3-3　光空間通信における物理レイヤ暗号に向けた通信路推定実験

遠藤寛之　藤原幹生　北村光雄　都筑織衛　伊藤寿之　清水亮介
豊嶋守生　竹中秀樹　武岡正裕　佐々木雅英

物理レイヤ暗号は、通信路の物理的な性質を利用することによって、情報理論的に安全な秘匿伝送や鍵共有を実現する技術である。本稿では、物理レイヤ暗号の基本的なモデルについて概説し、量子 ICT 先端開発センターが取り組んできた、光空間通信における物理レイヤ暗号実現に向けた通信路推定実験について述べる。

1　まえがき

IT 技術の急速な発達と普及によって、今や情報ネットワークは重要な生活基盤のひとつとなっており、我々に多くの恩恵をもたらしてきた。一方で、ネットショッピングや公的機関への電子申請など、機密性の高い情報をやりとりする場面も非常に多くなってきており、暗号技術によるそれらの機密情報の保護が必要不可欠となってきている。

現在のネットワークの安全性は、メッセージの秘匿性を確保する共通鍵暗号や、ユーザ間での鍵共有や認証などを担う公開鍵暗号などといった、いわゆる現代暗号によって守られている。現代暗号はアルゴリズムとして公開されており、ケーブルや電波といった通信を担う物理的媒質とは無関係に実装できる。さらに、安全性に現在の技術水準にかんがみたうえでの数学的な根拠が与えられている。例えば公開鍵暗号では、巨大な合成数の素因数分解のような、現在の計算機では現実的な時間で解を求めることの困難な数学的問題が安全性の根拠として利用されている。このような計算量的な安全性は比較的容易に担保できる一方で、効率的な解読アルゴリズムや量子計算機の実現によって脅かされるという側面も持つ。しかし、鍵長の延長や、量子計算機ですら解読が困難な数学的問題を利用するなど、それらの脅威に対する対抗策は年々開発され続けている。以上に挙げた特徴により、現代暗号は様々な機器やシステムへと実装され、まさに現代社会の根幹を支える技術となっている。

一方で、現代暗号に対して、情報理論の大家である Wyner は全く異なるパラダイムに基づく暗号技術を提案している。氏の発表したワイヤタップ（盗聴）通信路符号化 [1][2] は、通信過程で発生した誤りを訂正するだけでなく、盗聴者側のノイズを巧みに利用することで事前の鍵共有無しでの秘匿通信の機能までも実現する。さらに、ノイズという物理現象の予測不可能性に基づいて、いかなる計算能力を持った盗聴者も解読不可能な安全性、すなわち情報理論的安全性 [3] も証明できる。その後、Maurer [4] と Ahlswede [5] らはそれぞれ独立に Wyner のアイデアを援用することで、物理的雑音を利用した鍵共有の手法である秘密鍵共有を提唱した。ネットワーク・プロトコルを階層化した OSI モデルにおいて、現代暗号が高次のレイヤにて運用される一方で、これらの技術は最も下層の物理レイヤで運用されるとみなすことができる。そのため、ワイヤタップ通信路符号化と秘密鍵共有は、物理レイヤ暗号などと総称される。

驚くべきことに、Wyner のワイヤタップ通信路符号化 [1] は公開鍵暗号の原型である DH 鍵共有 [6] の前年には発表されていた。しかし、符号設計の際に盗聴者側に漏洩している情報量の推定の必要性など、計算量から安全性を保証できる現代暗号の利便さには遠く及ばず、現在のネットワークにおいて主流となることはなかった。しかしながら、情報理論的安全性に基づくという点は注目に値し、現在では一部の通信システムへの物理レイヤ暗号応用に向けた研究が進められている。例えば、電波無線通信 [7]–[12] では、多重反射によって生じる受信強度のランダムな時間変化から鍵を抽出する秘密鍵共有が検討されている。また、Maurer による秘密鍵共有よりも先立って提唱されていた量子鍵配送（QKD: Quantum Key Distribution）[13]–[15] では、乱数ビットを特殊な量子状態にある光子に符号化して伝送し、その誤り率から盗聴者の存在の検知や漏洩している情報量の推定を行えることが数学的・物理学的に証明できる。そのため、装置に情報漏洩につながる欠陥等が無い限り、QKD はいかなる計算能力を持った盗聴者に対しても成り立つ強力な鍵共有を実現できる。2017 年時点において、地上光ファイバネットワークにおける実証試験も行われ [16]–[20]、製品も市販されているなど [21]、唯一実用化されている物理レイヤ暗号システムであるとも言える。一方で、

その伝送可能距離／鍵生成レートは 50 km 光ファイバーで 1 Mbps[22] などシビアな制限が課されており、技術としての適用範囲にはいまだ課題が残っている。

現在、量子 ICT 先端開発センターでは、上記に挙げた QKD が直面しているスループットの問題に対して、その相補的な技術として古典光空間通信における物理レイヤ暗号の研究を推し進めている。光空間通信は、狭い広がりのビームによる見通し通信で行われるため、盗聴者はビームの端などの不利な状況で盗聴を行わざるを得ない。したがって、盗聴者に漏洩し得る情報量の上界を実装上の見地から与えることができ、結果、物理レイヤ暗号の利用が期待できる。さらに、光空間通信自体の性質から、数 Gbps に迫る高速度かつ長距離間での秘匿通信の実現が期待でき、現状の QKD では高速な鍵生成が困難である衛星通信や、安全性技術の必要性が叫ばれているドローン、各種 IoT 機器等への応用も期待できる。その一方で、確固とした安全性の証明が数学的及び物理学的見地から行われている QKD とは異なり、光空間通信における物理レイヤ暗号の安全性や漏洩している情報量の推定法については、いまだ決定的な議論が提出されていないのが現状である。実際に、豊富な理論的研究 [23]–[28] に対して、実用的な装置構成や想定し得る攻撃に対する議論が十分になされた実用的な研究は我々が知る限り存在しない。

以上の現状にかんがみ、我々は電気通信大学（UEC）と共同で、UEC と NICT の 2 地点間を結ぶ光空間通信テストベッドを構築し、そこから得られたデータを基にそのような通信路の状態及び漏洩情報量を推定するといった通信路推定実験などの、実験的なアプローチから光空間通信における物理レイヤ暗号の実現に向けた研究に取り組んできた。

本稿の目的は、物理レイヤ暗号という技術の基礎事項について概説し、その後我々が取り組んできた実験から得られた知見について概説することにある。まず、この後に続く **2** 及び **3** にて、物理レイヤ暗号の代表的なモデルであるワイヤタップ通信路符号化と秘密鍵共有の原理について述べる。そして、**4** にて NICT が取り組んできた通信路推定実験について概説する。

2　ワイヤタップ通信路符号化による秘匿通信

2.1　通信路符号化

本節の目的は、物理レイヤ暗号の内で最も基本的なモデルであるワイヤタップ通信路符号化を概説することにあるが、それに先立ち通信路符号化について述べる。なお、本論を通して情報は 0 または 1 のビットで表現されているとし、情報量（長さ）の単位をビットと定める。

送信者（アリス）が受信者（ボブ）に無線や光ファイバーといった通信路を通して通信を行う過程で、あるビットが別のビットに変化するといったエラーが生じると仮定する。アリスはボブに正しい情報を送るために対策を講じる必要がある。そこで、アリスは送りたいメッセージに対して誤り訂正のためにあえて冗長な情報を追加し、ボブがそれを手がかりとして元の情報を再生できるようにする。例えば、アリスが各ビットにそのコピーを 2 つ加えて送った（0 → 000 または 1 → 111）場合、3 つの連続するビットのうちの 1 つが他のビットに変化したとしても、ボブは多数決的な判断に基づいてその誤りを訂正できる。このように、冗長情報を加える処理を通信路符号化と呼び、メッセージに冗長情報を加えたビット列を符号語と呼ぶ。また、ボブが受信したビット列からメッセージを再生する操作を復号と呼ぶ。

直感的には、多くの冗長情報を加えるほど、復号に失敗する確率 ε_n を限りなく 0 に近づけることができるが、その反面、伝送効率が犠牲となる。そのため、誤りのない通信を実現可能な必要最低限の冗長情報の量を知ることはシステム設計上非常に重要である。そのようなモチベーションの下、Shannon は符号語の長さ n に対するメッセージの長さ k の比である符号化レート $R_B = k/n$ が、伝送を担う通信路ごとに定義される通信路容量 C よりも小さい場合に、n を長くすることで復号失敗確率 ε_n を任意に小さくできることを示した。この主張は通信路符号化定理と呼ばれ、情報理論における最も基本的な問題設定の 1 つである。

通信路容量 C の具体的な評価のために、通信システムを特徴づける確率をいくつか定義する。アリスは、独立で同一な確率 $P_X(x)$ に基づいてビット x を選択して伝送する。また、通信路におけるエラーの発生確率は、シンボル x が入力された場合にボブがシンボル y を得る条件付き確率（遷移確率）$W_B(y|x)$ によってモデル化される。なお、ここでは定常無記憶な通信路を仮定する。以上の準備の下、アリスとボブの間で伝送可能な情報量を表す、相互情報量 $I(X;Y)$ を下記の式で計算できる。

$$I(X;Y)=\sum_x\sum_y P_X(x)W_B(y|x)\log_2\frac{W_B(y|x)}{\sum_{x'}P_X(x')W_B(y|x')}$$

アリスはボブへとより多くの情報を伝送するために、入力確率 $P_X(x)$ の最適化を図る。結果として、通信路容量 C は下記の式で与えられる。

$$C=\max_{P_X(x)} I(X;Y)$$

2.2　ワイヤタップ通信路符号化

前節で述べた通信路符号化とは異なり、ワイヤタップ通信路符号化では図1のように、アリスとボブが主通信路を通して行っている通信を、盗聴者（イブ）が盗聴者通信路を用いて盗聴するという、1対2の通信が考察の対象となる。ただし、アリスとボブの目的は、メッセージをボブに対して誤り無く送ることだけではなく、同時にイブに対しては一切の情報も漏洩しないように伝送すること、すなわち高信頼かつ情報理論的安全な通信を行うことへと変化する。

直感的には、イブが誤り訂正に失敗するようなレートの通信路符号化を行えば、安全性も同時に担保されるように思える。ここで、アリスが長さ3ビットのメッセージを伝送したときに、ボブは誤り無しにメッセージを受け取れるが、イブ側には正しいメッセージと1ビット誤りが生じたビット列が等確率で現れるとする、模式的な例を考える。すなわち、アリスがあるメッセージ 000 を送ると、イブ側には4つのビット列 000, 100, 010, 001 のうちの1つが 1/4 の確率で現れる。ここで、イブはアリスが送ったメッセージの特定こそできないが、その候補をある程度まで絞り込める点に注目したい。例えば、イブがビット列 001 を得た場合には、アリスは 001, 101, 011, 000 のいずれかを送ったと推測できる。すなわち、メッセージと思われる候補が8つから半分の4つに減少したことから、メッセージに関する情報が1ビット分漏洩しており、もはや情報理論的安全とは言えない。

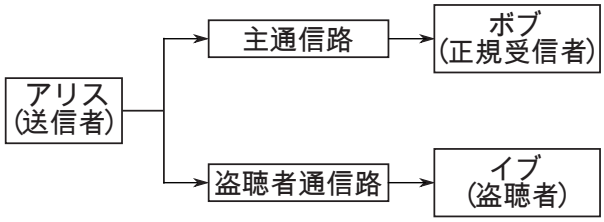

図1　ワイヤタップ通信路符号化の概要図

表1　3ビットメッセージとイブ側に発生する系列及び2ビット秘密メッセージ

メッセージ	イブ側に発生する系列	2ビット 秘密メッセージ
000	000, 100, 010, 001	00
111	111, 011, 101, 110	
100	100, 000, 110, 101	10
011	011, 111, 001, 010	
010	010, 110, 000, 011	01
101	101, 001, 111, 100	
001	001, 101, 011, 000	11
110	110, 010, 100, 111	

アリスとボブが情報理論的安全な通信を行う場合には、この1ビットの情報漏洩すら防ぎたい。そこで、表1のように、アリスがメッセージ伝送した際に、イブ側で発生する系列を列挙して比較してみる。すると、000 と 111 の両者について、イブ側に発生する系列を合わせると、3ビットで表現可能な系列を尽くしていることが分かる。そこで、アリスはそのような条件を満たす2つのメッセージを組にして、それぞれの組に対して2ビットのメッセージを対応させる。これが、情報理論的安全に伝送できる秘密メッセージとなる。ある秘密メッセージを送る際には、それに対応づけされている3ビットメッセージのいずれかをランダムに選択して伝送する。ボブは誤り無しで系列を受け取れるため、表1の対応付けを参照することにより秘密メッセージを再生できる。一方で、イブ側には、伝送系列選択の際のランダムな選択も考慮すると、メッセージとは無関係にすべての3ビット系列が等確率で現れる。以上より情報理論的安全性が成立する。

上記が、ワイヤタップ通信路の核となる議論である。実際には、ボブの通信路にも誤りが発生するため、誤り訂正も考慮する必要がある。以下、その性能を情報理論的に述べる。アリスは長さ k の秘密メッセージを長さ n の符号語に符号化する。復号失敗確率を通信路符号化定理同様に ε_n で表す。そして、漏洩情報量の尺度を δ_n で表す。この量は様々に定義されているが（例えば [29]–[31]）、基本的にはイブ側の確率分布と完全一様分布との間の統計距離によって計られる場合もある。Wyner は、秘密メッセージのレート $R_B = k/n$ が秘匿容量

$$C_S = \max_{P_X(x)} [I(X;Y) - I(X;Z)]$$

よりも小さい場合に、復号失敗確率 ε_n と漏洩情報量 δ_n の両方を、n を長くすることで任意に小さくできることを示した [1]。ここで、$I(X;Y)$ は通信路符号化定理から誤り訂正でアリスとボブが共有できる情報量、$I(X;Z)$ は盗聴者に漏洩している情報量に対応する。実際に、上記の模式例では、3ビットのメッセージから漏洩している1ビット分の情報量を引いた2ビットが情報理論的安全に伝送可能なビット数となっていた。なお、上記の Wyner の定理では条件 $I(X;Y) > I(X;Z)$ が成立している必要があるが、Csiszár と Körner[2] は情報理論的なテクニックを駆使し、この条件を外す一般化を行った。

3　秘密鍵共有

通信で発生するノイズの利用により、秘密鍵の共有無しに秘匿通信を実現できるワイヤタップ通信路符号

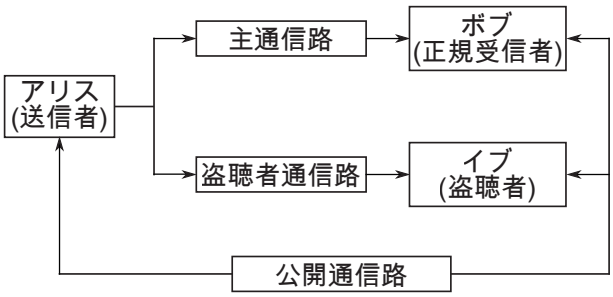

図 2　秘密鍵共有の概要図

化は、一見理想的な暗号技術である。しかし、盗聴者通信路で発生するエラーが主通信路で発生するそれよりも少ないといった、イブにとって有利な条件では機能しないという、実用上の問題を抱えている。対して、1993 年に登場した秘密鍵共有 [4][5] では、図 2 のように認証付き公開通信路の使用を許すことによって、イブが有利な条件で盗聴できたとしても鍵の生成を可能にしている。秘密鍵共有では、あらかじめアリスとボブが共有した相関を持つ乱数から、公開通信路を通した議論をとおして、秘密鍵の共有を行う。なお、乱数の共有の仕方によって秘密鍵共有というプロトコルをさらに 2 種に大別することができる。1 つは、アリスとボブ（とイブ）がある共通の乱数源から生成された乱数を受信する情報源モデルである。電波無線通信における秘密鍵共有 [7]–[12] はこちらに分類される。一方、アリスが乱数を用意して伝送する手法は通信路モデルと呼ばれる。光空間通信の豊富な帯域や見通し通信という特徴を取り入れて、大気の変調速度に律速されない高速な秘密鍵共有を行うためには、後者の通信路モデルが適している。以下では、単純な加法的ノイズを仮定して、通信路モデルに基づく秘密鍵共有の概説を行う。

はじめに、アリスは長さ n の乱数列 x^n を生成してボブとイブに伝送する。ボブとイブは主通信路と盗聴者通信路で発生した統計的に独立なノイズ e^n 及び d^n が加わった出力 $y^n = x^n \oplus e^n$ 及び、 $z^n = x^n \oplus d^n$ を得る。なお、⊕はビットごとの排他的論理和を表す。次に、アリスとボブは公開通信路を通して行う情報整合 [32] というプロトコルを通して、互いの系列の間の食い違いを修正していく。ここでは特に、ボブが誤り訂正のための情報をアリスに送って、その情報を基にしてアリスがボブの系列を推定する、いわゆる後方情報整合に注目する。当然、イブも公開情報でやりとりされる情報を利用してボブの乱数列の推定を試みる。しかし、イブはアリスが送った乱数列を盗聴するという状況に着目すると、そのアリスの乱数列に更に独立なノイズが印加されたボブの系列の推定には、アリスよりもハンデを負うことになる。実際に、アリスとイブの乱数列をボブの乱数列 y^n で表すと、$x^n = y^n \oplus e^n$ 及び、$z^n = y^n \oplus e^n \oplus d^n$ となる。すなわち、たとえイブがボブよりもノイズの少ない状況で盗聴を行ったとしても、後方情報整合によってイブに不利な状況を作り出すことができる。最後に、秘匿性増強 [33] [34] によって、イブに漏洩したビットの分だけ乱数列を圧縮する操作を行う。これは、イブに漏えいした情報量を除去していると解釈できる。そのためには、出力から入力の推定が困難である一方向関数が利用される。

なお、この秘密鍵共有を通して共有可能な鍵のレートは、Renner が QKD の文脈で行った安全性解析を援用することで求めることができる。Renner[35] は、任意の手法での情報整合と、ユニバーサル 2 ハッシュ関数 [36] を用いた秘匿性増強を用いた場合に共有可能な鍵レートが

$$C_K \geq \max_{P_X(x)} [I(X;Y) - I(Y;Z)]$$

と求めることができることを示した。ここで、前者が情報整合で共有できる情報量であり、後者が盗聴者に漏洩している、除去すべき情報量に対応している。このことは、LDPC のような実用化されている誤り訂正符号と、ユニバーサル 2 ハッシュ関数を利用することによって、実用的な秘密鍵共有プロトコルを構成することが可能であることを示している。

4　光空間通信テストベッドによる通信路推定実験

以上に述べてきたように、物理レイヤ暗号の性能はワイヤタップ通信路符号化の場合には秘匿容量、秘密鍵共有の場合には秘密鍵容量（の下限）により測られる。そこで、アリスとボブはあらかじめ通信路の確率分布を推定しておき、そのデータから通信路の確率モデルを推定、再構成したうえでこれらの量を計算し、適切な符号の設計を行う。しかし、ここにはいくつかの困難が存在する。まず、大気中の屈折率は、温度変化に応じて時々刻々と変化している。この効果は大気のゆらぎと呼ばれ、受信強度の数ミリ秒スケールでの変化や、ビーム方向のズレなどを生じる。そのため、大気のゆらぎの効果を加味した性能評価は困難を伴う。加えて、イブの漏洩情報量の評価も、現実的には困難であるという問題がある。

そこで、量子 ICT 先端開発センターでは、上記の問題について実験的なアプローチを行うために、図 3 に示すような電通大と NICT の 2 地点を結ぶ、7.8 km の光空間通信テストベッドを構築した。このテストベッドでは、電通大のビル屋上にあるドームがアリスの役割をし、NICT ビルの 6 階の受信システムをボブ、

屋上のターミナルをイブと見立てている。

本稿では、様々な気象条件において、物理レイヤ暗号の伝送性能を実験的に評価することで、天候が物理レイヤ暗号に及ぼす効果の関係を解明することを目的として、2015 年 11 月 19 日に行われた実験について述べる [37] [38]。この実験では、アリスは波長 1550 nm、出力パワー 100 mW のアイセーフレーザをオン－オフ変調することで、長さ 2^{15}-1 の擬似乱数列を伝送した。送信レンズのビーム拡がり角が約 1 ミリラジアンであったため、NICT 側でのビームの広がりの半径は約 8 m になる。なお、実験の都合上、イブ系も光を受信できるように、ビーム中心はボブ側からイブ側に 1 m ほど近づくよう調節している。ボブとイブはそれぞれ、直径約 100 mm の望遠鏡でビームを集光し、PIN フォトダイオード検出器とアバランシェフォトダイオード検出器で光パワーの測定を行う。このような検出器の感度差に加えて、ボブ側の検出器が窓ガラス越しにあることから、本実験はイブがボブよりも高感度な検出システムによって盗聴を行うという、光空間通信における盗聴シナリオの 1 つの典型例の模倣となっている。

上記の実験状況で、伝送時間 200 ms の間に長さ 2×10^6 の擬似乱数を伝送し、ボブとイブの持つ光検出器の出力を基にして通信路の通信路の強度分布を抽出し、そこから 4 ms ごとの相互情報量 $I(X;Y)$ 及び $I(X;Z)$ の計算を行った。なお、ボブの周りは十分な監視の下警護されており、屋上のイブが得られる以上の情報を得る盗聴者は現実的には存在しないと仮定している。以上の条件下で、物理レイヤ暗号としては最も単純であるワイヤタップ通信路符号化の伝送性能評価を行った。なお、前述のようにワイヤタップ通信路符号化の性能は秘匿容量にて測られるが、本研究ではパワーや擬似乱数源系列中の 0 と 1 の個数の最適化は行わないため、秘匿容量を求めることはできない。そのため、相互情報量の単純な差である秘匿レート

$$R_S = I(X;Y) - I(X;Z)$$

を用いて、秘匿伝送可能な情報量を評価する。このような解析を、14 : 43、15 : 57、16 : 33（当日の日没時刻）、17 : 37、18 : 10 の 5 つの時間帯で、20 秒ごとに 10 回行った。

図 4 に 16 : 43 : 20 と 17 : 37 : 00 に取得されたデータから計算された秘匿レートの時間変動を示す。なお、本実験ではボブの通信路がほぼエラーフリーとなっていた点に注意する。

図 4（a）に示した 16 : 43 : 20、すなわち日没直後の結果では、秘匿レートは 10 Mbps（24 ms から 28 ms の間）から、0 bps（144 ms から 148 ms）へと、200 ms の間でも大きく変化している。その一方で、図 4（b）に示す 17 : 37 : 00、すなわち日没後の結果では、この秘匿レートの時間変動は小さく抑えられている。以上より、日没前や直後では大気のゆらぎによって生じる強度変調やビームワンダリングの影響によって致命的な情報漏洩が発生する一方で、夜間にはその影響が抑えられ、物理レイヤ暗号を利用して安定した秘匿伝送が可能になることが示されている。

以上に述べた大気による影響をより統計的に考察するために、あるしきい値 R_{th} よりも秘匿レート R_S が下回る確率

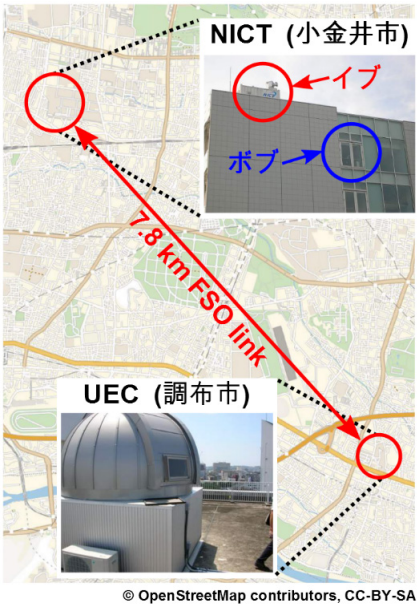

図 3　Tokyo FSO Testbed の概略図 [37]. ©OpenStreetMap contributors, CC-BY-SA.

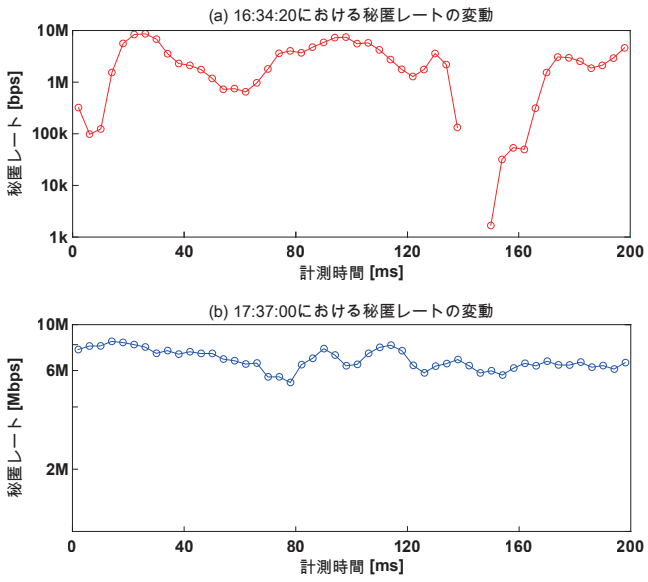

図 4　(a) 2015 年 11 月 17 日 16 :34 :20 及び (b) 同日 17 :37 :00 に取得されたデータから計算された秘匿レート。各点の測定時間幅は 4 ms であり、長さ 4×10^4 の擬似乱数系列に対応している [38]。

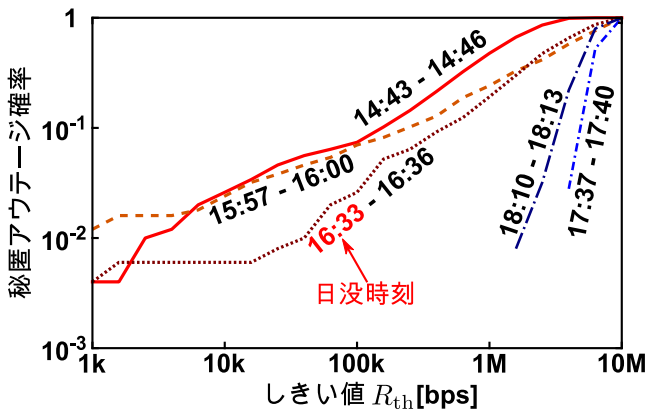

図 5　2015 年 11 月 17 日に取得されたデータから計算された秘匿アウテージ確率 [38]。

$$P_{Out}(R_{th}) = \Pr(R_{th} > R_S)$$

の評価を 5 つの時間帯ごとに得られた実験データに対して行った。このしきい値を符号設計の際に定める目標レートとみなせば、設計した符号が秘匿伝送に失敗する可能性としても解釈できるため、この量を秘匿アウテージ確率 $P_{Out}(R_{th})$ と呼ぶ。この $P_{Out}(R_{th})$ を、5 つの時間帯ごとの実験データに基づいて計算し、図 5 に示す。日没前ではしきい値 R_{th} をどれほど低くしても、秘匿アウテージ確率を 0 にすることはできない一方で、大気の状態が安定する日没後では秘匿アウテージ確率を 0 にできるしきい値が存在している。これは、図 4 で議論した日没前後における秘匿レートの時間変動に関する議論と合致している。

以上のような、実験データに基づく大気のゆらぎが物理レイヤ暗号に与える影響の議論は我々が知る限り上記の実験が最初であり、今後の光空間通信における物理レイヤ暗号の研究、ないしはプロトコルの開発に向けた、重要な知見を得ることができた。

5　まとめ

本稿では、物理レイヤ暗号という技術の情報理論的な概略と、その実用化に向けて量子 ICT 先端開発センターが取り組んできた、様々な気象条件とそれらが物理レイヤ暗号に及ぼす影響を実データから明らかにする研究について述べてきた。現在では更なる実用化に向けて、長年培ってきた QKD に関する技術を下敷きにした秘密鍵共有プロトコルの開発や、光通信の性質を活かした新機軸の鍵配布プロトコルといった研究に取り組んでいる。

当該技術の将来的な応用先としては、QKD では現実的な速度での鍵生成が困難である人工衛星–地上局間レーザ通信などが挙げられる。また、車々間通信や、主要ネットワークとユーザを結ぶラストマイル通信のような、安価で高速な秘匿通信が必要とされるアプリケーションも重要な応用先である。さらには、異なる OSI レイヤ上で運用される現代暗号と組み合わせることで多層レイヤ的な暗号プロトコルや、ユーザのニーズに合わせて QKD との使い分けを行う柔軟な暗号システムの提供も可能となる。冒頭でも述べたように、光空間通信における物理レイヤ暗号の実証例はいまだ報告されていないが、そのような技術の実証を世界に先駆けて行うことは、単なる通信システムの開発という以上に、学術的にも大きな意義を持つ。

しかしながら、解決すべき問題も山積している。光空間通信におけるビームが狭いとはいえ、無線通信は空間に対して開かれており、イブが講じることのできる手段はビームの中心から離れた位置での盗聴や反射光や散乱光の検出、小型機での盗聴など、実に多岐にわたる。これらの各手段に対して、監視などの手段によってイブの盗聴を防止し、なおかつ漏洩している情報量の最悪値を推定する決定的手段が現状では存在しておらず、何よりも優先すべき急務と言っても過言ではない。現在、量子 ICT 先端開発センターでは、上記で述べた実用的なプロトコル開発と並行して、盗聴者の能力推定や発見システムを検討することによって、光空間通信における物理レイヤ暗号が抱えるこの問題に対して真っ向から取り組んでいる。

謝辞

本研究は、総合科学技術・イノベーション会議により制度設計された革新的研究開発推進プログラム（ImPACT）により、科学技術振興機構を通して委託された。また、早稲田大学応用物理学科の青木隆朗教授、東京工業大学工学院の松本隆太郎准教授、東海大学通信ネットワーク工学科の高山佳久教授からの協力に感謝する。

【参考文献】

1　A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, Oct. 1975.
2　I. Csiszár and J. Körner. “Broadcast channels with confidential messages,” IEEE Trans. on Inform. Theory, vol.24, no.3, pp.339–348, March 1978.
3　C. E. Shannon, “Communication theory of secrecy systems,” Bell Labs Tech. J., vol.28, no.4, pp.656–715, 1949.
4　U. M. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol.39, no.3, pp.733–742, March 1993.
5　R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography: I. Secret sharing,” IEEE Trans. Inform. Theory, vol.39, no.4, pp.1121–1132, April 1993.
6　W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inform. Theory, vol.22, no.6, pp.644–654, Nov. 1976.
7　T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless

secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Trans. Antennas Propag, vol.53, no.11, pp.3776–3784, Nov. 2005.
8 S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. 14th Annu. Int. Conf. Mobile Comput. Netw., pp.128–139, 2008.
9 Jana, S., Pnemath, S., N., Clark, M., Kasera, S., K., Patwari, N., and Krishnamurthy, S., V., "On the effectiveness of secret key extraction from wireless signal strength in real environments," Proc. 15th Annu. Int. Conf. Mobile Comput. Netw., pp.321–332 , 2009.
10 S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," IEEE Trans. Mobile Comput., vol.12, no.5, pp. 917–930, May 2013.
11 J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol.4, pp.614–626, Jan. 2016.
12 Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," IEEE Wireless Commun. vol.18, no.2, pp.66–74, April 2011.
13 C. H. Bennett and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing," in Proc. IEEE ICCSSP, pp.175–179, 1984.
14 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol.74, no.1, pp.145–195, Jan. 2002.
15 V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Düsek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol.81, no.3, pp.1301–1350, July 2009.
16 C. Elliott, et al., "Current status of the DARPA quantum network," quantum information and computation III Proc. SPIE 5815 pp.138–149, 2005.
17 M. Peev, et al. "The SECOQC quantum key distribution network in Vienna," New J. Phys., 11, 075001, July 2009.
18 M. Sasaki, et al., "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express, vol.19, no.11, pp.10387–10409, May 2011.
19 D. Stucki, et al., "Long-term performance of the SwissQuantum quantum key distribution net-work in a field environment," New J. Phys. vol.13, 123001, Dec. 2011.
20 S. Wang, et al., "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express, vol.22, no.18, pp.21739–21756, Sept. 2014.
21 ID Quantique (2001), http://www.idquantique.com/; MagiQ Technologies, Inc. (1999), http://www.magiqtech.com/MagiQ/Home.html; QuintessenceLabs Pty Ltd. (2006), http://www.quintes-sencelabs.com/; QuantumCTekCo., Ltd. (2009), http://www.quantum-info.com.
22 A. R. Dixon, et al., "High speed prototype quantum key distribution system and long term field trial," Opt. Express, vol.23, no.6, pp.7583–7592, March 2015.
23 N. Wang, X. Song, J. Cheng, and V. C. M. Leung, "Enhancing the security of free-space optical communications with secret sharing and key agreement," IEEE/OSA J. Opt. Commun. Netw., vol.6, no.12, pp.1072–1081, Dec. 2014.
24 F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," IEEE Photon. J., vol.7, no.2, 7901014, April 2015.
25 A. Mostafa, and L. Lampe, "Physical-layer security for MISO visible light communication channels," IEEE J. Sel. Areas Commun, vol.33, no.9, pp.1806–1818, Sept. 2015.
26 H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," IEEE Photon. J., vol.7, no.5, 7903418, Sept. 2015.
27 X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," IEEE Photon. J., vol.8, no.1, 7901110, Feb. 2016.
28 D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," IEEE Photon. J., vol.8, no.5, 7804809, Jan. 2016.
29 M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," IEEE Trans. Inf. Theory, vol.57, no.6, pp.3989–4001, Jun. 2011.
30 T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," IEEE Trans. Inform. Theory, vol.60, no.11, pp.6819–6843, Nov. 2014.
31 J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in proc. IEEE ISIT, pp.601–605, June 2014.
32 G. Brassard, and L. Salvail, "Secret key reconciliation by public discussion," In Proc. EUROCRYPT '93, pp.410–423, 1994.
33 C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," SIAM J. Comput., vol.17, no.2, pp.210–229, 1988.
34 C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inform. Theory, vol.41, no.6, pp.1915–1923, June 1995.
35 R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Dept. Comput. Sci., ETH Zurich, Zurich, Switzerland, 2005.
36 J. L. Carter and M. N.Wegman, "Universal classes of hash functions," J. Comp. Syst. Sci., vol.18, pp.143–154, 1979.
37 H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone, P. Villoresi, T. Aoki, and M. Sasaki, "Free-space optical channel estimation for physical layer security," Opt. Express, vol.24, no.8, 259736, April 2016.
38 H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, H. Takenaka, R. Shimizu, T. Aoki, and M. Sasaki, "Physical layer cryptography in free-space optical communications: Performance estimation in real-field experiment and coding method," IEICE Tech. Report, vol.IEICE-116, no.183, pp.7–12, Aug. 2016.

遠藤寛之　（えんどう　ひろゆき）
未来 ICT 研究所
量子 ICT 先端開発センター
研究員
博士 (理学)
物理レイヤ暗号、光空間通信

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

北村光雄　（きたむら　みつお）
未来 ICT 研究所
量子 ICT 先端開発センター
研究技術員
光通信

都筑織衛　（つづき　おりえ）
未来 ICT 研究所
量子 ICT 先端開発センター
研究技術員
光空間通信

伊藤寿之　（いとう　としゆき）

未来 ICT 研究所
量子 ICT 先端開発センター
研究員
博士（地球環境科学）
物理レイヤ暗号、光空間通信

清水亮介　（しみず　りょうすけ）

電気通信大学
准教授
博士（理学）
量子光学

豊嶋守生　（とよしま　もりお）

ワイヤレスネットワーク総合研究センター
宇宙通信研究室
室長
博士（工学）
衛星通信、光通信、大気ゆらぎ、レーザ空間伝搬、量子暗号

竹中秀樹　（たけなか　ひでき）

ワイヤレスネットワーク総合研究センター
宇宙通信研究室
研究員
博士（工学）
光空間通信、誤り訂正符号

武岡正裕　（たけおか　まさひろ）

未来 ICT 研究所
量子 ICT 先端開発センター
センター長
博士（工学）
量子光学、量子情報理論

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