

光通信量子暗号(Y-00)の高セキュアフォトニック ネットワークへの展開に関する検討

二見 史生[†] 広田 修[‡]

[†] 玉川大学 学術研究所 〒194-8610 東京都町田市玉川学園 6-1-1
E-mail: [†] futami@lab.tamagawa.ac.jp, [‡] hirota@lab.tamagawa.ac.jp

あらまし 現代社会や生活において、ネットワーク (NW) の役割は非常に大きいものになっているが、個人情報や機密情報が平文で通信されていることが少なくない。暗号化された通信情報もあるが、主に計算量的安全性に頼った数理暗号化に基づくもので、過去の歴史を振り返ると、情報漏洩の可能性を完全に排除できているとは考え難く、情報漏洩のリスクが極限まで少ない高セキュアな NW の実現が急務である。本稿では、本学で実際に運用している光 LAN において NW モニタ実験を行い、現状の NW では、簡単に通信情報をモニタできることを示す。次に、数理暗号を遙かに凌ぎ、究極的に解読不可能な安全性を実現できる可能性のある、光通信量子暗号(Y-00)の特徴および性能を解説し、その試作器の性能について報告する。ワークショップでは、Y-00 の高セキュアフォトニック NW へ展開について、新世代 NW 構築を担う研究者等と議論したい。

キーワード ネットワーク, 安全性, 光通信量子暗号, Y-00, 量子ストリーム暗号

The quantum stream cipher by Yuen 2000 protocol (Y-00) and the step of Y-00 to the secure photonic network application

Fumio FUTAMI[†] and Osamu HIROTA[‡]

[†] Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo, 194-8610 Japan
E-mail: [†] futami@lab.tamagawa.ac.jp [‡] hirota@lab.tamagawa.ac.jp

Abstract Although the current networks are playing an essential role in modern societies, the personal information and proprietary information transmitted in such networks are not always encrypted. Some information encrypted is based on the mathematical cryptography whose security level is mainly dependent on the computational complexity. According to the decipher history, the mathematical cryptography cannot completely deny the possibility of the information leakage. Consequently, for securing user's security and convenience, a construction of an extremely highly secure network is an urgent matter. In the workshop, first, we experimentally demonstrate monitoring the data in the currently-operated optical local area network of Tamagawa university and reveal the easiness of monitoring the data, which draws attention to the need of the secure network construction. Next, features and performance of the quantum stream cipher by Yuen 2000 protocol (Y-00) are described. Unlike the mathematical cryptography, the Y-00 has potential of the realization of the ultimate security communication. We also report on the performance of the Y-00 prototype developed for the practical application.

Keyword Network, Security, Quantum stream cipher, Yuen-2000 protocol (Y-00)

1. はじめに

1.1. 研究の背景

クラウドコンピューティングに代表されるように、最近、ネットワーク(NW)を流れる情報の秘匿性の重要性が強く求められている。現状のNWでは、暗号化されていない平文で通信されている情報が少なくない。この現状は通信情報の盗聴が可能であることを意味し、盗聴を抑止するものは、モラルやいくつかの法律に過ぎない。テロリストなどモラルや法律遵守の精神のな

い者に良識を求めるのは、実質的に無意味である。様々な盗聴方法が研究されており、通信を瞬断させることさえなく、光ファイバから信号光をタップする技術など報告されている[1]。高セキュアNWを構築するために重要なことは、情報を盗聴されないよう情報に暗号化を施すことである。一部の通信情報が暗号化されているのは事実であるが、数理暗号に基づく暗号である。数理暗号の安全性は、主に数学理論および計算量的安全性を拠としているために、解読手法

が発見され解読に必要な計算量が激減する危険、また、計算機能力の増大による危険が避けられない。数理解暗号解読の歴史を振り返ると、解読の危険性を完全に否定できない。数理解暗号を用いる限り盗聴の危険性があり、クラウドコンピューティング等による便利なサービスの発展の妨げになることが危惧される。暗号には、数理解暗号と異なり、物理的理論に基づく物理暗号がある。中でも、光通信量子暗号(Yuen-2000)は、詳細は後述するが、数理解暗号概念を凌駕する新たな暗号であり、数理解暗号を遙かに凌ぐ高い安全性を確保した高セキュア NW 構築に繋がる有力な暗号方式である。数学的な解読法がないことが示されており、理論的にその高い安全性が示され、実験検証が行われつつある。既に、試作器が作製されており、単一光子光源を使う旧来の量子暗号方式と異なり、10Gbps の伝送速度で敷設光ファイバ伝送路 400km 弱の伝送実験に成功し、実用化の一手手前の所まで来ている。

1.2. 本報告の目的

本報告では、現状の NW の例として本学の光 LAN を挙げ、ホームページ閲覧や電子メール受信を、容易に第三者がモニタできることを実験的に示し、現状の NW の安全性に対する脆弱性を露わにする。次に、高セキュア NW 応用を目指し、本学で研究開発を進め、実用化が目前の光通信量子暗号(Y-00)とその試作器の特性を紹介し、新世代の NW 構築を担う研究者等と共に、NW に求められる安全性について議論し、Y-00 の実用に向けた検討を行いたい。

2. 現状ネットワークの安全性

果たしてどのくらいの人々が、現在の NW の安全性レベルを正確に把握しているであろうか？ SSL や IPsec など数理解暗号により暗号化されているものの、アプリケーション設定によっては、パスワードでさえ平文で NW を流れている。1969 年に ARPA(米国国防総省高等研究計画局)のプロジェクト ARPANET に起源を持つインターネットは、これまで幾度も部分的な改良が加えられ、今日に至っている。そのため、多くの致命的な問題が指摘されている[2]。安全性に関しては、新たな数理解暗号の発明とその解読の繰り返しである。最近のよく知られた暗号解読では、現在も無線通信に広く利用されている WEP(Wired Equivalent Privacy)がある[3,4]。鍵長 104 ビットの暗号であるが、標準化されてから 10 年程度で解読されてしまった。

P 対 NP 問題が未解決である以上、即ち、解読されることが不可能なことが証明されていない数理解暗号は、通信情報を第三者にモニタされる危険性ははらんでおり、情報漏洩の可能性を完全に否定できない。即ち、利用者が莫大な被害を受ける危険性ははらんでいる。実被害が発生する前に、また、NW の健全な発展のためにも、安全性を盲信できる NW の構築が急務ではないであろうか。

めにも、安全性を盲信できる NW の構築が急務ではないであろうか。

3. ネットワークモニタ実験

3.1. 実験構成

本学で実運用している光 LAN において、図 1 に示す系で、NW モニタ実験を実施し、パソコン(PC)①の通信をモニタした。二つのエッジスイッチ(Extreme Networks 社製 Summit 200-24)を結んでいるシングルモード光ファイバを流れる 1000BASE-LX の光信号をタップし、アンリツ社製データクオリティアナライザ(MD1230B)に入力し、Ethernet フレームをキャプチャした。次に、Wireshark を使用し、TCP/UDP をデコードし、コムワース社製のソフトウェア SwiftWing FlowHunter Basic を用いて、フレームを繋ぎ合わせ視覚化した。

なお、本実験は学内光 LAN に接続している他の情報端末を切り離すルータを介入させ、PC①のみをモニタする環境で実施した。

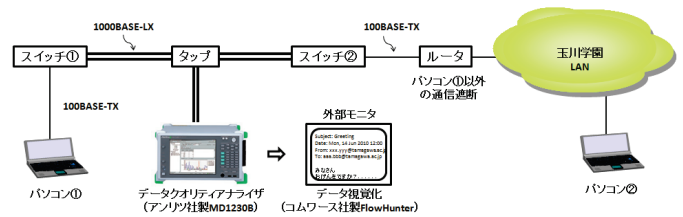


図 1: 本学光 LAN の一部を利用したモニタ実験系。なお、ルータでパソコン①以外の通信は遮断した。

3.2. 実験結果

暗号化されていないプロトコルである HTTP と POP3 の通信をモニタした。

HTTP モニタ実験では、本学の学術研究所のホームページを閲覧した。図 2(a)に、PC①のインターネットエクスプローラで閲覧した画面を示す。一方、(b)にモニタした画面を示す。同一のものが見られた。

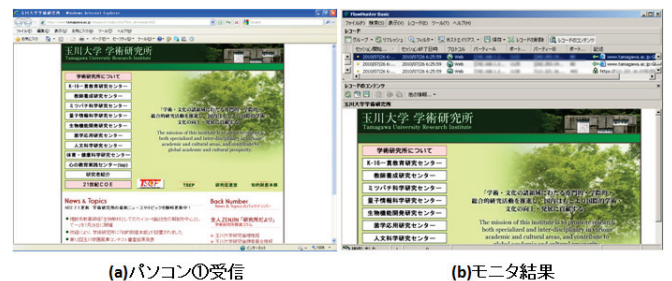


図 2: HTTP モニタ: (a)パソコン①閲覧, (b)モニタ結果

次に、POP3 のモニタ実験を行った。PC②から送付した電子メールを、PC①で POP3 を用いて受信した。PC①で受信した電子メールとモニタした電子メール

をそれぞれ図 3(a), (b)に示すが、メール内容が完全に読み取れた。

POP3 では、ID やパスワードもネットワーク上を暗号化されずにそのまま流れる。従って、容易にこれらをモニタすることが可能である(図 4 黒線枠内)。パスワードを暗号化する認証方式 APOP があるが、数理解暗号に基づいており、既に解読可能になっている[5]。

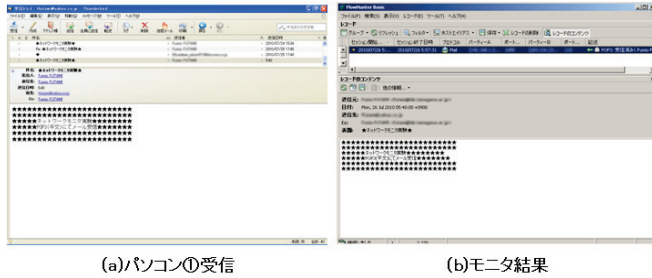


図 3 : POP3 モニタ : (a)パソコン①受信, (b)モニタ結果

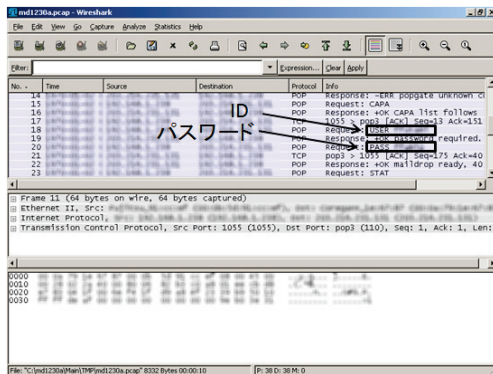


図 4 : POP3 の ID, パスワードのモニタ

4. 光通信量子暗号 Yuen-2000(Y-00)

4.1. Y-00 の特徴

Yuen-2000(Y-00)は、2000 年に Northwestern 大学の H. P. Yuen により提案された従来の数理解暗号の概念を凌駕する特長を有するストリーム暗号[6]で、送信端では、二つの値の信号を複数の値に変換し、1 ビット毎に 2 値の組み合わせ(基底)に振り分けて暗号化(変調)する。一方、受信端では、送受信器間で共有している共通鍵を利用して、基底情報にあわせた信号識別点をビット毎に移動させアナログ的に受信し、暗号信号を復号する。共通鍵を持っている正規受信者は容易に情報を受信することができるが、鍵を持っていない者は、識別点が分からないため、暗号信号を受信しても復号できない。また、基底数を大きくすることで、受信時に発生する量子雑音が多値レベルの認識を困難にし、安全性を強固にできる。

数理解暗号と Y-00 の暗号化原理を図 5 に示すが、Y-00 には数理解暗号に対する様々な利点がある。特に重要な利点は、安全性の保証である。数理解暗号は、主に暗号

化の数学理論と計算量的安全性に基づいているために、安全性を保証することができない。一方、Y-00 では、計算量的安全性には依存していないので高い安全性を確保できる上、雑音を定量化することにより安全性を定量的に保証することが可能になる。また、一般に暗号装置を購入し鍵を全数探索すれば盗聴が可能になるが、Y-00 の場合、ある一部の暗号文に対し正しくない鍵でも復号可能であるため、Y-00 暗号装置を入手し全数探索を行っても、正規の共通鍵を見いだすことができない。更に、二つの値の信号を複数の基底に振り分けるので、Key Redundancy[7]という数理解暗号にはない効果が生まれ盗聴を困難にする。これらが数理解暗号に対する全ての利点ではないが、数理解暗号にない高い安全性を担保できる特長がある。

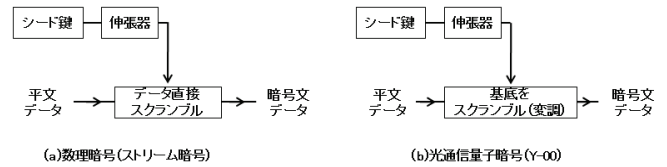


図 5 : 暗号化原理. (a)数理解暗号, (b)光通信量子暗号(Y-00)

4.2. 玉川大学 Y-00 方式

Y-00 の研究開発の構図を図 6 に示す。Y-00 を実現する方法として、光位相変調方式(Northwestern 大学)[8]、光強度変調方式(玉川大学)[9,10]、および直交位相振幅変調方式(QAM)(玉川大学, Northwestern 大学)[11]がある。玉川大学では、現状の光ファイバ通信システムと最も整合性がよく、大きな量子雑音効果が期待できる光強度変調方式の研究開発を中心に取り組んでいる。Y-00 は従来の数理解暗号の概念を凌駕するため、完全に体系付けられていないが、その性能は理論的に証明が進んでいる[12]。理論研究と併せて、実利用に向け、実験評価および装置化の研究開発も併せて行っている。現状、日立情報通信エンジニアリング社により本方式の試作器が完成しておりその特性評価を進めており、実用化の一手前まで来ている。

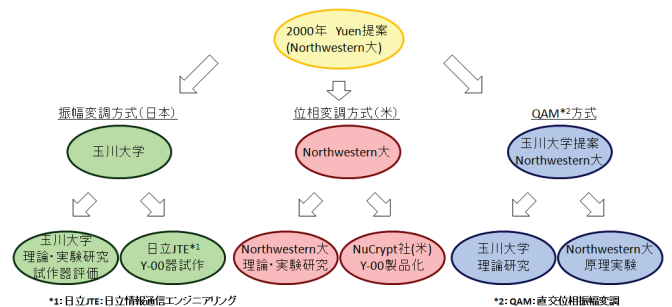


図 6 : 光通信量子暗号(Y-00)研究開発

4.3. Y-00 試作器

図 7(a), (b)にそれぞれ 10Gbps, 2.5Gbps の試作器概観を示す. 10Gbps は送信機と受信機の二つで構成され, 2.5Gbps は送受信器が一体化したトランシーバになっている. トランシーバ本体と電源の二つのユニットで構成されており, それぞれのサイズは, 215 (W) x 390(D) x 39(H) mm で, 実用化を指向し専用二重化電源を採用している. 外部から電源供給できる環境では, トランシーバ本体のみでよい. GbE, OC-48 に対応し, 暗号鍵は 128/256 ビットで, 信号数は 4000 以上である.



図 7: Y-00 試作器. (a)10Gbps, (b)2.5Gbps

図 8 に示す, 本学内に敷設してある光ファイバ伝送路「TAMA ネット 1」において, 10Gbps, 360km の伝送実験に成功している[13]. 符号誤り率特性および伝送した Y-00 暗号信号光波形を図 9 に示すが, 良好な伝送特性であることが検証された.



図 8: TAMA ネット 1 (本学敷設光ファイバ伝送路)

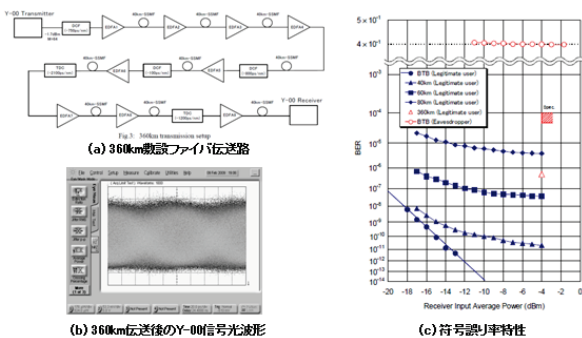


図 9: Y-00 試作器(10Gbps)の本学敷設光ファイバ伝送路 (360km)伝送特性[13]

4.4. 耐久試験

実用化に向け, 本学内敷設光ファイバ伝送路「TAMA ネット 1」で, Y-00 試作器の耐久試験の準備を進めて

いる. TAMA ネット 1 は, 端局で折り返す構成で総長 1,000km になり, 道路沿いに敷設されているので, 振動, 温度変化等あり, 実回線に近い環境での試験が可能である.

5. まとめ

現状 NW の安全性が脆弱であることに注意を喚起するため, 本学光 LAN において HTTP および POP3 モニタ実験を実施し, 第三者が容易に通信情報をモニタできることを示した. また, 通信情報漏洩の可能性を完全に排除した高セキュア NW 構築に有力な候補である, 従来の数値暗号と異なり新しい概念の光通信量子暗号 (Y-00) について概説した. 本学が研究開発を行っている強度変調方式の Y-00 は高速特性, 量子雑音効果利用特性に優れ, 現状の光ファイバ通信システムと高い整合性がある. 2.5Gbps, 10Gbps での試作器が済み, 10Gbps 試作器の敷設光ファイバ伝送路 360km 伝送実験を示し, 実用化が目前であることを紹介した.

新世代 NW 構築を担う研究者等と, Y-00 の新世代 NW への適用可能性について有意義な議論を行いたい.

謝辞

NW モニタ実験にあたり, NW 環境を本学 e エデュケーションセンターの南隆矢センター長に構築して頂いた. モニタ用実験装置およびソフトウェアは, それぞれアンリツ(株)殿, (株)コムワース殿に借用した. また, Y-00 特性評価には日立情報通信エンジニアリングの試作器を用いた. ここに謝意を表す. 本研究の一部は, 富士通研究所の委託研究により行った.

文 献

- [1] S. V. Kartalopoulos, Security of information and communication networks, John Wiley & Sons, New Jersey, 2009.
- [2] AKARI アーキテクチャ設計プロジェクト, 新世代ネットワークアーキテクチャ AKARI 概念設計書改訂版(ver2.0), NICT, 2009.
- [3] E. Tews et al., Cryptology ePrint, 2007.
- [4] M. Morii et al., Computer Security Symposium2008.
- [5] Y. Sasaki, et al., IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, Vol.E92-A, No.1, p. 96, 2009.
- [6] H. P. Yuen, "A new quantum cryptography," Report in Northwestern University, 2000.
- [7] H.P.Yuen et al, Quantum Information and Computing, vol-6, p.561, 2006.
- [8] G. A. Barbosa, et al., Phys. Rev. Lett., Vol.22, 227901, 2003
- [9] 広田修, 光通信ネットワークと量子暗号 電子情報通信学会論文誌 B, J-87-B, No.4, p.478, 2004.
- [10] O.Hirota, et al., Phys. Rev. A, 72, 022335, 2005.
- [11] K. Kato and O. Hirota, Proceedings of SPIE, vol-5893, 2005.
- [12] 広田修 他, 39 卷 1 号, p.17, 光学, 2010.
- [13] Y. Doi et al., Proceedings of OFC, OWC4, 2010.