光空間通信における
物理レイヤ暗号に関する研究

Studies on Physical Layer Cryptography in Free Space Optical Communications

2017年2月

遠藤 寛之

Hiroyuki ENDO

光空間通信における
物理レイヤ暗号に関する研究

Studies on Physical Layer Cryptography in Free Space Optical Communications

2017年2月

早稲田大学大学院 先進理工学研究科
物理学及応用物理学専攻 量子光学研究

遠藤 寛之

Hiroyuki ENDO

目次

第 1 章

序論

近年の携帯電話及びスマートフォン，Internet of Things，そして人工衛星通信に関連した技術の進歩は目覚ましく，我々は高速かつ大容量の情報ネットワークを手のひらサイズの端末によって手軽に，そしてたとえ地上インフラが整備されていない過疎地域においても普遍的に利用できるようになりつつある．しかし，ネットワークを行き交うデータの大容量化に対して，有限で貴重な資源であるとも表現される電波無線周波数が枯渇しつつあるという現状は無視できない．

以上の状況において，レーザーや LED を空間中に伝搬させることで行われる光空間通信 [1] は，無線通信におけるフロンティア技術としてその重要さを大きく増している．光空間通信は数十 G ビット/秒 (以下，bps) に迫る伝送速度という光周波数に起因する特徴を持つ．加えて，送受信機がコンパクトに設計でき，かつ電力消費も低いことから，ペイロードが限られている機器にも搭載可能である．一方で，濃霧中での通信におけるビット誤り率の劇的な増加や，雲による衛星－地上局間レーザー通信の遮断などに象徴されるように，光空間通信の性能は天候の条件に大きく影響される．その対策として，十分に離れた複数地点に位置する地上局の連携で雲による送信レーザー遮断を回避するサイトダイバーシチ技術や，成層圏プラットフォーム [2, 3] による中継，低速ではあるものの霧や雲の影響を受けにくい電波無線通信を併用する光空間－電波無線ハイブリッド通信 [4] などの研究が活発に行われている．

光空間通信の主たる応用先としては，ラストワンマイル通信を安価で提供する手段 [5, 6] や，軍事目的 [7] 等が挙げられる．とりわけ華々しいのは，衛星光通信への応用 [8, 9, 10] である．すでに衛星間での 5.6Gbps の通信 [11] や，衛星-地上局間での 10Mbps 級の通信 [12] が成功裏に実施されている．加えて，成層圏プラットフォーム [2, 3] やドローン [13, 14, 15] といった無人航空機への光空間通信の利用も検討されている．これらの無人航空機を端末，あるいは中継器として用いる，地球規模の移動通信ネットワークは現実的なものになりつつある．

一方，宇宙，成層圏，地上における様々な端末が地球規模でつながりはじめると，ネットワークに対する脅威も必然的に増加する．実際，衛星通信ネットワークに対するサイバー攻撃や盗聴，なりすましは，その被害が甚大になりうるため，大きな脅威となってい

る．サイバー攻撃に対するマルウェア対策の必要性は言うまでもないが，「情報漏えいは起こりうるもの」との前提に立って，漏洩したデータの機密性が担保されるよう，適切な暗号化を行うことが強く望まれる．特に，使用可能な電力や計算機能力，搭載可能な質量に制約が課されている移動体にも利用可能な暗号技術の開発は，光空間通信の需要が高まっている現在において極めて重要な課題である．しかし，現在実用化されている，あるいは実用化されつつある技術が光空間通信による移動通信ネットワークに最適であるかは自明ではない．

現在のインターネットや携帯電話のような地上の通信網では，現代暗号と呼ばれる技術が用いられている．現代暗号は数理アルゴリズムとして計算機上に実現可能であるため，通信を担う物理的媒体に依存せずに利用可能であるという特徴を持つ．しかし，その安全性は「現在のところ解くのが困難であると仮定できる数学問題」に基づいており，計算技術の進展とともに安全性が危殆化していくことが知られている．そこで，現代暗号では，鍵の長さの伸長などといった，定期的な更新が必要となる．このような仕様のアップデートは莫大なコストが必要となる上に，高々度を飛来する人工衛星などにおいてはアップデート自体が容易ではない．

上記の数理アルゴリズムに基づく現代暗号とは異なり，通信路の物理的過程を使うことで安全な鍵の交換/共有や情報の秘匿化を行う暗号技術も知られている．その中でも最も実用化レベルにある技術が，乱数を量子状態に符号化して伝送する，量子鍵配送 (QKD)[16, 17, 18] である．不確定性原理に基いて，如何なる技術をもってしても盗聴不可能な強力な安全性を持つ一方で，その鍵レートや直接配送距離には厳しい制約がある．都市間ファイバ網による実証実験 [19, 20, 21, 22] では実用レベルに達しているものの，衛星地上局間といった超長距離での QKD であｈ鍵の生成レートが著しく低下してしまう．

以上に挙げた現代暗号と QKD の両者とも，将来的には通信ネットワークの安全性を確保する上での要となるべき技術である．そして，ユーザーは伝送を行う媒体やその情報に要求される安全性のレベルといった観点に基づき，これらの内から適切な方法を選択できることが望ましい．しかし，幅広く利用されている一方で安全性の危殆化が避けられない現代暗号と，強固な安全性と引き換えに鍵生成速度や伝送可能距離といった意味でのユーザービリティが制限される QKD の間には，安全性とユーザービリティとの間のトレードオフといった観点から大きなギャップが存在していると言わざるを得ない．このギャップを埋める技術を開発して，幅広い選択肢を用意することができれば，ユーザーは用途とコストに応じて最適な技術を選択できるようになる．

そのような中間領域に位置する技術として，通信路に内在する雑音を利用して秘匿化や鍵共有を行う物理レイヤ暗号 [23, 24] が注目を集めている．盗聴者の能力に一切の仮定を必要としない QKD に対して，物理レイヤ暗号では盗聴者に対して合理的に課すことができる物理的な仮定 (監視下にある通信路へのアクセス能力，得られた情報と乱数源との無相関性など) を導入することにより，伝送性能の大幅な改善が期待できる．また，盗聴者に対する仮定が満足されている限り，どのような計算機をもってしても解読不可能であることが数学的に証明できる．

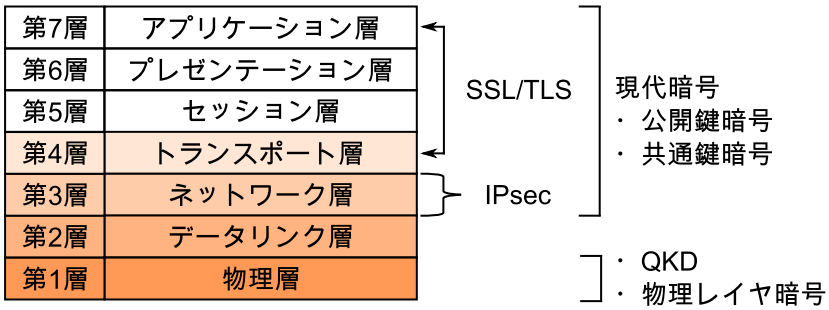

図 1.1　OSI 参照モデルの概念図.

特に，物理レイヤ暗号と光空間通信は親和性の高い技術である．すなわち，光空間通信は集光性の高い光源により見通し通信で行われるため，送信者と受信者が回線を広角視野のカメラで監視することで，盗聴者の通信路への物理的なアクセス能力を合理的に制限できる．以上に述べた背景及び着想の下，本研究では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を行った．

以降の各節では，通信における物理層と呼ばれる概念の取扱からはじめ，物理レイヤ暗号の概要とその周辺の話題について述べていく．そして，本研究の目的と当該分野への寄与について述べる．

1.1　はじめに：物理レイヤ暗号とは

本節では，本研究の主題ともなる，物理レイヤ暗号を導入する．その過程で，現時点において実際に利用されている，あるいは実用化レベルにある代表的な暗号技術を紹介していき，物理レイヤ暗号とそれらの技術の比較を様々な観点から行う．以降，慣習として，送信者をアリス，正規受信者をボブ，盗聴者をイブと呼称する．

通信の安全性を保証するためには暗号と呼ばれる技術が利用されている．暗号の起源はローマ時代のカエサル式暗号まで遡り，第二次世界大戦中にもエニグマ暗号をはじめとする多くの暗号が戦略上の機密保持のために用いられてきた．そのような古典的な暗号では，あるキーワード (鍵) に関する情報を一切持たないユーザーが秘密メッセージ (または平文) を参照できない仕組を用いることで情報を秘匿していた．現代ではインターネット上での商取引やデータのストレージサービスの発達に伴い，下記に挙げるような様々な機能が暗号に要求されるようになっている．

機密性の確保　特定のキーワード (鍵) を持たないイブへの情報漏洩を防ぐ機能.
鍵交換/鍵共有　他の暗号プロトコルに利用可能な鍵を供給する機能.
電子署名　ドキュメント，あるいは鍵が改ざんされていないことを保証する機能.
暗号化状態処理　暗号化されたデータに対する検索や，暗号化されたデータ同士の演算など，データを暗号化した状態のまま処理する機能.

暗号技術の発達は通信システムの発達と明確に相関があり，OSI 参照モデルとそこにおける「層」という概念を用いて大まかに特徴づけされる．OSI(Open Systems Interconnection) 参照モデルは ISO (International Organization for Standardization：国際標準化機構) によって作成された，ネットワーク機器に要求される動作を，図 1.1 に示すように 7 つの階層に分類した概念モデルである．ある層とそのすぐ下の層は参照/被参照の関係となっており，最下層に進むに連れて抽象化されたデータの単位 (パケット，フレーム，ビットなど) を扱っていき，最下層の物理層では，0 と 1 のビット列で表現されたデータを通信媒体 (金属ケーブル，光ファイバ，自由空間など) 中を伝搬する物理的実体 (電気信号，電波，光) に変換して他のユーザーに伝送する．

現代の地上網ネットワークでは，数理アルゴリズムとしてプログラム実装できる現代暗号が利用されている．これらは，OSI 参照モデルでは第 3 層以上の物理的実体が関与しない層において提供されている．現代暗号の内，共通鍵暗号は機密性の確保という最も基本的な機能を実現する．アリスとボブが同じ鍵を用いて秘密メッセージの暗号化と再生 (復号) を行うため高速な秘密メッセージ伝送を実現できる一方で，その鍵を安全に交換あるいは共有する必要がある．そこで，現代の多くの通信ネットワークでは，暗号化と復号に利用される鍵が異なる公開鍵暗号を用いて，必要な 2 者間での鍵交換を実現している．また，公開鍵暗号は電子署名の機能も実現できるため，ネットワーク上での商取引を行う上で重要な位置を占めている．現在広く使われている公開鍵暗号 (RSA 暗号など) は量子計算機が実現すれば解読されてしまうことが知られているため，暗号標準化機関では，量子計算機を用いた解読に対しても耐性を持つとされている，耐量子計算機暗号と呼ばれる新しい公開鍵暗号への移行準備を始めている．

以上のような計算機上で実現可能な現代暗号とは対象的に，近年では通信路の雑音等の物理現象を利用して安全性を確保する暗号技術も研究され始めている．その 1 つは，量子力学の原理に基づき，いかなる技術を持ったイブに対しても安全な鍵共有を提供する量子鍵配送 (QKD) である．そして，もう 1 つはイブに合理的な物理的仮定を課し，その仮定に基づいた実装の下で情報理論的に証明可能な安全性を保証する物理レイヤ暗号である．この名称は物理的な通信路に対応する OSI モデルの第 1 層，すなわち物理層に由来する．

図 1.2 に，以上の各暗号技術の比較を，横軸を方式としての速度，縦軸を機能でまとめたグラフを示す．QKD は鍵共有の機能のみを実現し，その速度は無条件安全性という強力な安全性と引き換えに大きく制限されたものとなっている．一方で物理レイヤ暗号は機密性の確保と鍵共有の 2 つの機能を実現する．そして，イブの物理的能力に一定の制限を仮定することで，QKD では到達不可能な鍵生成速度と伝送距離を実現する．

以上のように，数理アルゴリズムとして実装可能な現代暗号と，通信路の物理的過程を利用する暗号の 2 種類が現在主流な暗号となっている．以下本節の残りでは，それぞれの暗号技術の詳細について述べていく．

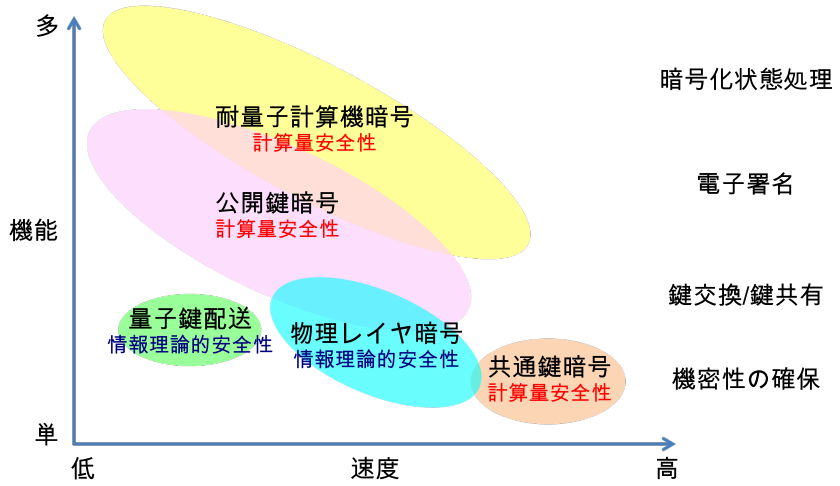

図 1.2　代表的な暗号技術における，速度と機能の関係図．

1.1.1　現代暗号：計算量的安全性に基づく暗号技術

現代暗号の特徴として，数理アルゴリズムによって計算機上に実装可能であることが挙げられる．そのため，OSI 参照モデルにおける第 3 層以降で定義され，通信を担う媒体とは無関係に利用することができる．これが現代のセキュリティインフラにおいて広く利用されている所以の一つである．

一方で，その安全性は，現在の技術水準を鑑み，イブが利用可能な計算機能力に仮定を設定した上での安全性となっている．このような安全性を計算量的安全性と呼ぶ．計算量安全性の危殆化の要因としては，これまで求解が困難であった数学的問題を量子の重ね合わせを利用して容易に解いてしまう量子計算機アルゴリズムの発見 [25, 26, 27, 28] が象徴的に挙げられることが多い．量子計算機の実現にはまだ時間がかかるとする意見もあるが，実際にはアルゴリズムの改良や分散コンピューティング技術の発達によって，現代暗号の安全性は日々危殆化していると言っても過言ではない．例えば，PC でグラフィックスの処理に用いられる GPU(Graphics Processing Unit) で並列計算を行う GPGPU(General Purpose GPU) という手法を暗号解読に転用する研究などもある [29, 30]．

以上の安全性の危殆化に対しては，鍵長を伸長し，解読にかかる時間を増加させるといった対策が取られる．そのため，定期的な仕様のアップロードが必要不可欠となる．記憶に新しい例としては，アメリカ国立標準技術研究所による，2010 年を目処にこれまで用いられてきた暗号を廃止して，より長い鍵長を持った暗号へ移行すべしとするガイドラインの発表が挙げられる [31]．しかし，ネットワークインフラに遍く浸透した暗号方式の変更には莫大なコストが必要となり，運用上の一つのネックとなる．

以下，このカテゴリに属する共通鍵暗号，公開鍵暗号，そして耐量子計算機暗号の 3 つについて述べる．

共通鍵暗号

共通鍵暗号とは，暗号化のための鍵と復号のための鍵が同一である暗号体系である．代表的な方式としては，DES(Data Encryption Standard)[32] や AES(Advanced Encryption Standard)[33] などが知られている．暗号化と復号を同じ鍵で行うということは，取りも直さず比較的高速な暗号化と復号が可能であり，大量データの秘匿伝送に適している．

一方で，アリスとボブの間での鍵をイブに漏洩せずに共有する手段が必要となる．そのため，ネットワーク層で提供される，IP パケット単位で改竄防止や秘匿通信を行うための IPsec というプロトコルや，第 4 層で定義されている SSL / TLS(Secure Socket Layer / Transport Layer Security) というプロトコルでは，後述する公開鍵暗号と組み合わせて利用される．

共通鍵暗号に対する有効な攻撃としては，鍵の候補となり得る系列を一つ一つしらみつぶしに試すことによって鍵を発見する全数探索が知られている．実際に，鍵長 56 ビットの DES は，1999 年にネットワークで接続された 10 万台の計算機を利用することで，所要時間 22 時間 15 分で解読されている [34]．一方で，鍵長 128 ビットの AES の解読には 2^{128} 回の試行を行う必要があり，毎秒 1 万の系列をチェックできるような計算機を 1 億台つないだとしても，全数探索には約 1000 京年を要する．

より洗練された攻撃としては，アルゴリズムの特徴を逆手に取って，全数探索の試行回数を減少させるものが知られている．例えば選択平文攻撃では，平文を公開されたアルゴリズムで暗号化し，得られた暗号文と平文のペアを収集することで鍵の推測を行う．実際に，2 つの異なる鍵を用いる鍵長 112 ビットの 2-key トリプル DES は，選択平文攻撃によってその安全性が 80 ビット相当に減少することが知られている．暗号文の統計的な偏りから鍵の範囲を限定し，少ない計算量で解読を目指すショートカット法 [35, 36] 等も有効な攻撃である．

公開鍵暗号

メッセージの暗号化と復号を同一の鍵で行った共通鍵暗号方式に対して，公開鍵暗号方式では，暗号化は全ユーザーに公開されている暗号化用の鍵 (公開鍵) で行われ，復号は受信者だけが秘密に保管している復号用の鍵 (秘密鍵) で行われる．そのため，共通鍵暗号のように鍵の事前共有の必要は無いが，アルゴリズムが比較的に複雑であるために処理速度は低速になる．従って，前述のように，公開鍵暗号は共通鍵暗号の鍵を共有する手段として用いられる．また，公開鍵と秘密鍵を分離したことにより，管理すべき鍵の量は大幅に削減されため，共通鍵暗号では多数ユーザー間での鍵管理の複雑さから現実的でなかった，電子署名としての機能も獲得できた．

公開鍵暗号方式の安全性は，解が正しいことの確認は容易であるが，求解が既存の技術では膨大な時間が必要となるために現実的に困難であるという一方向性を持つ数学的問題に依拠する．例えば，RSA 方式 [37] では非常に大きい素数の積からなる合成数の素因数

分解が利用され，ElGamal 方式 [38] では位数が大きい群の離散対数問題が利用されている．また，160 ビットの鍵長で，鍵長 1024 ビットの RSA 暗号と同等の安全性を持つとされる楕円曲線暗号 [39, 40] では楕円曲線上の離散対数問題を利用している．

以上のように，安全性を数学的問題に依拠しているため，それらの問題を効率的に解くアルゴリズムや，計算機能力の向上，あるいは計算機モデルの変化によって，その安全性はやはり危殆化する．計算機モデルの変化による危殆化の例としては，特定の問題を高速に解く量子計算機アルゴリズムの発見が挙げられる．実際に，量子計算機で素因数分解を高速に解く Shor のアルゴリズム [25, 26] によって RSA 暗号は解読可能であることが証明されている．

耐量子計算機暗号

量子計算機が得意とする問題は，素因数分解問題や離散対数問題などの整数論における問題であり，これらは前述した公開鍵暗号の基礎となっていた．対して，組合せ論等の量子計算機が苦手とする (つまり，量子計算機アルゴリズムが見つかっていない) 問題に基づく暗号の研究も活発に行われている．これらの暗号は総称して，耐量子計算機暗号と呼ばれる．以下に，いくつかの方式について概説する．

格子暗号 [41, 42, 43, 44] は，格子ベースの耐量子計算機暗号として知られている．格子暗号の安全性は，与えられたベクトルの組を整数倍することで構成される格子点の中から条件を満足するものを探索する，格子点探索問題に依拠する．さらに，格子暗号は，暗号化されたデータに対するキーワード検索 (秘匿検索) や統計処理及び数値計算 (秘匿計算) も実行可能である．これらはいわゆる暗号化状態処理技術と呼ばれ，クラウドサービス等で重要性が増している．そのため，格子暗号の生体認証やクラウドシステムでの実用化に向けた研究が活発に行われている [45].

符号ベースの耐量子計算機暗号としては，McEliece によるもの [46] や，それを元にした Niederreiter によるもの [47] が特に知られている．特に，二元 Goppa 符号を用いたこれらの方式は高い安全性を持つことが知られている．実際に，欧州における耐量子計算機暗号の勧告を行う組織の 1 つである PQCRYPTO は，量子計算機に対して長期間の安全性を持つ方式の 1 つとして，二元 Goppa 符号に基づく McEliece 暗号の利用を提案している [48].

また，RSA 暗号よりも高速な鍵共有を目的に開発された，多変数公開鍵暗号 [49] なる方式も，耐量子計算機暗号の一種として知られている．その安全性は，高次連立方程式の求解困難性に依拠している．

量子計算機アルゴリズムの内, データベース検索に関する Grover の量子アルゴリズムを用いると，全数探索に必要な計算量は平方根まで減少させることができる [27, 50, 51, 28]. 例えば，鍵長 128 の AES の安全性は鍵長 64 相当にまで低下するが，それでもこの鍵長の全数探索には莫大な計算量が必要となる．そのため，その他の有効な解読方法が発見されない限りは，十分に長い鍵長の共通鍵暗号も耐量子計算機性を持つ.

以上のように様々な方式が研究されている耐量子計算機暗号であるが，解読法の研究も

同時に進められている．例えば 2009 年に IEEE で標準化された [52] 格子暗号の一種である NTRU(NTRU:N-Th Degree Truncated Polynomial Ring) 暗号 [43] は，その後に開発されたアルゴリズムで解読できることが示され [53]，安全性レベルの見直しが行われている．また，多変数公開鍵暗号として最初の方式である MI(Matsumoto-Imai) 暗号 [49] を署名に応用した S-FLASH[54] という方式は，EU が制定した暗号規格 NESSIE(New European Schemes for Signature, Integrity, and Encryption) において 2003 年に選定されたが，Dubois らが考案した攻撃アルゴリズム [55] によって 1 時間で解読されてしまった．以上のように，耐量子計算機暗号と言えども安全性が数学的問題に依拠しているため，危殆化のリスクは依然として存在する点に注意を払う必要がある．

1.1.2 情報理論的安全性に基づく暗号

情報理論的安全性とは，計算量的安全性とは対象的に，例えイブが無限大の計算能力を持っていたとしても，解読が不可能であることを数学的，あるいは情報理論的に証明できる安全性である．その証明は，平文とイブが持つ全ての情報とが統計的に無関係であることを，Shannon エントロピーなどの情報理論的な諸量を用いて示すことにより行われる．従って，情報理論的安全性に基づく暗号は計算機技術の進歩では安全性が危殆化しない．しかし，情報を伝搬する媒質によっては速度に制約が課せられたり，そもそも現実的な運用が困難である可能性もある．

以下では，情報理論的に安全な暗号方式として，Vernam のワンタイムパッド暗号，量子鍵配送，そして物理レイヤ暗号についてまとめる．

Vernam のワンタイムパット暗号

節 1.1.1 で述べた共通鍵暗号において，平文が “0” と “1” からなる系列で表現されている場合を考える．同時に，平文と同じ長さの “0” と “1” からなる乱数列を鍵として利用する．暗号化は平文と鍵の間の排他的論理和によって行われ，復号も暗号文と鍵の間の排他的論理和で成される．そして，ボブが復号を完了した時点で，利用した鍵を破棄する．以上の演算のアイデアははじめ Vernam [56] によって提唱されたため，上記のステップを踏む暗号を Vernam のワンタイムパッド暗号と呼ぶ．

すでに述べたように，共通鍵暗号と Vernam のワンタイムパット暗号との違いは，前者では鍵長が平文の長さよりも短く，後者では鍵長と平文の長さが等しいという点にある．そのため，Vernam のワンタイムパット暗号では，鍵に関する情報を一切持っていないイブは暗号文から平文をランダムに推測する他の攻撃方法を持ち得ない．すなわち，破棄すべき暗号鍵を再利用するなどの不適切な運用を行わない限りにおいて，情報理論的安全性が担保される暗号方式となっている．実際に，平文の長さよりも長い鍵を用いた場合に情報理論的安全性が満足されることが Shannon [57] によって証明された．

当然ながら，共通鍵暗号同様にの鍵の配送及び管理に関する問題を抱えている．特に，平文と同じ長さの鍵が必要になるため，鍵配送の問題は共通鍵暗号のそれよりも深刻なも

のとなる．

量子鍵配送

量子鍵配送 (Quantum Key Distribution; QKD)[16, 17, 18] は，離れた 2 地点の間で，いかなる技術を持つイブに対しても情報が漏洩しない鍵共有の方法として，1984 年に Bennett と Brasard[16] によって考案された．提案後 10 年ほどは大きな関心を集めなかったが，前述のように公開鍵暗号がその安全性の根拠とする数学的問題を高速で解くアルゴリズムが発見され，既存の暗号方式に対する新たな脅威であると認識され始めたため，それに伴って QKD も注目を浴びることとなる．

QKD では “0” と “1” からなる乱数列を，偏光の重ね合わせ状態やもつれ状態に代表される量子状態を適切に制御した信号によって送る．通信路上でイブが試みるあらゆる盗聴行為は，この量子状態にある信号にその痕跡を残してしまうため，アリスとボブが公開通信路上でのディスカッションを通じて盗聴された疑いのあるビットを削除することによって，盗聴の恐れのない安全なビット列を共有することができる．実際に，イブが物理法則上許される如何なる技術で盗聴を行ったとしても，鍵長を長くすることで暗号鍵に関するイブへの漏洩情報量を任意に小さくすることができることを証明することができる．この証明には，イブの能力に対する一切の仮定が必要ないため，QKD の安全性は無条件安全性と呼ばれる．このように共有した鍵を，Vernam のワンタイムパッド暗号の鍵として利用することで，未来永劫如何なる技術によっても破られない，情報理論的に安全な秘匿通信が実現できる．

QKD は量子力学の原理を応用した通信技術の中でも特に実用化が進んでいる技術である．実際に，様々な企業から送受信機が製品として販売され [58, 59, 60, 61]，都市圏ファイバ網による実用実験が様々な研究機関によって実施されている [19, 20, 21, 22]．

しかしながら，無条件安全性と引き換えに伝送可能距離と鍵生成速度が大きく制限されているという問題を抱えている．光ファイバー伝送における直近の研究 [62] では，45km(伝送ロス 14.5dB) の伝送において，300kbps の鍵生成速度で 34 日間の連続稼働が報告されている．しかし，これが光空間通信による長距離実装となると，鍵生成速度は極端に小さいものとなる．そのような実験の中で代表的なものとして，LaPalma 天文台と欧州宇宙機関が所有する Tenerife 地上局を結ぶ，伝送距離 144km の光リンクを利用した一連の実験 [63, 64, 65] が知られている．この内，おとりつき BB84 と呼ばれる方式を利用した実験 [63] における鍵生成速度は 2bps であった．このことは，低軌道を地球の自転速度よりも高速に周回する低軌道衛星と地上局間の鍵共有を考えた場合，通信可能時間が数分程度しか確保できないため，十分な量の鍵の共有が本質的に困難であることを示唆している．

物理レイヤ暗号

以上のように，QKD はイブの能力に一切の仮定を置かない堅固な安全性を誇る一方で，伝送可能距離や鍵生成レートがどうしても制限されるため，超長距離の光空間通信では満

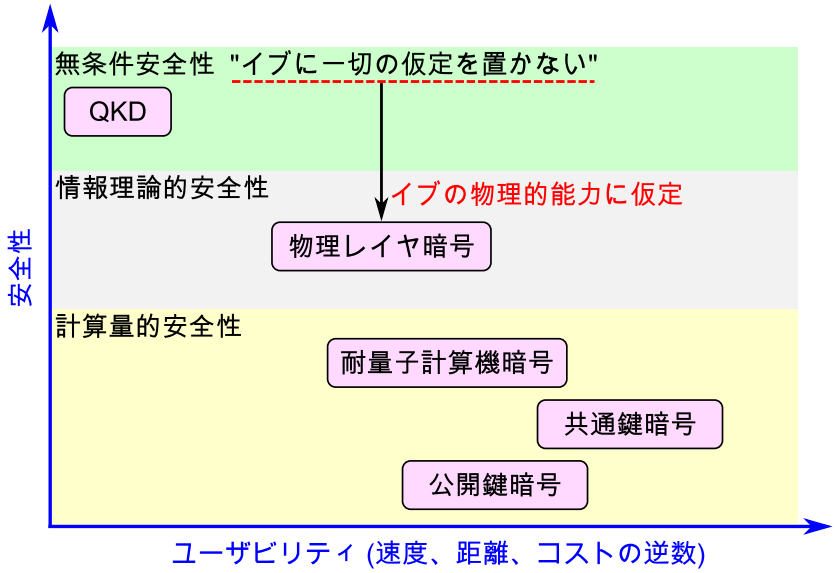

図 1.3 代表的な暗号技術における，ユーザビリティと安全性の関係図.

足な伝送性能を実現できなくなる.

これに対して，本論文で主題とする物理レイヤ暗号は，実際の利用シーンに則した「イブへの物理的制限」を仮定し，その過程の下で QKD よりも距離と速度を大幅に向上させることが期待できる．ここで，イブへの物理的制限に関する仮定としては，通信路や情報源へのアクセスに対する制約が挙げられる．例えば，狭いビームの見通し通信で行われる光空間通信では，アリスとボブが広角のカメラで対向して通信路上の監視を行うことができ，イブがビーム中心に入り込めば即座に検知されるため，結果として，イブは劣悪な状況での盗聴を余儀なくされる．また，電波無線通信では，電波のビルや壁などでの反射や回折，あるいは他の電波との干渉によって生じるフェージングによる，受信強度のランダムな時間変化が発生する．同じ伝搬路を通過してきた搬送波の強度変化には強い相関を持つ一方で，半波長分離れたい位置ではほぼ無相関となる，いわゆる相反性と呼ばれる性質を利用して，イブが得られる情報に対して制限を課すことが可能である．以上のようなイブへの仮定に基づき適切に設計及び運用された物理レイヤ暗号は，情報理論的に安全な秘匿通信及び鍵共有を実現できる.

図 1.2 は，横軸を速度や伝送可能距離，コストパフォーマンスといった意味でのユーザビリティととり，縦軸を安全性とした上で，ここまで紹介してきた暗号技術を整理，比較した概念図である．共通鍵暗号と公開鍵暗号，耐量子計算機暗号はイブの計算能力に仮定を課す計算量安全性に依拠する反面，高速かつ多機能であり，物理的媒体に無関係に運用可能である．そのため，この図では右下に位置する．一方で，QKD は無条件安全性という強力な安全性を持つものの，速度や伝送距離は制限されるため，この図では左上に位置する．すなわち，この図で述べると現代暗号と QKD の間には大きなギャップが存在することになる.

本研究の主題となる物理レイヤ暗号の安全性は，盗聴者に対して課すことができる物理

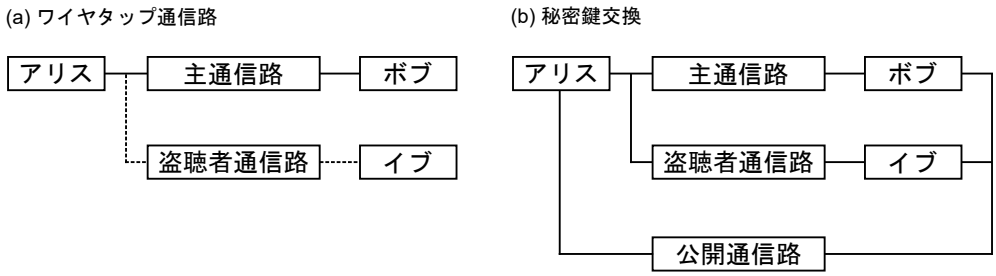

図 1.4 (a) ワイヤタップ通信路と (b) 秘密鍵共有のモデル.

的仮定に基いて，QKD の無条件安全性という強力な安全性を緩めたものとなっている．その上で，物理レイヤ暗号は QKD と比較してユーザビリティを大幅に向上させている．すなわち，物理レイヤ暗号は，現代暗号と QKD という 2 つの技術間に存在するギャップを埋める技術であると解釈できる．

本研究では物理レイヤ暗号にカテゴライズされる方式として，以下に挙げる 2 つの方式を扱う．1 つは，事前の鍵共有無しでの秘匿通信を実現するワイヤタップ通信路符号化 [66, 67] である．この方式は，図 1.4(a) に示すように，アリスがボブに秘密メッセージを伝送する主通信路と，イブが盗聴を行う盗聴者通信路という 2 つの通信路によってモデル化される．ここで，イブが通信路への物理的アクセスが制限されている等，イブがボブよりも悪い条件で通信を行うという仮定が成立するならば，イブには一切の情報が漏洩せず，ボブだけが情報を得ることができるような符号化をメッセージに施すことにより，鍵の共有が必要のない情報理論的に安全なメッセージ伝送を実現する．

もう 1 つの形式は，情報理論的に安全に鍵共有を行うための，秘密鍵共有 [68, 69] と呼ばれる方式である．図 1.4(b) に示すように，アリスは主通信路と盗聴者通信路を通して，それぞれボブとイブに乱数を送付し，その後 QKD 同様に公開通信路を通した後処理によって鍵を抽出する．ワイヤタップ通信路符号化との大きな違いは，公開通信路を利用した後処理を行うため，主通信路と盗聴者通信路の間の優劣に関する仮定が必要なく，イブがボブよりも好条件で盗聴が行えたとしても鍵を共有できるという点にある．一方で，公開通信路の使用に際して，その帯域や，認証の必要性などの議論が必要となる．

以上の各方式の詳細については次節，また，情報理論的な定式化については第 2 章について述べる．

1.2 物理レイヤ暗号の基本モデル

前節で述べたように，物理レイヤ暗号は，鍵無しでの秘匿通信を実現するワイヤタップ通信路符号化 [66, 67] と，QKD 同様に公開通信路を通した共有乱数に対する事後処理によって鍵を共有する秘密鍵共有 [68, 69] という 2 つの方式が存在する．本節では，第 2 章で与える情報理論的な定式化に先立ち，両者の概説を行う．

1.2.1 ワイヤタップ通信路符号化

情報理論において，誤りのない通信を行うために，伝送したいメッセージに冗長な情報を加える操作を通信路符号化と呼ぶ．ワイヤタップ通信路符号化は，情報理論的安全性が実現されるように拡張された通信路符号化であり，ボブに対する誤り無しの情報伝送と，イブに対する情報漏えい防止という 2 つの機能を備える．以下，通信路符号化について概説した後に，ワイヤタップ通信路符号化の機能について述べる．

通信路符号化

アリスが誤りの発生する通信路を通してメッセージを伝送すると，ボブは誤ったメッセージを受信する．そのような誤りの影響を打ち消して，ボブが正しいメッセージを再生できるようにするアイデアとしては，メッセージと誤り訂正のための情報を併せて伝送するといったものが挙げられる．例えば，3 ビットのメッセージ (0,1,0) を伝送する際には，各ビットのコピーを 2 つ同時に伝送 (0,0,0,1,1,1,0,0,0) すれば，3 つの同一のビットに生じた 1 つの誤りを多数決的に訂正することができる．

メッセージに誤り訂正のための冗長情報を加える操作を通信路符号化，あるいは単に符号化と呼ぶ．そして，符号化の結果として生成される，メッセージに冗長情報が加わった系列を符号語と呼ぶ．この符号語を誤りの発生する通信路に入力すると，符号語に誤りが重畳された系列，すなわち受信語が出力される．ボブは受信語からアリスの伝送したメッセージを再生する，復号と呼ばれる操作を行う．

通信路符号化には，訂正可能な誤りの数と伝送効率の間に明確なトレードオフの関係が存在する．上に挙げた多数決復号の例の場合では，同時に伝送するコピービットの数をより多くすればそれだけ多くの誤りが訂正できるが，それだけ伝送に多くの時間がかかるため効率的ではなくなる．そのため，アリスの目的は，メッセージに対してできるだけ少ない冗長情報を加えることで，ボブがメッセージの再生に失敗する確率を 0 にすることにある．

Shannon の通信路符号化定理は，通信路が与えられた場合に，通信路符号化によって誤りなしに伝送可能な情報量の上界を示す．今，アリスが k ビットのメッセージに対して $n-k$ ビットの冗長情報を加えて，n ビットの符号語に符号化したとする．通信路符号化定理によれば，通信路から通信路容量 C という量が計算でき，符号長 n に対するメッセージ長 k の比 k/n，すなわち符号化レート R_B がこの容量 C よりも小さいならば，ボブは復号誤り確率を符号長 n を長くすることで任意に小さくできる．

情報理論的安全性の達成法

図 1.4(a) に示すように，アリスとボブが主通信路で通信を行い，イブが盗聴者通信路で通信を盗聴する場合を考える．ワイヤタップ通信路符号化の目的は，鍵を予め共有すること無く，ボブに対する誤りなしのメッセージ伝送と，イブに対する情報理論的安全性を両

立することにある．前者については，通信路符号化同様に，誤り訂正のための冗長性を秘密メッセージに加えることで実現できる．一方で，盗聴者に対する情報理論的安全性は，符号語のグループ化という概念を利用することで実現される．以下では，その概説を模式的な例を用いて行う．

アリスが 3 ビットのメッセージをボブに伝送する状況を考える．ここで，主通信路には誤りが発生せず，盗聴者通信路には最大で 1 ビットの誤りが発生すると仮定する．このとき，アリスが (0,0,0) というメッセージを伝送すると，イブ側では (0,0,0)，(1,0,0)，(0,1,0)，(0,0,1) という 4 つの受信語が現れる．一方で，アリスがメッセージ (1,1,1) を伝送した場合に，イブ側に発生する受信語は (1,1,1)，(0,1,1)，(1,0,1)，(1,1,0) の 4 つである．すなわち，(0,0,0) と (1,1,1) の伝送の結果としてイブ側で発生する受信語の組を合わせると，3 ビットで表現可能な 8 系列すべてが尽くされることになる．

表 1.1　2 ビットメッセージと 3 ビットメッセージの組の対応付け

2 ビットメッセージ	3 ビットメッセージ
(0,0)	(0, 0, 0) or (1, 1, 1)
(1,0)	(1, 0, 0) or (0, 1, 1)
(0,1)	(0, 1, 0) or (1, 0, 1)
(1,1)	(0, 0, 1) or (1, 1, 0)

以上の議論は，その他のメッセージの組 (例えば (0,1,1) と (1,0,0)) に対しても成り立つ．そこで，アリスは表 1.1 のように 2 つの 3 ビットメッセージから成る組に対して，2 ビットのメッセージを対応させる．そして，ある 2 ビットメッセージを伝送する場合には，それに対応する 3 ビットメッセージの中から 1 つのメッセージをランダムに選んで通信路に入力する．上述の議論のように，任意の 3 ビットメッセージの組に対して，アリスが送った 2 ビットメッセージとは無関係に，イブ側では 8 つの受信語が現れる．すなわち，伝送可能なビットから 1 ビットを犠牲にすることによって，情報理論的安全性が達成される．

以上では直感的な議論を行ったが，実際に情報理論的安全性を示すためには，メッセージと受信語の無相関性を確率論的な尺度によって計量する必要がある．図 1.5 を用いて，その点に関する議論を行う．図中の丸点は n ビットの符号語を表しており，それを 2^l 個ずつ含んだ組をそれぞれ $C_1, C_2, \cdots$ とする．メッセージ 1 を伝送するためには，C_1 内の符号語をランダムに選んで通信路に入力する．そして，メッセージ i を伝送した場合，イブ側には $P_n^{(i)}$ に従って受信語が出力される．

メッセージと受信語の無関係性を示すためには，メッセージ i により生起される確率分布 $P_n^{(i)}$ と予め定めておいた任意の標的分布 π_n との間の統計的な距離 $D(P_n^{(i)}||\pi_n)$ が任意の i に対していくらでも小さくできることが要求される[*1]．これは，各組 $C_1, C_2, \cdots$

[*1] ここで，統計的な距離の具体的な定義は 2 章以降を参照されたい．

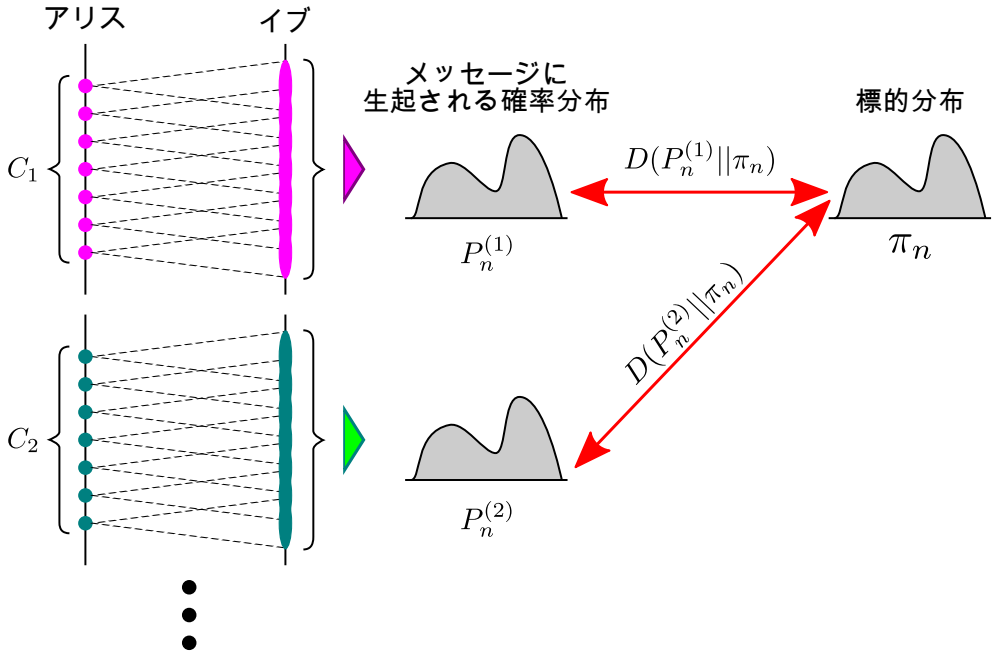

図 1.5 情報理論的安全性を達成する符号化の概要図

に含まれている符号語の出力を用いて，π_n を近似することに相当する．ここで，l を大きくすると各組に含まれる符号語の数が増加して確率分布の近似の精度が向上するため，統計的な距離 $D(P_n^{(i)}||\pi_n)$ は小さくなるが，一方で組の数自体が減少するため伝送可能メッセージ数は小さくなる．すなわち，アリスは統計的な距離を小さくしつつ，より多くの秘密メッセージが伝送できるように l を設定する必要がある．このような入力による出力の近似問題は始め Wyner[70] によって提起され，その後 Han と Verdú[71] によって通信路 Resolvability の文脈から解析された．各組 $C_1, C_2, \cdots$ の符号化率を $R_E = l/n$ によって定義し，この符号化率 R_E が盗聴者通信路の通信路容量よりも大きいならば，統計的距離が 0 になることが彼らによって示されている．

ワイヤタップ通信路符号化

以上の議論を総括した上で，ここではワイヤタップ通信路符号化と，その核となる確率的符号器について述べる．アリスは k ビットの秘密メッセージを n ビットの符号語に符号化し，ボブには誤り無く，イブに対しては情報理論的安全性を担保して伝送したい．そのため，図 1.6 に示すように，確率的符号器によってワイヤタップ通信路符号化を行う．ワイヤタップ通信路符号は k ビットの秘密メッセージと，l ビットのランダムネス，そして $n-k-l$ ビットの誤り訂正のための冗長情報から成る．アリスはワイヤタップ通信路符号の符号語を 2^{k+l} 個用意し，さらに $L = 2^l$ 個の要素を持つ $M = 2^k$ 個のグループ $\mathcal{C}_i \quad (i \in \{1, \cdots, M\})$ へとランダムに等分割する．符号器は，k ビットで表されるメッセージ i に対応するグループ $\mathcal{C}_i$ を選び，そこから l ビットで表される符号語を選び出し，伝送する．

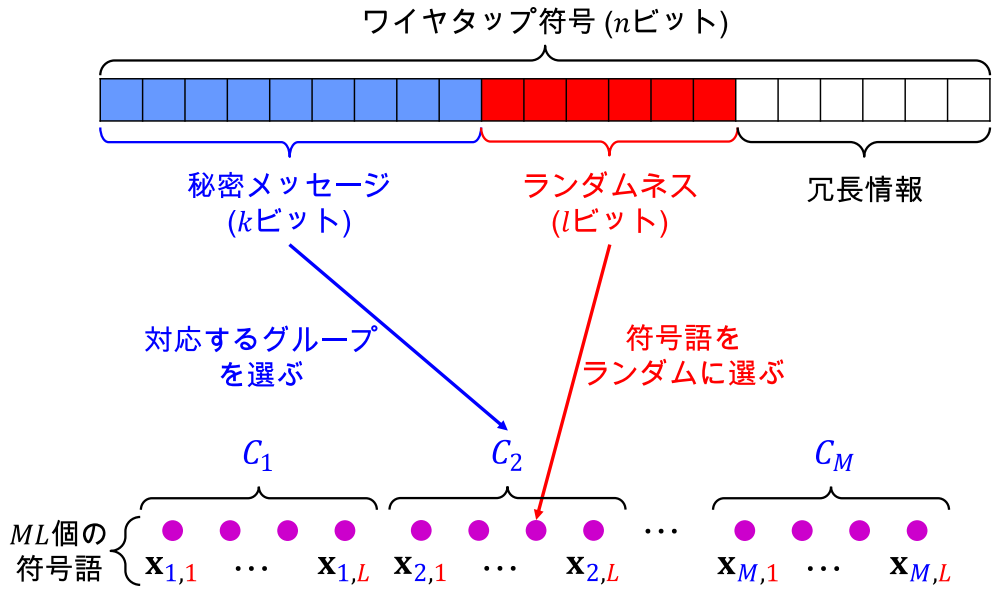

図 1.6　ワイヤタップ通信路符号と確率的符号器の概要図

ここで，符号化レート $R_B = k/n$ とランダムネスレート $R_E = l/n$ に対して，$R_B + R_E$ が主通信路の通信路容量よりも小さければ，ボブは $M_n L_n = 2^{k+l}$ 個全ての符号語を誤り無く復号できる．そして，再生された符号語から，その符号語が含まれているグループ $\mathcal{C}_i$ と秘密メッセージ i を誤り無く再生できる．一方で，ランダムネスレート R_E が盗聴者通信路の通信路容量よりも大きければ，イブに対する情報理論的安全性が達成される．つまり，符号化レート R_B を主通信路と盗聴者通信路の通信路容量よりも小さく取れば，誤りがなく，なおかつ情報理論的に安全な通信が達成される．以上の符号化がワイヤタップ通信路符号化であり，それを実現するランダムネスを取り入れた符号器を特別に確率的符号器と呼ぶ．

当然ながら，主通信路と盗聴者通信路の容量が等しい場合，あるいは盗聴者通信路のノイズの影響が小さく，主通信路よりも大きい容量を持つ場合には，イブはボブが用いる復号器と同じ復号器によりメッセージを全て解読できてしまう．そのため，盗聴者通信路が主通信路よりもノイズが大きいとした仮定が成り立たない限り，この符号化は機能しない．

1.2.2　秘密鍵共有

ここでは秘密鍵共有について述べる．鍵無しでの秘匿通信を目的とするワイヤタップ通信路符号化とは異なり，秘密鍵共有は情報理論的に安全な鍵の生成を目的とする．そこで，アリスとボブは予め共有した乱数に対して，QKD 同様の後処理 (鍵蒸留処理) を公開通信路を通して行う．

最初期の研究 [68, 69] では，補助情報を用いた情報源圧縮である Slepian-Wolf 符号化 [72] と，節 1.2.1 同様のメッセージのグルーピングを組み合わせた鍵蒸留処理が提案され

ている．しかし，QKD や電波無線通信における実装では，2 つの独立したプロトコルに分離されて実装されることが多い．そこで，本研究ではこれらに倣い，秘密鍵共有を以下の 3 つの要素に分離する．

1. 乱数送付
2. 情報整合
3. 秘匿性増強

以下，それぞれの要素について概説する．

乱数送付

乱数送付は，アリスとボブ，そしてイブに，乱数が送付されるステップであり，おおまかに 2 つのモデルが知られている．1 つは，人工衛星のような外部の乱数源から生成された乱数を，アリスとボブ，そしてイブが受信する，情報源モデルである．電波無線通信における実装例の多くは，フェーディングの効果による受信強度の経時変化を乱数として利用するため，このモデルで記述される．もう 1 つは，アリスが生成した乱数を，ワイヤタップ通信路符号化と同様に，主通信路及び盗聴者通信路を通してボブとイブに伝送する通信路モデルである．QKD は量子通信路を用いて特殊な量子状態にある光子を伝送するため，通信路モデルに基づく秘密鍵共有と見なせる．

ワイヤタップ通信路符号化が機能するためには，盗聴者通信路で発生する誤りが主通信路で発生するそれよりも多いことが要求された．しかし，以下に説明するように，通信路モデルに基づく秘密鍵共有では，ボブが不利な通信路を利用せざるを得ない状況においても鍵を生成することが可能になる．

図 1.7(a) に，アリスがボブとイブに 2 元乱数系列 $\mathbf{x}$ を送付した時点での秘密鍵共有の模式図を示す．ここで，主通信路と盗聴者通信路で発生する誤りを表したベクトルを $\mathbf{e}$ 及び $\mathbf{d}$ と表すと，ボブとイブが手にする出力乱数列は $\mathbf{y} = \mathbf{x} \oplus \mathbf{e}$ 及び $\mathbf{z} = \mathbf{x} \oplus \mathbf{d}$ となる．なお，$\oplus$ は mod2 による可算とする．また，主通信路で発生した誤りが，盗聴者通信路で発生した誤りよりも多い点に注意されたい．この状況ではワイヤタップ通信路符号化では機能しない．

アリスによる乱数送付が終了した後に，アリスが持つ乱数列 $\mathbf{x}$ とイブが持つ乱数列 $\mathbf{z}$ をそれぞれ $\mathbf{y}$ で表すと，$\mathbf{x} = \mathbf{y} \oplus \mathbf{e}$ 及び $\mathbf{z} = \mathbf{y} \oplus \mathbf{e} \oplus \mathbf{d}$ となる．すなわち，2 つの通信路で生じる誤りが独立であるために，ボブとアリスの乱数の間の差異より，ボブとイブの乱数の間の差異が大きくなる状況を作り出すことができる．そして，アリスの乱数列をボブの乱数列に合わせるように誤り訂正の操作を行い，鍵を抽出するための圧縮関数を用いることで，イブに対して情報理論的に安全な鍵を作り出すことができる．

以上のような，ボブの乱数列で全ての乱数列を書き直す操作は，秘密鍵共有の最終目的がアリスとボブの間でイブが持つ情報とは無関係な鍵の共有であることから正当化される．アリスが意味のあるメッセージを伝送するワイヤタップ通信路符号化では，このような操作は行えない．

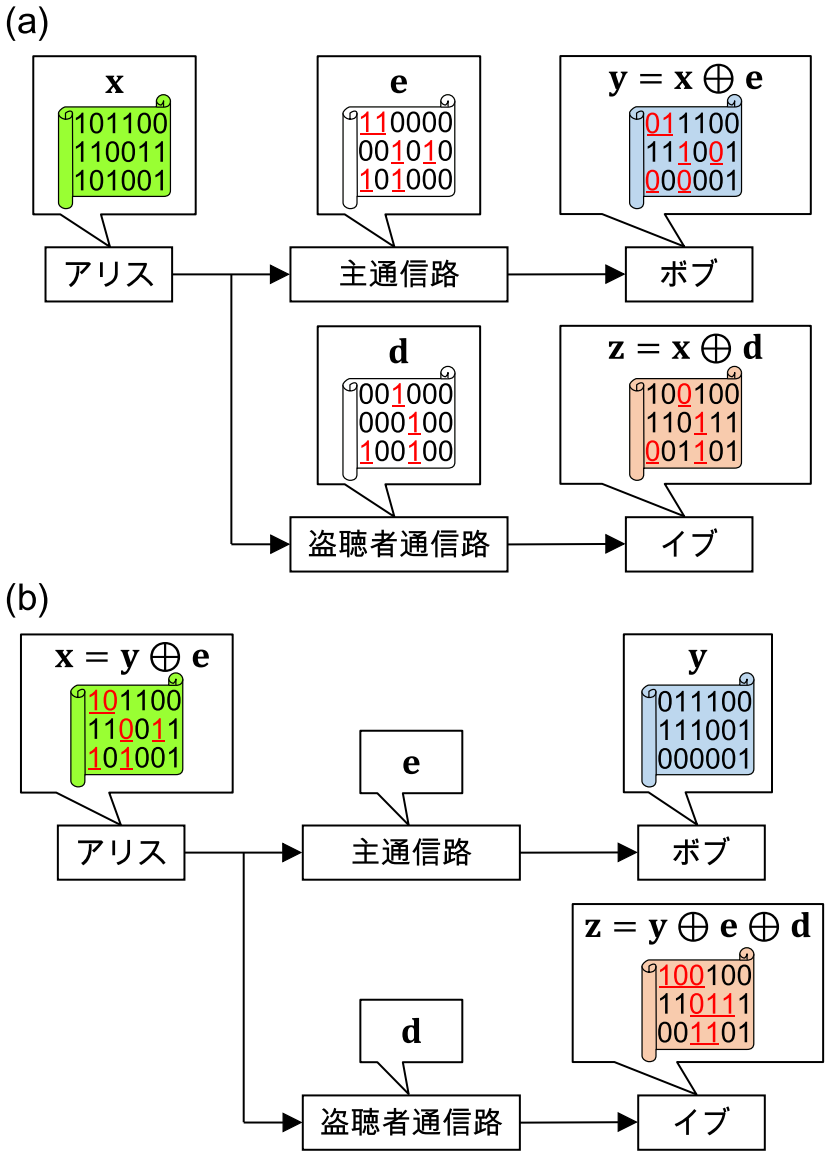

図 1.7　(a) アリスからの乱数送付直後の模式図．ここで，誤りが発生したビットを赤字と下線を付して表している．(b) アリスとイブが持つ乱数列をボブが持つ乱数列で置き換えた場合の模式図．

情報整合

情報整合の目的は，アリスとボブが公開通信路上で情報をやりとりして，それぞれが持つ乱数間の食い違いを訂正することにある．ここでは，図 1.7 において，ボブからアリスに情報を伝送し，アリスの乱数 $\mathbf{x}$ をボブの乱数 $\mathbf{y}$ と一致させる場合を考える．この操作を，特に後方情報整合と呼ぶ．一方で，従来の誤り訂正と同様に，アリスからボブに情報を伝送し，ボブに生じた誤りを訂正してアリスの乱数と一致させる操作を前方情報整合と呼ぶ．

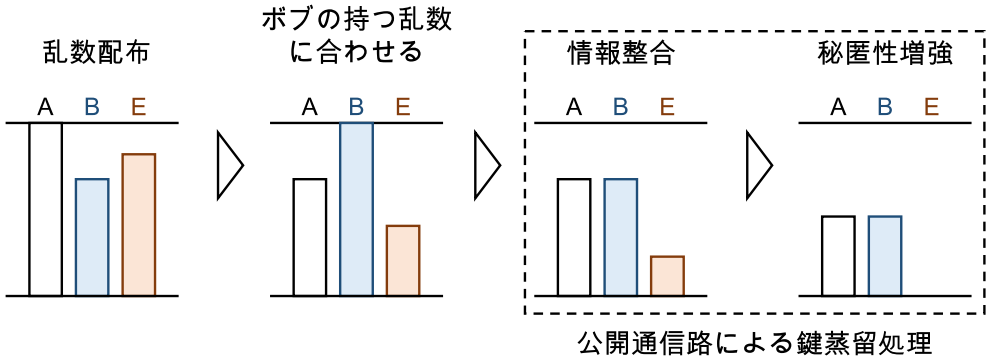

図 1.8　秘密鍵共有の各ステップにおける情報量変化の概念図．A，B，E はそれぞれアリス，ボブ，イブを表す．

ボブが公開通信路を通してアリスに伝送する情報としては，自身が持つ乱数 $\mathbf{y}$ を圧縮した系列を考えることができる．アリスは自分の乱数 $\mathbf{x}$ と公開通信路から送られてきた情報を元にして，ボブの乱数 $\mathbf{y}$ の再生を図る．ここで，ボブの乱数 $\mathbf{y}$ の圧縮率は，アリスはその再生に成功する一方で，アリスの乱数列よりも多くの誤りを含む乱数列 $\mathbf{z}$ を持つイブは再生に失敗するように，注意深く設計する必要がある．

アリスの操作を言い換えると，自身が持つ乱数を補助情報として，圧縮されたボブの乱数の再生を行うという操作である．このような補助情報を利用した圧縮は，第 2 章にて述べるように，Slepian-Wolf 符号化 [72] として定式化されている．

秘匿性増強

情報整合を通してアリスとボブが乱数列 $\mathbf{y}$ を共有したが，その乱数列 $\mathbf{y}$ とイブが持つ乱数列 $\mathbf{z}$ との相関は未だ存在しているため，情報理論的に安全な鍵とはみなせない．そのため，秘匿性増強のステップでは，ランダムに構成された圧縮関数を用いて情報整合後の乱数列を圧縮することで，イブが持つ乱数列と無相関な鍵を生成する．なお，この圧縮関数は公開されていても安全性に影響は無い．

以上の 3 ステップ (乱数送付，情報整合，秘匿性増強) と，それらを通した情報量の変化の概念図を図 1.8 に示す．乱数送付では，アリスがボブとイブに乱数を送付するが，イブがボブよりも誤りの少ない通信路を利用し，ボブがアリスの乱数列について得た情報よりも多くの情報をイブが手に入れていても構わない．その後の操作でボブの乱数列に合わせて全ての乱数列を書き直すことによって，秘密鍵共有が機能する状況を作り出せる．そして，情報整合によりアリスとボブが乱数を共有し，秘匿性増強によってイブが持つ乱数列と無相関な鍵を作り出す．

1.2.3　ワイヤタップ通信路符号化と秘密鍵共有の比較

以上に紹介してきたワイヤタップ通信路符号化と秘密鍵共有は，それぞれ通信路符号化と (補助情報付きの) 圧縮という情報理論における基本的な問題設定に，情報理論的安全

性を保証するための機能 (e.g. 確率的符号器) を付加した符号化と捉えることができた．以下では，ワイヤタップ通信路と秘密鍵共有の間に存在する違いについて考察する．

ワイヤタップ通信路符号化では，アリスは与えられたメッセージを符号化した上で，それをボブとイブに伝送する．しかし，大気のゆらぎによる強度変化や，イブが通信路を横切りつつ情報を掠めとするといった攻撃のような，通信路状態の急激な変化には対応できず，結果として突発的な情報漏えいを引き起こすという危険性は否定できない．光空間通信における物理レイヤ暗号には前述のようにアリスとボブが広角カメラで互いの通信路を監視する必要があるが，上記のような突発的な情報漏えいを監視だけで防止するのは難しい．

一方で，秘密鍵共有では，すでにアリスとボブ，イブの手元に相関のある乱数が存在し，その乱数に対して公開通信路を介した鍵蒸留プロトコルにより秘密鍵を生成する．この過程において，記録した映像の分析などから不穏な動きを発見できた場合にはその乱数を破棄することで情報漏えいを防ぐことができる．以上の理由から，秘密鍵共有はワイヤタップ通信路符号化と比較してより実用的な方式であると考えられる．実際に，秘密鍵共有の契機となった QKD に関する研究も後押しとなって，現在では多くの実証研究が主に電波無線通信の領域で行われている．

しかし，この公開通信路はアリスとボブの間での情報交換に様々なバリエーションを許してしまうため，秘密鍵共有に関する理論はワイヤタップ通信路符号化のそれと比較して難解なものとなる．そのため，ワイヤタップ通信路符号化は情報理論的安全性の理論研究を行う上での理想的モデルとして重宝される．実際に，ワイヤタップ通信路符号化で得られた知見を秘密鍵共有の解析に利用した例も少なからず存在する [73]．また，公開通信路の使用には通信相手の認証などの手続きを要求するため，セキュリティのループホールとも成り得る点にも十分な注意を払う必要がある．

1.3 物理レイヤ暗号の研究における現状及び課題

本節では，ワイヤタップ通信路符号化と秘密鍵共有の 2 つの方式について，過去に行われた研究の内で本研究と関連するものを挙げ，まだ明らかにされていない領域について明らかにしていく．

1.3.1 ワイヤタップ通信路符号化

容量と有限長解析

ワイヤタップ通信路符号の性能は，ボブには誤り無く，イブには情報理論的安全に伝送可能な情報量の上界値によって測られる．この上界値を秘匿容量と呼ぶ．秘匿容量の公式は，はじめ主通信路に盗聴者通信路が連接されている特殊な場合について，Wyner[66] によって明らかにされた．後に，Csiszár と Körner[74] は通信路に対して仮定を課さない，一般的な公式を得ている．さらに，Bloch と Laneman [75] は情報スペクトル [76] の手法

によって，入力確率分布にすら仮定を課さない，最も一般的な秘匿容量の公式を導出している．この公式は入力に制限が課されている，実用的なケースも内包している．

秘匿容量はシステム設計のための上界値を与えるが，符号長が無限大の極限における漸近的な量であるため，符号長が固定された符号の性能に関しては一切の情報を含まず，実際の設計には利用できないと考えられてきた．一方で，情報理論における有限長解析と呼ばれる分野では，復号誤り確率や漏えい情報量の符号長に対する減少の速度を与えることによって，有限の長さの符号にも利用可能な評価法を提供してきた．

有限長解析の歴史は古く，1968 年には Gallager[77] が 1 対 1 の通信路符号化問題における復号誤り確率の符号長の関数による上界を見出している．これにより，与えられた復号誤り確率の基準値を達成するために最低限必要な符号長が求められる．一方で，ワイヤタップ通信路符号化では，漏洩情報量を計量する必要がある．漏洩情報量の符号長の関数による上界は，Wyner による通信路出力の近似問題 [70] を拡張した Han と Verdú による通信路 resolvability[71] の登場を待たねばならない．Csiszár[74] がこの問題とワイヤタップ通信路符号化を結びつけ，Gallager と同様の漏洩情報量の符号長の関数によるバウンドを導出した．後に，Hayashi[73] は復号誤り確率と漏洩情報量に対するバウンドを同時に利用する定式化を発表した．現在では同様の漏洩情報量に対するバウンドがいくつか発表されている [78].

上記に述べた漏洩情報量のバウンドに関する各研究においては，入力に制約が課されている場合が扱われていなかった．そこで，Han，Endo，Sasaki[79] は 2014 年に漏えい情報量に対してもコスト制約が課されたバウンドを導出している．そのバウンドは最適化すべき変数領域を広げたという意味で，単なる漏えい情報量の上界の導出のみならず，Gallager の上界をも内包する結果となっていた．しかし，Han らの結果には，バウンドが満足すべき性質の証明など，未解決な問題が多く残されていた．

実証に向けた研究：符号化，電波無線通信，光空間通信

ここでは，ワイヤタップ通信路の実現に向けた研究を 3 つの視点から概観する．

まず 1 つは，ワイヤタップ通信路符号化を実現する構成的な符号化の提案である．情報理論における解析は伝送速度の限界 (Shannon 限界) を与えるが，その性能を実現する符号の構成法に関する情報は一切与えられない．具体的な符号の構成法は符号理論と呼ばれる分野において積極的に研究されてきたが，そこで提案されてきた符号の多くは Shannon 限界からはほど遠い性能しか持たなかった．しかし，近年の研究の進展及び実装技術の向上によって，低密度パリティ検査符号 (Low Desnsity Parity Check : LDPC)[80] や Polar 符号 [81] のような，Shannon 限界に迫る誤り訂正符号が提案及び実用化されてきている．このような符号に確率的符号器としての機能も持たせることができれば，ワイヤタップ通信路符号化は実現されたことになる．

この方向においては多くの実用的な研究がなされている [82]．Thangaraj ら [83] と Vardy ら [84] はそれぞれ LDPC と Polar 符号を利用したワイヤタップ通信路符号化を提案している．一方で，Hayashi と Matsumoto[85] は，具体的な誤り訂正符号を仮定せず

に，ユニバーサル 2 ハッシュ関数 [86] という一方向関数を利用するワイヤタップ通信路符号化を提案している．このアイデアは，後に Hayashi[73] によってより具体的に述べられている．

2 つ目としては，電波無線通信に向けた研究である．電波無線通信では，電波という指向性の低い伝搬媒質が物理的な仮定を課す上での問題となった．しかし近年では，複数のアンテナを利用ワイヤタップ通信路符号化 [87, 88, 89] が注目を集めている．この方法では，アリスはボブ側で搬送波の干渉の効果によって打ち消されるように，同時にイブ側ではノイズとして機能するように，各アンテナが出力する信号をデザインする．しかし，[90] に述べられていてるように，ボブは大気の強度変化を逐一監視し，その情報をアリスにフィードバックし，アリスはその情報を元に適切な符号を選択する必要がある．そのため，現状では実用的な方法とは言えない．

3 つ目としては，光空間通信に向けた研究である．Lopez-Martinez ら [91] は，ビル間通信において，ビームのフットプリントにイブがいる場合と，ビームの根本からイブがボブに盗聴を検知されない程度にビームをタップする場合における性能を数値的に計算した．Sun[92] らは軌道角運動量変調について，同様に性能の数値計算を行った．しかし，このように数値的な性能評価の例はあるものの，具体的な実装にまで踏み込んだ研究は殆ど存在しないというのが実情である．また，これらの数値計算の例はあくまで物理レイヤ暗号の潜在的な性能を評価したに過ぎず，現状の技術を用いた実現可能性については議論がなされていない点に気をつける必要がある．

1.3.2 秘密鍵共有

容量と有限長解析

秘密鍵共有において，送った乱数に対して共有可能な鍵の情報量の比の上界値は秘密鍵容量と呼ばれる．秘密鍵容量の公式は，情報源モデルにおいて公開通信路の使用を 1 回だけ許す場合には Maurer[68] 及び Csiszár と Ahlswede[69] によって見出されているものの，より一般的なケースでは未解決のままとなっている．また，秘密鍵共有の場合においても復号誤り確率及び漏えい情報量に対する符号長に依存するバウンドを導出した研究も存在する [93]．しかし，これも公開通信路の使用を 1 回だけ許す場合のみをその考察の対象としている．

情報整合と秘匿性増強

先立って提案されていた QKD が多大な成果を上げているため，それに牽引される形で秘密鍵共有の実証に向けた研究が多く報告されている．それらの多くは，既に述べたように，情報整合 [94, 95] と秘匿性増強 [94, 96] という 2 つの独立したプロトコルに分離して実装されている．以下，情報整合と秘匿性増強に関する研究の状況を述べる．

歴史上，最初に提案された実用的な情報整合プロトコルはカスケード [94, 95] と呼ばれる．カスケードプロトコルでは，パリティの計算と二分探索を繰り返すことにより，誤り

の訂正を図る．符号化率を理論限界近くまで達成可能なプロトコルであるが，一方で莫大な回数の公開通信路の利用が必要であり，通信の遅延に伴うスループットの低下及び公開通信路の使用に伴う認証の必要性という観点から非効率的な方法とみなされている．

そこで，現在では Slepian-Wolf の符号化 [72] を具体的に実装する方法が提案されている．既に Wyner[97] によって線形符号により当該符号化の実装が可能であることが示されており，現在では Turbo 符号 [98] や Polar 符号，さらには LDPC 符号といった符号による，理論限界に近い圧縮率での Slepian-Wolf 符号化が提案されている [99, 100, 101, 102, 103]．

一方で，秘匿性増強のプロトコルでは，逆関数の計算が一般に困難である，一方向性関数 [104, 86] が用いられる．特に，2 つの異なる系列に対して関数を作用させた結果の値が等しくなる (衝突する) 確率がランダムであることを要求する，ユニバーサル 2 ハッシュ関数が幅広く利用されている．ユニバーサル 2 ハッシュ関数ははじめ Carter と Wegman[86] によって導入され，その後 Bennett ら [96] によって QKD における秘匿性増強へ利用された．特に，現在の QKD の安全性に関する理論の多くは，ユニバーサル 2 ハッシュ関数の利用を前提として証明が行われている．現在では，高速実装に向けた効率的な計算法 [105, 106] も開発されている．

電波無線通信における実装例

以上のように，情報整合と秘匿性増強は具体的な手法で実現可能であるため，乱数送付の方法が確立すれば秘密鍵共有は実現される．実際に，強度変化の時間変動のランダムな変動を乱数源として利用可能な電波無線通信では，多くの実装例 [107, 108, 109] が報告されている．前述のように相反性という性質が成り立つため，アリスからボブへのリンクとボブからアリスへのリンクにおける通信路の強度変化は高い相関を持ち，半波長 (搬送波の周波数が 2.4 GHz ならば 6.25 cm) 離れた位置にいるイブが得る強度変化は殆ど無相関なものとなる．以上より，アリスとボブが共有した強度変化を適切に量子化し，それに対して情報整合と秘匿性増強を行うことで秘密鍵を抽出できる [110, 111]．

電波無線通信における秘密鍵共有は，無線 LAN 通信 [112, 113, 114, 115] におけるアクセスポイント間でのセキュリティ増強の目的や，センサネットワークのような低消費電力のシステムへの実装 [116, 117] に向けて，近年急速に成熟しつつあるが，いくつかの問題も指摘できる．まず，鍵の生成速度は強度の量子化の手法や通信路の状態に強く依存し，遮蔽物や送受信機の位置移動が存在しない定常的な状況では鍵生成そのものが実質的に不可能であることが知られている [116]．加えて，鍵生成レートは搬送波のドップラー周波数によって決定され，現時点では無線 LAN では 360 bit/packet[115]，センサネットワークでは 0.25 bps を下回る程度 [117] となっている．そのため，QKD のようにワンタイムパッド暗号のための鍵共有としての利用は現実的でなく，現代暗号における鍵としての利用が前提となる．また，現時点においてはラップトップ PC のオンボードのワイヤレスカードや小型マイコンといった近距離通信における実現がほとんどであり，ビル間や衛星間通信のような長距離通信における実装は報告されていない．

光空間通信における研究

以上のように，電波無線領域における研究は盛んであるが，光空間通信における秘密鍵共有の研究は電波無線通信の研究と比較して，その例に乏しいのが現状である．

光空間通信における秘密鍵共有を扱った研究として，Wang ら [118] の論文が挙げられる．彼らは，光空間通信における通信路相反性に関する，機上-地上局実験も含めた一連の研究 [119, 120, 121] に着想を得て，その相反性を利用した秘密鍵共有の性能の理論的に解析した．結果としては，典型的な大気の擾乱の条件において，256bit の鍵を 0.1 秒のオーダーで生成できると報告している．既に述べた電波領域における実験結果と比較すると十倍近く高速ではあるが，ここでも大気の相反性の帯域によって鍵生成レートが制約されていると言わざるを得ない．低軌道衛星-地上局間通信のように，限られた通信時間内でより多くの鍵を共有するためには，より高速に鍵を生成する方法が必要となる．

1.4 本研究の目的と本論文の構成

1.4.1 本研究の目的

ここまで見てきたように，光空間通信における物理レイヤ暗号は，ユーザビリティや安全性といった観点からは，現代暗号と QKD とのギャップを埋める技術であり，魅力的な特徴を持つ両技術とはまた異なる場面での使用に適した，新しい選択肢をユーザーに提供する．その場面の具体例の一つとしては，人工衛星などを中心とした移動通信ネットワークであり，回線の注意深い監視のもと，遠距離かつ高速な秘匿伝送及び鍵生成が期待できる光空間通信における物理レイヤ暗号は，移動体通信にとって魅力的な暗号技術である．

しかし，光空間通信における物理レイヤ暗号の実証研究は，電波無線通信と比較するとほぼ行われていないのが現状である．そのため，本研究では初めに理論的課題において欠落しているテーマから出発し，実データを元にした性能推定実験などを得た上で，最終的に実用的な物理レイヤ暗号のプロトコルの実現を目指す．

1.4.2 本論文の構成

本研究では，上記に掲げた目標の達成に向けて，以下の事柄に取り組む．

第 2 章

ワイヤタップ通信路符号化と秘密鍵共有という 2 つの手法について，情報理論的な観点から定式化を行い，以降の実験などでも用いる諸量の導入を行う．

第 3 章

第 3 章では，光空間通信における物理レイヤ暗号の実現可能性について，理論的アプローチから検討を行う．本章は 2 つのパートに大別されることになる．

前半では，理論的準備について述べる．本章では，理論的解析が容易であるワイヤタップ通信路符号化に着目し，物理的な制約が課されている通信路での性能を評価するために，入力分布に制約を導入するように再定式化を行う．なお，本章ではこの再定式化を情報理論における伝統的な手法とは異なる方法で行う．その上で，既存の定式化との比較から得られた新知見についても述べる．

後半のパートでは，前半で述べた理論的準備に基づく数値計算による性能評価を行う．ここでは，レーザーのオン-オフ変調によって通信を行うという，衛星-地上局間あるいは衛星間レーザー通信にて考えられるシナリオを設定する．そのシナリオにおける通信路の確率的モデルを構築し，それを元にして，ワイヤタップ通信路符号化によって秘密伝送可能な情報量を数値的に計算する．そして，算出された伝送可能情報量と QKD の鍵生成レートとを比較することで，図 1.3 にて議論したような，安全性を緩めた際の伝送可能情報量の増加について定量的な議論を展開する．

さらに，ワイヤタップ通信路符号化における復号誤り確率や漏えい情報量といった評価量の符号長依存性を調べることによって，ある性能を持つ物理レイヤ暗号の，現在の技術水準のハードウェアに実装可能な符号での実現可能性を検討する．

第 4 章

実環境においては，大気のゆらぎによる受信強度の時間変化が，光空間通信における物理レイヤ暗号の性能に大きな影響を与える．過去の研究 [91, 92] などは，この効果を取り込んだ上で光空間通信におけるワイヤタップ通信路符号化の漸近的な性能を解析的に計算しているが，それらは確率分布のパラメータを定めた上での計算結果である点に注意が必要である．

以上の状況を鑑み，本章では NICT が所有する，1 つの送信ターミナルに対して 2 つの受信ターミナルを備えた光空間通信テストベッドから得られた実験データを用いて，大気の揺らぎが物理レイヤ暗号の性能に及ぼす影響の定量化と，そこから得られた知見について述べる．

具体的には，ワイヤタップ通信路符号化に着目した上で，秘匿容量等の性能評価の諸量を実験データから評価する．それらの結果から，大気のゆらぎが物理レイヤ暗号に及ぼす影響について定量的に考察できると期待できる．本章では，このような方法を通信路推定実験と位置づけ，そこから得られた知見について述べる．

加えて，新しい知見として，物理レイヤ暗号使用の可否判断を行うための諸量を計算し，実用的な物理レイヤ暗号の符号化の理論的検討を行う．

第 5 章

第 3 章及び第 4 章では理論的解釈及び解析が容易であったワイヤタップ通信路符号化に着目して議論を進めてきた．しかし，既に節 1.2.3 で指摘したように，物理レイヤ暗号はそのメッセージ伝送という性格に起因するセキュリティ上の問題を孕んでいた．そこで，第 6 章では QKD に牽引されることによって実装技術が進んでいる秘密鍵共有の主要な信

号処理をプログラム実装したソフトウェアを用いて，テストベッドから得られたデータをもとに秘密鍵共有を行った結果について述べる．

加えて，より効率的な情報整合の実装に向けて，いくつかの誤り訂正符号による理論的検討を行う．そして，実験データからの鍵生成に利用した LDPC による情報整合と比較したベンチマークを取り，より効率的な情報整合に向けた考察を行う．

1.4.3 本研究の意義

上記で述べてきたように，本研究では理論的側面と実験的側面を含む研究となっている．

第 3 章では情報理論的なテーマを扱うが，これは単なる既存テーマの拡張及び証明のやり直しでなく，既存の評価量の問題点を指摘しており，純粋な情報理論的テーマとしても新しい地平を拓いている．また，これらの情報理論的評価量を利用することによって，QKD と物理レイヤ暗号の関係の定量的議論や，既存の計算機で処理可能な符号による実現可能性など，情報理論的な視点に立った上で漸近的な評価量を扱ってきた既存の光空間通信における物理レイヤ暗号に関する研究と比較しても，より暗号学的及び実装に向けた議論を展開している．

第 4 章では NICT が所有している光空間通信テストベッドを利用することによって，過去の研究では例のない，実環境データからの物理レイヤ暗号の性能評価というテーマに取り組んでいる．これにより，過去の理論的研究からは見えてこない，大気のゆらぎが物理レイヤ暗号に及ぼす影響等を実データから行うことが可能となる．

第 5 章では，QKD という分野や電波無線通信における物理レイヤ暗号で培われてきた秘密鍵共有に関する技術を利用し，光空間通信でも秘密鍵共有の実証実験を行う．これは，我々が知りうる限り世界初の秘密鍵共有の実験となる．

以上より，本研究は理論及び実験の両分野において不足していた知見を補いつつ，最終的には光空間通信における物理レイヤ暗号の実証実験にまで至る，この分野におけるさきがけ的な研究として位置づけることができる．

第 2 章

基礎概念の導入

本章では，はじめに情報理論において頻繁に用いられる表記や，エントロピーや相互情報量といった諸量，証明で用いる不等式等を導入し，それらの性質について述べる．そして，導入した諸量を用いて，ワイヤタップ通信路符号化と秘密鍵共有の情報理論的な定式化を行う．

なお，この節を通して，Han と Kobayashi による教科書 [122]，El-Gamal と Kim による教科書 [123]，Watanabe によるレビュー [124] を参考にした．また，各種の文献に証明が記載されている定理や補題についてはその証明を省略している．

なお，数値の範囲の定義に際して，閉区間 $a \leq x \leq b$ を $x \in [a,b]$，開区間 $a < x < b$ を $x \in (a,b)$ で表す．これらは，混合して利用される場合 ($a \leq x < b$ を $[a,b)$ など) もある．

2.1　確率論に関する基礎事項

情報理論では，入力されるシンボルや通信路で生じる誤りなどを確率論的にモデル化することによって通信システムの評価を行う．そのため，ここではエントロピーや相互情報量などの評価量を導入するに先立ち，確率論に関する基礎事項を導入する．同時に，情報理論の証明においてよく用いられる不等式なども，ここで導入する．

2.1.1　確率変数

確率的に値が決定する事象の一例として，サイコロを振ることを考える．サイコロの目は 1 から 6 までの値を持つが，実際に振られるまではその値は確定していない．振られた瞬間に 1 から 6 までの値が (等確率で) 確定する．

このサイコロの例のように，与えられた確率に従って特定の値を取る変数を確率変数と呼ぶ．慣習に従い，本論文では確率変数を大文字 $(X, Y, \cdots)$ で表す．そして，その確率変数が取り得る値の集合 (サイコロの目の場合には 1 から 6) をカリグラフィー体 $(\mathcal{X}, \mathcal{Y}, \cdots)$ で表し，その要素 (実現値) を小文字 $(x \in \mathcal{X}, y \in \mathcal{Y}, \cdots)$ で表す．本論では簡単のため，確率変数は有限集合上に離散値を持つとする．

2.1.2　確率分布

確率変数 X に対して，それがある値になる，あるいはある範囲内 (ないしは集合内) に存在する確率を与える関数を確率分布 P_X と書く．特に，確率変数 X が特定の実現値 x を取る確率であることを明記したい場合には，$P_X(x) = \Pr\{X = x\}$ と書く．ここで，$\Pr\{A\}$ はある事象が発生する確率である．

2 つの確率変数 X, Y の組の確率分布を X と Y の同時分布と呼び，P_{XY} と書く．同時確率分布 $P_{XY}(x, y)$ について，取り得る全ての y について和を取ると，

$$\sum_{y \in \mathcal{Y}} P_{XY}(x, y) = P_X(x) \tag{2.1}$$

が成立する．上記の特定の確率変数について和をとる操作を周辺化と呼び，特に得られた確率分布関数 $P_X(x)$ を周辺確率と呼ぶ．

確率変数 X の値が与えられたときの確率変数 Y の分布を条件付き確率分布と呼び，$P_{Y|X}$ と書く．なお，同時確率分布 P_{XY} と条件付き確率分布との間には

$$P_{XY}(x, y) = P_{Y|X}(y|x)P_X(x) = P_{X|Y}(x|y)P_Y(y) \tag{2.2}$$

なる関係が成り立つ．

2.1.3　確率の限界を与える不等式

通信システムの評価を行うにあたって，通信モデルの確率分布から正確な評価を行おうとすると大抵は数学的に困難なものとなる．しかし多くのモデルにおいて，確率の大まかな上界や下界などを利用すれば，数学的に取扱が容易で，かつ実用上は十分な評価を与えることができる．ここでは，確率の限界を与える不等式のうち，本論に登場する最低限のものを挙げる．

確率の限界を与える不等式として最も基本的な不等式は，与えられた非負の確率変数がある値よりも大きくなる確率の上限を与える Markov の不等式である．

補題 2.1.1（Markov の不等式）　非負の値を取る確率変数 Z と任意の $a > 0$ に対して，

$$\Pr\{Z \geq a\} \leq \frac{\mu}{a} \tag{2.3}$$

が成立する．ここで，$\mu \stackrel{\triangle}{=} \sum_z P_Z(z)z$ は，確率変数 Z の期待値である．　□

この Markov の不等式は確率論及び情報理論のどのような教科書にも記載されている基本的な不等式であるが，確率変数 Z を制限した上で，その確率変数がある値より大きくなる確率の下限を与える，以下の不等式も知られている．

補題 2.1.2（Markov の逆不等式 [122]） 確率変数 $Z \in [0, m]$ と任意の実数 $a \in [0, m)$ に対して，

$$\Pr\{Z \geq a\} \geq \frac{\mu - a}{m - a} \tag{2.4}$$

が成立する．ここで，μ は Z の平均値である． □

証明: 一般的な補題ではないため，ここに証明を書く．$p(z) = \Pr\{Z = z\}$, $S = \{z : z \geq a\}$ と置くと，

$$\begin{aligned}\mu &= \sum_{z \in S} zp(z) + \sum_{z \notin S} zp(z) \\ &\leq m \sum_{z \in S} p(z) + a \left(1 - \sum_{z \in S} p(z)\right) \\ &= a + (m - a) \Pr\{Z \geq a\}\end{aligned} \tag{2.5}$$

が成立する．以上より，式 (2.4) を得る． □

2.1.4 不等式と関数の性質

情報理論においては，関数をある変数で最大化する操作が頻繁に登場する．その際に，最大化の対象となる関数の凸性が示されることは，解析的にも数値計算的にも大きな利点を持つ．本論文でも第 3 章において凸性に関する議論を展開するため，ここで予め凸性の概念の導入を行う．

関数 f が凸関数であるとは，区間内の任意の 2 点 $\mathbf{x}, \mathbf{y}$ と任意の実数 $t \in (0, 1)$ に対して，

$$f(t\mathbf{x} + (1 - t)\mathbf{y}) \leq tf(\mathbf{x}) + (1 - t)f(\mathbf{y}) \tag{2.6}$$

を満足することをいう．また，関数 g が凹関数であるとは，関数 $-g$ が凸関数であることをいう．

一般的に，2 階偏微分可能な 1 変数関数が凸関数であるための必要十分条件は，2 階微分が非負であることである．また，一般の C^2 級関数が凸関数であるための必要十分条件はその関数のヘッシアン H が正定値であることすなわち，任意のベクトル $\mathbf{z}$ に対して，

$\mathbf{z}H\mathbf{z}^T$ が正になることである．ここでヘッシアンとは，

$$H \triangleq \begin{bmatrix} \dfrac{\partial^2 f}{\partial x_1^2} & \dfrac{\partial^2 f}{\partial x_1 \partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_1 \partial x_n} \\ \dfrac{\partial^2 f}{\partial x_2 \partial x_1} & \dfrac{\partial^2 f}{\partial x_2^2} & \cdots & \dfrac{\partial^2 f}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial^2 f}{\partial x_n \partial x_1} & \dfrac{\partial^2 f}{\partial x_n \partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_n^2} \end{bmatrix} \tag{2.7}$$

により定義される行列である．

凸関数 f に対しては次に述べる Jensen の不等式が成立する．

補題 2.1.3（Jensen の不等式）　確率変数 X 上に値を取る凸関数 f に対して，

$$f\left(\sum_{x\in\mathcal{X}} P_X(x)x\right) \leq \sum_{x\in\mathcal{X}} P_X(x)f(x) \tag{2.8}$$

が成立する．□

この不等式は，凸関数の定義 (2.6) より明らかである．

2.2　エントロピーと相互情報量

この節では Shannon エントロピーや相互情報量の定義を述べる．

なお，この節以降，対数が頻繁に登場するが，明記されない限りでは，対数の底は自然対数の底 e である．その場合には，情報量の単位は nat となる．また，対数の底として 2 を利用する場合には，情報量の単位は bit となる．

2.2.1　エントロピーの定義と性質

Shannon エントロピー (以降，単純にエントロピーと呼ぶ) は，ある事象の不確かさを特徴づける量である．情報理論では，ある確率分布に従って生成された系列を圧縮する際の，最適な圧縮率という操作的な意味を持つ．以下にその定義を示す．

定義 2.2.1（エントロピー）　確率分布 P_X に従う確率変数 X のエントロピー $H(X)$ は

$$H(X) \stackrel{\triangle}{=} -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x) \tag{2.9}$$

により定義される．また，同時確率分布 P_{XY} に従う確率変数 X, Y のエントロピーを同

時エントロピー $H(X,Y)$ と呼び，

$$H(X,Y) \stackrel{\triangle}{=} -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{XY}(x,y)\log P_{XY}(x,y) \tag{2.10}$$

と定義される．□

特に，確率変数 X が 0 か 1 という 2 つの値のみを取る場合のエントロピーを 2 値エントロピーと呼び，$p = P_X(X=1)$ に対して

$$h_2(p) \stackrel{\triangle}{=} -p\log p - (1-p)\log(1-p) \tag{2.11}$$

と定義される．

2 つの確率変数 X と Y が与えられた時，Y の値が y に確定したときの X のエントロピーを

$$H(X|Y=y) \stackrel{\triangle}{=} -\sum_{x\in\mathcal{X}} P_{X|Y}(x|y)\log P_{X|Y}(x|y) \tag{2.12}$$

と書く．このエントロピー $H(X|Y=y)$ の確率変数 Y に関する平均値を，確率変数 Y が与えられた際の確率変数 X の条件付きエントロピー $H(X|Y)$ と呼び，次のように定義する．

定義 2.2.2（条件付きエントロピー） 確率変数 Y が与えられた際の確率変数 X の条件付きエントロピー $H(X|Y)$ は

$$\begin{aligned} H(X|Y) &\stackrel{\triangle}{=} -\sum_{y\in\mathcal{Y}} P_Y(y)\sum_{x\in\mathcal{X}} P_{X|Y}(x|y)\log P_{X|Y}(x|y) \\ &= -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{XY}(x,y)\log P_{X|Y}(x|y) \end{aligned} \tag{2.13}$$

により定義される．ここで，1 行目から 2 行目の変形に関係式 (2.2) を用いた．□

エントロピーは，下記の補題に挙げる性質を持つ．

補題 2.2.1（エントロピーの性質） エントロピー $H(X)$ 及び条件付きエントロピーは次に述べる性質を持つ．

1. エントロピーの上界と下界について，$0 \le H(X) \le |\mathcal{X}|$ が成り立つ．不等式の左辺は特定の事象だけが出現する場合 (すなわち，ある 1 つの $x' \in \mathcal{X}$ に対して $P_X(x') = 1$ が成立し，それ以外の x に対しては $P_X(x) = 0$ となる場合)，右辺は確率分布が一様である場合 (すなわち，全ての $x \in \mathcal{X}$ に対して $P_X(x_i) = 1/|\mathcal{X}|$) に成立する．
2. $H(X) \ge H(X|Y)$．すなわち，Y について何かしらの情報を得たとしても，X のエントロピーは増加しない．
3. $H(X,Y) = H(X) + H(Y|X)$．この関係をエントロピーのチェインルールと呼ぶ．

4.　確率変数 X, Y, Z がこの順で Markov 連鎖を成すならば, $H(X|YZ) = H(X|Y)$.

□

性質 4. における，確率変数 X，Y，Z がこの順で Markov 連鎖を成すとは，これらの確率変数が従う確率分布関数が

$$P_{XYZ}(x,y,z) = P_X(x)P_{Y|X}(y|x)P_{Z|Y}(z|y) \tag{2.14}$$

と書けることを意味する．以降，記号で X-Y-Z と表記する．

2.2.2　相互情報量の定義と性質

エントロピーと並んで情報理論においてよく用いられる量が，相互情報量である．相互情報量は，X と Y の間の相関の度合いとして解釈される．Shannon の通信路符号化定理においては，入力を固定した場合に通信路で伝送可能な情報量という操作的な意味を持つ．以下に，その定義を述べる．

定義 2.2.3（相互情報量）　確率変数 X と確率変数 Y の間の相互情報量 $I(X;Y)$ は

$$I(X;Y) \triangleq \sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{XY}(x,y)\log\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)} \tag{2.15}$$

と定義される．□

なお，上記の定義式は

$$I(X;Y) \triangleq \sum_{y\in\mathcal{Y}} P_X(x)P_{Y|X}(y|x)\log\frac{P_{Y|X}(y|x)}{\sum_{x'}P_X(x')P_{Y|X}(y|x')} \tag{2.16}$$

と書き直すことができる．すなわち，入力確率分布 P_X と条件付き確率 $P_{Y|X}$ のみを与えても，相互情報量は決定される．そのため，必要に応じて $I(X;Y)$ の代わりに，$I(P_X, P_{Y|X})$ という表記によって相互情報量を表す場合もある．

また，エントロピー同様，ある確率変数 Z を知った場合の条件付き相互情報量も定義される．

定義 2.2.4（条件付き相互情報量）　確率変数 Z が与えられたときの確率変数 X と確率変数 Y の間の相互情報量 $I(X;Y|Z)$ は

$$I(X;Y|Z) \triangleq \sum_{x\in\mathcal{X},y\in\mathcal{Y},z\in\mathcal{Z}} P_{XYZ}(x,y,z)\log\frac{P_{XY|Z}(x,y|z)}{P_{X|Z}(x|z)P_{Y|Z}(y|z)} \tag{2.17}$$

により定義される．□

以下に相互情報量の持つ性質について述べる．

補題 2.2.2（相互情報量の性質） 相互情報量 $I(X;Y)$ 及び条件付き相互情報量 $I(X;Y|Z)$ は次に述べる性質を持つ．

1. $I(X;Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$ 及び $I(X;Y|Z) = H(Y|Z) - H(Y|XZ) = H(X|Z) - H(X|YZ)$.
2. $I(X;Y) \geq 0$. 等号は確率変数 X と Y が独立である場合，すなわち $P_{XY}(x,y) = P_X(x)P_Y(y)$ の場合のみ成立する．
3. 固定された入力 P_X に対して，相互情報量 $I(P_X, P_{Y|X})$ は通信路の凸関数である．すなわち，凸関数の定義 (2.6) により，任意の $t \in [0,1]$ と通信路 $P_{Y|X}$ 及び $Q_{Y|X}$ に対して

$$I(P_X, tP_{Y|X} + (1-t)Q_{Y|X}) = tI(P_X, P_{Y|X}) + (1-t)I(P_X, Q_{Y|X}) \quad (2.18)$$

が成立する．
4. $I(XY;Z) = I(X;Z) + I(Y;Z|X)$. この性質を相互情報量のチェインルールと呼ぶ．
5. 確率変数 X，Y，Z がこの順で Markov 連鎖を成すならば，$I(XY;Z) = I(Y;Z)$ が成立する．

□

また，相互情報量と同様に 2 つの確率分布の相関を測る量として，次に述べる Kullback-Leibler 情報量も用いられる．

定義 2.2.5（Kullback-Leibler 情報量） 確率変数 X が従う確率分布 P_X と Q_X の間の Kullback-Leibler 情報量 $D(P_X||Q_X)$ は

$$D(P_X||Q_X) = \sum_{x \in \mathcal{X}} P_X(x) \log \frac{P_X(x)}{Q_X(x)} \quad (2.19)$$

と定義される． □

次に，Kullback-Leibler 情報量の性質を述べる．

補題 2.2.3 Kullback-Leibler 情報量 $D(P_X||Q_X)$ は以下の性質を持つ．

1. $D(P_X||Q_X) \geq 0$.
2. $D(P_X||Q_X) = 0$ は $P_X(x) = Q_X(x)$ のときのみに成り立つ．
3. Kullback-Leibler 情報量 $D(P_X||Q_X)$ と相互情報量 $I(X;Y)$ の間には $I(X;Y) = D(P_{XY}||P_XP_Y)$ なる関係が成立する．

□

上記の性質 1. と性質 2. から，Kullback-Leibler 情報量は 2 つの確率分布がどれほど近いかを測る尺度として理解することができる．しかし，明らかに対称性が満足されず

($D(P_X||Q_X) \neq D(Q_X||P_X)$)，三角不等式も成り立たないため，数学的な意味での距離とは言えない．また，性質 3. は相互情報量が同時確率分布 P_{XY} が，2 つの確率分布の積 $P_X P_Y$ にどれほど近いか，すなわち同時分布がどれほど独立な分布に近いかを測っていることを意味する．

また，同様の計量として，次に述べる変動距離も用いられる．

定義 2.2.6（変動距離）　確率変数 X が従う確率分布 P_X と Q_X の間の変動距離 $d(P_X, Q_X)$ は

$$d(P_X, Q_X) = \frac{1}{2} \sum_{x \in \mathcal{X}} |P_X(x) - Q_X(x)| \tag{2.20}$$

と定義される．□

注意 2.2.1　変動距離の定義式 (2.20) 中の係数 $1/2$ は文献によっては省略されていることもある．しかし，本研究では変動距離の最大値を 1 に規格化する目的でこの係数を加えている．

変動距離は Kullback-Leibler 情報量とは異なり，距離の公理 (非負性，対称性，三角不等式) を満たすため，距離としての性質を持つ．

次に述べる変動距離と Kullback-Leibler 情報量の間に成立する Pinsker の不等式 [125] は，安全性の強度を議論する際に重要である．

補題 2.2.4（Pinsker の不等式 [125]）　変動距離 $d(P_X, Q_X)$ と Kullback-Leibler 情報量 $D(P_X||Q_X)$ の間には

$$2d(P_X, Q_X)^2 \leq D(P_X||Q_X) \tag{2.21}$$

なる関係が成立する．□

2.3　ワイヤタップ通信路符号化

本節では，物理レイヤ暗号の基本的モデルの 1 つであるワイヤタップ通信路符号化 [66] の情報理論的な定式化を行う．はじめに，ワイヤタップ通信路符号化の説明に先立ち，通信路符号化問題の定式化を行う．これは，その後に導入する情報理論的な記号などの導入の意味も兼ねている．

その次に，ワイヤタップ通信路符号化の定式化へと移っていく．本研究では第 3 章と第 4 章において，理論的に，あるいは実験データから通信路の確率モデルを構築し，秘匿伝送可能な情報量の評価などを行う．そのため，ここでは符号長 n の $n \to \infty$ の極限で復号誤り確率と漏えい情報量の両者が 0 になる伝送速度である秘匿容量と，復号誤り確率と漏えい情報量の符号長依存性を導入する．

2.3.1 通信路符号化

第 1 章の節 1.2.1 で述べたように，アリスは，誤りの発生する通信路を通してボブへとメッセージを伝送する状況を考える．正しいメッセージを伝送するため，アリスはメッセージに対して冗長情報を加えること，すなわち符号化を行う．ここでは，通信路の確率分布が与えられた場合の，伝送可能情報量の上界値を求める．

アリスは集合 $\mathcal{M}_n = \{1, \cdots, M_n\}$ からメッセージ i を選択する．そして，写像 $\varphi_n^A : \mathcal{M}_n \to \mathcal{X}^n$ によって抽象化される符号器によって，長さ n の符号語 $\varphi_n^A(i) \in \mathcal{X}^n$ を出力する。ここで，$\mathcal{X}$ を入力アルファベットと呼ぶ.

符号器の出力，すなわち符号語 $\varphi_n^A(i) \in \mathcal{X}^n$ は通信路 W に入力される．ここで，通信路は写像 $W^n : \mathcal{X}^n \to \mathcal{Y}^n$ として取り扱われ ($\mathcal{Y}$ は出力アルファベットと呼ばれる)，$\mathbf{x} \in \mathcal{X}^n$ が与えられたときの $\mathbf{y} \in \mathcal{Y}^n$ の条件付き確率分布関数 $W^n(\mathbf{y}|\mathbf{x})$ によって確率論的な特徴付けがされる．この確率分布は遷移確率分布とも呼ばれ，通信路で発生するノイズの確率的な構造を指定する．

ボブは通信路の出力 $\varphi_n^B(i) \in \mathcal{Y}^n$ を得て，それを復号器 $\psi_n^B : \mathcal{Y}^n \to \mathcal{M}_n$ に入力することで元のメッセージの推定 $\hat{i} \in \mathcal{M}_n$ を得る．以上のような符号器と復号器の組 (φ_n^A, ψ_n^B) を，情報理論において抽象化された意味での符号と呼ぶ.

以上の符号 (φ_n^A, ψ_n^B) に対して，ボブの復号誤り確率 ε_n^B を，

$$\varepsilon_n^B \triangleq \frac{1}{M_n} \sum_{i \in \mathcal{M}_n} \Pr\{\psi_n^B(\varphi_n^B(i)) \neq i\} \tag{2.22}$$

と定義する．すなわち，メッセージ i に関する符号語を通信路に入力したその出力を復号した結果が元のメッセージ i と異なる確率である．

既に第 1 章の節 1.2.1 にも述べたように，復号誤り確率 ε_n^B は伝送可能なメッセージの数 M_n とトレードオフの関係にある．アリスは，より多くのメッセージ M_n を送りつつ，同時に復号誤り確率 ε_n^B を小さくするような符号化を行いたい．そこで，符号長に対するメッセージの数の対数の比である符号化レート

$$R_B = \frac{1}{n} \log M_n$$

を定め，この符号化レートの上界を求める．ここで，$\log M_n$ は M_n 個のメッセージ全てを表現するために必要な文字の数 (例えば，対数の底が 2 ならばビット長) に対応するため，符号化レートは符号語のシンボル 1 個当たりで伝送可能な情報量，すなわち伝送速度として解釈することができる.

次の条件

$$\lim_{n \to 0} \varepsilon_n^B = 0$$

を満足する符号化レート R_B を，誤りが発生しないという意味で達成可能な符号化レート

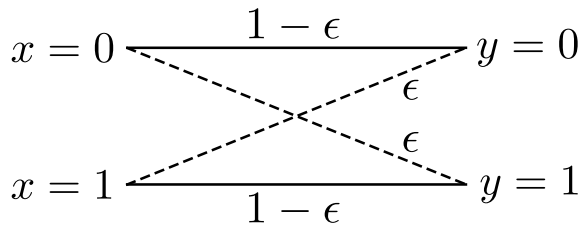

図 2.1　ビット反転確率が ϵ である二元対称通信路の概要図.

と呼ぶ．そして，達成可能な符号化レート R_B の上界

$$C \triangleq \sup\{ \text{達成可能な符号化レート } R_B\} \tag{2.23}$$

を通信路容量と呼ぶ．通信路符号化問題の目的は，様々な通信路の設定において，この C の具体的な表現を定めることにある．

なお，情報理論的な解析においては，通信路の遷移確率が $W^n(\mathbf{y}|\mathbf{x})$ が

$$W^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} W(y_i|x_i) \tag{2.24}$$

のように，遷移確率 $W(y|x)$ の n 個の積で記述できる場合を考察の対象とする事が多い．ここで，$\mathbf{x} = (x_1, \cdots, x_n)$，$\mathbf{y} = (y_1, \cdots, y_n)$ である．この式は通信路の状態が通信を行った回数や時間に依存しないことの現れであることから，この仮定が成り立つ通信路を定常無記憶通信路と呼ぶ.

通信路が定常無記憶である場合，通信路容量は

$$C \triangleq \max_{P_X} I(X;Y) \tag{2.25}$$

によって与えられる．

注意 2.3.1　例として，本論において何回か登場することになる，二元対称通信路 (BSC) について通信路容量を求める．図 2.1 に示すように，BSC は 2 入力-2 出力の定常無記憶通信路であり，入力シンボルがその値に関わらず，出力側で変化する確率 (ビット反転確率)ϵ によって特徴づけられる．すなわち，遷移確率分布を顕に書くと

$$P_{Y|X}(1|0) = P_{Y|X}(0|1) = \epsilon$$
$$P_{Y|X}(1|1) = P_{Y|X}(0|0) = 1 - \epsilon$$

となる．

ここで，入力確率が $P_X(x = 1) = p$ と書くと，ビット反転確率が ϵ である BSC の相互情報量は

$$I(X;Y) = h_2(p + \epsilon - 2p\epsilon) - h_2(\epsilon) \tag{2.26}$$

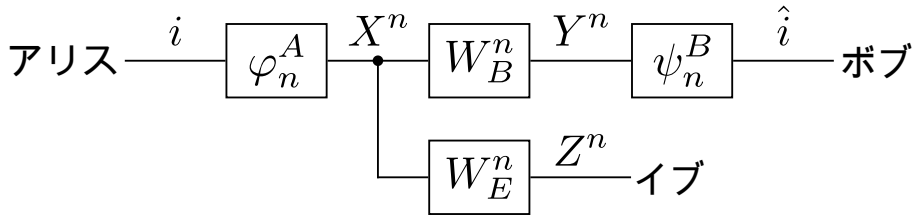

図 2.2　ワイヤタップ通信路の概念図.

となる．ここで, $h_2(p)$ は 2 元エントロピー (2.11) である．この右辺は, 入力確率 $p = 1/2$ により最適化されることが簡単な微分計算から分かるため，BSC の通信路容量 C は

$$C = \log 2 - h_2(\epsilon) \tag{2.27}$$

となる．　□

2.3.2　ワイヤタップ通信路符号化の情報理論的な定式化

次に，通信路符号化と同様の方法で，ワイヤタップ通信路符号化の定式化を行う．ワイヤタップ通信路 (W_B^n, W_E^n) は，アリスからボブへの主通信路 $W_B^n : \mathcal{X}^n \to \mathcal{Y}^n$ とアリスからイブへの盗聴者通信路 $W_E^n : \mathcal{X}^n \to \mathcal{Z}^n$ の組として定義される．ここで，$\mathcal{X}$ を入力アルファベット，$\mathcal{Y}$ 及び $\mathcal{Z}$ は出力アルファベットとし，長さ n の入力系列 $\mathbf{x} \in \mathcal{X}^n$ が与えられたときの系列 $\mathbf{y} \in \mathcal{Y}^n$ 及び $\mathbf{z} \in \mathcal{Z}^n$ の条件付き確率分布をそれぞれ $W_B^n(\mathbf{y}|\mathbf{x})$ 及び $W_E^n(\mathbf{z}|\mathbf{x})$ と定義する．

ワイヤタップ通信路符号化の目的は，復号誤り確率を抑えるだけでなく，イブ側でのメッセージの確率分布がメッセージに依存しないような，情報理論的安全性を満足する符号化を行うことにある．その目的のために節 1.2.1 で述べたような符号化の定式化を行う．

アリスはメッセージ集合 $\mathcal{M}_n = \{1, \cdots, M_n\}$ からメッセージ i を選んで伝送するために，符号語数が $M_n L_n$ 個の符号 $\mathcal{C}$ を用意し，さらにその符号を L_n 個の符号語を持つ M_n 個の符号 $\mathcal{C}_k$,　$(k \in [1, M_n])$ に等分割する．ここで，符号 $\mathcal{C}$ をメイン符号，$\mathcal{C}_k$ をサブ符号と呼ぶ.

図 2.2 に示すように, アリスは秘密伝送したいメッセージ i を確率的符号器 $\varphi_n^A : \mathcal{M}_n \to \mathcal{X}^n$ に入力する．節 1.2.1 でも導入したように，確率的符号器 φ_n^A は，メッセージ i に対応するサブ符号 $\mathcal{C}_i$ から符号語 $\varphi_n^A(i) \in \mathcal{X}^n$ をランダムに選んでボブ (とイブ) に伝送する．ボブは主通信路の出力 $\varphi_n^B(i) \in \mathcal{Y}^n$ を復号器 $\psi_n^B : \mathcal{Y}^n \to \mathcal{M}_n$ に入力することでサブ符号 $\mathcal{C}_i$ を特定し，メッセージの推定値 $\hat{i}$ を得る．以降，そのような確率的符号器と復号器の組 (φ_n^A, ψ_n^B) をワイヤタップ通信路の符号と呼ぶ.

ここで，ボブの復号誤り確率 ε_n^B は，通信路符号化で定義したものと同様に

$$\varepsilon_n^B \triangleq \frac{1}{M_n} \sum_{i \in \mathcal{M}_n} \Pr\{\psi_n^B(\varphi_n^B(i)) \neq i\}. \tag{2.28}$$

と定義される．一方で，イブへの漏えい情報量 δ_n^E を

$$\delta_n^E \triangleq \frac{1}{M_n} \sum_{i \in \mathcal{M}_n} D(P_n^{(i)} || \pi_n), \tag{2.29}$$

と定義する．ここで，$D(\cdot||\cdot)$ は Kullback-Leibler 情報量 (2.19) である．δ_n^E は，メッセージ $i \in \mathcal{M}_n$ に対応するイブ側での出力分布 $P_n^{(i)}$ と予め定めておいた任意の確率分布 π_n との間の統計距離的な距離であり，この量が小さくなることは，イブ側での出力分布が入力されたメッセージとは無関係となることを意味する．

注意 2.3.2　上記の Kullback-Leibler 情報量による安全性評価は Han, Endo, Sasaki [79] や Hou, Kramer [126] によって導入された．一方で，それ以前の情報量基準としては，Csiszár [74] や Maurer [127]，Hayashi [73] が導入した相互情報量基準

$$I_n^E \triangleq \frac{1}{M_n} \sum_{i \in \mathcal{M}_n} D(P_n^{(i)} || P_n), \quad P_n \triangleq \frac{1}{M_n} \sum_{i \in \mathcal{M}_n} P_n^{(i)}$$

が知られていた．これらの間にはピタゴラスの定理 [122] から

$$\delta_n^E = I_n^E + D(P_n || \pi_n) \tag{2.30}$$

なる関係が成立するため，I_n^E は δ_n^E よりも若干弱い安全性評価を与えることになる．

また，相互情報量基準を符号長 n で規格化した I_n^E/n もよく利用される [66]．しかしながら，この量はその定義から符号長 n の増加に対して減少していくことは自明である．そのため，現在では基準 I_n^E/n に基づく安全性は最も弱い安全性とみなされている．　□

ワイヤタップ通信路の符号の設計には，式 (2.28) 及び式 (2.29) で定義された復号誤り確率と漏えい情報量を任意に小さくできるような伝送速度が明らかにされる必要がある．ボブがメッセージの推定を誤らないためには，メイン符号 $\mathcal{C}$ の $M_n L_n$ 個全ての符号語を誤らずに復号できる必要がある．メイン符号の符号化レートは

$$\frac{1}{n} \log M_n L_n = \frac{1}{n} \log M_n + \frac{1}{n} \log L_n = R_B + R_E$$

と定めることができる．ここで，

$$R_B \triangleq \frac{1}{n} \log M_n$$

はワイヤタップ通信路符号化での秘匿伝送可能な情報量に対応し，符号化レートと呼ぶ．一方で，

$$R_E = \frac{1}{n} \log L_n$$

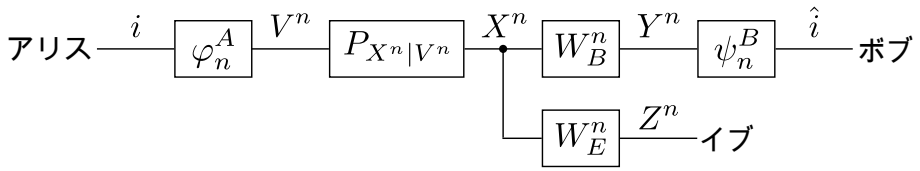

図 2.3 連接ワイヤタップ通信路の概念図.

はサブ符号 $\mathcal{C}_k$ のレートであり，イブに対する目眩ましのために犠牲となる情報量に対応する．これをランダムネスレートと呼ぶ.

ここで，次の条件を満足する符号化レート R_B，すなわち，復号誤り確率と漏えい情報量を $n \to \infty$ の極限で任意に小さくできる符号化の符号化レートを達成可能なレートと呼ぶ.

定義 2.3.1（達成可能なレート） 以下の条件を満たす場合に，符号化レート R_B を達成可能なレートと呼ぶ.

$$\lim_{n\to 0} \varepsilon_n^B = 0, \quad \lim_{n\to 0} \delta_n^E = 0$$

□

また，達成可能な符号化レート R_B の上界を秘匿容量と呼ぶ.

定義 2.3.2（秘匿容量） ワイヤタップ通信路の秘匿容量は

$$C_{\mathrm{S}} \triangleq \sup\{\text{ 達成可能な符号化レート } R_B\} \tag{2.31}$$

により定義される． □

2.3.3 通信路の連接

Wyner がはじめに行った定式化 [66] では，主通信路 W_B^n と盗聴者通信路 W_E^n に対して任意の通信路 $P_{Z^n|Y^n} : \mathcal{Y}^n \to \mathcal{Z}^n$ が存在し，それらの遷移確率関数に対して

$$W_E^n(\mathbf{z}|\mathbf{x}) = \sum_{\mathbf{y}\in\mathcal{Y}^n} W_B^n(\mathbf{y}|\mathbf{x}) P_{Z^n|Y^n}(\mathbf{z}|\mathbf{y}) \tag{2.32}$$

が成立する，特殊な条件が課されていた．すなわち確率変数 X，Y，Z がこの順番で Markov 連鎖 X-Y-Z を成す場合 (節 2.2.1 を参照) を考察の対象とした．この条件はボブが受信した信号にさらにノイズが重畳された信号をイブが受信するといった状況を意味するため，必然的にイブが得られる情報はボブの得られるそれよりも小さいものとなる．以降この条件を劣悪性の条件と呼ぶ．劣悪性の条件が満たされない場合の達成可能な符号化レートの上界を，Wyner は見出すことができなかった.

一方で，Csiszár ら [67] は，図 2.3 のように，補助通信路 $P_{X^n|V^n} : \mathcal{V}^n \to \mathcal{X}^n$ をワイヤタップ通信路に連接させることで，劣悪性の条件が成立しないワイヤタップ通信路

についても符号化レートの上界を示した．すなわち，補助確率変数 $V^n \in \mathcal{V}^n$ を導入して，入力確率変数 $X^n \in \mathcal{X}^n$ と出力確率変数 $Y^n \in \mathcal{Y}^n$，$Z^n \in \mathcal{Z}^n$ の間に Markov 連鎖 $V^n - X^n - Y^n Z^n$ が成立するような通信路を考えた．以降，この補助確率変及び補助通信路付きのワイヤタップ通信路のことを連接ワイヤタップ通信路 (W_B^{n+}, W_E^{n+}) と呼び，その遷移確率関数を以下に定義する．

$$W_B^{n+}(\mathbf{y}|\mathbf{v}) = \sum_{\mathbf{x}\in\mathcal{X}^n} W_B^n(\mathbf{y}|\mathbf{x}) P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \tag{2.33}$$

$$W_E^{n+}(\mathbf{z}|\mathbf{v}) = \sum_{\mathbf{x}\in\mathcal{X}^n} W_E^n(\mathbf{z}|\mathbf{x}) P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \tag{2.34}$$

2.3.4　復号誤り確率と漏えい情報量の上界

定義 2.3.1 からも明らかなように，秘匿容量は符号長 n が非常に長い符号に対する漸近的な評価量であり，現実のシステム設計で要求される，長さが有限である符号の評価には適用できないものであった．実際的には，復号誤り確率と漏えい情報量が符号長の関数として明らかになっており，それらを元にして符号長や符号化レートが設計できることが望ましい．

そこで，復号誤り確率 ε_n^B と漏えい情報量 δ_n^E の符号長の関数として表された上界がしばしば利用される [77, 74, 128, 73]．特に，漏洩情報量が最も強い尺度 (2.29) で計量される場合については，[79] で証明されている．次の定理は，[79] で証明された最も強い尺度 (2.29) で計量される場合についての上界である．

定理 2.3.1（復号誤り確率と漏えい情報量の上界 [79]）　任意のワイヤタップ通信路 (W_B^n, W_E^n) とメッセージ数 M_n 及びサブ符号の符号語数 L_n が与えられたとき，その復号誤り確率 ε_n^B 及び漏えい情報量 δ_n^E に対して

$$\varepsilon_n^B \le 2 \inf_{0\le\rho\le 1} (M_n L_n)^\rho e^{-\phi(\rho|W_B^{n+}, P_{V^n})} \tag{2.35}$$

$$\delta_n^E \le 2 \inf_{0<\rho<1} (\rho L_n^\rho)^{-1} e^{-\phi(-\rho|W_E^{n+}, P_{V^n})} \tag{2.36}$$

が成立する符号 (φ_n^A, ψ_n^B) が存在する．ここで，

$$\phi(\rho|W_B^{n+}, P_{V^n}) \stackrel{\triangle}{=} -\log \sum_{\mathbf{y}} \left(\sum_{\mathbf{v}} P_{V^n}(\mathbf{v}) W_B^{n+}(\mathbf{y}|\mathbf{v})^{\frac{1}{1+\rho}} \right)^{1+\rho} \tag{2.37}$$

$$\phi(-\rho|W_E^{n+}, P_{V^n}) \stackrel{\triangle}{=} -\log \sum_{\mathbf{z}} \left(\sum_{\mathbf{v}} P_{V^n}(\mathbf{v}) W_B^{n+}(\mathbf{z}|\mathbf{v})^{\frac{1}{1-\rho}} \right)^{1-\rho} \tag{2.38}$$

である．また，P_{V^n} は $\mathcal{V}^n$ 上の入力確率分布である．　□

注意 2.3.3　式 (2.35) ははじめ Gallager[77] によって，盗聴者なしの通信路符号化定理問題の文脈で導入された．対して，式 (2.36) は [79] において，通信路 Resolvability[71] の方法を援用することで示された．　□

定理 2.3.1 の式 (2.35) と (2.36) により，通信路と入力の確率分布が与えられれば，符号長 n に対する復号誤り確率 ε_n^B と漏洩情報量 δ_n^E が十分に小さいとみなせる符号長 n を見出すことができる．しかし，これらの式中には符号長 n が陽に現れていない上に，通信路の確率分布 $W_B^{n+}(\mathbf{y}|\mathbf{v})$，$W_B^{n+}(\mathbf{y}|\mathbf{v})$ の計算は符号長 n が増大するに連れて指数関数的に困難になっていく．そのため，以降では主通信路 W_B と盗聴者通信路 W_E が定常無記憶通信路である場合を考察の対象にする．すなわち，通信路 $W_B : \mathcal{X} \to \mathcal{Y}$, $W_E : \mathcal{X} \to \mathcal{Z}$ が存在し，

$$W_B^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n W_B(y_i|x_i), \quad W_E^n(\mathbf{z}|\mathbf{x}) = \prod_{i=1}^n W_E(z_i|x_i) \tag{2.39}$$

と書けると仮定する．ここで，$\mathbf{x} = (x_1, \cdots, x_n)$，$\mathbf{y} = (y_1, \cdots, y_n)$，$\mathbf{z} = (z_1, \cdots, z_n)$ である．以降，2 つの定常無記憶通信路からなるワイヤタップ通信路を定常無記憶ワイヤタップ通信路 (W_B, W_E) と表記する．

また，入力確率変数 $V^n X^n$ も独立同分布 (i.i.d.) に，$\mathcal{V} \times \mathcal{X}$ 上の確率分布 P_{VX} から生成されるとする．ここで，分布 P_{VX} の周辺確率分布 P_X，P_V と補助通信路 $P_{X|V} : \mathcal{V} \to \mathcal{X}$ 遷移確率分布関数は

$$P_{X^n}(\mathbf{x}) = \prod_{i=1}^n P_X(x_i), \quad P_{V^n}(\mathbf{v}) = \prod_{i=1}^n P_V(v_i), \tag{2.40}$$

$$P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) = \prod_{i=1}^n P_{X|V}(x_i|v_i) \tag{2.41}$$

と書ける．なお，$\mathbf{v} = (v_1, \cdots, v_n)$ である．

すると，定常無記憶な連接ワイヤタップ通信路の遷移確率分布関数は次のように書ける．

$$W_B^+(y|v) = \sum_{x \in \mathcal{X}} W_B(y|x) P_{X|V}(x|v) \tag{2.42}$$

$$W_E^+(z|v) = \sum_{x \in \mathcal{X}} W_E(z|x) P_{X|V}(x|v) \tag{2.43}$$

定常無記憶ワイヤタップ通信路に対しては，式 (2.37) を

$$\begin{aligned} &- \log \sum_{\mathbf{y}} \left(\sum_{\mathbf{v}} P_{V^n}(\mathbf{v}) W_B^{n+}(\mathbf{y}|\mathbf{v})^{\frac{1}{1+\rho}} \right)^{1+\rho} \\ &= - \log \left[\sum_{y \in \mathcal{Y}} \left(\sum_{v \in \mathcal{V}} P_V(v) W_B^+(y|v)^{\frac{1}{1+\rho}} \right)^{1+\rho} \right]^n \\ &= -n \log \sum_{y \in \mathcal{Y}} \left(\sum_{v \in \mathcal{V}} P_V(v) W_B^+(y|v)^{\frac{1}{1+\rho}} \right)^{1+\rho} \end{aligned}$$

のように書き直せるため (式 (2.38) についても同様)，定理 2.3.1 の各上界を $\exp(-nc)$ のような符号長 n が顕になった形で表現できる．復号誤り確率 ε_n^B に対するこの指数 c を誤

り指数と呼び，漏えい情報量 δ_n^E に対しては秘匿性指数と呼ぶ．次の定理に，その具体的な表現を記す．

定理 2.3.2（誤り指数と秘匿性指数 [79]）　定常無記憶ワイヤタップ通信路 (W_B, W_E) と任意の符号化レート R_B とランダムネスレート R_E が与えられたとき，誤り指数 $F(P_V, R_B, R_E)$ と秘匿性指数 $H(P_V, R_E)$ を

$$F(P_V, R_B, R_E) \stackrel{\triangle}{=} \sup_{0\le\rho\le 1} \left[\phi(\rho|W_B, P_V) - \rho(R_B + R_E)\right] \tag{2.44}$$

$$H(P_V, R_E) \stackrel{\triangle}{=} \sup_{0<\rho<1} \left[\phi(-\rho|W_E, P_V) + \rho R_E\right] \tag{2.45}$$

と定義する．ここで，関数 $\phi(\rho|W_B, P_V)$ と $\phi(-\rho|W_E, P_V)$ は

$$\phi(\rho|W_B, P_V) \stackrel{\triangle}{=} -\log\left[\sum_{y\in\mathcal{Y}}\left(\sum_{v\in\mathcal{V}} P_V(v)\left[\sum_{x\in\mathcal{X}} W_B(y|x)P_{X|V}(x|v)\right]^{\frac{1}{1+\rho}}\right)^{1+\rho}\right] \tag{2.46}$$

$$\phi(\rho|W_E, P_V) \stackrel{\triangle}{=} -\log\left[\sum_{z\in\mathcal{Z}}\left(\sum_{v\in\mathcal{V}} P_V(v)\left[\sum_{x\in\mathcal{X}} W_E(z|x)P_{X|V}(x|v)\right]^{\frac{1}{1-\rho}}\right)^{1-\rho}\right] \tag{2.47}$$

と定義される．

すると，復号誤り確率 ε_n^B 及び漏えい情報量 δ_n^E が

$$\varepsilon_n^B \le 2e^{-nF(P_V, R_B, R_E)} \tag{2.48}$$

$$\delta_n^E \le 2e^{-nH(P_V, R_E)} \tag{2.49}$$

を満足するようなワイヤタップ通信路符号 (φ_n^A, ψ_n^B) が存在する．　□

この誤り指数 $F(P_V, R_B, R_E)$ と秘匿性指数 $H(P_V, R_E)$ は，入力確率分布と通信路の遷移確率分布の関数だけではなく，符号化レート R_B とランダムネスレート R_E の関数ともなっている．そのため，これらの上界と指数は，レートを具体的に設定した場合の性能評価のための関数としても利用できる．

下記の補題に，この指数が持つ性質を列挙する．

補題 2.3.1（誤り及び秘匿性指数の性質）　誤り指数 $F(P_V, R_B, R_E)$ と秘匿性指数 $H(P_V, R_E)$ は下記の性質を持つ．

1. $R_B + R_E = I(V;Y)$ において，$F(P_V, R_B, R_E) = 0$ かつ連続である．
2. $R_E = I(V;Z)$ において，$H(P_V, R_E) = 0$ かつ連続である．
3. $R_B + R_E < I(V;Y)$ では $F(P_V, R_B, R_E)$ は $R_B + R_E$ の単調減少かつ正の凸関数であり，$R_B + R_E \ge I(V;Y)$ では $F(P_V, R_B, R_E) = 0$ となる．
4. $R_E > I(V;Z)$ では $H(P_V, R_E)$ は R_E の単調増加かつ正の凸関数であり，$R_E \le I(V;Z)$ では $H(P_V, R_E) = 0$ となる．

□

性質 1. と 3. は，主通信路の相互情報量 $I(V;Y)$ 以下のレート $R_B + R_E$ の符号を用いるならば，上界 (2.48) の指数が 0 にならないため，任意の誤り率を十分な長さの符号で達成できることを示している．すなわち，Shannon の通信路符号化定理そのものとなっている．また，レート $R_B + R_E$ を小さくする，すなわち伝送可能情報量を妥協することにより指数の値が増加し，ある基準の復号誤り確率をより短い符号長で達成できることを示している．

一方で，性質 2. と 4. は，盗聴者通信路の相互情報量 $I(V;Z)$ 以上のランダムネスレート R_E を持つ符号を用いるならば，上界 (2.49) の指数が 0 にならないため，任意の漏えい情報量を十分に長い符号で達成できることを示している．これは，盗聴者通信路の出力を入力でコントロールして，どのような入力に対してもほぼランダムな出力が現れるために必要なレートという解釈が可能である．また，レート R_E を大きくする，すなわちサブ符号の符号語数を増やすことにより指数の値が増加し，ある基準の漏えい情報量をより短い符号長で達成できることを示している．

2.3.5 定常無記憶ワイヤタップ通信路の秘匿容量の具体的表現

補題 2.3.1 の性質から，$R_B + R_E = I(V;Y) - \gamma$ かつ $R_E = I(V;Z) + \gamma$ を満足する符号化レート R_B は達成可能であることが直ちに示される．ここで，γ は符号長 n に対して任意に小さくできる定数である．以上より，定常無記憶ワイヤタップ通信路 (W_B, W_E) の秘匿容量は次の定理のように与えられる．

定理 2.3.3（秘匿容量） 定常無記憶ワイヤタップ通信路 (W_B, W_E) の秘匿容量は

$$C_{\mathrm{S}} = \max_{VX} [I(V;Y) - I(V;Z)] \tag{2.50}$$

である．ここで，最大化 $\max_{VX}$ は入力確率分布 P_V と補助通信路 $P_{X|V}$ に亘って成される．

□

ここで，通信路間に $I(X;Y) - I(X;Z) \geq 0$ が任意の P_X について成立するという優劣関係が成立していると仮定する．この条件を more capable と呼ぶ．同様の通信路間に成り立つ優劣関係としては，既に劣悪性 (2.32) を導入したが，劣悪性が担保されれば，more capable も成り立つことが知られている．実際に

$$\begin{aligned} I(X;Y) - I(X;Z) &\overset{(1)}{=} H(X) - H(X|Y) - H(X) + H(X|Z) \\ &= H(X|Z) - H(X|Y) \\ &\overset{(2)}{\geq} H(X|ZY) - H(X|Y) \\ &\overset{(3)}{=} H(X|Y) - H(X|Y) = 0 \end{aligned}$$

が成立する．なお，(1)，(2)，(3) でそれぞれ節 2.2 で導入した相互情報量の性質 1.，エントロピーの性質 2.，エントロピーの性質 4. を利用した．

さらに，ワイヤタップ通信において more capable の条件が成立しているとき，

$$\begin{aligned} I(V;Y)-I(V;Z) &\overset{(1)}{=} I(VX;Y)-I(X;Y|V)-I(VX;Z)+I(X;Z|V) \\ &\overset{(2)}{=} I(X;Y)-I(X;Z)-\sum_{v\in\mathcal{V}} P_V(v)I(X;Y|V=v)+I(X;Z|V=v) \\ &\overset{(3)}{\leq} I(X;Y)-I(X;Z) \end{aligned}$$

が成立する．ここで，(1)，(2) でそれぞれ節 2.2 で導入した相互情報量の性質 4.(相互情報量のチェインルール) と相互情報量の性質 5. を用い，(3) では上で述べた more capable の条件を利用した．

以上の議論から，ワイヤタップ通信路が more capable(あるいは劣悪性) の条件を満足しているならば，秘匿容量 C_{S} は

$$C_{\mathrm{S}} = \max_X [I(X;Y)-I(X;Z)] \tag{2.51}$$

となり，補助通信路は不要となる．ここで，最大化 $\max_X$ は入力確率変数に亘って成される．

注意 2.3.4　例として，主通信路 W_B と盗聴者通信路 W_E をそれぞれビット反転確率が ϵ_y と ϵ_z の BSC(図 2.1) について，秘匿容量 C_{S} の計算を行う．ここで，ビット反転確率が $0 \leq \epsilon_y < \epsilon_z < 0.5$ ならば，劣悪性の条件 (2.32) が満足される点に注意する．それは，ビット反転確率が $(\epsilon_z-\epsilon_y)/(1-2\epsilon_y)$ である BSC，$W_{Z|Y}$ を主通信路 W_B に連接させると，結果の通信路がビット反転確率

$$(1-\epsilon_y)\frac{\epsilon_z-\epsilon_y}{1-2\epsilon_y} + \left(1-\frac{\epsilon_z-\epsilon_y}{1-2\epsilon_y}\right)\epsilon_y = \epsilon_z$$

である BSC，すなわち盗聴者通信路 W_E になることにより確かめられる．そのため，補助変数及び補助通信路を考慮する必要が無い．また，$0 \leq \epsilon_z < \epsilon_y < 0.5$ ならば，秘匿容量 C_{S} は 0 となる．

反転確率 ϵ の BSC の相互情報量は式 (2.26) により与えられるため，ビット反転確率が ϵ_y の主通信路 W_B と ϵ_z である盗聴者通信路 W_E の相互情報量の差は

$$I(X;Y)-I(X;Z) = h_2(p+\epsilon_y-2p\epsilon_y)-h_2(p+\epsilon_z-2p\epsilon_z)-h_2(\epsilon_y)+h_2(\epsilon_z) \tag{2.52}$$

となる．

秘匿容量はこの相互情報量の差を入力確率 p で最大化することにより求められるが，簡単な微分計算から $p=1/2$ で最大化されることが示せるため，BSC-ワイヤタップ通信路の秘匿容量は

$$C_{\mathrm{S}} = h_2(\epsilon_z)-h_2(\epsilon_y) \tag{2.53}$$

となる． □

注意 2.3.5 more capable(あるいは劣悪性) の条件を満足している場合，誤り及び秘匿性指数における関数 (2.46) 及び (2.47) は

$$\phi(\rho|W_B, P_V) \stackrel{\triangle}{=} -\log\left[\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} P_X(x)W_B(y|x)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right] \tag{2.54}$$

$$\phi(\rho|W_E, P_V) \stackrel{\triangle}{=} -\log\left[\sum_{z\in\mathcal{Z}}\left(\sum_{x\in\mathcal{X}} P_X(x)W_E(z|x)^{\frac{1}{1-\rho}}\right)^{1-\rho}\right] \tag{2.55}$$

となる． □

注意 2.3.6 秘匿容量 (2.50) の具体的な表現の証明には，情報理論において伝統的な手法である大数の法則を利用して確率収束の立場から行うものもある．しかし，本論で導入した復号誤り確率と漏洩情報量のバウンドから証明する方法では，独立した指数の性質から秘匿容量を導いている．これは，後者では誤り訂正符号器としての機能と確率的符号器としての機能を独立に設計可能であることを意味している．

前者の証明に則り，1 つの符号に誤り訂正と確率的符号器の機能を両立させた例としては [129, 130] を挙げることができる．一方で，後者の証明に則り，確率的符号器の機能を暗号学的なハッシュ関数に担わせ，任意の誤り訂正符号からワイヤタップ通信路符号が構築可能であることを示した例として，[85, 73] が知られている． □

2.3.6 誤り指数と秘匿性指数の解釈:信頼性-安全性トレードオフ

ここでは，前節までに導出した誤り指数と秘匿性指数について計算例を示し，これらの関数を用いた評価法とその解釈について述べる．計算の対象となる通信路として，二元対称通信路 (BSC) を扱う．

BSC の誤り指数は Gallager[77] によって，最適化すべき変数 ρ の媒介変数表示の形で与えられている．

定理 2.3.4（BSC の誤り指数） ビット反転確率 ϵ_y である BSC が与えられたときの誤り指数とレート $R = R_B + R_E$ の $\rho \in [0, 1]$ による媒介変数表示は

$$F(\rho) = T_\rho(\epsilon_y) - h(\epsilon_y, \rho) \tag{2.56}$$

$$R(\rho) = \log 2 - h(\epsilon_y, \rho) \tag{2.57}$$

と与えられる．ここで，

$$h(\epsilon, \rho) \stackrel{\triangle}{=} -\delta(\epsilon, \rho)\log\delta(\epsilon, \rho) - (1-\delta(\epsilon, \rho))\log(1-\delta(\epsilon, \rho)) \tag{2.58}$$

$$\delta(\epsilon, \rho) \stackrel{\triangle}{=} \frac{\epsilon^{\frac{1}{1+\rho}}}{\epsilon^{\frac{1}{1+\rho}} + (1-\epsilon)^{\frac{1}{1+\rho}}} \tag{2.59}$$

と定義した．

ただし，以上の媒介変数表示は $\rho \in [0,1]$ で有効である．$R \leq R(\rho=1) = \log 2 - h(\epsilon,1)$ を満足するレート R に対しては，誤り指数は

$$F(P_X, R_B, R_E) = h(\epsilon,1) + T(\epsilon,1) - R \tag{2.60}$$

となる．

□

Gallager[77] の導出は ρ の符号を反転しても有効であるため，BSC の秘匿性指数も直ちに導出される．ただし，以下では確率分布を秘匿性指数と与える，$\Pr\{x=1\} = 1/2$ としている点に注意する．

定理 2.3.5（BSC の秘匿性指数）　ビット反転確率 ϵ_z である BSC が与えられたときの秘匿性指数とランダムネスレート R_E の $\rho \in [-1,0]$ による媒介変数表示は

$$H(\rho) = T(\epsilon_z, \rho) - h(\epsilon_z, \rho) \tag{2.61}$$
$$R_E(\rho) = \log 2 - h(\epsilon_z, \rho) \tag{2.62}$$

と与えられる．

一方で，$\rho = -1$ では，

$$\begin{aligned}
&\lim_{\rho\to-1} \phi(\rho|W_B, P_X) \\
&= \lim_{\rho\to-1} \left[\rho \log 2 - (1+\rho)\log\left(\epsilon^{\frac{1}{1+\rho}} + (1-\epsilon)^{\frac{1}{1+\rho}}\right)\right] \\
&= \lim_{\rho\to-1} \left[\rho \log 2 - (1+\rho)\log\left(\frac{\epsilon^{\frac{1}{1+\rho}}}{(1-\epsilon)^{\frac{1}{1+\rho}}} + 1\right) - \log(1-\epsilon)\right] \qquad (2.63) \\
&= -\log 2 - \log(1-\epsilon) \qquad (2.64)
\end{aligned}$$

が成り立つため，$R_E \geq \lim_{\rho\to-1} R_E(\rho) = \log 2$ を満足するレート R_E に対しては，秘匿性指数は

$$H(P_X, R_E) = R_E - \log 2 - \log(1-\epsilon) \tag{2.65}$$

となる．

□

図 2.4 に，ビット反転確率 $\epsilon_y = 0.05$ の主通信路 W_B の誤り指数と，ビット反転確率 $\epsilon_z = 0.2$ である盗聴者通信路 W_E の秘匿性指数をそれぞれ示す．主通信路と盗聴者通信路の通信路容量はそれぞれ $C_B = 0.495$ [nats] と $C_E = 0.193$ [nats] となり，秘匿容量は単純にそれらの差である $C_{\mathrm{S}} = 0.302$ [nats] となる．この図からは，各通信路の容量の値付近で各指数が 0 になっており，誤り指数はレートに対して単調減少な凸関数，秘匿性指数はレートに対して単調増加な凸関数となっているといった，補題 2.3.1 に述べた性質を確認できる．

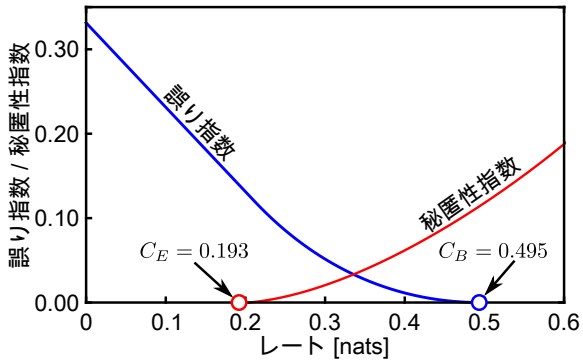

図 2.4　ビット反転確率 $\epsilon_y = 0.05$ の主通信路 W_B の誤り指数と，ビット反転確率 $\epsilon_z = 0.2$ である盗聴者通信路 W_E の秘匿性指数．

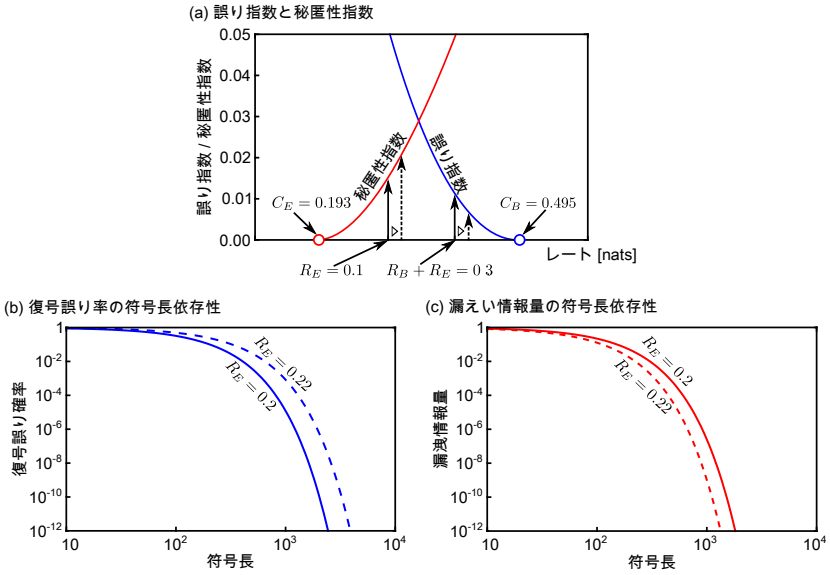

図 2.5　(a) 図 2.4 の BSC ワイヤタップ通信路に関する信頼性-秘匿性トレードオフ概念図．(b) (a) の誤り指数に対する復号誤り率の符号長依存性．(c) (a) の秘匿性指数に対する漏えい情報量の符号長依存性．

ここから，誤り指数と秘匿性指数の操作的な意味について述べる．秘匿容量はワイヤタップ通信路符号化における伝送可能情報量の理想的に長い符号に対する上界値であるが，有限の長さの符号ではこの限界を達成することはできず，性能を妥協する必要がある．そこで，誤り指数と秘匿性指数により，符号化レート R_B とランダムネスレート R_E を設計する上での定量的な指標を与える．

図 2.5(a) は図 2.4 を拡大したものである．この図中の実線の矢印で示すように，主通信路の通信路容量 0.495 [nats] に対して $R_B^* + R_E^* = 0.3$ [nats] ととり，盗聴者通信路の容量 0.193 [nats] に対して $R_E^* = 0.2$ [nats] ととる符号の設計を考える．これは，秘匿指数により与えられる限界よりも，冗長性を多く取り，多くの情報量をイブに対する目眩ましとして犠牲にする設計である．

このときの誤り指数と秘匿性指数の値から，上界 (2.48) と (2.49) によって復号誤り確率と漏えい情報量の符号長依存性を描くと，図 2.5(b) 及び (c) の実線のようになる．この図からは，図 2.5(a) に示したレートで符号を設計した場合には，符号長 2000 程度の符号によって，復号誤り率と漏えい情報量の両方を 10^{-12} 以下に抑えることが可能であることが示される．

もう一つの指数の利用法として，安全性と信頼性間のトレードオフの定量化を挙げることができる．図 2.5(a) に示す実線の矢印から破線の矢印の変化に示すように，R_B^* を固定しながら $R_E^* = 0.2$ [nats] を $R_E = 0.22$ へと増加させる．これは，メッセージの個数 M_n を固定しつつサブ符号 $\mathcal{C}_i$ の個数 L_n を増加させる操作に対応しているこの操作後に，秘匿性指数は増加するが，誤り指数は減少する．すなわち，信頼性を犠牲にしつ安全性を向上させる，一種のトレードオフ関係を操作していることになる．また，この操作後の符号長依存性は図 2.5(b) の破線に示すように，復号誤り確率を達成する符号長が増加するものの，漏えい情報量を達成する符号長は減少している．以上のような誤り指数と秘匿性指数を利用したトレード・オフ関係の定量化は，ワイヤタップ通信路符号化の文脈では [79] で導入され，秘密鍵共有では Chou ら [93] によって議論されている．

以上に述べてきたように，誤り指数と秘匿性指数は，有限の長さの符号の設計を行う上での指標を与える，強力なツールとなり得る．第 3 章及び第 4 章では，理論及び実験データから構築された通信路モデルを用いて，上記と同様の議論を展開することになる．

2.4　秘密鍵共有

本節では，秘密鍵共有の情報理論的な定式化について述べる．

はじめに，Maurer[68] によって導入された通信路モデルについて簡単に触れる．このモデルでは，鍵蒸留プロトコルはワイヤタップ通信路符号化をベースに構築されている．しかし，QKD をはじめとする実用化が進んでいる方式では，アリスとボブの間での鍵の一致を図るためのプロトコルである情報整合と，そこからイブの持つ情報とは無関係な鍵を作り出すプロトコルである秘匿性増強の 2 つを分離して設計する場合が多い．

そのため，本節の後半ではそれらの先行研究に倣って，鍵蒸留プロトコルを情報整合プロトコルと秘匿性増強プロトコルに分離する場合について述べる．そして，最終的にはこのような分離設計の導入が秘密鍵生成レートを損なわないことを議論する．

2.4.1　通信路モデルに基づく秘密鍵共有

秘密鍵共有は乱数の送付方法の違いによって，情報源モデルと通信路モデルの 2 つに大別できる．情報源モデルでは，人工衛星に搭載された乱数源や大気の揺らぎのような自然界に存在する物理過程を乱数と見なし，アリスとボブはそれらから出力される乱数から鍵を抽出する．このモデルは，無線電波通信における秘密鍵共有の基礎となっているが，単位時間当たりの生成鍵レートが使用する乱数源の帯域によって本質的に制限されるという

問題を孕む.

一方で，通信路モデルでは，既に述べたように，アリスが生成した乱数を誤りのある通信路でボブに伝送することにより，鍵送付が行われる．通信路モデルの場合，乱数の生成速度を高速にするほど，単位時間当たりの鍵生成レートを向上させることができる．

その鍵レートについて議論を行うために，ここで再び，図 1.4 の状況を考える．この図では，ボブの受信系列 $\mathbf{y}$ に対して，アリスは $\mathbf{x} = \mathbf{y} \oplus \mathbf{e}$ という系列を持ち，イブは $\mathbf{z} = \mathbf{y} \oplus \mathbf{e} \oplus \mathbf{d}$ という系列を持つ状態を作り出せた．

この乱数配布後，ボブから 1 回だけ公開通信路を使ってアリスへと情報を伝送することで鍵蒸留を行う．以下では，$\mathcal{M}_n$ は公開通信路で公開されるメッセージの集合，$\mathcal{K}$ は鍵の集合とする．ボブは符号器 $\varphi_B : \mathcal{Y}^n \to \mathcal{M}_n$ を用いてメッセージ $i \in \mathcal{M}_n$ を出力し，公開通信路でアリスに伝送する．同時に，ボブは自身が持つ復号器 $\psi_B : \mathcal{Y}^n \to \mathcal{K}$ によって受信系列 $\mathbf{y}$ から鍵 $k_B \in \mathcal{K}$ を出力する．一方，アリスは自分の復号器 $\psi_A : \mathcal{X}^n \times \mathcal{M}_n \to \mathcal{K}$ に，自分が送信した乱数列 $\mathbf{x}$ とボブから送られてきたメッセージ i を入力することにより，鍵 $k_A \in \mathcal{K}$ を得る．以上のような復号器及び復号器の組 (ψ_B, ψ_B, ψ_A) を鍵蒸留プロトコルの符号と呼ぶ.

このプロトコルの誤り確率 ε_n^B，すなわちアリスの鍵 K_A とボブの鍵 K_B が異なる確率は

$$\varepsilon_n^B \triangleq \frac{1}{M_n} \sum_{k_A, k_B \in \mathcal{K}} \Pr\{k_A \neq k_B\} \tag{2.66}$$

と定義される．また，漏えい情報量を計量する基準としては相互情報量基準 [127]

$$I_n^E \triangleq D(P_{K M_n Z^n} || P_{\mathrm{K,Unif}} \times P_{M_n, Z^n}) \tag{2.67}$$

を採用する．ただし，$P_{\mathrm{K,Unif}}$ は $\mathcal{K}$ 上の一様分布である.

ワイヤタップ通信路で符号化レートを定義したのと同様に，ここでも秘密鍵の生成効率を計量するため秘密鍵レート R_{K} を

$$R_{\mathrm{K}} \triangleq \frac{H(K)}{n} = \frac{\log |K|}{n} \tag{2.68}$$

により定義する．ここで，2 番目の等式は鍵が一様な確率変数であることによる．そして，下記の条件を満足する R_{K} を達成可能な秘密鍵レートと呼ぶ.

定義 2.4.1（達成可能な秘密鍵レート） 以下の条件を満たす場合に，レート R_{K} を達成可能な鍵レートと呼ぶ.

$$\lim_{n \to 0} \varepsilon_n^B = 0, \quad \lim_{n \to 0} I_n^E = 0$$

□

また，達成可能な鍵レート R_{K} の上界を秘密鍵容量と呼ぶ.

定義 2.4.2（秘密鍵容量）　秘密鍵共有における秘密鍵容量は

$$C_{\mathrm{K}} \stackrel{\triangle}{=} \sup\{\text{ 達成可能な } R_{\mathrm{K}}\} \tag{2.69}$$

により定義される．□

以上の定義の元，鍵蒸留プロトコルの符号 $(\psi_B,\ \psi_B,\ \psi_A)$ はワイヤタップ通信路符号の符号器と復号器を用いて構築することができる．これは，Y-X-Z なる Markov 連鎖，すなわち劣悪性の条件 (2.32) が成立しているワイヤタップ通信路において，ボブが乱数 Y^n をアリスとイブに伝送したという状況と等価であるためである．従って，ワイヤタップ通信路の秘匿容量が

$$C_{\mathrm{K}} \geq I(X;Y) - I(Y;Z) \tag{2.70}$$

のように，達成可能な秘密鍵レートの下界を与えている．ボブは生成した乱数をこのレートで設計した長さ n のワイヤタップ通信路符号で符号化し，それを公開通信路で伝送する．そして，アリスとボブは共通のワイヤタップ通信路符号の復号器で復号することによって鍵を蒸留できる．

注意 2.4.1　ここで，秘密鍵レートに関していくつかの注意を述べる．

ここまで公開通信路の使用を 1 回しか許さない場合について議論を行ったが，アリスが奇数ラウンド $(l = 1, 3, 5, \cdots, q-1)$，ボブが偶数ラウンド $(l = 2, 4, 6, \cdots, q)$ に公開通信路でメッセージを伝送するといった一般化も考えられる．しかし，この場合の秘密鍵容量は判明していない．

また，ワイヤタップ通信路符号化の秘匿容量は秘密鍵容量の下界を与えるが，上界値がこれと一致しない．そこで，本論文では，式 (2.70) を通信路モデルにおける秘密鍵レートと見なして議論及び解析を行う．

また，式 (2.70) は Y-X-Z なる Markov 連鎖が成立する場合の下界であり，X-Y-Z なる Markov 連鎖が成立する場合には $I(X;Y) - I(X;Z)$ が秘密鍵容量の下界を与える．□

2.4.2　情報整合と秘匿性増強を分離したプロトコル

前節では符号器と復号器の組として，すなわち 1 つの符号で抽象化されていた秘密鍵蒸留プロトコルであったが，この節では，アリスの乱数とボブの乱数の間の誤りを訂正するプロトコルである情報整合 [94, 95] と，イブの持つ情報と無相関かつ完全にランダムな鍵を作り出すプロトコルである秘匿性増強 [94, 96] に分けて実装可能であることを示す．特に，実用的な観点からは，この 2 つのプロトコルが互いに独立に設計可能であることが望ましい．秘匿性増強の節で，そのような手法を導入し，その上で，秘密鍵容量の下界が，前節で導入した方法よりも劣化しないことを示す．

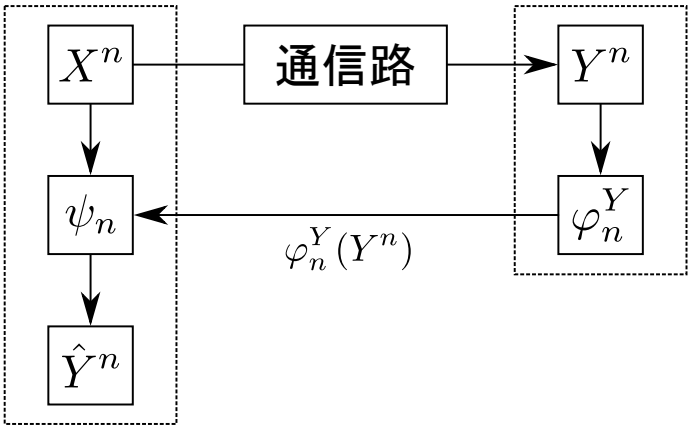

図 2.6 Slepian-Wolf 符号化の概念図.

Slepian-Wolf 符号化による情報整合

図 2.6 の概要図を用いて情報整合の説明を行う.

アリスは乱数源から乱数 $X^n \in \mathcal{X}^n$ を生成し，それを誤りのある通信路でボブに伝送し，ボブは乱数 $Y^n \in \mathcal{Y}^n$ を得る．ボブは，自分の乱数を符号器 $\varphi_n^Y : \mathcal{Y}^n \to \mathcal{M}_n$ にて圧縮して，メッセージ $\varphi_n^Y(Y^n) \in \mathcal{M}_n$ を得る．そのメッセージ $\varphi_n^Y(Y^n)$ をアリスに認証付き公開通信路で伝送し，アリスは $\varphi_n^Y(Y^n)$ と自身が持つ乱数 X^n を復号器 $\psi_n : \mathcal{X}^n \times \mathcal{M}_n \to \mathcal{Y}^n$ に入力してボブの乱数の推定を得る．すなわち，情報整合の目的が達成される.

以上のプロセスは，アリスの系列 X^n を補助情報とする，Y^n の圧縮問題として捉えられる．そのような圧縮問題は，Slepian-Wolf 符号化 [72, 131] によって定式化することができる．以降，以上で説明した符号器-復号器の組 (φ_n^Y, ψ_n) を Slepian-Wolf 符号と呼ぶ.

いま，圧縮レートを

$$R_Y = \frac{1}{n} \log |\mathcal{M}_n| \tag{2.71}$$

により定義し，復号誤り確率を

$$\epsilon_n = \Pr(\psi(X^n, \varphi_n^Y(Y^n)) \neq \hat{Y}^n) \tag{2.72}$$

と定義する．この誤り確率が十分に長い符号長に対して漸近的に 0 に近づくようなレート R_Y の上界は，下記に示す Slepian-Wolf の定理 [72] によって与えられる.

定理 2.4.1（Slepian-Wolf の定理 [72]） レート R_Y が

$$R_Y \geq H(Y|X) \tag{2.73}$$

を満足すれば，復号誤り確率 ϵ_n が漸近的に 0 に近づく Slepian-Wolf 符号 (φ_n^Y, ψ_n) が存在する. □

この定理から，ボブが Slepian-Wolf 符号の符号器 φ_n^Y によって，受信した乱数列 $\mathbf{y}$ を圧縮率 $H(Y|X)$ まで圧縮すれば，アリスは自分の持つ系列 $\mathbf{x}$ とボブが公開したメッセージ $\varphi_n^Y(Y^n)$ から，ボブの乱数列 Y^n を再生可能であることが示される．

ユニバーサル 2 ハッシュ関数による秘匿性増強

秘匿性増強のステップでは，アリスとボブが情報整合を経て共有した乱数列に対して特定の圧縮操作を施すことによって，イブの持つ全ての情報と無相関で，なおかつ完全にランダムな乱数列を生成することが目的となる．そのような圧縮操作がユニバーサル 2 ハッシュ関数を用いれば構成可能であることが示されている [96, 73, 132]．

はじめに，ユニバーサル 2 ハッシュ関数 [86, 104] を導入する．

定義 2.4.3（ユニバーサル 2 ハッシュ関数）　集合 $\mathcal{X}^n$ から $\mathcal{K}_n$ への関数族 $\mathcal{F}_n$ を考える．ここから関数 $F_n \in \mathcal{F}_n$ が一様分布に従って選択されるとしたときに，

$$\Pr(F_n(\mathbf{x}) \neq F_n(\mathbf{x}')) \geq \frac{1}{|\mathcal{K}_n|} \tag{2.74}$$

が任意の $\mathbf{x} \neq \mathbf{x}' \in \mathcal{X}^n$ について成立するならば，$\mathcal{F}_n$ をユニバーサル 2 ハッシュ関数族と呼ぶ．□

ユニバーサル 2 ハッシュ関数族としての性質を持つ関数の簡単な例としては，全ての行と列が $\{0,1\}$ から一様に選択される行列が挙げられる．しかし，そのような行列のアリスとボブ間での共有や計算処理は実用的ではない．その問題を回避するために，対角線上に並ぶ要素が全て等しいテプリッツ行列が用いられる [73][*1]．アリスとボブが使用するユニバーサル 2 ハッシュ関数はイブも知っていると仮定する．

なお以降では，これまで利用してきた相互情報量や Kullback-Leibler 情報量に基づく安全性基準の代わりに，秘密鍵共有や QKD の文脈では次に述べる変動距離を元にした安全性基準

$$d_n^E = d(P_{K_B M_n F_n Z^n}, P_{\mathrm{K,Unif}} \times P_{M_n F_n Z^n}) \tag{2.75}$$

に基いて議論を展開する．ここで，$P_{K_B M_n Z^n}$ はボブが持つ鍵 K_B，情報整合において公開された情報 M_n，ハッシュ関数に関する情報 F_n，イブが持つ全情報 Z^n に跨る確率分布であり，$P_{M_n F_n Z^n}$ はその K_B に関する周辺分布である．また，$P_{\mathrm{K,Unif}}$ は鍵全体を定義域として持つ一様分布である．この安全性基準は汎用的安全性基準 [133, 134] と呼ばれる．

秘密鍵共有や QKD 自体は鍵を交換するプロトコルに過ぎず，それらとワンタイムパッド暗号のような暗号プロトコルの併用が前提とされている．そのようなシステムにおいて，プロコトル全体の安全性を鍵共有のプロトコルの安全性に帰着できるように導入された概念である．なお，[79] や [75] 等で述べられているように，Pinsker の不等式 (2.21) から汎用的安全性基準は相互情報量基準よりも弱い安全性基準となっている．

[*1] その具体的な構成法については第 5 章で論ずる．

以上の汎用的安全性基準に対して，次の定理 [132] が成り立つ．

定理 2.4.2（汎用的安全性基準に対する上界） 任意の関数 $\varphi_n^Y : \mathcal{Y}^n \to \mathcal{M}_n$ に対し $M_n = \varphi_n^Y(Y^n)$ とし，ユニバーサル 2 ハッシュ関数族 F_n からランダムに選んだ関数 F_n に対して $K_B = F_n(Y^n)$ とすると，汎用性安全基準に対して

$$d(P_{K_B F_n M_n Z^n}, P_{\mathrm{K,Unif}} P_{F_n M_n Z^n}) \le P_{YZ}^n(\mathcal{T}_{Y|Z}(\gamma)^c) + \frac{1}{2}\sqrt{\frac{|\mathcal{K}_n||\mathcal{M}_n|}{2^{\gamma^n}}} \tag{2.76}$$

が成り立つ．ここで，$\mathcal{T}_{Y|Z}(\gamma)$ は

$$\mathcal{T}_{Y|Z}(\gamma) = \left\{(\mathbf{y},\mathbf{z}) : \frac{1}{n}\log\frac{1}{P_{Y^n|Z^n}(\mathbf{y}|\mathbf{z})} \ge \gamma\right\} \tag{2.77}$$

である． □

式 (2.76) は安全性基準に対する上界ではあるが，情報整合と秘匿性増強のプロセスで公開される情報を区別した上界となっている．しかも，その右辺は Slepian-Wolf 符号の符号器 φ_n とユニバーサル 2 ハッシュ関数 f_n の具体的な関数型には依存せず，それら値域のサイズ $|\mathcal{M}_n|$，$|\mathcal{K}_n|$ のみに依存している．従って，秘匿性増強と情報整合に用いる関数を独立に設計しても成立する上界となっている．現在の QKD を含む秘密鍵共有における安全性の議論の多くは，秘匿性増強と情報整合とを分離可能な状況における議論となっている [135, 136, 137, 138, 139, 140, 141]．

式 (2.76) の第 1 項は，$\gamma = H(X|Y) - \delta$ と置くと，十分長い符号長 n に対して 0 に収束することが示せる．また，式 (2.76) の第 2 項については

$$\frac{1}{n}\log|\mathcal{K}_n| = H(X|Z) - 2\delta - \frac{1}{n}\log|\mathcal{V}_n| \tag{2.78}$$

と設定することにより，十分長い不等長 n に対して 0 に収束することが示せるため，汎用的安全性基準を満たすことを示せる．

注意 2.4.2 ここでは汎用的安全性基準による上界について議論を行ったが，ユニバーサル 2 ハッシュ関数による秘匿性増強を前提とした相互情報量基準に対する上界は Hayashi によって導出されている [73, Section V]．ただし，Hayashi の上界はユニバーサル 2 ハッシュ関数を元に構成されたワイヤタップ通信路符号を使って秘密鍵共有を行うものであり，情報整合と秘匿性増強を分離して設計する目的にはそぐわない．そのため，本研究では取り上げなかった． □

注意 2.4.3 Pinsker の不等式 (2.21) は Kullback-Leibler 情報量の変動距離による下限を与えたが，同様に

$$\begin{aligned} &D(P_{K M_n Z^n}||P_{\mathrm{K,Unif}} \times P_{M_n,Z^n}) \\ &\quad \le 2d(P_{K F_n M_n Z^n}, P_{\mathrm{K,Unif}} P_{F_n M_n Z^n}) \log\frac{|\mathcal{K}|}{d(P_{K F_n M_n Z^n}, P_{\mathrm{K,Unif}} P_{F_n M_n Z^n})} \end{aligned} \tag{2.79}$$

なる上界が成り立つことが知られている [142]．この上界を用いることで，n に対する収束の速度は遅くなるが，定理 2.4.2 を強安全性基準についても示すことができる．

秘密鍵レート

最後に，情報整合と秘匿性増強を分離した場合の秘密鍵レートについて議論する．鍵が一致しない確率 (2.66) は Slepian-Wolf の符号化における復号失敗確率 (2.72) に上から抑えられ，安全性基準は汎用性安全基準 (2.75) によって計量される．

Slepian-Wolf の定理 (定理 2.4.1) から，$H(X|Y) \leq \frac{1}{n}\log|\mathcal{M}_n|$ ならば，Slepian-Wolf の復号失敗確率は $n \to \infty$ で 0 に漸近する．これと式 (2.78) から，

$$\begin{aligned}\frac{1}{n}\log|\mathcal{K}_n| &= H(X|Z) - 2\delta - \frac{1}{n}\log|\mathcal{M}_n| \\ &\geq H(X|Z) - H(X|Y)\end{aligned} \tag{2.80}$$

とすれば，汎用性安全性基準も $n \to \infty$ で 0 に漸近する．以上より，達成可能な秘密鍵レート $R_K = \frac{1}{n}\log|\mathcal{K}_n|$ について，以下の定理が成り立つ．

定理 2.4.3　秘密鍵レート R_K について，

$$R_K \leq H(X|Z) - H(X|Y) \tag{2.81}$$

ならば，その秘密鍵レートは達成可能である．　□

節 2.2.1 の相互情報量の性質 1. から，$H(X|Z) - H(X|Y) = I(X;Y) - I(Y;Z)$ が成り立つことに注意する．これは式 (2.70) に示した秘密鍵レートの下界と等しい．

第 3 章

光通信におけるワイヤタップ通信路符号化実現に向けた理論的検討

前章では，物理レイヤ暗号の情報理論的な定式化を通して，その性能を評価するための公式を導入した．しかし，それらは物理的背景を仮定しない数学的な公式にすぎず，様々な物理的制約下での物理レイヤ暗号の実行可能性を保証するものでは無かった．実際の通信システムの設計には，物理的背景を持つ通信モデルを設定した上での物理レイヤ暗号の性能評価及び実現可能性の検討を具体的に行う必要がある．本章では，典型的な光通信方式について物理モデルを設定し，その上で光空間通信における物理レイヤ暗号の実現可能性について議論をする．なお，ここでは，秘匿容量が完全に判明しており，数学的な取扱が容易なワイヤタップ通信路符号化をその考察の対象とする．

情報理論における光通信の取扱には大別して 2 つのモデルが存在する．一つは検出器のノイズ x が分散 σ^2 の正規分布

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{3.1}$$

に従うとする Gauss 通信路による取扱である．主通信路と盗聴者通信路の双方が Gauss 通信路である場合のワイヤタップ通信路の秘匿容量は Leung-Yan-Cheong と Hellman[143] によって知られている．

もう一つのモデルは，Poisson 確率分布に従ってオン-オフの二値判定を行う単一光子検出器を使うモデルである．ここで，単一光子検出器は光子数識別まではできないものの，理想的に無限の帯域を持ち，二値判定した系列から入力された光波形を完全に再現できるとする．このモデルを Poisson 通信路と呼ぶ．

Poisson 通信路の定式化ははじめに 1 対 1 通信路において Wyner[144] により行われ，通信路容量と誤り指数が導出された．その後，主通信路と盗聴者通信路の両者が (劣悪性の条件を満足する)Poisson 通信路である場合の秘匿容量が Laourine と Wagner[145] によって導出された．しかし，これらの研究については，下記の問題点が指摘できる．

1. Wyner は誤り指数導出の際に Gallager が導出した入力に制約が課されている場合

の指数 [77] を利用したが，Gallager の証明には本論で指摘するように誤りが存在するため，結果として Wyner の導出にも前提と証明結果の間に矛盾が存在する．

2. 無限の帯域を持つ単一光子検出器は現状の技術の視点から見てもあまりに理想化しすぎている条件である．そのため，時間分解能が有限である場合の定式化を行うべきである．
3. Laourine らの研究では秘匿容量が導出されたものの，有限長解析の定式化 (すなわち，秘匿性指数の導出) は行われていない．

本章では，上記の各問題点を踏まえた上で，衛星-地上局間通信などで典型的な単一光子検出器を用いたオン－オフ変調方式について，ワイヤタップ通信路符号化の性能評価を行う．しかし，第 2 章におけるワイヤタップ通信路符号化の定式化では，物理的背景を持つ通信システムの解析に不可欠である，入力への制約が取り扱われていない．そのため，はじめに入力に制約が課されているワイヤタップ通信路の再定式化を行う．その過程において，Han, Endo, Sasaki [79] と同様の手法で誤り指数や秘匿性指数の再導出も行うが，これらは Gallager が過去に導出し，これまで情報理論において伝統的に用いられていた指数に内在する証明の誤りを修正した上で，さらに最適化のためのパラメータを増やしたより一般的な指数となっている．本論では Han らの指数について，指数の性質の証明や，Gallager の指数との解析的な比較など，Han らが証明しなかった事項を取り扱う．

次に，時間分解能を有限とした上で単一光子検出器を用いたオン-オフ変調の定式化を行う．そして，秘匿容量の数値計算を行い，イブの能力に仮定を課さない極限である QKD との性能比較を行う．加えて，誤り指数と秘匿性指数から復号誤り確率と漏えい情報量の符号長依存性を計算し，現状の計算機や素子で処理可能な長さ符号での，ワイヤタップ通信路符号の実現可能性について議論を行う．

3.1　入力への制約の導入

第 2 章で導入したワイヤタップ通信路では，入力確率分布を自由に最適化することで秘匿容量を最大化できた．しかし，現実の通信では，入力には実験装置の要請などにより，制約が課されている場合が多い．例えば，光通信の場合には，光源が出力可能な電力という制限が存在する．従って，物理的背景を持つ通信モデルの評価のためには，入力への制約を取り入れた形でワイヤタップ通信路の定式化を行う必要がある．

3.1.1　コスト制約

長さ n の任意の入力変数 X^n に対して，コスト関数 $c_n : \mathcal{X}^n \to \boldsymbol{R}^+ = [0, \infty)$ を定義する．そして，シンボル毎のコスト関数の値が非負の実数 Γ 以下になる入力系列 $\mathbf{x}$ の集合を

$$\mathcal{X}^n(\Gamma) \stackrel{\triangle}{=} \left\{ \mathbf{x} \in \mathcal{X}^n \left| \frac{1}{n} c_n(\mathbf{x}) \leq \Gamma \right. \right\} \tag{3.2}$$

と定義する．そして，あるメッセージ $i \in \mathcal{M}_n$ の符号器の出力 $\varphi_n^A(i)$ に対して，次のような制約を課す．

$$\Pr\{\varphi_n^A(i) \in \mathcal{X}^n(\Gamma)\} = 1 \quad \text{for all} \quad i \in \mathcal{M}_n \tag{3.3}$$

この制約 (3.3) をコスト制約 Γ と呼ぶ．また，このようなコスト制約 Γ が課されているワイヤタップ通信路 (W_B^n, W_E^n) を，単純にコスト制約付きワイヤタップ通信路 (W_B^n, W_E^n) と呼ぶ．

ここで，コスト関数 c_n は，ある 0,1 からなる系列をパルスなどの信号に符号化する際に消費する電力と捉えることができる．対して，Γ はそれらの平均値に対する制約，すなわち光源が出力可能なパワーとして解釈できる．

3.1.2 誤り指数と秘匿性指数

コスト制約付きワイヤタップ通信路 (W_B^n, W_E^n) が与えられた場合，復号誤り確率 ε_n^B 及び漏えい情報量 δ_n^E の上界について次の定理が成立することが Han, Endo, Sasaki[79, Theorem 3.1] によって示されている．

定理 3.1.1（コスト制約付きワイヤタップ通信路の ε_n^B と δ_n^E の上界） コスト制約 Γ 付きワイヤタップ通信路 (W_B^n, W_E^n) と任意の正定数 M_n, L_n が与えられたとき，$\mathcal{V}^n$ 上の確率分布 P_{V^n} に従う確率変数 V^n が入力である補助通信路 $P_{X^n|V^n}$ の出力 X^n が，

$$\Pr\{X^n \in \mathcal{X}^n(\Gamma)\} = 1 \tag{3.4}$$

を満足すると仮定した場合にも，定理 2.3.1 の上界は成立する． □

この上界を大きい n に対して現実的に計算可能な形，すなわち誤り指数と秘匿性指数に書き直すため，前章にて定理 2.3.1 から定理 2.3.2 を導く過程で行ったように，情報源及び通信路の定常無記憶性を仮定する．加えて，$c_n(\mathbf{x}) = \sum_{i=1}^n c(x_i)$ を満足する加法的コスト関数 $c : \mathcal{X} \to \boldsymbol{R}^+$ を考察の対象にする．すると，コスト制約 (3.4) を満足する入力変数 X^n は，入力確率分布 P_X に対する制約

$$\sum_{x \in \mathcal{X}} c(x) P_X(x) \le \Gamma, \tag{3.5}$$

を満足する入力確率分布 P_X によって生成されることが直ちに分かる．

Gallger[77] はコスト制約付きの誤り指数の導出の際にこの制約 (3.5) のみを考慮したが，連接ワイヤタップ通信路では補助通信路への入力確率分布 P_V に対して，P_X に対する制約と等価な制約を導入できる．実際に，$\mathcal{V}$ 上に値を取るシンボル v に対して加法的コスト関数 $\bar{c} : \mathcal{V} \to \boldsymbol{R}^+$ を

$$\bar{c}(v) \stackrel{\triangle}{=} \sum_{x \in \mathcal{X}} c(x) P_{X|V}(x|v) \tag{3.6}$$

と定義すると，

$$\sum_{x\in\mathcal{X}} c(x)P_X(x) = \sum_{v\in\mathcal{V}} \bar{c}(v)P_V(v) \tag{3.7}$$

なる等式が成り立ち，入力確率分布 P_X に対するコスト制約 (3.5) は

$$\sum_{v\in\mathcal{V}} \bar{c}(v)P_V(v) \le \Gamma \tag{3.8}$$

と書き直される．以降，この章を通して，P_X に対する制約 (3.5) を X- 制約 Γ と呼び，P_V に対する制約 (3.8) を V- 制約 Γ と呼ぶ．

以上のような加法的コスト関数を導入することで，コスト制約付きの定常無記憶ワイヤタップ通信路 (W_B, W_E) についても誤り指数と秘匿性指数を導出できる．X- 制約付きの誤り指数は Gallager によって，イブに対するセキュリティは考慮しない，1 対 1 のコスト制約付き通信路符号化問題の解析において導入された [77, Eq. (7.3.20)]．しかしながら，Han ら [79, Remark 3.5] によって指摘されているように，また，本論文でも後ほど議論されるように，Gallager が導出した指数は，いくつかの通信路モデルに対して物理的な解釈が不可能な評価を与えるという問題を孕んでいた．Han, Endo, Sasaki はその問題を回避して，より多くの通信路モデルに対して評価が可能になるように，Gallager とは異なる手法を用いて，誤り指数と秘匿性指数のコスト制約付きでの表現を導出した [79, Eqs. (59) と (60)]．さらに，その表現は X- 制約 (3.5) のみならず，V- 制約 (3.8) の両者を取り入れており，より一般的な表現となっている．

定理 3.1.2（コスト制約付きワイヤタップ通信路の誤り指数と秘匿指数）　コスト制約 Γ 付きの定常無記憶ワイヤタップ通信路 (W_B, W_E) と X- 制約 (3.5) と V- 制約 (3.8) をそれぞれ満足する入力確率分布 P_X と P_V，そして任意の符号化レート R_B とランダムねスレート R_E が与えられたとき，誤り指数 $F_c(P_V, R_B, R_E, n)$ と秘匿性指数 $H_c(P_V, R_E, n)$ を

$$F_c(P_V, R_B, R_E, n) \stackrel{\triangle}{=} \sup_{r\ge 0, s\ge 0} \sup_{0\le\rho\le 1} [\phi(\rho|W_B, P_V, r, s) - \rho(R_B + R_E) + \kappa_n] \tag{3.9}$$

$$H_c(P_V, R_E, n) \stackrel{\triangle}{=} \sup_{r\ge 0, s\ge 0} \sup_{0<\rho<1} [\phi(-\rho|W_E, P_V, r, s) + \rho R_E + \lambda_n] \tag{3.10}$$

と定義する．ここで，任意の定数 $1/2 < a < 1$ に対して $\kappa_n = O(n^{a-1})$ と $\lambda_n = O(n^{a-1})$[*1]であり，関数 $\phi(\rho|W, P_V, r, s)$ は

$$\begin{aligned}&\phi(\rho|W, P_V, r, s)\\ &\stackrel{\triangle}{=} -\log\left[\sum_{u\in\mathcal{U}}\left(\sum_{v\in\mathcal{V}} P_V(v)e^{s[\Gamma-\bar{c}(v)]}\left[\sum_{x\in\mathcal{X}} W(u|x)P_{X|V}(x|v)e^{(1+\rho)r[\Gamma-c(x)]}\right]^{\frac{1}{1+\rho}}\right)^{1+\rho}\right]\end{aligned} \tag{3.11}$$

[*1] この範囲にある $1/2 < a < 1$ は，符号長 n について指数的に減少する指数に対して，その影響を無視できる．

と定義される．但し，式中の u は，$W = W_B$ または $W = W_E$ に対して，y または z を指示する．

すると，その復号誤り確率 ε_n^B 及び漏えい情報量 δ_n^E が

$$\varepsilon_n^B \leq 2e^{-nF_c(P_V,R_B,R_E,n)} \tag{3.12}$$

$$\delta_n^E \leq 2e^{-nH_c(P_V,R_E,n)} \tag{3.13}$$

を満足するような符号 (φ_n^A, ψ_n^B) が存在する． □

証明: この定理は確かに [79, Eqs. (59) と (60)] にて述べられたが，証明は与えられていなかった．そこで，付録 A.1 に証明を付す． □

この定理の証明の核となる部分は，コスト制約が満足されている入力か否かを判定する指標関数 (A.11) 及び (A.12) に指数的な上界を与えた点である．これにより，コスト制約の条件 (3.4) が追加された場合においても，誤り指数と秘匿性指数の導出が可能となる．式 (3.11) 中の変数 s, r は，その指標関数の上界を最適化するために導入されている．

ここで，既存の X- 制約のみが課されている指数 (cf. [77] の (7.3.20) 式や，[79] の (45), (46) 式) と比較すると，指数 (3.9)，(3.10) は 2 つの制約に由来する 2 つのパラメータによって最適化が行われる．そのため，これらの指数一つの制約のみが課されている指数よりも強い評価を与えることが期待できる．以降，これらの指数 (3.9)，(3.10) を強化指数と呼ぶ．また，区別のために $s = 0$ あるいは $r = 0$ と固定した指数を X- 制約指数と V- 制約指数とそれぞれ呼ぶ．

既に述べたように，誤り指数と秘匿性指数には満足すべき性質 (補題 2.3.1 を参照) が存在している．これらの性質は，X- 制約のみが課されている場合には満足されることが [79, Lemma 3.1] にて示されたが，さらに V- 制約も課された強化指数については未解決であった．本研究では，強化指数に関しても同様の性質が成り立つことを証明した．

補題 3.1.1（強化指数の性質） X- 及び V- 制約が $I(V;Y) > 0$ 及び $I(V;Z) > 0$ に対して満たされているとする．すると，強化指数は下記の性質を持つ．

1. $R_B + R_E = I(V;Y)$ において，$F_c(P_V, R_B, R_E, \infty) = 0$ かつ連続である．
2. $R_E = I(V;Z)$ において，$H_c(P_V, R_E, \infty) = 0$ かつ連続である．
3. $R_B + R_E < I(V;Y)$ では $F_c(P_V, R_B, R_E, \infty)$ は $R_B + R_E$ の単調減少かつ正の凸関数であり，$R_B + R_E \geq I(V;Y)$ では $F_c(P_V, R_B, R_E, \infty) = 0$ となる．
4. $R_E > I(V;Z)$ では $H_c(P_V, R_E, \infty)$ は R_E の単調増加かつ正の凸関数であり，$R_E \leq I(V;Z)$ では $H_c(P_V, R_E, \infty) = 0$ となる．

□

証明: 証明は付録 A.2 に記す． □

なお，第 2 章にて補題 2.3.1 から定常無記憶ワイヤタップ通信路の秘匿容量の具体的表現 (定理 2.3.3) を導出したように，性質からコスト制約付きの定常無記憶ワイヤタップ通

信路の秘匿容量の具体的表現を導出することができる．

定理 3.1.3（コスト制約付きワイヤタップ通信路の秘匿容量）　コスト制約 Γ 付き定常無記憶ワイヤタップ通信路 (W_B, W_E) の秘匿容量は

$$C_{\mathrm{S}} = \max_{VX:\sum_x P_X(x)c(x)\leq\Gamma} [I(V;Y) - I(V;Z)] \tag{3.14}$$

である．ここで，最大化 $\max_{VX}$ は入力確率分布 P_V と補助通信路 $P_{X|V}$ に亘って，加法的コスト制約 $\sum_x P_X(x)c(x) \leq \Gamma$ が満足される範囲でなされる．□

注意 3.1.1　本論で行った定式化では，Han ら [79] に倣って，X 上の入力確率分布 P_X と同時に V 上の入力確率分布にも等価な制約を課していた．ここで，等価な制約であるとは，等式 (3.7) が成り立つことであり，すなわち $\sum_x P_X(x)c(x) \leq \Gamma$ が満足されれば $\sum_v \bar{c}(v)P_V(v) \leq \Gamma$ も同時に満足された．そのため，制約が 1 つだけ課されている場合と，等価な制約が課されている場合とにおいて，秘匿容量の値の変化は無い．□

注意 3.1.2　例として，主通信路と盗聴者通信路がいずれも 2 元対称通信路から成るコスト制約付きのワイヤタップ通信路について，秘匿容量を求める．主通信路と盗聴者通信路のビット反転確率をそれぞれ ϵ_y，ϵ_z(但し，$0 \leq \epsilon_y < \epsilon_z \leq 1/2$) とし，入力確率を $q = P_X(x = 1)$ とした場合の相互情報量の差は，式 (2.52) より

$$I(X;Y) - I(X;Z) = h_2(p + \epsilon_y - 2p\epsilon_y) - h_2(p + \epsilon_z - 2p\epsilon_z) - h_2(\epsilon_y) + h_2(\epsilon_z) \tag{3.15}$$

であった．

ここで，コスト関数 $c(x)$ とコスト制約 Γ が与えられた場合，このワイヤタップ通信路に関して最適な q^* は

$$q^* = \min\left[\frac{1}{2}, \frac{\Gamma - c(0)}{c(1) - c(0)}\right] \tag{3.16}$$

によって与えられる．すなわち，コスト制約なしの二元対称通信路からなるワイヤタップ通信路を最適化する確率 $(q = 1/2)$ よりも，加法的コスト制約 $qc(1) + (1-q)c(0) \leq \Gamma$ を等式で満足する入力する確率が小さいならば，それが最適な入力確率となる．□

3.1.3　制約の数による指数の振舞の数値的比較

強化指数と V- 制約及び X- 制約指数との比較のために，いくつかの数値計算を行った．なお，以下の数値計算において，変数 $(r,\ s,\ \rho)$ の最適化は数値的に行われている．

初めに，図 3.1 に，ビット反転確率が $W_B(0|1) = 0.05$, $W_B(1|0) = 0.15$ である非対称な主通信路 W_B と，ビット反転確率が $W_E(1|0) = 0.15$, $W_E(0|1) = 0.05$ であるやはり非対称な盗聴者通信路 W_E からなるワイヤタップ通信路 (W_B, W_E) に関して，3 種類 (強化指数，V- 制約指数，X- 制約指数) の指数を計算した結果を示す．なお，コスト関数とコ

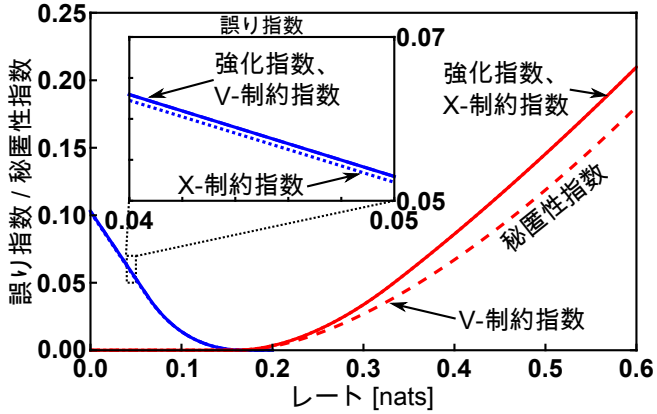

図 3.1　主通信路 $W_B(W_B(0|1) = 0.05,\ W_B(1|0) = 0.15)$ と盗聴者通信路 $W_E(W_E(1|0) = 0.15, W_E(0|1) = 0.05)$ から成る二元ワイヤタップ通信路 (W_B, W_E) の誤り指数と秘匿性指数．実線が強化指数，破線が V- 制約指数，点線が X- 制約指数を表す．ここで，コスト関数を $c(x) = x + 1$，コスト制約を $\Gamma = 1.4$ とした．また，入力確率 $P_V(v = 1) = 0.759$ と補助通信路の遷移確率 $P_{X|V}(0|1) = 0.21$ and $P_{X|V}(1|0) = 0$ は秘匿容量 $C_S = 9.61 \times 10^{-3}$ [nats] が達成されるように選ばれている．

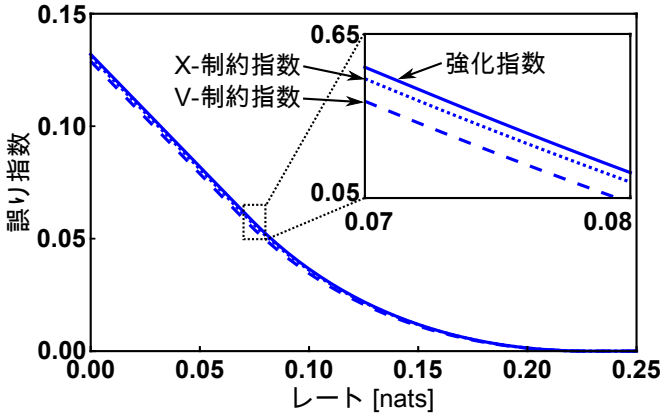

図 3.2　二元対称通信路 $W_B(W_B(0|1) = W_B(1|0) = 0.05)$ に対する誤り指数．ここで，コスト関数を $c(x) = x + 1$，$\Gamma = 1.98$ とした．また，入力確率 $P_V(v = 1) = 0.2$ と補助通信路の遷移確率 $P_{X|V}(0|1) = 0.21$ 及び $P_{X|V}(1|0) = 0$ は固定している．

スト制約をそれぞれ $c(x) = x + 1$，$\Gamma = 1.4$ と定め，その制約下で秘匿容量が与えられるように入力確率分布 P_V と補助通信路 $P_{X|V}$ を最適化している．

誤り指数に関しては，強化指数 (図中の実線) は V- 制約指数 (図中の破線) を上回るものの，X- 制約指数 (図中の点線) と等しくなっている．一方で，秘匿性指数に関して，強化指数は X- 制約指数を上回り，V- 指数と等しくなっている．以上より，2 つの入力に対して等価な制約が課されている強化指数は，必ずしも 1 つのコスト制約のみが課されている V- 制約指数及び X- 制約指数よりも真にタイトな指数となっているわけではないことが分かる．

一方で，入力確率や通信路の選び方によっては，強化指数がその他の指数よりも真に大きい値をとる場合も存在している．図 3.2 は，ビット反転確率が $W_B(0|1) = W_B(1|0) = 0.05$ である二元対称通信路 W_B について，強化指数と V- 制約及び X- 制約指数を計算した結果である．ここでは，コスト関数とコスト制約をそれぞれ $c(x) = x + 1$，$\Gamma = 1.98$ とした．図 3.1 とは異なり，通信路容量の達成は要求せずに，入力確率分布 P_V と補助通信路 $P_{X|V}$ を固定し，計算を行っている．

以上の条件では，強化指数の値がその他の指数を厳密に上回っている．ここでは誤り指数のみを示したが，秘匿性指数 (3.10) についても同様の例を示すことができる．以上より，入力確率分布や通信路の条件によっては，強化指数は，X- 及び V- 指数よりも真に強い評価を与えると結論できる．すなわち，Han ら [79] 及び本論で行ったような 2 つの入力変数に対して等価な制約を課すという方法は，情報理論的に無意味な操作では無いことが示された．

3.1.4　Gallager の指数との比較

既に述べたように，Han ら [79] が Gallager とは異なる方法で定理 3.1.2 に示す指数を導入した理由は，Gallager が示した指数 [77] では正しい評価が行われない通信路モデルが存在したためであった．一方で，両方の指数が機能する通信路モデルについて，Han らによる指数と Gallager による指数を比較することには十分に意味がある．そのため，この節では，上記の比較を数値計算によって行う．

はじめに，Gallager の手法に基づく指数を導入する．なお，Gallager が指数を導出した当時の興味の対象はワイヤタップ通信路ではなく，1 対 1 の通信路符号化問題であったため，これ以降，連接通信路無し (すなわち，$V \equiv X$) の特殊例のみを考察の対象とする．そのため，関数 $\phi(\rho|W, P_V, r, s)$ を下記の関数に置き換える．

$$\phi_H(\rho|W, P_X, r) = -\log \left[\sum_{u\in\mathcal{U}} \left(\sum_{x\in\mathcal{X}} P_X(x) W(u|x)^{\frac{1}{1+\rho}} e^{r[\Gamma - c(x)]} \right)^{1+\rho} \right] \tag{3.17}$$

ここで，u は $W = W_B$ または $W = W_E$ に対応して，y または z を表すとする．この関数 $\phi_H(\rho|W, P_X, r)$ に基づく指数を HES 型の指数と呼ぶ．

Gallager の方法と Han らの方法の大きな違いは入力系列がコスト制約を満足しているか否かを判定する指標関数の上界の与え方にある．Gallager は指標関数とその上界を，定理 3.1.2 の証明における指標関数 (A.1) の代わりに

$$\chi_G(\mathbf{x}) = \begin{cases} 1 & \text{for } n\Gamma - \delta \le \sum_{i=1}^{n} c(x_i) \le n\Gamma \\ 0 & \text{otherwise} \end{cases} \tag{3.18}$$

$$\chi_G(\mathbf{x}) \le \exp\left[(1+\rho) r \left(\sum_{i=1}^{n} c(x_i) - n\Gamma + \delta \right) \right] \tag{3.19}$$

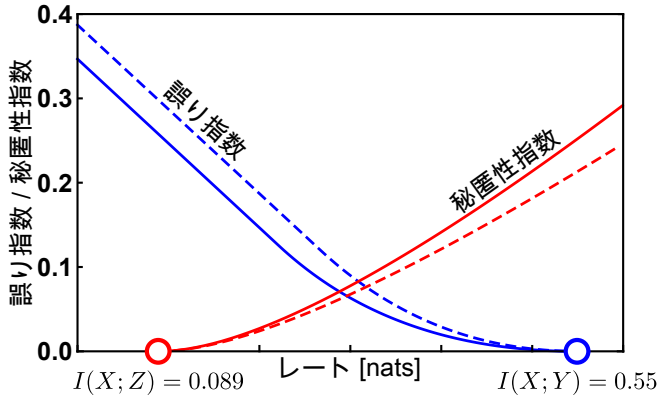

図 3.3　ガウスワイヤタップ通信路に関する HES 型指数 (実線) と G 型指数 (破線).
$A_y = 1$, $\sigma_y = 0.5$, $A_z = 0.5$, $\sigma_z = 0.8$, $\Gamma = 0.5$ として計算を行った.

と与えた [77, Eqs. (7.3.14) and (7.3.18)]. ここで, $\delta > 0$ は任意に小さい定数である. すなわち, 指標関数 $\chi_G(\mathbf{x})$ は X- 制約を等式で満足している入力系列のみが, X- 制約をほぼ等式で満足していると判定される.

この指標関数の上界を利用することで, 以下の関数を得る [77, Eq. (7.3.20)].

$$\phi_G(\rho|W_B, P_X, r) = -\log\left[\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} P_X(x)W_B(y|x)^{\frac{1}{1+\rho}} e^{-r[\Gamma - c(x)]}\right)^{1+\rho}\right] \tag{3.20}$$

この関数 $\phi_G(\rho|W, P_X, r)$ と式 (3.17) に記した関数 $\phi_H(\rho|W, P_X, r)$ の差は, 最適化すべき変数 r の符号の違いにすぎない (すなわち, $\phi_G(\rho|W, P_X, r) = \phi_H(\rho|W, P_X, -r)$). 以降, Gallager の関数 $\phi_G(\rho|W, P_X, r)$ に基づく指数を G 型の指数と呼ぶ.

注意 3.1.3　Gallager が導出した関数 $\phi_G(-\rho|W_E, P_X, r)$ に基づく秘匿性指数は, はじめ [79, Eq. (203)] に証明無しで導入された. しかし, その証明は, Gallager の誤り指数の証明において ρ を $-\rho$ と置き換えることによって容易に行われる. □

HES 型と G 型の指数を比較するために, いくつかの通信路について数値計算を行う. 初めに, 離散時間定常無記憶ガウスワイヤタップ通信路の各指数を示す. この通信路に関する計算と指数の比較は Han ら [79, Section 9] によって行われているが, 後に BSC での結果との比較のためにここで再び行う.

ガウス通信路は, 既に述べたように, 入力信号に対して正規分布 (3.1) に従う検出器のノイズが重畳されるような通信路のモデルである. 与えられた入力 X に対して通信路 W_B, W_E の出力は $Y = A_yX + N_y$, $Z = A_zX + N_z$ と表される. ここで, $A_y > 0$, $A_z > 0$ は通信路のゲインあるいは減衰を表し, N_y と N_z は分散がそれぞれ σ_y^2 及び σ_z^2 である正規分布に従う確率分布である. 加法的コスト関数は $c(x) = x^2$ と定義される. ガウスワイヤタップ通信路の場合, 最適な入力 P_X はコスト制約を常に等式で満足することが知られている [143]. これは, 与えられたパワーを全て使い切る戦略が, 信頼性のある通

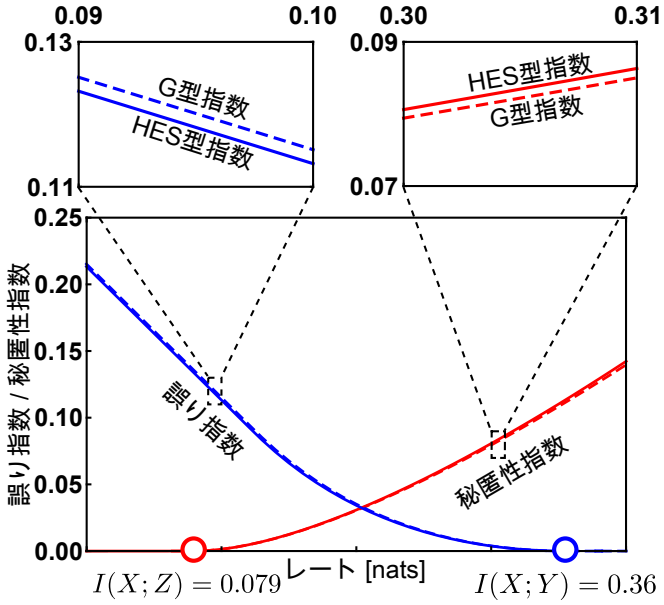

図 3.4　主通信路と盗聴者通信路のビット反転確率をそれぞれ $\epsilon_y = 0.1$, $\epsilon_z = 0.3$ であるワイヤタップ通信路のの HES 型指数 (実線) と G 型指数 (破線)．ここで，コスト関数を $c(x) = x + 1$，制約を $\Gamma = 1.4$ と定めている．

信を行う上だけでなく，秘匿性のある通信を行う上でも最適であることを意味している．

図 3.3 にガウスワイヤタップ通信路に対して計算した HES 型と G 型の指数を示す[*2]．Han らが指摘したように [79]，G 型の誤り指数は HES 型の誤り指数よりも大きく，対して秘匿性指数については HES 型の指数が G 型の指数よりも大きくなっている．この振る舞いは，最適化パラメータ r の符号の違いに起因する．HES 型の誤り指数の場合には，$r \leq 0$ の領域にある r が指数を最適化するが，r の定義されている範囲の外にあるため，$r = 0$ によって最適化される．一方で，G 型の誤り指数は $r \geq 0$ で最適化される．秘匿指数についても同様である[*3]．

次に，図 3.4 に，主通信路と盗聴者通信路がそれぞれ BSC から構成されているワイヤタップ通信路について，HES 型と G 型の指数の数値計算を行った結果を示す．ここで，主通信路と盗聴者通信路のビット反転確率をそれぞれ $\epsilon_y = 0.1$, $\epsilon_z = 0.3$ とした．また，コスト関数を $c(x) = x + 1$，制約を $\Gamma = 1.4$ と定めたため，注意 3.1.2 内の式 (3.16) から，$q^* = 0.4$ が最適な入力となる．この入力は X- 制約を等式で満足する，すなわちコスト制約の境界上に位置する．

図中の拡大図で示すように，誤り指数については G 型指数が HES 型の指数を若干上回り，秘匿性指数については HES 型指数が G 型の指数より若干大きい値をとる．すなわち，ガウス通信路の場合と同様の関係が成立する．なお，この関係は通信路と入力に依存

[*2] G 型の誤り指数は Gallager[77] によって得られた．一方で，HES 型の指数と G 型の誤り指数は Han らによって得られた [79, Theorem. 9.1, 9.3, 9.4].

[*3] 詳しい証明は付録 A.4 に示す．

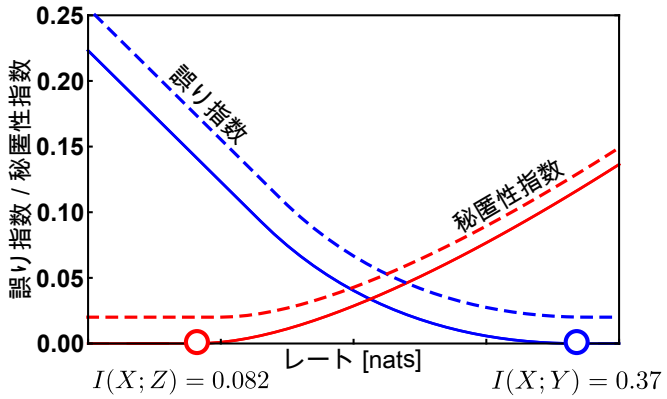

図 3.5　図 3.4 のワイヤタップ通信路について，$\Gamma = 1.6$ とした場合の HES 型指数 (実線) と G 型指数 (破線).

し，この関係が逆転するような入力も構成することができる．

3.1.5　Gallager の手法に内在する問題点について

ここでは，Gallager の手法によって導出された G 型の指数に内在する問題点について指摘する．Gallager の定式化では，指標関数 (3.18) の定義にも現れているように，X- 制約が等式で満足される入力確率分布のみが評価の対象となった．一方で，HES 型指数の証明で用いられた指標関数 (A.1) は X- 制約を満足しさえすれば 1 となるため，HES 型指数は G 型指数よりも広い入力確率分布をその評価の対象とすることができる．実際に，次の定理が成立する．

定理 3.1.4（G 型指数に内在する問題点）　コスト制約 Γ 付きの定常無記憶ワイヤタップ通信路 (W_B, W_E) について，X- 制約が厳密な不等式で満足されていると仮定する．すると，G 型の指数は任意のレート (R_B, R_E) に対して非零の正値関数となる．　□

注意 3.1.4　定理 3.1.4 の含意は，G 型指数が定理 3.1.1 で述べた基本的性質を満足しておらず，任意のレート (R_B,R_E) に対して十分に長い符号長で誤り確率 ε_n^B と漏えい情報量 δ_n^E の両者を十分に小さくできる符号が存在するといった，物理的に実現不可能な評価を行うという主張にある．　□

証明: 証明は付録 A.5 に示す．　□

この定理の主張が成立する例として，図 3.5 に，図 3.4 の計算を $\Gamma = 1.6$ で行った場合の各指数を示す．この場合，注意 3.1.2 内の式 (3.16) から最適な入力確率 $q^* = 1/2$ となり，X- 制約は厳密な不等式で満足される．実際に，G 型の指数は任意のレート $R_B \geq 0, R_E \geq 0$ に対して非零かつ正の値を示し，誤り及び秘匿性指数が持つべき基本的性質 (定理 3.1.1 の 1 及び 2) が破られている．ゆえに，注意 3.1.4 でも述べたように，G 型の指数による評価は，任意の符号化レートでも十分に長い符号長で信頼性と秘匿性

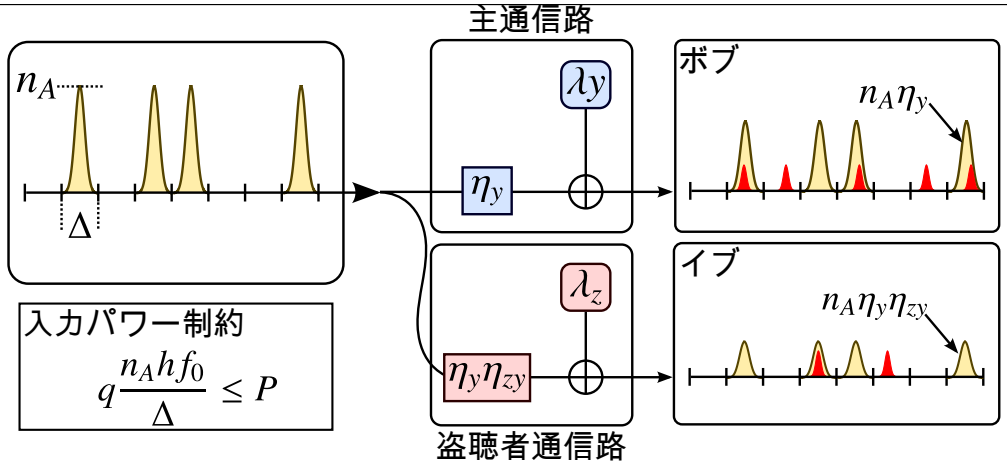

図 3.6　光パルスによる一方向秘匿メッセージ伝送.

を両立させる符号が存在するという，物理的に意味を成さず，漸近的な解析とも一致しない通信路評価となっている．一方で，HES 型の誤り指数と秘匿性指数は，それぞれ $R_B + R_E \ge I(X;Y)$ と $R_E \le I(X;Z)$ で 0 となり，定理 3.1.1 の 1 及び 2 を満足している．

実際に，Gallager は自身の方法に内在するこのような問題について認識しており，それを回避するために入力確率分布が X- 制約を等式で満足する場合には $r = 0$ になるというタイブレークルールを用いていた．この場合には，コスト制約付きの誤り指数は，コスト制約付きではない誤り指数に帰着される．しかし，そのようなルールの導入は，G 型の指数がコスト制約付きワイヤタップ通信路の性能評価に関する統一的手法として成立していないことを意味する．

上記の議論は，離散無記憶通信路に対しては，一般的に成立する．このような 2 つの指数間の性質の違いが顕著に現れた例として，Wyner によって提唱された Poisson 通信路 [144] が挙げられる．Wyner は入力確率分布に対してコスト制約 $P_X(x = 1) = q \le \Gamma$ を課した上で，G 型誤り指数を導出した．しかし，実際に導出された指数は，定理 3.1.4 に述べたように $q = \Gamma$ でのみ有効であり，与えられたパワー制約下で入力確率を最適化を許した自身の問題設定と矛盾する [144, (1.5c)]．Han，Endo，Sasaki [79, Section VI] は HES 型指数を利用することでこの問題を回避し，Poisson ワイヤタップ通信路における誤り指数と秘匿性指数を，証明上の矛盾を発生させることなく導出している．

3.2　オン-オフ変調のモデル化

以降では, 図 3.6 に示すような, 光パルスのオン-オフによって情報を伝送するモデルを考察する．アリスは確率 $\Pr(x = 1) = q$ でシンボル $x = 1$ を，また，確率 $\Pr(x = 0) = 1 - q$ でシンボル $x = 0$ を，時間間隔 Δ 秒で生成する．そして，オン信号 $x = 1$ に対応する時間スロットでは，幅 Δ_{p} 秒で平均光子数 n_A 個のパルスを伝送し，オフ信号 $x = 0$ に対応する時間スロットでは真空パルスを伝送する．特に，アリスが使用可能なレーザーパワー

は P W に制限されていると仮定する．

アリス-ボブ間の主通信路 W_B とアリス-イブ間の盗聴者通信路は，それぞれ大気伝搬による損失や，検出器の量子効率，レンズの大きさといった幾何学的な要素を全て含んだ損失を表すパラメータである通信路透過率 η_y，η_z によって特徴づけられる．このパラメータにより，ボブとイブが受信するパルスの平均光子数は，それぞれ $n_B = \eta_y n_A$，$n_E = \eta_z n_A$ と表される．特に，ボブとイブが受信可能なパワーを比較するために，比透過率 $\eta_{zy} \equiv \eta_z/\eta_y$ を導入する．光空間通信における物理レイヤ暗号では，アリスとボブが回線をカメラによって監視しているため，イブはビームの主軸から離れた位置から盗聴を行わざるを得ない．そのため，この比透過率は 1 よりも小さいと仮定できる．なお，本論では，好条件において達成可能な性能の議論を行うため，フェーディングの効果が含まれていない通信について考察する．

ボブとイブは，それぞれ暗計数率 λ_y [counts/sec] (cps)，λ_z [cps] の光子検出器でパルスの受信，盗聴を行う．暗計数率は，アリスが送信するパルスとは無関係に，検出器が光に起因しない入力を増幅して誤計数を行う確率である．ボブとイブの検出器の時間分解能は有限であり，パルス生成レートと等しい Δ 秒であると仮定する．また，異なる時間スロット間へのパルスのクロストークを防ぐため，パルス幅は検出器の時間分解能より十分に小さい ($\Delta > \Delta_{\rm p}$) と仮定する．

このような物理的な問題設定に基いて一方向メッセージ伝送の性能評価を行うに当たって，以降の数小節に亘って数学的な定式化を行う．

3.2.1 パワー制約

アリスは使用可能な電力の範囲でスロット毎のパルス生成確率 q とパルスあたりの平均光子数 n_A を最適化する必要がある．そのため，与えられたパワー P と，q 及び n_A の関係を最適化する必要がある．

本論では，搬送波の周波数を $f_0 = 200$ THz (波長 1.5 μm 相当) と仮定する．また，整形されるパルスはフーリエ変換限界を満足しており，スペクトル幅 B Hz とパルス幅 $\Delta_{\rm p}$ の間に $B\Delta_{\rm p} = 1$ が成立しているとする．パルス幅 $\Delta_{\rm p}$ が検出器の時間分解能 Δ よりも十分に小さいとする仮定から，B の値は検出器の時間分解能の逆数 Δ^{-1} より十分に大きい．そして，簡単のため，伝送パルスにおける周波数毎の平均光子数の分布 $\bar{n}(f)$ は，スペクトル幅 B に亘って定数 n_A であるとする．

以上の仮定の元，伝送パルス当たりの電力は

$$P_{\rm p} = \int_{-\infty}^{\infty} \bar{n}(f) h f df \simeq \int_{f_0 - B/2}^{f_0 + B/2} n_A h f df = \frac{n_A h f_0}{\Delta_{\rm p}} \tag{3.21}$$

と与えられる．ここで h はプランクの定数である．そして，伝送において消費される平均パワーは

$$P_{\rm total} = q \frac{\Delta_{\rm p}}{\Delta} P_{\rm p} = q \frac{n_A h f_0}{\Delta}, \tag{3.22}$$

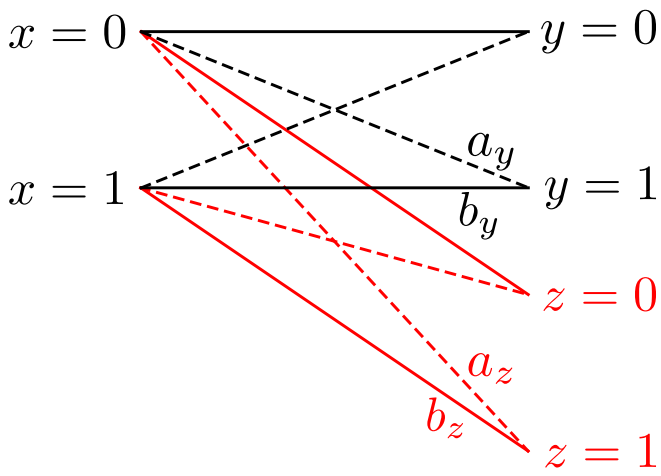

図 3.7　通信路遷移確率の概要図

と計算され，これが使用可能パワー P を超過することは禁止される．以上より，以下のパワー制約を得る．

$$q\frac{n_A h f_0}{\Delta} \leq P. \tag{3.23}$$

3.2.2　通信路の遷移確率

本章で扱う通信はパルスを入力して単一光子検出器で受信するため，図 3.7 に示す 2 元定常無記憶通信路に帰着できる．ここでは，このモデルに基いてアリス-ボブ間及びアリス-イブ間の通信路遷移確率を導出する．なお，Wyner[144] は帯域が無限である (すなわち $\Delta \to 0$) という極限において解析を行っている．一方で，本論ではより実用的な評価を目指して，検出器の時間分解能が有限の場合を扱う．

単一光子検出器が Poisson 確率に従って計測を行うと仮定すると，主通信路の W_B の遷移確率は下記の式で与えられる．

$$\begin{aligned} W_B(1|0) &= 1 - e^{-\lambda_y \Delta} \triangleq a_y \\ W_B(1|1) &= 1 - e^{-(\eta_y n_A + \lambda_y \Delta)} \equiv b_y \end{aligned}$$

ここで，$W_B(1|0) = a_y$ は暗計数による誤検出の確率，$W_B(1|1) = b_y$ はパルスを正確に検出する確率である．その他の遷移確率も，a_y と b_y から直ちに

$$\begin{aligned} W_B(0|0) &= 1 - a_y \\ W_B(0|1) &= 1 - b_y \end{aligned}$$

と計算される．同様に，盗聴者通信路 W_E の遷移確率も，下記の式で与えられる．

$$\begin{aligned}
W_E(1|0) &= 1 - e^{-\lambda_z \Delta} \equiv a_z \\
W_E(1|1) &= 1 - e^{-(\eta_z n_A + \lambda_z \Delta)} \equiv b_z \\
W_E(0|0) &= 1 - a_z \\
W_E(0|1) &= 1 - b_z
\end{aligned}$$

3.2.3 通信路容量と秘匿レート

以上のパワー制約と遷移確率が与えられると，通信路容量と秘匿容量の表現を導出できる．但し，ここでは補助通信路と補助変数を導入しない表式 (2.51) に基いて計算を行う．補助変数付きの秘匿容量については節 3.4.1 で考察する．

相互情報量 $I(X;Y)$ のエントロピーによる表現 (補題 2.2.2 の性質 1.) から，アリスとボブの相互情報量 $I(X;Y)$ は

$$f_B(q, n_A) \equiv h_2((1-q)a_y + q(1-b_y)) - (1-q)h_2(a_y) - qh_2(b_y), \tag{3.24}$$

と計算される．ここで h_2 は二元エントロピー (2.11) である．

通信路容量は相互情報量 $I(X;Y) = f_B(q, n_A)$ を最大化することで得られる．本論では入力確率 q のみならず，平均光子数 n_A も最適化可能なパラメータとして取り扱う．そのため，通信路容量 C は

$$C \equiv \max_{q, n_A} f_B(q, n_A) \tag{3.25}$$

と与えられる．

一方，アリスとイブの間の相互情報量 $I(X;Z)$ は

$$f_E(q, n_A) \equiv h_2((1-q)a_z + q(1-b_z)) - (1-q)h_2(a_z) - qh_2(b_z) \tag{3.26}$$

と与えられるため，秘匿容量は

$$f_{BE}(q, n_A) \equiv f_B(q, n_A) - f_E(q, n_A) \tag{3.27}$$

を最適化することで得られる．但し，本論で扱う計算例では more capable の条件を満足していない場合を扱う．この場合では，補助変数を導入しない限りは秘匿容量は得られない．そのため，本章を通して，補助変数と補助通信路無しで $f_{BE}(q, n_A)$ を最適化した量

$$R_{\mathrm{S}} \equiv \max_{q, n_A} f_{BE}(q, n_A) \tag{3.28}$$

を秘匿レート R_{S} と呼び，秘匿容量とは区別して考える．

3.3 秘匿レートの数値計算

この節では各種レート，即ち，通信路容量 (3.25) と秘匿レート (3.28) の評価を行う．但し，ガウス通信路や二元対称通信路のような通信路容量及び秘匿容量の公式が明らかに

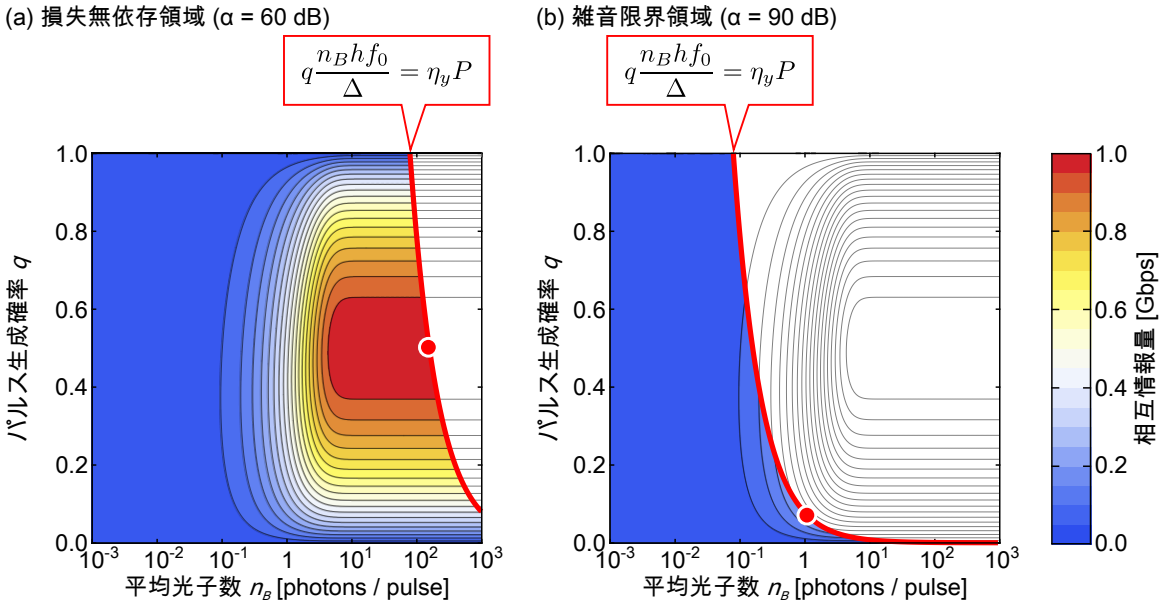

図 3.8 相互情報量 $f_B(q, n_A)$ の等高線図．(a) 損失無依存領域 ($\alpha = -\log_{10}\eta_y = 60$ dB)．(b) 雑音限界領域 ($\alpha = 90$ dB)．点は通信路容量を表し，実線はパワー制約を関数として描いた曲線である．計算のパラメータ： $P = 10$ mW, $\lambda_y = 10$ kcps, $\Delta = 1$ ns.

なっている特殊な通信路を除き，容量を得るためには数値計算を行う必要がある．本研究でも，その最適化を Mathematica により数値的に行った．

なお，この節を通して，$P = 10$mW，$\lambda_y = 10$kcps，$\lambda_z = 1$cps，$\Delta = 1$ns と固定する．時間分解能 Δ は 1GHz のパルス繰り返しレートに対応する．また，ボブの暗計数の値は既存の技術水準を考慮して決め，イブの暗計数の値はイブの検出器がボブの検出器よりもより高性能であると仮定して決定した．この場合には，ワイヤタップ通信路符号化における more capable の仮定はもはや成り立たない．

3.3.1 通信路容量

まず初めに，後に秘匿レート (3.28) の振る舞いと比較するために，通信路容量 (3.25) の数値計算を行い，その振る舞いについて検証する．

通信においてパルスが被る減衰を $\alpha = -\log_{10}\eta_y$ で定義すると，通信路容量の振る舞いは α の値によって大別して 2 つに変化する．1 つは減衰 α の値が小さく，受信光パルスが，光子検出器が確実に光子検出を行える程度には十分な強度を持つ場合である．この場合には，暗計数が主たる検出エラーの原因となる．もう 1 つは減衰 α の値が大きいために，受信光パルスの平均光子数が数光子以下のオーダーである場合である．この場合には，検出器のショットノイズもエラーの原因となる．

そのような減衰 α の値による振る舞いの違いを検証するために，図 3.8 にボブが受信するパルスの平均光子数 $n_B = \eta_y n_A$ とパルス生成レートの関数としての相互情報量

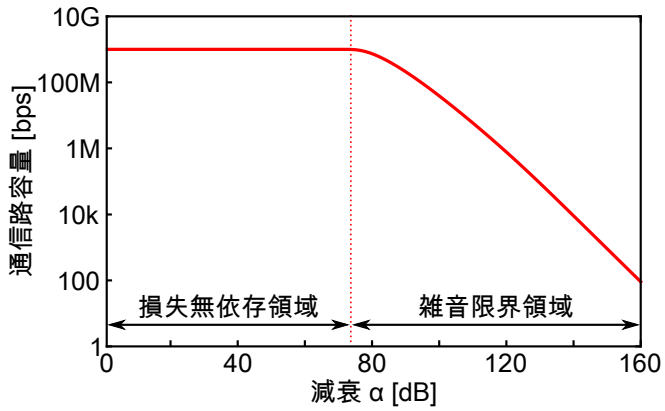

図 3.9　減衰 $\alpha = -\log_{10}\eta_y$ の関数としての通信路容量 C．パラメータ：$P = 10$ mW, $\lambda_y = 10$ kcps, $\Delta = 1$ ns.

$f_B(q, n_A)$ の等高線図を，(a) $\alpha = 60$dB と (b) $\alpha = 90$dB の場合について示す．図中の実線は，パワー制約 (3.23) を受信パルスの平均光子数 n_B で換算した場合の曲線であり，この曲線よりも左下の領域がパワー制約を満足するパラメータ領域に対応する．以降，この領域を伝送可能領域と呼び，パワー制約を表す曲線より右上の領域を伝送不可領域と呼ぶ．減衰 α が増加して受信可能な総エネルギー $\eta_y P$ が減少すると，パワー制約の曲線は左側に移動し，伝送可能領域は徐々に限られていく．通信路容量 C(図中の点) は，より信頼性の高い通信を行うために与えられたパワーを全てつぎ込むとすると，この領域上に存在する．

図 3.8(a) では，パワー制約を表す曲線は，相互情報量 $f_B(q, n_A)$ の等高線図の最大平面と交わっている．曲線が最大平面と交わっている限りは，通信路容量 C と最適なパルス生成レート q は α に無依存の定数となる．すなわち，前述の通り，ショットノイズの影響を受けない程度に十分なパワーで通信が行えていることを意味する．以上のような振る舞いを示す減衰 α の領域を，損失無依存領域とよぶ．

一方で，図 3.8(b) に示すように，パワー制約を表す曲線が相互情報量 $f_B(q, n_A)$ の最大平面を通り過ぎてしまうと，通信路容量は減衰 α の増加に連れて減少していく．図 (a) の損失無依存領域と比較すると，最適な q も減少していることが確認できる．この事実から，十分な信号間距離を確保するために，パルスの生成レートを犠牲にして受信パルスの平均光子数を数光子程度に確保することが最適な戦略であると解釈できる．以上のような振る舞いを示す減衰 α の領域を，雑音限界領域とよぶ．

図 3.9 に減衰 α の関数として描いた通信路容量 C のグラフを示す．損失無依存領域では C が一定であり，なおかつほぼエラーフリーに近い通信を実現できている．これは，損失無依存領域における主たる誤りの原因である暗計数の寄与が非常に小さいためであると考えられる．実際に，通信路の遷移確率 $W(1|0) = a_y$ を計算すると，10^{-4} 程度である．また，$\alpha = 70$dB 前後で雑音限界領域にさしかかると，C は減少に転じる．

図 3.10 に示す，通信路容量 C を与える最適な受信パルスの平均光子数 n_B^* からは，損

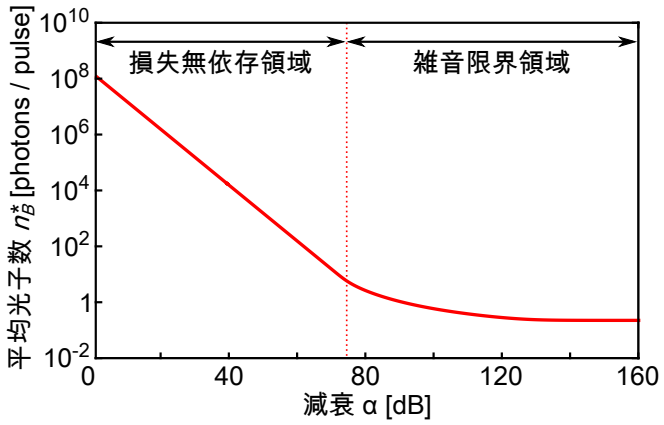

図 3.10　図 3.9 において通信路容量 C を与える受信パルスの平均光子数 n_B^*.

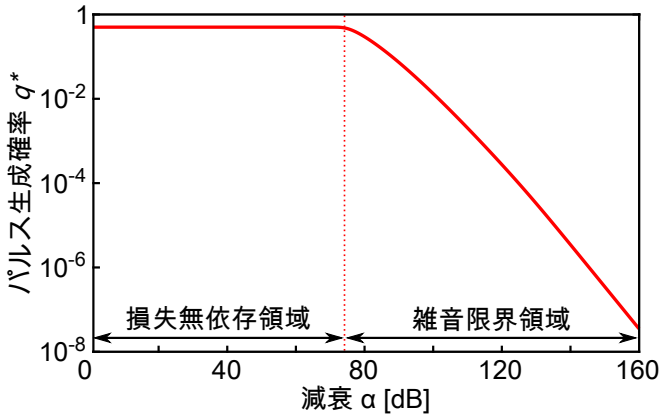

図 3.11　図 3.9 において通信路容量 C を与えるパルス生成確率 q_B^*.

失無依存領域では α の減少に応じて n_B^* が減少する一方で，雑音限界領域においてはほぼ一定になるという振る舞いを確認できる．

図 3.11 に示すように，通信路容量 C を与える最適な受信パルスの平均光子数 q^* は，損失無依存領域においては低エラーの通信が実現できているため，q^* の値は最も高いエントロピーを与える 0.5 に近い値となっている．その一方で，雑音限界領域に差し掛かると，n_B^* を一定に保つための犠牲となって，q^* は減少に転じることとなる．

3.3.2　秘匿レート

次に，ここでは秘匿レート R_S の計算を行いその振る舞いについて議論する．ここで，非透過率 η_{zy} は 0.95 とした．すなわち，イブが受信するパルス強度は，ボブが受信するそれの 95% に相当する．

図 3.12 に，通信路量量の C の解析でも行ったように，ボブが受信するパルスの平均光子数 $n_B = \eta_y n_A$ とパルス生成レートの関数としての相互情報量の差 $f_{BE}(q, n_A)$ の等高線図を示す．相互情報量 $f_B(q, n_A)$ のみを描いた図 3.12 とは異なり，$f_{BE}(q, n_A)$ の等高

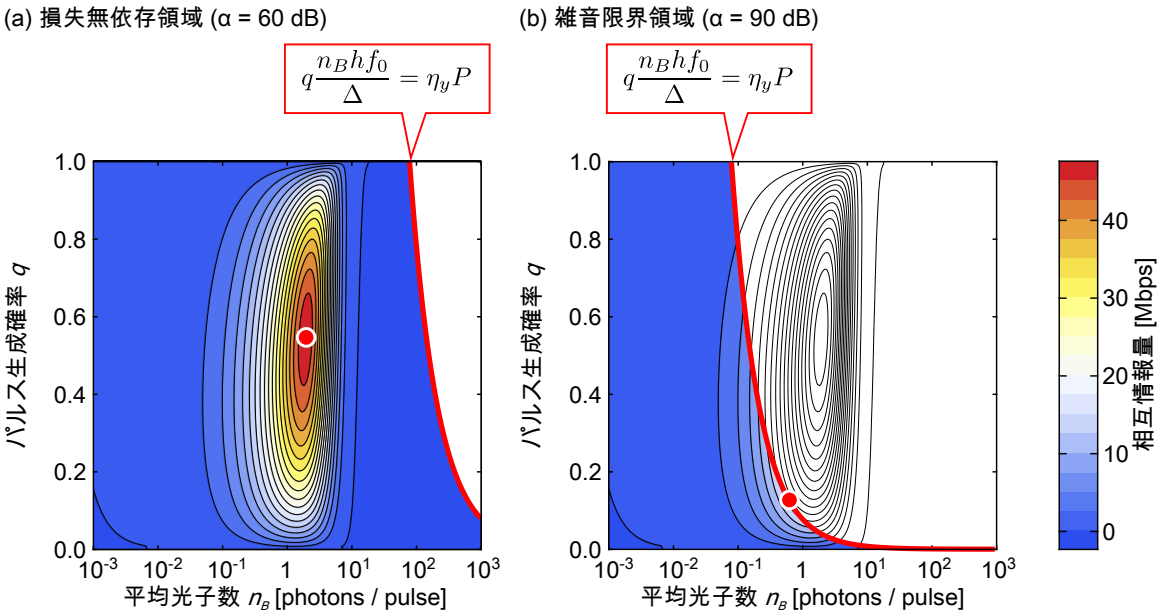

図 3.12　相互情報量の差 $f_{BE}(q, n_A)$ の等高線図．(a) 損失無依存領域 ($\alpha = -\log_{10}\eta_y = 60$ dB)．(b) 雑音限界領域 ($\alpha = 90$ dB)．図中の円は秘匿レートを表し，実線はパワー制約を関数として描いた曲線である．計算のパラメータ：$P = 10$ mW, $\eta_{zy} = 0.95$, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, $\Delta = 1$ ns.

線は n_B が大きい領域では急激に減少している．これは，イブが，ボブが受信するパルスの 95% の強度しか持たないパルスを受信するという不利な状況にあったとしても，イブの検出器がパルスを識別可能なほど強度の高いパルスが伝送された場合には，イブにも情報が漏洩するという現象を表している．さらに，イブがより低ノイズな検出器を利用していると仮定したため，イブがボブよりも多くの情報を得るようなパラメータ (n_B, q) も存在する．そのため，mora capable の条件は満足されず，相互情報量の差 $f_{BE}(q, n_A)$ は負になる．

図 3.12(a) は損失無依存領域に対応する等高線図である．通信路容量における図 3.8(a) とは異なり，$f_{BE}(q, n_A)$ の最大値 (図中の円)，すなわち秘匿レートはもはやコスト制約を表す曲線上には存在していない．換言すると，パラメータ (q^*, n_A^*) は与えられたパワー制約を，厳密な不等式

$$q^* \frac{n_A^* h f_0}{\Delta} < P, \tag{3.29}$$

で満足している．すなわち，盗聴を防ぐために，パワーを絞っていることに対応する．

図 3.12(b) に示す雑音限界領域における振る舞いは，通信路容量と同様である．秘匿レートはコスト制約を表す曲線が左方に移動するに連れて減少する．この場合には，パラメータ (q^*, n_A^*) は与えられたパワー制約を

$$q^* \frac{n_A^* h f_0}{\Delta} = P. \tag{3.30}$$

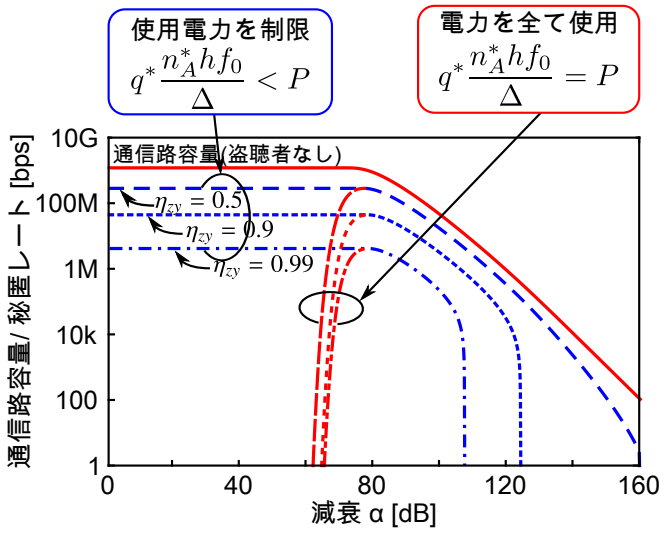

図 3.13　減衰 $\alpha = -\log_{10}\eta_y$ の関数としての通信路容量 C(実線) と秘匿レート R_{S}(破線，点線，一点鎖線)．秘匿レートについては，減衰に応じてパワーを調節する場合と，利用可能な電力を全て使い切る場合の両方を示している．パラメータ：$P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, $\Delta = 1$ ns.

のように等式で満足する．すなわち，より高い SN 比を確保するために，イブの盗聴を考慮せずに利用可能な全ての電力を使用することが最適な戦略となる．

図 3.13 に，上記の点を考慮した上で計算した秘匿レート R_{S} を，減衰 α の関数として示す．図中には比透過率 η_{zy} が異なるいくつかの曲線を描いているが，η_{zy} が 1 に近づくにつれ，すなわちイブとボブが得られる送受信電力が等しくなるに連れて，秘匿レートは減少していくことが確認できる．

加えて，実線で描いた通信路容量と秘匿レートの振る舞いを比較すると，秘匿レートのみに見られる，イブを考慮に入れた上で初めて現れる現象をいくつか確認できる．初めに，雑音限界領域では，秘匿レートが急激に 0 になる減衰 α の値が存在する．これは，イブがボブよりも低暗計数な検出器を利用していることによる．次に，損失無依存領域で使用可能な電力を全て使い切ってしまった場合には，上でも議論したように，イブも十分な強度のパルスを検出できるため，R_{S} は α が減少するにつれて急激に 0 になる．

図 3.14 から図 3.16 に，秘匿レートを与えるパラメータの値を示す．興味深いことに，秘匿レートそのものとは異なり，これらのパラメータの振る舞いは比透過率 η_{zy} によって大きく変化していない．

図 3.14 に最適な受信パルスの平均光子数 n_B^* を示す．通信路容量における n_B^* の振る舞いとは異なり，損失無依存領域では n_B^* の値はほとんど変化しない．しかし，雑音限界領域においては，これらはほぼ同じ振る舞いをする．図 3.15 に示す，送信パルスの平均光子数 n_A^* からは，減衰 α が変化するに連れて，アリスが送信パルスを調節していることが分かる．このような，入力側でのパルス強度の調節が必要な点は，信頼性のみを追求すれば良い 1 対 1 の通信と，安全性も考慮に入れる必要がある一方向秘匿メッセージ伝送と

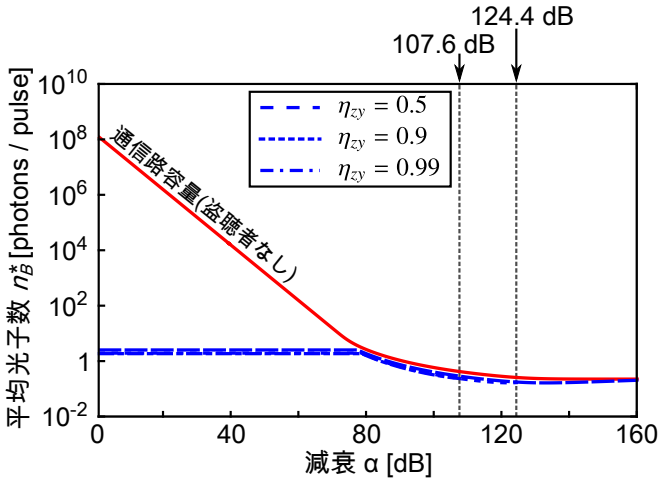

図 3.14　図 3.13 において通信路容量 C(実線) 及び秘匿レート R_{S}(破線，点線，一点鎖線) を与える受信パルスの平均光子数 n_B^*．秘匿レートが 0 になるため，$\eta_{zy} = 0.9$ と $\eta_{zy} = 0.99$ に関しては $\alpha = 124.4$ dB と 107.6 dB まで示している．

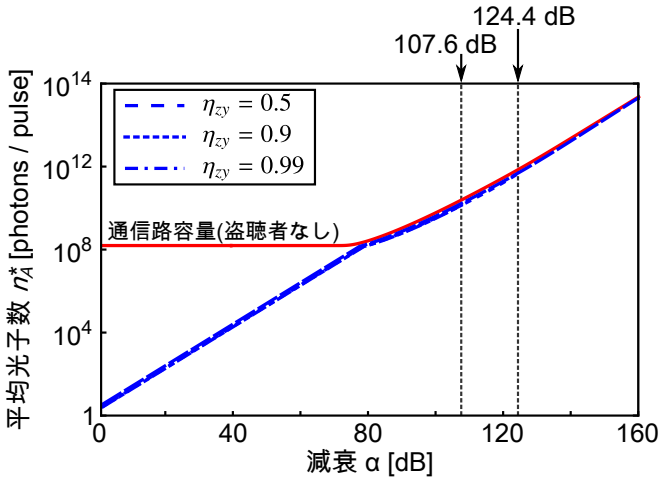

図 3.15　図 3.13 において通信路容量 C(実線) 及び秘匿レート R_{S}(破線，点線，一点鎖線) を与える送信パルスの平均光子数 n_A^*．

の大きな違いである．

一方で，図 3.16 に示す最適なパルス生成確率は q^*，通信路容量と秘匿レートの間で大きなふるまいの違いは見られない．

3.3.3　量子鍵配送との比較

第 1 章において，無条件安全性を持つ量子鍵配送 (QKD) に対して，物理レイヤ暗号ではイブに対する物理的な仮定を課すことでユーザビリティを高めた暗号技術であると位置づけた (図 1.3)．ここでは，その点について秘匿容量と QKD の鍵生成レートを比較することによって，定量的な議論を行う．なお，秘匿レートは古典ワイヤタップ通信路符号

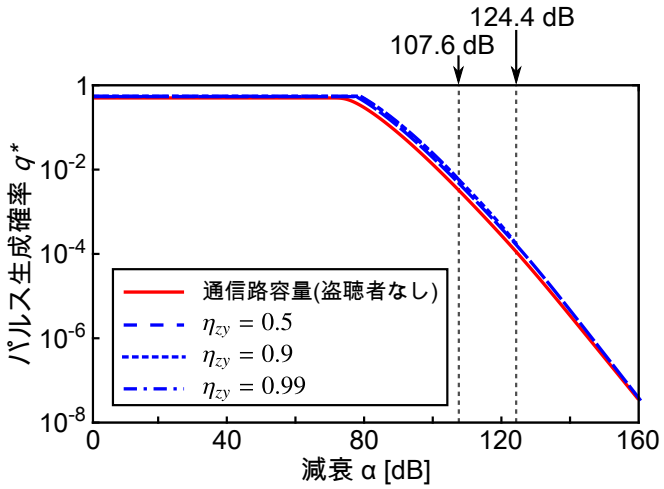

図 3.16　図 3.13 において通信路容量 C(実線) 及び秘匿レート R_{S}(破線，点線，一点鎖線) を与えるパルス生成確率 q^*.

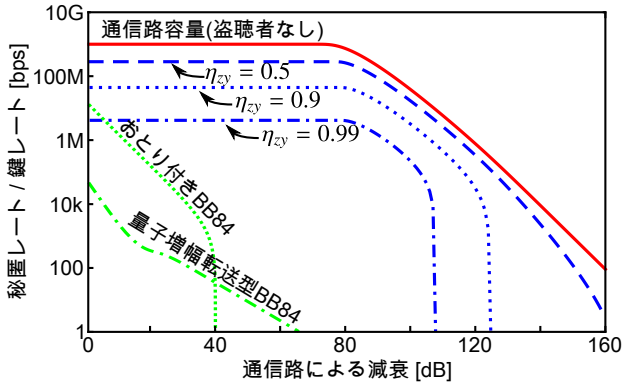

図 3.17　秘匿レート R_{S} と QKD(BB84 [16] protocol) の鍵生成レート．ワイヤタップ通信路のパラメータ：$P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, $\Delta = 1$ ns. QKD の鍵生成レートは，パルス生成レートを 1GHz 検出器の暗計数率を 100cps として計算した．

化による一方向メッセージ伝送におけるメッセージ伝送効率の尺度であることに対して，QKD の秘密鍵レートは量子通信路と認証付き公開通信路を利用した上での鍵共有の効率の尺度である点に注意する．

図 3.17 に，前小節と同様のパラメータで計算した秘匿レート R_{S} と QKD の秘密鍵レートを同時に示す．図中の “おとり付き BB84”は，信号光とは強度が異なるパルスを敢えて挿入する手法 [146] により，複数の光子を含むパルスによる安全性の劣化を防ぐ BB84[16] の方式 (おとり付き BB84) の鍵生成レートである．ここで，現在の実用化されている QKD システムにおける典型的な値からパルス生成レートを 1GHz，暗計数率を 100cps と仮定した．

類似した BB84 の方式の中では長距離伝送を可能としたおとり付き BB84 であるが，そ

の鍵レートは $\alpha = 40$dB 付近において急激に減少する．これは，低軌道衛星と地上局間を結ぶ通信路のリンクバジェットと同等である [147]．すなわち，この結果は QKD による衛星-地上局間通信は困難であることを示している．より長距離伝送可能な手法として，パルスを増幅しつつリレーする方式 [148] も提案されている．しかし，図中の “量子増幅転送型 BB84”のカーブに示すように，伝送距離が増加する一方で，全体の鍵レートは大きく減少してしまう．

一方で，秘匿レート R_{S} は，例えイブが $\eta_{zy} = 0.99$ という状況，すなわち，ボブが得られるパワーの 99% のパワーを得られる状況であったとしても，QKD による鍵生成が困難であるような遠距離をカバーできている．特に，$\alpha = 80$dB という静止軌道衛星－地上局間通信のリンクバジェットに対応する距離であっても，情報理論的に安全な光空間通信が実現可能であることを図 3.17 の計算は示している．以上の結果は図 1.3 における議論を定量的に裏付けたものとなっている．

3.4 補助通信路が連接された場合の解析

この節では，補助通信路と補助変数を導入することにより，光子通信路における秘匿容量の完全な定式化を行う．その上で，Csiszár と Körner[67] によって数学的便宜として導入された補助通信路の，光子通信路における物理的な意味についても議論を行う．

3.4.1 パワー制約と通信路の遷移確率

節 3.2 で述べたオン-オフ変調によるモデルでは，イブがボブよりも低雑音な検出器を用いている場合には more capable の条件は満足されず，従ってパラメータによっては相互情報量の差が負になる場合があることを図 3.12 でも見てきた．そこで，第 2 章でも述べたように，more capable の条件が満足されないワイヤタップ通信路に対しては，アリスの入力 X に架空の補助変数 V を補助通信路で連接する必要があった．

そのようなモデルを実現するために，節 3.2 で定式化した通信路に新しい操作を加える．アリスは，バイナリ列 $\mathbf{v}$ を確率 $q = \Pr\{V = 1\}$ で生成する．その後，そのバイナリ列からいくつかのビットをランダムに選択して反転させて，伝送用のバイナリ列 $\mathbf{x}$ を得る．このバイナリ列をパルスに変換してボブ (とイブ) へと伝送する．

以上の定式化において，補助変数 V は真のメッセージを符号化した際のシンボルであり，入力変数 X は実際に通信路で伝送されるシンボルに対応している．ここで，ワイヤタップ通信路の符号化レートを最適化するためには，V の要素は X の要素数以上である必要が無いことが知られている [67] ため，V を 2 元の確率変数でモデル化しても問題はない．

以上に述べた通信路モデルの通信路遷移確率図は，図 3.18 で与えられる．ここで，補助通信路 $P_{X|V}$ の遷移確率を，定数 $0 \le a, b \le 1$ によって

$$P_{X|V}(1|0) = a, \quad P_{X|V}(1|1) = b \tag{3.31}$$

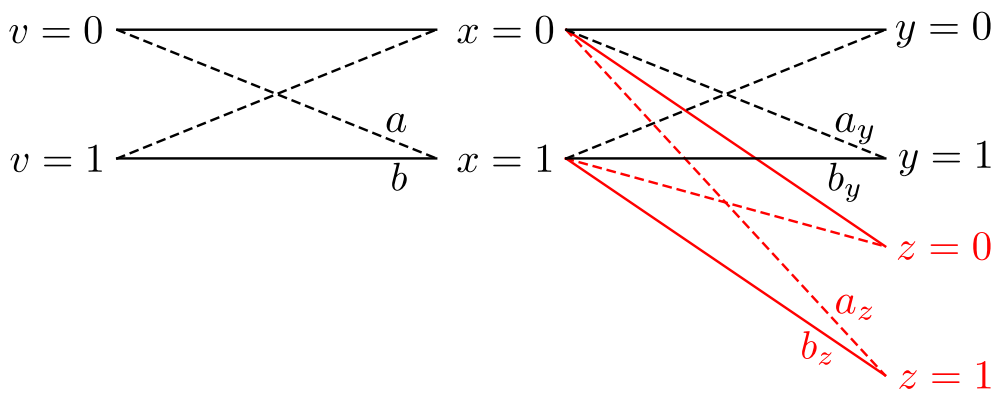

図 3.18　補助通信路付きの通信路遷移確率の概要図

と定義する．

パワー制約については，補助変数を考慮した場合，第 3 章で述べたように 3 種類の課し方 (強化指数，X- 制約，V- 制約) が存在した．しかし，上記のモデルの場合，実際にレーザーによってパルスの伝送を行っているのは入力 X のシンボルである．そのため，X- 制約によるパワー制約を考える．

補助変数 V における入力を $q = \Pr\{V = 1\}$ と定義すると，$q^+ = \Pr\{X = 1\}$，すなわちスロット毎にパルスが伝送される確率は $q^+ \equiv (1-q)a + q(1-b)$ と与えられる．そのため，パワー制約は

$$q^+ \frac{n_A h f_0}{\Delta} \leq P. \tag{3.32}$$

と与えられる．

3.4.2　秘匿容量

補助変数を加えた上で，入力 $q = \Pr\{V = 1\}$，平均光子数 n_A，補助通信路の遷移確率 a，b の最適化を行ことによって，秘匿容量 C_{S} が得られる．ここで，その具体的な式を与える．

アリスとボブの間の相互情報量は，補助通信路が連接されている場合には

$$f_B^+(q, n_A, a, b) \triangleq h_2((1-q)a_y^+ + q(1-b_y^+)) - (1-q)h_2(a_y^+) - qh_2(b_y^+) \tag{3.33}$$

によって求められる．ここで，$a_y^+ \triangleq W_B^+(1|0)$ 及び $b_y^+ \triangleq W_B^+(1|1)$ と置いているが，連接ワイヤタップ通信路の遷移確率分布の定義式 (2.42) から

$$\begin{aligned} a_y^+ &= P_{X|V}(0|0)W_B(1|0) + P_{X|V}(1|0)W_B(1|1) \\ &= (1-a)a_y + ab_y \\ b_y^+ &= P_{X|V}(0|1)W_B(1|0) + P_{X|V}(1|1)W_B(1|1) \\ &= (1-b)a_y + bb_y \end{aligned}$$

と具体的に計算できる．

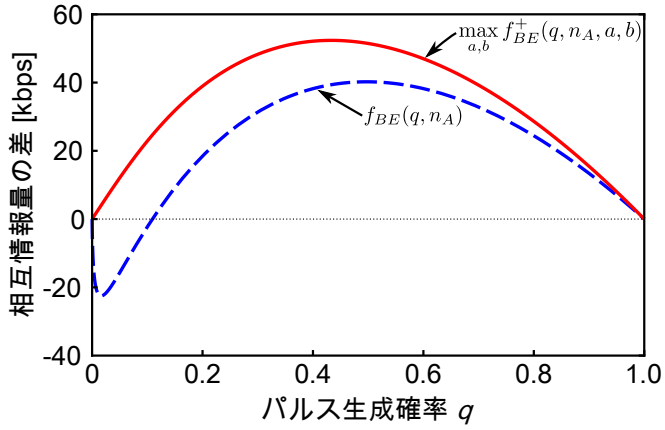

図 3.19　$\max_{a,b} f^+_{BE}(q,n_A,a,b)$ と $f_{BE}(q,n_A)$ の比較．パラメータ:$n_B = 3.2\times10^{-3}$ photons/pulse，$\eta_{zy} = 0.95$，$\lambda_y = 10$ kcps，$\lambda_z = 1$ cps，$\Delta = 1$ ns.

同様に，アリスとイブの間の相互情報量は

$$f^+_E(q,n_A,a,b) \stackrel{\triangle}{=} h_2((1-q)a^+_z + q(1-b^+_z)) - (1-q)h_2(a^+_z) - qh_2(b^+_z), \qquad (3.34)$$

と求められる．ここで，$a^+_z \stackrel{\triangle}{=} W^+_E(1|0)$ 及び $b^+_z \stackrel{\triangle}{=} W^+_E(1|1)$ は

$$a^+_z = (1-a)a_z + ab_z$$
$$b^+_z = (1-b)a_z + bb_z$$

となる．

以上より，相互情報量の差を $f^+_{BE}(q,n_A,a,b) \stackrel{\triangle}{=} f^+_B(q,n_A,a,b) - f^+_E(q,n_A,a,b)$ と定義すると，秘匿容量は

$$C_{\rm S} = \max_{q,n_A,a,b} f^+_{BE}(q,n_A,a,b), \qquad (3.35)$$

と与えられる．ここで，最適化はパワー制約 (3.32) を満足する範囲で行われる．

ここで，補助変数が相互情報量の差に及ぼす影響を数値計算的に確認しておくことは，続く節における議論の理解に役立つ．図 3.19 に，横軸を入力確率 q ととり，n_B を固定した上での，相互情報量の差を補助通信路の遷移確率で最大化した $\max_{a,b} f^+_{BE}(q,n_A,a,b)$(実線) と，補助変数無しの相互情報量の差 $f_{BE}(q,n_A)$(破線) の比較示す．more capable が満足されていないことから，$f_{BE}(q,n_A)$ が $q < 0.1$ で負になることを確認できる．一方で，補助通信路を最適化した $\max_{a,b} f^+_{BE}(q,n_A,a,b)$ は $q \in (0,1)$ で正の値をとり，なおかつ $f_{BE}(q,n_A)$ よりも大きな値をとっている．このような相互情報量の差の増加は，次小節で見るように，伝送距離の増加につながる．

3.4.3　秘匿容量の数値計算

図 3.20 に，秘匿容量 $C_{\rm S}$(実線)(3.35) と秘匿レート $R_{\rm S}$(破線)(3.28) を減衰 α の関数として比較した．この図に示すように，補助変数 V を考慮する，すなわち，真の符号語に

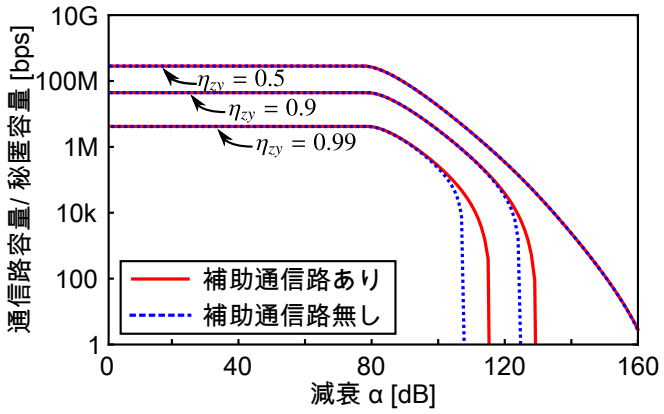

図 3.20 秘匿容量 C_{S} と秘匿レート R_{S} の比較．パラメータ：$P = 10$ mW，$\lambda_y = 10$kcps，$\lambda_z = 1$cps，$\Delta = 1$ns.

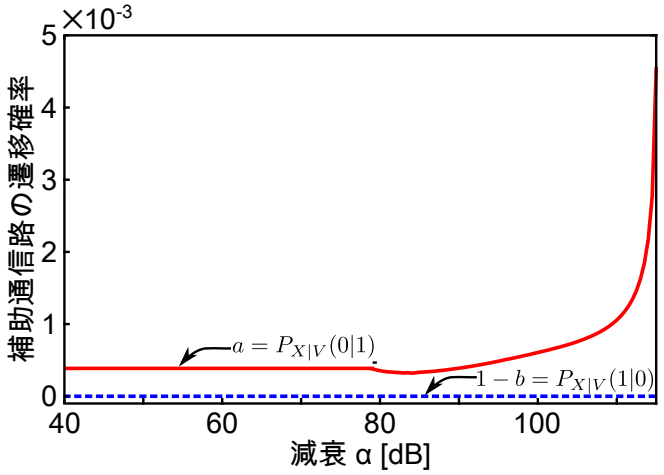

図 3.21 図 3.20 の $\eta_{zy} = 0.99$ の場合について，秘匿容量を与える遷移確率 $a = P_{X|V}(1|0)$ と $1 - b = P_{X|V}(0|1)$.

対して敢えてエラーを加えることによって，雑音限界領域において伝送距離が向上することが確認できる．例えば，$\eta_{zy} = 0.99$ においては，レートが急激に減少する α は 6 dB 増加している．これは，距離に換算して 40% の向上に相当する．補助変数による距離の増加は，比透過率 η_{zy} が増加するにつれて顕著になる．

図 3.21 では，図 3.20 の内，$\eta_{zy} = 0.99$ の場合に秘匿容量を与える遷移確率 $a = P_{X|V}(1|0)$ と $1 - bP_{X|V}(0|1)$ を示している．確率 a が非零で，雑音限界領域に差し掛かると急激に増加する一方で，$1 - b$ は α の値に関わらず，定数 0 のままである．ここで，確率 a はシンボル $v = 0$ をシンボル $x = 1$ に置き換える確率に対応しており，ダミーパルスの挿入を意味している．b がほぼ時間変化しないことから，ダミーパルスの挿入が距離向上の本質的要因であることが分かる．

以上のような，距離向上あるいは安全性向上のために，敢えて信号にノイズを加える方式は，物理レイヤ暗号の分野では特に受信者が複数のアンテナを持つ状況の解析が行われ

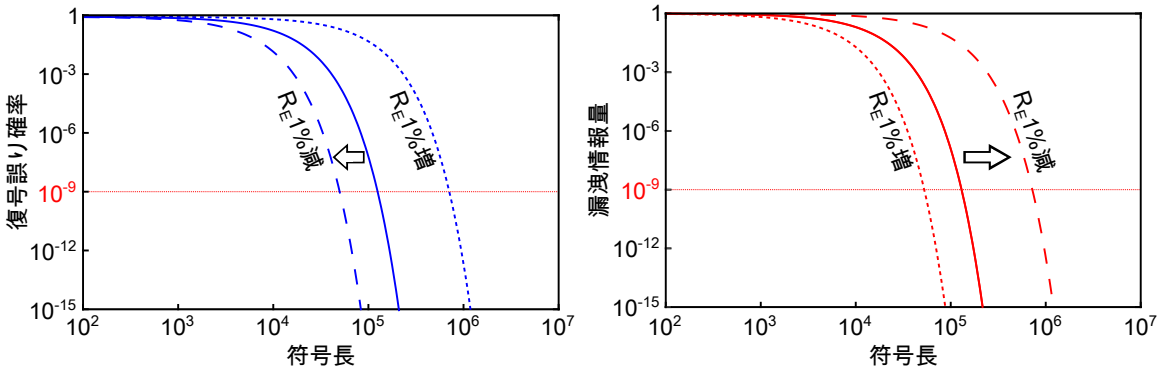

図 3.22　(a) 復号誤り確率 ε_n^B と (b) 漏えい情報量 δ_n^E の符号長依存性．符号化レートは $R_B^* = 0.5R_{\rm S} = 22.1$ Mbps とした．図中の矢印は，ランダムネスレート R_E を $R_E^* = 0.641$ Gbps から 1% 減少させた場合の符号長依存性の変化を示す．

ている [149, 150, 151]．ここでは，加えたノイズがアンテナ間で発生する干渉によって打ち消されるように，巧妙に設計を行う．一方で，図 3.20 では，低雑音な検出器を持つイブに対して，ランダムなパルス挿入を行うことが距離向上に繋がった．この意味で，当該手法はおとり付き BB84[146] と同様のはたらきをしていると考えられる．

3.5　復号誤り確率及び漏洩情報量の符号長依存性の解析

ここでは，誤り指数と秘匿性指数から，復号誤り確率と漏えい情報量の符号長依存性を示す．

図 3.22 に，図 3.13 及び図 3.14 で示した結果の内，$\eta_{zy} = 0.9$ 及び $\alpha = 70$ dB の点を選んで復号誤り確率と漏えい情報量の符号長依存性を示す．秘匿レートは $n_A^* = 1.94 \times 10^7$ と $q^* = 0.544$ に対して，$R_{\rm S} = 44.2$ であったため，図中では符号化レートを秘匿レートの半分である，$R_B^* = 22.1$ と固定した．

図 3.22 中の実線は，ランダムネスレートを $R_E^* = 0.641$ Gbps と固定した場合の符号長依存性である．この場合には，誤り確率 ε_n^B と漏えい情報量 δ_n^E の両者は $n = 10^4$ から減少を始め，$n = 10^5$ で $\varepsilon_n^B < 10^{-9}$ 及び $\delta_n^E < 10^{-9}$ に達する．この $n = 10^5$ という長さは，LDPC 符号などによって現時点で実現可能な符号長である．以上より，例え $\eta_{zy} = 0.9$ という多くのパワーがイブに漏れている状況であっても，十分に小さい誤り確率と漏えい情報量を達成可能な，現実的な長さのワイヤタップ通信路符号を構成可能できることが示された．

最後に，前節でも議論したように，ランダムネスレートを変化させた場合の信頼性と秘匿性の間のトレードオフ関係について述べる．図 3.22 の破線は，ランダムネスレート R_E を R_E^* から 1% 減少させた場合の符号長依存性の変化である．表 3.1 に示すように，誤り指数は符号 $\mathcal{C}_1$ の符号化レート $R_B + R_E$ の減少に伴って増加するため，復号誤り確率は減少する．その一方で，秘匿性指数はランダムネスレートとともに減少するた

表 3.1　図 3.22 におけるレートと各指数の表

	R_E [Gbps]	$R_B^* + R_E$ [Gbps]	誤り指数	秘匿性指数
$R_E = R_E^*$	0.641	0.663	1.59×10^{-4}	1.59×10^{-4}
$R_E = 0.99R_E^*$	0.634	0.656	4.00×10^{-4}	0.29×10^{-4}
$R_E = 1.01R_E^*$	0.647	0.669	0.28×10^{-4}	3.94×10^{-4}

め，漏えい情報量は増加する．結果として，図 3.22 にも示すように，$\varepsilon_n^B < 10^{-9}$ となる符号長は $n = 7 \times 10^4$ と短くなるが，その符号長では δ_n^E は 10^{-1} 程度に留まる．そして，$\delta_n^E < 10^{-9}$ を達成するためには，$n \geq 9 \times 10^5$ という長い符号長が必要になる．図中の点線は，R_E を R_E^* から 1% 増加させた場合の符号長依存性の変化である．この場合には，1% 減少させた場合とは逆に，ε_n^B は増加し，δ_n^E は減少する．

3.6　まとめ

本節では，はじめに物理的に意味を持つ通信路モデルの評価に必要不可欠である，入力へのコスト制約の定式化を行った．そして，コスト制約が課されているワイヤタップ通信路について，誤り指数と秘匿性指数の導出について述べた．本節で導出した指数は入力確率分布のみならず，補助変数が従う確率分布にも等価なコスト制約が課されたより一般的な指数であり，数値計算を通して，コスト制約が 1 つしか課されていない場合よりも強い指数となっていることを確かめた．

なお，これらの指数は Han, Endo, Sasaki ら [79] によって既に導出されていたが，本研究では [79] で省略されていた証明を明確に行い，指数の性質の証明を行った．また，本研究で述べた方法とは異なる手法で導出された Gallager の指数との比較を行い，Gallager の指数に内在している証明上の不備を明らかにした．これにより，本論で述べた方法で導出された指数がより広いクラスの通信路の評価に適用可能であることを示した．

次に，光通信の典型例として，パルスのオンとオフによる通信を行う通信路の定式化を行い，通信路容量及び秘匿レート (秘匿容量) の数値計算を行った．特に，QKD と秘匿レートの比較からは，無条件安全性を持つ QKD に対する，物理レイヤ暗号の，イブに対する物理的な仮定を課すことでユーザビリティを高めた暗号技術とする位置づけ (図 1.3) を定量的に明確にした．また，伝送可能距離が，入力側に敢えてノイズを加えることによって，さらに増加することも明らかにした．これは，QKD においておとりノイズが加えられる状況と類似している．

最後に，コスト制約付き誤り指数と秘匿性指数を利用した符号長依存性の解析から，十分な伝送速度を持った符号化が，計算機や素子で処理可能な長さの符号でも十分に実現可能であることが示された．

第 4 章

物理レイヤ暗号実現に向けた光空間通信路推定実験

前章で行った光空間通信におけるワイヤタップ通信路符号化の実現可能性の解析は，大気のゆらぎの無い理想的な状況で行われていた．しかし，理論と実環境の間の大きな違いはこの大気のゆらぎの効果であると言っても過言ではなく，実環境においてはその効果を勘案した上で符号設計を行う必要がある．

既存の研究にはこの大気のゆらぎの効果を様々な手法で考慮し，物理レイヤ暗号の性能評価を行ったものも非常に多い [91, 92, 152, 153] ものの，それらの多くは実データに基づいた解析ではなく，理想的に長い時間の伝送を行った場合の平均値に基づく漸近的な解析に過ぎなかった．しかし，大気の状態は現実には気象，気温，風速などといった実環境の要因により，時々刻々と変化をしている．そのため，光空間通信における物理レイヤ暗号の性能評価を行うためには，実環境において取得された実験データが必要になる．

本章では，そのような実環境における物理レイヤ暗号の性能評価の一環として行われた，回線長 7.8km の光空間通信テストベッドを用いた通信路推定実験について述べる．光空間通信の実験は現在でも数多く知られているが，本章で述べる光空間通信テストベッドは 1 送信ターミナルに対して 2 受信ターミナルを備え，光空間通信における物理レイヤ暗号の典型例を再現したものとなっており，これまでの研究において前例が無い実験設備となっている．本実験設備の目的は，実験データから大気の揺らぎが物理レイヤ暗号の性能に及ぼす影響を定量化することにある．また，実データ解析のための基盤を整備し，後の章で述べる光空間通信における秘密鍵共有を実証するための準備を行うといった目的もある．

以降では，このテストベッドに搭載されている装置群について述べ，そこから実験データを用いた評価法について述べる．本章では情報理論的な諸量 (秘匿レート，秘匿アウテージ確率) に加えて，大気光学においてよく用いられる量 (大気の構造定数，Fried パラメータ) 等を導入する．実験データからそれらを評価し，大気の揺らぎの効果が物理レイヤ暗号に及ぼす影響を推定する，すなわち実験データからの通信路状態の推定が本章における主題となる．そして，それらの知見を活かして，物理レイヤ暗号使用の可否判断を行

図 4.1　(a) Tokyo FSO Testbed の概要図．アリスの送信系は電通大ビル屋上に設置されている．ボブとイブの検出系は情報通信研究機構のビルに設置されている．©OpenStreetMap contributors, CC-BY-SA.

うための諸量を計算し，実用的な物理レイヤ暗号の符号化の理論的検討を行う．

4.1　Tokyo FSO Testbed

本節では，物理レイヤ暗号の文脈において実環境データを取得する目的で構築された Tokyo FSO Testbed について述べる．

4.1.1　テストベッドの概要

図 4.1(a) に，Tokyo FSO Testbed の概要図を示す．Tokyo FSO Testbed はアリス，ボブ，イブの役割を担う 3 つのターミナルで構成されている．アリスのターミナルは電気通信大学 (東京都調布市:35°39′28.8″N, 139°32′39.5″E) の 9 階建てビル屋上に設置されている．ボブとイブはそれぞれ電気通信大学から直線距離で 7.8km 離れた，情報通信研究機構 (東京都小金井市:35°42′24.2″N, 139°29′19.3″E) の 6 階建てビルの 6 階と屋上に設置されている．ボブとイブは直線距離で 10m 離れている．

4.1.2　アリスの送信系

ここでは，図 4.2 に示したアリスの送信系について，実験装置の各要素の詳細について述べる．

アリス送信系の設置場所について

アリスの送信系は電気通信大学キャンパス内にある 9 階建てビルの屋上に設置された全天候型ドーム内に構築されており，0.005° の回転精度を持つ雲台 (望遠鏡などの光学機

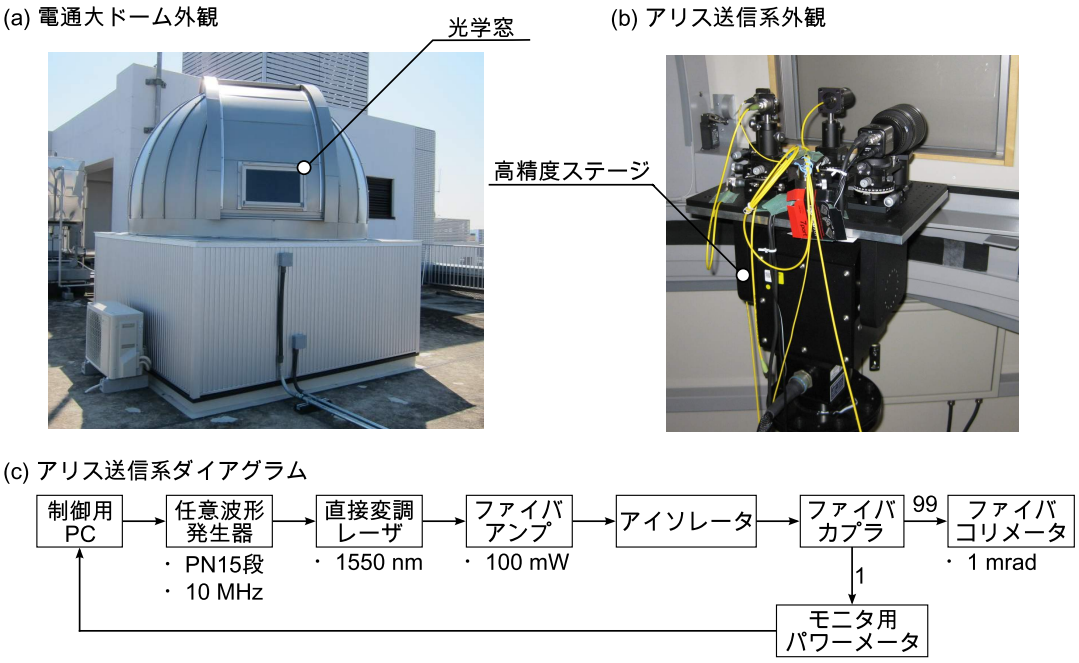

図 4.2 (a) 電通大に設置されたドームの外観．(b) ドーム内に構築されたアリスの送信系の外観．(c) 送信系のダイアグラム．

器を搭載して，左右 360° と上下 180° の回転が可能なステージ) によってビーム射出方向の調整が可能となっている．この雲台の制御は，NICT からの遠隔操作が可能となっている．

光源

中心波長 λ_c =1550 nm の狭帯域直接変調レーザー (Sense Light Semiconductors DL-BF10-CLS101B-S1550: 帯域は CW 駆動で 50 kHz 以下) を光源として利用している．この波長は，光空間での減衰に比較的強く [154]，アイセーフの条件にも合致している [155]．このレーザーに任意波形発生機で生成した帯域 10MHz の RF 信号を印加することで，オンーオフ変調を行う．

レーザーのパワーはファイバアンプ (IPG Laser GMBH : EAU-4-C-PM-NT) により 100mW に増幅される．そして，このファイバアンプからの出力を分岐比 99:1 のファイバカプラで分割し，パワーメータにより出力パワーの監視を行っている．

擬似乱数信号

本研究では，図 4.3 に示す 15 ビットの線形帰還シフトレジスタから生成される擬似乱数系列 (PN15 段) を送信している．このシフトレジスタは 15 ビットで表現された「状態」を持ち，その第 14 ビットと第 15 ビットの排他的論理和を乱数ビットとする．同時に，出力された乱数ビットは 1 ビットシフトした「状態」の第 1 ビットへ入力される．このような方法で構成されるシフトレジスタは，15 ビット全てが 0 となる「状態」以外の

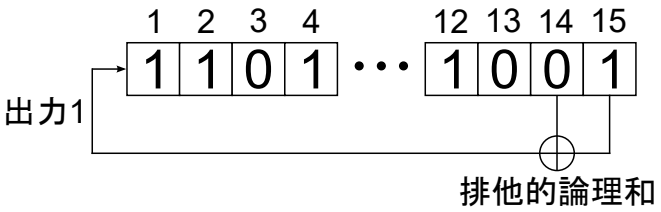

図 4.3　15 ビットの線形帰還シフトレジスタ.

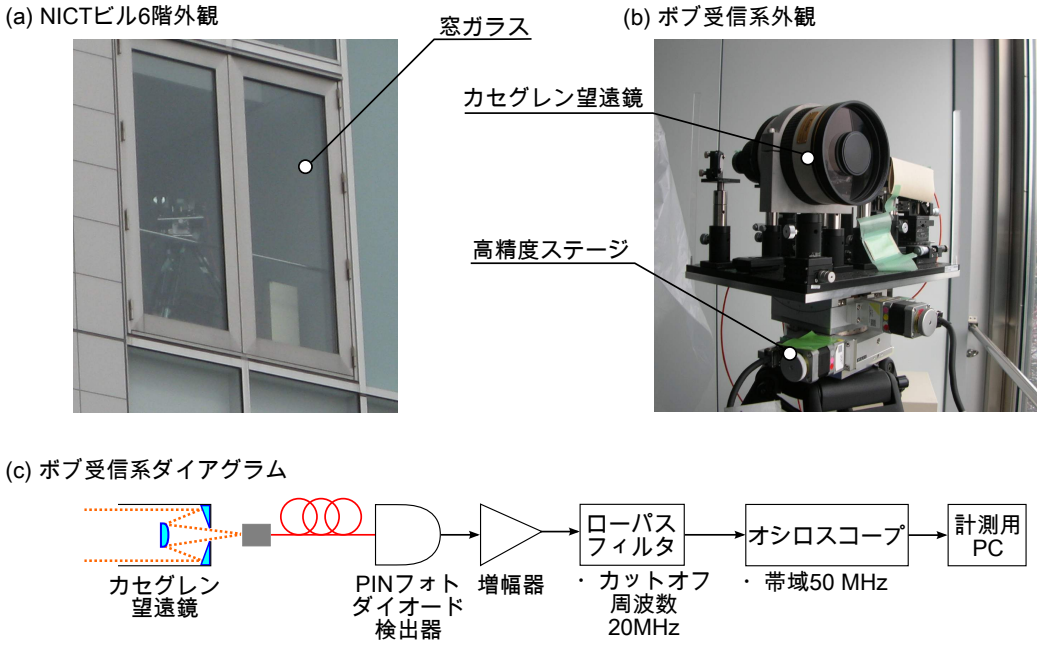

図 4.4　(a) ボブの受信系が設置されている NICT ビル 6 階の外観. (b) ボブの受信系の外観. (c) 受信系のダイアグラム.

$2^{15} - 1$ 個の「状態」が現れるため，出力された擬似乱数系列は周期 $2^{15} - 1$ を持つ.

PN15 段は，自己相関を計算すると元の系列と一致する場合のみで急峻なピークを持ち，”1”と”0”がほぼ等確率 (1/2) で出現するため，通信システムの特性を計測する目的で利用される.

出力レンズ

変調されたレーザーは雲台上のブレッドボードに固定されているファイバコリメータ (開口径 10 mm 及び拡がり角 1.0 mrad) にカップルされ，直径約 5.5 mm にコリメートされる．このビームは，7.8km 離れている NICT 側では直径 8m のビームに広がる.

4.1.3 ボブの受信系

ここでは，図 4.4 に示したボブの実験系について，実験装置の各要素の詳細について述べる．

ボブ受信系の設置場所について

ボブの受信系は，三脚上に構築された光学系と，データ取得のための処理系に分けられる．光学系は精度 0.003° の回転ステージ (中央精機： ARS-136-HP) と精度 0.002° のゴニオステージ (中央精機： ATS-130-HP) に載せられており，PC 制御によってアライメントを行えるようになっている．これらの検出系は NICT ビル 6 階の窓越しに設置されており，受信光強度は窓に施されたコーティングによる減衰を受ける．

光学系

ボブは直径 111 mm 及び焦点距離 800 mm であるカセグレン望遠鏡 (ケンコー： 800mm F8 DX) により電通大からのビームを集光する．この望遠鏡によって，受信光は直径 10 mm にコリメートされ，その後レンズ系を得て光検出器に導波される．これらの光学系の損失は，窓ガラスによる減衰を含めて，-14 dB 程度であると計測されている．

光検出器及びデータの保存

光強度は雑音等価電力が $3.0\mathrm{pW}/\sqrt{\mathrm{Hz}}$ である PIN フォトダイオード検出器 (Terahelz Technology Inc： TIA-525) で電圧に変換される．検出器の出力電圧はアンプユニット (浜松ホトニクス： C-6438) で増幅された後に，USB 接続型のオシロスコープ (日本データシステム：UDS-1G02S-HR) で収録される．このオシロスコープのサンプリングレートは 50MHz であるが，ローパスフィルターによる 20MHz の帯域制限が設けられている．

4.1.4 イブの受信系

ここでは，図 4.5 に示したイブの受信系について，実験装置の各要素の詳細について述べる．

イブ受信系の設置場所について

イブの受信系はボブの検出系が設置されたビルの屋上に設置されたコンテナシステム (図 4.1(a)) 内に設置されている．このコンテナは屋上に左右 360° と上下 100° の回転を行うスキャナ (図 4.1(b)) を備える．そのスキャナに備えられた光学窓から入射した光はミラー対によってコンテナ内の光学定盤上に導かれる．

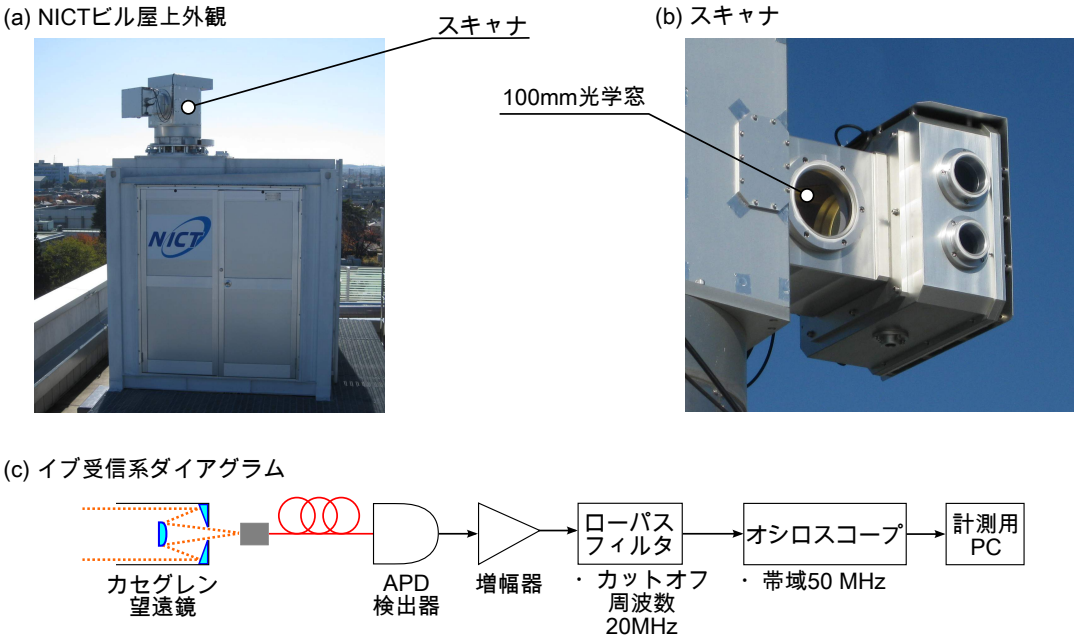

図 4.5　(a) イブの受信系が構築されているコンテナシステム．(b) スキャナの外観．(c) 受信系のダイアグラム．

光学系

光学定盤上に導かれた入射光はカセグレン望遠鏡 (直径 100 mm 及び焦点距離 2000 mm) により直径 10 mm へとコリメートされる．光学系全体の損失は-9dB 程度であった．すなわち，窓越しであるという設置条件も含めて，イブの検出系の方がボブの検出系よりも低損失である．

受信機及びデータの保存

イブの入射光の光強度は雑音等価電力が $160\mathrm{fW}/\sqrt{\mathrm{Hz}}$ であるアバランシェフォトダイオード (Laser Components： A-CUBE-I200-10) によって電圧に変換される．雑音等価電力の比較からも明らかなように，この検出器はボブの検出器よりも高感度である．電圧はボブと同様にアンプユニット (浜松ホトニクス：C-6438) で増幅された後に，USB 接続型のオシロスコープ (日本データシステム：UDS-1G02S-HR) で収録される．

データ処理系

ボブとイブによって保存されたデータは LabVIEW で作成されたオフラインソフトウェアに通すことで伝送データの復調が行われる．はじめに，高周波ノイズをカットオフ周波数 f_c が 6 MHz であるローパスフィルターによって取り除く．次に，受信データからクロック情報を再生するために，クロックデータ再生 (CDR : Clock data recovery) プロセスを行う．そのクロックを元に 50MHz から 10MHz へとデータのダウンサンプリング

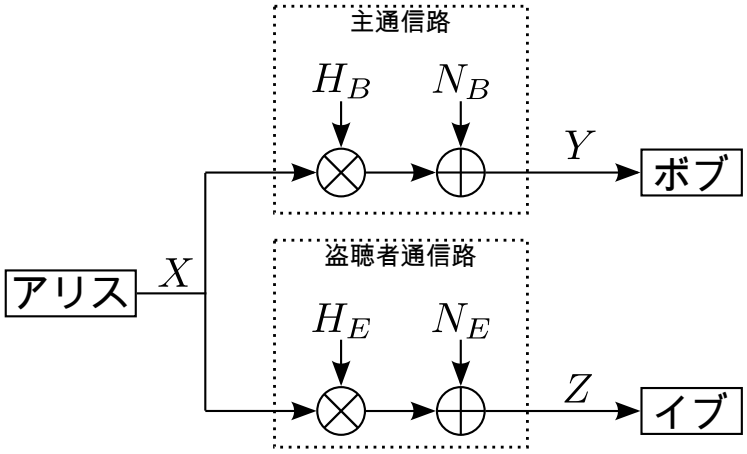

図 4.6 本節で扱うワイヤタップ通信路モデルの概要図.

(DS) 処理を行う．最後に，伝送した擬似乱数系列との間での相関を計算することにより，伝送データとのフレーム同期を図る．

4.2 実験データからの解析手法

本実験の目的は，実験データから通信路の状態を推定し，ワイヤタップ通信路符号化の観点からの知見を得ることにある．そのために，秘匿伝送可能な情報レートと光空間通信で頻繁に用いられる指標により実験データの解析を行う．以下に，その各手法について述べる．

4.2.1 秘匿伝送可能な情報レートの評価

通信路のモデル化

前節で述べた Tokyo FSO Testbed における検出器はアナログな電圧値を出力し，そのノイズはガウス分布に従っていると考えられる．加えて，レーザー光は大気の揺らぎの影響を受けて，時々刻々変化をしている．以上の設定から，Tokyo FSO Testbed を図 4.6 に示すワイヤタップ通信路でモデル化する．アリスは確率分布 P_X に従う長さ n の確率変数 X^n を生成し，$X = 0$ ならばレーザーをオフ，$X = 1$ ならばレーザーをオンにするオン−オフ変調を行う．なお，本研究では擬似乱数系列を伝送するため，確率分布 P_X は固定されているものとして扱う．

ボブが観測する出力確率変数 Y は

$$Y = H_B X + N_B \tag{4.1}$$

と表される．ここで，H_B は大気のゆらぎを表す確率変数であり，N_B はガウス分布に従う確率変数である．同様に，イブが観測する出力確率変数は，盗聴者通信路のゲインを表

す確率変数 H_E と，ガウス分布に従う確率変数 N_E によって，

$$Z = H_E X + N_E \tag{4.2}$$

と表される．

秘匿レートの定義

本研究では大気ゆらぎは準静的な確率過程であるとし，ある時間間隔では通信路ゲイン H_B，H_E は定数 h_B，h_E であるとする．そのような定常時間における秘匿レートを

$$R_{\mathrm{S,i}}(h_B, h_E) \equiv \max[0, I(P_X, P_{Y|X,H_B}) - I(P_X, P_{Z|X,H_E})] \tag{4.3}$$

と定義する．ここで，相互情報量を入力 P_X と通信路 W が与えられた場合の表記 $I(P_X, W)$ で書いている．また，$P_{Y|X,H_B}$ を入力変数 X と大気揺らぎ H_B で条件付けした主通信路の遷移確率分布，$P_{Z|X,H_E}$ を入力変数 X と大気揺らぎ H_E で条件付けした盗聴者通信路の遷移確率分布とする．このように定義された秘匿レート $R_{\mathrm{S,i}}(h_B, h_E)$ を h_B と h_E が与えられたときの瞬時秘匿レートと呼ぶ．以降，必要がなければ単純に $R_{\mathrm{S,i}}$ と表記する．

実験データから瞬時秘匿レート $R_{\mathrm{S,i}}$ を評価するためには，遷移確率分布 $P_{Y|X,H_B}$，$P_{Z|X,H_E}$ を特徴づける必要がある．本研究では，ボブはある閾値よりも小さい出力を $y = 0$，大きい出力を $y = 1$ に割り当てる，硬判定に基づく復号を行うと仮定する．この場合には，遷移確率分布は次の式で与えられる．

$$P_{Y|X,H_B}(1|x, h_B) = \frac{N(y \geq y_{\mathrm{th}}|x, h_B)}{N(x)}, \quad P_{Y|X,H_B}(0|x, h_B) = \frac{N(y \leq y_{\mathrm{th}}|x, h_B)}{N(x)} \tag{4.4}$$

ここで，$N(x)$ はアリスが伝送したシンボルの内 x となるものの総数であり，$N(y \geq y_{\mathrm{th}}|x, h_B)$ と $N(y \leq y_{\mathrm{th}}|x, h_B)$ はそれぞれ与えられた閾値 y_{th} とシンボル x，そして h_B に対して，$y \geq y_{\mathrm{th}}$ 及び $y \leq y_{\mathrm{th}}$ となる y の個数である．以上の遷移確率を元に，相互情報量 $I(P_X, P_{Y|X,H_B})$ は次のように評価される．

$$\begin{aligned} &I(P_X, P_{Y|X,H_B}) \\ &\quad = \sum_{x\in\{0,1\}} \sum_{y\in\{0,1\}} P_X(x) P_{Y|X,H_B}(y|x, h_B) \log_2 \left[\frac{P_{Y|X,H_B}(y|x, h_B)}{\sum_{x'} P_X(x') P_{Y|X,H_B}(y|x', h_B)} \right] \end{aligned} \tag{4.5}$$

なお，閾値 y_{th} は $I(P_X, P_{Y|X,H_B})$ が最大になるように，数値的に最適化される．

一方で，イブは出力の閾値による 2 値化ではなく，全ての出力値から相互情報量を計算する，軟判定復号を行うとする．これは，一般的に軟判定による相互情報量は硬判定による相互情報量よりも大きい値を与えるため，安全性という観点からも厳しい評価を与えるからである．本研究では，測定データが有限であるため，測定データを幅 Δ の K 個のビ

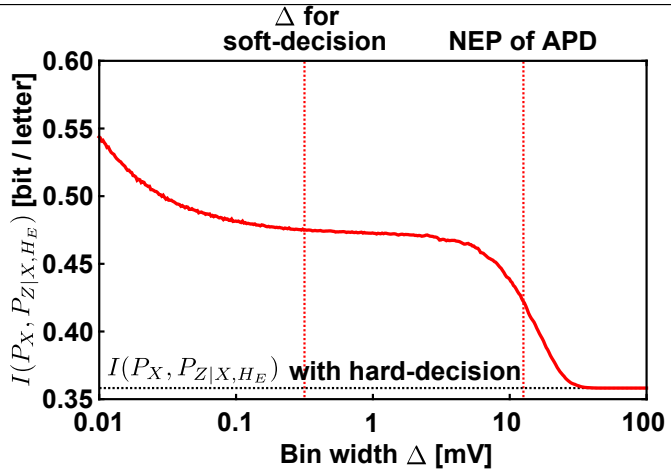

図 4.7　相互情報量 $I(P_X, P_{Z|X,H_E})$ のビン依存性．図 4.9 の 76 ms から 80 ms のデータを利用．

ンに分割して評価を行った．この場合，通信路の遷移確率分布関数 $P_{Z|X,H_E}(z^{(i)}|x,h_E)$ は

$$P_{Z|X,H_E}(z^{(i)}|x,h_E) = \frac{N(z^{(i)}|x,h_E)}{N(x)} \tag{4.6}$$

と与えられる．ここで，$N(z^{(i)}|x,h_E)$ は伝送シンボル $x \in \{0,1\}$ と h_E が与えられたときに，i 番目のビンに含まれている z の個数である．従って，相互情報量 $I(P_X, P_{Z|X,H_E})$ は下記のように計算される．

$$I(P_X, P_{Z|X,H_E}) = \sum_{x\in\{0,1\}} \sum_{i=1}^{K} P_X(x) P_{Z|X,H_E}(z^{(i)}|x,h_E) \log_2 \left[\frac{P_{Z|X,H_E}(z^{(i)}|x,h_E)}{\sum_{x'} P_X(x') P_{Z|X,H_E}(z^{(i)}|x',h_E)} \right] \tag{4.7}$$

最適なビン幅の決定

イブの軟判定に基づく相互情報量 $I(P_X, P_{Z|X,H_E})$ を最大化するためには，ビン幅 Δ を可能な限り細分化し，イブの出力分布の近似精度を高めることが望ましい．しかし，実験データが有限であるため，ビン幅 Δ には下限が存在する．その下限について議論するために，相互情報量 $I(P_X, P_{Z|X,H_E})$ のビン幅依存性を図 4.7 に示す．

ビン幅が 10 mV を超える場合には，$I(P_X, P_{Z|X,H_E})$ は実質的には硬判定と等しい値をとる．一方で，Δ が十数 mV から数 mV へと細分化するにつれて，相互情報量は増加していき，最終的には $I(P_X, P_{Z|X,H_E})$ は定常値をとるようになる．本研究では，この値を軟判定による値として採用した．なお，上記の定常値を与えるビン幅はイブの検出器 (APD) の雑音等価電力に対応する電圧よりも小さいことが確認できる．

さらに Δ を減少させると，$\Delta = 0.3$ mV 付近から $I(P_X, P_{Z|X,H_E})$ は再び増加に転じる．しかし，このような領域ではビンの数に対してサンプルが不足しているため，分布の形状は本来の分布から均一な分布に近づいている．そのため，細かすぎるビンは，相互情

報量を最適化するためには不適当である．

4.2.2　大気のゆらぎの効果を計量する指標

大気の局所的な密度は温度のゆらぎや圧力の変化，風の影響によって時々刻々と変化している．そして，その密度の揺らぎは屈折率密度の局所的あるいは時間的な揺らぎとなり，大気を伝搬してきた光の強度のゆらぎであるシンチレーションや受光面におけるビーム位置の変化であるビームワンダリングなどという形で通信の品質に影響を及ぼす．ここでは，そのような大気の揺らぎの効果の指標として，光空間通信の研究において頻繁に用いられる大気の構造定数 C_n^2 と Fried パラメータの 2 つを導入する．

大気の構造定数

大気の揺らぎのダイナミクスは，乱流中におけるエネルギー輸送モデルである Kolgomorov の乱流理論によって説明される [156]．その Kolgomorov 理論の枠組みの中で，大気の揺らぎの強さを表すパラメータとして大気の構造定数 $C_n^2[\mathrm{m}^{2/3}]$ が用いられる．大気の構造定数 C_n^2 は 10^{-17} から 10^{-13} までの値を取り得て，一般的に弱い擾乱に対しては $C_n^2 = 10^{-17}$，強い擾乱に対しては $C_n^2 = 10^{-13}$ であるとされる．

この C_n^2 を実験データから求めるためには，Rytov 法 [157] から導かれる下記の式を用いる．

$$\sigma_I^2 \stackrel{\triangle}{=} \mathrm{E}\left[(\ln I - \mathrm{E}[\ln I])^2\right] = 1.23 C_n^2 k^{\frac{6}{7}} L^{\frac{11}{6}} \tag{4.8}$$

ここで，σ_I^2 は実験データ I から計算される受信強度の揺らぎを表すパラメータ，$k = \pi/\lambda$ は波数 $[\mathrm{m}^{-1}]$，L は伝搬距離 [m] である．ただし，この式は強度の揺らぎが $\sigma_I^2 < 1$ と比較的大きくない場合，かつ構造定数 C_n^2 が強度によって変化しない水平伝搬[*1]の場合にのみ適用可能である点に気をつける．

なお，計算の際には実験データから計算された強度揺らぎが受光レンズのサイズによる平均化の影響を受ける点を考慮する必要がある．水平伝搬の場合には，受光サイズが理想的に点と見なせる場合の強度揺らぎ $\sigma_I^2(0)$ と，直径 D の受光レンズを用いた場合の強度揺らぎ $\sigma_I^2(D)$ の比に関して，

$$\frac{\sigma_I^2(D)}{\sigma_I^2(0)} = \left[1 + 1.07\left(\frac{kD^2}{4L}\right)^{\frac{7}{6}}\right] \tag{4.9}$$

なる近似が知られている [158]．

以上より，実験データから $\sigma_I^2(D)$ を求めることにより，大気の構造定数を

$$C_n^2 = \frac{\sigma_I^2(D)}{1.23 k^{\frac{6}{7}} L^{\frac{11}{6}}}\left[1 + 1.07\left(\frac{kD^2}{4L}\right)^{\frac{7}{6}}\right] \tag{4.10}$$

[*1] 大気の密度は標高 h によって薄くなっていくため，一般的には大気の構造定数は h に依存する関数である．

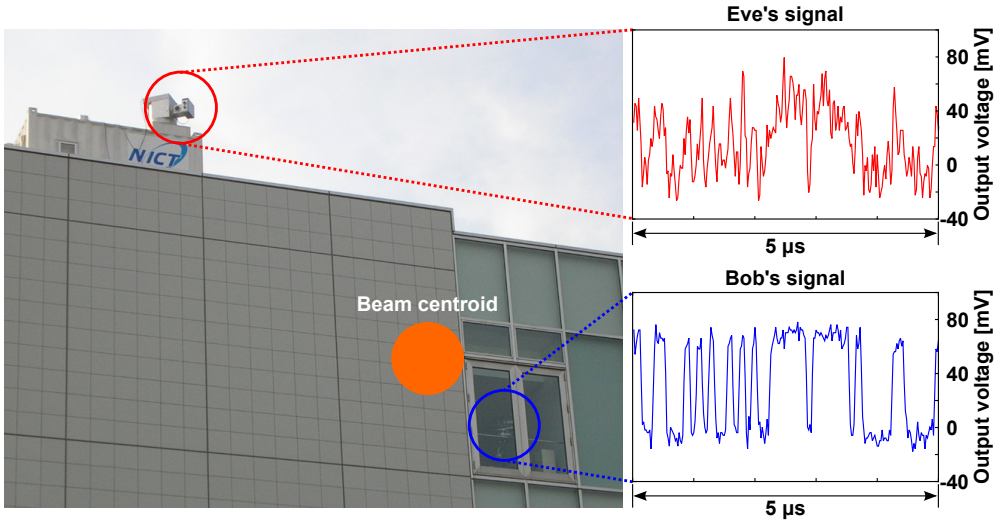

図 4.8 2015 年 11 月 17 日に行われた実験におけるビームの位置．また，グラフはボブとイブの受信電圧の 5μs における波形である．このグラフのデータは 14:43:00 に取得された．

から求めることができる [159, 160].

Fried パラメータ r_0

Fried パラメータ r_0[m] は，大気の揺らぎの中を伝搬してきたビームの波面の最小の空間コヒーレンス長であり，大気の揺らぎの強さを表すパラメータとして用いられる．定量的には，波面の収差の二乗平均平方根が 1rad である長さを r_0 とする．水平伝搬のように，大気の構造定数が標高に依らない場合には，Fried パラメータ r_0 と大気の構造定数 C_n^2 は次の式で関係付けられる [156].

$$r_0 = (0.16 C_n^2 k^2 L)^{-\frac{3}{5}} \tag{4.11}$$

4.3 通信路推定実験

本節では 2015 年 11 月 17 日 (曇り) に行われた通信路推定実験と，その実験データを基に行われた解析について述べる．

4.3.1 実験条件

まずはじめに，本実験の設定について述べる．

光空間通信において高い信頼性を得るためには，アリスのビームはボブの検出器の位置を正確に指向すべきであるが，Tokyo FSO Testbed の場合にはビームの中心をボブに向けた際に，イブの検出器の信号を受信することができなかった．本研究の目的の 1 つは，大気のゆらぎの効果が物理レイヤ暗号に及ぼす影響を定量化することにあるため，イブも

表 4.1　各時間帯におけるボブ側での受信強度のゆらぎ σ_I^2 と大気の構造定数 C_n^2 の平均値及び Fried パラメータの平均値.

実験時間	平均 σ_I^2	平均 C_n^2 [$\mathrm{m}^{-2/3}$]	r_0 [m]
14:43 - 14:46	0.076	2.17×10^{-16}	0.41
15:57 - 16:00	0.408	1.16×10^{-15}	0.15
16:33 - 16:36 (日没)	0.168	4.79×10^{-16}	0.25
17:37 - 17:40	0.034	9.69×10^{-17}	0.66
18:10 - 18:13	0.044	1.26×10^{-16}	0.57

ある程度の強度の信号が得られるように，図 4.8 中の赤円で示す位置に敢えてビームの中心を傾けた．図 4.8 の強度変化のグラフからは，ボブはほぼエラーフリーの通信状況を維持しているのに対して，イブもある程度の強度の信号を得ていることが分かる．

また，この実験を通して，0.2 [mrad/hour] 程度のビーム位置の推移を観測している．これは，ボブとイブの検出器が置かれている NICT ビルの熱膨張による効果であると考えられる．この熱膨張による効果を補正して，図 4.8 に示した幾何学的関係を保持するために，1 時間毎にビーム位置の補正を行っている．

本実験は，実験時刻による瞬時秘匿レートの変化を定性的に述べるために，14:43 - 14:46，15:57 - 16:00，16:33 - 16:36(日没)，17:37 - 17:40，18:10 - 18:13 という 5 つの時間帯で行われた．データの AD 変換に用いているオシロスコープに搭載されているメモリの都合上，1 回の伝送で取得可能なデータは 200ms 相当分までである．そのため，より多くのデータを取得するため，各時間帯毎に 200ms の伝送を 10 回行っている．既に述べたように，10MHz の帯域で擬似乱数を伝送しているため，200ms の伝送では 2×10^6 の擬似乱数系列が伝送されている．

各 200ms の伝送毎に，4ms の時間スロットで瞬時秘匿レート $R_{\mathrm{S,i}}$ を計算した．この長さの時間スロットでは，通信路ゲイン h_B と h_E が定常的であると見なすことができ，なおかつ 4×10^4 という，秘匿レートを計算する上で統計的に十分な長さのデータが含まれている．そのため，この時間スロットで計算された瞬時秘匿レートの変化に，大気の擾乱の影響が十分に反映されることが期待できる．

表 4.1 に，各実験時間帯におけるボブ側での受信強度のゆらぎ σ_I^2 と大気の構造定数 C_n^2，Fried パラメータ r_0 を示す．ここで各時間帯ごとに，10 回の 200ms 伝送毎に計算した値を平均している．また，本実験では変調信号を伝送しているため，ここでの計算のためには 0 に対応する信号は抜き去った上で計算を行っている．変調の帯域が大気の強度変化の帯域よりも十分高速であるとみなせるため，この操作は計算結果に大きな結果を及ぼさないと考えられる．実際に，当日の日の入り時刻である 16:33 以降では大気の構造定数の値は低下しており，Fried パラメータは増加している．以上の C_n^2 の振る舞いと値のオーダーは，過去にこのテストベッドを用いて実施された研究 [160] の結果とも整合性が取れている．

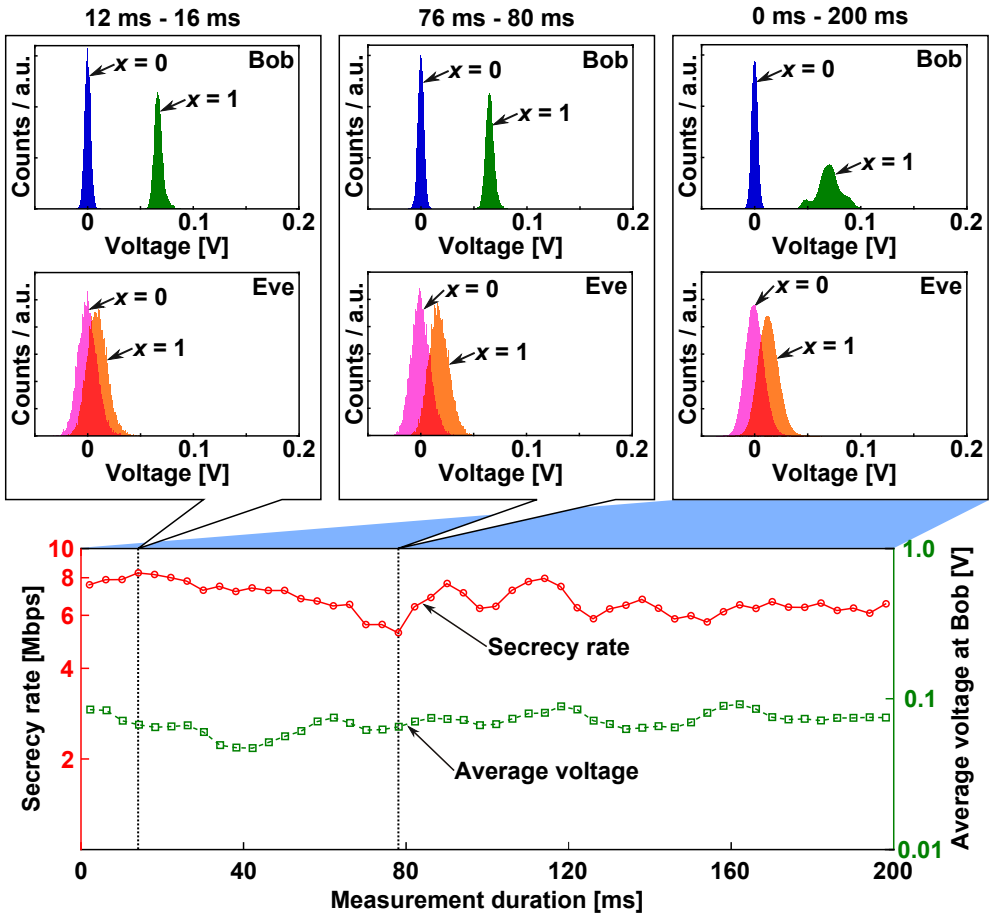

図 4.9　2015 年 11 月 17 日の日没後 1 時間 (17:37:00) における瞬時秘匿レート $R_{\mathrm{S,i}}$ の時間変化 (実線) とボブの検出器の平均出力電圧の時間変化 (点線)．瞬時秘匿レートは 4 ms 毎に，長さ 4×10^4 の系列から計算された．図上部には，瞬時秘匿レートが最大になった時間スロット (12 ms - 16 ms) と最小になった時間スロット (76 ms - 80 ms) における出力電圧のヒストグラム，そして 200 ms 全てのデータから構成したヒストグラムを示す．

4.3.2　瞬時秘匿容量の時間変化

図 4.9 と図 4.10 に，17:37:00(日没から約 1 時間後) と 16:34:20(日没直後 1 分) に行った 200ms 伝送における瞬時秘匿レート $R_{\mathrm{S,i}}$ の時間変化を実線で示す．それぞれの図における秘匿レートの時間変化を比較すると，図 4.9 では 8.30 Mbps(12 ms から 16 ms) から 5.25 Mbps(76 ms から 80 ms) の間で変化している一方で，図 4.10 では 8.75 Mbps(24 ms から 28 ms) から 0 bps(144 ms から 148 ms) と，大きな幅を持って変化している．特に，前者の時間帯 (17:37:00) では大気の状態が安定しているために最大 5.25 Mbps の情報を伝送可能である一方で，後者の時間帯 (16:34:20) では大気の揺らぎの効果が顕著であり，イブに対する突発的な情報漏えいがあるために，ワイヤタップ通信路符号化による

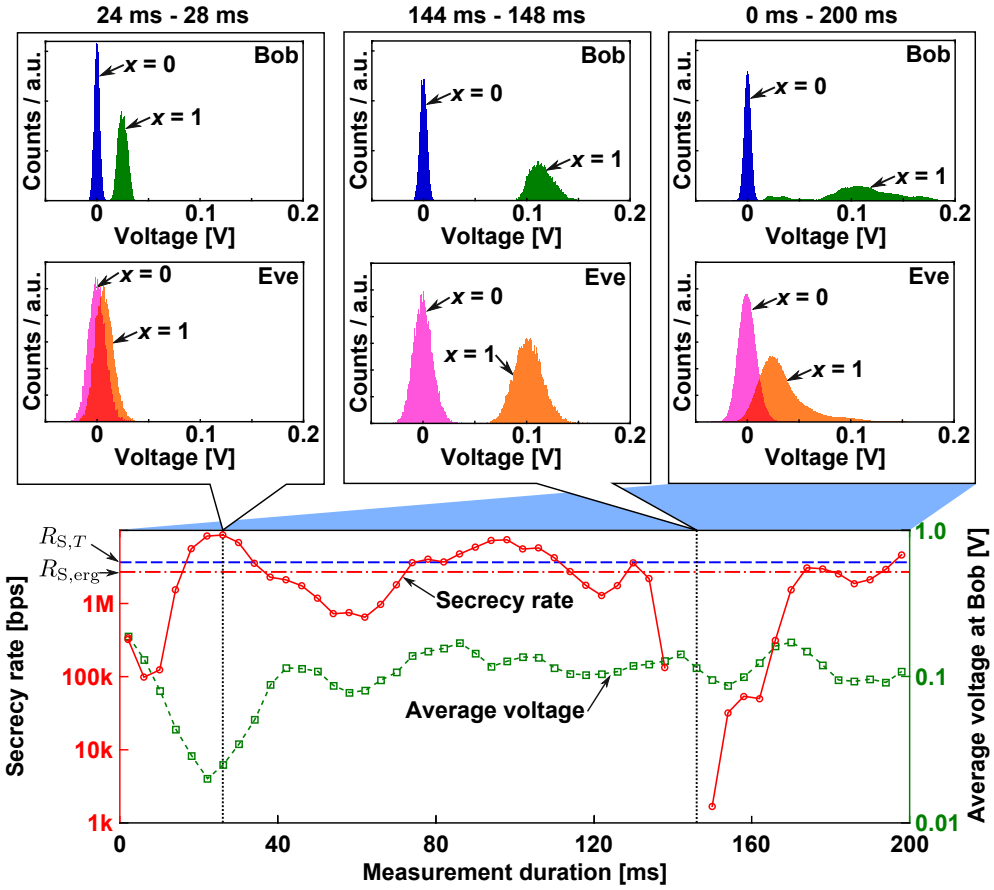

図 4.10　2015 年 11 月 17 日の日没直後 (16:34:20) における瞬時秘匿レート $R_{\mathrm{S,i}}$ の時間変化 (実線) とボブの検出器の平均出力電圧の時間変化 (点線)．瞬時秘匿レートは 4 ms 毎に，長さ 4×10^4 の系列から計算された．図上部には，瞬時秘匿レートが最大になった時間スロット (24 ms - 28 ms) と最小になった時間スロット (144 ms - 148 ms) における出力電圧のヒストグラム，そして 200 ms 全てのデータから構成したヒストグラムを示す．

一方向秘匿メッセージ伝送が困難であることを示している．

各図の上部に，秘匿レートが最大なる時間スロットと秘匿レートが最小になる時間スロットにおけるデータ，そして 200ms 間全体のデータから構築した，検出器の出力電圧分布を示す．なお，各ヒストグラムの構成の際に直流成分を補正している．また，各ヒストグラムのビン幅は，イブの相互情報量が最適になるように計算した上で，0.3mV としている．

図 4.9 の秘匿レートが最大になるスロット (12 ms から 16 ms) と最小になるスロット (76 ms から 80 ms) では，イブのヒストグラムにおける $x = 0$ に対応する分布と $x = 1$ に対応する分布は重なりを持っており，対してボブのヒストグラムでは両者は十分に離れている．このことは，明らかに盗聴者通信路は主通信路よりもエラーの多い通信路となっていることを示している．また，両時刻におけるボブとイブの分布が大きく変化していないことから，大気の状態が安定していることも確認できる．

一方で，図 4.10 の秘匿レートが最大になる時間スロット (24 ms から 28 ms) におけるイブの検出器の出力分布を見ると，図 4.9 の分布とは異なり，$x = 1$ に対応する分布と $x = 0$ に対応する分布が完全に重なっており，区別が困難になっている．そして，秘匿レートが 0 なる時間スロット (144 ms から 148 ms) では，2 つの分布が完全に分離しており，盗聴者通信路はほぼエラーフリーであると見なせることが確認できる．このような振る舞いから，この時間帯では大気の状態が不安定になり，強度が大きく変動していることが確認できる．特に，このような突発的な情報漏えいはビームワンダリングが主な要因であると考えられる．

上に述べたビームワンダリングの効果をより詳細に，あるいは定量的に議論するにはビーム中心の変化を 2 次元的に捉えることができるカメラが必要となるが，本研究の実験系にはそのような計測機器は装備されていないため，この点についての議論を行うためのデータが不足している．加えて，直径 8m にわたるビームの中心の追跡は，カメラを以ってしても困難なものとなる．しかし，Tokyo FSO Testbed は 10m 離れたボブとイブという 2 つの検出系を持つため，両者の検出系から得られた強度分布を元に計算された瞬時秘匿レートの時間変動はビームワンダリングの効果を反映していると考えられる．ただし，本実験ではボブがエラーフリーの通信を行える状況，すなわちボブが得られる相互情報量が常に 1 となる状況で測定を行っているため，瞬時秘匿レートの変化にはボブの強度変化に関する情報は含まれていない点に注意を払う必要がある．そのため，既に上で具体的な議論を行ったように，“$x = 1$”と “$x = 0$”に対応する分布間の統計的な距離の変化からビームワンダリングの効果を定量的に議論できるはずである．本研究ではその点について定量的な指標を提示するまでには至らなかったが，ビームワンダリングの定量化は物理レイヤ暗号の性能を評価する上で極めて重要であるため，今後の計測における課題となる．

ここまで議論してきた結果は，時間帯によっては大気のゆらぎの効果がワイヤタップ通信路符号化に致命的な影響を与えることを示している．アリスとボブは，図 4.10 のような突発的な情報漏えいがある時刻を避ける必要がある．ここで，表 4.1 に示したような大気のゆらぎの効果の指標となるパラメータは重要な意味を持つ．アリスとボブは，予め C_n^2 と情報漏えいが発生する確率の相関を推定しておき，通信に先立って測定した C_n^2 と比較することによってワイヤタップ通信路符号化の可否判断を行うことができる．

なお，その他の手法として，ボブの出力とイブの出力の時間変化の相関を利用する方法も考えられる．ボブの出力の平均電圧とイブの秘匿レートが相関を持つ場合には，その平均電圧から通信の可否を判断することができる．そこで，各図の点線にボブの検出器の平均出力電圧の時間変化を示すが，図 4.9 と図 4.10 からも明らかなように，両者の間に顕著な相関は見れなかった．

4.3.3 秘匿アウテージ確率

前小節の最後で，アリスとボブが通信の可否判断を行う手法について考察した．しかし，通信の状況や伝送する情報の性質によっては，機密性を上位レイヤの現代暗号の併用

により補いながらも，物理レイヤ暗号による秘匿通信を敢えて実行するという妥協案も考えられる．ここでは，伝送速度と安全性の間のトレードオフ関係を定量的に明らかにする尺度として，秘匿アウテージ確率を導入する．

秘匿アウテージ確率 $P_{\mathrm{S}}(R_{\mathrm{S,i}} < R_{\mathrm{th}})$ は，瞬時秘匿レート $R_{\mathrm{S,i}}$ が予め設定された閾値 R_{th} を下回る確率として定義される．すなわち，符号化率 R_{th} のワイヤタップ通信路符号を利用した場合に情報漏えいが発生する確率として解釈できる．そこで，以降この閾値 R_{th} を設計レートと呼ぶ．明らかに，秘匿アウテージ確率 P_{S} は設計レート R_{th} に関する単調増加な関数であり，スループットと安全性の間のトレードオフの関係を定量的に与えている．

注意 4.3.1　なお，秘匿アウテージ確率には文献によっていくつかの異なる定義が存在する [161, 162, 163]．その中には，符号化率 R_B とランダムネスレート R_E に対して個別にアウテージ確率を導入するものもある．しかし，本研究では主通信路はほぼエラーフリーであり，ボブの誤り確率については考慮する必要が無いため，上で述べた定義を導入した．□

図 4.11 に，前節で述べた 5 つの実験時間帯毎の瞬時秘匿レート $R_{\mathrm{S,i}}$ の時間変化と，秘匿アウテージ確率 $P_{\mathrm{S}}(R_{\mathrm{S,i}} < R_{\mathrm{th}})$ を計算した結果を示す．なお，前小節同様に，各時間帯において 200 ms(擬似乱数系列 20 Mbit に対応) の伝送を 10 回行っており，瞬時秘匿レートを 4 ms 毎に計算している．

明らかに，日没前の時刻では瞬時秘匿レートが大きく変化しており，秘匿アウテージ確率は 0 にならない．そのため，この時刻では安全なワイヤタップ通信路符号化は行えない．しかし，設計レートに対して秘匿アウテージ確率が判明していれば，それに合わせて現代暗号を併用するといった指標を立てることができる．すなわち，秘匿アウテージ確率は物理レイヤ暗号と現代暗号を併用する上での，クロスレイヤ的な指標を提供していると考えられる．一方で，日没後の時刻 (17:37 - 17:40 及び 18:10 - 18:13) では秘匿アウテージ確率は 1 Mbps 以下の設計レートで 0 となるため，この時刻では比較的高速なレートでワイヤタップ通信路符号化のみによる秘匿伝送が実現可能である．

4.4　符号化に関する理論的検討

前節で述べた結果は，大気のゆらぎによる突発的な情報漏えいなど，大気のゆらぎがワイヤタップ通信路符号化に及ぼす悪影響について議論を行った．一方で，本節ではそのような大気のゆらぎの影響下でも実行可能な符号化についての理論的検討を行う．

大気のゆらぎに強い符号化としては，予め異なる符号化レートの符号を複数設計しておき，受信強度変化を逐一監視し，その情報を元にして使用する符号を変更するといった方法が提案されている [90]．この方法は理論的には最適な性能を達成するものの，ボブは大気のゆらぎによる受信光の強度変化の帯域よりも十分高速なフィードバックをアリスへと行う必要があり，技術的に実現困難である．本節では，本実験の設定で実現可能な，突発

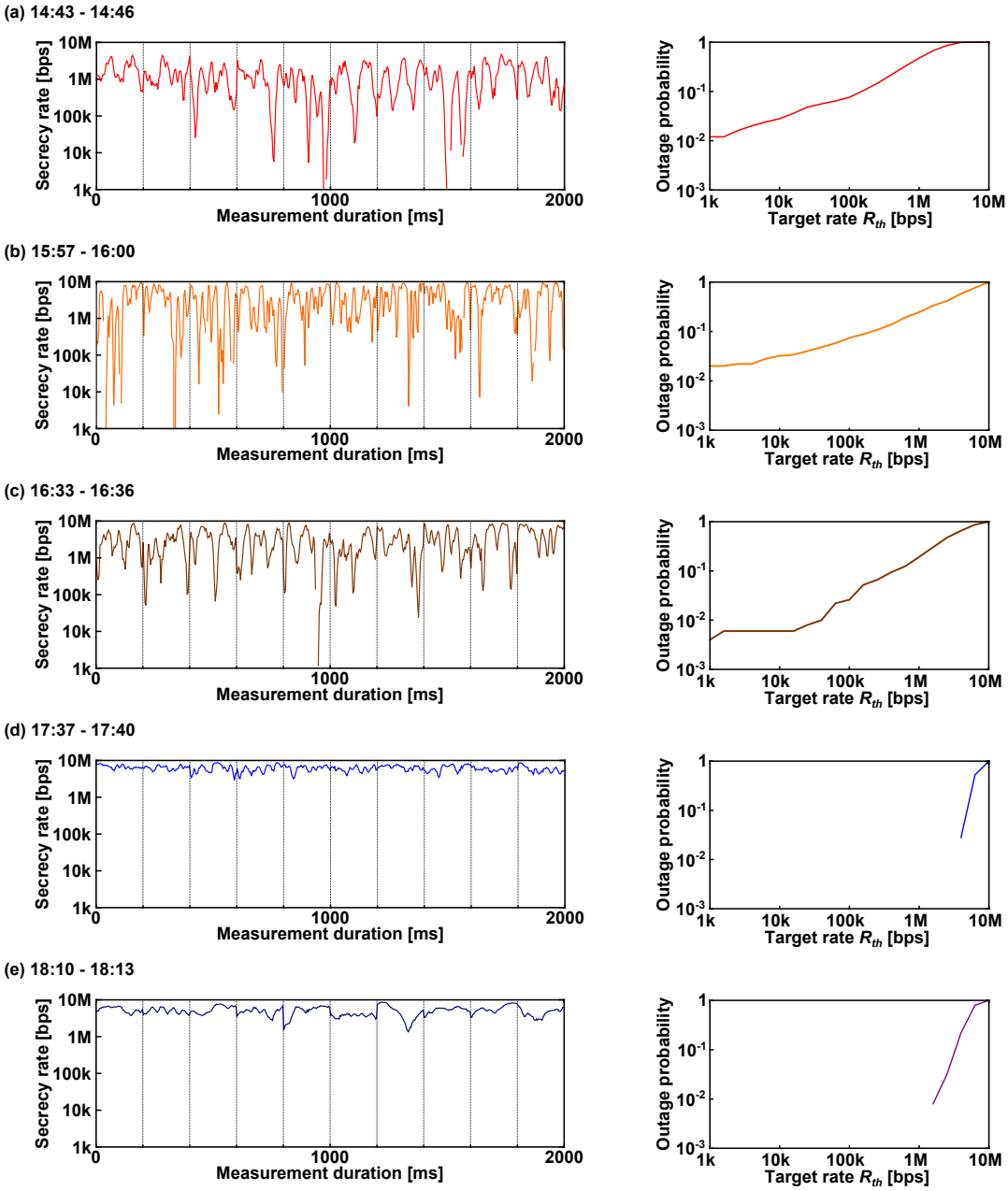

図 4.11　5 つの時間帯における，瞬時秘匿レートの時間変化と秘匿アウテージ確率.

的な情報漏えいが存在したとしても高いレートで一方向秘匿メッセージ伝送が可能な方法について提唱する.

加えて，第 2 章及び第 3 章でも行ったで導入した漏えい情報量の上界の議論をここでも行うことによって，ワイヤタップ通信路符号化の実現可能性についての検討を行う.

4.4.1　長期間に亘る符号による符号化

符号化の工夫による大気の揺らぎへの対抗策としては，大気の揺らぎの変化の時間スケールよりも長い時間をかけて一つの符号を伝送するといったものが考えられる．すなわち，突発的な情報漏えいによる効果を，時間的に平均化することで，盗聴への対抗策とする．そのためには，前章の図 4.10 の右上のヒストグラムのように，十分に長い時間に亘って取得された強度分布に基いて符号を設計する必要がある．以降，長時間に亘る強度分布を長時間確率分布と呼び，主通信路と盗聴者通信路について，それぞれ $\mathrm{E}[P_{Y|X,H_B}]$ 及び $\mathrm{E}[P_{Z|X,H_E}]$ と表記する．

長時間に亘って伝送された符号の伝送速度の限界は，長時間確率分布に基いて計算された相互情報量の差

$$R_{\mathrm{long}} \equiv I(P_X, \mathrm{E}[P_{Y|X,H_B}]) - I(P_X, \mathrm{E}[P_{Z|X,H_E}]) \tag{4.12}$$

で定義される長時間秘匿レート R_{long} によって計量される．

一方で，受信強度変化の情報から伝送する符号を変化させる場合の伝送速度の限界は，瞬時秘匿レートの単純な時間平均である平均秘匿レート $R_{\mathrm{S,erg}}$

$$\bar{R}_{\mathrm{long}} \equiv \mathrm{E}[R_{\mathrm{S,i}}(h_B, h_E)] \tag{4.13}$$

によって与えられる．ここで，E は大気の揺らぎの確率分布が分かっている場合は統計平均，実験データから瞬時秘匿レートが計算されている場合にはサンプル平均を表す．

本研究で扱ったオン-オフ変調の場合には，アリスはボブから受け取った受信強度の変化の情報を元に，入力確率分布 P_X の変更や，入力パワーの制御，場合によっては通信を中止するといった最適化が許される．そのような以上の最適化を経た上で，時々刻々と変化する強度の変化に合わせて符号化率が異なる符号を伝送することで，理想的なスループットを得ることができる．

しかし，本実験のように，入力確率分布 P_X 及び入力パワーを変更せず，なおかつ主通信路がエラーフリーであるという特殊な状況であるならば，次に議論するように，長時間秘匿レート R_{long} は平均秘匿レート $R_{\mathrm{S,erg}}$ よりも大きい値をとり得る．第 2 章で述べたように，相互情報量 $I(P, W)$ は固定された入力に対しては通信路の遷移確率 W について凸関数である．そのため，以下が Jensen の不等式 (2.8) から成立する．

$$\mathrm{E}[I(P, W)] \geq I(P, \mathrm{E}[W]) \tag{4.14}$$

この関係式を使って，

$$\begin{aligned}
\bar{R}_{\mathrm{long}} &= \mathrm{E}[I(P_X, P_{Y|X,H_B}) - I(P_X, P_{Z|X,H_E})] && (4.15)\\
&\leq I(P_X, \mathrm{E}[P_{Y|X,H_B}]) - I(P_X, \mathrm{E}[P_{Z|X,H_E}]) && (4.16)\\
&= R_{\mathrm{long}} && (4.17)
\end{aligned}$$

を得る．ここで，式 (4.16) では主通信路がほぼエラーフリーであることを利用した．

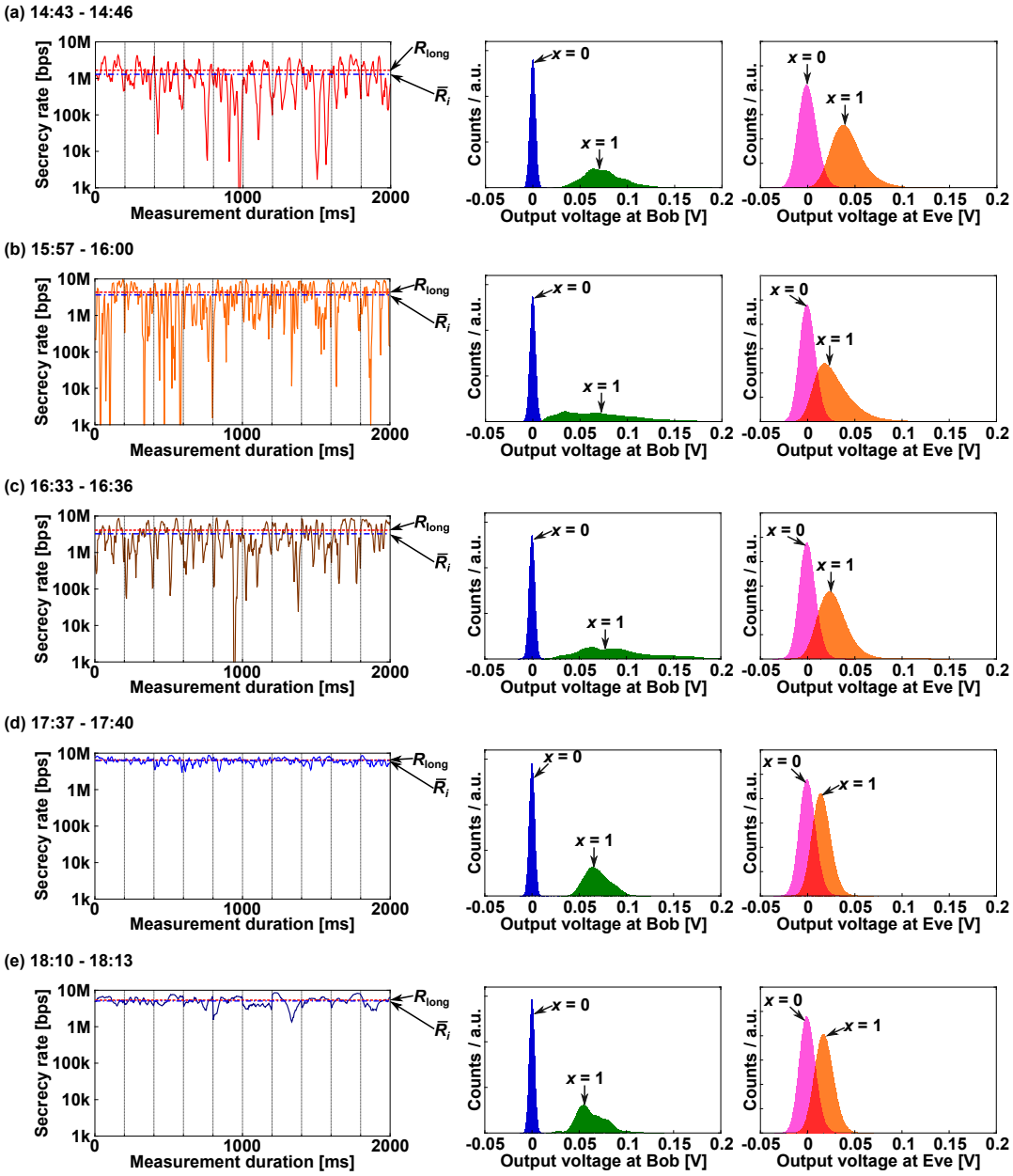

図 4.12　5 つの時間帯における，瞬時秘匿レートの時間変化と全ての実験データから構成した検出器からの出力電圧分布．なお，点線に長時間秘匿レート R_{long} と一点鎖線に平均秘匿レート $\bar{R}_{\mathrm{long}}$ を示す．

図 4.12 に，5 つの時間帯における，瞬時秘匿レートの時間変化と全ての実験データから構成した検出器からの出力電圧分布を示す．そして，秘匿レートの変化のグラフ中に，点線で長時間秘匿レート R_{long}，一点鎖線で平均秘匿レート $\bar{R}_{\mathrm{long}}$ を示す．すべての時間帯において，$R_{\mathrm{long}} > \bar{R}_{\mathrm{long}}$ が成立していることが確認できる．また，秘匿レート変動の分散が大きいほど，両者の差が大きくなっていることが確認できる．前述のように，この秘匿レートを達成するためには，大気のゆらぎによる強度変化に対応可能な，高速なフィー

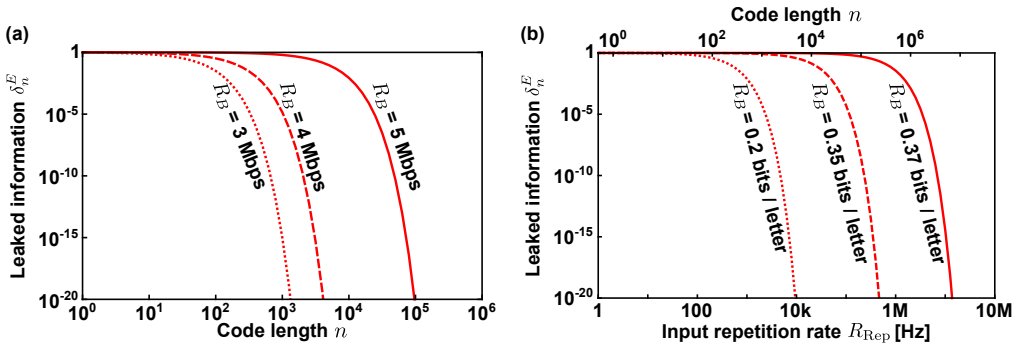

図 4.13　(a) 図 4.9 の 76ms − 80ms のタイムスロットにおける，δ_n^E の符号長依存性．(b) 図 4.10 の 200ms に亘る統計を元に計算された，漏洩情報量 δ_n^E の伝送レート依存性．

ドバックシステムが必要になる．そのため，本実験のような状況が成立するならば，長時間に亘る符号化がリーズナブルに達成可能であると考えられる．

4.4.2　有限長解析

ここまではワイヤタップ通信路符号実現に向けた通信路推定実験の解析を瞬時秘匿レートと長時間秘匿レートに基づいて行ってきた．しかし，第 2 章や第 3 章において見てきたように，符号長が有限の状況においては秘匿レートを達成することはできず，符号化レートは与えられた符号長に対して十分な誤り確率あるいは漏洩情報量が達成されるように妥協される必要があった．それらの評価量の間のトレードオフ関係を定量的に測る指標が，誤り指数及び秘匿性指数，そしてそれらから計算される復号誤り確率と漏洩情報量の符号長依存性であった．以下では，これらの量を大気のゆらぎの影響を受けている実験データに適用する方法について考察する．

はじめに，図 4.9(17:37:00) のような，大気のゆらぎの影響が少ない場合について考える．この時間帯では，大気のゆらぎの影響の小ささから突発的な情報漏えいは起きておらず，最低の瞬時秘匿レートでも 5.25Mbps(76ms-80ms の時間スロット) であった．その時間スロットで安全な符号はこの時間帯に亘って安全であると考えられることから，その時間スロットにおける統計を元に符号のデザインを行う．

符号のデザインを行う上での興味は，そのような符号化を実現するために最低限必要な符号長である．そこで，図 4.13(a) に，図 4.9 における 76ms-80ms の時間スロットの電圧分布を元にして計算した漏洩情報量の符号長依存性を示す．なお，本研究ではボブの通信路はエラーフリーであったため，復号誤り確率の計算はここでは行わない．

図 4.13(a) の点線に示したように，符号化レート R_B を 3Mbps に設定すると，$\delta_n^E < 10^{-20}$ は符号長 $n = 10^3$ で達成できる．また，4ms の時間スロット内には変調帯域 10MHz で 4×10^4 のシンボルを伝送できるため，実験条件から考えても伝送可能な符号長である．この時間スロットにおける秘匿レートは 200ms 内で最も低かったため，上

記の符号化レート及び符号長の符号はこの時間帯に亘って十分な安全性を持ったワイヤタップ通信路符号による一方向秘匿メッセージ伝送を行うことができる．破線で示した $R_B = 4$Mbps の場合には，$\delta_n^E < 10^{-20}$ を達成する符号長は $n = 10^4$ であるため，大きく増加するわけではない．一方で，実線で示した $R_B = 5$Mbps という瞬時秘匿レート $R_{\mathrm{S,i}} = 5.25$Mbps に非常に近い場合には，$\delta_n^E = 10^{-20}$ を達成するためには $n = 10^5$ の符号長が必要になる．しかし，この符号長はスロット内で伝送可能なシンボル数を超過しているため，より高速の変調を行わない限りは実現不可能である．

次に，図 4.10 のような大気ゆらぎの効果が強い時間帯 (16:34:20) について考える．前小節では，このような場合に突発的な情報漏えいを防ぐ符号化として長時間統計に基づいた符号設計を提案した．長い符号の符号化を考えた場合には，その符号の性能に加え，実装上の複雑さも考慮に入れる必要がある．

10MHz の変量レートでは 200ms 内に 2×10^6 の符号シンボルを伝送可能であるが，この符号の符号化にかかる計算量のコストを抑えて，短い符号を伝送するという戦略は十分に考えられる．そのような実装のコストを抑えるためには，符号長 n が変調レート R_{rep} とその符号を伝送する時間 T_{O} の積で $n = R_{\mathrm{rep}} T_{\mathrm{O}}$ と決定されるため，この変調レート R_{rep} を減少させればよい．

図 4.13(b) に，漏洩情報量 δ_n^E の変調レート R_{rep} に対する依存性を示している．なお符号化レートの単位は 1 つのシンボルに対する伝送情報量 ([bits/letter]) としている．符号化レートが $R_B = 0.2$ bits/letter である場合には，変調レートを $R_{\mathrm{rep}} = 10$kHz とすれば $\delta_n^E = 10^{-20}$ を達成できる．この変調レートは符号長に換算すれば $n = 2 \times 10^3$ であり，2kbps の秘密伝送レートに対応する．また，$R_B = 0.37$ bits/letter の場合には，$\delta_n^E = 10^{-20}$ を達成する変調レートは $R_{\mathrm{rep}} = 13.8$ MHz であり，符号長に換算すると $n = 2.77 \times 10^6$ である．この場合には，5.13Mbps の秘匿メッセージ伝送が実現可能である．

4.5 まとめ

本章では，NICT と電通大間を結ぶ回線長 7.8km の光空間通信テストベッドである Tokyo FSO Testbed から得られたデータから通信路の統計を構成し，それを元に，理論的解析や意味付けが容易であるワイヤタップ通信路符号化の性能を評価する諸量，すなわち，大気の状態が定常的であると見なせる時間スロット毎に計算された瞬時秘匿レートと，その秘匿レートが予め定められた閾値を下回る確率である秘匿アウテージ確率を計算し，大気のゆらぎが物理レイヤ暗号の性能に及ぼす影響に関する議論を行った．

瞬時秘匿レートのふるまいと大気の構造定数などの大気の状態を表す指標との比較から，大気のゆらぎの効果が大きい時間帯では突発的な情報漏えいが起き，ワイヤタップ通信路符号化の利用が制限されるという知見が得られた．また，秘匿アウテージ確率に対しては，物理層で定義される物理レイヤ暗号と，より上位の層で定義される現代暗号の併用のための定量的な指標という解釈を与えた．このような，実データに基づく物理レイヤ暗

号に関するリスクの定量化は，知りうる限り前例のない解析である．

さらに，長時間に亘る統計を元に符号の設計を示す方法も提示した．今回の実験で行ったような特殊な条件 (確率分布の固定，パワーの固定) 下では，長時間に亘る統計に基づく秘匿レートは，フィードバック情報を元に符号化を行う場合よりも高くなることを示した．

第 5 章

光空間通信における秘密鍵共有実証実験及び情報整合の高効率化に向けた検討

前章までは物理レイヤ暗号の最も基礎的なモデルとして，公開通信路を用いないワイヤタップ通信路符号化について，その実現可能性の理論的検討と，実データに基づく通信路推定実験を行ってきた．しかし，前章で得られた知見である，ワイヤタップ通信路符号化が急激な情報漏えいに脆弱であるという点は，実証を考える上で無視できない事実である．加えて，光空間通信における物理レイヤ暗号では，見通し回線中の広角カメラなどによる監視は前提となっていたが，この方法では急速に回線に割り込んで盗聴を行うといった攻撃を防ぐことは困難である．以上の事実を合わせると，ワイヤタップ通信路符号化の適切な運用は現実的には困難であると予想される．

一方で，物理レイヤ暗号のもう 1 つの方式である秘密鍵共有では，先に乱数を送付しておき，通信状況が劣悪であったり，回線中に不穏な動きが認められた場合にはその時間に送付された乱数を破棄するなど，後処理により安定かつ安全なイベントを選択することができる．そのため，現時点ではワイヤタップ通信路符号化よりも実用的なプロトコルであると考えられる．

本章では，上記の理由から秘密鍵共有に着目し，その心臓部とも言える秘密鍵蒸留プロトコルをプログラム実装したソフトウェアを用いて，Tokyo FSO Testbed で取得されたデータを用いて秘密鍵共有の実験を行う．はじめに，第 2 章ではやや抽象的に導入した秘密鍵蒸留の具体的な実装方法として，線形符号とユニバーサル 2 ハッシュ関数を利用した，現代の技術で実現可能なものについて述べる．次に，低密度パリティ検査 (LDPC) 符号とユニバーサル 2 ハッシュ関数に基づく鍵蒸留アルゴリズムによって，鍵を抽出する実験について述べる．その後，より光空間通信に適した方式として，Reed-Solomon 符号による情報整合を提案し，その問題点や，改善方法等について議論を行う．

5.1　秘密鍵蒸留プロトコルの実装

本節では，秘密鍵蒸留プロトコルをプログラム実装したソフトウェアを説明するに先立ち，線形符号と Toeplitz 行列を元にした秘密鍵蒸留プロトコルについて述べる．はじめに線形符号に関する最低限の基礎に述べて，その線形符号を用いて情報整合を実現する方法を述べる．そして，ユニバーサル 2 ハッシュ関数の一種である Toeplitz 行列を導入し，その高速演算法について説明する．

5.1.1　線形符号の基礎

ここでは，秘密鍵共有のプロトコルを実装する上で最低限必要な線形符号の基礎事項を述べる．なお，この節では，2 個の元からなる有限体 $\mathbb{F}_2$[*1]を考え，その元の上で定義される，2 元線形符号に限定して述べる．

$\mathbb{F}_2$ 上のベクトル空間 $\mathbb{F}_2^n$ を定義する．すなわち，$\mathbb{F}_2^n$ の元同士の可算 (減算) は要素ごとに行われ，元とスカラー $c \in \mathbb{F}_2$ の積は c をその元の要素毎に乗算することで行われる．この空間の元の集合で，可算で閉じているものを $\mathbb{F}_2^n$ の部分集合あるいは，長さ n の 2 元線形符号 $\mathcal{C}$ と呼ぶ[*2]．すなわち，線形符号 $\mathcal{C}$ の符号語 $\mathbf{x} \in \mathcal{C}$ と $\mathbf{y} \in \mathcal{C}$ の和 $\mathbf{x}+\mathbf{y}$ もその線形符号の符号語となる．

特に，長さ k のメッセージベクトル $\mathbf{m} \in \mathbb{F}_2^k$ を，長さ n の符号語 $\mathbf{x} \in \mathbb{F}_2^n$ へと符号化する線形符号を (n,k) 線形符号と呼ぶ．(n,k) 線形符号は k 個の線形独立な基底ベクトルを持つ．それらを縦に並べた $k \times n$ 行列のことを，その符号の生成行列 G と呼ぶ．そして，長さ k のメッセージベクトル $\mathbf{m}$ は符号語ベクトル $\mathbf{x}$ へと，$\mathbf{x} = \mathbf{m}G$ という操作を通じて符号化される．以上のように，生成行列 G を与えることは，(n,k) 線形符号を定義することと同値である．

以上の生成行列による定義の他に，$(n-k) \times n$ パリティ検査行列 H によって線形符号を定義する方法も存在する．すなわち，

$$\{\mathbf{x} \in \mathbb{F}_q^n | \mathbf{x}H^T = \mathbf{0}\} \tag{5.1}$$

を満足するベクトル $\mathbf{x}$ の集合をそのパリティ検査行列 H で特徴づけられる (n,k) 線形符号と呼ぶ．なお，$\mathbf{0}$ は長さ $n-k$ の零ベクトルである．

パリティ検査行列 H は，符号の誤り訂正能力と密接な関係がある．今，アリスが伝送した符号語 $\mathbf{x}$ に誤りベクトル $\mathbf{e}$ で表現される加法的な誤りが生じたベクトル $\mathbf{y} = \mathbf{x} + \mathbf{e}$ をボブが受信したとする．この受信語 $\mathbf{y}$ の右からパリティ検査行列の転置 H^T をかける

[*1] 2 元体には四則演算が定義されており，加法:$1 \oplus 1 = 0 \oplus 0 = 0$ 及び $1 \oplus 0 = 1$ と乗法:$1 \times 1 = 1$ 及び $1 \times 0 = 0 \times 0 = 0$ が成立する．

[*2] 以降，単純に線形符号とも呼ぶ．

と，線形性により，

$$\mathbf{y}H^T = (\mathbf{x}+\mathbf{e})H^T = \mathbf{e}H^T \tag{5.2}$$

が成立する．この最右辺の次元 $n-k$ のベクトルはシンドローム $\mathbf{s}$ と呼ばれ，ベクトル空間 $\mathbb{F}_2^n$ を $n-k$ 個の排反な部分空間に分割する．そのような部分空間を，誤りベクトル $\mathbf{e}$ をコセットリーダーとする，線形符号のコセットという．

このシンドローム $\mathbf{s}$ から，コセットリーダーである誤りベクトル $\mathbf{e}$ を再生し，それを伝送ベクトル $\mathbf{y}$ に加えることで符号語 $\mathbf{x}$ を推定する．以上の復号法を，シンドローム復号法と呼ぶ．

5.1.2 線形符号による情報整合

以上の線形符号を用いて情報整合を行う方法はいくつか知られている．本節では通信路符号化に基づく方法と，Slepian-Wolf 符号化に基づく方法の 2 つを導入する．

なお，Maurer が秘密鍵共有の通信路モデルの文脈で述べたような乱数送付が完了していると仮定する．すなわち，アリスは長さ n の二元の乱数 $\mathbf{x}$ を乱数源から生成し，それをボブに伝送する．ボブはこの伝送系列に誤り系列 $\mathbf{e}_B$ が加算された受信系列 $\mathbf{y} = \mathbf{x} \oplus \mathbf{e}_B$ を得る．すなわち，$\mathbf{x} = \mathbf{y} \oplus \mathbf{e}_B$ なる関係が成立する．

通信路符号化に基づく方法

線形符号で情報整合を行う 1 つの方法として，符号化に基づく方法が挙げられる．このために，ボブは自分で新たに乱数源を用意し，その乱数から生成された長さ k の新しい乱数列 $\mathbf{v}$ を符号化して長さ n の符号語 $\mathbf{v}'$ を得る．そして，その符号語 $\mathbf{v}'$ と自分の乱数列との排他的論理和をとった系列 $\mathbf{v}' \oplus \mathbf{y}$ をアリスに公開通信路で伝送する．

アリスは自分の受信系列とこの系列の排他的論理和を計算することにより，$\mathbf{v}' \oplus \mathbf{e}_B$ を得る．このとき，符号が誤り $\mathbf{e}_B$ を十分に訂正できるように設計されているならば，この誤りを取り除いて乱数 $\mathbf{v}$ が共有できたことになり，情報整合が完遂される．

Slepian-Wolf 符号化に基づく方法

ここでは，既に第 2 節で導入した Slepian-Wolf 符号化による情報整合を，線形符号で実現する方法について議論する．Slepian-Wolf の定理から，ボブは長さ n の乱数列を長さ $nH(Y|X)$ まで圧縮してアリスに伝送することによって，アリスはボブの乱数列を再生することができる．この圧縮率の限界は，アリスとボブの間の乱数送付用の通信路が二元対称通信路であるならば，線形符号を用いることで達成可能であることが Wyner[97] によって示されている．当然ながら，多くの通信路は二元対称ではないため，この性能限界まで達成することは困難である．しかし，Wyner の提唱した方法は，効率の良い Slepian-Wolf の符号化を行う上での重要な示唆を与えている．以下に，その方法を説明する．

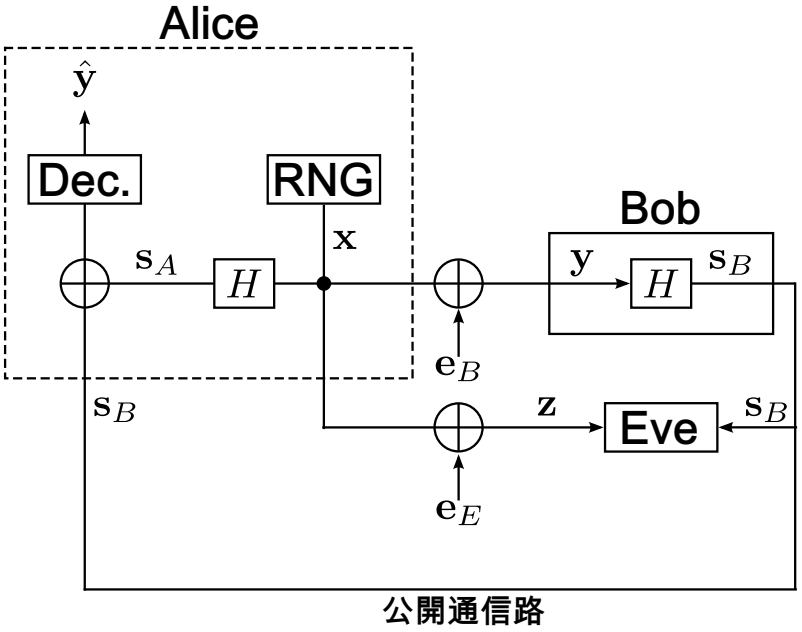

図 5.1　シンドローム圧縮に基づく情報整合.

図 5.1 に，Wyner の方法による情報整合の概念図を示す．ボブは受信系列 $\mathbf{y}$ のシンドローム $\mathbf{s}_B$ を線形符号のパリティ検査行列 H から計算し，そのシンドローム $\mathbf{s}_B = \mathbf{y}H^T$ を公開通信路でアリスに伝送する．一方，アリスも同じパリティ検査行列 H から自分が持つ系列 $\mathbf{x}$ に対応するシンドローム $\mathbf{s}_A = \mathbf{x}H^T$ を計算し，ボブの系列のシンドローム $\mathbf{s}_B$ との和を計算する．ここで，

$$\mathbf{s}_B \oplus \mathbf{s}_A = (\mathbf{y} \oplus \mathbf{x})H^T = \mathbf{e}H^T \tag{5.3}$$

が成り立つため，アリスは誤りベクトル $\mathbf{e}$ に対するシンドロームを得る．このシンドロームに対して復号処理を行うことによって，誤りベクトル $\mathbf{e}$ を再生し，そしてボブの持つ系列 $\mathbf{y} = \mathbf{x} + \mathbf{e}$ を再生することができる．

以降の 2 つの方法の違いを下記に述べる．

1. 通信路符号化に基づく方法ではボブ側にも乱数源が必要であるが，Slepian-Wolf 符号化に基づく方法ではそれは不要である．ただし，前者については長さ k の系列を長さ n の符号語に符号化したときに生じる長さ $n-k$ の系列 (これをパリティ系列と呼ぶ) を伝送する方法をとれば，ボブ側の乱数源は不要になる．
2. 通信路符号化に基づく方法，あるいはパリティ系列を伝送する方法は Slepian-Wolf の符号化に基づく方法と比較して，共有乱数に関する多くの情報をイブに開示することになるため安全性という観点から劣るという記述が見られるが，この点について情報理論的な根拠は何もない．実際に，シンドロームにはボブの誤りベクトルに関する情報しか含まれていないことは事実であるが，イブもアリスと全く同じ方法を取ることで，公開情報から自分の系列の誤りを修正できる．

3. 通信路符号化に基づく方法は符号語を伝送するため，シンドロームベクトルを伝送する Slepian-Wolf 符号化に基づく方法と比較すると公開通信路の帯域が要求される．

5.1.3 秘匿性増強：ユニバーサル 2 ハッシュ関数の高速演算

本研究では秘匿性増強を実現するユニバーサル 2 ハッシュ関数として，対角要素がすべて等しい Toeplitz 行列に着目する．その一例として，下記の 3×4 行列

$$\begin{pmatrix} c & d & e & f \\ b & c & d & e \\ a & b & c & d \end{pmatrix} \tag{5.4}$$

を挙げることができる．なお，ここで全ての文字は乱数源から供給される乱数を表すとする．

Toeplitz 行列を用いた秘匿性増強は，アリスとボブが共有した系列 $\mathbf{x}$ に対して，予め合意した Toplitz 行列を掛けるという極めてシンプルなものである．この際に，対角要素が全て等しいため，最小限の乱数を共有あるいは保持しておくことで Toeplitz 行列を構築できるという利点がある．加えて，一般的に行列とベクトルの積の計算量は入力系列長 n の 2 乗のオーダー $O(n^2)$ であるため，長い系列への秘匿性増強は計算量的に非現実的に見える．しかし，Toeplitz 行列が巡回行列の一般形であるという事実に基づき，以下に述べるような計算量を著しく低下させる手法が提案されている [105, 106].

一例として，長さ 4 の入力系列 $\mathbf{x} = \{x_1, x_2, x_3, x_4\}$ に式 (5.4) の Toeplitz 行列をかけることによる，長さ 3 の系列 $\mathbf{y} = \{y_1, y_2, y_3\}$ への圧縮を考える．この場合には

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} c & d & e & f \\ b & c & d & e \\ a & b & c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \tag{5.5}$$

という演算を実行することになる．

この行列演算を実行するにあたり，3×5Toeplitz 行列を下記に表すように，$3 + 4 - 1$ 次巡回行列へと拡張する．

$$\begin{pmatrix} c & d & e & f \\ b & c & d & e \\ a & b & c & d \end{pmatrix} \rightarrow \begin{pmatrix} c & d & e & f & a & b \\ b & c & d & e & f & a \\ a & b & c & d & e & f \\ f & a & b & c & d & e \\ e & f & a & b & c & d \\ d & e & f & a & b & c \end{pmatrix} \tag{5.6}$$

すると，式 (5.5) の計算は下記の計算と同値になる．

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \times \\ \times \\ \times \end{pmatrix} = \begin{pmatrix} c & d & e & f & a & b \\ b & c & d & e & f & a \\ a & b & c & d & e & f \\ f & a & b & c & d & e \\ e & f & a & b & c & d \\ d & e & f & a & b & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ 0 \\ 0 \end{pmatrix} \tag{5.7}$$

ここで，$\times$ は，値に関わらず無視をする成分を意味する．すなわち，長さ $3+4-1=6$ の系列 $\mathbf{y}$ の最初の 3 成分を鍵として利用する．

よく知られているように，$\mathbf{c}$ から生成される k 次巡回行列と長さ k の系列 $\mathbf{x}$ の積は

$$T'(\mathbf{c})\mathbf{x}^T = \mathcal{F}^{-1}[\mathcal{F}[\mathbf{c}] \cdot \mathcal{F}[\mathbf{x}]] \tag{5.8}$$

と，畳込みで表すことができる．ここで，$\mathbf{c}$ は巡回行列の 1 列目，$\mathcal{F}[\cdot]$ は系列の Fourier 変換，$\mathcal{F}^{-1}[\cdot]$ はその逆変換である．この Fourier 変換を高速 Fourier 変換で実行することにより，計算量は $O(n^2)$ から $O(n \log n)$ へと大幅に減少する．そのため，長い系列に対しても現実的な計算時間で秘匿性増強が実行可能である．

5.2　鍵共有ソフトウェアを利用した秘密鍵共有

本節では，秘密鍵共有の主要な機能をプログラム実装したソフトウェアを用いた秘密鍵共有実験について述べる．

ここまで述べてきたように，秘密鍵共有における秘密鍵蒸留プロトコルを構成する 2 つのプロトコルである情報整合と秘匿性増強は，それぞれ線形符号とテプリッツ行列で実現可能であった．本節で述べるソフトウェアでは，情報整合を高性能な誤り訂正符号である低密度パリティ検査 (LDPC: Low Density Parity Check) 符号で実現している．

以降，本節では LDPC 符号の概要に触れつつ，それによって情報整合を行う方法について述べる．そして，それらを実装したプログラムについて説明する．最後に，Tokyo FSO Testbed から得られたデータに対して鍵蒸留を行った結果を示す．

5.2.1　LDPC 符号による情報整合

LDPC 符号

計算機や集積回路上に実装可能な符号の研究開発を行う符号理論の歴史は古く，1950 年にはベル研の R. Hamming によって 1 つの誤りを確実に訂正可能な線形符号 (Hamming 符号) が発明されている．その後，線形符号の 1 つの完成形として，有限群上に定義される Reed-Solomon 符号が 1964 年に提案されるが，情報理論が導き出す理論限界 (Shannon 限界) からは程遠い性能であった．

一方で，Gallager は自身の博士論文 [80] において，グラフ理論に基づく復号方法によって，Shannon 限界に近い性能を持つ符号の存在を示していた．この符号は疎 (1 より 0 の

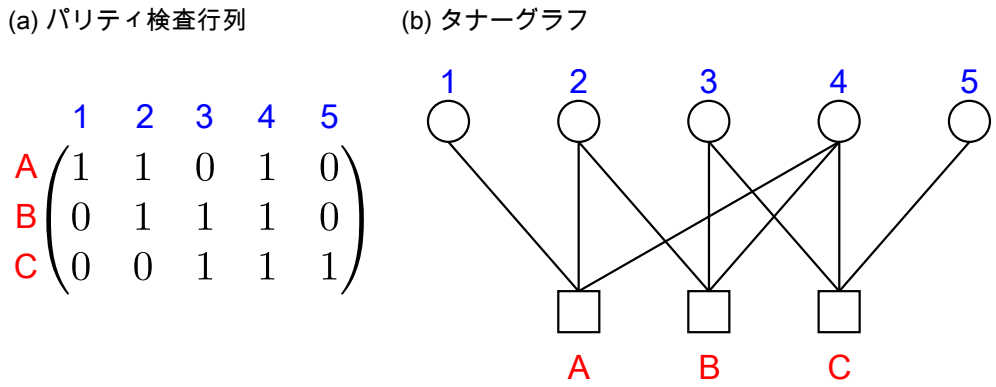

図 5.2　(a) パリティ検査行列．(b) 対応するタナーグラフ．

方が圧倒的に多い) なパリティ検査行列を持つため，低密度パリティ検査行列 (LDPC) 符号と呼ばれることとなる．しかし，1960 年代当時の実装技術では効率的な実装が行えず，結果として 1990 年代の再発見まで忘れ去られることとなる．

LDPC 符号の最大の特徴は，復号をグラフ理論上の問題に帰着させたことにある．図 5.2(a) に示したある符号のパリティ検査行列に対して，図 5.2(b) のようなタナーグラフを描くことができる．図 5.2(b) 中の丸は変数ノードと呼ばれ，パリティ検査行列の各列に対応している．一方四角はチェックノードと呼ばれ，パリティ検査行列の各行に対応している．パリティ検査行列中の i 行 j 列の要素が 1 であった場合，j 番目の変数ノードと i 番目のチェックノードが線 (エッジ) で結ばれることになる．

LDPC 符号の復号アルゴリズムは和積アルゴリズムと呼ばれ，このエッジで結ばれたノード間で尤度などの情報をやり取りすることによって行われる．このアルゴリズムの計算量はエッジの本数に依存する．そのため，1 の数が少ない，すなわちエッジの本数が少ない LDPC の場合は効率的な計算量的に効率的な復号を行うことができる．

LDPC 符号による情報整合

本節で述べるソフトウェアでは，LDPC を用いた情報整合を行う．具体的な情報整合のフローは後の節に譲り，ここでは本ソフトウェアに実装された LDPC のパラメータについて述べる．

本ソフトウェアには，通信路の状態が変化し，ビット誤り確率が変化する状況においても利用できるように，複数の符号化率 R_{LDPC} を持つ LDPC 符号が実装されている．ここで，符号化率は LDPC の符号長 n に対するメッセージビット k の比 $R_{\mathrm{LDPC}} = k/n$ として定義される．アリスとボブは通信路の状態に合わせて適切な符号化率を選択する必要があるが，本研究ではボブが受信したビット列から少数のビットをランダムに選び出し，それをアリスに公開通信路で送り返して誤り確率 P_e の推定を行うという方法をとっている．

表 5.1 に，本ソフトウェアに実装されている LDPC 符号について，誤り率 P_e と符号

表 5.1　ソフトウェアにおけるビット誤り率と LDPC の符号化率 R_{LDPC} の関係

ビット誤り率 P_e	符号化率 R_{LDPC}	通信路容量 C
0	1	1
$0 < P_e < 0.01$	0.85	$0.955 < C < 1$
$0.01 \leq P_e < 0.02$	0.85	$0.919 < C \leq 0.955$
$0.02 \leq P_e < 0.03$	0.75	$0.888 < C \leq 0.919$
$0.03 \leq P_e < 0.04$	0.70	$0.859 < C \leq 0.888$
$0.04 \leq P_e < 0.05$	0.65	$0.831 < C \leq 0.859$
$0.05 \leq P_e < 0.06$	0.60	$0.806 < C \leq 0.831$
$0.06 \leq P_e < 0.07$	0.55	$0.781 < C \leq 0.806$
$0.07 \leq P_e$	0.50	$C \leq 0.781$

化率 R_{LDPC}，そして誤り率 P_e から推定される通信路容量 C の 3 つを示す．ここで，通信路はビット反転確率が $P_e/2$ である二元対称通信路を仮定している．この表から明らかなように，いくら Shannon 限界に近いとされる LDPC であっても，通信路容量から 0.1 ビットから 0.3 ビット低いレートとなっている．後に見るように，この理論と実装の差によって，理論上は鍵共有が可能でも，実際には秘密鍵共有が失敗する場合も存在する．

なお，本ソフトウェアはボブからアリスへの，符号語を送る形式での後方情報整合を行うため，ボブのソフトウェアには符号化を行うための生成行列，アリスのソフトウェアには復号に用いるためのパリティ検査行列が符号化率 R_{LDPC} 毎に記憶ストレージに格納されている．

5.2.2　鍵蒸留ソフトウェア概要

図 5.3 に，本研究で利用した鍵蒸留ソフトウェアの動作フローを説明する．

はじめに，アリスは長さ $n + r$ の乱数列をボブに対して伝送し，ボブはクロック抽出や同期処理などを経て，誤りが加わった長さ $n + r$ の受信系列を得る．ボブは誤り率 P_e を推定するために，受信系列から r ビットをランダムに抽出し，アリスに公開通信路で伝送する．アリスはボブから送られてきた r ビットの系列と，自身の乱数列のうち対応するビットを比較することでビット誤り率 P_e を計算し，その値から表 5.1 に従って LDPC の符号化率 R_{LDPC} を決定し，その情報をボブに伝送する．なお，本研究ではここまでのフローは Mathematica で作成したプログラムにより行っている．

このソフトウェアでは LDPC 符号の符号語を伝送することで情報整合を行う．ボブは，自身が持つ物理乱数源から nR_{LDPC} ビットの乱数を生成し，それを符号化率 R_{LDPC} の LDPC 符号の符号語に符号化する．その符号語と n ビットの受信系列の排他的論理和をとり，その結果の系列を公開通信路でアリスに伝送する．

アリスはビット誤り率の計算に用いた r ビットを取り除いた残りの伝送系列と，ボブが

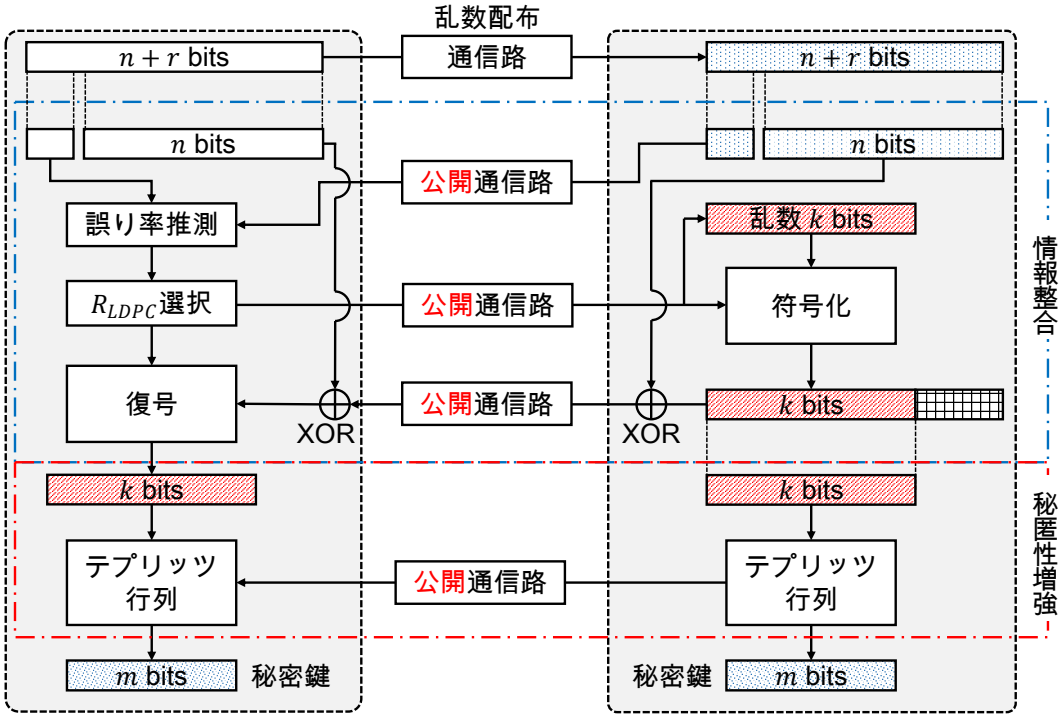

図 5.3　LDPC で情報整合を行う鍵蒸留フロー．

伝送した系列の間で XOR を計算することによって，ボブの系列が被ったエラーと同じ誤りが発生した LDPC の符号語を得る．アリスはこの LDPC の符号語を復号器に入力することで，長さ nR の乱数列を復号できる．

その後，イブの相互情報量から Toplitz 行列を設計し，それに共有したビット列をかけることによって秘匿性増強を行い，鍵ビットを生成する．そして，アリスとボブは MD5 と呼ばれるハッシュ関数により自身の鍵のダイジェストメッセージを求め，それを互いに比較することによって，秘密鍵蒸留プロトコル成否の判断を行う．この検査をクリアした乱数列を鍵として利用することができる．

5.2.3　実験結果

ここでは Tokyo FSO Testbed から得られたデータに対して，前小節で説明したプログラムによって鍵蒸留を行った結果を示す．なお，実験は 2016 年 10 月 16 日に行われた．当日の天気は曇りであり，日没の時刻は 17:05 であった．

本実験では得られた 200ms(=2M サンプル) 分の PN15 段 (図 4.3 参照) データの内，はじめの 32767 サンプルをフレーム同期に用い，残りの $1024 \times 1024 + 64000 = 1112576$ サンプルを鍵蒸留プログラムに入力した．ここで，ビット誤り確率の推定のために乱択抽出されるサンプルの数を 64000 としたため，情報整合プロトコルへの入力は 1048576 サンプルである．

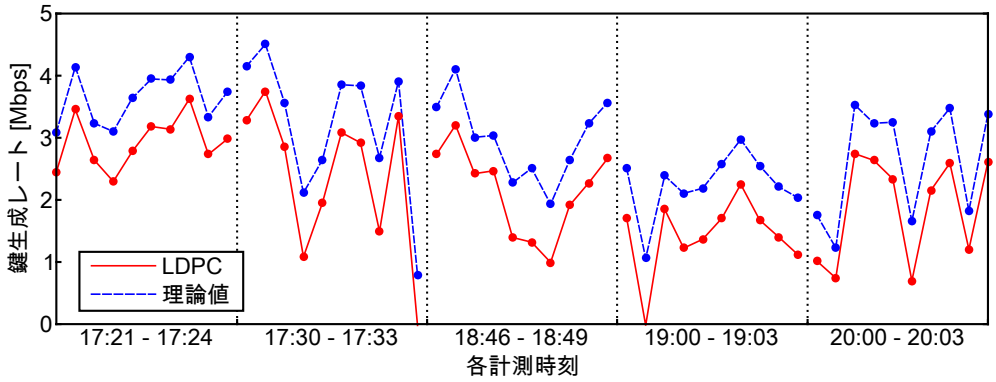

図 5.4　2016 年 10 月 16 日に行われた実験データに対する秘密鍵蒸留結果．各点において，1112576 サンプルが鍵生成に利用されている．

第 2 章において，情報整合と秘匿性増強を行った場合の秘密鍵レート R_{K} は

$$R_{\mathrm{K}} = I(X;Y) - I(Y;Z) \tag{5.9}$$

であると述べた．ここで，ボブの相互情報量 $I(X;Y)$ は硬判定，イブの相互情報量 $I(Y;Z)$ は軟判定により計算されている (第 4 章参照)．しかし，実際には情報整合は LDPC を用いており，ボブの相互情報量 $I(X;Y)$ は表 5.1 に示した LDPC の符号化率 R_{LDPC} に置き換わる．以上より，実際の鍵長 k は

$$k = 1024 \times 1024(R_{\mathrm{LDPC}} - I(Y;Z)) \tag{5.10}$$

となる．なお，Renner による汎用的安全性基準の上界 (定理 2.4.2) の議論では，その証明においてユニバーサル 2 ハッシュ関数の利用を前提としているため，イブの相互情報量について修正を加える必要は無い．

図 5.4 に，横軸を実験を行った時間帯，縦軸を bps 換算した鍵レートにとった，鍵蒸留プロトコルを実行した結果を示す．ここで，実線は LDPC により情報整合を行った結果 (5.10) であり，破線は情報理論から導かれた値 (5.9) である．また，ビーム位置は第 4 章における実験よりも，イブ側に近づけているため，アリスとボブ間の通信路はエラーフリーではない．

ほぼ全ての時間に亘って，理論値 (5.9) が LDPC による値 (5.10) よりも数 Mbps 程度大きくなっている．これは，LDPC 符号のレート (表 5.1) と理論的に導かれる相互情報量との間のギャップに起因する．既に述べたように，ボブからの逆方向情報整合を行う場合には式 (5.9) の理論値は必ず 0 に大きくなるが，いくつかの時間で LDPC による値 (5.10) が 0 になっている．これは，LDPC 符号のレートが相互情報量 $I(Y;Z)$ よりも小さくなったために，秘密鍵蒸留が失敗している現象に対応する．

結果として，このプログラムを用いることによって，光空間通信における秘密鍵共有が実証されたことになる．ここでの鍵レートは平均で数 Mbps であり，無線電波通信における鍵レートよりも高いオーダーの鍵共有が潜在的に行えることが実験により示された．

5.3 Reed-Solomon 符号を用いた情報整合の理論的検討

前節では，Shannon 限界を達成する符号の代表として LDPC 符号を利用した情報整合を行ったが，LDPC 符号の適正性にはいくつかの議論の余地が存在する．例えば，衛星等の機器に搭載する場合には，計算機能力や電力等の制約が存在するため，符号化/復号に計算機の能力を要する LDPC とはよりも軽量に動作する符号が好ましい．以上の理由から，本節では LDPC 符号の代案として，Reed-Solomon 符号による情報整合の理論的検討を行う．

5.3.1 Reed-Solomon 符号

本節では Reed-Solomon(以下，RS) 符号について述べる．RS 符号は LDPC 符号 [80] や Polar 符号 [81] のように Shannon 限界に迫る性能はないものの，それでも高い誤り訂正能力を持ち，CD や DVD，地上デジタル放送など，幅広い分野において利用されている．

RS 符号は，有限体 (付録 B.1 を参照)$\mathbb{F}_{2^m}$ 上に定義される線形符号である．特に，符号長 $n = 2^m - 1$，メッセージ長 k である RS 符号を (n, k)RS 符号と呼ぶ．(n, k)RS 符号は，$t = (n - k)/2$ 個の誤りシンボルを訂正可能である．

一般的な線形符号同様，生成行列[*3]を元に定義することもできる．しかし，ここでは公開通信路で伝送する情報が少なくて済む，シンドロームを伝送する Slepian-Wolf 符号化に基づく情報整合を想定し，RS 符号をパリティ検査行列で定義する．

(n, k)RS 符号のパリティ検査行列は，

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(2t-1)} & \alpha^{2(2t-1)} & \cdots & \alpha^{(2t-1)(n-1)} \end{pmatrix} \tag{5.11}$$

で与えられる．ここで，α は有限体 $\mathbb{F}_{2^m}$ を定義している規約多項式の根である．

着目すべきは，パリティ検査行列の構造が完全に決定しているという点である．前節で扱った LDPC 符号のパリティ検査行列の各要素はランダムに決定されていた．そのため，複数の符号化率を持つ LDPC 符号を設計して通信状況に応じて使い分ける際には，それぞれの符号に対応したパリティ検査行列をデザインして記憶しておく必要がある．また，前節のプログラムのように，情報整合の過程に符号化を伴う場合には，パリティ検査行列から生成行列を作り出し，それも保持しておく必要がある．特に，パリティ検査行列が疎

[*3] RS 符号の符号語を巡回シフトしたベクトルも RS 符号の符号語となる．このような性質を持つ線形符号のクラスを巡回符号と呼ぶ．巡回符号の符号語は行列ではなく，多項式で表現したほうが扱いが容易になるため，生成行列よりも生成多項式で定義する方が一般的である．

であっても，生成行列が疎であるとは限らないため，一般的には生成行列が多くの記憶ストレージを消費する．

一方で，RS 符号のパリティ検査行列 (5.11) は，α と訂正可能シンボル数 t が与えられてさえいれば帰納的にシンドロームを計算することができる．誤りが t 個発生している場合には，RS 符号の符号語 $(x_0, x_1, \cdots, x_{n-1})$ から，そのシンドロームの各成分を

$$s_j = \alpha^{j(n-1)} x_{n-1} + \alpha^{j(n-2)} x_{n-2} + \cdots + \alpha x_1 + x_0 \tag{5.12}$$

のように計算し，$j = 1$ から $j = 2t$ までを伝送すれば良い．特に，このシンドロームの計算は，多項式の計算を高速に行うアルゴリズムとして知られるホーナー法により，

$$s_j = (\cdots \alpha^j (\alpha^j x_{n-1} + x_{n-2}) + \cdots + x_1) + x_0 \tag{5.13}$$

と変形することで高速に計算可能であることが知られている [164]．

加えて，[165] でも指摘されているように，このようなパリティ検査行列の構造は，誤り訂正能力の動的な調節が可能であることを示唆している．即ち，ボブが $2t$ 要素のシンドロームをアリスに伝送し，結果として情報整合に失敗した場合には，アリスがボブにシンドロームの再送要求を行い，ボブは $2t + 1$ 要素以降のシンドロームを再伝送することによって，全ての誤りの訂正が可能となる．LDPC 符号に基づく情報整合が失敗した場合には，異なる符号を選択し直し，新しい符号語を伝送し直すことになる．しかし，イブはボブの系列とイブの系列の間に発生した誤りの情報をそれ以前に伝送した符号語を通して得ているため，新しい符号の再伝送は安全性の観点から現実的でない．RS 符号で実現可能なシンドロームの追加伝送は，必要最低限のシンドロームを伝送すれば十分であるため，この問題を回避することができる．

5.3.2 ハミング符号を内符号としたビット訂正

前小節では RS 符号を用いる場合の利点について指摘をしたが，ここでは問題点について述べる．様々な通信システムで使われている RS 符号に $(255, k)$RS 符号というものが存在するが，この符号は有限体 $\mathbb{F}_{2^8}$ 上で定義されているため，情報整合のプロセスにおいて，ビットシンボル $(\{0, 1\})$ からバイトシンボル $(\{0, 1, \cdots, 255\})$ への変換過程が必要となる．しかし，このような変換は，乱数列長を 1/8 にするため，符号語内でのシンボル誤り率の相対的な増加を引き起こす．従って，最終的なシンボル誤り率増加による復号の計算量が増大する問題や，あまつさえ符号語そのものを破棄せざるを得ないといった問題が引き起こされる可能性がある．

上記の問題点を解決するための方法として，本研究では符号の組み合わせを提案する．すなわち，ビット誤りを訂正する短い符号と，それが訂正しきれなかった誤りを訂正するために誤り符号を利用することによって，上記の問題点の解決を図る．このような手法は，誤り訂正符号の文脈では連接符号と呼ばれている．

本研究では，ビット誤りを訂正する符号 (連接符号の文脈になぞらえて，内符号と呼ぶ) として (7,4) ハミング符号を選択した．この符号は符号長 7，メッセージ長 4 で，1 個の

誤りを訂正することができる．そのパリティ検査行列は以下の式で与えられる．

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{5.14}$$

この行列は，長さ 3 の列ベクトルを $(0,0,0)^T$ を除いて全て並べた行列である．

長さ 7 の符号語に 1 つの誤りだけが生じていた場合には，そのシンドロームとして，誤りの位置に対応する列ベクトルが出力される．一方で，2 つ以上の誤りが発生していた場合には，確実に誤りの存在を発見できるものの，1 つだけ発生している誤りと区別がつかない．また，パリティ検査行列の 3 つの列ベクトルの組の内，線形独立でない組が存在するため，3 つ以上の誤りについては誤りの発見すら行えない場合がある．以上より，ハミング符号は 1 誤り訂正-2 誤り検出が可能な符号である．

このハミング符号を内符号とし，RS 符号を外符号とした情報整合アルゴリズムについて述べる．はじめに，ボブは入力ビット列を 7 ビット毎に分割し，それぞれについてハミング符号のシンドロームを計算する．なお，このアルゴリズムの問題点は，3/7 のビットが犠牲になるというハミング符号の符号化率が生成レートのボトルネックとなる点である．そのため，予め入力波形の分散に対して閾値を計算しておき，分散が低いビット列に対してはハミング符号によるビット訂正はスキップする．次に，長さ 7 のビット列に予め定めておいた 1 ビットを連接して長さ 8 のビット列にし，それを 1 バイトに変換する．この処置は，隣接するバイト列に対する誤り伝搬を防ぐためである．以上の処置後，RS 符号によってシンドロームを計算する．公開情報としては，ハミング符号と RS 符号のシンドロームが含まれる．

アリス側では，伝送されてきたハミング符号のシンドロームからボブのビット列の再生を行う．この過程で，7 つのビット列の内に 1 つだけの誤りビットがあればそれが訂正されるが，2 つ以上の誤りビットは訂正されずにむしろ訂正の過程で誤りが増加する．しかし，7 ビットの内に生じた複数のビット誤りは変換の過程で 1 つのバイト誤りになるため，その後のプロセスや誤り訂正の能力には影響を与えない．そして，ボブ同様に予め定めていたビットを連接した後に 8 ビットを 1 バイトに変換し，RS 符号のシンドロームからボブのバイト列を再生する．

この情報整合により共有できる乱数列の長さ $N_{\mathrm{H,RS}}$ は入力乱数列の長さを N，分散が低い条件で受信できた乱数列の長さを N_{good}，RS 符号のシンドロームの長さを S_{RS} とすると，

$$N_{\mathrm{H,RS}} = N_{\mathrm{good}} + \frac{4}{7}(N - N_{\mathrm{good}}) - 7S_{\mathrm{RS}} \tag{5.15}$$

によって概算できる．

5.3.3 各方式による情報整合の比較

図 5.5 に，図 5.4 のデータを元に概算した，LDPC 符号と RS 符号，そして RS 符号と Hamming 符号 (点線) の組み合わせによる情報整合を行った場合の効率について比較し

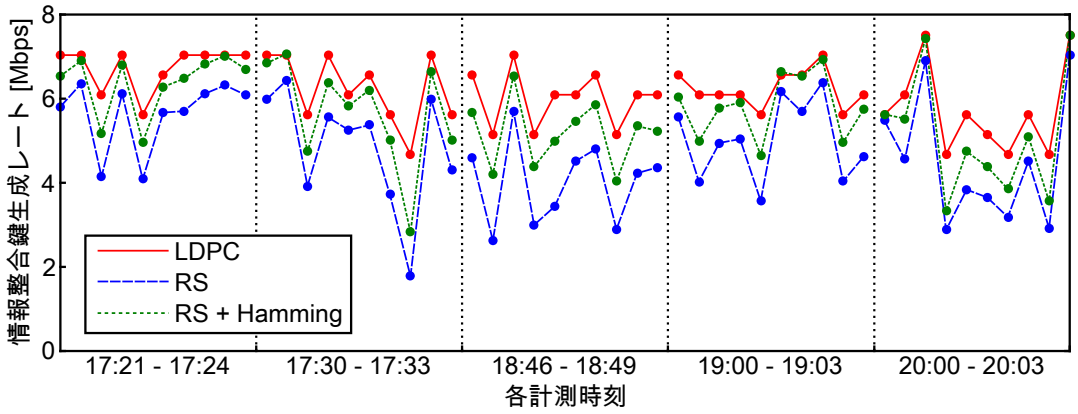

図 5.5　LDPC(実線)，(255,k)RS 符号 (破線)，(255,k)RS 符号と Hamming 符号 (点線) の組み合わせ符号による情報整合のレートの比較.

た．LDPC 符号 (実線) の符号化率は理論限界ではなく，データから計算された誤り確率を元に，表 5.1 に記載されている値を用いている．対して，RS 符号 (破線) の効率については，2040 ビット (=255 バイト) 毎における誤り数を求めておき，その誤りを全て訂正するために必要なシンドロームの数から計算している．そして，RS 符号と Hamming 符号の組み合わせ (点線) 効率については，式 (5.15) から概算している．以上より，単純比較は可能ではないが，それでも現在実装されているシステムと比較して，RS 符号による情報整合がどれだけの性能を潜在的に持ちうるかのベンチマークを行うことはできる．

LDPC 符号と RS 符号の比較からは，RS 符号の情報整合が圧倒的に効率が低いことが分かる．これは，上でも述べたように，ビット列からバイト列への変換過程において符号語内の誤り確率が相対的に増加するためである．一方で，Hamming 符号を同時に用いることによって，RS 符号の効率が増加していることが確認できる．しかし，一部の実験データでは LDPC の効率に迫る性能をマークしているものの，全体としては LDPC の方がまだ高い効率であると言わざるを得ない．以上の結果から，今回提案した情報整合では LDPC の高い効率を破るには至らなかったと結論できる．

5.4　まとめ

本章では，実用的な物理レイヤ暗号プロトコルとして秘密鍵共有に着目し，その実証に関する研究を扱った．

はじめに，秘密鍵共有用に作成した秘密鍵蒸留プログラムによって，Tokyo FSO Testbed から得られたデータに対する秘密鍵蒸留を行った．本実験はイブの位置などを決めた模擬的な実験に過ぎないが，それでも光空間通信による秘密鍵共有が潜在的に数 Mbps の鍵共有が可能であることが示された．電波無線通信における秘密鍵共有が数百 bps 程度のレートであったことと比較すると，劇的な増加であると言える．

次に，LDPC 符号による情報整合と RS 符号による情報整合の比較を行った．結果とし

ては，LDPC 符号による情報整合がより効率的であったが，RS 符号には下記の利点が存在している．

1. 現状でより軽量な実装が可能であり，衛星通信などにおける実績があること．
2. フィードバックによりシンドロームの追加計算が可能であること．

そのため，軽量な暗号が求められる移動通信ネットワークへの実装に向けて，RS 符号による秘密鍵交換は一考の余地がある．

本研究では Hamming 符号との組み合わせによって高効率化を図ったが，その他の符号 (BCH 符号など) を組み合わせることによって，更なる効率化も期待できる．その意味で，本研究は RS 符号による情報整合を否定したわけではなく，より軽量かつ高効率な情報整合を実装するための知見を与えている．

第 6 章

結論

本章では，本研究の総括を行う．

まず，図 6.1 を用いて，当該研究分野におけるこれまでのマイルストーンをまとめ，その中での本研究の位置付け，及び今後の展望について概説する．次に，本研究で行った事項をまとめ，これまでの当該分野の研究の流れの中での意義について説明する．最後に，今後の展望及び，本研究を起点として発展が期待される技術について述べる．

6.1　物理レイヤ暗号の研究の流れを振り返って

歴史上，最初に提唱された物理レイヤ暗号の方式は，通信路符号化に情報理論的安全性を担保する機能を加えた，ワイヤタップ通信路符号化 [66, 67] であった．そして，ワイヤタップ通信路符号化のエッセンスを取り込みつつ，既に Bennett と Brassard らによって提唱されていた QKD と同様の鍵共有を古典通信路を用いて実現する方法として，秘密鍵共有方式 [68, 69] が提案された．

その後，ワイヤタップ通信路符号化は理論的方向に研究が進み，Han らによる通信路 Resolvability[71] を契機として，漏えい情報量の有限長解析 [74, 73, 79] という，Gallager[77] がすでに提唱していた誤り確率に対する上界と合わせて，実用的な符号設計にも利用できる理論が登場する．しかし，光空間通信への実現に向けた研究については，近年になってようやく理論的研究が行われている一方で，符号設計に関する研究あるいは実験は手付かずの状態であった．

一方で，秘密鍵共有は，ワイヤタップ通信路符号化と比較すると電波無線分野における膨大な実験成果 (e.g. [110, 113, 116]) が報告されているが，それらは QKD の学術分野としての発達に牽引されていくこととなる．特に，QKD の領域で確立された，秘密鍵の蒸留を情報整合 [94, 95] と秘匿性増強 [94, 96] という 2 つのプロトコルに分離して実装するという手法は，後に Renner[132] によって理論的に一般化されたことも相まって，電波無線通信における秘密鍵共有においても用いられていくことになる．しかし，光空間通信における秘密鍵共有は未だ実証されていなかった．

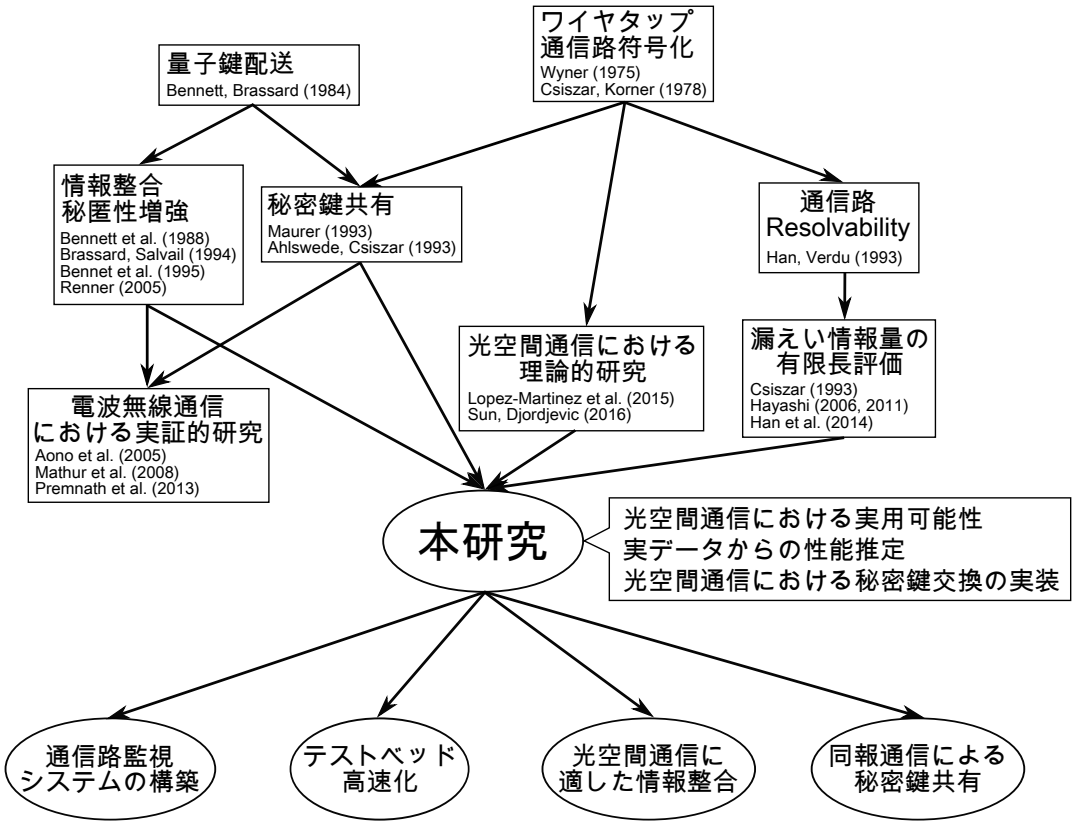

図 6.1　当該分野におけるマイルストーン的研究，その中での本研究の位置付け，及び今後の展望に関する俯瞰図.

6.2　本研究の意義

次に，各章で取り扱った主要な成果とその歴史的な意義付けを行う.

6.2.1　第 3 章

はじめに，入力にコスト制約が課されているワイヤタップ通信路符号化の定式化を行い，その誤り指数と秘匿性指数について，Han ら [79] が証明していなかった性質の証明を行った．これは，通信路 resolvability の研究に端を発した漏洩情報量の有限長解析という，情報理論における先端領域における一つの到達点である Han らの理論に，さらなる基礎付けを行ったことを意味する．特に，本研究で述べた方法とは異なる手法で導出された Gallager の指数との比較を行い，その不備を明らかにし，Han らの指数は Gallager の指数よりも広いクラスの通信路の評価に適用可能であるという知見を得た点は，情報理論における歴史を鑑みても大きな意味を持つ.

次に，光パルスのオン-オフ変調という物理的モデルを設定した上で，ワイヤタップ通信路符号化の秘匿レート (秘匿容量) を数値的に求め，その結果を無条件安全性が証明さ

れている QKD の秘密鍵レートと比較することによって，QKD と物理レイヤ暗号の関係に関する定量的な議論を行った．これは，既存の光空間通信における物理レイヤ暗号の理論研究では語られて来なかった，物理レイヤ暗号の既存の暗号技術における立ち位置を定量的に明らかにする，極めて重要な知見である．

最後に，コスト制約付きのワイヤタップ通信路符号化の誤り指数と秘匿性指数による有限長解析の例を示した．すなわち，Han らの情報理論における最先端理論を用いることで，与えられた物理モデルに対して，LDPC 符号などの現在実装されている技術によるワイヤップ通信路符号の実現可能性を議論できた．この点は，漸近的な評価量だけを与えてきた既存の数値計算の結果などと比較しても，より実用的な知見を述べていると言える．

6.2.2 第 4 章

光空間通信における物理レイヤ暗号の実験を行える設備としては世界に類を見ない，NICT と電通大間を結ぶ回線長 7.8km の光空間通信テストベッドである Tokyo FSO Testbed を利用して，大気の揺らぎに関するデータを取得し，そのデータを元にして，瞬時秘匿レートの時間変化や秘匿アウテージ確率などといった，物理レイヤ暗号における典型的な量を評価した．

既存の研究においては理論的な状況を設定した上で，モンテカルロ法や解析計算によって上記の評価量を与えていた．対して，本研究では実データを用いて上記の量を評価しているため，より実際の使用状況に沿った，大気の揺らぎが物理レイヤ暗号の性能に及ぼす効果を捉えることに成功している．さらには，第 3 章同様の有限長解析の理論をここでも用いることにより，符号のデザインに関したより実用的な知見を述べることにも成功している．

6.2.3 第 5 章

本章では秘密鍵共有における主要な処理である，情報整合と秘匿性増強を実装したソフトウェアを用いて，Tokyo FSO Testbed から得られたデータに対して秘密鍵蒸留を行い，数 Mbps の鍵共有を生成する実証実験を行った．既に電波無線通信では大気のゆらぎの効果を鍵に用いるために数百 bps 程度のレートの鍵しか生成できないことを述べていたが，本研究のように秘密鍵をアリスから光変調で伝送することによって，より高速な秘密鍵共有が可能であることを示したことになる．

また，今後の実用的符号化実装に向けて，RS 符号による情報整合の理論的検討を行った．結果としては LDPC を凌駕する程の性能を出すことはできなかったが，本研究で述べた知見 (フィードバックによるシンドローム追加計算，その他の符号との組み合わせによる高効率化) は，より軽量かつ高速な情報整合を行う上で有用である．

6.3　今後の展望

本研究は光空間通信における物理レイヤ暗号の実現に向けた先駆として位置付けられる研究である．そのため，本研究では扱いきれなかった未解決の問題や，より実際的なネットワークインフラへの実装など多くの課題が残されているのも事実である．

本研究では秘密鍵共有の主要な処理を実装した鍵蒸留ソフトウェアを開発し，それを利用した秘密鍵共有の実証実験を行った．しかし，物理レイヤ暗号において符号化の処理と同様に重要な要素は，イブの通信路へのアクセスを合理的に制約するための手法である．光空間通信における物理レイヤ暗号では，アリスとボブが広角カメラで回線を常に監視可能であると仮定していた．そこで，そのような回線監視システムの実際の開発が喫緊の課題となる．当然ながら，アリスとボブが回線の監視を手動で行うのは非現実的であり，両者が持つカメラの焦点を変化させて 3 次元的な走査を行う，画像認識により不穏な動きを察知した瞬間に通信を遮断するといった，アクティブな監視ないしは遮断機能を備えていることが望ましい．そして，そのような監視システムを用いた場合の，イブが得られる情報量の上限などの安全性に関わる理論的議論も必要となる．

また，今回の研究では Tokyo FSO Testbed にて帯域 10MHz の擬似乱数伝送を行い，大気のゆらぎが物理レイヤ暗号に及ぼす影響について議論を行った．しかし，光空間通信が有する広大な帯域と比較すると，これは非常に低い伝送レートであると言わざるを得ない．数 Gbps のような高速度の伝送では，大気のゆらぎのタイムスケールである数 ms 程度も一つのビットに対しては十分に長いスケールとなる．そのため，本研究において議論した大気のゆらぎの効果は，高速変調の通信においてまた違った容貌を呈すると予想される．ひいては，本論で議論したものとは，また異なった安全性上のリスクが発生する可能性もある．以上より，伝送システムを高速化した上での性能推定実験は大きな意味を持つ．

本研究で利用した情報整合は， QKD において培われた技術を転用しており，従って，0 あるいは 1 というビット列に対する処理となっている．しかし，古典光空間通信はアナログ値を情報として利用できるので，例えば明らかに受信条件が悪くなっているイベントは棄却するなどの処理を行うことが可能である．そのような古典通信の特徴を強く意識した設計により，単なる QKD の技術転用以上の性能を持つ情報整合を実現可能であることが期待できる．そのため，今回 RS 符号による検討を行ったように，様々な線形符号を元にして，大気のゆらぎの効果に強い情報整合の方法を模索することが，より高速な秘密鍵共有の実現につながる．

現代暗号が現在のセキュリティインフラにおいて広く用いられてきた理由として，計算機上に実装でき，物理的媒体に無依存であることが挙げられるのは第 1 章で述べた通りである．もう 1 つの理由として，公開鍵基盤というインフラを利用して，複数ユーザー間で鍵を交換可能であるという点を挙げられる．本研究では 1 体 1 での秘密鍵共有を扱ったが，上記の現代暗号に纏わる経緯を鑑みると，複数ユーザー間での鍵共有を行うことが

できれば，秘密鍵共有のセキュリティインフラにおける実用性を大きく引き上げることなる．一つの可能性としては，人工衛星のような送信ターミナルから発せられた送信光ビームの広がりの中に複数のドローンや成層圏プラットフォームのような移動体受信ターミナルが集結してブロードキャスト型の秘密鍵共有を行い，その後，各移動体ターミナルが次のミッションに向けて場所を移動し，新たな送信あるいは中継プラットフォームとなることでダイナミカルにネットワークを構成するといった方法が考えられる．これにより，衛星から複数の成層圏プラットフォーム，そして各成層圏プラットフォームから複数のドローンへといった，ヒエラルキー型のネットワーク構造を柔軟に構成できるようになることが期待される．以上のような鍵のブロードキャストは，双方向での強度変化から鍵を抽出する電波無線通信における秘密鍵共有では実現が困難である，光空間通信特有の実装であると言える．この方向の理論的研究では Csiszár らによるもの [142] が知られているが，1 対多というトポロジー，各機器に搭載可能な質量及びエネルギー制約を考慮した上で，注意深く秘密鍵蒸留ソフトウェアをデザインする必要がある．

付録 A

第 3 章の各定理の証明について

この章では，第 3 章で述べた定理について，証明を省略したものを記載する．

A.1　定理 3.1.2 の証明

この定理の証明は [79, Appendix B] にて与えられているが，そこでは V- 制約も課された場合についての詳細な証明が省略されていた．そのため，ここでその証明を行う．

初めに，復号誤り確率 ε_n^B に対する上界 (3.12) を示す．確率分布 P_X に対する X- 制約 (3.5) と，確率分布 P_V に対する V- 制約 (3.8) がそれぞれ満足されているとしよう．系列 $\mathbf{x} \in \mathcal{X}^n$ と $\mathbf{v} \in \mathcal{V}^n$ に対して，それぞれの系列が加法的コスト制約を満足しているならば 1 を値に取るような指標関数を導入する：

$$\chi(\mathbf{x}) \stackrel{\triangle}{=} \begin{cases} 1 & \text{for } \sum_{i=1}^{n} c(x_i) \leq n\Gamma \\ 0 & \text{otherwise} \end{cases}, \tag{A.1}$$

$$\bar{\chi}(\mathbf{v}) \stackrel{\triangle}{=} \begin{cases} 1 & \text{for } \sum_{i=1}^{n} \bar{c}(v_i) \leq n\Gamma + n^a \\ 0 & \text{otherwise} \end{cases} \tag{A.2}$$

ここで，a は $1/2 < a < 1$ を満足する任意の実数である．そして，X- 制約と V- 制約を満足する系列 $\mathbf{x}$ と $\mathbf{v}$ の生成確率を

$$\mu_n \stackrel{\triangle}{=} \sum_{\mathbf{x}} \chi(\mathbf{x}) \prod_{i=1}^{n} P_X(x_i) \tag{A.3}$$

$$\bar{\mu}_n \stackrel{\triangle}{=} \sum_{\mathbf{x}} \chi(\mathbf{v}) \prod_{i=1}^{n} P_V(v_i) \tag{A.4}$$

とそれぞれ定義する．

ここで，μ_n を

$$\begin{aligned}\mu_n &= P_{X^n}(\mathcal{X}^n(\Gamma)) \\ &= \sum_{\mathbf{v}\in\mathcal{V}^n} P_{X^n|V^n}(\mathcal{X}^n(\Gamma)|\mathbf{v})P_{V^n}(\mathbf{v}) \end{aligned} \tag{A.5}$$

と書き直す．Markov の逆不等式 (補題 2.1.2 を参照) により，$E[P_{X^n|V^n}(\mathcal{X}^n(\Gamma)|\mathbf{v})] = 1-\lambda$ ならば，

$$\Pr\{V^n \in \mathcal{T}_0\} \geq 1-\sqrt{\lambda} \tag{A.6}$$

が成立する．ここで，$\mathcal{T}_0 \stackrel{\triangle}{=} \{\mathbf{v} : P_{X^n|V^n}(\mathcal{X}^n(\Gamma)|\mathbf{v}) \geq 1-\sqrt{\lambda}\}$ である．従って，$1-\mu_n$ を上式の λ に代入すると，

$$\alpha_n \stackrel{\triangle}{=} P_{V^n}(\mathcal{T}_0) \geq 1-\sqrt{1-\mu_n} \stackrel{\triangle}{=} \beta_n \tag{A.7}$$

$$\gamma_n(\mathbf{v}) \stackrel{\triangle}{=} P_{X^n|V^n}(\mathcal{X}^n(\Gamma)|\mathbf{v}) \geq \beta_n \quad \text{for all } \mathbf{v}\in\mathcal{T}_0 \tag{A.8}$$

を満足する集合 $\mathcal{T}_0 \subset \mathcal{V}^n$ の存在が示される．

さらに，$\sum_{i=1}^n c(x_i) < n\Gamma$ ならば，中心極限定理により $\lim_{n\to\infty}\mu_n = 1$ が成り立ち，一方加法的コスト制約が等式で満足される (すなわち，$\sum_{i=1}^n c(x_i) = n\Gamma$) ならば，$\lim_{n\to\infty}\mu_n = 1/2$ が成り立つ．このことから，$\sum_{x\in\mathcal{X}} P_X(x)c(x) < \Gamma$ ならば，$\lim_{n\to\infty}\alpha_n = \lim_{n\to\infty}\beta_n = \lim_{n\to\infty}\gamma_n(\mathbf{v}) = 1$ ($\mathbf{v}\in\mathcal{T}_0$) となり，$\sum_{x\in\mathcal{X}} P_X(x)c(x) = \Gamma$ ならば，$\liminf_{n\to\infty}\alpha_n = \liminf_{n\to\infty}\gamma_n(\mathbf{v}) \geq \lim_{n\to\infty}\beta_n = 1-1/\sqrt{2}$ となることが分かる．さらに，$1/2 < a < 1$ ならば，$\lim_{n\to\infty}\bar{\mu}_n = 1$ も成り立つ．

よって, $\mathbf{v}\in\overline{\mathcal{T}}_0$ なる系列 $\mathbf{v}$ の生成確率と，そのような $\mathbf{v}$ が与えられた場合の $\mathbf{x}$ の条件付き確率を

$$\tilde{P}_{V^n}(\mathbf{v}) \stackrel{\triangle}{=} \frac{P_{V^n}(\mathbf{v})}{\bar{\alpha}_n} \quad (\mathbf{v}\in\overline{\mathcal{T}}_0) \tag{A.9}$$

$$\tilde{P}_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \stackrel{\triangle}{=} \frac{P_{X^n|V^n}(\mathbf{x}|\mathbf{v})}{\gamma_n(\mathbf{v})} \quad (\mathbf{x}\in\mathcal{X}^n(\Gamma)\mathbf{v}\in\overline{\mathcal{T}}_0) \tag{A.10}$$

として得る．ここで，$\bar{\alpha}_n = P_{V^n}(\overline{\mathcal{T}}_0)$ であり，$\overline{\mathcal{T}}_0 \stackrel{\triangle}{=} \mathcal{T}_0 \cap \{\mathbf{v}\in\mathcal{V}^n | \bar{\chi}(\mathbf{v}) = 1\}$ である．また，明らかに $\liminf_{n\to\infty}\bar{\alpha}_n \geq 1-1/\sqrt{2}$ が成立する．

上記の指標関数を ε_n^B の指数的上界に組み込むために，$\chi(\mathbf{x})$ と $\bar{\chi}(\mathbf{v})$ の上界を

$$\chi(\mathbf{x}) \leq \exp\left[(1+\rho)r\left(n\Gamma - \sum_{i=1}^n c(x_i)\right)\right] \tag{A.11}$$

$$\bar{\chi}(\mathbf{v}) \leq \exp\left[s\left(n\Gamma + n^a - \sum_{i=1}^n \bar{c}(v_i)\right)\right] \tag{A.12}$$

のように導入する．ここで，$r \geq 0$ と $s \geq 0$ である．

ここで，確率分布に対する制約を満足する確率分布 $\tilde{P}_{V^n}(\mathbf{v})$ と $\tilde{P}_{X^n|V^n}(\mathbf{x}|\mathbf{v})$ を，一般のワイヤタップ通信路についての復号誤り確率の上界 (2.35) の式中の P_{V^n} と式 (2.33) 中

の連接通信路の確率分布関数 $P_{X^n|V^n}(\mathbf{x}|\mathbf{v})$ に代入すると，

$$\begin{aligned}
\varepsilon_n^B &\leq 2(M_nL_n)^\rho \sum_{\mathbf{y}} \left(\sum_{\mathbf{v}} \tilde{P}_{V^n}(\mathbf{v}) \bar{\chi}(\mathbf{v}) W^{n+}(\mathbf{y}|\mathbf{v})^{\frac{1}{1+\rho}} \right)^{1+\rho} \\
&\leq \frac{2(M_nL_n)^\rho}{\bar{\alpha}_n} \sum_{\mathbf{y}} \left(\sum_{\mathbf{v}} P_{V^n}(\mathbf{v}) \bar{\chi}(\mathbf{v}) W^{n+}(\mathbf{y}|\mathbf{v})^{\frac{1}{1+\rho}} \right)^{1+\rho} \\
&\leq \frac{2(M_nL_n)^\rho e^{s(1+\rho)n^a}}{\bar{\alpha}_n} \sum_{\mathbf{y}} \left(\sum_{\mathbf{v}} P_{V^n}(\mathbf{v}) \exp\left[s\left(n\Gamma - \sum_{i=1}^n \bar{c}(v_i) \right) \right] W^{n+}(\mathbf{y}|\mathbf{v})^{\frac{1}{1+\rho}} \right)^{1+\rho}
\end{aligned} \tag{A.13}$$

と

$$\begin{aligned}
W^{n+}(\mathbf{y}|\mathbf{v}) &= \sum_{\mathbf{x}\in\mathcal{X}^n(\Gamma)} W_B^n(\mathbf{y}|\mathbf{x}) \tilde{P}_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \\
&= \frac{1}{\gamma_n(\mathbf{v})} \sum_{\mathbf{x}} \chi(\mathbf{x}) W_B^n(\mathbf{y}|\mathbf{x}) P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \\
&\leq \frac{1}{\gamma_n(\mathbf{v})} \sum_{\mathbf{x}} W_B^n(\mathbf{y}|\mathbf{x}) P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \times \exp\left[r(1+\rho)\left(n\Gamma - \sum_{i=1}^n c(x_i) \right) \right] \\
&\leq \frac{1}{\beta_n} \sum_{\mathbf{x}} W_B^n(\mathbf{y}|\mathbf{x}) P_{X^n|V^n}(\mathbf{x}|\mathbf{v}) \times \exp\left[r(1+\rho)\left(n\Gamma - \sum_{i=1}^n c(x_i) \right) \right]
\end{aligned} \tag{A.14}$$

を得る．これらを合わせることで，ε_n^B についての上界を得る．

次に，漏えい情報量に対する上界 (3.13) を示す．しかし，その導出は，ここまで行ってきた議論において ρ と $-\rho$ とするだけで成り立つため，ここでは省略する． □

A.2 補題 3.1.1 の証明

補題 3.1.1 の証明には下記の補題が必要となる．

定理 A.2.1 任意の入力確率分布 P_V，通信路 W，補助通信路 $P_{X|V}$，定数 $-1 \leq \rho \leq 1$ について，関数 $\phi(\rho|W, P_V, r, s)$ は変数の組 (r, s) の凹関数である． □

証明: 付録 A.3 を参照のこと． □

初めに，性質 1 を示す．式 (3.9) において，$n \to \infty$ ならば $\kappa_n \to 0$ であるから

$$F_c(P_V, R_B, R_E, \infty) \stackrel{\triangle}{=} \sup_{r\geq 0, s\geq 0} \sup_{0\leq\rho\leq 1} [\phi(\rho|W_B, P_V, r, s) - \rho(R_B + R_E)] \tag{A.15}$$

となる．ここで，$\rho = 0$ が式 (A.15) の右辺の ρ についての最大化を達成するための条件は，式 (A.15) の右辺を ρ で微分することにより

$$R_B + R_E = \phi_\rho(0|W_B, P_V, r, s) \tag{A.16}$$

と求められる．ここで，関数の下添字は対応する変数による偏微分を表す．さらに，式 (A.15) の右辺の r と s についての最大化を達成する r と s を求めるために，

$$\begin{aligned} f(r,s) &\stackrel{\triangle}{=} \phi(\rho=0|W_B,P_V,r,s) \\ &= -\log\left[\sum_{v\in\mathcal{V}}\sum_{x\in\mathcal{X}} P_V(v)P_{X|V}(x|v)e^{s[\Gamma-\bar{c}(v)]+r[\Gamma-c(x)]}\right] \end{aligned}$$

と置く．すると，

$$f(0,0)=0, \tag{A.17}$$

$$f_r(0,0) = -\left(\Gamma - \sum_{x\in\mathcal{X}} P_X(x)c(x)\right) \le 0 \tag{A.18}$$

$$f_s(0,0) = -\left(\Gamma - \sum_{v\in\mathcal{V}} P_V(v)\bar{c}(v)\right) \le 0 \tag{A.19}$$

が成立することが分かる．ここで不等式は，入力確率分布に対するコスト制約 (3.7) が満足されているという仮定による．従って，式 (A.17)-(A.19) と定理 A.2.1 から，$\phi(0|W_B,P_V,r,s)$ は $r=s=0$ において，最大値 0 を取ることが示される．即ち，式 (A.16) は

$$R_B + R_E = \phi_\rho(0|W_B,P_V,0,0) \tag{A.20}$$

へと帰着される．この式の右辺が $I(q,W_B^+)$ と等しいことは容易に確かめられる (cf. Gallager [77])．よって，性質 1 は示された．同様の方法で性質 2 も示される．性質 3 と 4 は Gallager[77] と同様の手法で示される．

A.3 補題 A.2.1 の証明

関数 $\phi(\rho|W,P_V,r,s)$ の凹性を示すに当たり，以下の関数の凸性を示す．

$$\phi(r,s) \stackrel{\triangle}{=} \log\left[\sum_{u\in\mathcal{U}}\left(\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\left[\sum_{x\in\mathcal{X}}\epsilon(v,x,u)e^{rg(x,t)}\right]^{\frac{1}{t}}\right)^t\right]$$

ここで，

$$\begin{aligned} \epsilon(v,x,u) &= W(u|x)P_{X|V}(x|v) \\ t &= 1+\rho \in [0,2] \\ f(v) &= \Gamma - \bar{c}(v) \\ g(x,t) &= t(\Gamma - c(x)) \end{aligned}$$

と定義した．

第 2 章で述べたように，関数 $\phi:(r,s)^T \to \boldsymbol{R}$ が (r,s) の凸関数であることと，関係式

$$\mathbf{v}^T H \mathbf{v} \ge 0 \tag{A.21}$$

が任意のベクトル $\mathbf{v} = (r, s)^T$ に対して成立することは同値であった．式 (A.21) の H はヘッセ行列と呼ばれ，

$$H \triangleq \begin{bmatrix} \phi_{rr}(r,s) & \phi_{rs}(r,s) \\ \phi_{rs}(r,s) & \phi_{rr}(r,s) \end{bmatrix}$$

と定義される．なお，以降この証明において，関数の下添字は対応する変数による偏微分を表すとする．例えば，関数 $\phi_{ss}(r,s)$ は関数 $\phi(r,s)$ の変数 s による二階偏微分を表す．

初めに，変数 $t = 1+\rho$ が $t \in (0,2]$ である場合について示す．$t = 0$(すなわち，$\rho = -1$) については，極限に関する議論が必要になるため，後ほど証明を行う．記述の簡単のために，

$$\begin{aligned} \phi(r,s) &= \log \psi(r,s) \\ \psi(r,s) &\triangleq \sum_{u \in \mathcal{U}} \alpha(r,s)^t \\ \alpha(r,s) &\triangleq \sum_{v \in \mathcal{V}} P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}} \\ \beta(r) &\triangleq \sum_{x \in \mathcal{X}} \epsilon(v,x,u) e^{rg(x,t)} \end{aligned}$$

と置く．関数 $\phi(r,s)$ について $\mathbf{v}^T H \mathbf{v}$ を示すために，これらの関数についていくつかの不等式を導入する．

初めに，$\beta(r)$ の r による一階及び二階偏微分

$$\begin{aligned} \beta_r(r) &= \sum_{x \in \mathcal{X}} g(x) \epsilon(v,x,u) e^{rg(x,t)} \\ \beta_{rr}(r) &= \sum_{x \in \mathcal{X}} g(x)^2 \epsilon(v,x,u) e^{rg(x,t)} \end{aligned}$$

と $\beta(r)$ について，Cauchy-Schwartz の不等式から，不等式

$$\beta_{rr}(r)\beta(r) \geq \beta_r(r)^2 \tag{A.22}$$

が成立する．

次に，$\alpha(r,s)$ の各変数について偏微分を計算すると下記のようになる．

$$\begin{aligned} \alpha_r(r,s) &= \frac{1}{t} \sum_{v \in \mathcal{V}} P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}-1} \beta_r(r) \\ \alpha_s(r,s) &= \sum_{v \in \mathcal{V}} f(v) P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}} \\ \alpha_{rr}(r,s) &= \frac{1}{t} \sum_{v \in \mathcal{V}} P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}-2} \left[\beta(r)\beta_{rr}(r) + \left(\frac{1}{t} - 1 \right) \beta_r(r)^2 \right] \\ \alpha_{rs}(r,s) &= \frac{1}{t} \sum_{v \in \mathcal{V}} f(v) P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}-1} \beta_r(r) \\ \alpha_{ss}(r,s) &= \sum_{v \in \mathcal{V}} f(v)^2 P_V(v) e^{sf(v)} \beta(r)^{\frac{1}{t}} \end{aligned}$$

ここで，不等式 (A.22) を援用すると，

$$\alpha_{rr}(r,s) \geq \frac{1}{t^2}\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}-2}\beta_r(r)^2 \tag{A.23}$$

なる不等式が成立する．以上の $\alpha(r,s)$ の各偏微分とその不等式について，下記の不等式が成立する．

$$\begin{aligned}
&\alpha(r,s)\left[r^2\alpha_{rr}(r,s)+2rs\alpha_{rs}(r,s)+s^2\alpha_{ss}(r,s)\right]\\
&\geq \left[\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}}\right]\left[\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}-2}\right.\\
&\qquad\left.\times\left(\frac{r^2}{t^2}\beta_r(r)^2+2\frac{rs}{t}f(v)\beta(r)\beta_r(r)+s^2f(v)^2\beta(r)^2\right)\right]\\
&\geq \left[\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}}\right]\left[\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}-2}\left(\frac{r}{t}\beta_r(r)+sf(v)\beta(r)\right)^2\right]\\
&\geq \left[\frac{r}{t}\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}-1}\beta_r(r)+s\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\beta(r)^{\frac{1}{t}-1}\beta(r)\right]^2 \qquad \text{(A.24)}\\
&= (r\alpha_r(r,s)+s\alpha_s(r,s))^2 \qquad \text{(A.25)}
\end{aligned}$$

ここで，不等式 (A.24) では Cauchy-Schwartz の不等式を利用した．

最後に，$\psi(r,s)$ の変数 r と s についての偏微分を求めると

$$\psi_i(r,s) = t\sum_{u\in\mathcal{U}}\alpha(r,s)^{t-1}\alpha_i(r,s) \tag{A.26}$$

$$\psi_{ij}(r,s) = t\sum_{u\in\mathcal{U}}\alpha(r,s)^{t-2}[\alpha(r,s)\alpha_{ij}(r,s)+(t-1)\alpha_i(r,s)\alpha_j(r,s)] \tag{A.27}$$

となる．なお，下添字 i と j は r または s を表す．従って，不等式 (A.25) を利用すると，

$$\begin{aligned}
&\psi(r,s)\left(r^2\psi_{rr}(r,s)+2rs\psi_{rs}(r,s)+s^2\psi_{ss}(r,s)\right)\\
&= t\psi(r,s)\sum_{y\in\mathcal{Y}}\alpha(r,s)^{t-2}\left[(t-1)(r\alpha_r(r,s)+s\alpha_s(r,s))^2\right.\\
&\quad\left.+\alpha(r,s)(r^2\alpha_{rr}(r,s)+2rs\alpha_{rs}(r,s)+s^2\alpha_{ss}(r,s))\right]\\
&\geq \psi(r,s)\left(t^2\sum_{y\in\mathcal{Y}}\alpha(r,s)^{t-2}(r\alpha_r(r,s)+s\alpha_s(r,s))^2\right)\\
&\geq \left(rt\sum_{y\in\mathcal{Y}}\alpha(r,s)^{t-1}\alpha_r(r,s)+st\sum_{y\in\mathcal{Y}}\alpha(r,s)^{t-1}\alpha_s(r,s)\right)^2\\
&= \left(r\psi_r(r,s)+s\psi_s(r,s)\right)^2, \qquad \text{(A.28)}
\end{aligned}$$

が成立する．なお，2 つ目の不等式で Cauchy-Schwartz の不等式を利用した．

以上の準備の元，実際に $\mathbf{v}^T H\mathbf{v}$ を評価する．$\phi(r,s)$ の r と s についての偏微分は，下添字 i と j を r または s を表すとすると，

$$\phi_{ij}(r,s) = \frac{\psi_{ij}(r,s)\psi(r,s) - \psi_i(r,s)\psi_j(r,s)}{\psi(r,s)^2} \tag{A.29}$$

となる．ここで，$\phi(r,s)$ について $\mathbf{v}^T H\mathbf{v}$ を展開すると，

$$\begin{aligned}\mathbf{v}^T H\mathbf{v} &= r^2\phi_{rr}(r,s) + 2rs\phi_{rs}(r,s) + s^2\phi_{ss}(r,s) \\ &= \frac{(r^2\psi_{rr}(r,s) + 2rs\psi_{rs}(r,s) + s^2\psi_{ss}(r,s))\psi(r,s) - (r\psi_r(r,s) + s\psi_s(r,s))^2}{\psi(r,s)^2} \\ &\geq 0 \end{aligned} \tag{A.30}$$

が成立することが，不等式 (A.28) から示される．すなわち，$t \in (0,2]$ について，関数 $\phi(r,s)$ は変数 (r,s) の凸関数である．

最後に，例外として残していた $t=0$ の場合について証明を行う．ここで，

$$\gamma(v,u,t) \stackrel{\triangle}{=} \sum_{x\in\mathcal{X}} \epsilon(v,x,u)e^{rg(x,t)} \tag{A.31}$$

と，任意の u について

$$v_u^* \stackrel{\triangle}{=} \arg\max_v W^+(u|v) = \arg\max_v \left(\sum_x \epsilon(v,x,u)\right) \tag{A.32}$$

を定義する．そして，関数 $\phi(r,s)$ を

$$\begin{aligned}\phi(r,s) &= \log\left[\sum_{u\in\mathcal{U}}\left(\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\gamma(v,u,t)^{\frac{1}{t}}\right)^t\right] \\ &= \log\left[\sum_{u\in\mathcal{U}}\left(\sum_{v\in\mathcal{V}} P_V(v)e^{sf(v)}\gamma(v_u^*,u,t)^{\frac{1}{t}}\left[\frac{\gamma(v,u,t)}{\gamma(v_u^*,u,t)}\right]^{\frac{1}{t}}\right)^t\right]\end{aligned} \tag{A.33}$$

と書き直した上で，その $t\to 0$ への極限を求めると，

$$\left[\frac{\gamma(v,u,t)}{\gamma(v_u^*,u,t)}\right]^{\frac{1}{t}} \to \begin{cases} 1 & \text{for } v = v_u^* \\ 0 & \text{for } v \neq v_u^* \end{cases}, \tag{A.34}$$

が成り立つことから，$v = v_u^*$ について

$$\begin{aligned}&\left(P_V(v)e^{sf(v)}\gamma(v,u,t)\left[\frac{\gamma(v,u,t)}{\gamma(v_u^*,u,t)}\right]^{\frac{1}{t}}\right)^t \qquad = P_V(v)^t e^{stf(v)}\gamma(v_u^*,u,t) \\ &\to \max_v W^+(u|v)\end{aligned} \tag{A.35}$$

が成立する．以上より，式 (A.34) と式 (A.35) を式 (A.33) に代入すると，$\phi(r,s)$ の極限は

$$\lim_{t\to 0}\phi(r,s) = \log\sum_{u\in\mathcal{U}}\max_v W^+(u|v) \tag{A.36}$$

と計算される．

式 (A.36) の右辺は (r,s) については明らかに定数であるため，関数 $\phi(r,s)$ の $t=0$ における凸性は自明である．従って，以上の議論から，関数 $\phi(\rho|W,P_V,r,s)$ は変数 (r,s) の凸関数であることが，$\rho\in[-1,1]$ について示された．

A.4　ガウスワイヤタップ通信路

ここでは，ガウスワイヤタップ通信路の誤り指数と秘匿性指数について，第 3 章における，ガウスワイヤタップ通信路に関する議論の補完を行う．

なお，ガウス通信路は連続値通信路であるため，式 (3.17) 及び式 (3.20) の和の記号を下記のように積分に置き換える．

$$\phi_H(\rho|W,P_X,r)=-\log\int\left(\int P_X(x)W(u|x)^{\frac{1}{1+\rho}}e^{r[\Gamma-c(x)]}dx\right)^{1+\rho}du \tag{A.37}$$

$$\phi_G(\rho|W,P_X,r)=-\log\int\left(\int P_X(x)W(u|x)^{\frac{1}{1+\rho}}e^{-r[\Gamma-c(x)]}dx\right)^{1+\rho}du \tag{A.38}$$

初めに，誤り指数について考える．第 3 章同様に，入力 X に対して出力が $Y=A_yX+N$ で与えられる通信路を考える．ここで，A_y は通信のゲインであり，N は分散 σ_B^2 の正規分布に従う雑音である．そのため，通信路の遷移確率は

$$W_B(y|x)=\frac{1}{\sqrt{2\pi\sigma_B^2}}\exp\left[-\frac{(y-A_yx)^2}{2\sigma_B^2}\right] \tag{A.39}$$

にて与えられる．

入力確率分布については，分散が与えられたパワー制約 Γ と等しい正規分布

$$P_X(x)=\frac{1}{\sqrt{2\pi\Gamma}}\exp\left[-\frac{x^2}{2\Gamma^2}\right] \tag{A.40}$$

で与えられることが知られている [143]

以上の遷移確率分布と入力確率分布を代入した上で，関数 $\phi_H(\rho|W_B,P_X,r)$ の積分を実行すると，

$$\begin{aligned}&\phi_H(\rho|W_B,P_X,r)\\&=-r(1+\rho)A_y^2\Gamma+\frac{1}{2}\log(1+2rA_y^2\Gamma)+\frac{\rho}{2}\log\left[1+2rA_y^2\Gamma+\frac{A_y^2\Gamma}{(1+\rho)\sigma_B^2}\right] &\text{(A.41)}\\&=\frac{1}{2}\left[(1-\beta_B)(1+\rho)+A_B+\log\left(\beta_B-\frac{A_B}{1+\rho}\right)+\rho\log\beta_B\right] &\text{(A.42)}\end{aligned}$$

を得る．ここで，

$$A_B=\frac{A_y^2\Gamma}{\sigma_B^2} \tag{A.43}$$

$$\beta_B=1+2rA_y^2\Gamma+\frac{A_B}{1+\rho} \tag{A.44}$$

と置いている．一方で，関数 $\phi_G(\rho|W_B, P_X, r)$ の積分は

$$\begin{aligned}
&\phi_G(\rho|W_B, P_X, r) \\
&\quad = r(1+\rho)A_y^2\Gamma + \frac{1}{2}\log(1-2rA_y^2\Gamma) + \frac{\rho}{2}\log\left[1-2rA_y^2\Gamma + \frac{A_y^2\Gamma}{(1+\rho)\sigma_B^2}\right] \qquad \text{(A.45)} \\
&\quad = \frac{1}{2}\left[(1-\beta_B^*)(1+\rho) + A_B + \log\left(\beta_B^* - \frac{A_B}{1+\rho}\right) + \rho\log\beta_B^*\right] \qquad \text{(A.46)}
\end{aligned}$$

となる．ここで

$$\beta_B^* = 1 - 2rA_y^2\Gamma + \frac{A_B}{1+\rho} \qquad \text{(A.47)}$$

である．

式 (A.42) と (A.46) を比較すると，r の符号に起因する，β_B と β_B^* という違いが存在するにすぎない．次のステップとして，r による最適化の代わりに，定義の内に r を含む β の最適化を行うが，上記の定義の違いが取りうる値の範囲の違いとなって現れる点に注意する．まず，β_B の取りうる範囲は，$0 \le r$ であることから，

$$1 + \frac{A_B}{1+\rho} \le \beta_B < +\infty \qquad \text{(A.48)}$$

である．一方で，β_B^* の取りうる範囲は，$0 \le r$ 及び式 (A.45) の第 2 項に起因する制約より，

$$\frac{A_B}{1+\rho} < \beta_B^* \le 1 + \frac{A_B}{1+\rho} \qquad \text{(A.49)}$$

となる．

ここで，式 (A.42) 及び式 (A.46) を $f(\beta)$(ただし，$\beta = \beta_B$ か β_B^*) とおいて，その性質を調べる．その β による 2 階微分は

$$\frac{\partial^2}{\partial\beta^2}f(\beta) = \frac{1}{2}\left[-\frac{(1+\rho)^2}{((1+\rho)\beta - A_B)^2} - \frac{\rho}{\beta^2}\right] \le 0 \qquad \text{(A.50)}$$

となり，任意の β に対して負になるため，関数 $f(\beta)$ の β による 1 階微分

$$\frac{\partial}{\partial\beta}f(\beta) = \frac{1}{2}\left[-(1+\rho) + \frac{1+\rho}{(1+\rho)\beta - A_B} + \frac{\rho}{\beta}\right] \qquad \text{(A.51)}$$

は β の単調減少関数となる．

ここで，$f'(\beta) \triangleq \frac{\partial}{\partial\beta}f(\beta)$ に対して，

$$f'\left(1 + \frac{A_B}{1+\rho}\right) < 0 \qquad \text{(A.52)}$$

$$\lim_{\beta\to\infty} f'(\beta) < 0 \qquad \text{(A.53)}$$

$$\lim_{\beta\to\frac{A_B}{1+\rho}} f'(\beta) > 0 \qquad \text{(A.54)}$$

であることは容易に確かめられるため，関数 $f(\beta)$ を最大化する β は β_B^* の範囲 (A.49) に存在する．そのため，関数 $\phi_G(\rho|W_B, P_X, r)$ は関数 $f(\beta)$ を最大化する β により最大化され，一方で関数 $\phi_H(\rho|W_B, P_X, r)$ は $\beta_B = 1 + A_B/(1+\rho)$ で最大化される．これは，$\beta = 1 + A_B/(1+\rho)$ と $r = 0$ が同値であることから考えると，$\phi_G(\rho|W_B, P_X, r)$ を最適化する r は $r \leq 0$ という r の定義域に存在している一方で，$\phi_H(\rho|W_B, P_X, r)$ を最適化する r は r の定義域の範囲外に存在しているため，$r = 0$ で最大化されるという状況に対応している．

ここから，$\beta_B = 1 + A_B/(1+\rho)$ を式 (A.42) に代入した上で，ρ に関する定常点を微分から求めることによって，ガウス通信路の H 型誤り指数の媒介変数表示を以下の形で得る．

定理 A.4.1 ガウス通信路の H 型誤り指数の媒介変数表示は，$0 \leq \rho \leq 1$ では，

$$F_c(\rho) = \frac{\rho^2 A_B}{2(1+\rho)(1+\rho+A_B)} \tag{A.55}$$

$$(R_B + R_E)(\rho) = \frac{1}{2}\log\left(1 + \frac{A_B}{1+\rho}\right) - \frac{\rho^2 A_B}{2(1+\rho)(1+\rho+A_B)} \tag{A.56}$$

となる．一方で，$0 \leq R_B + R_E \leq (R_B + R_E)(1)$ の範囲では，

$$F_c(P_X, R_B, R_E) = \frac{1}{2}\log\left(1 + \frac{A_B}{2}\right) - (R_B + R_E) \tag{A.57}$$

となる． □

一方で，関数 $f(\beta)$ を最大化する β を求めて，それを式 (A.46) に代入した上で，さらに ρ についても最大化することにより，ガウス通信路の G 型誤り指数を以下の形で得る．

定理 A.4.2 ガウス通信路の G 型誤り指数は

$$\begin{aligned} F_c(P_X, R_B, R_E) = {} & \frac{A_B}{4\beta_B}\left[(\beta_B+1) - (\beta_B-1)\sqrt{1 + \frac{4\beta_B}{A_B(\beta_B-1)}}\right] \\ & + \frac{1}{2}\log\left[\beta_B - \frac{A_B(\beta_B-1)}{2}\left(\sqrt{1+\frac{4\beta_B}{A_B(\beta_B-1)}} - 1\right)\right] \end{aligned} \tag{A.58}$$

により与えられる．ただし，$\beta_B \triangleq e^{2(R_B+R_E)}$ とおいた．この表式は

$$\frac{1}{2}\log\left[\frac{1}{2} + \frac{A_B}{4} + \frac{1}{2}\sqrt{1 + \frac{A_B^2}{4}}\right] \leq R_B + R_E \leq \frac{1}{2}\log(1+A_B) \tag{A.59}$$

の範囲で有効であり，この式の左辺よりも小さいレート $R_B + R_E$ に対しては，

$$F_c(P_X, R_B, R_E) = 1 - \beta_B + \frac{A_B}{2} + \frac{1}{2}\log\left(\beta_B - \frac{A_B}{2}\right) + \frac{1}{2}\log\beta_B - (R_B + R_E) \tag{A.60}$$

となる．

次に，分散 σ_z^2 及び通信路ゲイン A_z の盗聴者通信路 W_E の秘匿性指数について考える．秘匿性指数と誤り指数は ρ の符号が異なるだけであるので，上記と同様の議論から，最適化すべき関数として，

$$\phi_H(-\rho|W_E,P_X,r)=\frac{1}{2}\left[(1-\beta_E)(1-\rho)+A_E+\log\left(\beta_E-\frac{A_E}{1-\rho}\right)-\rho\log\beta_E\right] \tag{A.61}$$

$$\phi_G(-\rho|W_E,P_X,r)=\frac{1}{2}\left[(1-\beta_E^*)(1-\rho)+A_E+\log\left(\beta_E^*-\frac{A_E}{1-\rho}\right)-\rho\log\beta_E^*\right] \tag{A.62}$$

を得る．ここで，

$$A_E=\frac{A_z^2\Gamma}{\sigma_E^2} \tag{A.63}$$

$$\beta_E=1+2rA_z^2\Gamma+\frac{A_E}{1-\rho} \tag{A.64}$$

$$\beta_E^*=1-2rA_z^2\Gamma+\frac{A_E}{1-\rho} \tag{A.65}$$

と置いている．そして，β_E と β_E^* の取りうる範囲は

$$1+\frac{A_E}{1-\rho}\le\beta_E<+\infty \tag{A.66}$$

$$\frac{A_E}{1-\rho}<\beta_E^*\le 1+\frac{A_E}{1-\rho} \tag{A.67}$$

となる．

誤り指数での議論同様に，式 (A.61) と式 (A.62) をまとめて，$g(\beta)$(ただし，$\beta=\beta_E$ か β_E^*) とおくと，この $g(\beta)$ が β の単調減少関数であることは容易に確認できる．一方で，ここで，$g'(\beta)\triangleq\frac{\partial}{\partial\beta}g(\beta)$ に対して，

$$g'\left(1+\frac{A_E}{1-\rho}\right)>0 \tag{A.68}$$

$$\lim_{\beta\to\infty}g'(\beta)<0 \tag{A.69}$$

$$\lim_{\beta\to\frac{A_E}{1-\rho}}g'(\beta)>0 \tag{A.70}$$

が成立するため，$g(\beta)$ を最大化する β は (A.66) の範囲内に存在している．従って，誤り指数とは反対に，H 型の指数を最適化する r は r の定義域内に存在し，G 型の指数を最適化する r はその定義域内に存在しないため，$r=0$ が最適値となる．そして，結果として HES 型指数が G 型指数よりも大きい値を持つことになる．

誤り指数と同様に ρ で最適化を行うことにより，秘匿性指数をえる．

定理 A.4.3 ガウス通信路の G 型誤り指数は，$R_E\ge\frac{1}{2}\log(1+A_E)$ を満たす R_E に対

して，

$$H_c(P_X, R_E) = \frac{A_E}{4\beta_E}\left[(\beta_E+1) - (\beta_E-1)\sqrt{1+\frac{4\beta_E}{A_E(\beta_E-1)}}\right] + \frac{1}{2}\log\left[\beta_E - \frac{A_E(\beta_E-1)}{2}\left(\sqrt{1+\frac{4\beta_E}{A_E(\beta_E-1)}}-1\right)\right] \tag{A.71}$$

となる．ただし，$\beta_E = e^{2R_E}$ とした． □

定理 A.4.4　ガウス通信路の H 型誤り指数の媒介変数表示は，$R_E \geq \frac{1}{2}\log(1+A_E)$ を満たす R_E に対して，

$$H_c(P_X, R_E) = \frac{\rho^2 A_E}{2(1-\rho)(1-\rho+A_E)} \tag{A.72}$$

$$R_E = \frac{1}{2}\log\left(1+\frac{A_E}{1-\rho}\right) - \frac{\rho^2 A_E}{2(1-\rho)(1-\rho+A_E)} \tag{A.73}$$

となる．但し，$0 \leq \rho < 1$ であり． □

A.5　定理 3.1.4 の証明

初めに，誤り指数に対する主張を示す．そのためには，

$$\begin{aligned} g(r) &\stackrel{\triangle}{=} \phi_G(\rho=0|W_B, P_X, r) \\ &= -\log\left[\sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} W(y|x)P_X(x)e^{-r[\Gamma-c(x)]}\right] \\ &= -\log\left[\sum_{x\in\mathcal{X}} P_X(x)e^{-r[\Gamma-c(x)]}\right]. \end{aligned} \tag{A.74}$$

が正の値をとることを，コスト制約が厳密な等式で満足されている場合に示せば十分である．実際に，関数 $g(r)$ の r による微分 $g_r(r)$ について，

$$g_r(0) = \Gamma - \sum_{x\in\mathcal{X}} P_X(x)c(x) > 0, \tag{A.75}$$

が $\sum_x c(x)P_X(x) < \Gamma$ ならば成立する．補題 A.2.1 が任意の r と $s=0$ で成立し，かつ $g(0)=0$ であることから，$\phi_G(\rho=0|W_B, P_X, r)$ の最大値は $r>0$ に存在し，正の値を持つことが分かる．そのため，誤り指数に関する主張が示された．同様の方法で秘匿性指数についての主張も示される．

付録 B

第 5 章における補足事項

ここでは，第 5 章において必要な補足事項をまとめた．

B.1　有限体とその表現及び演算

節 5.1.1 で述べた 2 元線形符号とは異なり，RS 符号は 2 元体 $\mathbb{F}_2$ を拡大した，拡大体 $\mathbb{F}_{2^m}$ 上で定義される．拡大体 $\mathbb{F}_{2^m}$ の定義に先立ち，下記の規約多項式を導入する．

定義 B.1.1　各係数が $f_i \in \mathbb{F}_2 \quad (i = [0, m])$ である多項式

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_m x^m \tag{B.1}$$

のについて，この多項式がより低次数の多項式の積に因子分解されないならば，$\mathbb{F}_2$ 上の m 次規約多項式と呼ぶ．□

このような $\mathbb{F}_2$ 上の m 次規約多項式 $f(z)$ の根 α は，規約多項式の規約性から $\alpha \notin \mathbb{F}_p$ であることは明らかである．

この根 α を $\mathbb{F}_2$ に追加することによって，拡大体 $\mathbb{F}_{2^m}$ を定義する．

定義 B.1.2　素体 $\mathbb{F}_2$ 上の m 次規約多項式の根 α を $\mathbb{F}_2$ に添加することで構成される体を $\mathbb{F}_2$ の拡大体 $\mathbb{F}_{2^m}$ と呼ぶ．その任意の元 $a \in \mathbb{F}_{2^m}$ は

$$a(\alpha) = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha^1 + a_0 \tag{B.2}$$

と表現される．ここで，任意の $i \in [0, m-1]$ に対して $a_i \in \mathbb{F}_p$ である．□

なお，有限体の元の表現には様々な種類が存在し，本研究ではこの表現を多項式表現と呼ぶ．他の表現の 1 つとして，多項式表現における係数 a_i のみを表記するベクトル表現

$$a = (a_{m-1}, a_{m-2}, \cdots, a_1, a_0) \tag{B.3}$$

が考えられる．特に，これらの要素が 2 元体の元であるならば，このベクトルを整数の 2 進展開と解釈して，その 10 進あるいは 16 進表示を取る数値表現も考えられる．また，多

項式表現に対してその拡大体を定義している規約多項式を繰り返し作用させることによって，その根の指数で元を表現することもできる．このような表現を以降指数表現と呼ぶ．

この拡大体 $\mathbb{F}_{p^m}$ に対して，可算と乗算は下記のように定義される．

定義 B.1.3 根 α を持つ m 次規約多項 $f(x)$ により定義される拡大体 $\mathbb{F}_{p^m}$ の任意の元

$$a(\alpha) = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha^1 + a_0 \tag{B.4}$$
$$b(\alpha) = b_{m-1}\alpha^{m-1} + b_{m-2}\alpha^{m-2} + \cdots + b_1\alpha^1 + b_0 \tag{B.5}$$

について，和と積は

$$a(\alpha) + b(\alpha) = \sum_{i=0}^{m-1} [a_i + b_i]\alpha^i \tag{B.6}$$
$$a(\alpha) \times b(\alpha) = a(\alpha)b(\alpha) \bmod f(z) \tag{B.7}$$

により定義される．ここで，式 (B.6) 右辺の演算は $\mathbb{F}_2$ 上の演算であり，式 (B.7) 右辺の積 ab は多項式の積である． □

2 元体上の加減は両者とも排他的論理和そのものであったため，$\mathbb{F}_{2^m}$ 上の加減はベクトル表現における要素ごとの排他的論理和，あるいは数値表現におけるビット毎の排他的論理和として実装される．

一方で，$\mathbb{F}_{2^m}$ 上の乗除は，その簡便さから指数表示での計算が一般的である．しかし，上で述べたように加減演算は数値表現で行われるため，両者の同時の実装を考えた場合には元の表現を統一する方が好ましい．そのため，本研究では数値表現による乗除の実装を考える．

一つの有効な手段としては，積を対数の和への帰着させる方法が考えられる．すなわち，

$$a \times b = \exp_n(\log_n(a \times b)) = \exp_n(\log_n a + \log_n b) \tag{B.8}$$

が成立することを利用する．ここで，和は $(a + b) \bmod 255$ を意味し，$\exp_n$ と $\log_n$ はそれぞれ n を底とした指数関数と対数関数である．実装に先んじて，予め全ての元 a に対して $\exp_n a$ と $\log_n a$ を計算し，配列に格納しておくことにより，配列上の指定と和で積が計算される．なお，本研究では $n = 13$ を選択している．

また，同様の手法により，a の逆元 a^{-1} も

$$a^{-1} = \exp_n(255 - \log_n a) \tag{B.9}$$

により求められる．

参考文献

[1] V. W. S. Chan, "Free-space optical communications," *J. Lightwave Technol.*, vol. 24, no. 12, pp. 4750–4762, Dec. 2006.

[2] F. Fidler, M. Knapek, J. Horwath, and W. R. Leeb, "Optical communications for high-altitude platforms," *IEEE J. Sel. Topics Quantum Electron.*, vol. 16, no. 5, pp. 1058–1070, Sep. 2010.

[3] M. Sharma, D. Chadha, and V. Chandra, "High-altitude platform for free-space optical communication: Performance evaluation and reliability analysis," *IEEE J. Opt. Commun. Networ.*, vol. 8, no. 8, pp. 600–609, Aug. 2016.

[4] I. I. Kim and E. J. Korevaar, "Availability of free-space optics (FSO) and hybrid FSO/RF systems," in *proc. International Symposium on the Convergence of IT and Communications*, 2001, pp. 84–95.

[5] D. Kedar and S. Arnon, "Urban optical wireless communication networks: the main challenges and possible solutions," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. S2–S7, May 2004.

[6] Twibright Labs, "Ronja - Twibright Labs," http://ronja.twibright.com/, (visited on 11/11/2016).

[7] W. S. Rabinovich, C. I. Moore, R. Mahon, P. G. Goetz, H. R. Burris, M. S. Ferraro, J. L. Murphy, L. M. Thomas, G. C. Gilbreath, M. Vilcheck, and M. R. Suite, "Free-space optical communications research and demonstrations at the u.s. naval research laboratory," *Appl. Opt.*, vol. 54, no. 31, pp. F189–F200, Nov. 2015.

[8] T. Jono, Y. Takayama, N. Kura, K. Ohinata, Y. Koyama, K. Shiratama, Z. Sodnik, B. Demelenne, A. Bird, and K. Arai, "OICETS on-orbit laser communication experiments," in *Proc. SPIE*, vol. 6105, 2006, p. 610503.

[9] B. S. Robinson, D. M. Boroson, D. A. Burianek, and D. V. Murphy, "Overview of the lunar laser communications demonstration," in *Proc. SPIE*, vol. 7923, Jan. 2011, p. 792302.

[10] 豊嶋守生, "宇宙光通信の実用化に向けた研究開発動向," 光学 - *Japanese journal of optics : publication of the Optical Society of Japan*, vol. 45, no. 2, pp. 62–67,

Feb. 2016.

[11] R. Fields, C. Lunde, R. Wong, J. Wicker, D. Kozlowski, J. Jordan, B. Hansen, G. Muehlnikel, W. Scheel, U. Sterr, R. Kahle, and R. Meyer, "Nfire-to-terrasar-x laser communication results: satellite pointing, disturbances, and other attributes consistent with successful performance," in *Proc. SPIE*, vol. 7330, May 2009, p. 73300Q.

[12] H. Takenaka, Y. Koyama, M. Akioka, D. Kolev, N. Iwakiri, H. Kunimori, A. Carrasco-Casado, Y. Munemasa, E. Okamoto, and M. Toyoshima, "In-orbit verification of small optical transponder (SOTA): evaluation of satellite-to-ground laser communication links," in *Proc. SPIE*, vol. 9739, May 2016, p. 973903.

[13] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[14] Google, "Loon Project," https://x.company/loon/, (visited on 11/11/2016).

[15] Facebook, "Connectivity Lab," https://info.internet.org/en/story/connectivity-lab/, (visited on 11/11/2016).

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process*, Dec.10–12, 1984, pp. 175–179.

[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[19] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network (invited paper)," in *Proc. SPIE*, vol. 5815, 2005, pp. 138–149.

[20] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, 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 Journal of Physics*, vol. 11, no. 7, 2009.

[21] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," *Opt. Express*, vol. 18, no. 26, pp. 27 217–27 225, Dec. 2010.

[22] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, 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. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[23] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. NOW Publishers, Hanover, MA, USA, 2009.

[24] M. Bloch and J. Barros, *Physical Layer Security*. Cambridge University Press, 2011.

[25] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *proc. 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134.

[26] ——, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[27] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *proc. the Twenty-eighth Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[28] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1510–1523, 1997.

[29] D. J. Bernstein, T.-R. Chen, C.-M. Cheng, T. Lange, and B.-Y. Yang, "ECM on graphics cards," in *proc. 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Apr. 2009, pp. 483–501.

[30] J. Hermans, M. Schneider, J. Buchmann, F. Vercauteren, and B. Preneel, "Parallel shortest lattice vector enumeration on graphics cards," in *proc. Third International Conference on Cryptology in Africa*, May 2010, pp. 52–68.

[31] 宇根 正志, 神田 雅透, "暗号アルゴリズムにおける 2010 年問題について," 日本銀行金融研究所/金融研究, Jun. 2006.

[32] National Institute of Standards and Technology, "Data encryption standard

(DES)," 1976.

[33] ——, "Announcing the advance encryption standard (AES)," 2001.

[34] distributed.net, "Project des," http://www.distributed.net/des/.

[35] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," in *proc. CRYPTO' 92: 12th Annual International Cryptology Conference*, Aug. 1993, pp. 487–496.

[36] M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," in *proc. CRYPTO '94: 14th Annual International Cryptology Conference*, Aug. 1994, pp. 1–11.

[37] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[38] T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *proc. Advances in Cryptology*, 1985.

[39] V. S. Miller, "Use of elliptic curves in cryptography," in *proc. CRYPTO '85*, 1986, pp. 417–426.

[40] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comp.*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[41] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *proc. the Twenty-ninth Annual ACM Symposium on Theory of Computing*, 1997, pp. 284–293.

[42] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *proc. CRYPTO '97: 17th Annual International Cryptology Conference*, Aug. 1997, pp. 112–131.

[43] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *proc. Algorithmic Number Theory: Third International Symposiun*, Jun. 1998, pp. 267–288.

[44] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *proc. the Thirty-seventh Annual ACM Symposium on Theory of Computing*, 2005, pp. 84–93.

[45] 青野良範, 林卓也, LE TRIEU PHONG, 王立華, "セキュリティアップデータブル準同型暗号を用いた秘匿データの線形回帰計算," in *proc. SCIS 2015,* **暗号と情報セキュリティシンポジウム**, Jan. 2015.

[46] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Deep Space Network Progress Report*, vol. 44, pp. 114–116, Jan. 1978.

[47] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Probl. Control Inf. Theory*, vol. 15, pp. 159–166, 1986.

[48] D. Augot, "Initial recommendations of long-term secure post-quantum sys-

tems," PQCRYPTO, Sep. 2007.

[49] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *proc. EUROCRYPT '88: Workshop on the Theory and Application of Cryptographic Techniques*, May 1988, pp. 419–453.

[50] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325–328, Jul. 1997.

[51] ——, "From Schrödinger's equation to the quantum search algorithm," *Pramana*, vol. 56, no. 2, pp. 333–348, 2001.

[52] IEEE1363.1, "Public-key cryptographic techniques based on hard problems over lattices," 2009.

[53] Y. Chen and P. Q. Nguyen, "BKZ 2.0: Better lattice security estimates," in *proc. Advances in Cryptology – ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security*, Dec. 2011, pp. 1–20.

[54] N. Courtois, L. Goubin, and J. Patarin, "SFLASHv3, a fast asymmetric signature scheme," Cryptology ePrint Archive, Report 2003/211, http://eprint.iacr.org/, 2003.

[55] V. Dubois, P.-A. Fouque, and J. Stern, "Cryptanalysis of SFLASH with slightly modified?parameters," in *proc. Advances in Cryptology - EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, May 2007, pp. 264–275.

[56] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *J. Am. Inst. Elect. Eng.*, vol. 45, no. 2, pp. 109–115, Feb. 1926.

[57] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[58] "Id Quantique," http://www.idquantique.com/.

[59] "MagiQ Technology," http://www.magiqtech.com/Home.html.

[60] "Quintessence labs," http://www.quintessencelabs.com/.

[61] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, Nov. 2012, pp. 156–161.

[62] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "High speed prototype quantum key distribution system and long term field trial," *Opt. Express*, vol. 23, no. 6, pp. 7583–7592,

Mar. 2015.

[63] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, Jan. 2007.

[64] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, "Entanglement-based quantum communication over 144 km," *Nature physics*, vol. 3, no. 7, pp. 481–486, 2007.

[65] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova *et al.*, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[66] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[67] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[68] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[69] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Sep. 2006.

[70] A. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[71] T. S. Han and S. Verdu, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[72] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[73] 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.

[74] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Inf. Transm.*, vol. 32, no. 1, pp. 48–57, 1996.

[75] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[76] T. S. Han, *Information-Spectrum Methods in Information Theory.* Springer, 2003.

[77] R. G. Gallager, *Information Theory and Reliable Communication.* Wiley, 1968.

[78] M. B. Parizi and E. Telatar, "On the secrecy exponent of the wire-tap channel," in *proc. IEEE Information Theory Workshop*, Oct. 2015, pp. 287–291.

[79] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014.

[80] R. G. Gallager, *Low Density Parity Check Codes*. MIT Press, 1963.

[81] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[82] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[83] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[84] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[85] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *proc. IEEE International Symposium on Information Theory*, Jun. 2010, pp. 2538–2542.

[86] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comp. Syst. Sci.*, vol. 18, pp. 134–154, 1979.

[87] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[88] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[89] ——, "Secure transmission with multiple antennas –;part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[90] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[91] 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, p. 6034749, Apr. 2015.

[92] 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, Feb. 2016.

[93] T. H. Chou, S. C. Draper, and A. M. Sayeed, "Key generation using external source excitation: Capacity, reliability, and secrecy exponent," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.

[94] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, Apr. 1988.

[95] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT*, 1994, pp. 410–423.

[96] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[97] A. D. Wyner, "Recent results in the shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 2–10, Jan. 1974.

[98] C. Berrou and G. Alain, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Trans. Commun.*, vol. 40, no. 10, pp. 1261–1271, Oct. 1996.

[99] J. Bajcsy and P. Mitran, "Coding for the slepian-wolf problem with turbo codes," in *Proc. IEEE Globecom*, 2001.

[100] A. Aaron and B. Girod, "Compression with side information using turbo codes," in *Proc. IEEE DCC*, 2002, pp. 252–261.

[101] S. B. Korada and R. Urbanke, "Polar codes for slepian-wolf, wyner-ziv, and gelfand-pinsker," in *Information Theory (ITW 2010, Cairo), 2010 IEEE Information Theory Workshop on*, Jan. 2010, pp. 1–5.

[102] E. A. Bilkent, "Polar coding for the slepian-wolf problem based on monotone chain rules," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, Jul. 2012, pp. 566–570.

[103] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using ldpc codes," *IEEE Communications Letters*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[104] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, 1989, pp. 12–24.

[105] T. Asai and T. Tsurumaru, "Efficient privacy amplification algorithms for quantum key distribution (in japanese)," *IEICE technical report*, vol. 110, no. 442, pp. 327–332, feb 2011.

[106] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 2213–2232, April 2016.

[107] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over

fading channels," in *proc. Military Communications Conference, 2001*, vol. 1, Oct. 2001, pp. 54–58.

[108] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[109] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[110] 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.

[111] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Comput. Commun. Security*, 2007, pp. 401–410.

[112] 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. Mag.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[113] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *proc. the 14th ACM International Conference on Mobile Computing and Networking*, Sep. 2008, pp. 128–139.

[114] W. Xi, X.-Y. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *proc. IEEE 22nd International Symposium of Quality of Service (IWQoS)*, May 2014, pp. 350–359.

[115] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual ofdm subcarrier's channel response," in *proc. IEEE Globecom Workshops*, Dec. 2015, pp. 1–6.

[116] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.

[117] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. on Mob. Comput.*, vol. 13, no. 12, pp. 2763–2776, 2014.

[118] 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," *J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1072–1081, Dec. 2014.

[119] R. R. Parenti, J. M. Roth, J. H. Shapiro, F. G. Walther, and J. A. Greco, "Ex-

perimental observations of channel reciprocity in single-mode free-space optical links," *Opt. Express*, vol. 20, no. 19, pp. 21 635–21 644, Sep. 2012.

[120] J. H. Shapiro and A. L. Puryear, "Reciprocity-enhanced optical communication through atmospheric turbulence – part I: Reciprocity proofs and far-field power transfer optimization," *IEEE J. Opt. Commun. Netw.*, vol. 4, no. 12, pp. 947–954, Dec. 2012.

[121] A. L. Puryear, J. H. Shapiro, and R. R. Parenti, "Reciprocity-enhanced optical communication through atmospheric turbulenc – part II: Communication architectures and performance," *J. Opt. Commun. Netw.*, vol. 5, no. 8, pp. 888–900, Aug. 2013.

[122] T. S. Han and K. Kobayashi, *Mathematics of Information and Coding*. Amer. Mathematical Society, 2007.

[123] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[124] 渡辺 峻, "情報理論的に安全な秘密鍵共有と周辺話題," **電子情報通信学会基礎・境界ソサイエティ** *Fundamentals Review*, vol. 7, no. 1, pp. 38–50, 2013.

[125] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. San Francisco, CA, USA: Holden-Day, 1964.

[126] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *2014 IEEE International Symposium on Information Theory*, Jun. 2014, pp. 601–605.

[127] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'00, 2000, pp. 351–368.

[128] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[129] E. SaSoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, Jul. 2013, pp. 1117–1121.

[130] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of ldpc codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[131] T. M. Cover, "A proof of the data compression theorem of slepian and wolf for ergodic sources," *IEEE Trans. Inf. Theory*, vol. 22, no. 2, pp. 226–228, Mar. 1975.

[132] R. Renner, "Security of quantum key distribution," *International Journal of*

Quantum Information, vol. 6, no. 1, pp. 1–127, 2008.

[133] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *proc. 42nd IEEE Symposium on Foundations of Computer Science*, Oct. 2001, pp. 136–145.

[134] B. Pfitzmann and M. Waidner, "Composition and integrity preservation of secure reactive systems," in *proc. the 7th ACM Conference on Computer and Communications Security*, 2000, pp. 245–254.

[135] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, p. 012332, Jul. 2005.

[136] M. Hayashi, "Practical evaluation of security for quantum key distribution," *Phys. Rev. A*, vol. 74, p. 022307, Aug. 2006.

[137] ——, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Phys. Rev. A*, vol. 76, p. 012329, Jul. 2007.

[138] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, no. 4, p. 045018, 2009.

[139] M. Koashi and J. Preskill, "Secure quantum key distribution with an uncharacterized source," *Phys. Rev. Lett.*, vol. 90, p. 057902, Feb 2003.

[140] H.-K. Lo, "Method for decoupling error correction from privacy amplification," *New Journal of Physics*, vol. 5, no. 1, p. 36, 2003.

[141] Z. Luo and I. Devetak, "Efficiently implementable codes for quantum key expansion," *Phys. Rev. A*, vol. 75, p. 010303, Jan. 2007.

[142] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[143] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[144] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel –Part I," *IEEE Trans. Inf. Theory*, vol. 34, no. 6, pp. 1449–1461, Nov. 1988.

[145] A. Laourine and A. B. Wagner, "The degraded poisson wiretap channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7073–7085, Dec. 2012.

[146] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, pp. 057 901–1 – 057 901–4, Aug. 2003.

[147] M. Sasaki, M. Fujiwara, R. B. Jin, M. Takeoka, T. S. Han, H. Endo, K. Yoshino, T. Ochi, S. Asami, and A. Tajima, "Quantum photonic network: concept, basic tools, and future issues (invited paper)," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, Nov. 2014.

[148] J. S. Neergaard-Nielsen, Y. Eto, C.-W. Lee, H. Jeong, and M. Sasaki, "Quan-

tum tele-amplification with a continuous-variable superposition state," *Nature Photon.*, vol. 7, pp. 439–443, May 2013.

[149] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC 2005-Fall*, vol. 3, Sep. 2005, pp. 1906–1910.

[150] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Apr. 2009, pp. 2437–2440.

[151] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE ICC*, Jun. 2014, pp. 3342–3347.

[152] M. Z. I. Sarkar and T. Ratnarajah, "Secrecy capacity over correlated log-normal fading channel," in *proc. IEEE International Conference on Communications*, Jun. 2012, pp. 883–887.

[153] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Communications Letters*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[154] I. I. Kim, B. McArthur, and E. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in *Proc. SPIE*, vol. 4214, Feb. 2001, pp. 26–37.

[155] W. S. Rabinovich, R. Mahon, H. R. Burris, G. C. Gilbreath, P. G. Goetz, C. I. Moore, M. F. Stell, M. J. Vilcheck, J. L. Witkowsky, L. Swingen, M. R. Suite, E. Oh, and J. Koplow, "Free-space optical communications link at 1550 nm using multiple-quantum-well modulating retroreflectors in a marine environment," *Opt. Eng.*, vol. 44, p. 056001, 2005.

[156] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*. Bellingham, WA, USA: SPIE, 2005.

[157] V. I. Tatarski, R. A. Silverman, and N. Chako, "Wave propagation in a turbulent medium," *Physics Today*, vol. 14, p. 46, 1961.

[158] H. Yuksel and C. C. Davis, "Aperture averaging experiment for optimizing receiver design and analyzing turbulence on free space optical communication links," in *proc. Conference on Lasers and Electro-Optics*, vol. 1, May 2005, pp. 743–745.

[159] P. Liu, K. Kazaura, K. Wakamori, and M. Matsumoto, "Studies on c_n^2 and its effects on free space optical communication system," in *proc. 8th Asia-Pacific Symposium on Information and Telecommunication Technologies*, vol. 1, Jun. 2010.

[160] S. Arisa, Y. Takayama, H. Endo, M. Fujiwara, M. Sasaki, and R. Shimizu, "Coupling efficiency of laser beam to multimode fiber for free space optical communication," in *proc. International Conference on Space Optics*, 2014.

[161] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in

proc. IEEE International Symposium on Information Theory, Jul. 2006, pp. 356–360.

[162] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[163] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[164] C. K. P. Clerk, *Reed-Solomon error correction.* BBC White Paper, 2002.

[165] S. Li and A. Ramamoorthy, "Algebraic codes for slepian-wolf code design," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, July 2011, pp. 1861–1865.

謝辞

本研究は，早稲田大学 応用物理学科教授 青木隆朗先生のご指導の元，国立研究開発法人情報通信研究機構 (NICT) との協力研究として，NICT 及び早稲田大学で行われたものであります．NICT との協力研究の場をアレンジして下さり，学部生時代から博士時代まで長きにわたり御指導して頂いた青木隆朗先生に感謝の意を表します．

また，本論文を完成させるにあたり，早稲田大学 応用物理学科教授 中島啓幾先生，同応用物理学科教授 小松進一先生，同物理学科教授 湯浅一哉先生には副査として本論文の詳細に渡り御査読いただくとともに，丁寧な御指導を賜りました．ここに謹んで感謝の意を表します．

共同研究機関である NICT 未来 ICT 研究所主管研究員 佐々木雅英博士，同量子 ICT 先端開発センター協力研究員 韓太舜先生，同研究マネージャー 藤原幹生博士には実際の研究の場を与えていただき，指導者，あるいは共同研究者として多くの御指導並びに御援助をいただきました．各氏にも深甚なる謝意を表します．また，武岡正裕センター長を始めとする量子 ICT 先端開発センターの皆様からは研究をすすめる上での御助言，御指導を多く賜りました．特に，本研究における実験装置の開発は，北村光雄技術支援員，都筑織衛技術支援員，そして伊藤寿之研究員をはじめとする皆様のご活躍に依るものです．ここに厚く御礼申し上げます．

本論文の原型となった各研究を進めるにあたり，NICT 宇宙通信研究室室長 豊嶋守生博士，同研究員 竹中秀樹博士，電気通信大学情報理工学研究科基盤理工学専攻准教授 清水亮介先生，東海大学通信ネットワーク工学科教授 高山佳久先生，東京工業大学通信情報工学専攻准教授 松本隆太郎先生，パドヴァ大学 (University of Padova) Prof. Paolo Villoresi, 同 Assistant Prof. Nicola Laurenti, 同 Assistant Prof. Giuseppe Vallone には研究環境の整備の支援や共同執筆者としての御助言などを頂きました．各氏にも謹んで感謝の意を表します．

加えて，NICT 宇宙通信研究室主任研究員 國森裕生氏からは，HAYABUSA2-地上局間通信レーザー通信実験をはじめ，多くの共同研究の場を提供していただきました．また，同研修員 中園純一氏 及び 小林優輔氏とは，超電導ナノワイヤ単一光子検出器の性能評価や，PPM 通信の大気伝搬特性シミュレーションなどといった，貴重な共同研究を行わせていただきました．上記結果は本研究とは無関係ではありますが，各氏にもこの場を借りてお礼を申し上げます．

その他，早稲田大学 応用物理学科 青木研究室，情報通信研究機構 未来 ICT 研究所 量子 ICT 先端開発センター，同 ワイヤレスネットワーク総合研究センター 宇宙通信研究室においては，上記の方々以外の多くの方々からも様々な形で御支援や御助言をいただきました．この場を借りて心から感謝の意を表したいと思います．

最後に，長年の学生生活を金銭的精神的に支えてくださった両親に対して心からの敬意と謝意を表して本論文を締めくくります．

業績集

論文

1. Hiroyuki Endo, Te Sun Han, and Masahide Sasaki,"Error and secrecy exponents for wiretap channels under two-fold cost constraints, "
IEICE Transactions on Fundamentals E99-A (12), 2136-2146 (2016).

2. Hiroyuki Endo, Mikio Fujiwara, Mitsuo Kitamura, Toshiyuki Ito, Morio Toyoshima, Yoshihisa Takayama, Hideki Takenaka, Ryosuke Shimizu, Nicola Laurenti, Giuseppe Vallone, Paolo Villoresi, Takao Aoki, and Masahide Sasaki, "Free-space optical channel estimation for physical layer security,"
Optics Express 24, 8940-8955 (2016).

3. Hiroyuki Endo, Te Sun Han, Takao Aoki, and Masahide Sasaki,
"Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels,"
IEEE Photonics Journal 7 (5), 7903418 (2015).

4. Masahide Sasaki. Mikio Fujiwara, Rui-Bo Jin, Masahiro Takeoka, Te Sun Han, Hiroyuki Endo Ken-Ichiro Yoshino, Takao Ochi, Shione Asami, and Akio Tajima,
"Quantum photonic network: concept, basic tools, and future issues,"
IEEE Journal of Selected Topics in Quantum Electronics 21 (3), 49-61 (2015).

5. Te Sun Han, Hiroyuki Endo, and Masahide Sasaki,
"Reliability and secrecy functions of the wiretap channel under cost constraint,"
IEEE Transactions on Information Theory 60 (11), 6819-6843 (2014).

講演

1. 遠藤寛之，藤原幹生，北村光雄，伊藤寿之，豊嶋守生，竹中秀樹，清水亮介，青木隆朗，佐々木雅英，
「[奨励講演] 光空間通信における物理レイヤ暗号 ～ 実環境における性能推定と符号化 ～」
衛星通信研究会 (SAT)，東北学院大学，宮城県，(2016 年 8 月).

2. 遠藤寛之，藤原幹生，北村光雄，伊藤寿之，豊嶋守生，竹中秀樹，清水亮介，青木隆朗，佐々木雅英，
「光空間通信の物理レイヤセキュリティ技術」
衛星通信研究会 (SAT)，広島工業大学，広島県，(2016 年 2 月).

3. 遠藤寛之，韓太舜，佐々木雅英，
「光子直接検出による物理レイヤ暗号の秘密伝送レート」
ImPACT “量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現” 第 1 回全体会議, 科学技術振興機構 東京本部，東京都 (2015 年 3 月).

4. 遠藤寛之，韓太舜，佐々木雅英，
「コスト制約付きワイヤタップ通信路の信頼性・秘匿性関数計算問題」
第 37 回情報理論とのその応用シンポジウム (SITA 2014)，宇奈月ニューオータニホテル，富山県 (2014 年 12 月).

5. 遠藤寛之，韓太舜，青木隆朗，佐々木雅英，
「物理レイヤ暗号の秘密伝送可能情報量の具体的評価」
第 75 回応用物理学会秋季学術講演会，北海道大学，北海道 (2014 年 9 月).

6. Hiroyuki Endo, Te Sun Han, Masahide Sasaki, and Takao Aoki,
“Reliability and Security Functions of a Wiretap Channel under Power Constraint,”
4th International Conference on Quantum Cryptography (QCrypt 2014), Paris, France (September 2014).

7. Masahide Sasaki, Te Sun Han, and Hiroyuki Endo,
“Quantifying Reliability and Security of Physical Layer Cryptography”
4th International Conference on Quantum Cryptography (QCrypt 2014), Paris, France (September 2014).

8. 遠藤寛之，藤原幹生，韓太舜，青木隆朗，佐々木雅英，
「伝送効率と安全性を両立させる物理レイヤ暗号システムの研究」
第 61 回応用物理学会春季学術講演会，青山学院大学，神奈川県 (2014 年 3 月).

9. 韓太舜，遠藤寛之，佐々木雅英，
「Wiretap 通信路のコスト制約付き信頼性関数および安全性関数」
第 36 回情報理論とのその応用シンポジウム (SITA 2013)，伊東ホテル聚楽，静岡県 (2013 年 11 月).

10. 遠藤寛之，
「ポアッソンワイアタップ通信路による物理レイヤセキュリティ」
Symposium on New Frontiers of Quantum Photonic Network, 電気通信大学，東京都 (2013 年 11 月).

その他

1. (講演) 國森裕生，久保岡俊宏，布施哲治，遠藤寛之，藤原幹生，佐々木雅英，青木隆朗，
「光リンク/スペースデブリ観測のための波長 1um レンジングシステムの構築」
衛星通信研究会 (SAT)，広島工業大学，広島県，(2016 年 2 月).

2. (講演)Suguru Arisa, Yoshihisa Takayama, Hiroyuki Endo, Mikio Fujiwara, Masahide Sasaki, and Ryosuke Shimizu,
“Coupling efciency of laser beam to multimode ber for free space optical communication,”
International Conference on Space Optics (ICSO 2014), Tenerife, Spain (October 2014).