなくバイナリ検出が可能になる。この基底の選択は、送受信者間で 1 ビットごとにランダムに行い伝送するため、ストリーム暗号が実現できる。

盗聴者は、共通鍵の情報が無いため、基底の選択情報を持てないため“１”、“０”のバイナリ検出は不可能となる。そこで盗聴者は、多値レベルの変化を正確に観測し、その動きから共通鍵の情報を得ようと試みる。しかし、前述のように多値数が多くなると、量子雑音による信号レベルの変動（量子揺らぎ）が回避できず、常に誤った観測結果を得ることになる。このため量子雑音によるランダムなエラーを含む観測結果から正しい解を一意に求めることはできない。

このように正規受信者と盗聴者の信号と雑音効果の関係（SNR：Signal to Noise Ratio）を極端に差別化（正規受信者には小さく、盗聴者には大きく）することで、計算処理（計算量）では解決できない物理的な安全性を担保することができる。盗聴者は、直接的な盗聴ができないため、物理的に全数探索攻撃を試みようとする。SNR の差別化を回避するためには、盗聴用に正規受信者と同等性能の Y-00 受信機を用意し、考えられる全ての鍵を用いて一斉に解読する全数探索の攻撃が考えられる。しかし、これを

[8] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, T. Hosoi, Y. Doi, K.Ohhata, T. Katayama, T. Shimizu, “Consideration of the Implementation Circuit of Randomization for Physical Cipher by Yuen 2000 protocol”, *The Transactions of the IEICE C*, Vol. J91-C, No8, p1-10, 2008; K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, and Y. Doi, “Quantum encryption communication over a 192 Km, 2. 5 Gbit/sec line with optical transceivers employing Yuen-2000 protocol based intensity modulation", IEEE/OSA. *Journal of Light Wave Technology*, vol-29, No. 3, p316-323, 2011.

同時に実行しようとすると盗聴者は 10^{79} 台（256 ビットの共通鍵を使う Y-00 の場合）の受信機による並列検出を行う必要がある。この数は、宇宙を構成している原子の総数（10^{80}）と同等の個数であり、非現実的である。また、1 台の受信機で盗聴者がシリアルに解読を試みる場合、10^{79} ビットのデータを取得する必要があり、暗号データの伝送速度が 10Gbps の場合のは、10^{60} 年間データを取得し続ける必要がある。これも非現実的な時間である。

このように Y-00 の安全性は、計算能力（計算量）に依存しない天文学的な物理量やデータ取得時間で決定することができる[9]。

5　Y-00 の研究体制

Y-00 の基本アイディアは、ノースウェスタン大学の H.P.Yuen 教授によって発案され、玉川大学の廣田修教授との共同研究で理論の体系化を開始し、2000 年に Yuen 教授によって公開されたことで、Y-00（Yuen2000 プロトコル）と呼ばれるようになった[10]。

アメリカでは、Northwestern 大学が中心となり DARPA がきっかけとなりプロジェクトで本格的な研究が開始さてきれた。日本では、玉川大学と日立グループ、東北大学で異なる変調方式で研究開発が進められてきている[11]。

---

[9] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, T. Hosoi, Y. Doi, K.Ohhata, T. Katayama, T. Shimizu, “Consideration of the Implementation Circuit of Randomization for Physical Cipher by Yuen 2000 protocol”, *The Transactions of the IEICE C*, Vol. J91-C, No8, p1-10, 2008; K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, and Y. Doi, “Quantum encryption communication over a 192 Km, 2. 5 Gbit/sec line with optical transceivers employing Yuen-2000 protocol based intensity modulation", IEEE/OSA. *Journal of Light Wave Technology*, vol-29, No. 3, p316-323, 2011.

[10] H. P. Yuen, “A new quantum cryptography,” Report in Northwestern University, 2000.

[11] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, "QAM quantum stream cipher using digital coherent optical transmission," *Opt. Express* Vol. 22, No. 4, pp. 4098-4107, February (2014); KEN TANIZAWA AND FUMIO FUTAMI, “Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels”, Vol. 27, No. 2, 21 Jan 2019, *OPTICS EXPRESS* 1071; K.Harasawa, “New Quantum Cipher Optical Communication: Y-00”, 2012, *Optical Communication*, Intech open, https://www.intechopen.com/books/optical-communication/new-quantum-cipher-optical-communication-y-00; E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, “Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks,” *Phys. Rev. A*, Vol. 71, p. 062326, 2005; O. Hirota, “Optical communication network and quantum cryptography,” *IEICE Trans. Commun.*, Vol. J87-B, No. 4, pp. 478–486, 2004.

最近では、中国の研究機関が、積極的に研究を始めている。中国の研究機関が公開している Y-00 伝送実験の例では、ISK（光強度変調方式）を採用し、2.5Gbps で 100km の伝送試験が報告されている[12]。しかし、まだ日本の技術のトレースのように見えるが、中国は量子技術の研究開発に莫大な投資を行う計画であり驚異的である。そのためには、中国に負けないよう、国家的な計画と支援が必要である。

項目	日本			米国	中国
研究機関	HITACHI	Tamagawa University	Tohoku University	Northwestern University	College of Communication Engineering, Army Engineering University of PLA
変調方式	強度変調	強度変調 位相変調	直角位相振幅変調	位相変調	強度変調
伝送速度	1.25Gbps 10Gbps	1.25Gbps 28Gbps	70Gbps	2.5Gbps	2.5Gbps
伝送距離 光ファイバアンプ中継	500km	1000km 800km	100km	100km	100km

表 3　各国の Y-00 暗号プロトコルの開発状況

まとめ

現代の情報通信は、更に進化をし続け、その役割は国家を安全に維持するために重要な存在となっている。このような社会の中枢を担う情報通信のネットワークは、テロリストや外敵の攻撃的な活動から確実に守り抜くことが重要である。

量子力学を核とした技術（量子技術）は、一部の分野で実用化段階に入り出した。これらの技術を先行開発することにより国際関係やテロ対策などに対して常に優位性を保つことができるため、各国で大きな研究開発投資が行われるようになった。特に量子コンピュータの分野では、米国の大手企業が実用化に向けた大きな成果が報告され、クラウドサービスの試行も始まっている。また、中国では、国家的に莫大（年間 1 兆円規模）な研

[12] Haisong Jiao, Tao Pu, Jilin Zheng, Hua Zhou, Lin Lu, Peng Xiang, Jiyong Zhao, and Weiwei Wang “Semi-quantum noise randomized data encryption based on an amplified spontaneous emission light source” https://www.osapublishing.org/oe/abstract.cfm?uri=oe-26-9-11587

究開発投資がおこなわれ、国をあげて量子技術での先行優位性を急速に確立しようとしている。

量子コンピュータの実用化が加速すると現在使用されている計算量的安全性を安全性の根拠とする暗号技術は、一気に解読の脅威に襲われる。このため、計算量だけに頼らない量子暗号の実用化開発も急務になってきた。

本稿では、現代の進化し続ける情報通信ネットワークへ適用可能で早期実用化に期待ができ、実用化理論と実装技術おいて日本主導で世界に先行してきてた量子暗号である Y-00（Yuen2000 プロトコル）を中心に紹介した。このような、技術を実際に国内の重要ネットワークへ適用し、活用することで日本のネットワークの安全性を世界に向けて発信することにより、情報通信セキュリティ分野における国家的な優位性を確立することが重要だと考える。そのためには、日本においても量子技術の「実用性・実用化」について真剣に考え、理論や実験室内での成果だけでなく、社会や安全保障のフィールドにおいて実際に装備し運用できる国家的な研究開発投資が急務と考える。更に、日本の情報通信を守り抜くためには、データセンタやイントラネットワーク等の限られたエリアのサイバーセキュリティだけではなく、専用線をはじめ、ラスト・ワンマイルと言われる加入者線路等を物理的に盗聴から守ることも必須であり、ネットワーク全体を総合的に守り抜くサイバーセキュリティをいち早く構築することが必要である。