量子セキュアネットワークの研究

情報科学研究科　情報ｴﾚｸﾄﾛﾆｸｽ専攻

田島　章雄(79165011)

目次

特記事項

(1)世界初の商用光ファイバでのリアルタイム量子鍵生成の達成

当時、量子鍵配送技術は光子伝送・受信結果を用いたオフライン鍵抽出処理によって実現していたため実システムとしての実現性は不透明であった。光子伝送から鍵抽出まで一気通貫のリアルタイム処理を行うシステムを考案し、さらに実使用環境での温度変動などの変動の影響を受けない安定化技術を開発し、商用アクセスファイバでの 14 日間連続リアルタイム量子鍵生成を世界で初めて達成。また、開発した量子鍵配送システムを活用し量子鍵配送ネットワークの初期検証を世界に先駆けて行った。

(2)長期間連続運転において世界最高レベルの鍵生成速度かつ低誤り率の達成

独自の単一方向・偏波無依存型波長多重システム、高速光子検出技術、リアルタイム量子鍵抽出 H/W 技術により、世界最高レベルの鍵生成速度 100 kbps 以上かつ誤り率 1.7%以下を損失 13 dB のフィールド光ファイバ伝送路において達成。また、実使用環境(サーバ室とオフィス環境)に設置した装置によって 21 週間の長期連続動作試験を達成した。

(3)多様なアプリケーションへ量子鍵を配送する量子鍵配送ネットワークを実証

量子鍵配送ネットワークアーキテクチャ提案、提案ネットワークの構築と秘匿通信アプリケーションの実証。

１．背景

2011 年、流出件数が全世界で 1 億人を超える、過去最大規模の個人情報流出事件[1]が起きた。この情報流出事件によりクラウド時代における情報管理の重要性があらためて認識されることとなった。さらに、Wiki リークスによる国家機密の流出[2]など、確実に守るべき情報が公開されるという、これまでには考えられないような危機に接し、社会の情報管理基盤のあり方が問われている。また、アメリカ国家安全保障局（NSA）および中央情報局(CIA) の元局員であった Edward Joseph Snowden による、NSA が他国の機密に関する通信を盗聴していることやイギリス・政府通信本部(GCHQ)が光ケーブル網の通信を傍受していることを暴露(Snowden 事件) [3]は、全世界に大きな衝撃を与えた。実際にリボンファイバ間でのクロストークが観測可能であるとの実験結果も報告されている[4]。

一般に重要な情報を安全に通信するためには暗号技術が必要であり、さまざまな研究機関が開発を続けてきた。様々な社会活動が情報通信ネットワークへの依存性を高めてきているなかで、国家機密に関わる情報以外にも金融情報、遺伝子情報をはじめとする重要個人情報についても将来の如何なる技術によっても盗聴・解読されることがあってはならない。数学を利用した従来の暗号[5][6]は、解読に膨大な時間を要することで安全性を担保しているが、コンピュータや解読アルゴリズムの発展によっていずれは解読可能であることが指摘されており、日々進歩する暗号解読技術[7]への究極的対抗手段が必要とされている。

量子鍵配送(Quantum Key Distribution: QKD)[8][9]技術は、第三者に情報を漏洩することなく暗号鍵を共有する。その安全性は物理法則によって保証されている。QKD によって共有した暗号鍵を用いて、情報理論的安全性が証明されている One-time pad 暗号[10]を用いると、盗聴不可能な暗号鍵共有と解読不可能な暗号化を実現することができる。重要な情報を盗聴・解読から保護する技術として量子鍵配送技術/量子暗号技術の実用化が求められている。

QKD 技術は基本的には一対一接続による二点間の鍵共有技術である。この技術を応用した、多対多のネットワークにおける量子暗号鍵配送及び秘匿通信実現へ向けた研究が世界中で行われている。欧州では、2006 年に id Quantique 社、東芝欧州研、ジュネーブ大学、Telecom ParisTech and LTCI らが 6 地点を結ぶ量子暗号ネットワークの屋外実証実験に成功[11]し（M.Peev（AIT）らによる)、日本では、2010 年に NICT を中心として日本電気株式会社、三菱電機株式会社、日本電信電話株式会社ら、計 7 機関が、6 拠点からなる高秘匿通信ネットワーク(M. Sasaki(NICT)らによる)を敷設ファイバ上に構築し、高秘匿 TV 会議の実証に成功[12]している。いずれのデモンストレーションも、光ファイバベースの位相変調方式から量子もつれ光子を用いたもの、さらに前者では自由空間量子鍵配送まで組み込まれ、ニーズ・用途に応じた秘匿通信リンクを組み合わせた秘匿通信ネットワークを実現している。スイスでは、id Quantique 社の量子暗号装置が、国会選挙において集計データを通信する際に使用された（2007 年 10 月）[13][14[。さらに南アフリカでは、FIFA サッカーワールドカップに合わせて Durban スタジアムと治安当局の間での通信に量子暗号技術

が使用されている（2010 年 6 月）[14][15]。いずれも期間限定の使用例ではあるものの、特定回線の秘匿性を確保するために量子暗号技術が使用され始めている。

２．量子鍵配送技術

2.1　概要

現在実用化に最も近い量子鍵配送(QKD)技術は、1984 年 Benett と Brassard によって提案された BB84[8]プロトコルをベースにした Decoy[16-18] BB84 と呼ばれるものである。BB84 プロトコルは、図 2.1.1(a)(b)に記載するように、送信者から受信者へ単一光子(量子チャネル)によって暗号鍵の元となる乱数をランダムに割り振った基底(+、X)に合わせて送付する。受信者は光子をランダムに基底を選択して光子を検出する。光子を検出したときの基底と送信した基底を照合(基底照合)し、送受で一致したものだけを暗号化鍵として用いる。伝送路の途中に、盗聴者がいたとしても単一光子はそれ以上分割することができないので盗聴者と受信者が同じ光子情報を持つことができないこと、たとえ盗聴者が光子を観測後伝送路へ光子を戻したとしても、盗聴者は正しい基底情報を持っていないため必ず誤りを生じる(図 2.1.1(c))。そのためテストビットを送りチェックすることによって盗聴があったことを確実に検出することができる(図 2.1.1(d))。

次に上記を実現するためのシステムの概要を説明する。従来の光通信技術が 1 ビットの情報を送るのに多数の光子を用いるのに対し、量子鍵配送システムは図 2.1.2 に示すように 1 ビットにつき 1 個の光子を伝送・検出し、その情報に基づいて送信者(Alice)－受信者(Bob)間での暗号化に用いる鍵(最終鍵)の生成・共有を行う鍵抽出(鍵蒸留)処理の二つの過程からなる。鍵生成のフローを図 2.1.3(a)に、鍵生成を行う際の送受信間での手順を図 2.1.3(b)に示す。光子伝送では、鍵の元となる物理乱数によって単一光子を変調し、送信機から送出する。その際、二つの基底(＋、X)をランダムに選ぶ。受信側では、光子がどのような基底で送られてくるかわからないので、ランダムに選択した基底に基づいて光子を検出する。鍵抽出過程は、基底照合、誤り訂正、秘匿増強の三段階からなる。図 2.1.3(b)に示す送受信間の通信は、古典通信(量子レベルではないという意味)を用いる。まず、基底照合では、送出した基底、受信に用いた基底と検出データに基づいて、送受で照合のとれたもの以外破棄(残った bit をふるい鍵と呼ぶ)する。次にふるい鍵に含まれる誤り(散乱光や検出器の暗カウントによるノイズ起因)を誤り訂正処理によって排除し、さらに盗聴されている可能性のある情報量をおとす秘匿増強処理を経て、安全な暗号鍵を抽出する[19]。

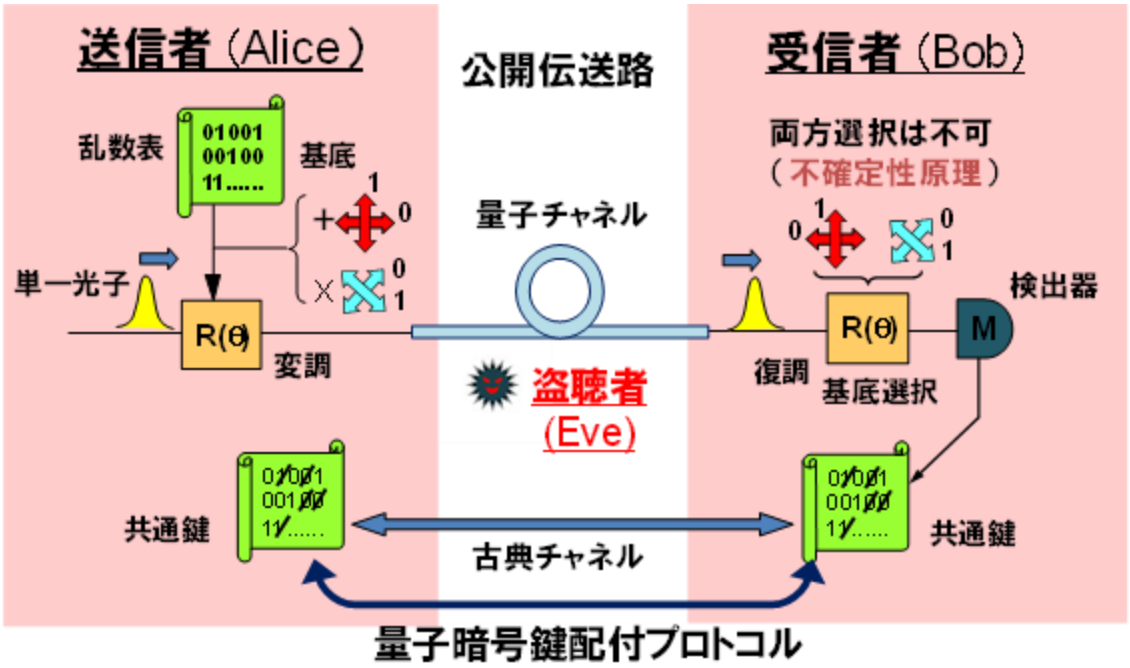


図 2.1.1(a)　BB84 プロトコル概要

送信者 Alice	送信乱数	1	0	1	1	0	0	1	1	0	0	1	1	1	0
	送信基底	✢	✕	✢	✢	✕	✕	✢	✢	✕	✢	✕	✕	✢	✢
	送信偏光	↕	↙	↕	↕	↙	↙	↕	↕	↙	↔	↘	↘	↕	↔
受信者 Bob	受信基底	✢	✢	✕	✢	✕	✕	✕	✢	✕	✢	✢	✕	✕	✢
	受信偏光	↕	—	—	↕	↙	↙	—	↕	↙	↔	—	↘	—	↔
	受信bit列	1	—	—	1	0	0	—	1	0	0	—	1	—	0
双方チェック	テストbit	○				○					○				
	完成bit列				1		0		1	0			1		0

図 2.1.1(b)　BB84 プロトコルによる鍵生成の例

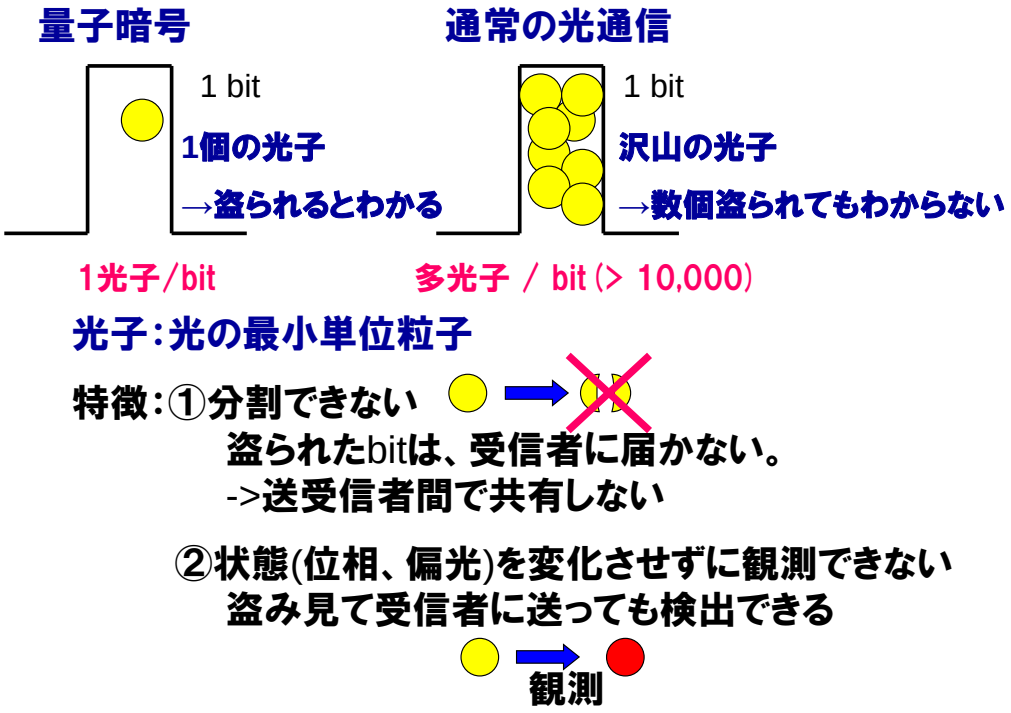


図2.1.1(c)　単一光子伝送による安全な鍵共有

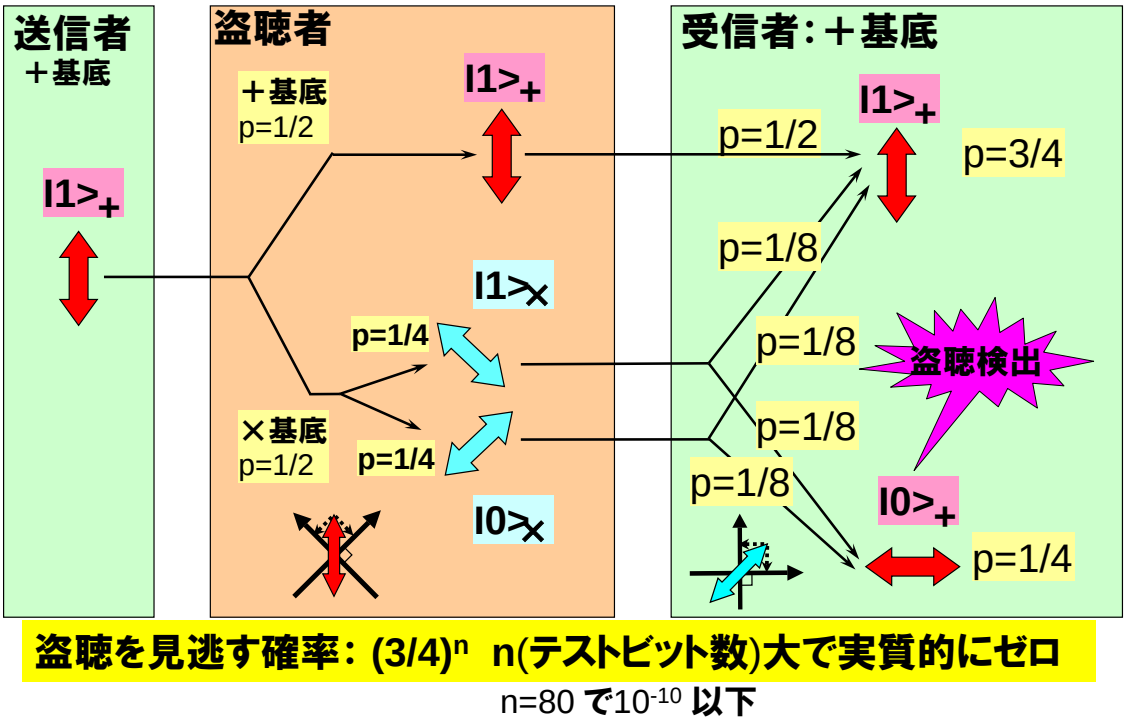


図 2.1.1(d)　盗聴＋再送出の検出

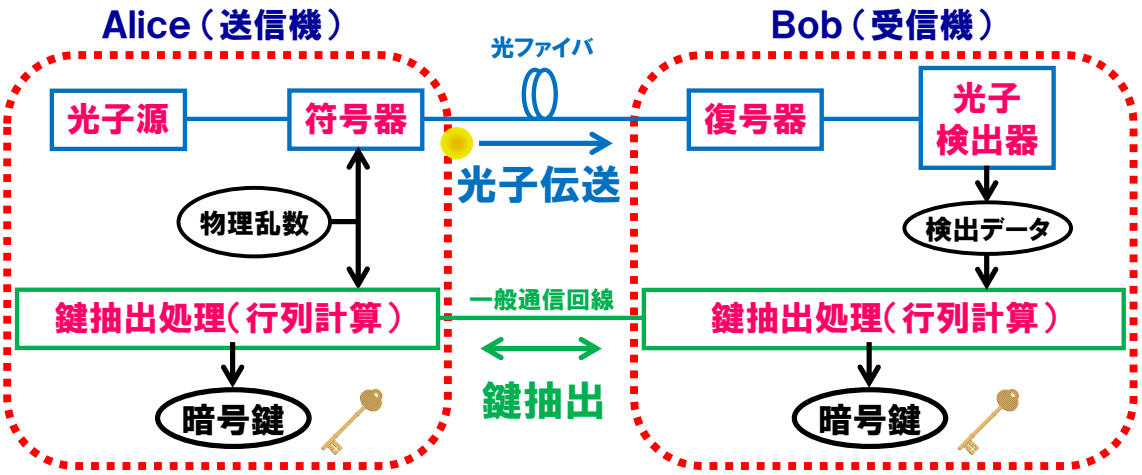


図 2.1.2　量子鍵配送システム

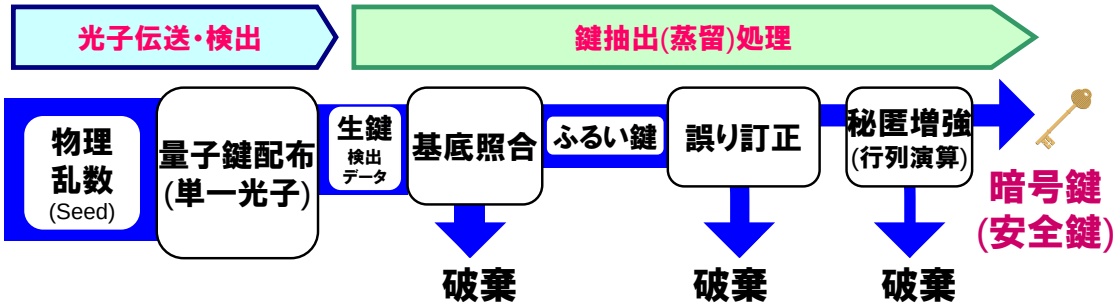


図2.1.3(a)　鍵生成フロー

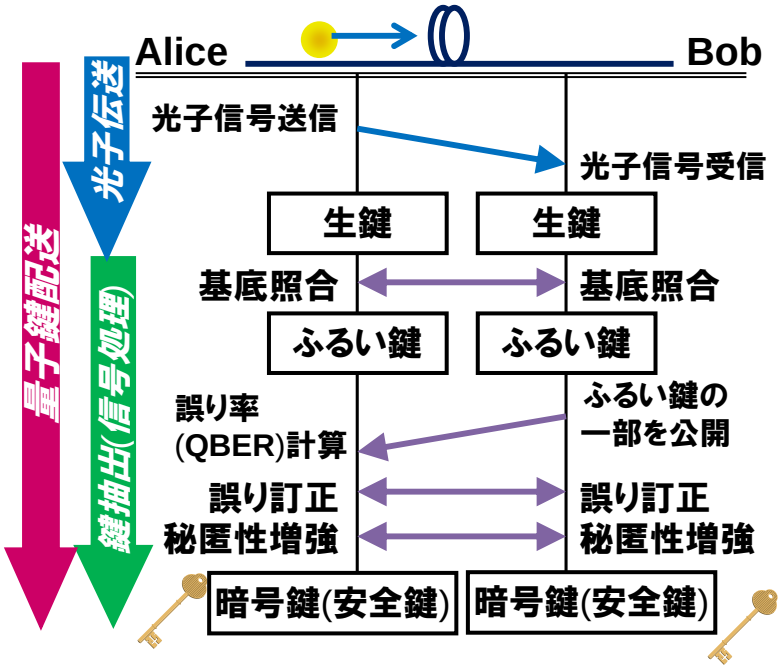


図2.1.3(b)　送受間での鍵生成手順

2.2　光子伝送要素技術

ここでは量子鍵配送システムを実現するうえで特徴的な技術である光子伝送に関して、光学系と光子検出の実現技術概要とシステム化する上での重要なポイントについて説明する。

2.2.1　光学系

図 2.2.1 に代表的な単一光子量子暗号の光学系[9][20]を示す。システムに組み込めるレベルの単一光子源がないことにより、光源として半導体レーザなどのコヒーレント光を減衰させてパルスあたりの平均光子数を 1 以下に設定し、1 パルス中に 2 光子以上含まれる確率を減らす。Photon Number Splitting(PNS)攻撃[21][22]を考慮した Decoy 法[16-18]では、さらに複数種類の強度(Signal、Decoy、Vacuum)をランダムに選択する。送信側(Alice)の光源から送り出された光パルスは非対称型マッハツェンダ干渉計 A により時間差Δt の二つのパルス(ダブルパルス)に分離され、変調器 A によって分離されたパルス間に位相差ϕ_A(＋基底:0、π、X 基底:π/2、3π/2)を設定する。光ファイバ伝送路を通って受信側(Bob)に到達したダブルパルスの片側を光変調器 B によって基底選択のためϕ_B(＋基底:0、X 基底:π/2)の変調を加え干渉計 B に入力する。干渉の結果、送信基底と受信基底が一致したときのみ検出器 PD0($\phi_A+\phi_B=0$)もしくは PD1($\phi_A+\phi_B=\pi$)のどちらか一方に光子信号が入力するので検出器でこの信号を検出し受信データ(生鍵)として用いる。送受の基底が一致しなかったときは、干渉計の二つの出力に光が分かれ PD0、PD1 両方に入力し検出されることになるので、このときの検出データは破棄する。干渉計 A で生成したダブルパルスが受信側の干渉計 B で干渉するためには、送受信器内の光学干渉計の遅延差を波長精度で一致させかつ外乱の影響を受けず安定である必要がある。また、光ファイバ伝送路での偏波はファイバの曲げや振動によってランダムに変化するため、干渉計を含む受信器は偏波無依存であることが必要である。

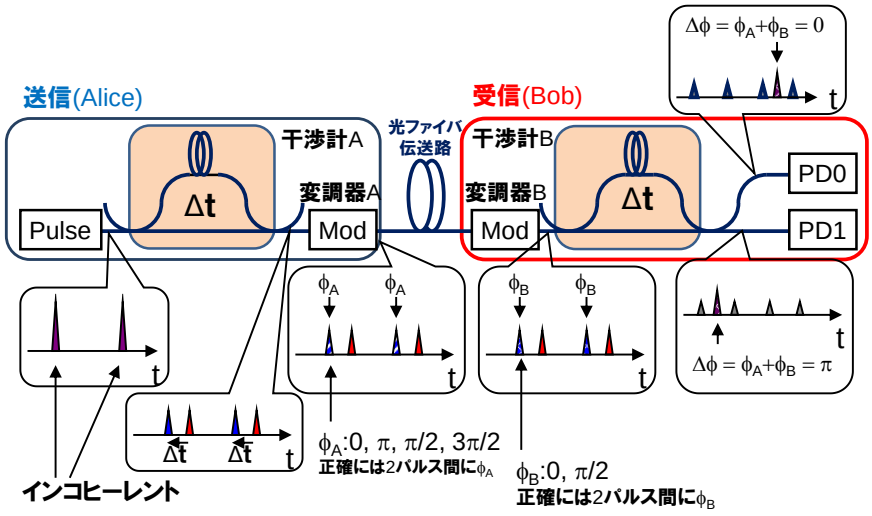


図2.2.1　代表的な単一光子量子暗号の光学系

2.2.2　光子検出器

表 2.2.1 に代表的な光子検出素子と特性の一覧を、図 2.2.2 に検出効率と波長帯域のマッピングを示す。光ファイバ伝送による QKD 技術では、伝送距離、鍵生成レートは光ファイバ損失によって決まるため、光ファイバ損失が最小となる 1550 nm 帯を用いることが望ましい[23][24]。波長帯域、検出効率、実装サイズ、信頼性から、ペルチェ素子で冷却可能な温度で検出動作する InGaAs 系 APD を用いることが一般的である。InGaAs 系 APD のダークカウント確率を減らすため、素子を冷却することで熱雑音を低減し、さらに光子が存在する可能性のある時間にだけ APD に対する印加電圧がブレークダウン電圧を越えるようにパルス電圧を印加するゲートモードを用いている[25][26]。APD をゲートモードで用いると、図 2.2.3 に示すように、充放電に伴うスパイク状雑音(容量性ノイズ)が生じるため、この影響を受けないような検出回路[27-29]が必要である。光子検出器の動作速度は、主に図 2.2.4 に示すようなアフターパルスと呼ばれる現象によって制限される。アフターパルスは、直前の光子検出時の残留キャリアが種となって生じるなだれ現象であり、その確率は時間と共に減少する。従って、アフターパルスによる誤りを排除するため、残留キャリア寿命程度まで光子信号の時間間隔を空ける必要がある。これが動作速度の制限要因である。また、高速動作時には個体差の影響が顕著になることも動作速度制限要因となる。

表 2.2.1　光子検出素子と特性一覧

素子	波長帯	検出効率	温度	速度	現象
PMT	紫外～赤外	0.001~ 0.01	室温	~ MHz	電子増倍
VLPC	可視	0.9	~ 数 K	~ 10 MHz	
Si-APD	可視	~ 0.5	< 室温	~ 10 MHz	ダイオードのブレークダウン
Ge-APD	1 ~ 1.3 um	~ 0.01	< 200K	~ 10 MHz	
InGaAs-APD	1 ~ 1.6 um	~ 0.2	< 200K	~ 1 GHz	
SSPD	可視～赤外	~ 0.8	~ 数 K	~ 10 GHz	超伝導の破壊

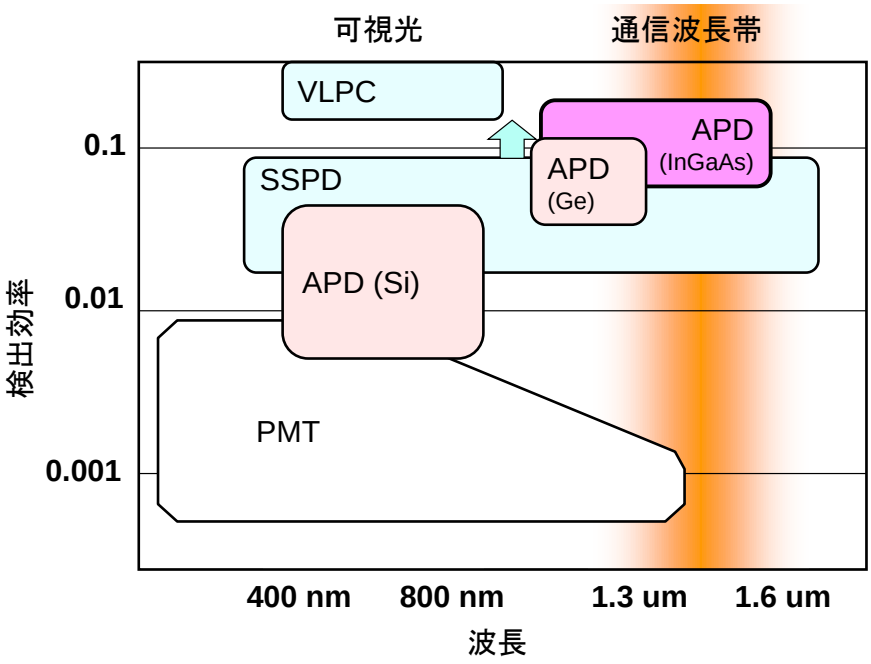


図 2.2.2　検出効率と波長帯域のマッピング

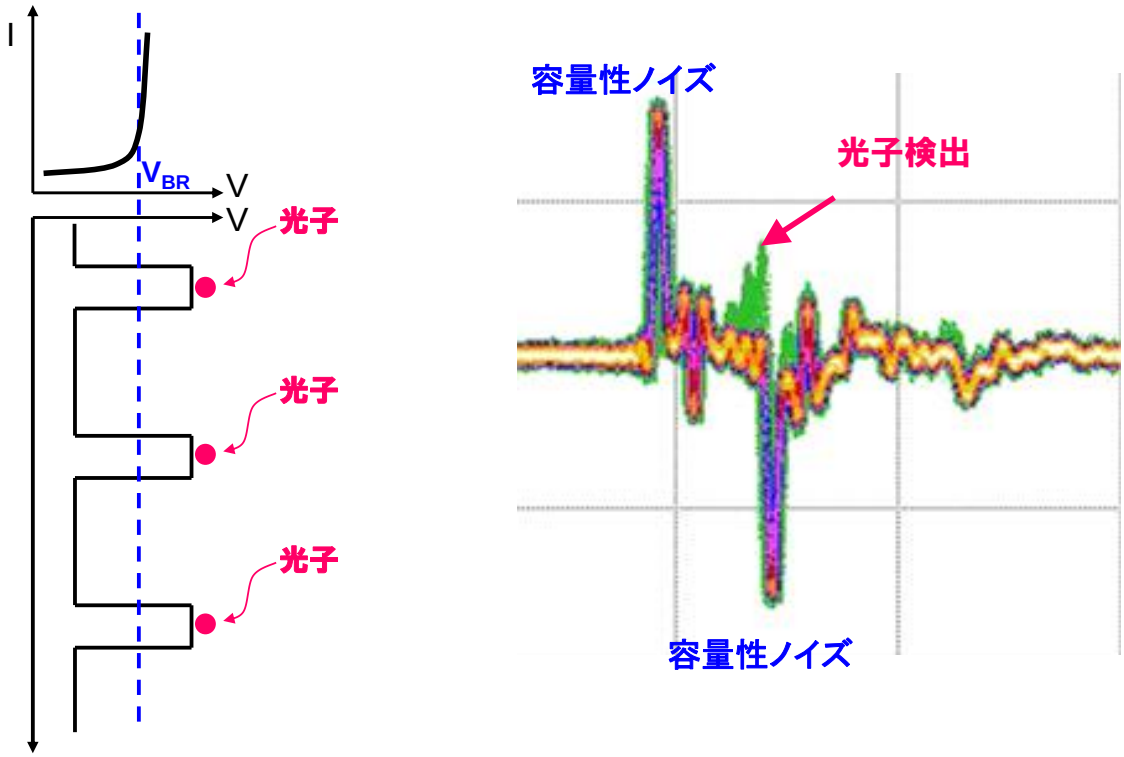


図 2.2.3　APD をゲート駆動したときの光子検出波形

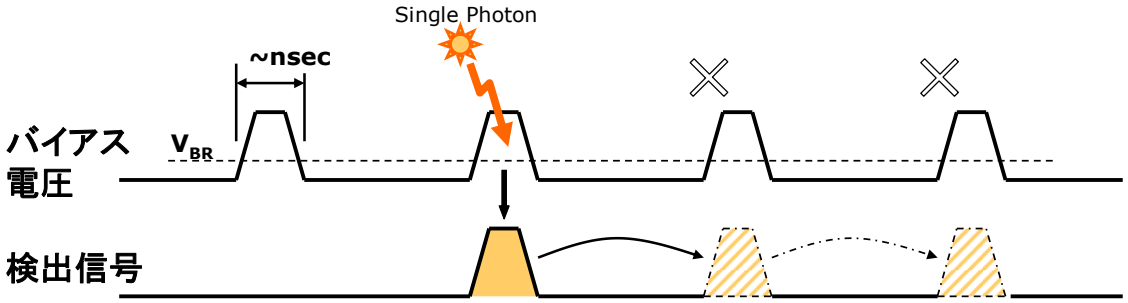


図 2.2.4　アフターパルス現象

2.3　実用化に向けた研究開発動向

1989 年の Bennett 等による距離 30 cm の空間伝送実験(鍵生成レート~10bit/s)[30]、1993 年の Townsend 等による 10 km の光ファイバ伝送実験(光子検出レート 20 KHz)[31]が行われて以来、光子をいかに短い時間間隔で送り出し、いかに遠くへ伝送し検出するか、すなわち鍵生成レートの高速化と長距離伝送という光子レベルの伝送技術を中心に研究開発が進められてきた。1996 年に Gisin 等によって考案された Plug & Play 型[32]とよばれる QKD によって光ファイバ中の擾乱の一つである偏波変動の影響を受けないシステムが実現され、研究の重点が実験室内での実験から、フィールドファイバでの実証実験にシフトしはじめた。2000 年頃からレマン湖の湖底に敷設された 67km ファイバでの実験[33]、けいはんな地区 96 km のフィルードファイバでの実験(鍵生成速度 8.2 bps, QBER = 9.9%) [34]、中国北京-天津間 125 km での実験 (QBER = 6%) [35]をはじめとするフィールドファイバを用いシステム実験の報告が相次いだ。NEC は、世界で初めて光子伝送・検出だけでなく安全鍵生成まで一気通貫で行うフルシステムを用いて商用アクセスファイバを介した 2 週間の安定化動作試験に成功した[36][37]。アップコンバージョン技術を用いた検出器[38]や超伝導検出器[39][40]による特性改善についての報告が行われるとともに、安定したシステムが実現されたことによって、2005 年頃からは鍵配送ネットワークとしての研究が行われるようになり、米国ボストン[41]、オーストリア ウィーン[11]、東京[12]で量子鍵配送ネットワークテストベッド構築とデモンストレーションが行われた。2010 年頃には、GHz クラスの高速動作かつ低雑音の光子検出器[42]-[44]が実現されたことにより最終鍵生成速度 Mbps[45]-[46]の高速化が達成された。近年では商用化を見据えた半年レベルの安定化試験[46][47]やネットワーク運用、アプリケーションとの連携[48]が行われるようになっている。表 2.3.1 にこれら量子鍵配送技術の進展のトピックスを、図 2.3.1 に研究開発の潮流を示す。

表 2.3.1　量子鍵配送技術の進展

1970	Basic idea of QKD Two non-commuting observables	Wisner
1984	BB84 protocol First QKD protocol, two bases of the same 2D Hilbert space[8]	Bennett, Brassard
1989	First QKD experiment 32 cm free space transmission, polarization-based QKD[30]	Bennett
1993	10 km over optical fiber Phase-modulation-based QKD [31]	BT
1996	Plug & Play QKD Self-balanced interferometer, 23 km transmission[32]	Geneva Univ
1997	Multi-user QKD based PON	BT
2000 ～	Practical QKD experiments (including field trial) Under lake leman [33] Keihannna area 96 km field trial [34] Beijing and Tianjin 125 km [35] Two-weeks continuous QKD [36][37] Differential phase shift QKD w/ SSPD [40]	 Geneva Univ. Mitsubishi team Univ. of Science and Technology of China NEC NTT
2005 ～	Quantum Key Distribution Network R&D Boston area QKD network [41] QKD Network in Viena [11] Tokyo QKD Network [12]	 BBN, Boston U., Harvard U. SECOQC Pj. Japan (NICT) team
2010 ～	High-speed QKD System Sinusoidally gated APDs [42] The self-differencing avalanche photodiode [43] Self-training single-photon detector [44] PLC based WDM QKD system [45]	 Nihon Univ. and NTT Toshiba NEC NEC
2015 ～	Stable QKD system (30+ days) Koganei-Ohtemachi [46] Koganei-Fucyu[47], Cyber Security Factory (21-week) [48]	 Toshiba NEC

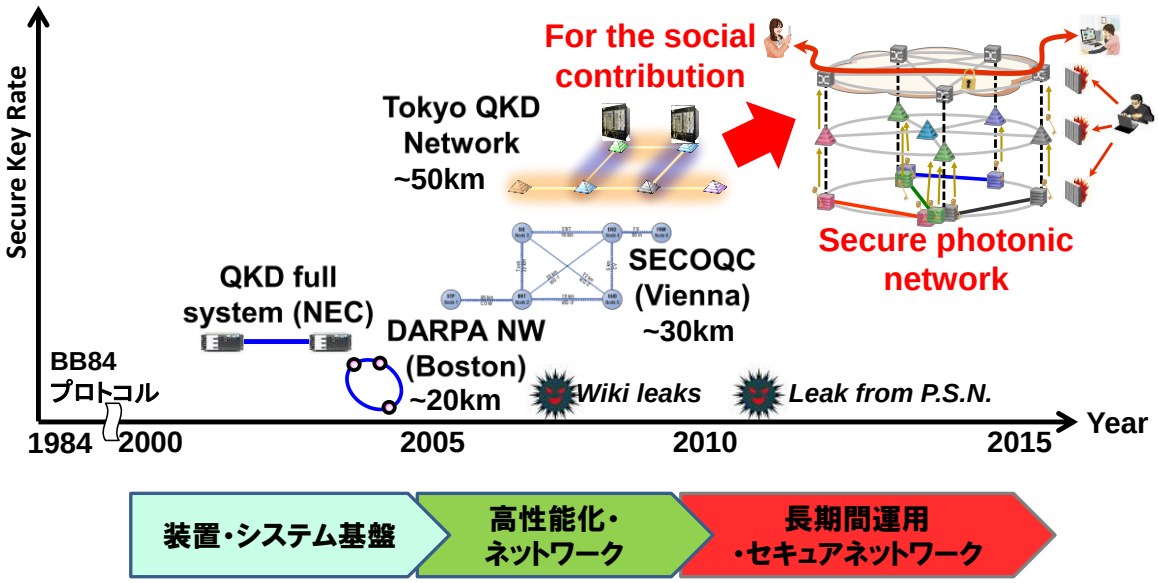


図 2.3.1　量子鍵配送技術および量子鍵配送ネットワークの研究開発動向

３．量子鍵配送システム技術

2 章で説明したように、従来の光通信技術が 1 ビットの情報を送るのに多数の光子を用いるのに対し、量子鍵配送技術は図 2.1.1 に示すように 1 ビットにつき 1 個の光子を伝送し、その情報に基づいて送信者(Alice)－受信者(Bob)間での暗号化に用いる鍵(最終鍵)の生成・共有を行う。このような技術を活用し実際に運用する場合、一般室内環境下に装置を設置し、屋外環境の光ファイバ伝送路へ接続して、長期間安定かつ連続動作することが求められる。しかしながら、これまでは、光子伝送と最終鍵生成をシームレスに結びつける技術が確立されていなかったため、実使用環境下で長期間にわたって連続して最終鍵の生成・共有を行った報告はなかった。そこで、我々は伝送された情報から最終鍵をシームレスかつ連続に生成・共有するリアルタイム連続鍵生成システム技術の研究開発に取り組んだ。さらに、実使用環境下で運用するための課題として、微弱な光信号である光子信号を使用環境や伝送路での変動、擾乱があった場合でも安定に変調・伝送・検出する安定化技術の研究開発に取り組んだ。以下でそれぞれについて説明する。さらに、これら技術を組み込んで試作した装置をアクセス系光ファイバに接続して長時間連続最終鍵生成実験を行い、世界初となる 14 日間以上の連続動作に成功した結果について述べると共に光スイッチを用いた 1:2 量子鍵実験結果および異機種システムの相互接続実験を行った結果について述べる。

3.1　リアルタイム量子鍵生成技術

これまでは、光子伝送と、最終鍵生成をシームレスに結びつけるシステム技術がなかったため、光子伝送から最終鍵生成・共有を実使用環境下で長期間連続して行った報告は無かった。そこで、実使用環境下で最終鍵を連続に生成し続けるために必須な bit 同期、フレーム同期[49]、異常検出と再同期技術からなる連続鍵生成システム技術[36]の確立に取り組んだ。以下でそれぞれについて説明する。

3.1.1　bit 同期技術

量子暗号鍵配送を実現するためには、図 3.1.1(a)に示すように光パルスに同期した位相変調や光子検出器でのゲートパルスが必要である。光ファイバ伝送路は、環境温度変動により遅延特性が大きく変動する。たとえば、20 km のファイバが温度 10℃上昇すると、62.5 MHz の 1 タイムスロット相当である 3.2 m 伸長する。図 3.1.1(b)に示すように同期未確立では、干渉計の消光比が大きく変動する。通常の光通信技術では、光信号から同期用クロック信号を抽出して用いることで、これらの変動の影響を受けない技術が確立されている。しかしながら、量子鍵配送は単一光子伝送であるため、光パワーが非常に小さく、光子信号自身からクロックを抽出することができない。そのため、光子信号の変調・受信タイミングを合わせることすなわち bit 同期が実現できないという問題がある。この問題に対しては表 3.1.1 に示すように、①光子信号とは別の信号を同じ光ファイバに多重伝送して、常に光子信号の変調・受信タイミングの同期をとる方法[49]、②送信側、受信側でそれぞれ原子発振器のよう

な高精度なクロック源をもち、変調・受信のタイミングずれを検知した場合に位相設定を初期化する方法[50]、の二つアプローチがある。光ファイバは温度をはじめとする外部環境の変動で遅延が大きく変動するため、②の方法では遅延変動による初期化が頻発すること、特に動作速度が高い場合には初期化完了前に変動が許容値を超えることが懸念される。そこでアプローチ①を採用した。光子信号(以下量子チャネル)と同期信号は波長の異なる信号によって多重化した。この同期信号は、量子チャネルとは異なり通常の光パワーの信号(以下古典チャネル)である。この同期信号は量子チャネルと同一のファイバを伝送するため、ファイバの伸縮によるタイミング変動を反映することができる。しかしながら、(1) 群速度遅延(GVD: Group Velocity Delay)と(2)クロストークの問題がある。以下でそれぞれについて説明する。

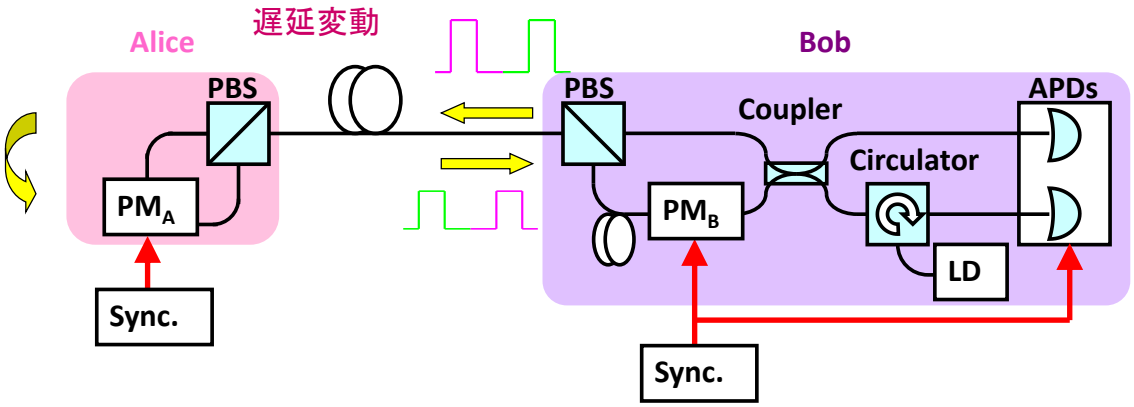


図 3.1.1(a)　bit 同期の必要性

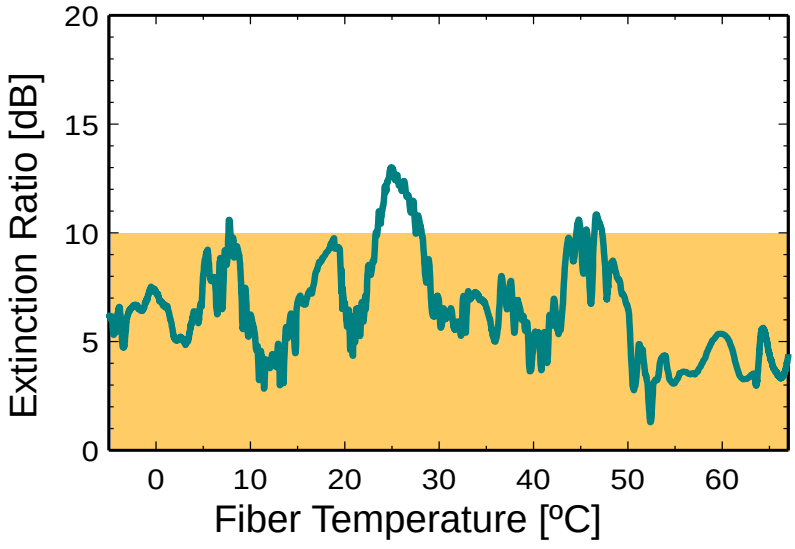
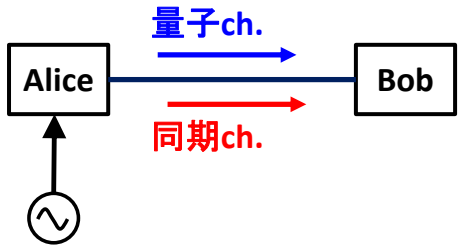
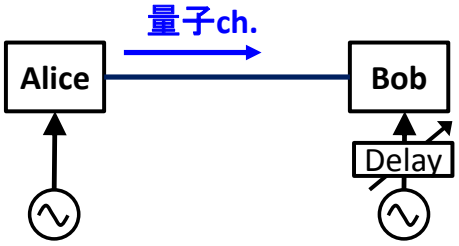


図 3.1.1(b)　干渉計消光比の温度依存性(bit 同期未確立)

表 3.1.1　QKD システム向け同期技術の比較

①　WDM	②高精度クロック源
● 量子 ch.と別の波長によって同期信号送信 ● ファイバ遅延変動に確実に追従 ● 高速動作にも対応 ● 同期 ch.による雑音 ● 群速度分散による量子/同期位相差 ● 低コスト	● 送受それぞれに高精度クロック源(原子発振器)を配置、受信側でファイバ遅延変動に合わせて Clock 位相制御 ● 同期 ch.不要 ● 早い遅延変動に追従不可、高速動作に不適 ● 高精度クロック源は高コスト
 NEC, Toshiba, etc.	 Los Alamos National Laboratory

(1)GVD 補償による bit 同期

古典チャネルで伝送した同期信号と量子チャネルの光パルスの位相は一致しない。量子チャネルと古典チャネルは波長が異なるため、群速度遅延(GVD: Group Velocity Delay)も異なるからである。この GVD を自動で補償する Phase Alignment 機構[49]を図 3.1.2(a)に示すように新たに組み込んだ。Phase Alignment は Delay Locked Loop 回路を用いて図 3.1.2(b)のような手順で実現している。図 3.1.2(c)に示す例では、2 ns の遅延差があった信号のエッジを本機構によって揃えられていることがわかる。同期信号と光子信号の位相が揃ったら変調器と光子検出器の bit 同期を行う。まず、量子チャネルの光干渉消光比を光子受信器で測定し、消光比が最大となるように Alice 側の変調位相を合わせ、次に Bob 側では光子受信が最大となるように受信位相を合わせる(詳細手順は(2)に記載)ことで図 3.1.2(d)に示すような高精度な bit 同期を実現した。

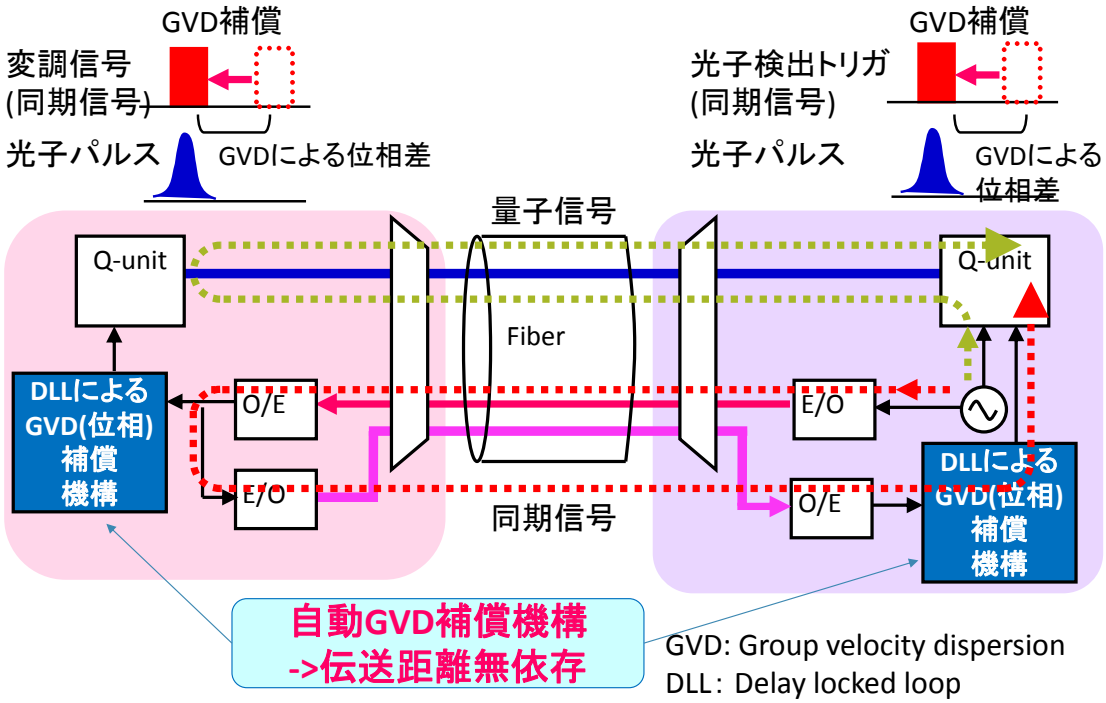


図 3.1.2(a)　自動 GVD 補償機構による bit 同期

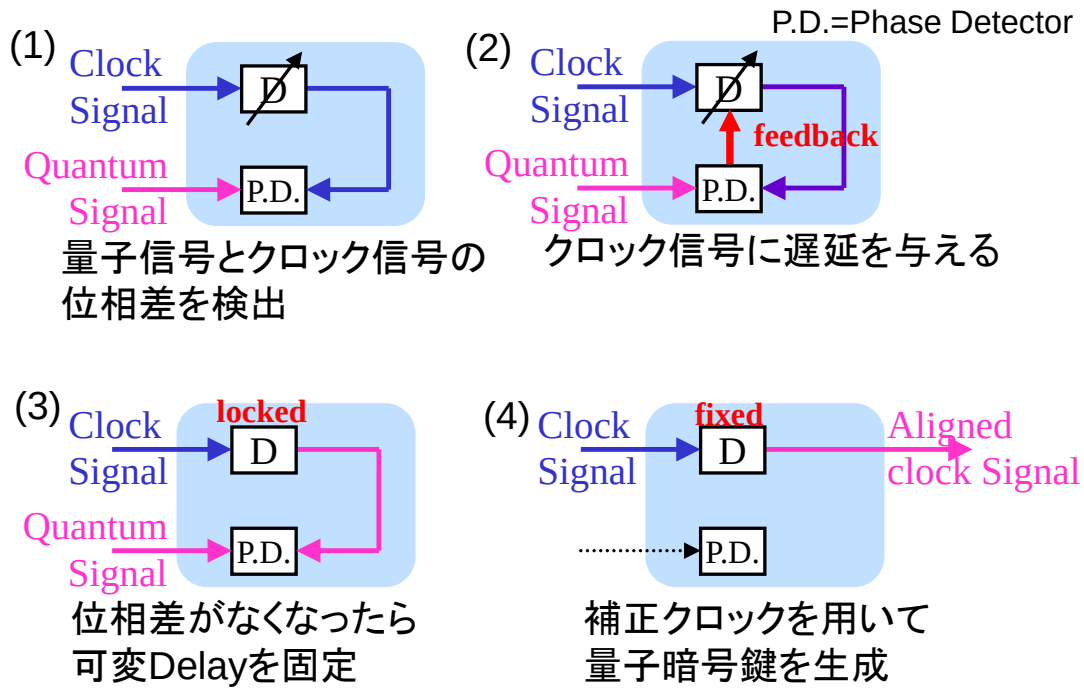


図 3.1.2(b)　DLL 技術を用いた自動位相補正機構

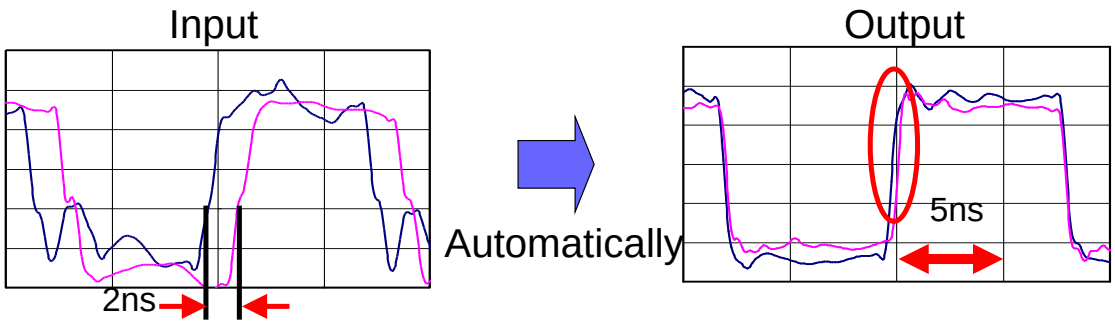


図 3.1.2(c)　自動位相補正機構の動作

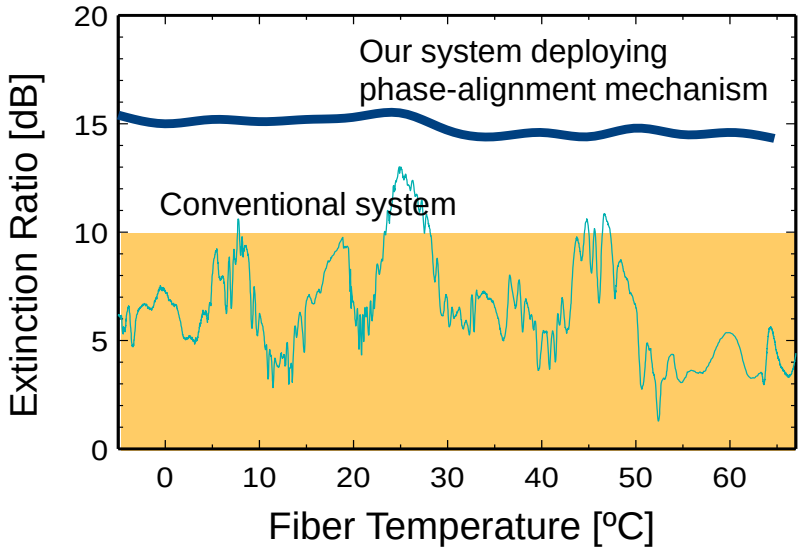


図 3.1.2(d) 干渉計消光比の温度依存性(bit 同期確立)

(2) 自動初期設定技術

(1)に記載した量子チャネルの光干渉消光比を光子受信器で測定し、消光比が最大となるように Alice 側の変調位相を合わせ、次に Bob 側では光子受信が最大となるように受信位相を合わせる方法[51]の詳細について記載する。

Alice 側変調器のタイミングを制御し消光比を最大とするようにするためには接続する伝送路に応じて平均光パワーを測定し、初期位相を設定する必要があった。しかし、光子検出器はある単位時間内の光子の有無を判定するのみで、光子検出の時間平均である平均光パワーを測定することができない。そこで、光子検出器を用いた平均光パワー測定技術を新規に提案する。図 3.1.3(a)において Bob の P.A.B.(Phase Alignment Block)は光子検出器にゲートパルスを供給するが，位相を 0 から 2π まで 2π/N rad（N は整数）毎シフトさせることができる。図 3.1.3(b)に光子カウントと平均光パワーの関係を示す。ゲートパルスの位相を 2π/N rad 毎シフトしながら各位相において受信した光子をカウントした光子カウ

ント数を P(i)とする。このとき，平均光パワーは各位相における光子カウント数の和ΣP(i)で表され，図 3.1.3(b)中の斜線部の面積に相当する。このように，ゲートパルスを掃引し，その間の光子カウント数を積分することによって，光子検出の時間平均である平均光パワーを測定することが可能となる。

本手法を用いてまず Alice の位相調整を行う。図 3.1.3(a)において Alice の P.A.B.は Bob からの指示により変調器 PM_A に供給するドライブ信号の位相を 0 から 2π まで 2π/256 rad ずつシフトさせる。1 ステップシフトする度に光子検出器のゲートパルスを 0 から 2π までシフトさせて平均光パワーを測定する。繰り返し周波数 62.5 MHz のとき，PM_A に供給されるドライブ信号の位相シフト量とそのときの干渉消光比を図 3.1.3(c)に示す。これより，ドライブ信号の最適位相は Alice が”1”を送信したとき，Bob で”1”が出力される範囲，すなわちシフト量が 9～12 ns のときである。

次に Bob の位相調整を行う。Bob の光子検出器に供給されるゲートパルスの位相を 2π/256 rad ずつシフトさせながら光子カウントを行った結果を図 3.1.3(d)に示す。ゲートパルスの最適位相は光子がカウントできる範囲，即ちシフト量が 5 ns のときである。

本手法の再現性について検証した結果を図 3.1.3(e)(f)に示す。最適位相の分布は Alice が 3 ns、Bob が 0.652 ns と量子暗号鍵を生成することが可能な範囲である。

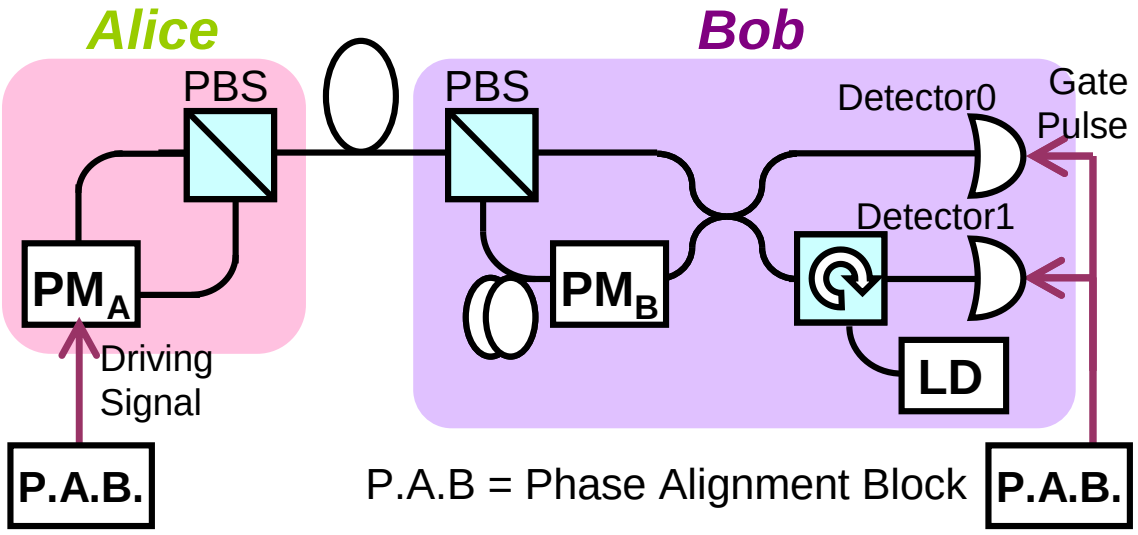


図 3.1.3(a)　自動位相補正機構の動作

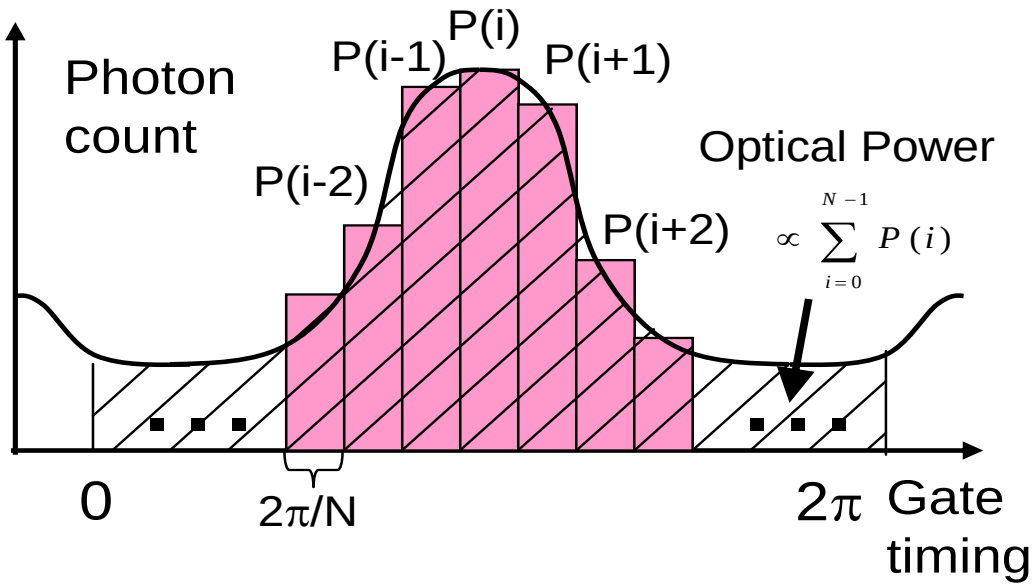
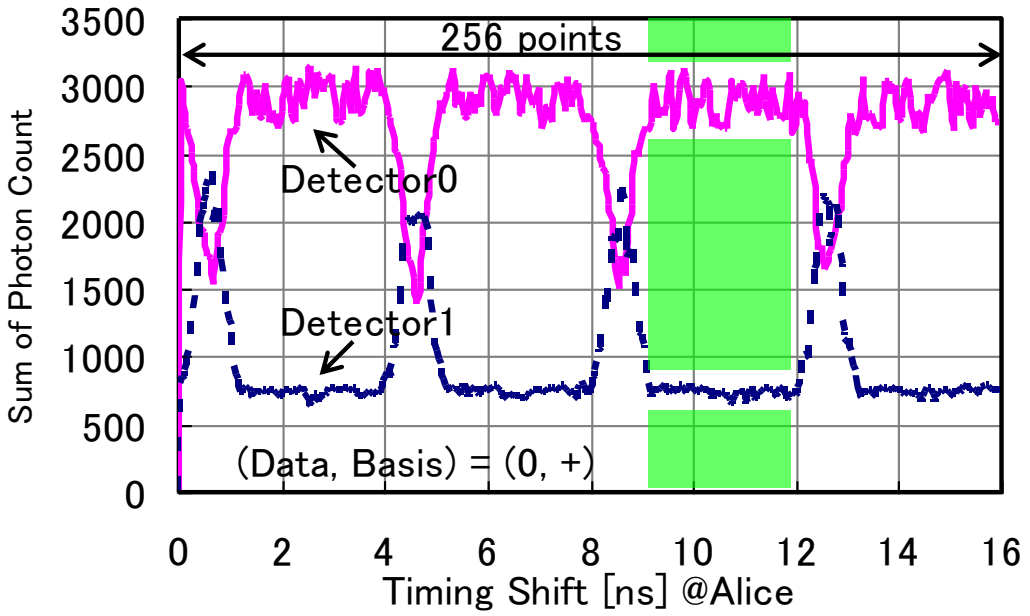
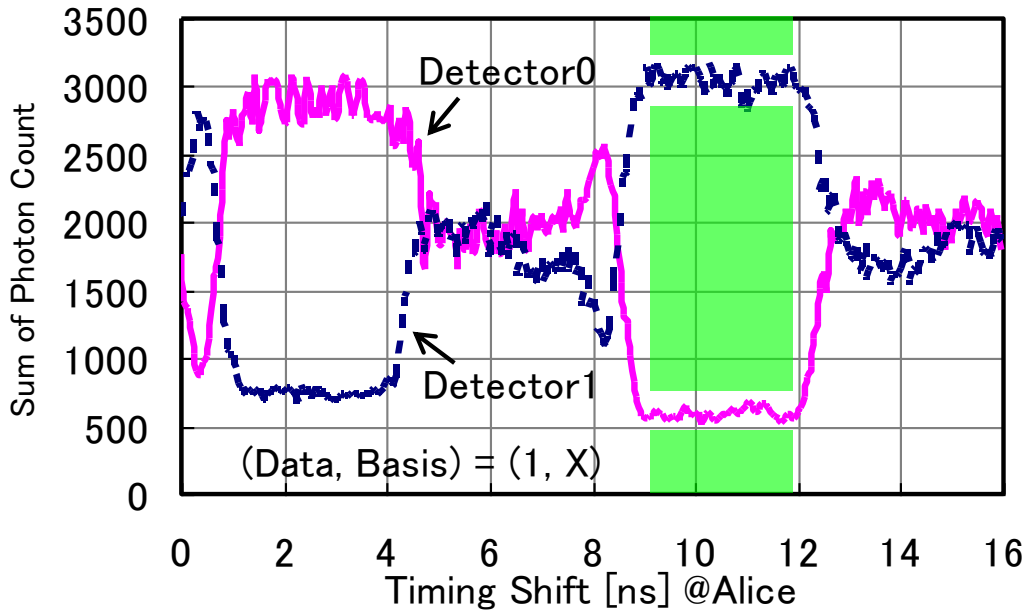


図 3.1.3(b)　自動位相補正機構の動作

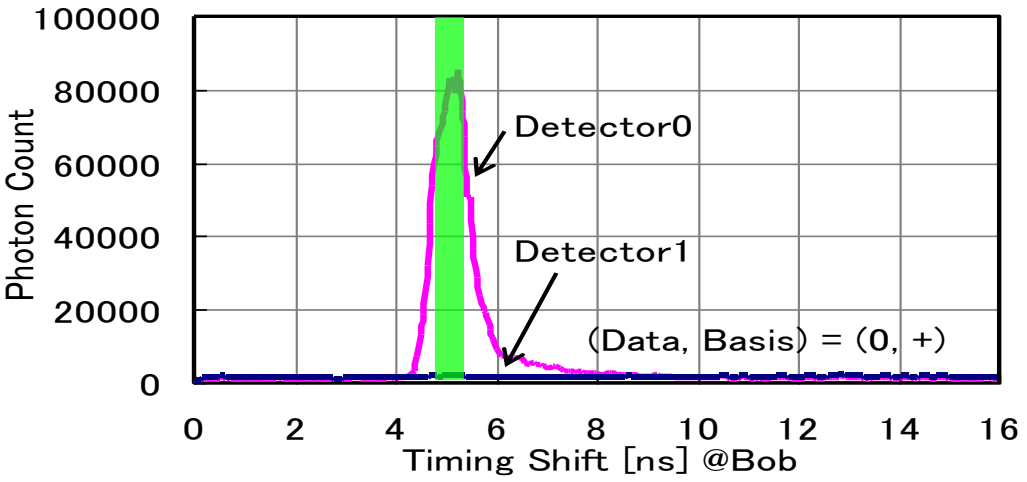


Alice (Data, Basis) = (0, +), Bob (Basis) = (+)　(Alice 側の変調器 0, Bob 側の変調器 0)

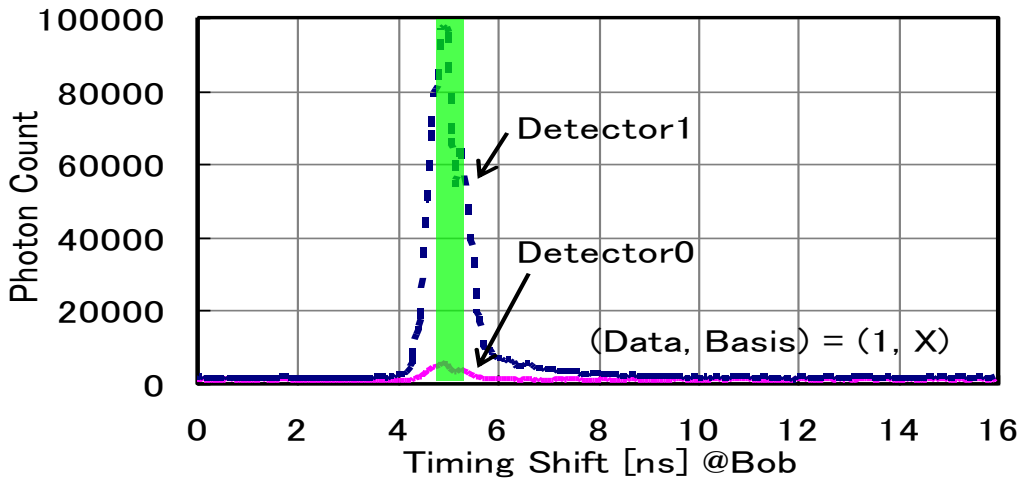


Alice (Data, Basis) = (1, X) , Bob (Basis) = (X)　(Alice 側の変調器 3/2 π , Bob 側の変調器 1/2 π)

図 3.1.3(c)　変調位相と干渉消光比の関係



(Data, Bias) = (0, +)



(Data, Bias) = (1, X)

図 3.1.3(d)　ゲート位相と光子カウント数の関係

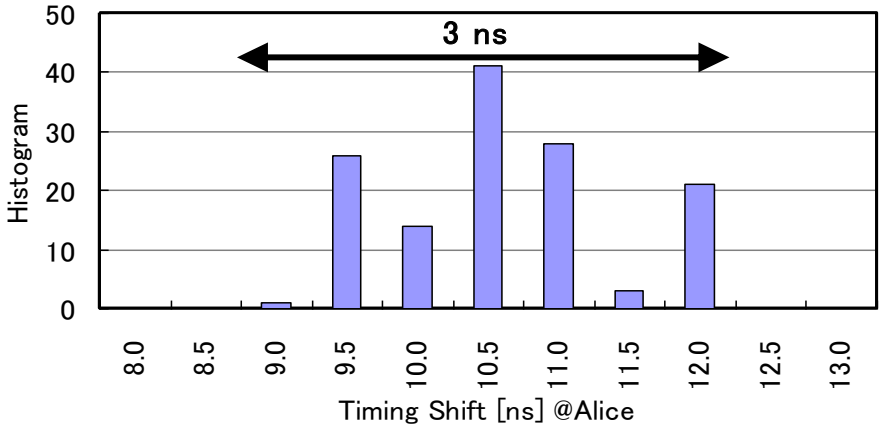


図 3.1.3(e)　Alice 最適位相分布

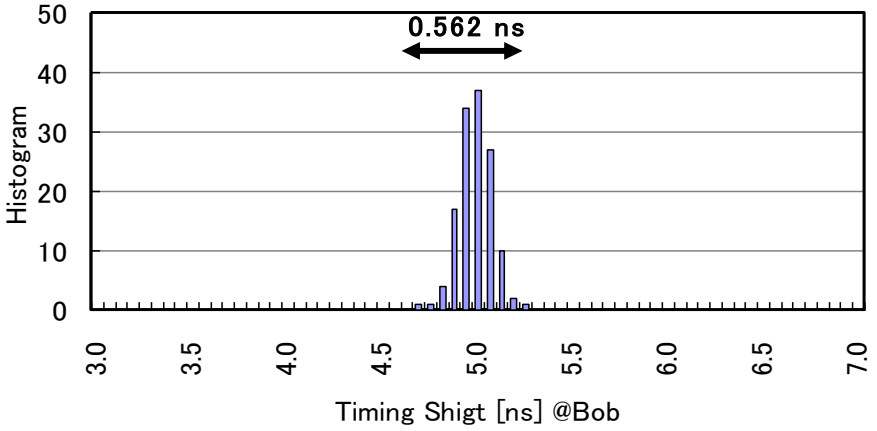


図 3.1.3(f)　Bob 最適位相分布

(3)古典信号によるクロストーク

さらに波長多重(WDM)伝送を行う際に、通常の光通信と異なり量子光信号と同期信号の強度差が非常に大きいために、図 3.1.3(a)に示すように同期信号の光源に含まれる自然放出光と図 3.1.3(b)のような同期信号の自然 Raman 散乱をはじめとする非線形光学効果による波長変換光が量子チャネルへのクロストークとして生じる。そこで、図 3.1.3(c)に示すように、波長多重時には、自然放出光の量子チャネル波長成分を抑圧(アイソレーション> 50 dB)、波長分離時には量子チャネル波長以外の波長変換光を抑圧(アイソレーション> 80 dB)するように狭帯域フィルタを用いた光多重分離器を構成するとともに、非線形雑音を抑圧するため同期信号のパワーを制御することによりクロストークを排除[52]した。図 3.1.3(d)は同期信号パワーと量子誤り率の関係を示したものである。この図より、高アイソレーションフィルタと狭帯域フィルタの組み合わせにより、光ファイバ 20 km を伝送した場合でも量子誤り率を量子鍵生成が可能な 10%以下にすることできることがわかる。

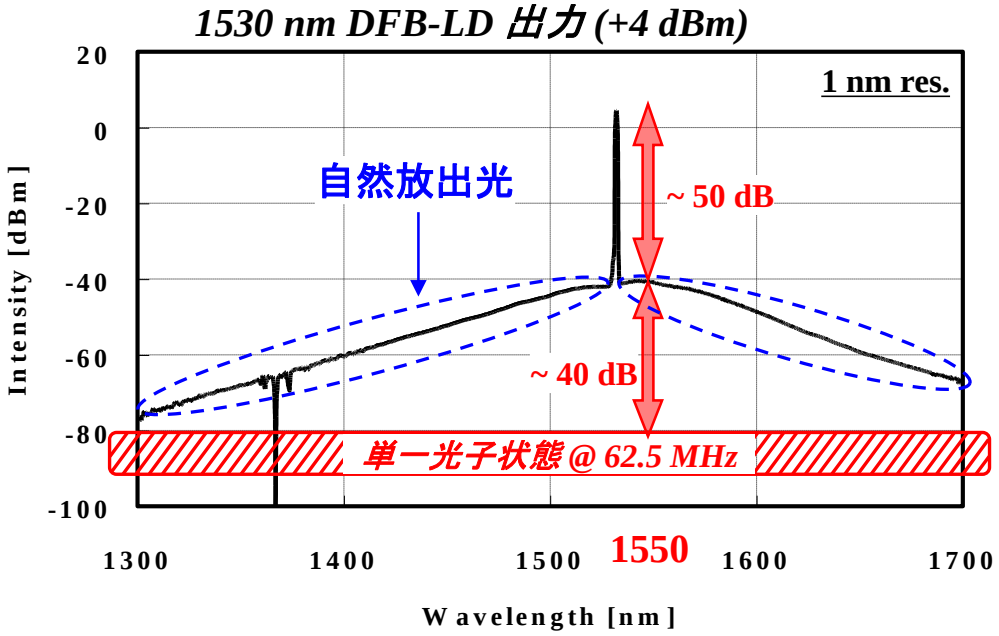


図 3.1.3(a)　同期光源の自然放出光

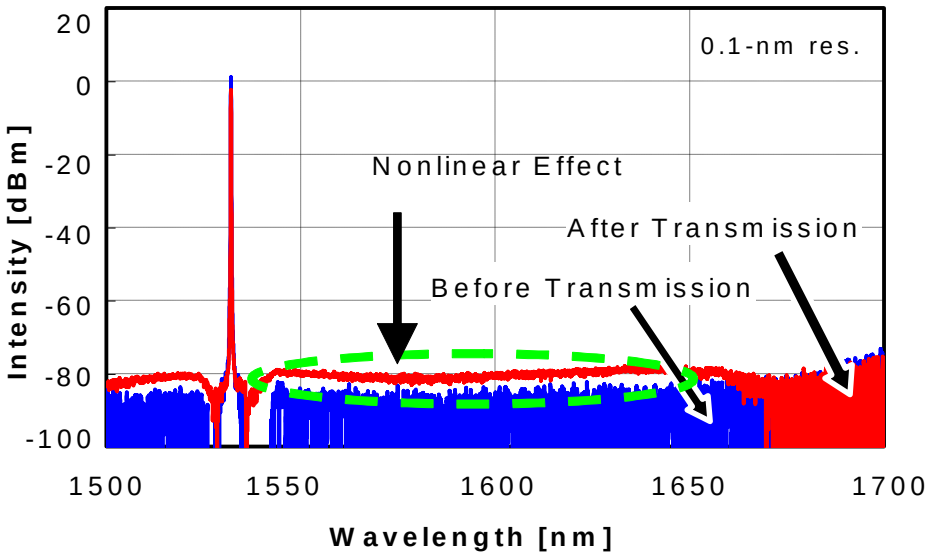


図 3.1.3(b)　量子信号への非線形クロストーク

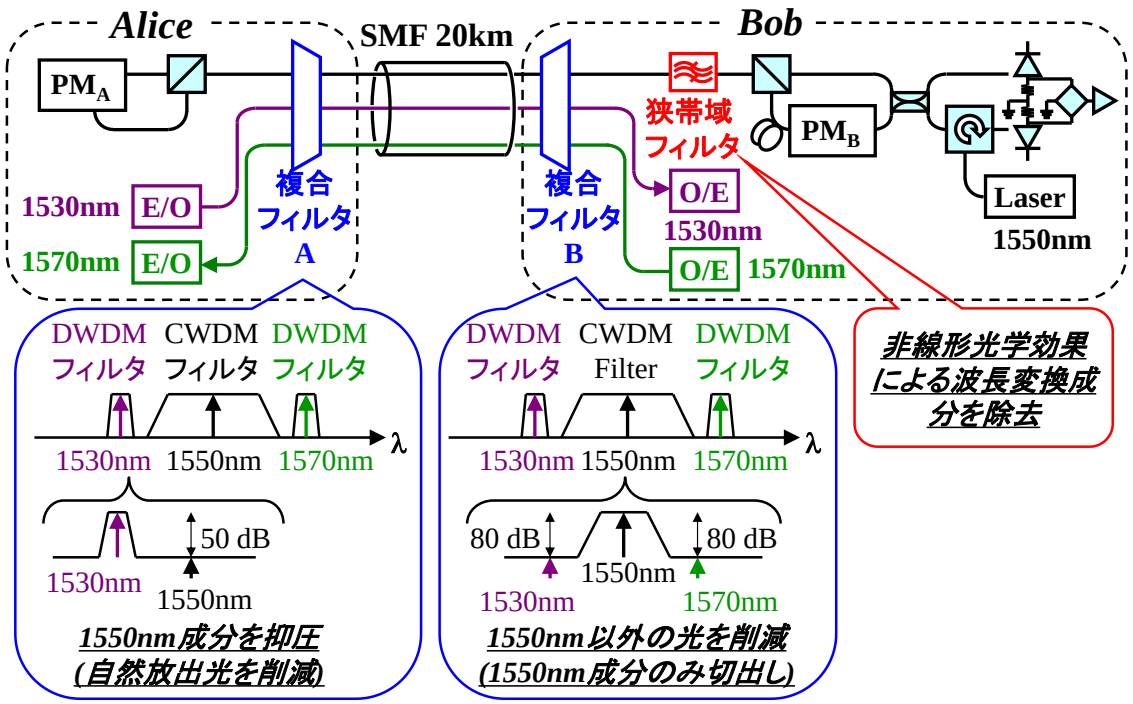


図 3.1.3(c)　クロストーク抑圧フィルタを用いたシステム構成

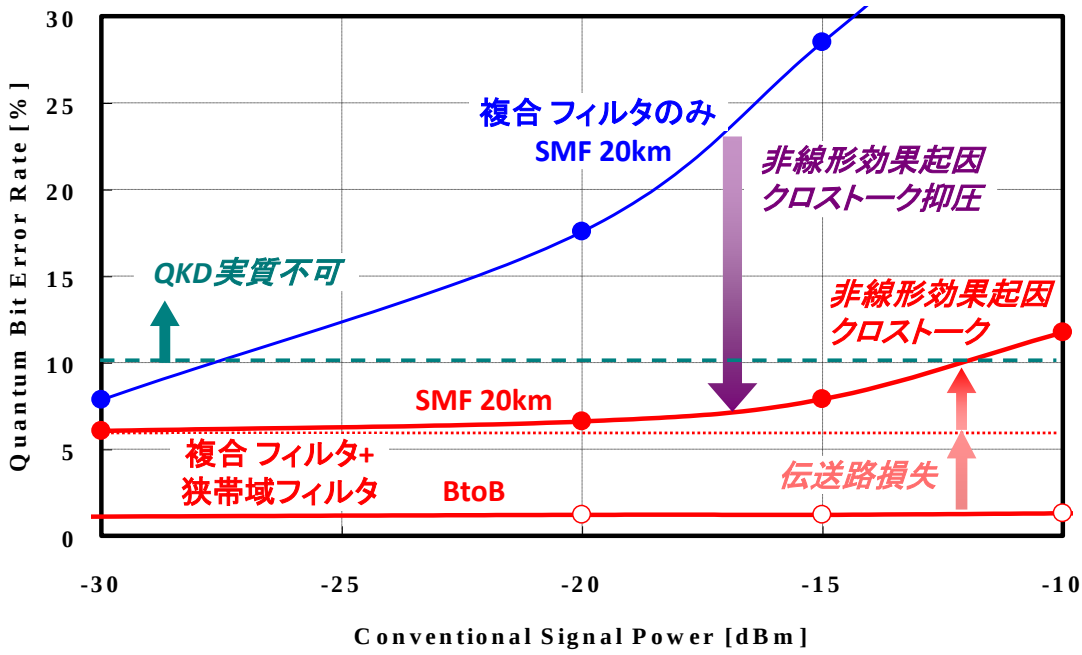


図 3.1.3(d)　クロストーク削減効果

3.1.2　フレーム同期技術

量子鍵配送では、図 3.1.4 に示すような手順により、光子伝送結果から、誤りや盗聴の疑いのある bit を基底照合／誤り訂正／秘匿増強処理によりふるって暗号化に用いる最終鍵生成・共有処理を実現する。その際、bit 同期だけではなく、Alice で送った bit と Bob で受信した bit のページの先頭を合わせるフレーム同期が必要となる。特に、光子伝送からシームレスに鍵生成処理を行うためには常にフレーム同期が確立されていなければならない。しかしながら、SONET[53]/SDH [54]のような通常の光通信と同様にフレーム同期用の固定パターンを用いることはできない。その理由は、通常の光通信では伝送誤り率が 10^{-12} 以下と誤りがほとんどないのに対し、光子伝送では伝送途中で大半の光子すなわち bit が消失してしまうためである。

図 3.1.5(a)に示すようにフレーム同期信号を別波長で WDM 伝送し同期を行う手法を採用した。但し、本手法では、bit 単位での詳細な同期位置の合わせ込みは難しいため、詳細な同期は鍵生成処理の最初のステップである基底照合処理において行った。図 3.1.5(b)に示すように基底照合では、フレーム同期が確立していない場合は、相関のないランダムな bit 同士の比較となるため、照合結果の誤り率(QBER)が 50%となるが、フレーム同期が確立された場合誤り率は 10%以下となる。従って図 3.1.5(c)のフローのように QBER をモニタしながら bit をシフトさせ QBER が 50%以下となった位置で同期確立とする[55]。図 3.1.5(d)上段はフレーム同期はずれがおきるように大きな長周期ゆらぎを与え再同期が行われていることを確認した結果である。実際は同図下段に示すように、本機構を用いることによって

フレーム同期を確立し長時間誤り率を 10%以下に維持することができることを確認した。

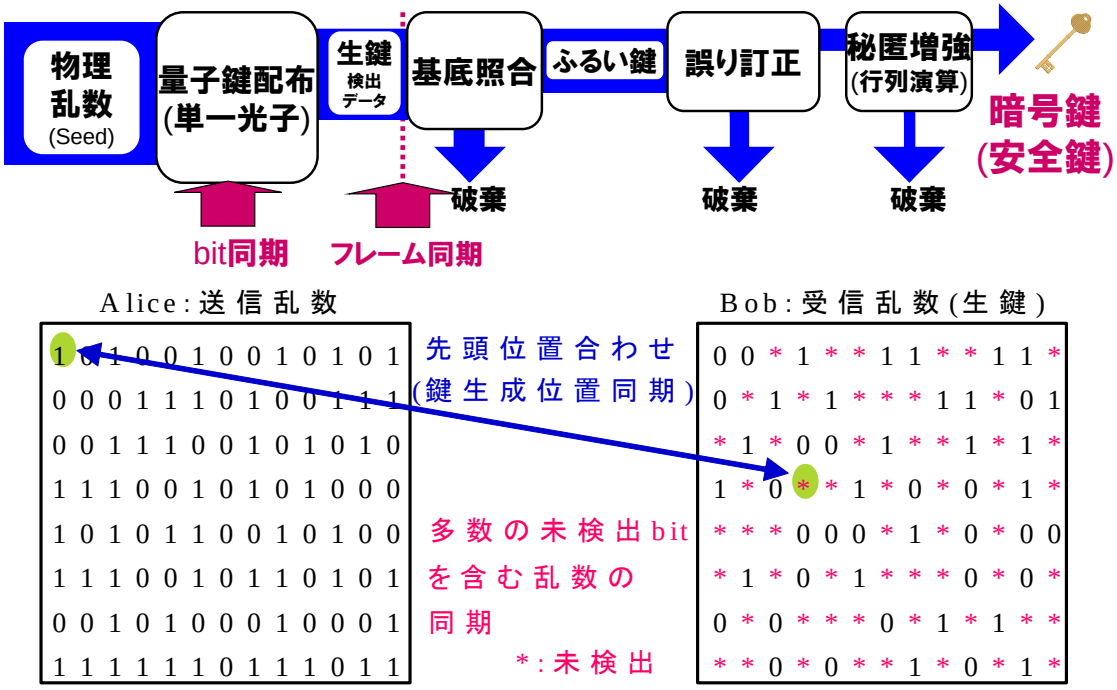


図 3.1.4　鍵抽出(鍵蒸留)フロー

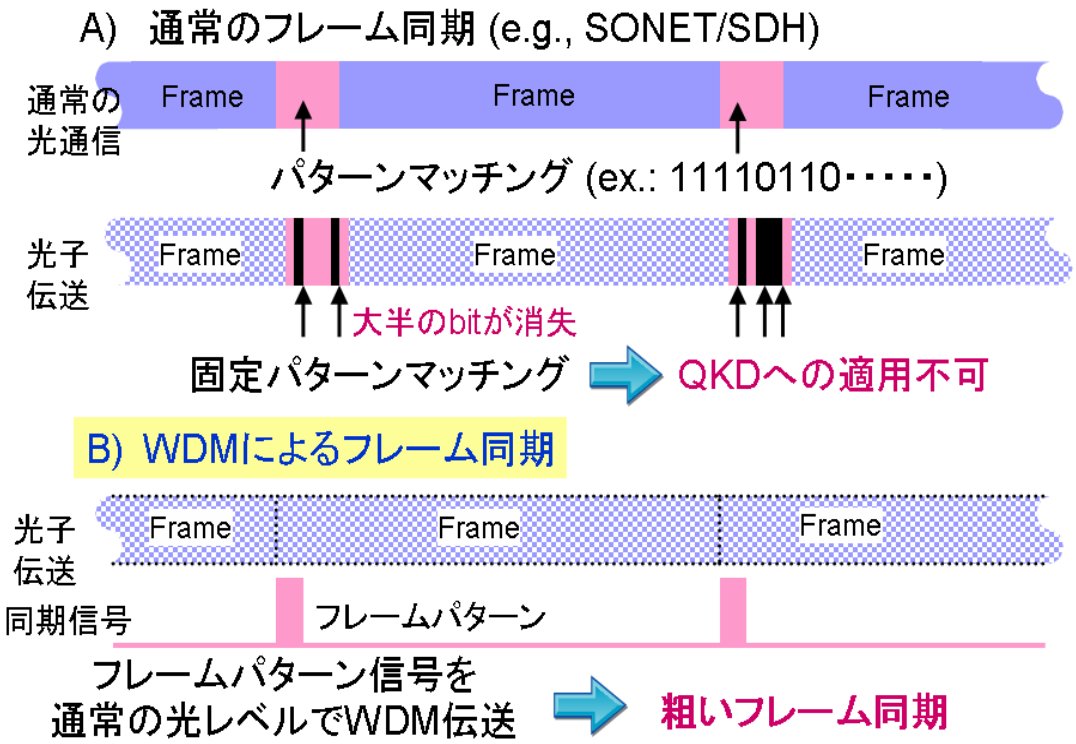


図 3.1.5(a)　フレーム同期技術

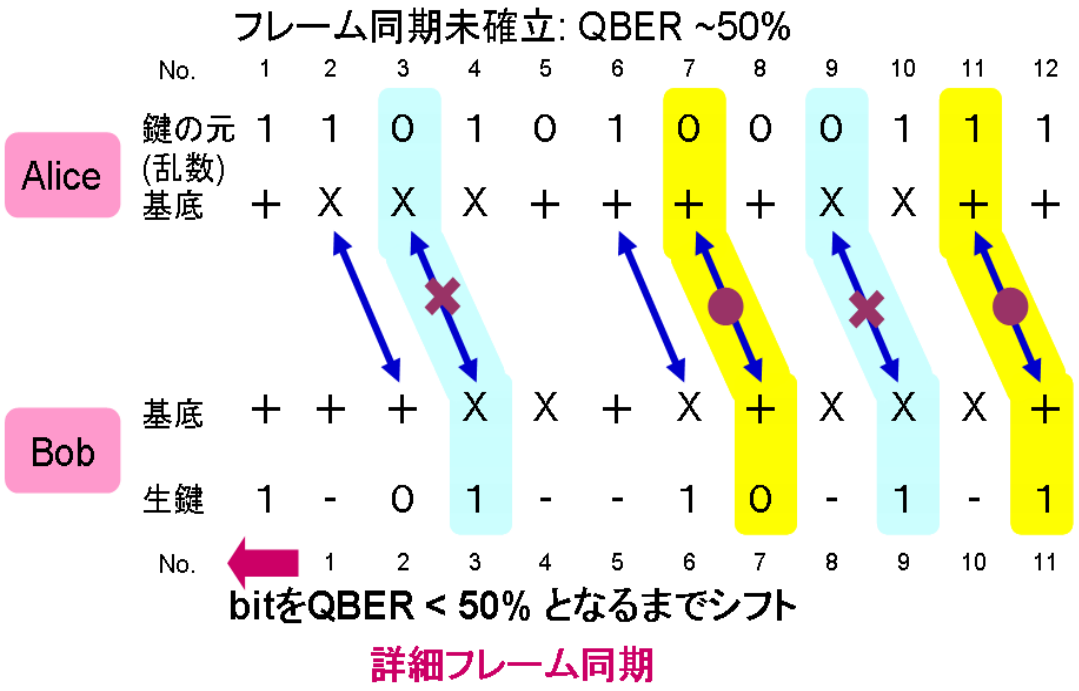


図 3.1.5(b)　フレーム同期技術(詳細)

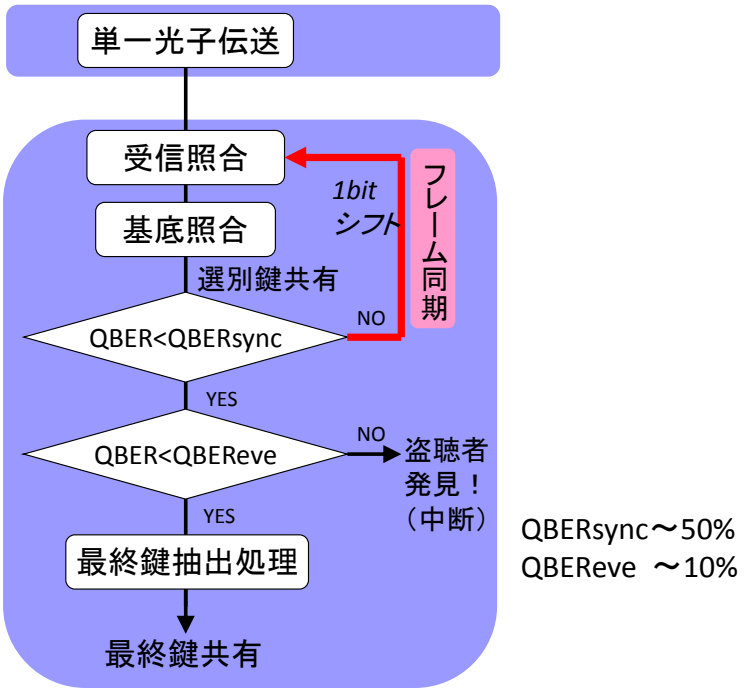


図 3.1.5(c)　フレーム同期フロー

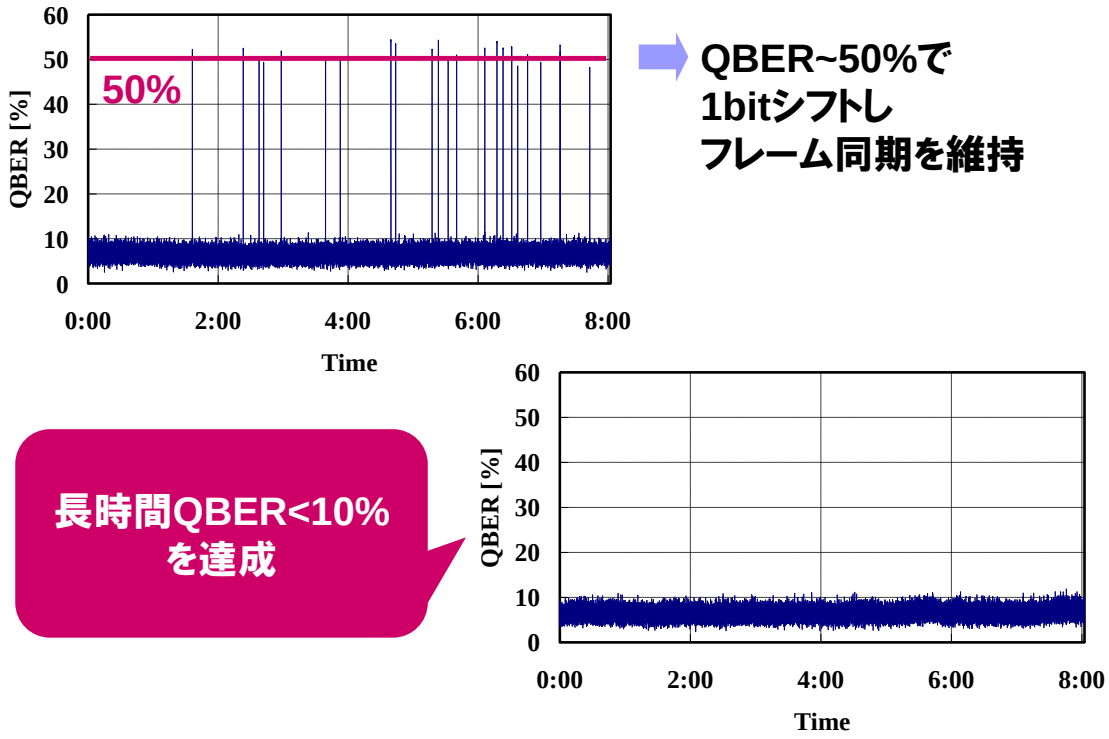


図 3.1.5(d)　フレーム同期の効果(上段:長周期揺らぎを大きくした場合、下段:実際の動作)

3.1.3　異常検出と同期復旧技術

これまで説明した技術により安定な動作が実現可能となるが、さらに実運用では、盗聴やbit/フレーム同期外れをはじめとする異常を切り分け、システム復旧や停止処理を行う機能が欠かせない。そこで誤り率(QBER)モニタによる異常検出と切り分け、そして異常に対応した同期復旧を行う機構[36][56]を新規に開発した。このスキームを図 3.1.6(a)に示す。表 3.1.2 に示すように bit 同期状態の変化は遅延変動の影響が主要因であるため、その場合 QBER は秒単位の比較的ゆっくりとした劣化となって現れる。フレーム同期状態は確立しているか外れているかのどちらかであるため、同期が外れた場合 QBER は 1 タイムスロットで約 50%へ変化する。bit/フレーム同期外れの場合 bit 位相もしくはフレーム位相をシフトさせることで復旧できる。この復旧の様子を図 3.1.6(b)に示す。復旧プロセスを経ても特性が改善されない場合は、盗聴を含む重大エラーと判断しシステムを停止させる。

表 3.1.2　bit 同期はずれとフレーム同期はずれの比較

	ビット同期ずれ	フレーム同期ずれ
QBER 劣化	比較的緩やか	急激に劣化
劣化検出 QBER 閾値	～10%(盗聴検出と区別)	～40%
復旧時間	比較的長い ハード調整を含むため	比較的短い CPU 処理のみのため

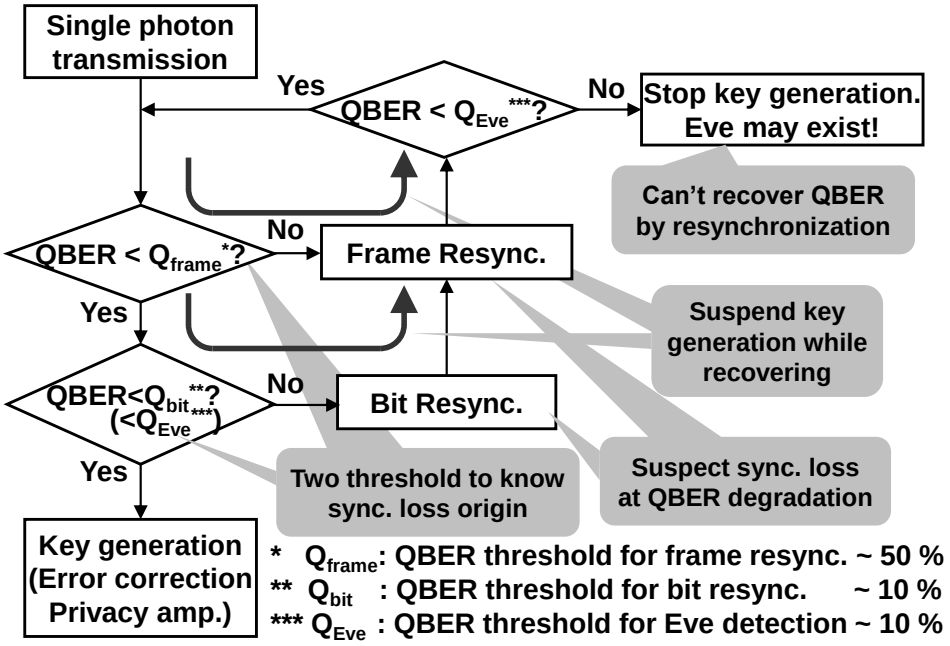


図3.1.6(a)　異常検出と再同期プロセス

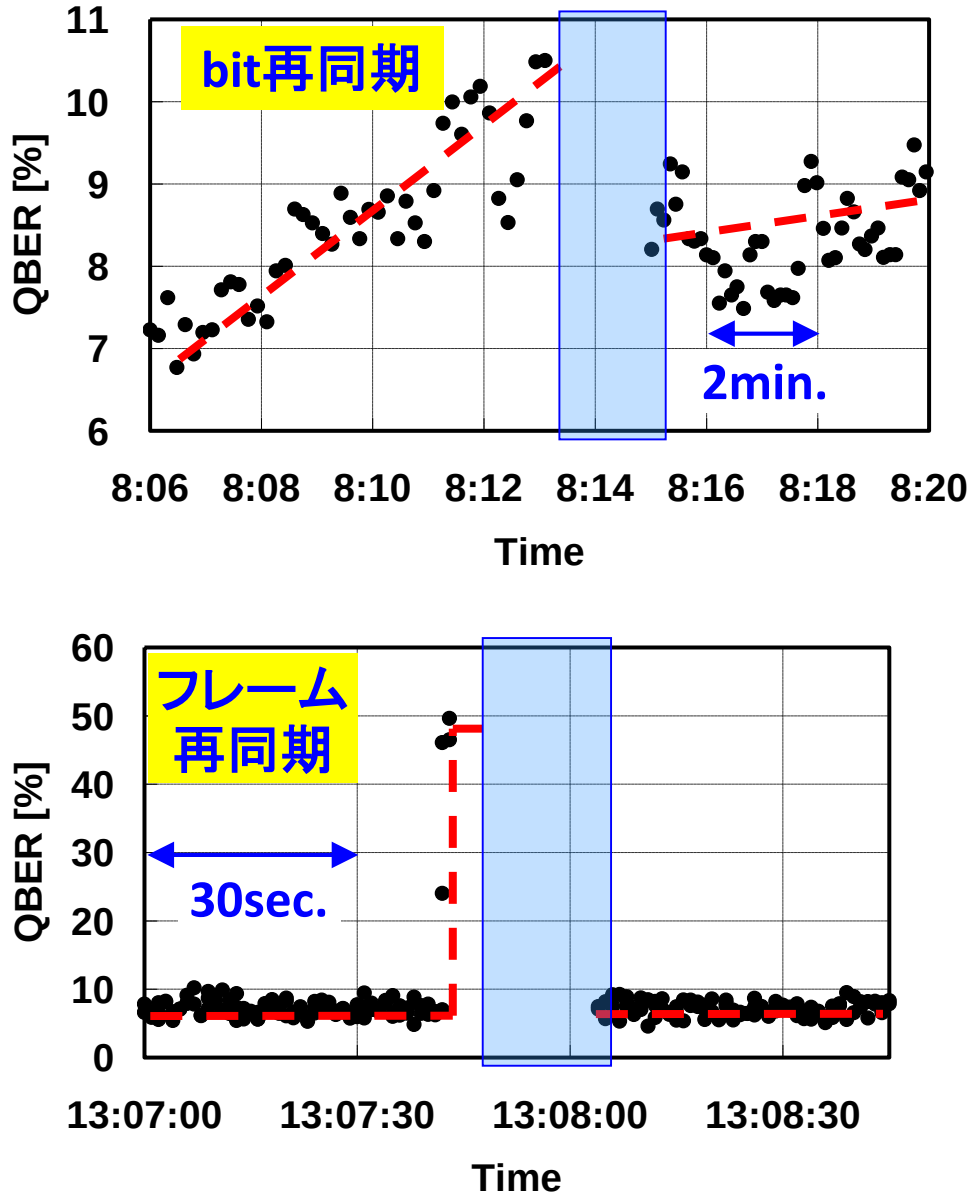


図3.1.6(b)　異常検出と再同期の様子　（上段bit再同期、下段フレーム再同期）

3.2　実使用環境下での安定化技術

量子鍵配送システムでは、単一光子の位相を変調することによって鍵の素情報である乱数を送り、受信側で光の干渉により位相情報を復調し、超高感度な光子受信器によって受信を行う。光子受信器では、熱雑音を下げ S/N 比を上げて高感度受信を実現する。そのために、Avalanche Photo Diode (APD)素子を-50℃以下に冷却してゲートモードで用いる[25][26]。従って、単一光子を使用環境や擾乱の影響を受けずに、安定して変調・伝送・検出するためには、①光干渉系を環境温度に依存しないようにすること、②広温度範囲で動作する高信頼な光子検出器を実現すること、③伝送路の接続点での反射光や散乱光の影響を受けないこと、が重要課題である。以下でそれぞれの課題への取り組みについて説明する。

3.2.1　干渉系の環境温度無依存化

実用化に適した量子鍵配送システムのひとつは“Plug & Play”システム[32]と呼ばれる往復型のシステムである。図 3.2.1(a)にその構成(Type Ⅰ)を示す。送信者(Alice)に Faraday Mirror (FM)を使用することで σ_x(Pauli 行列)の偏波回転を実現し、伝送路における偏波依存の影響をなくしている。

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Bob から Alice へ向かう光信号の偏波ベクトルを以下のように表し、

$$\overrightarrow{E_O} = \begin{pmatrix} E_x \\ E_y \end{pmatrix}$$

伝送路での偏波の回転を以下のように記載すると、

$$R_T = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

もし Alice 側での偏波回転 R_A がσ_x,であれば Alice から Bob へ戻ってくる光の偏波ベクトルは以下のように表すことができる。

$$\overrightarrow{E_H} = R_T R_A R_T \overrightarrow{E_O} = R_T \sigma_x R_T \overrightarrow{E_O} = \sigma_x \overrightarrow{E_O} = \begin{pmatrix} E_y \\ E_x \end{pmatrix}$$

これは、光ファイバを往復した際、光ファイバ伝送路での偏波変動を相殺し、入力偏波の状態が保たれることを表している。

しかし、FM の回転角には温度依存性があり、Alice での偏波回転は常に σ_x になるわけではない。環境温度が変化すると、Alice における回転角も変化し、その結果干渉系の消光比すなわち暗号鍵生成速度が劣化してしまうという問題があった。

この問題に対して、我々は図 3.2.1(b)に示す新変調方式[57]を提案した(TypeⅡ)。偏光ビームスプリッタ(PBS)と光ファイバループよって Alice を構成し、右回りと左回りの光パルス間にπだけ位相差をつけて位相変調を行うことにより FM と同じ効果を実現する。本方式を交互シフト位相変調(Alternative shift phase modulation: ASPM)と呼ぶ。ASPM は変調器の温度依存性を補償した駆動回路を用いることで温度無依存とすることができる。図 3.2.2 に Alice でのσx 回転を示す。従来の FM タイプでは、直交する二つの偏波 P_a 、P_b ともに 90°回転する。ASPM によって、これと等化な偏波回転を実現する。偏波 P_a に対しては、図 3.2.2 (b)-1 に示すように位相変調を行わない、その一方で、偏波 P_b に対しては図 3.2.2 (b)-2 に示すようにπ位相シフトを行う。さらに、FM タイプでは偏波無依存の位相変調器が必要(現状入手困難)であったが、ASPM では不要であるという実用上の大きなメリットがある。加えて、FM タイプは FM における偏波回転角の残留エラーの影響を打ち消すことができないが、ASPM では PBS や PMF をはじめとする光コンポーネントの残留エラーは位相変調によって補償することができるというメリットもある。

(a)

(b)

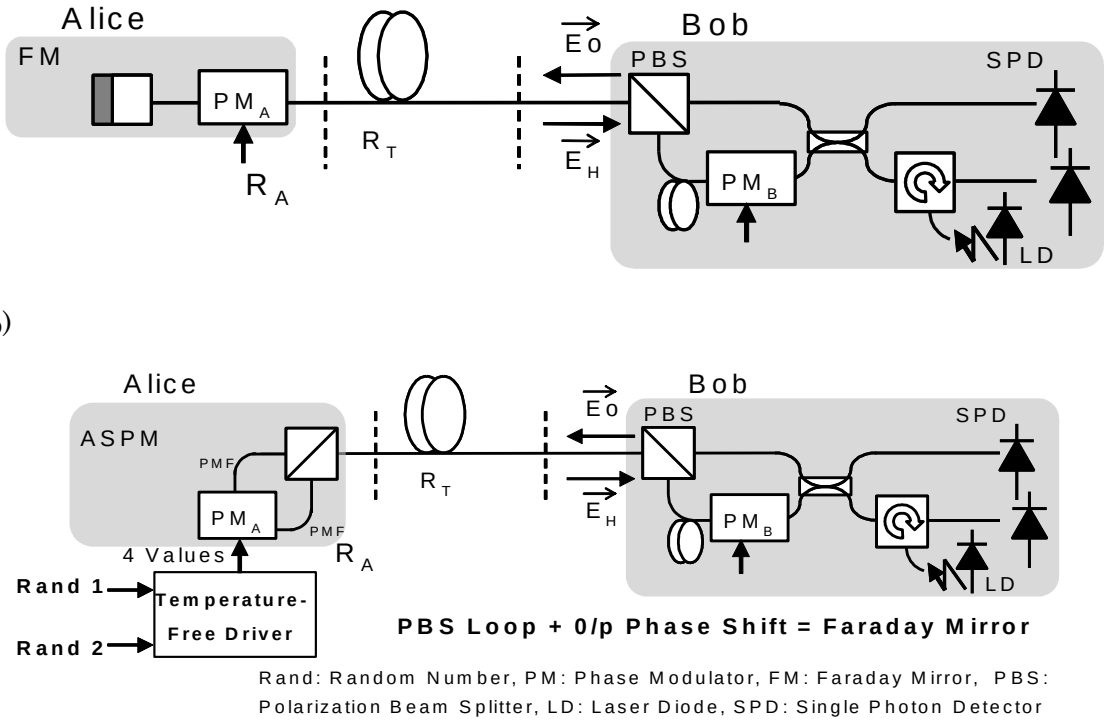


図 3.2.1 往復型 QKD の光学系構成 (a) FM タイプ (b) ASPM タイプ

(a) (b)-1 (b)-2

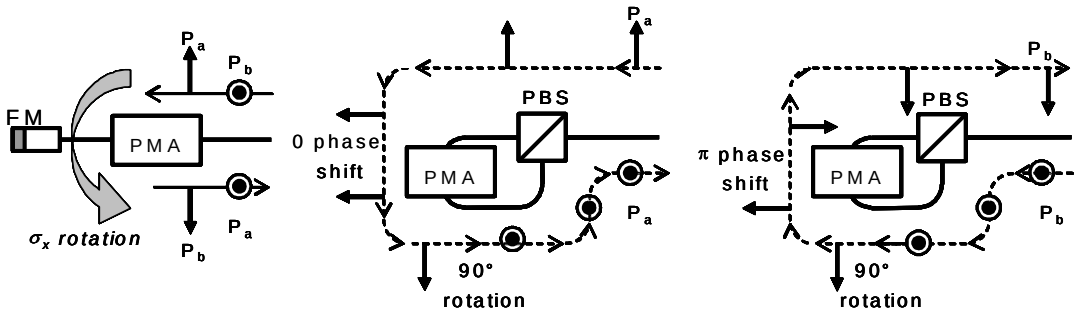


図 3.2.2　Alic 側での σ_x 回転の様子: (a) FM Type; (b) ASPM Type

図 3.2.3 に環境温度による消光比の変化を示す。図中の波線は計算結果、実線が実験結果である。これらより、温度が上がると FM タイプの消光比は大きく劣化していく一方、ファラデー素子を含まない ASPM タイプには変化が見られない。Type Ⅱ では、環境温度に依らず安定した暗号鍵を生成できることがわかる。

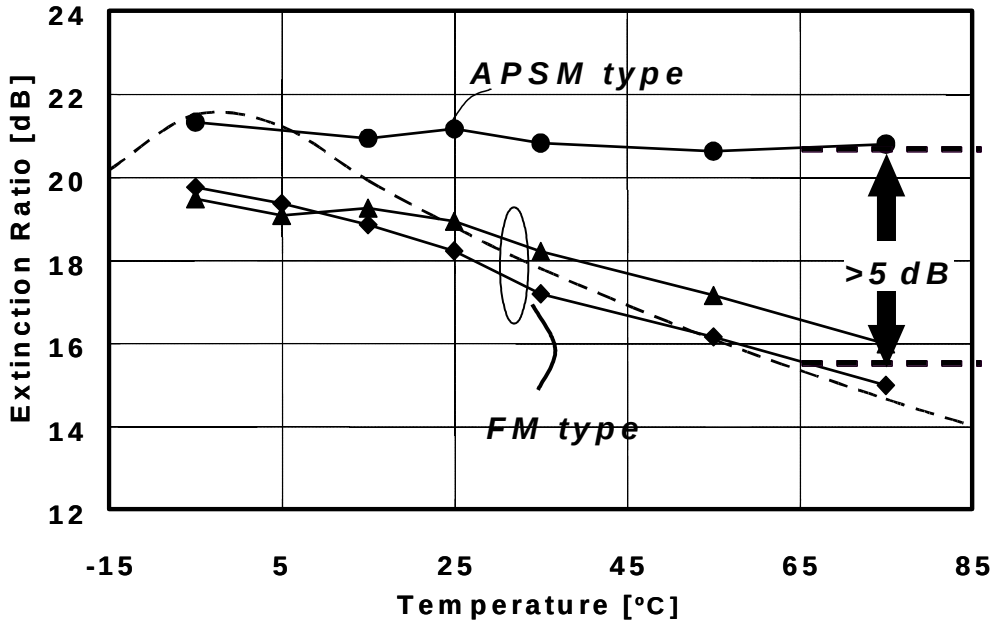


図 3.2.3　偏波消光比の温度依存性

次に、動作速度について検討する。往復型 QKD では Bob から送出された光信号は Alice で

折り返され、再び Bob へ送られる。ASPM タイプでは、Alice において図 3.2.4 に示すように光信号は偏波分離されてそれぞれ時計まわりと反時計まわりに位相変調器を通過する。従って、動作変調器は(pulse repetition frequency, f) の上限は、以下のようになる。

$$f \le \frac{1}{4nL/C + \tau}$$

ここで、n は屈折率、L は位相変調器の長さ、C は光速、τ は光パルス幅である。変調周波数の上限は、変調器の電極を伝搬する電気信号パルスを考慮して約 100 MHz となる。上記より動作マージンを含めシステム動作周波数を 62.5 MHz として設計を行った。

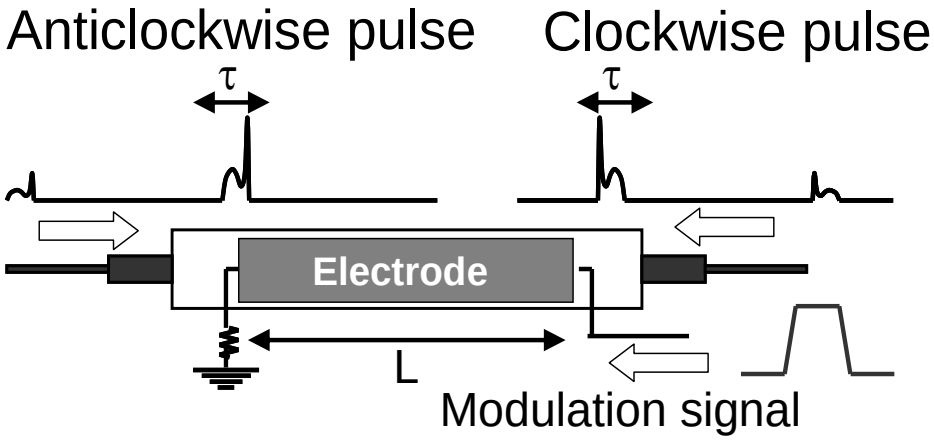


図 3.2.4　Alice における位相変調器を通過する光信号の様子

3.2.2　小型高信頼光子受信器

QKD の波長帯としては、シングルモードファイバの損失が最も低い 1550 nm 帯がもっとも望ましい[23] [24]。この波長帯での光子受信器は、InGaAs/InP 系の APD 素子を-50℃以下に冷却し受信 S/N 比を上げゲーテッドガイガーモードとする[25] [26]ことで実現する。

受信効率 η　ダークカウント確率 P_d, によってエラーレート e_B は [58]:

$$e_B = \frac{1}{2}\frac{S(1-\nu)\eta + P_d}{P_{DET}} = \frac{1}{2}\frac{S(1-\nu) + P_d/\eta}{S(1-P_d) + P_d/\eta},$$

ここで ν は干渉計の明瞭度 P_{DET} はパルスごとの検出確率を表す。P_{DET} は少なくとも 1 フォ

トンが検出器に到達する確率Sに関連する。

$$P_{DET} = S\eta + P_d - S\eta P_d ;$$

S は伝送路損失と受信器の損失の関数である。L [km]の光ファイバの伝搬損失はαL [dB]となるので、受信器の損失が β [dB]のとき、

$$S = 1 - \exp[-\mu 10^{-(\alpha+\beta)/10}]$$

となる。こここで、コヒーレント光を光子源としたときの平均光子数を μとした。エラーレートは QKD の安全性を保証できるしきい値以下とならねばならない。しきい値は仮定する攻撃や誤り訂正にもよるが、11% [59]が典型的な値である。実際に動作ささせる場合、効率的な鍵生成のためには低ければ低い方が好ましい。P_d/η は 40km 圏を想定した場合 1 x 10^{-3} 以下が望ましい。

図 3.2.5 は、二種類の APD(NEC NR8300 と EPM239BA)のダークカウント(DK) とアフターパルス(AP)確率の温度依存性を測定した結果である。-50°C 以下であればどちらの素子でもクロックサイクルあたりのダークカウント確率 1.4 x 10^{-4} を得ることができる。検出確率η = 7%.が達成できる。DK は温度と共に低下するが、素子を冷却による QKD 装置内温度上昇をさけること、ペルチェ素子で冷却可能な温度である-50°C とした。

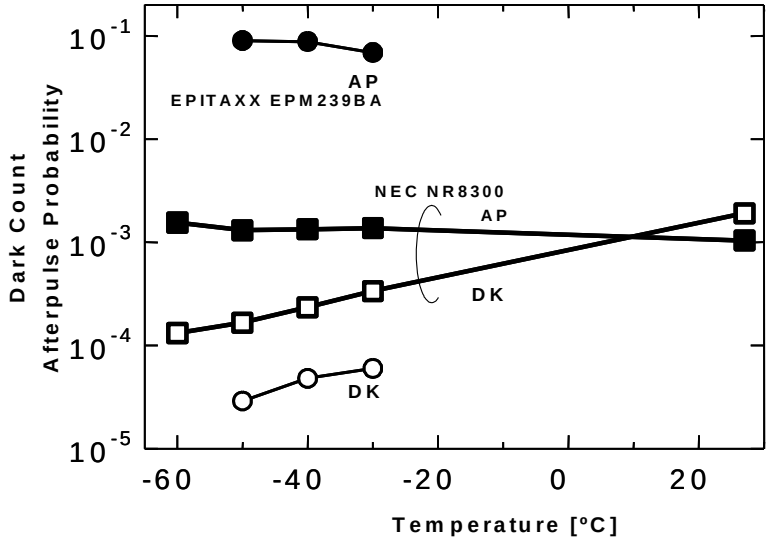


図3.2.5　ダークカウントとアフターパルス確率の温度依存性(at 16 nsec)

2.2 で説明したように QKD システムの動作速度は、主に APD のアフターパルスによって律速されているため、アフターパルス発生確率を下げるためにできる限りバイアス電圧低くする、使用温度を下げすぎないなど対策が必要である。図 3.2.5 をみるとアフターパルスはわずかながら温度依存性があること、NEC NR8300 APD/SPD の方が EPITAXX EPM239BA よりも 2 桁近くアフターパルス確率が小さいことがわかる。そこで、我々は NR8300 APD を用いることで、アフターパルス確率 1×10^{-3} とカウントレート 250 kbps を得ることができた。

冷却受信器を量子鍵配送システム装置への搭載する際、光子受信器を構成する冷却器の体積、消費電力、重量、長時間連続稼働の信頼性からの制約により、従来の実験で用いられている真空気密雰囲気や冷凍機などを用いて極低温状態を実現することは困難である。さらに、装置内の温度範囲は 0～50℃程度と広範囲であるためこのような条件下で安定して長期間動作することが要求される。このため、冷却器は、結露防止を小型で実現する常圧気密構造と、長期信頼性の観点からペルチェ素子による冷却と強制空冷による放熱方式を採用した[60]。図 3.2.6(a)に光子受信モジュールの外観を示す。コネクタは光、電気共に気密構造を採用している。ヒートシンクを含めた外寸は、150×100×82 mm^3 (突起部を含まず)である。モジュールには、高感度受信を実現するための図 3.2.6(b)に示すように差動型ノイズキャンセル回路(図 3.2.6(c))[27]からなる Trans- Impedance (TIA)回路を内蔵している。TIA は、ゲートパルスの印加と同時に APD が光子を受信することで発生する光電流を電圧に変換する回路である。トランスインピーダンスは 500 ohm である。増幅回路には、高速 OP アンプを使用した。本回路によって、図 3.2.6(d)のように二つの APD 出力の容量性ノイズをキャンセルし、高感度化を実現している。

モジュール外には、ゲート回路、識別回路、ブランキング回路、自動温度制御回路(ATC)がある。

ゲート回路は、DC バイアス電圧と、光子の入射に同期する Sync CLK を基にゲートパルスを生成する。ゲートパルス幅は約 2.5 nsec である。ゲート振幅は、一般には大振幅であるほど、S/N 比の改善が期待出来る。しかしながら、実用的な装置化を行うに当たり、増幅回路設計の制約を考慮して、ゲートパルスの振幅を最大 5 V(可変)とした。これは、ゲートパルスには、サブ nsec で遷移する高速なパルスが必要とされると同時に、ゲート間隔が 16 nsec から最大数μsec のため、パルスのマーク率 1/2 から大きく離れた信号を扱う必要がある。このような、高速・広帯域と大振幅の 3 つを同時に実現する増幅回路を設計する事は非常に困難なためである。さらに、APD に印加する DC バイアス電圧の生成と、DC バイアス電圧にゲートパルスを重畳するバイアス T 回路を含んでいる。

識別回路では、Sync CLK に従い TIA 出力の符号識別を行い、論理レベル(LVDS)に変換し、光子受信信号として CPU へ出力する。

ブランキング回路は、APD のアフターパルスによる QBER 劣化を抑制するため、APD が光子受信を行った場合には、その直後にゲート回路をある一定間隔だけ停止する信号を

生成する。ゲートの停止時間は、0 から約 2 μsec まで可変とした。

光子検出確率は温度依存性があるため自動温度制御回路(ATC)によりペルチェ素子を温度一定制御し安定した光子検出を行う。温度安定性の精度は、量子鍵生成レートの変動幅を 10 %程度に抑える事を目標とした。APD の量子効率の温度依存性(図 3.2.6 (e))から、APD の素子温度の変化に対して、バイアス電圧は 0.1 V/deg.でシフトしている。これと、量子効率ηの変化率が $d\eta/dV = 0.2$ (@η~0.1)である事から、$\Delta\eta < 0.1$ を満足する条件は、$\Delta T < 0.5$ deg. と算出した。冷却の温度制御にはデジタル PID 制御を用いて温度安定性の向上を図った。冷却性能を、図 3.2.6 (f)(g)に示す。図 3.2.6 (f)のように室温から-50℃まで冷却する時間は、3 分弱である。図 3.2.6 (g)に示すように PID 制御を用いた ATC 回路により、定常状態での温度変動幅は 0.05 deg.以下であり、十分に安定な光子受信特性が期待出来ることを確認した。

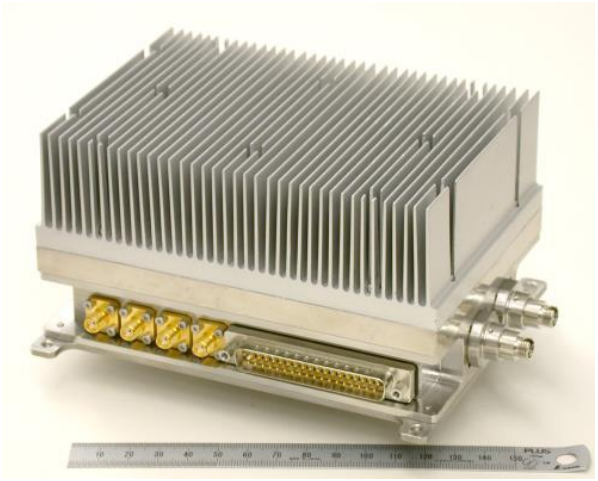


図3.2.6(a)　光子検出モジュール外観

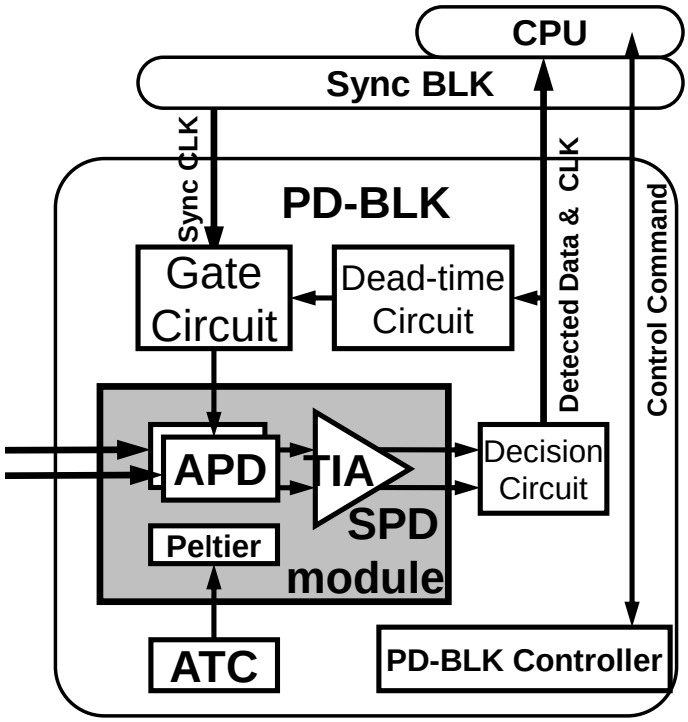


図3.2.6(b)　光子検出回路

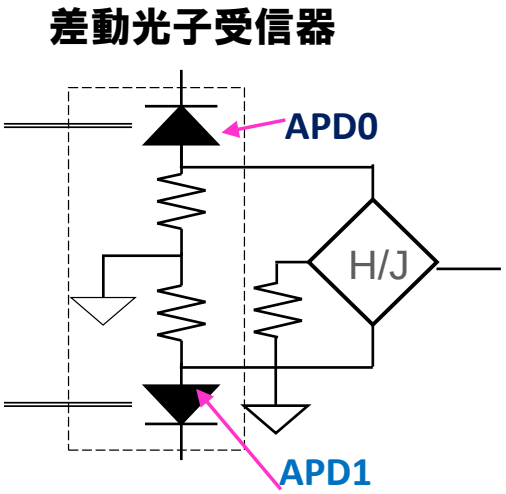


図3.2.6(c) 差動型ノイズキャンセル回路

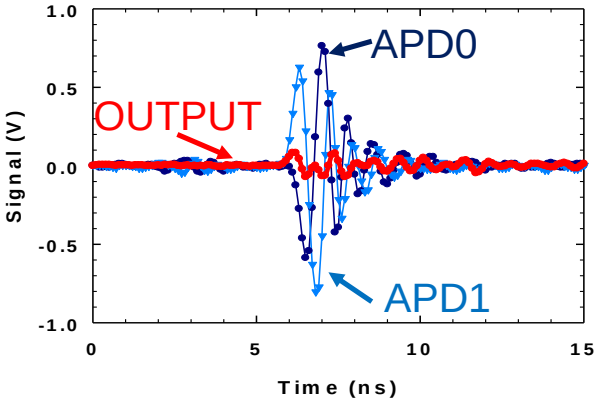


図3.2.6(d)検出波形

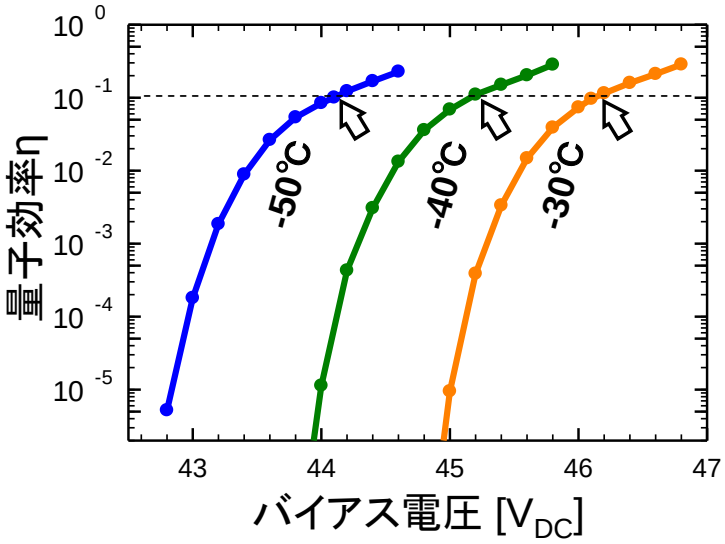


図 3.2.6 (e) 量子効率の温度依存性

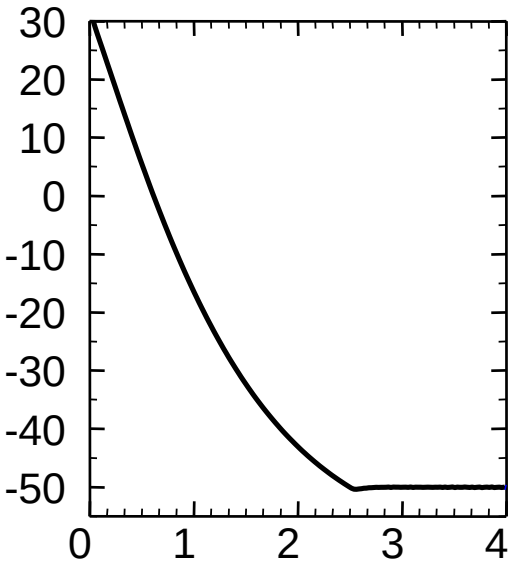


図 3.2.6 (f) 冷却特性

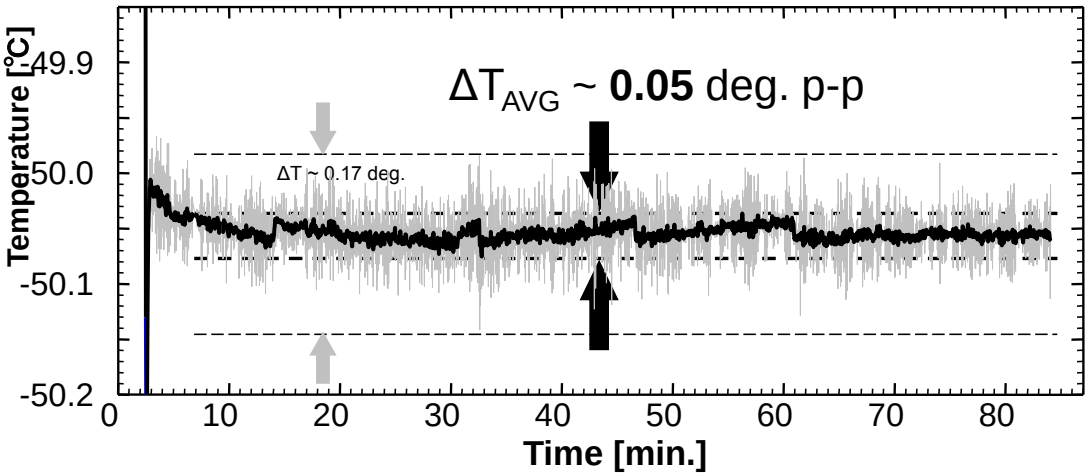


図 3.2.6(g)　冷却温度安定性

上記光子受信器の受信性能評価(62.5 MHz)結果について記載する。図 3.2.6 (h)に、光子検出モジュールの受信位相トレランスと量子効率の安定性を示す。測定は、APD に印加する DC バイアス電圧一定の下で、約 0.1 photon per pulse の光子信号に対してゲートパルス位相スキャンを繰り返し、信号検出数を記録した。7 時間強の連続測定で、量子効率の変動は 5%と、目標の 10 %より十分に安定であることを確認した。10%トレランスのための位相余裕は、500 ps であった。この位相余裕は、同期ブロックから供給される Sync CLK の位相精度より十分に広いため、システム的な安定動作が可能である。図 3.2.6 (i)に、ブランキング回路の動作を示す。光子受信した A 点でオシロスコープのトリガを掛け、B 点までの約 500 ns のブランキングの後、再び光子受信をしている様子が分かる。図下方のヒストグラムは、B 点以降で再び光子受信した頻度の分布を示す。

図 3.2.6 (j)に、ブランキング時間による量子効率とダークカウントの実測例を示す。検出数の多い領域に於けるブランキング時間による見かけの量子効率低下に対して、測定値の補正処理を行った結果、ブランキング時間の差による量子効率及びダークカウントの差は、ほとんど見られなかった。この結果から、約 62 ns のブランキング時間で十分にダークカウントの抑制が可能と見なせる。バイアス電圧方向のシフトは、ブランキング中の平均バイアス電圧の変化による影響である。この測定結果に対し、ファイバ伝送した場合の QBER を概算により検討する。Alice から送信する平均光子数を 0.6 とし、ファイバ長 40 km の伝送を行う場合、Bob 側干渉計の損失を含め、伝送損失は約 15 dB となる。このときの光子検出率は、約 1.9×10-3 となる。その場合の QBER は 3.7 %と十分に低い値であり、高速な鍵生成レートが期待出来る。

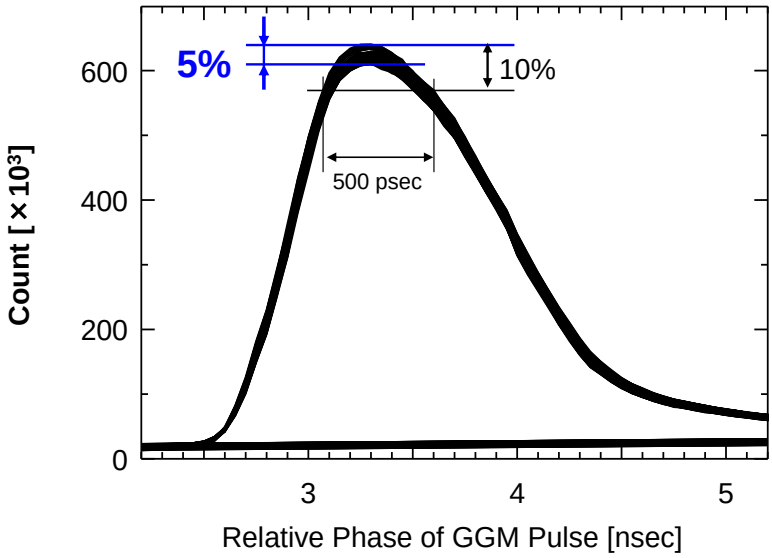


図 3.2.6 (h) 光子受信の位相トレランスと時間安定性

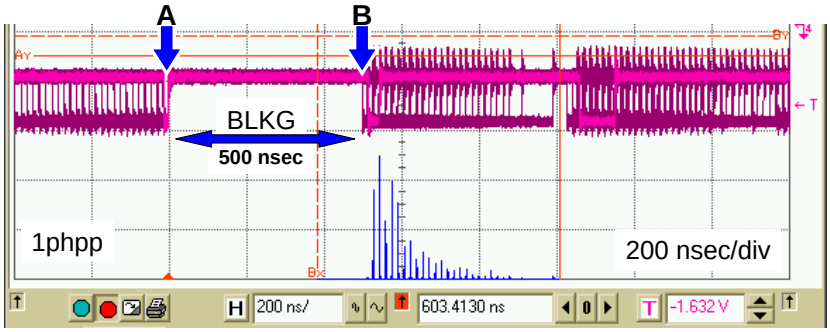


図 3.2.6 (i) ブランキング回路の動作

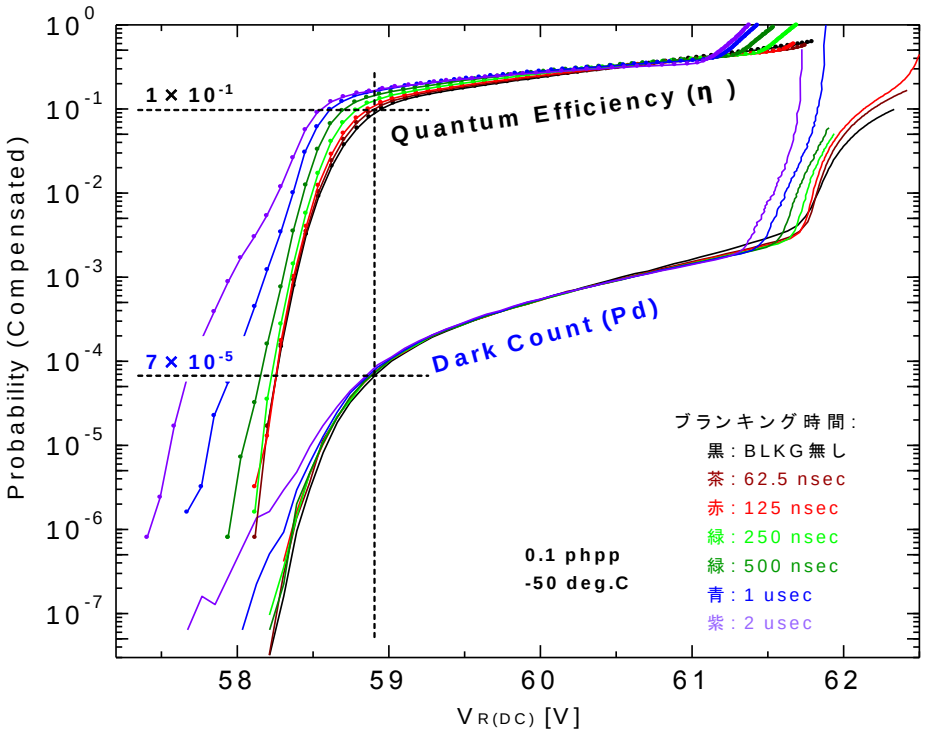


図 3.2.6 (j) 量子効率及びダークカウント確率のブランキング時間依存性

3.2.3　バーストモード伝送技術

実際の光ファイバ伝送路は、つなぎ目のない一本の光ファイバではなく、短いファイバの融着によって構成されている。さらに、局舎内では光コネクタによってファイバを接続している。量子鍵配送技術は単一光子レベルすなわち、微弱な光による伝送技術であるため、このような接続点での Bob から Alice への送出光の反射や、伝送路内での散乱光による影響を無視できない。特に、3.2.1 で説明した“Plug & Play”型は往復型のシステムであるために影響が大きい。これらの影響を回避するためバースト伝送[61][62]を採用した。バーストタイミングの設定は、自動測定用信号により Bob-Alice 間距離を測定することによって自動に行う。図 3.2.7(a)に示すように、連続信号では戻り光によって特性が劣化するものの、バースト伝送の採用により特性が大きく改善されることがわかる。

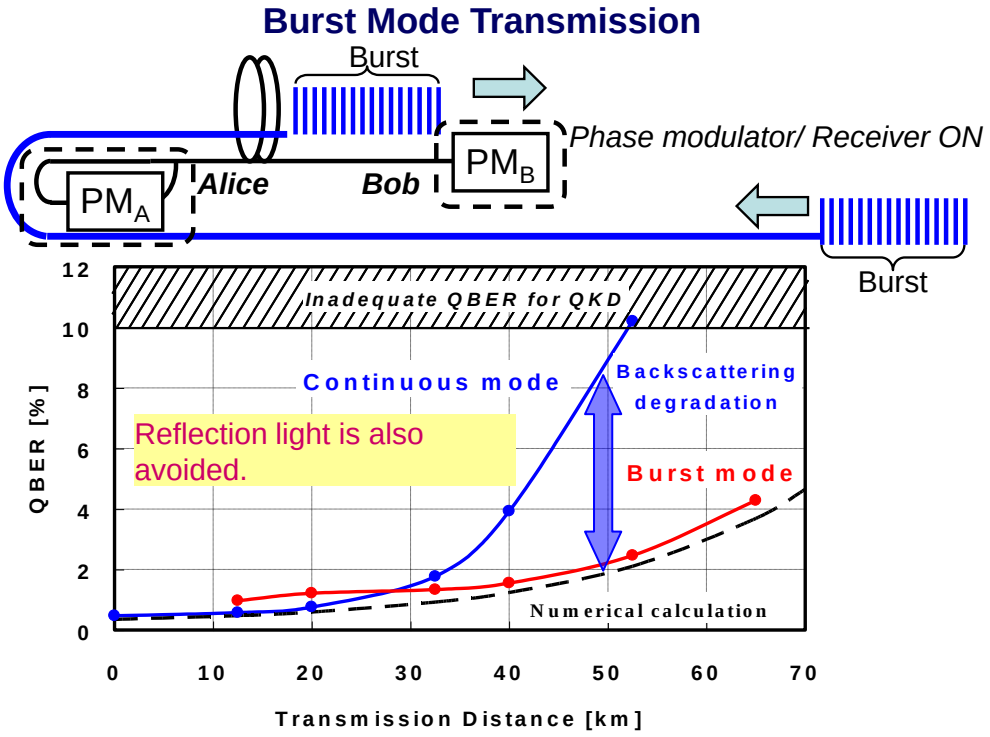


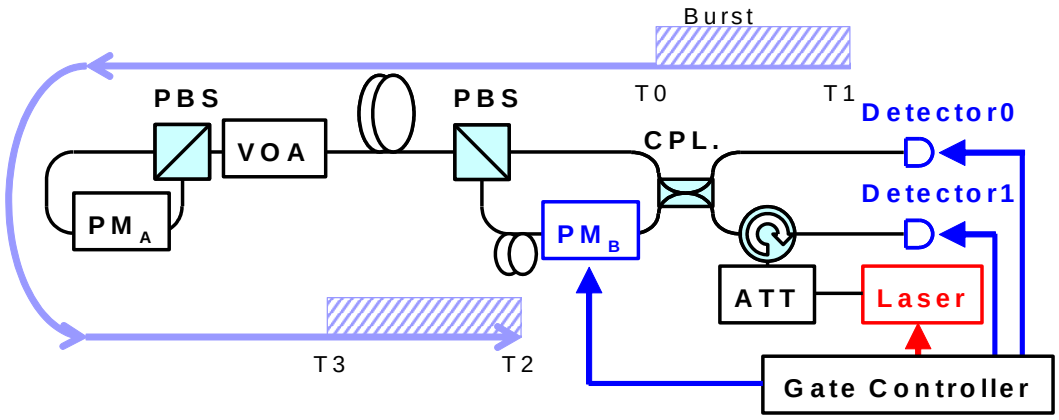
図 3.2.7(a)　バーストモード伝送による QBER 特性改善

このバースト長は、片道遅延(Bob-Alice)時間とほぼ等しくすることで、戻り光雑音の影響排除や、Bob での選択変調が可能となる。そこで以下の手順に従い距離を測定し、図 3.2.7(b)に示すようなバーストタイミング(T0：バースト送出開始、T1:ハースト送出終了、T2:バースト受信開始、T3:バースト受信終了)を設定する。

①同期チャネルを用いて、リファレンスパルスを生成し Bob から Alice へ送る。(T0)
②Alice でリファレンスパルスを受信しそれを Bob へ送り返す。(T1)
③Bob がリファレンスパルスを受信。(T2)

④T0 と T2 により距離を計算し、T1 を計算する。
⑤同様に T3 を計算する。(T3 = T2 + (T1-T0))

図 3.2.7(c)に Alice-Bob 間のファイバ長を 10、20、30 km としたときの、ファイバ距離とリファレンスパルスカウント数を示す。これらより、ばらつきなく高精度に測定ができていることがわかる。



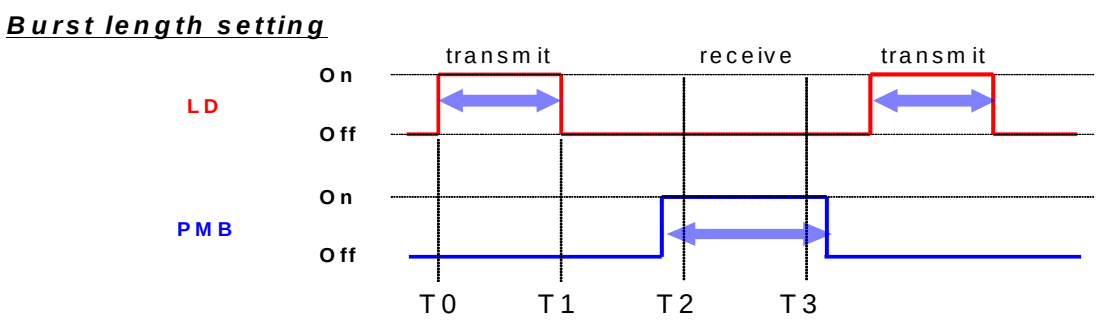


図 3.2.7(b)　バースト設定手順

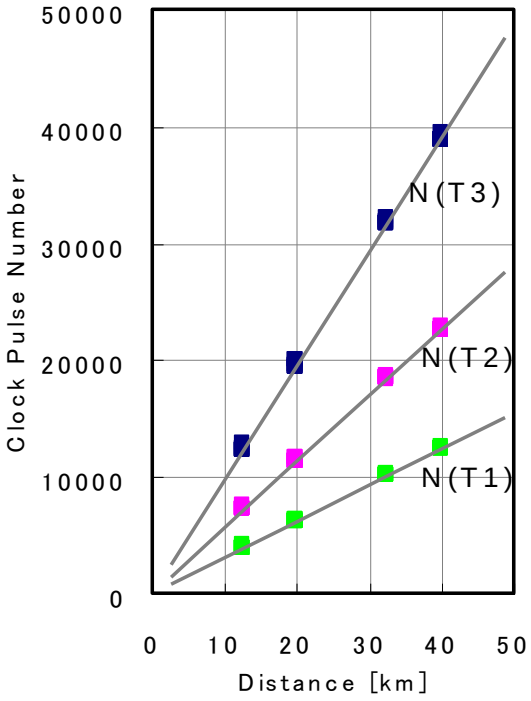


図 3.2.7(c)　距離とリファレンスパルスカウント数

3.3　量子鍵配送システム

これまで説明した技術を組み込んだ量子暗号システムを Alice(送信)、Bob(受信)それぞれ 19 inch ラックに収容できる(サイズ 480 mm x 180 mm x 375 mm)形態[63]で実現した。装置外観と機能ブロックを図 3.3.1 に示す。Alice は、量子光学部、同期部、データ通信部と CPU、Bob は、量子光学部、同期部、データ通信部、光子検出部と CPU によって構成されている。CPU によって、暗号化通信(量子鍵を用いた One Time Pad)、システム制御(装置の初期化と状態監視制御)を実現している。装置の内部クロックは、62.5 MHz である。本装置を一芯の光ファイバを介して対向接続することで、暗号鍵生成・共有と暗号鍵を用いた暗号化通信が実現できる。暗号化通信の一例として、本装置に IP 電話を接続し Voice over IP (VoIP)データの One Time Pad 暗号化[10]通信を確認した。

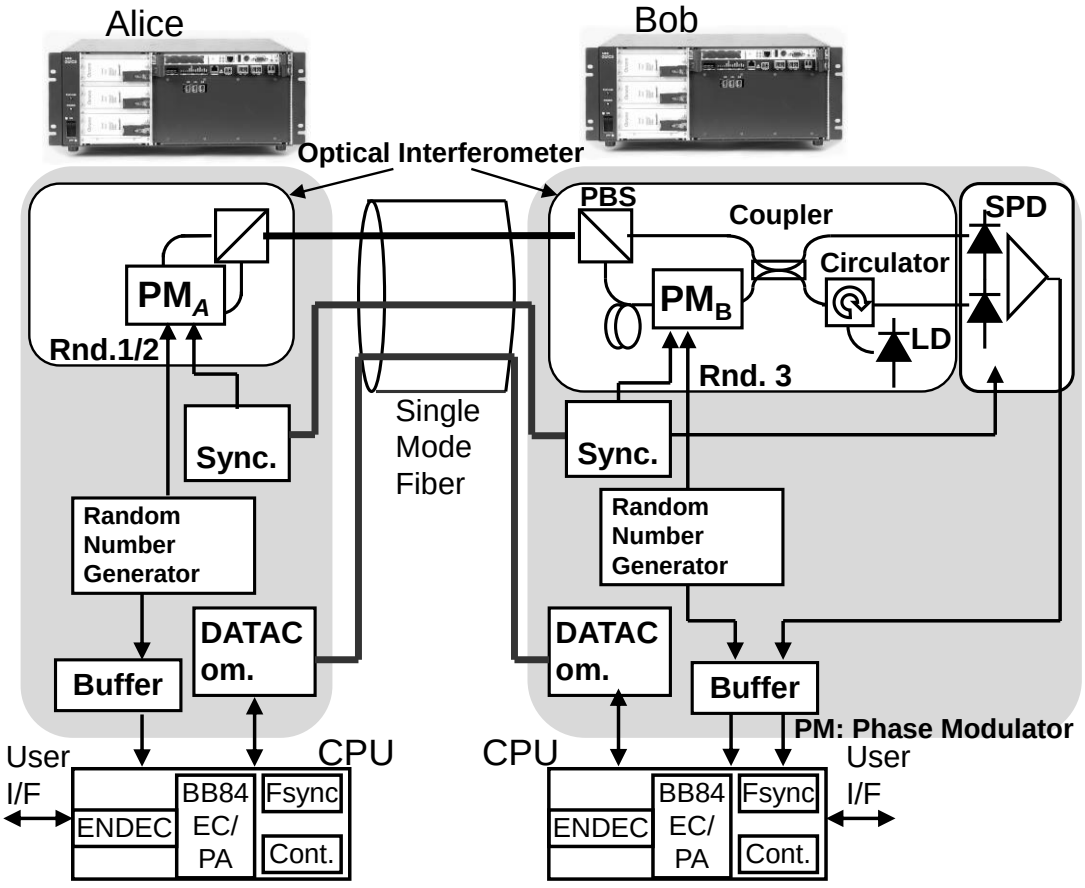


図 3.3.1　QKD 装置機能ブロックと外観

3.4　実使用環境下での長時間連続鍵生成実験

実使用環境下での連続動作を実証するために、3.3 で説明した装置を一般の室内環境下に設置し、アクセスファイバ 16.3 km (区間の大部分は架空)、伝送路損失 8 dB を介して接続し、24 時間連続で 14 日間以上にわたる長時間連続最終鍵生成実験を行った。図 3.4.1 に実験イメージ、結果を図 3.4.2 に示す。実験の結果、無調整で 14 日間以上連続最終鍵生成を

達成した[36]。図 3.4.2 に示すように平均の量子誤り率は 7.5%、平均の最終鍵生成レートは 13.0 kbps であった。但し、最終鍵は秘匿増強に必要となる計算処理量の実現可能性確認のため、計算量が最大となる暗号鍵破棄率 0 %とした。

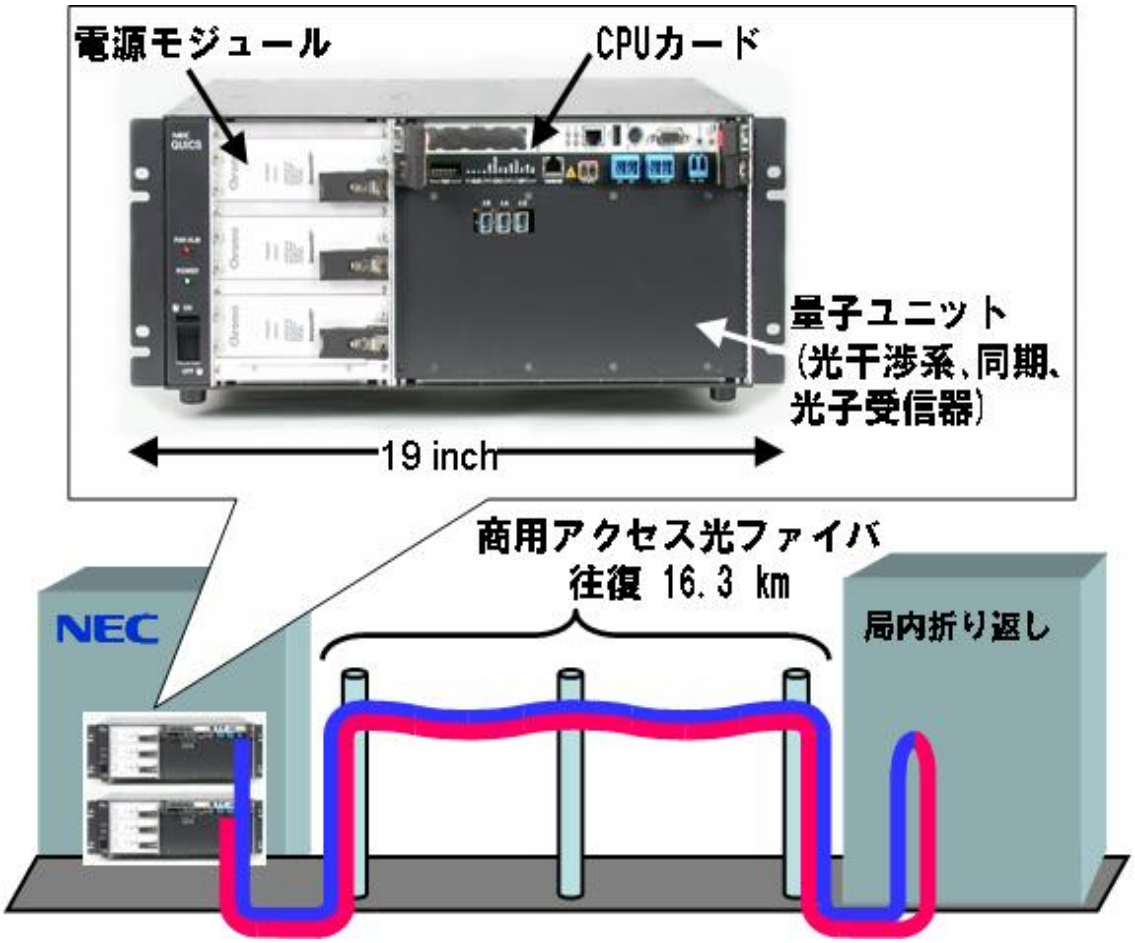


図 3.4.1　フィールドファイバ実験のイメージ

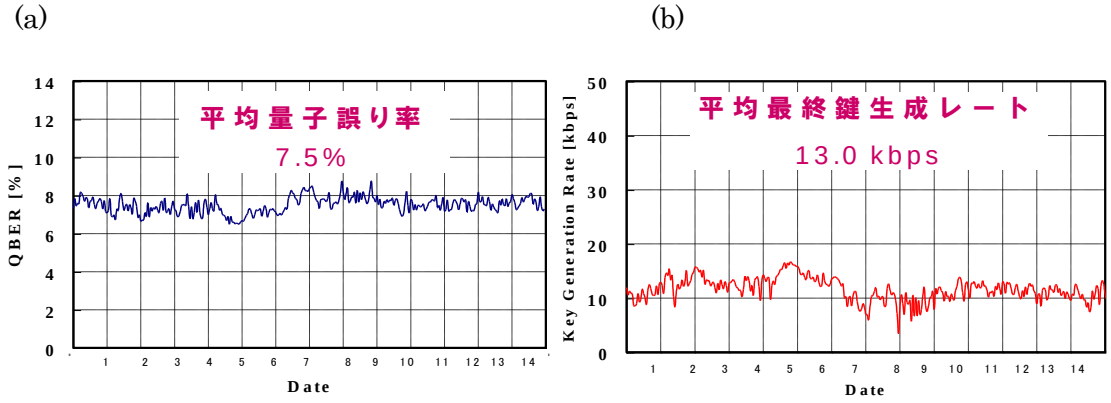


図 3.4.2　二週間連続動作試験結果　(a)誤り率、(b)鍵生成レート

3.5　1:2 量子鍵生成・共有実験

3.3 で説明した装置による実使用環境下での連続動作実証に成功したことを 3.4 で述べた。本節では、本量子暗号システム(Alice x 2 台、Bob x 1 台)と、光スイッチング技術の活用による、1 対 2 の暗号鍵共有実験[64][65]について述べる。光スイッチは、損失の少なくかつ、精密な設定制御が不要で高安定な機械式スイッチを採用した。光スイッチにより、量子 ch.、同期信号及び鍵生成・共有を行う古典 ch.も同時に切り替え、図 3.5.1 に記載するタイミングチャートのように時分割により、いずれか 1 台の Alice と Bob 間で鍵生成を行う(同時に複数の Alice と鍵生成を行うことはない)。光スイッチの制御は、Operation Support System をはじめとする外部からの制御または、Bob からの制御のどちらかを選択可能である。

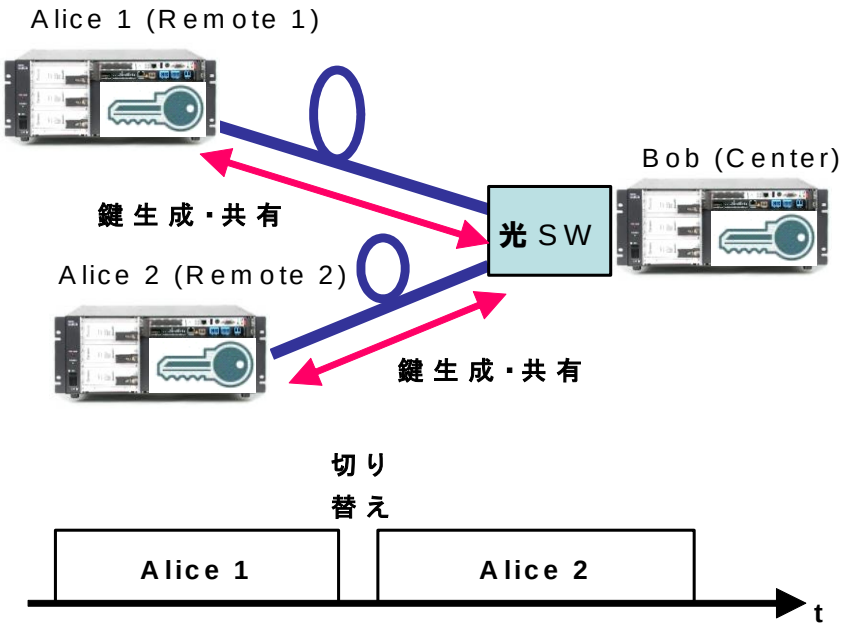


図 3.5.1　1:2 鍵生成・共有システム構成図

光スイッチ切り替え後の、位相およびバースト設定手順は、図 3.5.2 に示すように、3.1.1、3.2.3 で説明したよう高精度な設定(a)通常初期設定と、(b)高速初期設定の二通り設けた。これは(a) 通常初期設定に 5 分以上の時間を要することによる。

(a)通常初期設定：3.1.1、3.2.3 で説明した高精度位相・バースト設定

(b)高速初期設定：(a)の値をメモリに蓄え、この値を用いての位相・バースト設定

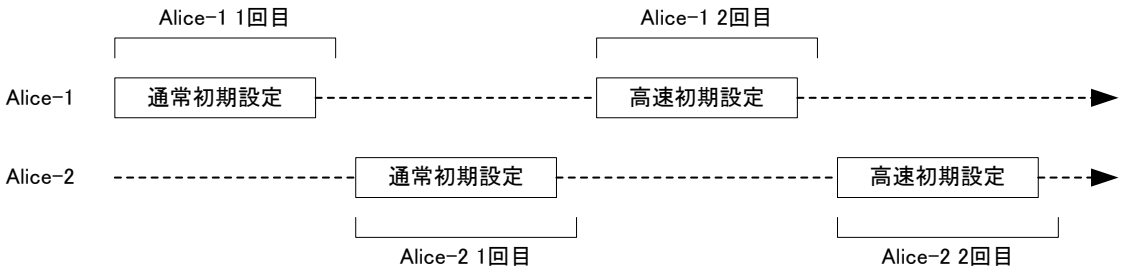


図 3.5.2　切り替え手順

経路切り替えによる 1:2 量子鍵生成・共有実験について述べる。図 3.5.3 に示すような実験系により、1:2 量子鍵生成・共有実験を行った。ここで、

・光スイッチの切り替えは、1 時間毎、
・切り替え時には暗号鍵生成通信も同時に切断される
・状態制御信号は常に開通

とした。図 3.5.4 に 3 日間に渡っての 1:2 鍵生成・共有の実験結果を示す。初期設定時の問題による大きな変動と、APD バイアスの変化などに伴うレートの変動はあるものの 3 日間にわたり問題なく動作を確認することができた。

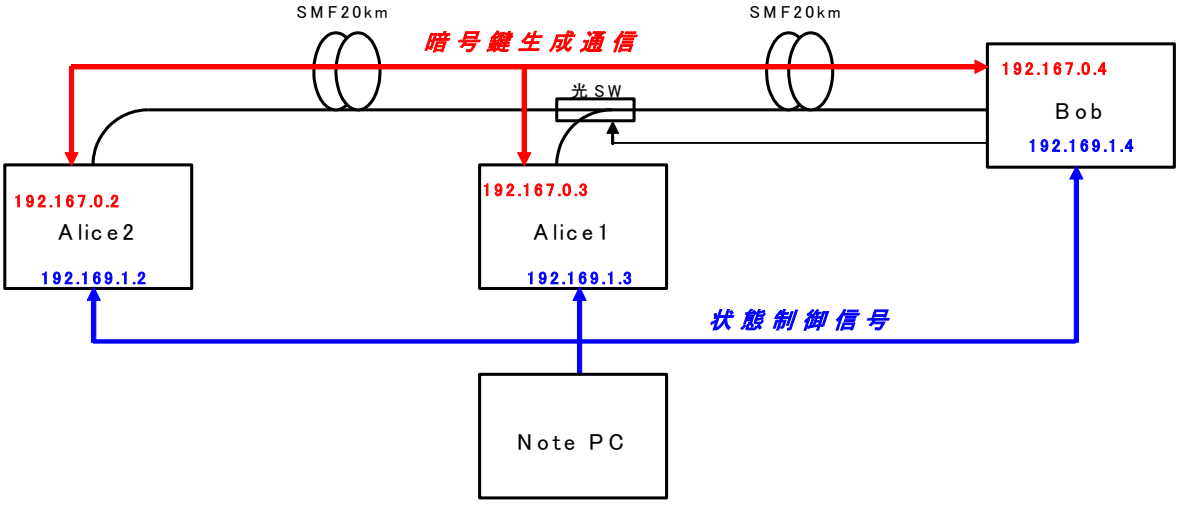


図 3.5.3　1:2 量子鍵生成・共有実験系

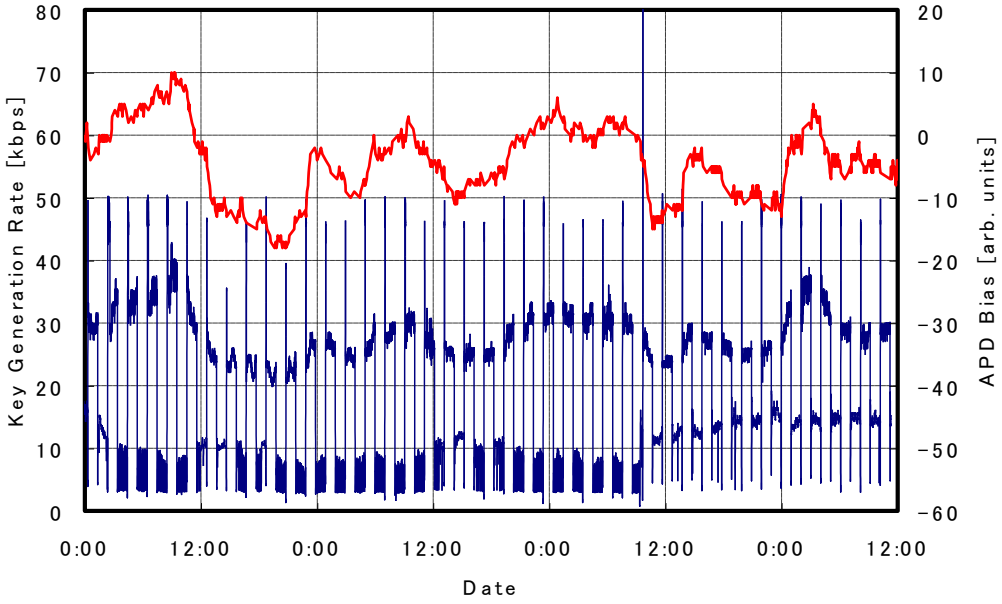


図 3.5.4　実験結果

3.6 異機種量子暗号システムの相互接続実験

量子鍵配送技術をセキュリティシステム技術として活用していくためには、長距離化や高速化といった性能向上だけではなく、相互接続性、標準化、安全性、利用技術をはじめとするセキュリティシステム技術の研究開発が重要と考えられる。そこで異なる量子暗号システム間の相互接続性について方式検討、インタフェース及び接続機能の開発を行い、3.3 で説明した装置と三菱電機製装置[34]のシステム間相互接続実験を行った[66]。

量子暗号システムのプロトコルスタックの一例を図 3.6.1 に示す。異機種システム間の接続を行う際の接続インタフェースとしては、①単一光子伝送後の生鍵、②量子鍵生成処理後の量子鍵、③量子鍵を用いたアプリケーション、の三通りが考えられる。今回、実現の難易度と利便性を考え③を選択した。量子鍵はリンク毎に固有となるが、図 3.6.2 のように量子鍵とは別の暗号化通信用の鍵を準備し、リンク毎の量子鍵によって One-time Pad 暗号化して伝送することで、同一の鍵のマルチキャストすなわち多者間の絶対安全な鍵共有が実現できる。

上述した方式によって、異なるシステムを接続する場合の技術課題は、①相互接続機能(接続インタフェースの実現、鍵ファイル形式の統一)、②方式／特性の違うシステム間の整合性確保(光子伝送系/誤り訂正方式/秘匿性増強方式の違い)、③暗号鍵の同期(暗号化・復号化に際しての暗号鍵の同期、誤り率/鍵転送速度の違いを補償)、が挙げられる。上記課題①～③に取り組みインタフェース及び接続機能を開発し、接続実験を行った。図 3.6.3 に実験系を示す。この系では、物理乱数回路で発生した乱数による通信用鍵 K0 をセンター局からリモート局へ量子暗号鍵 QK1/QK2 によって One-time pad 暗号化して転送す

る。リモート局 1、2 では、通信用鍵 K0 によって One-time pad 暗号化通信(今回はメールを暗号化)を行う。リモート局の Alice/David は消費した分量の鍵を要求し、Bob/Carol を経由して鍵サーバから鍵を取得する。センター局とリモート局 1、2 の距離はそれぞれ 20km とした。リモート局 1 と 2 で暗号鍵 300 kbit を共有し暗号鍵がエラーフリー(鍵の BER < 3.3 x 10-6)であることを確認し、メールの転送を行うことを確認した。

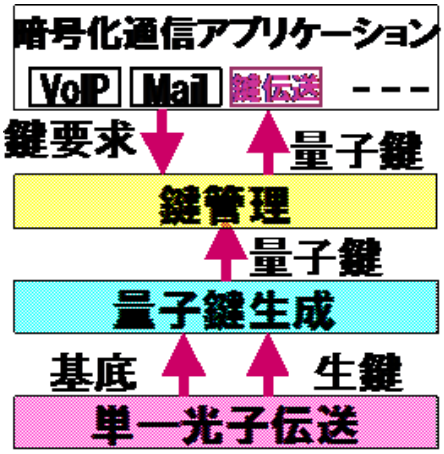


図 3.6.1 プロトコルスタック

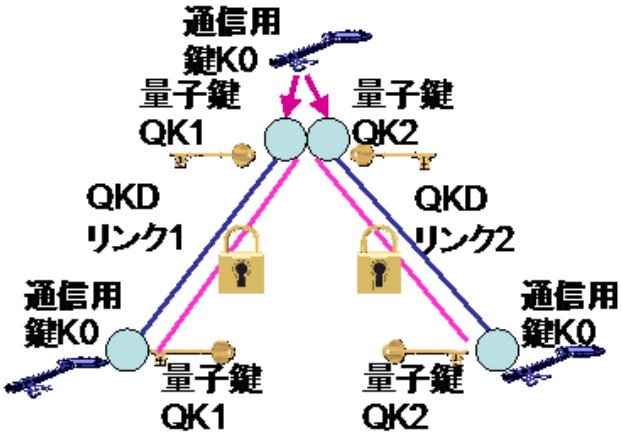


図 3.6.2 異機種接続方式

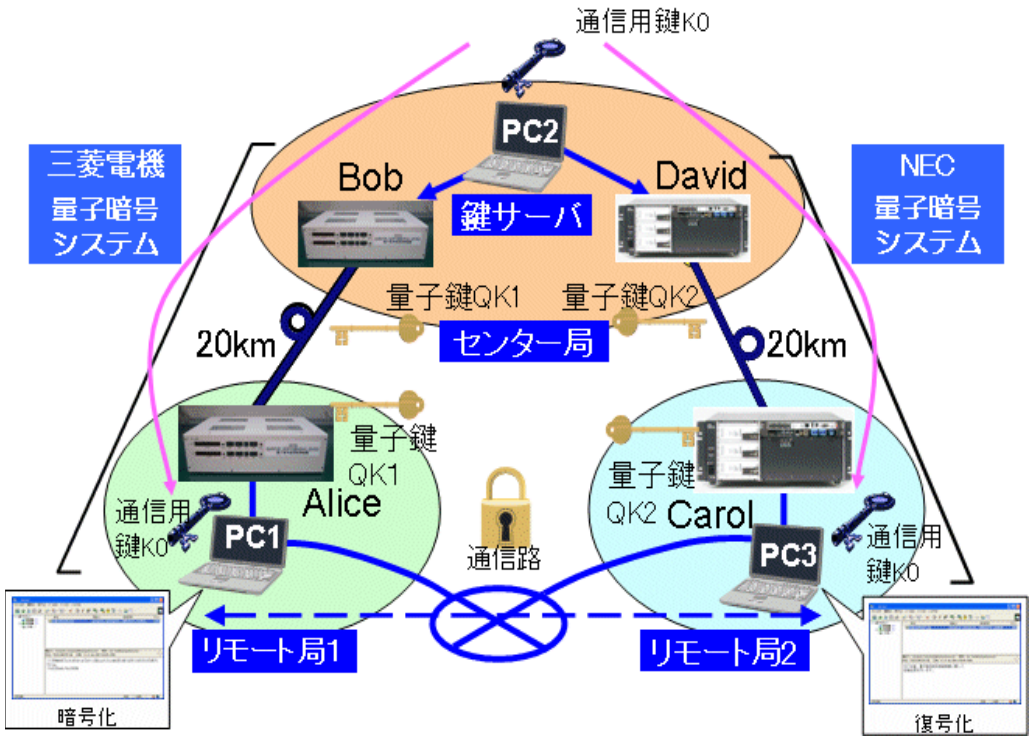


図 3.6.3　異機種量子暗号システム相互接続実験系

４．高速化技術

3 章では、往復(Plug & Play)型 QKD システム(動作周波数 62.5 MHz)を用いたシステムにより、アクセス系フィールドファイバで 14 日間の連続動作達成について述べた。しかしながら、伝送損失 8 dB での鍵生成レートは 13. 0 kbps と One Time Pad 暗号化の鍵として用いるにはテキスト主体の E-mail や Voice over IP などのアプリケーションに限定されてしまうという問題があった。鍵生成速度を向上させるためには、動作周波数を上げること、検出効率を上げること、鍵生成効率を上げることが考えられる。動作周波数と検出効率は検出器によって制限されている。InGaAs-APD による光子検出器を用いたシステムでは光子検出器のアフターパルスを抑圧するためのデッドタイムで制限され動作速度は GHz クラス[42][67]、検出効率も 10%程度となっており特性改善のためには、ブレークスルーが必要である。光ファイバ通信波長帯の光子検出器としては、InGaAs-APD 以外に超伝導光子検出器（SSPD）[40][68]も候補として挙げられている。SSPD にはアフターパルスがほとんどなく、高速性に優れ動作周波数 10 GHz による DPS-QKD[40]も実験されている。しかしながら、超伝導状態には数Kまで冷却する必要があり、冷却機構を含めるとサイズ、メンテナンスおよび信頼性の問題により実システムとして用いることは困難である。

鍵生成効率改善による鍵生成速度を向上は具体的には、光子伝送・検出における誤り率を低減することである。誤りが減ることよって誤り訂正処理において失われるビット数を削減できるだけでなく、秘匿性増強のために捨てるビットを少なくできるからである。誤り率低減には、干渉計の明瞭度向上、スレー光の低減、検出雑音の低減が挙げられる。

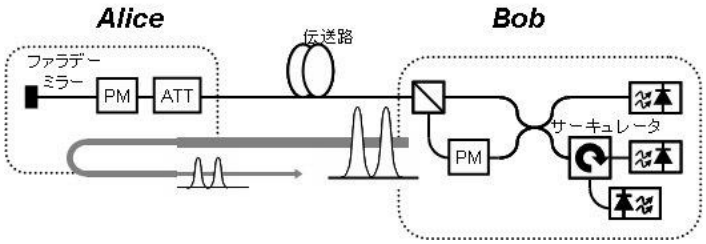
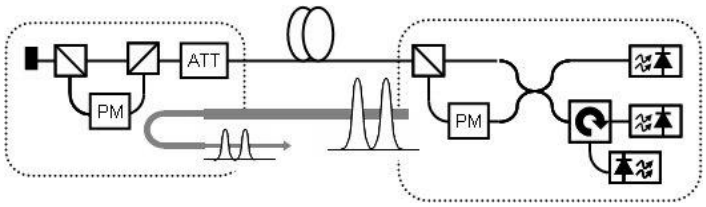
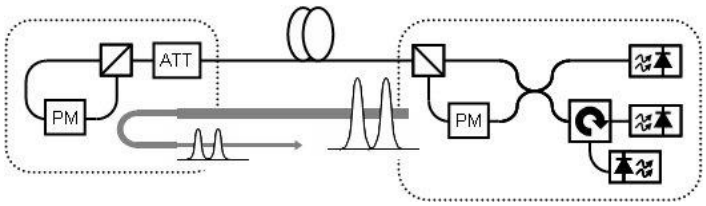
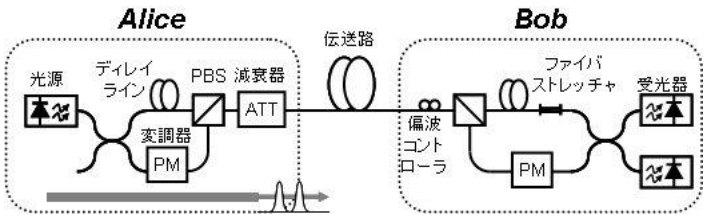
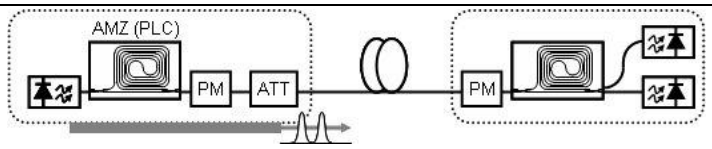
我々は干渉計の明瞭度を高くするために PLC (Planar Lightwave Circuit)単一方向型システム[69][70]を、さらに異なる複数の波長の信号を多重化する WDM (Wavelength Division Multiplexing)[71]を採用することで鍵生成速度 Mbps クラスの高速化[72]を実現した。GHz で動作する光子検出器の低雑音化のためには、新たに信号処理技術によるセルフトレーニング型検出回路[73]を考案した。また、動作速度向上、WDM 化により光子伝送・検出部が高速化した際、鍵生成処理の高速化[74]も必要である。以下でそれぞれについて説明し、これら提案技術を用いて構築した高速 QKD システムとフィールド実験について述べる。実験の結果、高速かつ長期間安定動作[47][75]を達成した。

4.1　PLC による単一方向・偏波無依存型波長多重技術

4.1.1　一方向型量子暗号技術

表 4.1.1 に代表的な光学系をまとめる。往復型方式(a)~(c)による量子暗号技術は、3.2.3 に記載したようにその光学系構成に起因する速度の制限があった。それに対して、単一方向型(d)(e)は、干渉計の送受信者で独立に非対称干渉計を持つ必要があり両者の遅延量の同期制御[76]が必須となるものの、QKD の長距離・高速化を達成できる。特に、PLC を用いた干渉計は、光ファイバによる干渉計に対して、精度良く同一の光回路を量産可能で、振動の影響が少なく、温調のみにより安定な動作を実現可能という特徴を有している[69]。

表 4.1.1　BB84 量子暗号鍵配送技術の光学系比較

	Type	構成	特徴	Ref.
往復型	(a)		・偏波無依存 ・偏波無依存光変調器必要(Alice)	[32]
	(b)		・偏波無依存 ・偏波依存性のある位相変調器可(Alice)	[34]
	(c)		・偏波無依存 ・温度無依存干渉計 ・偏波依存性のある位相変調器可(Alice)	[37]
単一方向型	(d)		・偏波コントローラ、ファイバストレッチャによる変動補償	[76]
	(e)		・高精度・偏波無依存PLC 干渉計	[69]

一方向型方式において BB84 を実装する際の 2 つの有力な方法として、4 値位相(XY 基底)コーディング(以下、方式 A)と、2 値位相+時間(XZ or YZ)コーディング（方式 B)が報告されている。一般に光変調器は偏波依存性を有するために、方式 A では偏波制御器を組み込み光ファイバ伝送路中での偏波変動を補償するか、偏波分離しそれぞれの偏波ごとに変調する偏波ダイバーシティを用いることになる。偏波制御器はメカニカルなものしかなく信頼性の問題から実システムで用いられることはない。偏波ダイバーシティは構成が複雑で、サイズが大きくなり、過剰損失が問題となる。一方、方式 B は受信側に変調器が不要となるため、その損失分だけ伝送速度の高速化が図れるというメリットがある。方式 A でも受信信号をビームスプリッタによりそれぞれ位相差の異なる干渉計へ入力することにより変調器を不要とすることも可能だが、過剰損失があることや制御対象である干渉計が増えるという問題がある。今回提案した構成は、上記 AB 両方式に対応できる汎用性の高い量子暗号送信器であり 2x2 干渉計と 2 電極 MZ 変調器を使用することで実現することができる[70]。

4.1.2　量子暗号送信器構成

図 4.1.1 に 2x2 干渉計と 2 電極 MZ 変調器を使用した量子暗号送信器構成を示す。LD によって生成した光パルスを、2x2 干渉計を通すことで 2 連パルスへと時間分離する。2 電極 MZ 変調器を使用して、この 2 連パルスの相対位相及び相対強度を変調する。2 電極 MZ 変調器の入出力は MZ 各経路における位相シフトϕ1 及びϕ2 を用いて次式で表すことができる。

$$E_{out} = E_{in} \cos\left((\phi_1 - \phi_2)/2\right) \cdot \exp\left(i(\phi_1 + \phi_2)/2\right)$$

方式 A では Fig.2 左上に示す様に、同強度で 90° ずつ位相の異なる 4 状態が必要となる。MZ 変調器の片経路を 0° と 180° の変調位相で、他方を 90° と 270° の変調位相で駆動することで、式(4-1)の強度項である cos((ϕ1 - ϕ2)/2)は常に一定となり、位相項である exp(i(ϕ1+ϕ2)/2)に従って a～d の 4 状態を準備できる。前段の干渉計で時間分離された 2 連パルスに対して、a→a の駆動条件により位相差 0°(X0)、a→c で位相差 180°(X1)、a→b で位相差 90° (Y0)、a→d で位相差 270° (Y1)の 4 状態を生成できる。方式 B では、Y 基底に対応する強度 1/2、位相差 90° の 2 状態と、Z 基底に対応する強度 0、1 の 2 状態が必要となる(Fig.2 左下)。MZ 変調器片経路を 90°、他方を 0° と 180° の変調位相で駆動することで、強度 1/2、位相差 90° の e、f、片経路を 0°、他方を 0° と 180° で駆動することで、強度 0、1 の g、h を準備できる。2 連パルスに対して、e→f の変調で位相差 90°(Y0)、f→e で位相差 270° (Y1)、g→h で前パルス (Z0)、h→g で後パルスのみ (Z1)の 4 状態を生成できる。

この量子暗号送信器の特性を調べるために実証実験を行った。LD により、1.6 ns 間隔、100 ps 幅の光パルスを生成し、遅延差 800 ps の PLC MZ 干渉計を使用して 800 ps 間隔の

2 連パルスへと時間分離した。この 2 連パルスに対して Fig.2 の変調を行い、受信側の 2x2 干渉計及び 2x4 干渉計を通して干渉特性を測定した。X と Y 基底の 2 連パルスの位相差が 90° 異なっていること、及び、Z 基底で消光した光パルスが十分消光されていることを確認するため、送信側 PLC の温度を変化させて出力 2 連パルス間の位相を変えたときの、受信側 PLC の各ポートに出力される光パルス強度の変化を測定した。測定結果を図 4.1.3 に示す。方式 A の場合は、ポート 0、1 出力共に 4 つの送信状態に対応する光パルス強度が、位相 90° ずつずれた正弦波曲線を描くことが確認できた。各正弦波のピーク高さの違いは、変調器駆動信号の設定値からのずれにより強度項が等しくならなかったことによる。方式 B の信号を受信側 PLC の Y0、Y1 ポートで観測すると、PLC 温度に従って Y 基底の 2 パルスの光強度が変化する一方、Z 基底の 2 パルスの光強度は PLC 温度によらず一定となることを確認できた。表 4.1.2 に、各光パルスの消光比から計算される誤り率をまとめる。誤りは変調器駆動信号のずれや干渉計の精度に起因しているが、平均して 0.7%以下の良好な誤り率を得た。

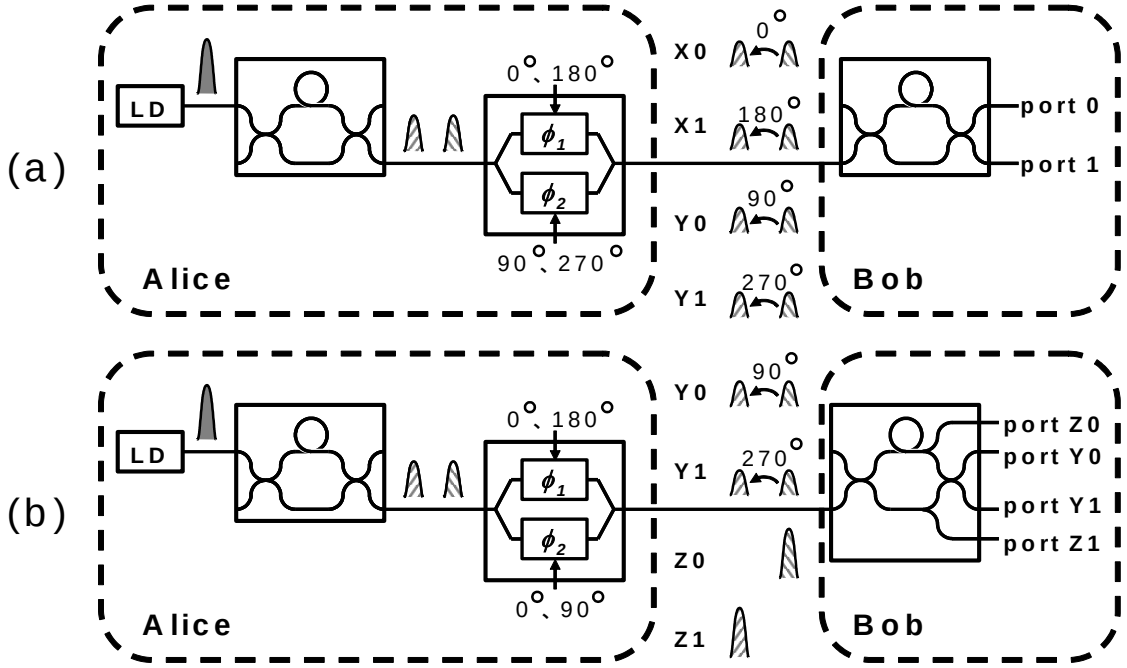


図 4.1.1　一方向型 QKD システムの光学構成

(a) 位相コーディング **(b)** 位相-時間コーディング

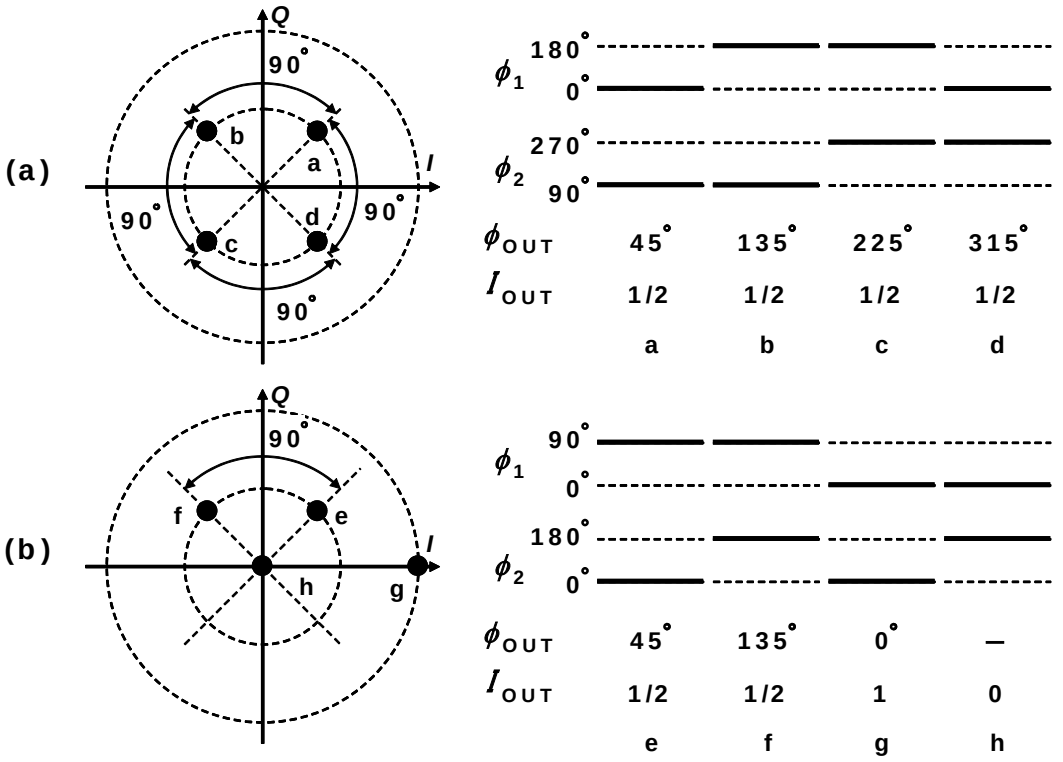


図 **4.1.2**　変調方法　**(a)** 位相コーディング **(b)** 位相-時間コーディング

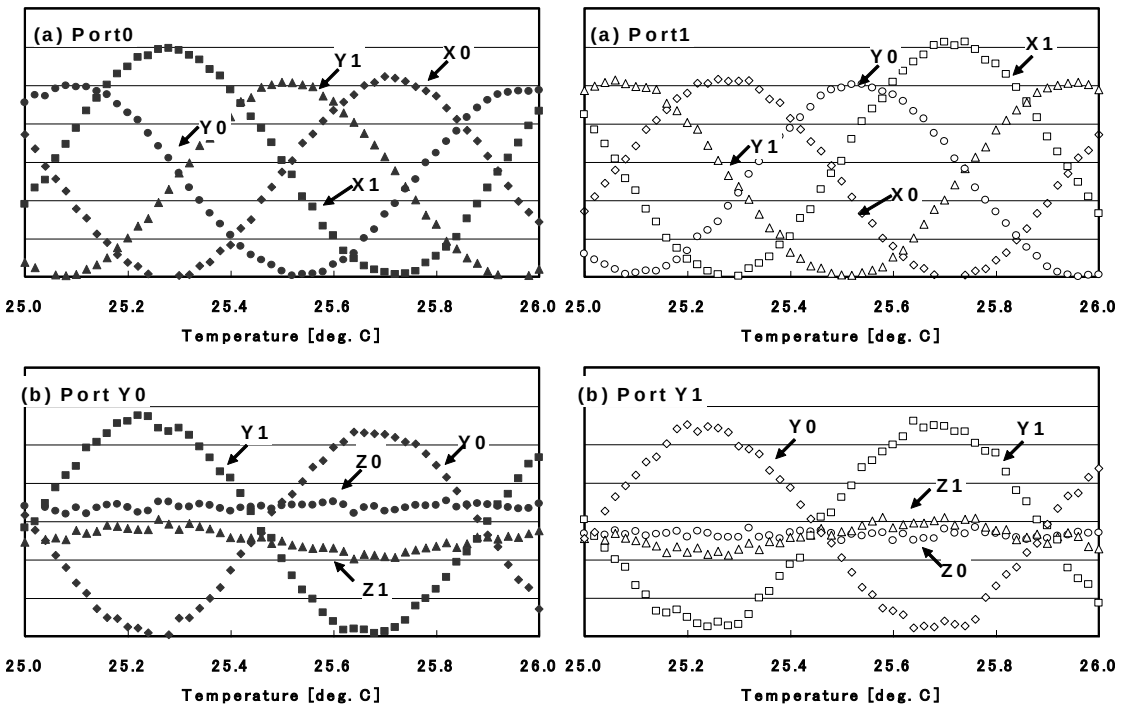


図 **4.1.3**　干渉度測定結果　**(a)** 位相コーディング **(b)** 位相-時間コーディング

表 4.1.2　パルス強度から見積もったエラーレート

		Type A				Type B			
Transmission	Bits	X0	X1	Y0	Y1	Y0	Y1	Z0	Z1
Error Rate [%]		0.3%	0.5%	1.3%	0.5%	1.1%	0.3%	<0.1%	1.4%

4.1.3　干渉計を複数波長で共用する波長多重 QKD 技術

QKD システムでは、光学干渉計を送受 信器両方において使用する。WDM を用いて複数波長を多重して QKD を行う際にはこの光学干渉計を複数波長で共用することにより、システムのコスト・サイズ削減が期待できる。しかし、光学干渉計を複数波長で共有する際には、送受信器内の 2 つの干渉計の遅延量の差が問題となる。主に屈折率の波長依存性の製造ばらつきによって、複数波長の干渉点を同時に制御することは困難になる。この問題を解決するため、各波長λn に追加の位相変 調Δθ(λn)を施す方法を提案する(図 4.1.4)[71]。Alice 側の光学 干渉計で光パルスを時間分離した後、2 連光パルス間 に、2 つの光学干渉計の位相差に相当する位相変調を補償用位相変調として施す。図 4.1.4 において、λ1 の信号 にだけ補償用位相変調を施していないのは、1 波長の 干渉動作だけは光学干渉計の遅延量を温度により制御 できるためである。本送受信器内の 2 つの干渉計の遅延量差の波長依存性を位相変調により補償する。本方式の有効性を評価した結果を図 4.1.5 に示す。図中の■は補償用位相変調信号の振幅を 0 にしたままで測定した消光比であり、◆は補償用位相変調信号の振幅を調整して消光比が最大となる状態で測定した結果である。図より明らかなように、補償用位相変調を最適化しない状態では消光比は大きく変化し、1547.72 nm の波長に至ってはピークとボトムが逆転する状況まで発生している。反面、補償用位相変調の振幅を最適化した状態では、いずれの波長においても消光比 20 dB 以上を確保できている。得られた干渉消光比は、単一波長での実験での値と同等であり、使用している Mach-Zehnder 干渉計の性能及び変調精度によって制限されているものと推測する。また、この消光比は量子誤り率（QBER）1 %以下に相当し、最終鍵生成速度を計算する際においた仮定を満たす。実験により各波長信号の誤り率 1%以下に対応する良好な干渉特性を確認し、提案方式が QKD の大容 量化に有効な方法であることを実証した。

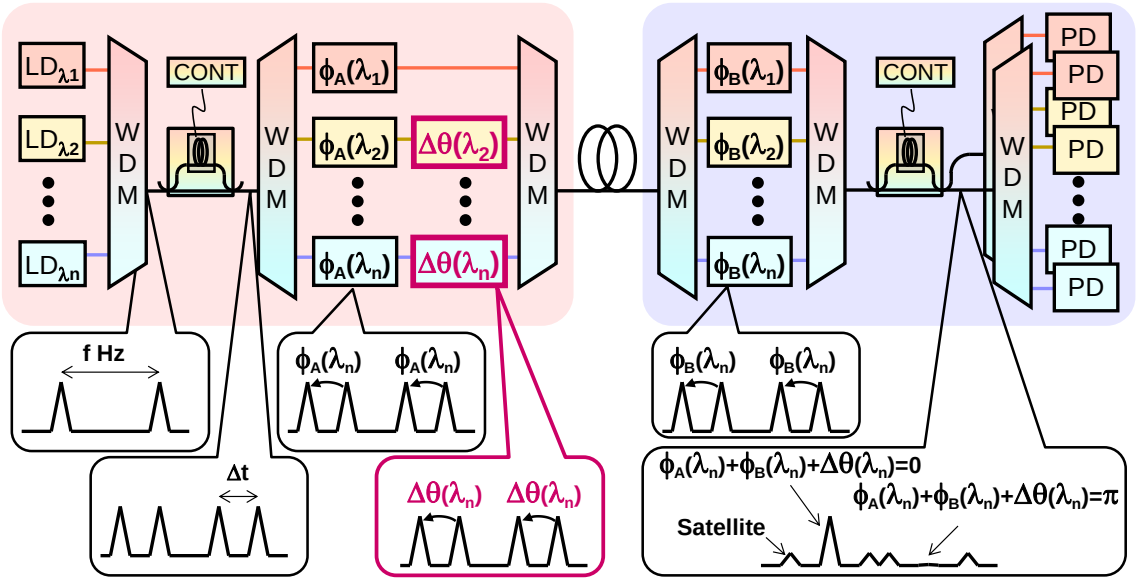


図 4.1.4　波長多重型 QKD システム

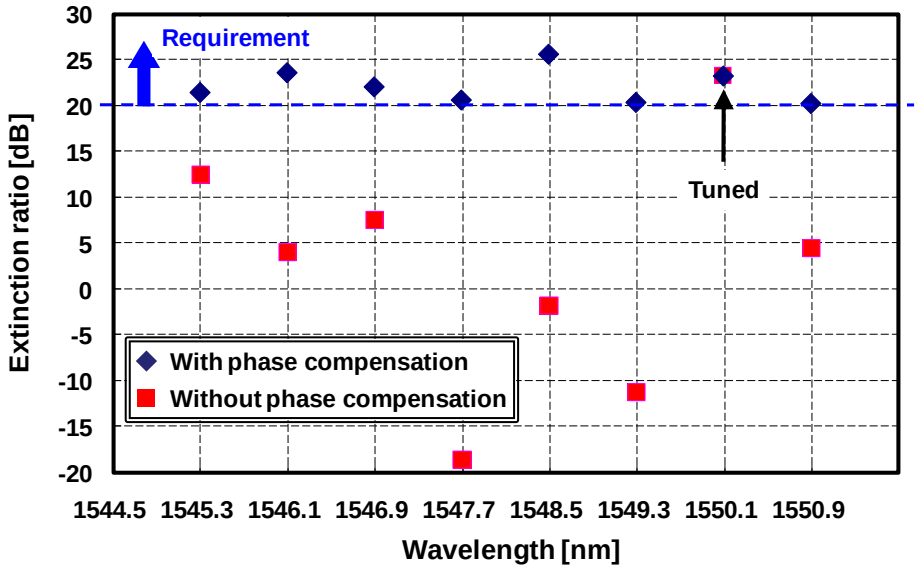


図 4.1.5　各波長における干渉消光比測定結果

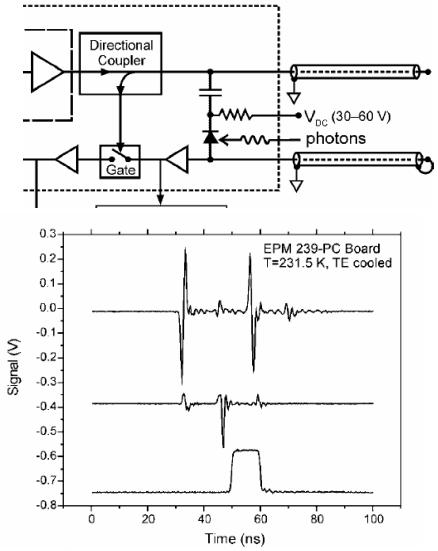
4.2　高速光子検出技術

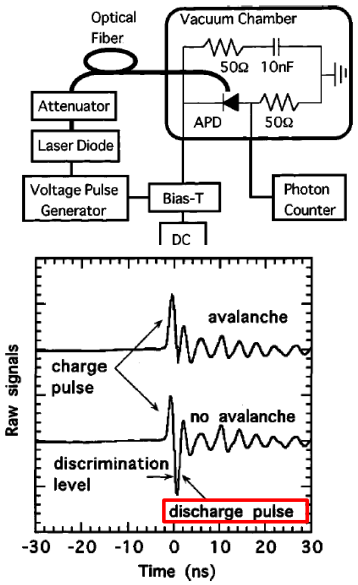
4.2.1　セルフトレーニング型識別回路

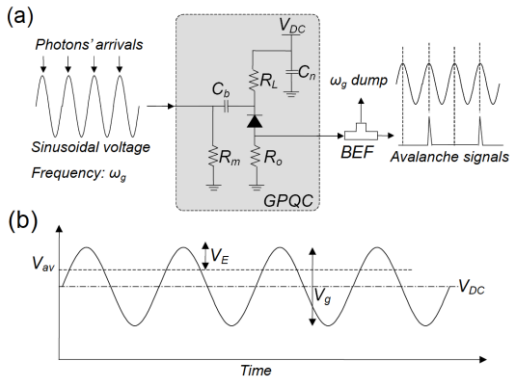
単一光子検出には、InGaAs-APD を冷却し、ゲートモード動作を用いる)[25][26]。ゲートモードを用いた単一光子検出器では、信号識別回路での容量性ノイズを補償した識別回路が必要となる。この容量性ノイズを抑制するため、各種容量性ノイズキャンセル方式が報告されている(表 4.2.1)[27,29,67,77]。しかしながら、それらを用いた高速化には、表 4.2.2 の問題がある。従来は、帯域制限による波形の鈍りと、位相トレランスの広さから、光子検出回路内に若干の個体差があっても大きな問題にならなかった。しかし、動作速度が高速化するに連れて、上記の複数の問題の相乗効果により、容量性ノイズキャンセル誤差が顕著になり、光子検出性能の劣化に繋がることが懸念される。一例として、既存の光子検出器を用いて、回路帯域と容量性ノイズキャンセル誤差の関係を簡易的に評価した結果を図 4.2.1 に示す。検出回路の帯域が拡大するにつれ、容量性ノイズキャンセルの誤差が拡大することがわかる。この問題を解決するために、図 4.2.2(a)に示す A/D コンバータ(ADC)とデジタル信号処理による、セルフトレーニング型識別回路を提案した[73]。周期的なゲートパルスの印加タイミングを基準として、ADC を用いて APD 出力波形のサンプリングを行い、ロジック回路を用いた数値演算により、履歴の平均値との差を取ることで容量性ノイズを除去する。これは、量子暗号において、光子検出とダークカウント・アフターパルスの発生確率が低く、APD 出力信号の平均と容量性ノイズ波形とが同等と見なせることを利用している。ロジック回路は、DSP 的な回路を用いた逐次処理を想定し設計を行った。この信号処理回路を FPGA によって実現し 1.5 GS/s の ADC から出力される光子検出信号の識別を行った。

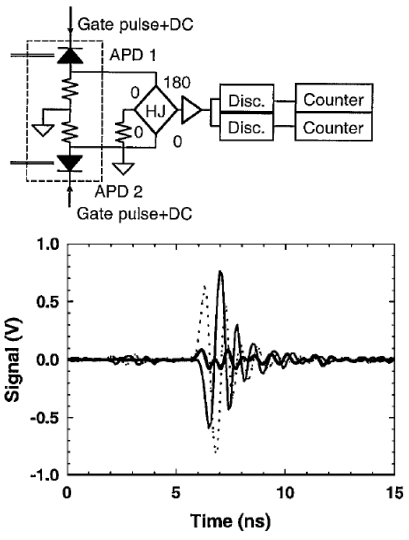
図 4.2.2(b)は、セルフトレーニング動作を示したものである。図 4.2.2(b)-(1)は 32 回重ね書きしたサンプル波形、(2)は平均化した波形をそれぞれの波形から引き算した結果である。これらより、容量性ノイズをキャンセルし十分な S/N が得られることがわかる。

表 4.1.1　各種光子検出回路

<table>
<tr><th>反射波形[77]</th><th>Discharge[29]</th></tr>
<tr><td>


D. S. Bethune, et al., J. of Mod. Optics, Vol. 51, No. 9-10, p.p. 1359 (2004)
</td><td>


A. Yoshizawa, et al., Appl. Phys. Lett. Vol. 84, No. 18, p.p. 3606 (2004)
</td></tr>
<tr><th>正弦波除去[67]</th><th>バランス検出[27]</th></tr>
<tr><td>


BEF: Band Elimination Filter
</td><td>


</td></tr>
</table>

表 4.2.2　光子検出の高速化により影響の予想される回路方式とその内容

	検出方式				原因	対策
	波 形 反射	Dis-charge	正 弦 波	バ ラ ンス		
振幅	●	●	-	●	GP 波形・APD 寄生容量の個体差	回路利得を精密に調整
位相	●	○	-	●	光ファイバ・同軸ケーブル長の公差	GP 位相・回路の位相を独立に、精密に調整
f 特	●	●	●	●	帯域制限・分散による高域の歪み	周波数特性の厳密な調整
増倍率	○	●	○	●	雪崩増倍時間の短縮	高感度化

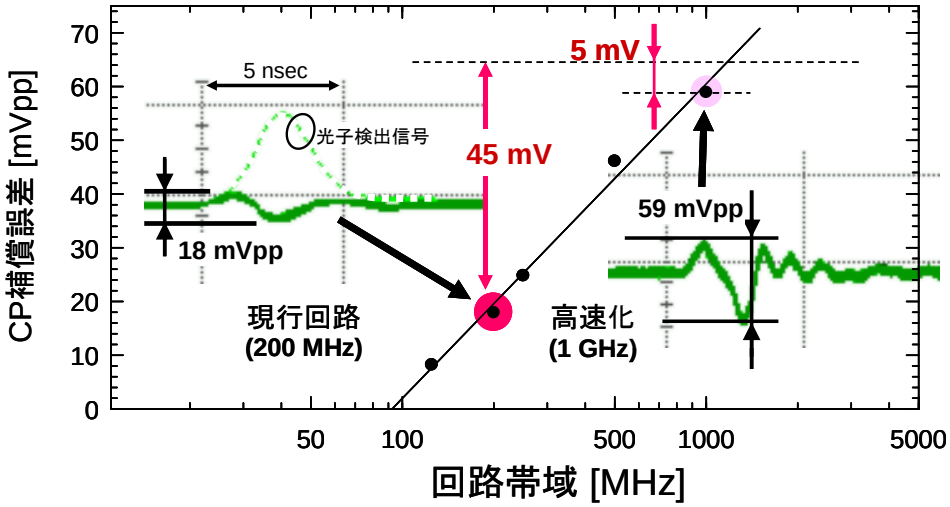


図 4.2.1 検出回路の帯域と容量性ノイズキャンセル誤差の関係

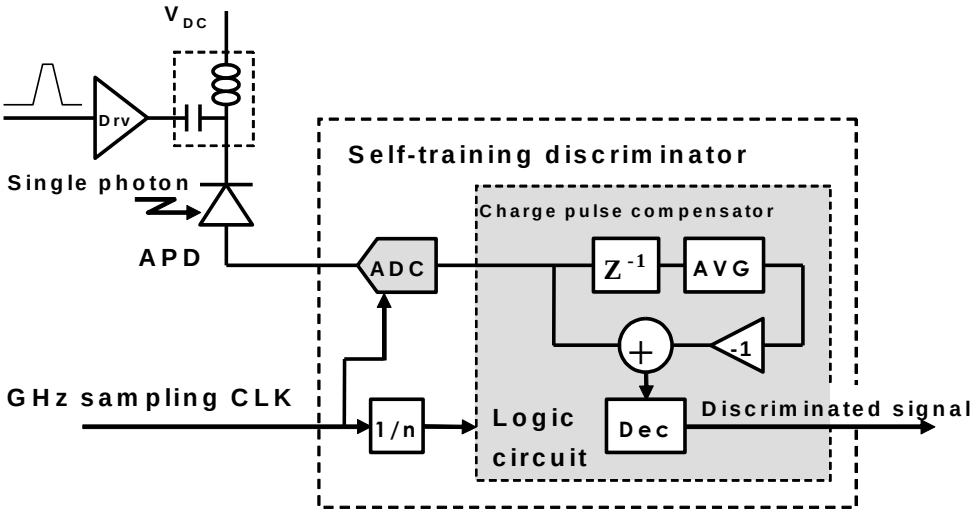
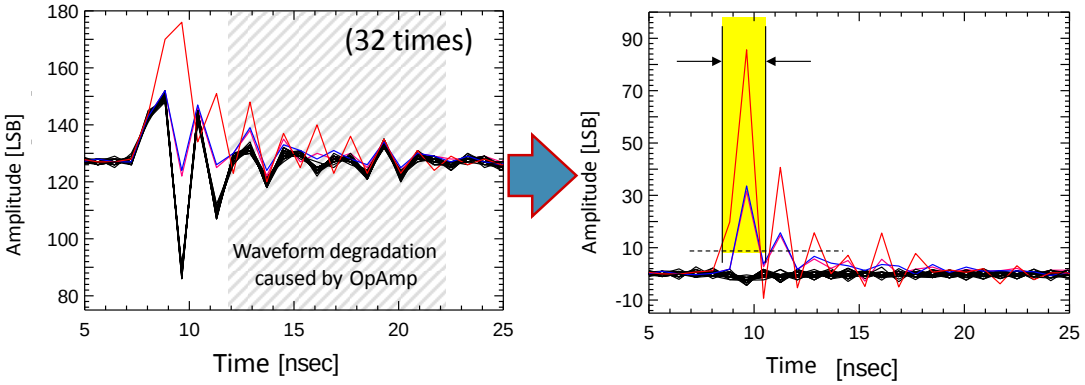


図 4.2.2(a) セルフトレーニング型検出回路の構成



(1)重ね書きしたサンプル波形　　(2)平均化した波形をそれぞれの波形から引き算

図 4.2.2(b) セルフトレーニング型検出回路の動作

4.2.2　特性評価

超小型 APD モジュール[73]と組み合わせ、光子検出器の特性評価を行った。まず、APD へ印加するゲートパルスの振幅と、識別閾値の評価を行った。ゲートパルスとダークカウント特性の関係を図 4.2.2(c)に示す。光子検出率一定の条件では、ゲートパルス振幅が 6 V 以下では、ダークカウント確率が急激に増加し、量子鍵生成レートの劣化につながる。識別閾値は、識別回路で非光子検出状態でのノイズ分布を解析し、ノイズ振幅の標準偏差の 5 倍を閾値とした。これはノイズを正規分布として、ダークカウント確率 2.9×10^{-7} に相当する。以上の結果を用いて測定したバイアス電圧に対する光子検出特性を図 4.2.2(d)に示す。ゲー

ト幅 500-ps、300-ns の dead time 条件では、ダークカウント確率 $P_d = 3.0\times10^{-4}$ において、光子検出効率 $\eta = 30\%$、$P_D = 2.5\times10^{-5}$ において $\eta = 10\%$が得られた。これらは、以前[78]よりも同じ光子検出効率 η において 1/10 の P_D と十分な性能である。

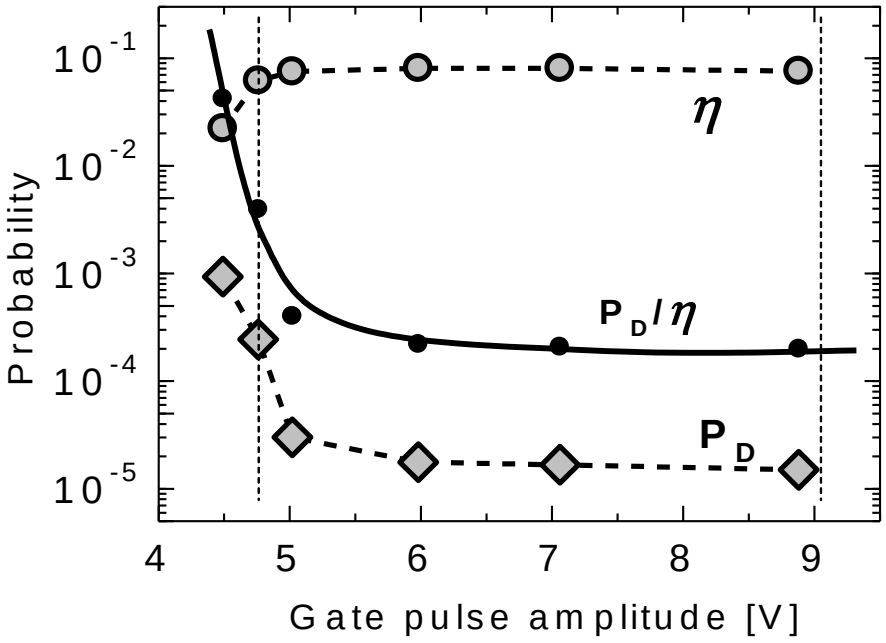


図 4.2.2(c)　ゲートパルス振幅とダークカウント確率の関係

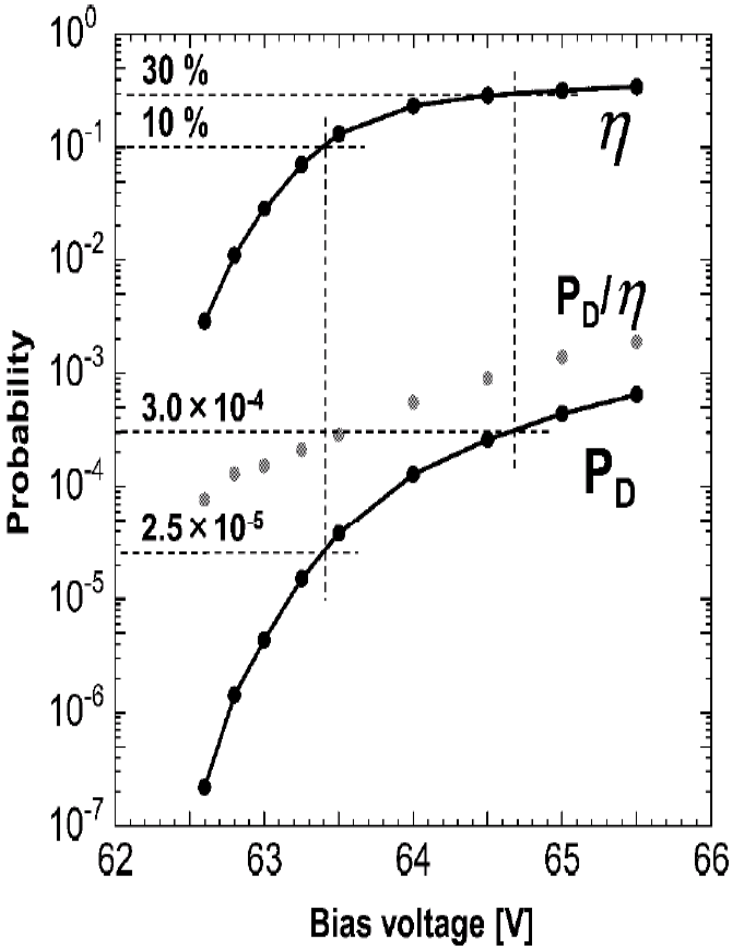


図 4.2.2(d)　光子検出特性

4.3　リアルタイム量子鍵抽出ハードウェア技術

量子鍵配送は光子伝送と光子伝送・検出結果に基づいた鍵抽出(蒸留)処理の大きく二つのブロックから構成される。単一光子を媒体とした光子伝送では、送信側（Alice）において光子源により単一光子を生成し、符号器により乱数情報をエンコードして送信する。受信側（Bob ）では、送られてきた光子信号を復号器によりデコードし、光子検出器で検出する。その後、光子信号に施した変調情報及び検出情報を元に信号処理部で最終鍵を抽出する。従って、最終鍵生成速度を向上させるためには、光子伝送の高速化・高効率化のみならず、最終鍵抽出のための信号処理の高速化・高効率化が必須となる。3 章で説明した QKD 装置のシステム周波数は 62.5MHz、最終暗号鍵生成速度が～kbps であったのに対し、最終暗号鍵生成速度の目標が 3 桁高い 1 Mbps であるため、暗号鍵蒸留処理も 3 桁程度の高速化が必要となる。図 4.3.1 に鍵抽出処理部への性能要求をまとめる。Decoy-BB84 プロトコルでは、1 ビットの光子信号を表すために、鍵情報に 1 ビット、基底情報に 1 ビット、光強度を 4 値で変調する Decoy state に 2 ビットの乱数が、さらにランダムパーミュテーションに 1 ビットが必要になる。後述(4.4.1 で説明)する鍵生成速度 1 Mbps を実現するシステムは、1.25 Gbps x 8 チャネル= 10 Gbps 構成なので、10 Gbps x 5 ビット=50Gbps の入力データ処理が必要となる。秘匿増強処理は、n ビットの暗号鍵に、m×n－mビット（n＞m）の秘匿増強行列を積算しmビットの最終鍵を得るので、 1 Mbit 単位[79][80]で秘匿増強処理を行うためにはブロック長 1Mbit の大規模行列演算が必要となる。

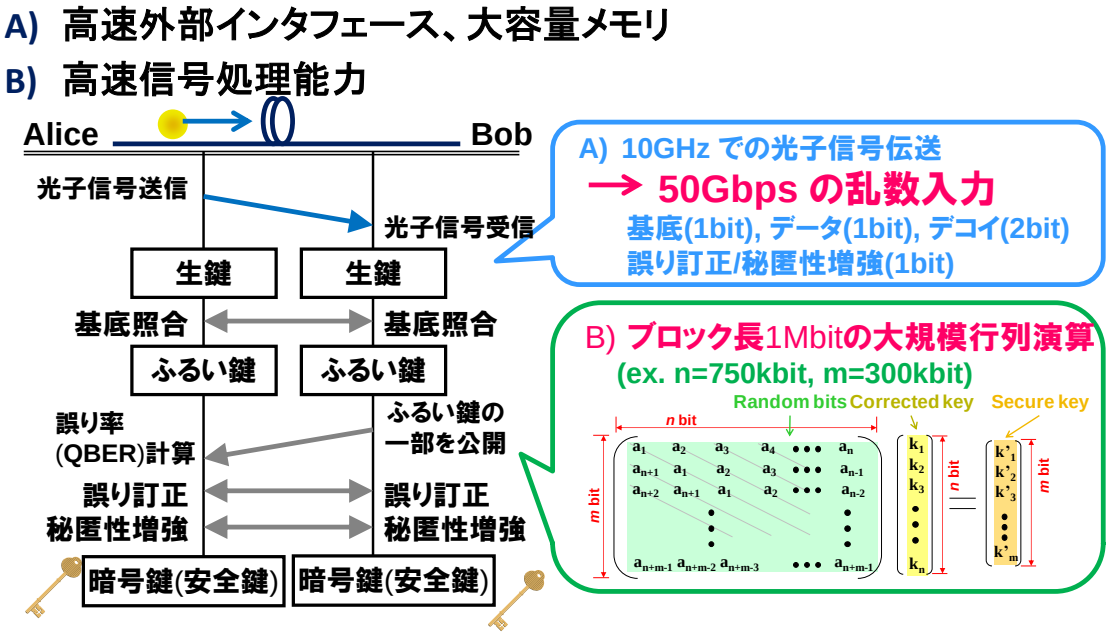


図 4.3.1　鍵抽出処理部の性能への要求

図 4.3.1 の要求を満たすために FPGA を利用して鍵蒸留処理をハードウェア化し、処理の並列化も活用することによって目標とする鍵生成速度を達成することとした。本ハードウェアエンジンは、大規模 FPGA／高速外部インタフェース／大規模メモリを搭載した基板と、基板上で動作する FPGA コードから成り、光子伝送システム、および光子検出器より乱数データ、および検出データを受け取った後、フレーム同期、基底照合、ランダムパーミュテーション、誤り訂正、秘匿増強を行う。秘匿増強の際の漏洩情報推定は、文献[79][80]を参照して行った。図 4.3.2 に鍵蒸留基板のブロック図を、表 4.3.1 にインタフェース一覧をまとめる。フレーム同期確立のためには送受信に使用した乱数全てを基板上で処理する必要があり、1.244 GHz 動作の QKD リンク 8 チャネルの波長多重システムに対応するために、10-Gbps 光インタフェース(XFP)を 8 ポート実装し、また 1 Mbit のシフト鍵を 1 ブロックとしてランダムパーミュテーション、誤り訂正、秘匿増強を行うために最大規模の FPGA を 6 つ搭載し、さらに各乱数や誤り訂正処理の一次推定値、行列値等を記憶しておくために合計 5 GByte のメモリも搭載している。

8 チャネルの入力情報を 4 チャネルずつ 2 系統に分け、2 つの FPGA （IA 、1B ）で収容、フレーム同期、基底照合、及び、ランダムパーミュテーションをこれらの FPGA で行う。誤り訂正用に FPGA2 及び 3 を搭載し、秘匿増強処理用 FPGA4 を搭載している。さらに、対向装置との通信を制御するために FPGA5 と XFP を搭載し、外部サーバから各 FPGA にアクセスするために PCI –Express x 8 のデータパスを配備している。各 FPGA 間は 10G 電気パス（XAUI ）で接続されている。

図 4.3.3 に実装した誤り訂正符号(LDPC：Low Density Parity Check)[81]の誤り訂正効率 f(e)を、図 4.3.4 に誤り訂正および秘匿増強の処理時間の測定結果の一例をまとめる。シャノン限界を実現できる誤り訂正符号を用いた場合には誤り訂正効率 f(e)は 1.0、誤り訂正性能が劣化するにつれて f(e)は大きくなり、より多くの情報量が誤り訂正に費やされる。

誤り率に応じて符号化率を変更することで、3～10%までの誤り率範囲で、誤り訂正効率が 1.3 以下となる誤り訂正符号を準備することができた。この値はシャノン限界より約 1 dB の劣化に相当する。秘匿増強処理よりも誤り訂正処理に時間を要する結果となり、使用する検査行列によって処理時間は大きく変化する。各処理はパイプライン的に実行されるので処理時間を最も要する過程がスループットを制限する。したがって、検出効率を含めた光子伝送過程で十分な生鍵およびシフト鍵生成速度が得られている状況では、最終鍵生成速度は誤り訂正処理速度で制限されることになり、量子誤り率（QBER：Quantum Bit Error Rate）3%以下の場合に 6 Mbps 以上、QBER4%の場合に 4 M bps のシフト鍵を処理できる。文献[82]の例では QBER が約 3%、シフト鍵の約 30%が最終鍵として残るため、総じて、今回開発した鍵蒸留高速化エンジンが 1 Mbps 以上の最終鍵速度を達成できる性能を有していることが確認できた。

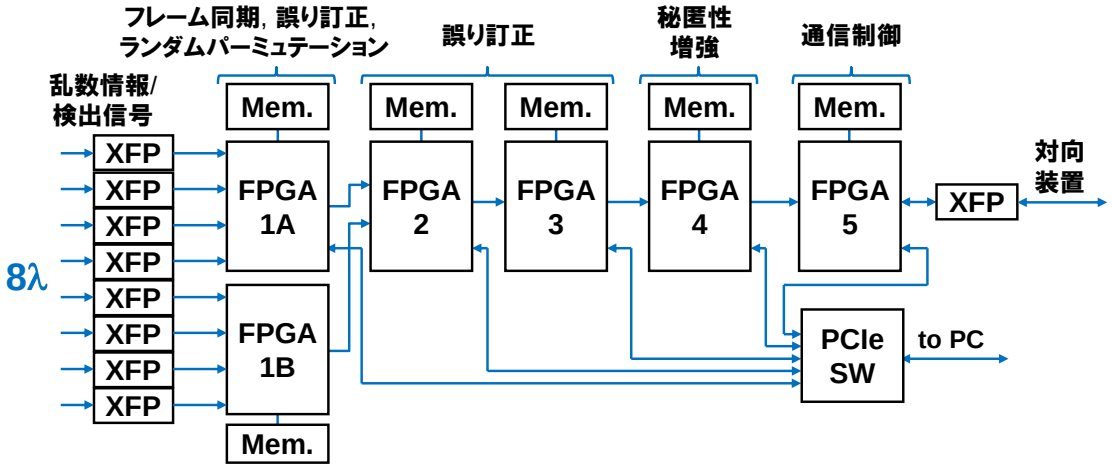


図 4.3.2　鍵蒸留基板のブロック図

表 4.3.1 鍵蒸留基板のインタフェース一覧

	IF	ポート数	備考
外部 IF	XFP (10G 光 IF)	送受 3 ポート 受信のみ 6 ポート	QKD 装置からの乱数受信に 8 ポート、対向間通信に 1 ポート
	10/100/1000 Ether	4 ポート	バックボード経由で他のスロットと接続
	PCI -Express	8 レーン	制御用 IA サーバより各 FPGA にアクセス
	SMA	クロック入力 1 ポート データ出力 1 ポート	外部からの 500MHz クロック入力に同期した 1Gbps データを出力
FPGA 間 IF	XAUI (10G 電気パス)	各 FPGA 間 10Gbps 送受	FPGA 間のデータ送受用

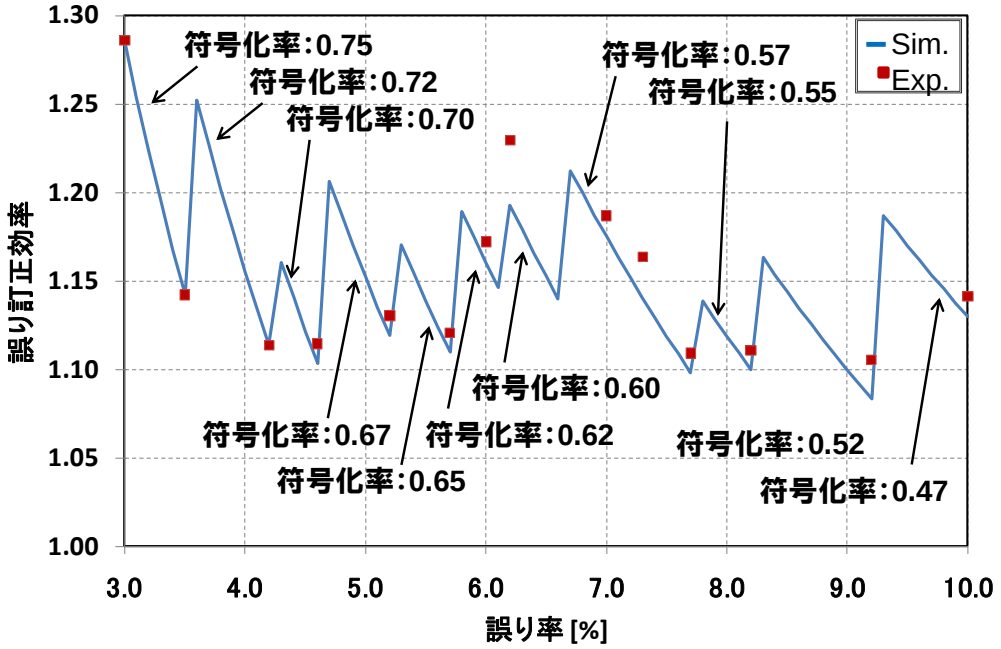


図 4.3.3 誤り訂正効率

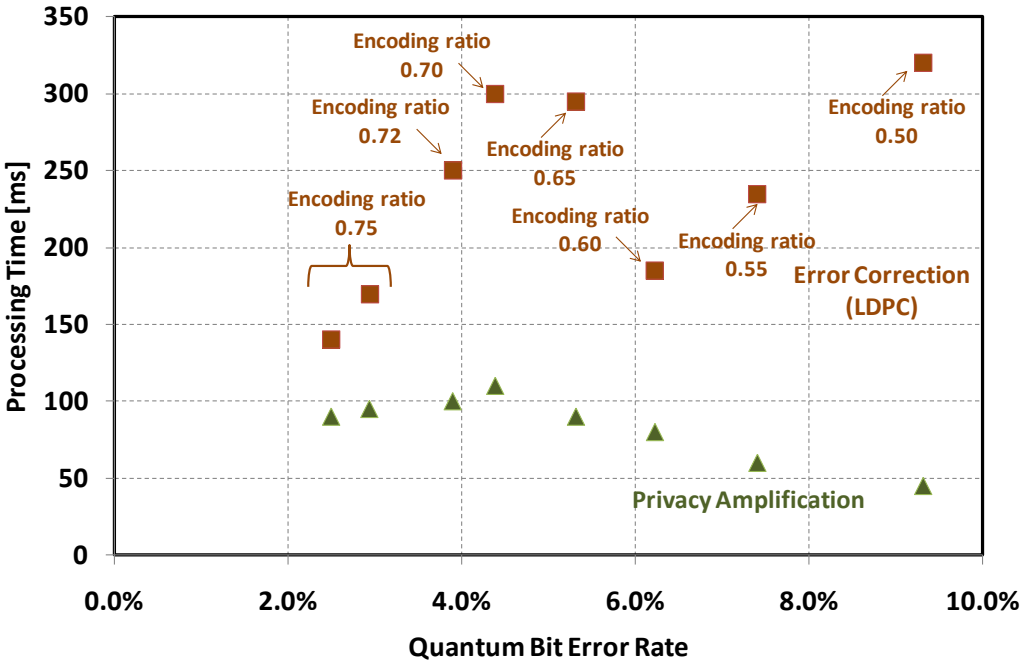


図 4.3.4 鍵蒸留基板処理時間測定結果

4.4　高速量子鍵配送システムによる長期間安定化動作

4.4.1　システム構成

メトロ圏内で動画の One-time pad 暗号化が可能な Mbps クラスの鍵生成を実現する QKD システムを目標とした。図 4.1.1 に鍵生成速度の見積もりを示す。光子検出器の動作速度をほぼ上限の GHz とした場合、シングルモードファイバ 50 km(純粋なファイバ損失 10 dB)伝送したときの鍵生成速度は、100 kbps と見積もることができる。そこで、動作速度 1.25 GHz、8 波長多重まで拡張可能な高速 QKD システムとした。本システムは、4.1 PLC による単一方向・偏波無依存型 WDM 技術、4.2 高速光子検出技術、4.3 リアルタイム量子鍵抽出ハードウェア技術によって構築した。送受信器間の同期については、3.1.1 で説明した同期信号を量子信号と WDM 伝送する技術を用いた。本システム構成のブロック図を図 4.4.2 に示す。本システムは、光子送信部、Decoder 部、光子検出部、同期系、制御部、鍵抽出のブロックによって構成され、各ブロックは、advanced telecom computing architecture (ATCA) [83]に準拠したシャーシに挿入できるブレード構成となっている。図 4.4.3 に示すように、必要な鍵生成速度に合わせた数の光子送信部、受信部、光子検出部のブレードを実装できるようになっている(Pay as you grow)。

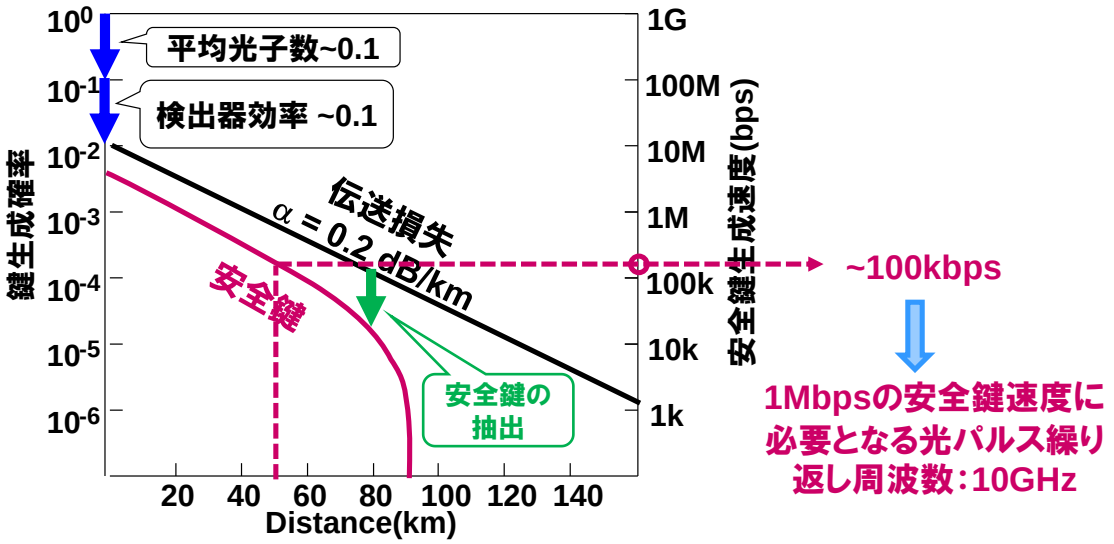


図 4.4.1　鍵生成速度の見積もり

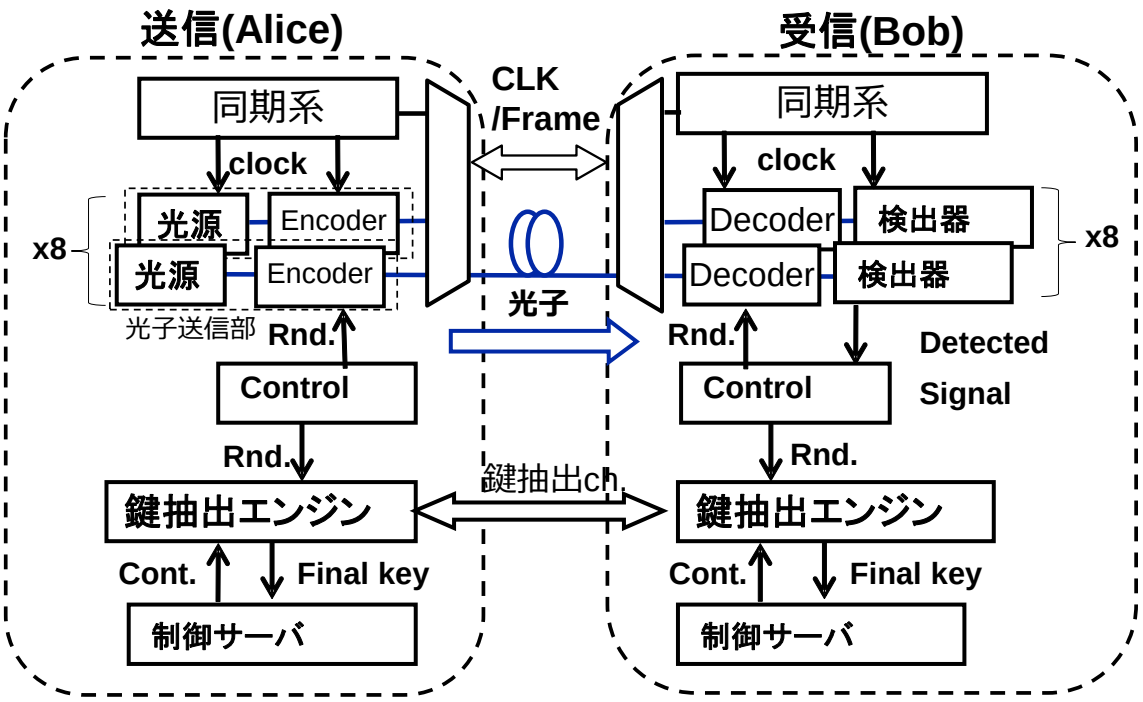


図 4.4.2　QKD システムのブロック図

図 4.4.3　WDM QKD システムのハードウェア構成

光子送信部は、光源、Encoder（PLC干渉計、変調器)から構成される。送信波長は、ITU-T 100-GHzグリッドの1545.3 nm – 1550.9 nmである。Decoder部は、構成が簡易で光学損失のより少ない2 x 4干渉計を用いた位相-時間コーディング(方式B)を採用した。同期系は、同期信号用光源と受信フォトダイオード、遅延制御回路から構成される。制御計は乱数発生

回路や各ブロックへのclock信号の供給を行う。光子検出部は、Decoder部から受け取った光子信号を検出・識別を行う。鍵抽出部は、光子伝送・検出信号から最終鍵をリアルタイムで抽出する。本システムは、8波長多重まで対応可能、各チャネルの動作周波数は1.25 GHzである。

4.4.2　長期間フィールドテスト

上記システムを用いて、以下に示すように(1)光ファイバ伝送路の変動の影響評価、(2)実使用環境下に置いた装置の安定動作評価をそれぞれ切り分けて行うために、二通りの長期間フィールドテストを行った。

(1) 屋外ファイバを用いた動作試験

図4.4.4(a)に実験に用いたフィールドファイバのイメージ、(b)にOTDR測定結果、(c)には直交する二つの偏波光をフィールドファイバに入力・伝送し、それぞれについて測定した光パワーの時間変動を測定した例を示す。図4.4.4(a)に示すようなNICT小金井、NEC府中事業所を接続するフィールドファイバ(ファイバ区間の95%以上が架空ケーブル、伝送距離は往復22 km、伝送損失は13 dB(理想的なファイバでは65kmに相当))を用い、装置は送受信ともNICT小金井に設置して実験を行った。図(b)からわかるように、折り返し地点以外にも二か所の接続点があり、2.5 dBの接続損がある。図(c)をみると、偏波はランダムに変動、特に7:00から17:00の昼の時間帯に激しく変動していることがわかる。一般的にフィールドファイバ中の偏波は道路を走る自動車などの振動によって変動すると言われており、実験に用いたファイバの大部分が架空ケーブルであったため影響が顕著に現れていると思われる。

このような光ファイバ伝送路としては十分厳しい条件において、λ1 (1547.72 nm)、λ2 (1550.92 nm)の二波長の量子信号を多重し30日間連続動作実験を行った。このとき、光子検出器のAPDへのゲートパルスタイミングを常に検出効率が最大となるようにフィードバック制御を行い(A)、変調器バイアス(B)、PLC干渉計の温度(C)および位相補償用変調器の振幅(D)をQBERが最小となるようにフィードバック制御を行った(図4.4.5)[47]。30日間連続動作実験を行った際のQBER、鍵生成速度の時間変動結果を図4.4.6に、30日間での平均値一覧を表4.4.1に示す。これらより、30日間にわたってメンテナンスフリーで誤り率3%以下の安定した鍵生成が行えたことがわかる。平均の量子ビット誤り率は1.70%、安全鍵生成速度は229.8 kbpsであった。一方のチャンネル(λ2)では1ヶ月間で徐々に鍵生成速度が減少しているが、用いた光子検出器のAPD冷却部の着霜により冷却効率が低下したためであるが、λ1と同様のものを用いることで着霜は起きずこのような劣化は生じないと考えられる。以上により、提案したPLCによる単一方向・偏波無依存型波長多重QKDシステムが光ファイバ伝送路での変動の影響を受けず安定動作することを実証することができた。

図 4.4.4(a)　実験に用いたフィールドファイバのイメージ

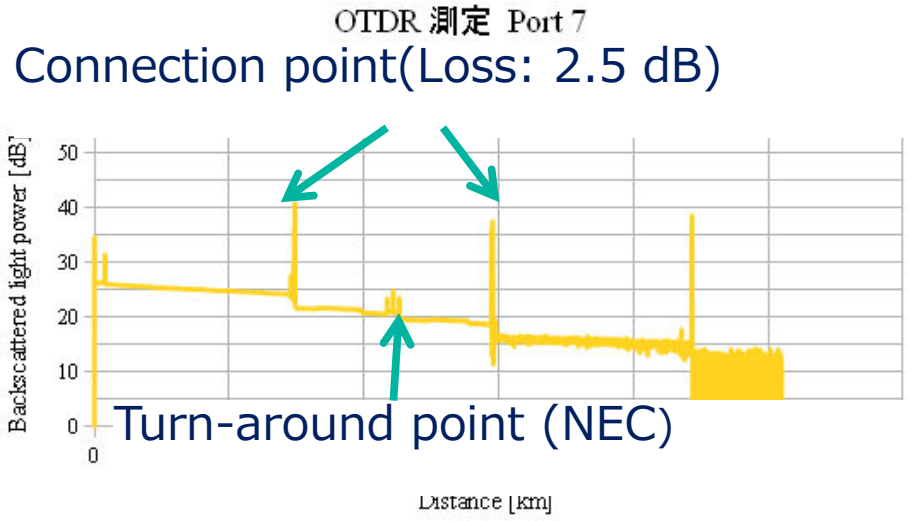


図 4.4.4 (b) 実験に用いたフィールドファイバの OTDR 測定結果

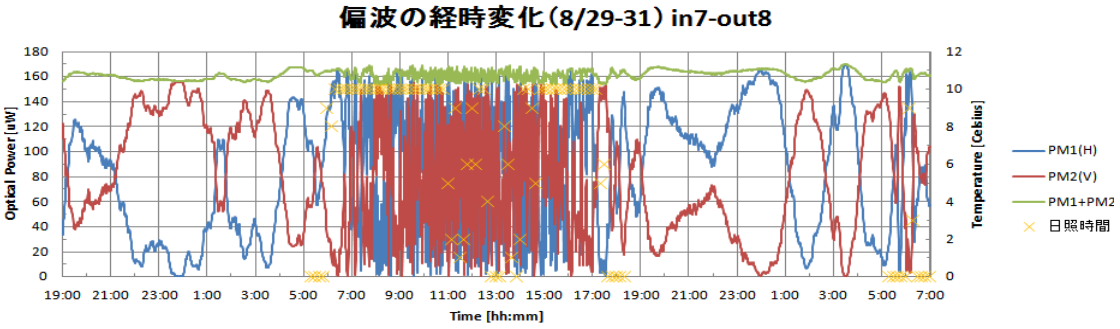


図 4.4.4 (c) 実験に用いたフィールドファイバにおける偏波の時間変動の測定例

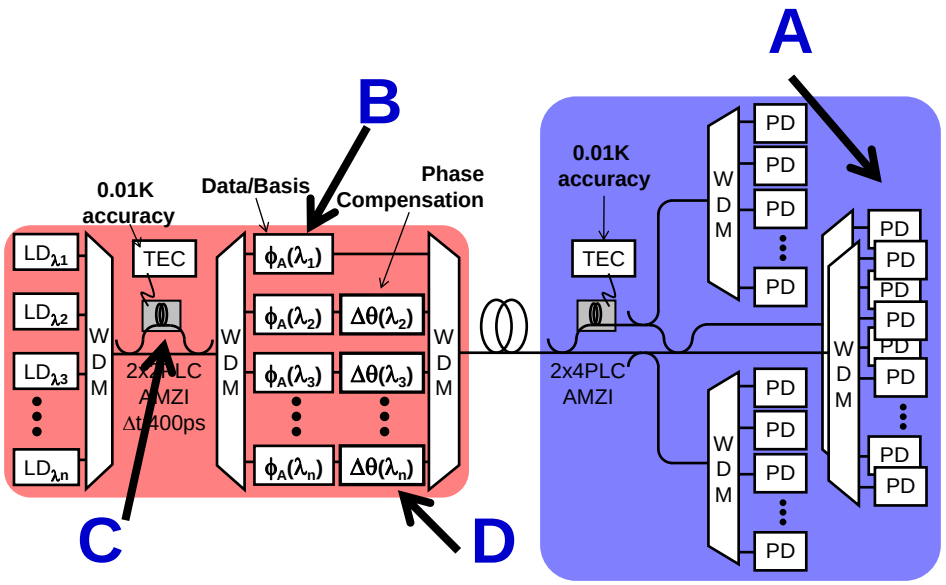


図 4.4.5 QKD 装置内のフィードバック制御ポイント

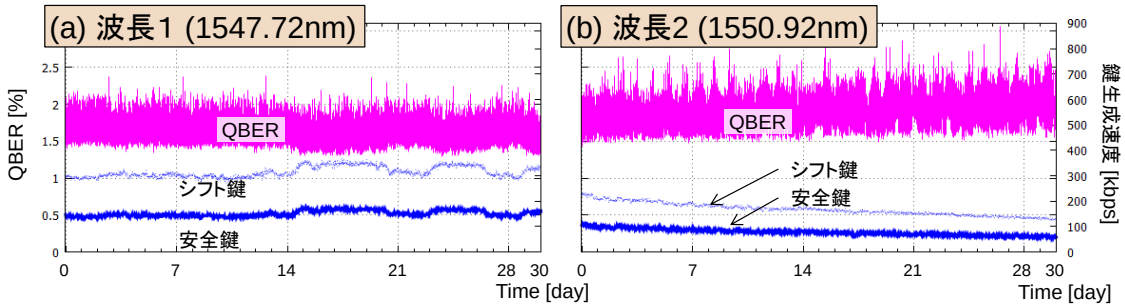


図 4.4.6　30 日間連続動作実験結果

表 4.4.1　30 日間連続動作実験結果一覧

	QBER [%]	シフト鍵生成速度 [kbps]	安全鍵生成速度 [kbps]
λ1 (1547.72 nm)	1.61	315.3	151.5 (w/o Decoy)
λ2 (1550.92 nm)	1.86	168.0	78.3 (w/o Decoy)
2 波長での合計	1.70	483.3	229.8 (w/o Decoy) 112.4 (w/ Decoy†)

(2)実使用環境下に置いた装置の動作試験

(1)の結果により、提案した PLC による単一方向・偏波無依存型波長多重 QKD システムが光ファイバ伝送路での変動の影響を受けず安定動作することを実証することができたため、実使用環境に装置を設置し長期間運用試験を行った[48]。設置場所は、NEC のサイバー攻撃対策の中核拠点である「サイバーセキュリティ・ファクトリー」[84]である。本試験には単一波長での運用に特化したコンパクトな装置を用いた。本システムには鍵管理システムや、課題エで開発した回線暗号アプリケーションも搭載されている。本試験では、送受信機間を結ぶ伝送ファイバは 30 m であるが約 11dB の減衰器を挿入している、装置設置場所は実験室環境ではなく、送信機がサーバ室、受信機が通常のオフィス環境であるため室温などの環境変動が大きい。このような実利用環境下で 21 週間の長期間連続運転試験を行った。その結果を図 4.4.6 に示す。フィードバック制御安定化制御を適用することにより、鍵生成速度の揺らぎを±8.6%と＜±10%に抑制することに成功した。なお、長期運用試験を 21 週間で終了した理由は設置場所ビルの法定点検による停電である。以上により、提案した PLC による単一方向・偏波無依存型 QKD システムが設置環境の変動(特に温度)の影響を受けず安定動作することを実証することができた。

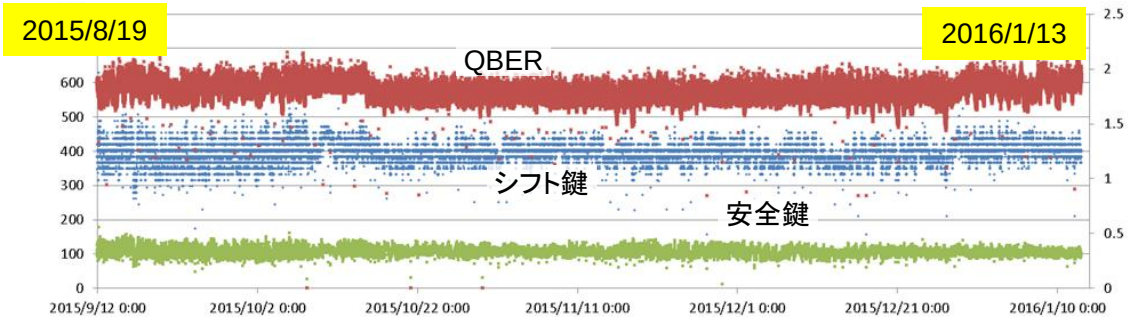


図 4.4.6　21 週間連続動作実験結果

表 4.4.2　21 週間連続動作実験結果一覧

	QBER [%]	シフト鍵生成速度　[kbps]	安全鍵生成速度 [kbps]
1 波長	1.79	393.2 kbps	107.7 kbps (w/ Decoy)

以上の二つの長期間動作試験により、提案した QKD システムが光ファイバ伝送路の変動の影響、設置環境変動の影響を受けず長期間の安定動することを実証することができた。

５．量子鍵配送ネットワークとアプリケーション

3 章ではリアルタイム量子鍵生成が可能な量子鍵配送システムの実証とこのシステムを用いた 1:2 量子鍵生成・共有実験や異機種量子暗号システムの相互接続実験といった量子鍵配送ネットワークの初期実験を世界に先駆けて行ったことについて述べた。4 章では、PLC (Planar Lightwave Circuit)単一方向型システムを WDM し、高速検出回路と鍵抽出専用ハードウェアにより鍵生成速度 Mbps クラスの高速化が達成できることを実証、さらに、提案した要素技術を用いて構築した高速 QKD システムを用いた長期間のフィールド実験により、高速かつ長期間安定な量子鍵配送を達成したことを述べた。

量子鍵配送技術は二者間の Point to point(P2P)鍵共有技術であるが、実際の秘匿通信への応用を考えると、P2P に限らず携帯端末をはじめとする複数端末間での秘匿通信をサポートすることが求められる。さらに、3 章で実証したような異機種量子暗号システムから成るネットワーク構成に対応できることや、ネットワークの可用性や信頼性、スケーラビリティも要求される。以下では、QKD の応用を広げ、セキュア鍵配送ネットワークインフラストラクチャ構築に向けた、ネットワークへの要求、その要求に基づいたネットワークアーキテクチャ、ネットワーク運用管理、鍵管理、アプリケーションへの鍵供給機能そして、代表的なアプリケーションについて述べる。

5.1　量子鍵配送ネットワークへの要求

QKD は P2P リンクであるため、量子鍵配送(QKD)ネットワークに対しては、複数の携帯端末間での秘匿通信のサポートやネットワークの可能性、信頼性、スケーラビリティを実現するために鍵リレーと呼ばれる機能が要求される。さらに、QKD は BB84 [8]以外に、CV-QKD [85]、RR-DPS QKD [86]をはじめとする複数の方式があること、方式が同じであってもベンダ毎に鍵生成速度などの性能が異なることから、これら複数の方式や幅広い鍵生成速度に対応することが求められる。それぞれの QKD リンクは連続して鍵を生成するので、この鍵を管理する機能が非常に重要である。

二つ目の要求は、全てのアプリケーションに対して鍵を渡すユニバーサルなインタフェースである。アプリケーションとしては、データセンタと遠隔バックアップ間の秘匿通信のような、QKD ネットワークによる鍵を用いた高速 P2P 秘匿通信や P2P 以外の multi-parties to multi-parties (MPTMP) 、複数のスマートフォン間での秘匿通信が期待されている。

QKD ネットワークから供給された鍵が使われる際、暗号化鍵、復号化鍵は同一であり、改ざんされていないことが要求される。図 5.1.1 に鍵リレーを用いた QKD ネットワークのコンセプトを示す。この例では、ノード A-C での鍵同期を、Key_{AB} を Key_{BC} によってカプセル化することで実現する。その結果ノード A と C が同じ鍵を共有することができる。さらに QKD ネットワークは様々なネットワークトポロジー(P2P、リング、メッシュ)をサポートすること、スケーラビリティを有すること、複数のアプリケーションをサポートすることが要求される。

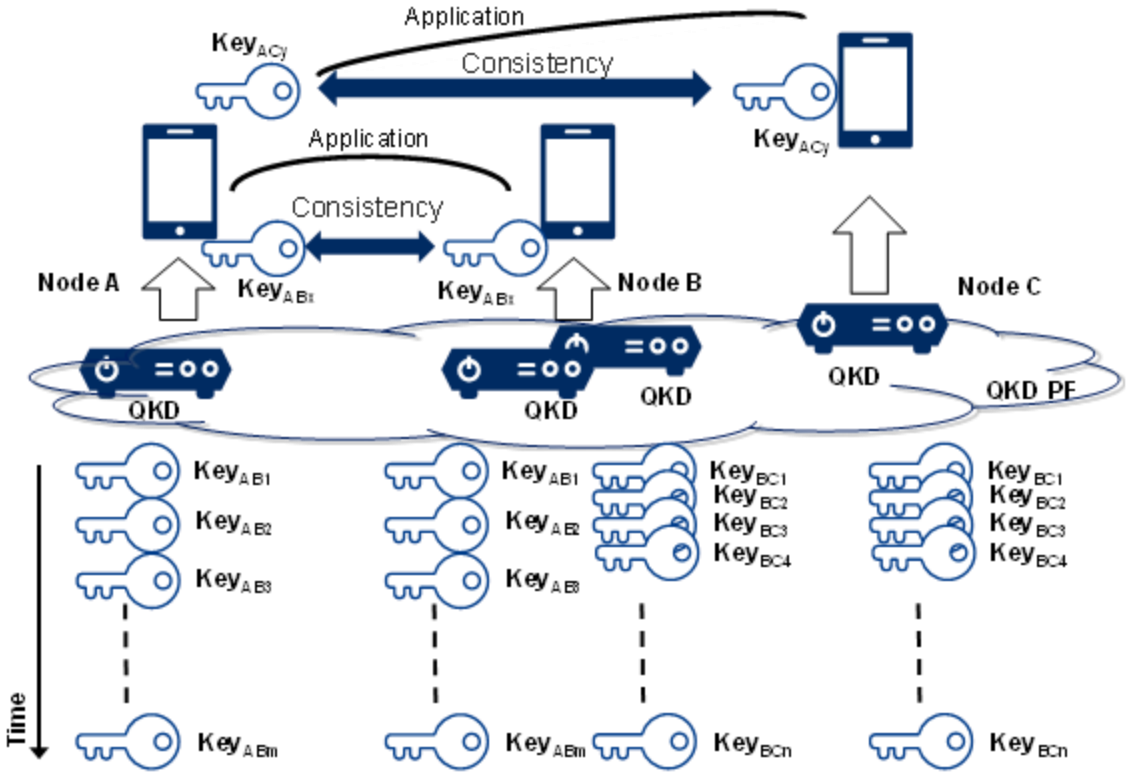


図 5.1.1 QKD ネットワークから供給された安全鍵の一致

(Key_{ABx} は QKD によりノード A-B で共有した鍵、Key_{ACy} は QKD と鍵リレーによってノード A-C 間で共有した鍵)

5.2 QKD ネットワークのアーキテクチャと機能

前節で述べたような要求を満たすために図 5.2.1 に示すような量子レイヤ、鍵管理レイヤ、鍵供給レイヤの 3 レイヤからなる QKD ネットワークを提案した。図 5.2.1(a)はアーキテクチャの概要、(b)はレイヤスタックを示す。鍵管理エージェント(KMA)は QKD リンクから量子鍵を収集するエージェントシステム、鍵管理サーバ(KMS)は集中管理サーバ、鍵供給エージェント(KSA)は安全鍵をアプリケーションに渡すエージェントである。各々のレイヤの機能を表 5.2.1 にまとめる。

量子レイヤでは、それぞれの QKD リンクはそれぞれの方式にした方って安全鍵を生成し続ける。鍵生成速度は、ファイバ損失をはじめとする動作条件によって異なるので、生成した鍵が一定量に達したところで、鍵管理レイヤにある KMA に鍵を push up する。

鍵管理レイヤの機能は、鍵の蓄積とリレー、ネットワークの運用管理である。鍵リレーによって様々なネットワークトポロジーや長距離での鍵共有を実現する。図 5.2.2(a)は 2 つの QKD リンクによって接続された 3 ノードネットワークの例である。この例では、QKD リンク 1 はノード A と B を接続しノード A と B は共通鍵 $Key_{A\text{-}B}$ を共有、QKD リンク 2 は、ノード B と C を接続しノード B と C は共通鍵 $Key_{B\text{-}C}$ を共有する。ノード A と C が共通

鍵を共有するためには、鍵 $Keys_{A\text{-}B}$ をノード B において $Keys_{B\text{-}C}$ によって One-time pad 暗号化しノード C に送る。ノード C では受け取った鍵を $Keys_{B\text{-}C}$ によって復号化する。鍵リレーを行うノードの認証は Wegman-Carter 認証[87]によって行い、鍵リレーの後鍵の同一性を確認するため鍵の同期は MD5 ハッシュを用いて行う。この認証過程では Strongly Universal$_2$ Hash 関数を用い、1500-byte のパケットに対して 256-byte の鍵を消費する。同時に、鍵リレーの暗号化に用いた鍵は破棄する。上記手順によって、直接接続する QKD リンクがないノード A と C で共通鍵を共有することができる。このケースでは、one-hop の鍵リレーを例に挙げて説明したが様々なネットワークトポロジーをサポートするために必要な multi-hop のリレーについても図 5.2.2(b)に示すように同様の技術によって実現することができる。

提案する QKD ネットワークは集中制御型をとっている。KMS は全 QKD リンクの鍵生成レートや誤り率(QBER)のほか、蓄積された鍵の量や消費した鍵の量をモニタするとともに、鍵生成の日時、鍵 ID、ユーザとアプリケーションの ID、鍵使用日時をチェックする。もしある鍵があらかじめ定めた期間よりも長い期間未使用であった場合は消去する。このように鍵のライフサイクルを適切に管理する。KMS はまた鍵リレーの経路や、異常があったときの QKD の経路再設定も行う。もし QBER が上昇するような異常があった場合、KMS は異常のあった機器を切り離し、ネットワーク運用者に異常を通知する。

鍵供給レイヤは二つの機能を提供するために導入した。ひとつはアプリケーションに非依存な鍵供給機能であり、もうひとつは安全鍵を QKD ネットワークから鍵を消費するユーザへ確実に供給する機能である。同一性を確保するために、鍵をクライアントに渡す前に、鍵の同期と相手の認証を行う。鍵供給と同時にリレーに使った鍵(図 5.2.2(a)の $Keys_{A\text{-}B}$, $Keys_{B\text{-}C}$ and $Keys_{AB*BC}$)は廃棄する。

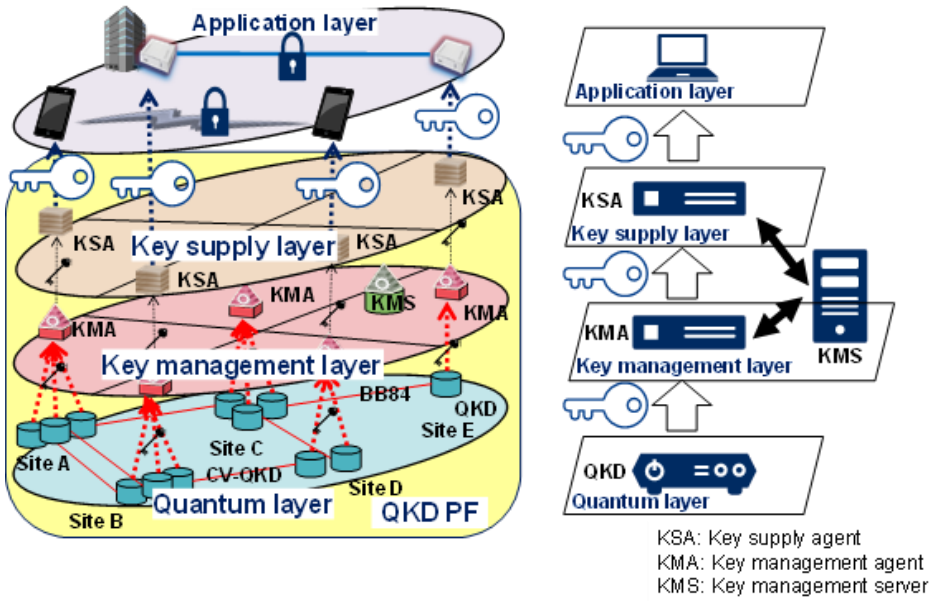
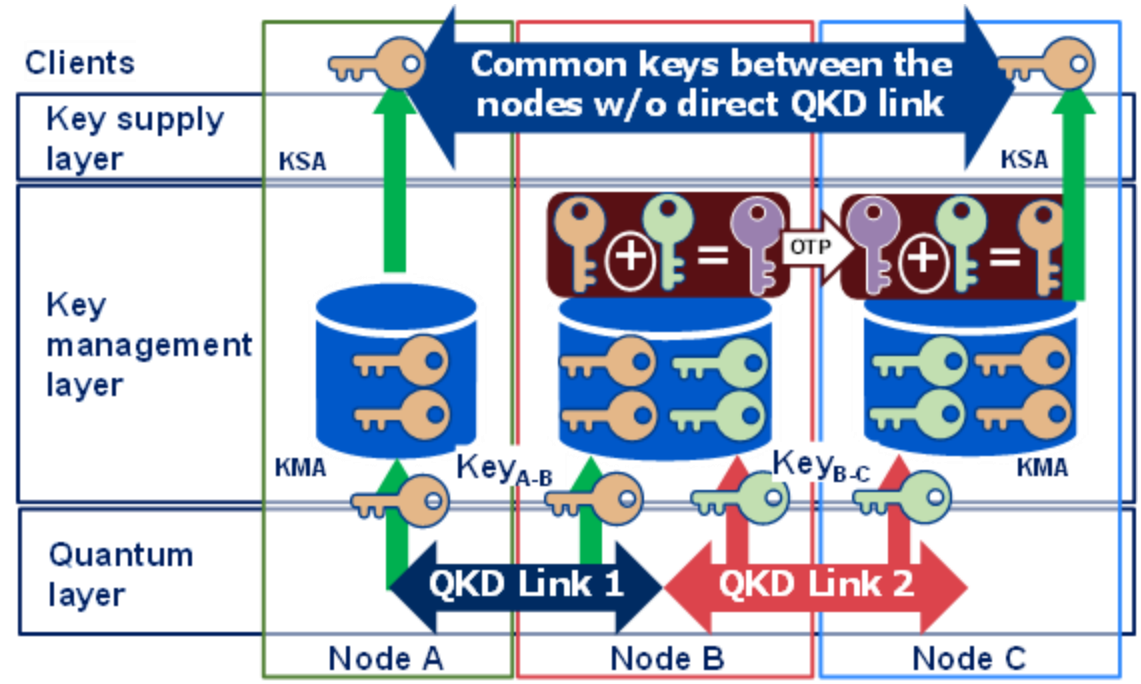
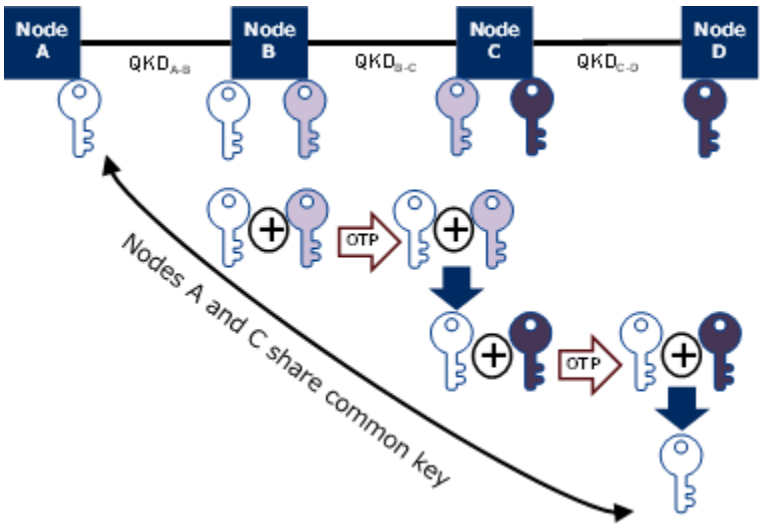


図 5.2.1　QKD ネットワークアーキテクチャ: (a) 概要, (b) システムレイヤ構成



(a)



(b)

図 5.2.2　鍵のカプセルリレー: (a) 3 ノード、2-QKD リンクの場合 (b) multi-hop 鍵リレー

表 5.2.1　QKD ネットワークのレイヤと機能一覧

Layer	Equipment	Function
Key Supply	KSA	Key supply to client
		Key synchronization
		Key identification (Wegman-Carter authentication)
		Key reception from KMA
Key Management	KMS	Statistics information of KMA and QKD collection
		Key relay management
	KMA	Key transfer to KSA
		Administration of QKD PF
		History management
		Key relay
		Key synchronization
		Key identification (Wegman-Carter authentication)
		Status monitor
		Secure-key collection
Quantum	QKD	Secure-key push up to KMA
		Secure-key generation

5.3　鍵管理方法

各レイヤの機能をサポートするために、図 5.3.1 と表 5.3.1、5.3.2 に示すような鍵フォーマットを定めた。QKD ネットワークにおける典型的なライフサイクルは以下のようになる。まず、安全鍵が各々の QKD リンクにおいて生成され、鍵生成時刻のタイムスタンプ、鍵サイズ、暗号化/復号化のタイプ識別子、その鍵を生成した QKD 機器名を含むヘッダ情報が付加される。鍵管理レイヤにおいては、鍵 ID ヘッダと鍵リレーフッタ(リレー開始ノードアドレス、リレー先ノードアドレス)が付加される。鍵リレーを行う際、Wegman-Carter authentication によってリレー先の機器認証を行う、また鍵の同期を MD5 認証によって行う。ヘッダ/フッタ情報は集中管理・制御を行う KMS へ送られる。鍵ファイルは KSA からの要求があると、ヘッダ情報と共に KSA に転送される。KSA がクライアントからの要求を受け取ると同期、認証を再度行い、タイムスタンプ、アプリケーション側の Source/Destination、アプリケーション ID の情報を含むヘッダを付加して KMS に送られる。最終的に鍵ファイルがクライアントに供給される。このように鍵のライフサイクルは統一的に管理される。

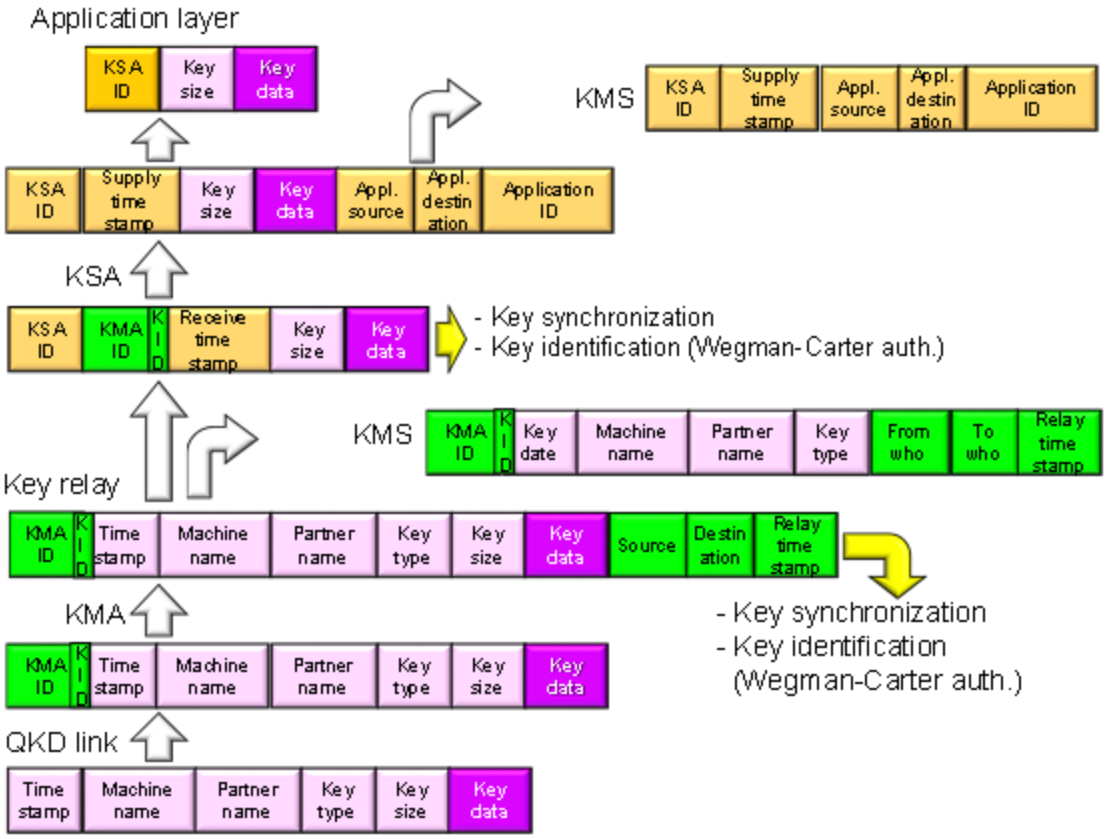


図 5.3.1　鍵のライフサイクル

表 5.3.1 鍵フォーマット(基本情報)

Header/Footer	Description
Time stamp	Time stamp of quantum key generation
Machine name	ID of QKD equipment at local site
Partner name	ID of QKD equipment at opposite site
Key type	Identifier of encoding key or decoding key
Key size	Secure-key size
Key data	Secure-key data
KMA ID	ID of KMA that receives quantum key
KID	ID of received quantum key at KSA
KSA ID	ID of KSA that receives quantum key
Receive time stamp	Time stamp of secure key reception at KSA
Supply time stamp	Time stamp of secure key supply from KSA
Appl. source	Source ID of application
Appl. destination	Destination ID of application
Application ID	Application ID

表 5.3.2 鍵フォーマット（リレー情報）

Header/Footer	Description
Relay time stamp	Time stamp of secure key relay
Source	Relay source
Destination	Relay destination

これらのアーキテクチャ、ネットワークおよび鍵管理手法を用いて図 5.3.2 に示すような Tokyo QKD ネットワークを構築し、運用試験を行っている。

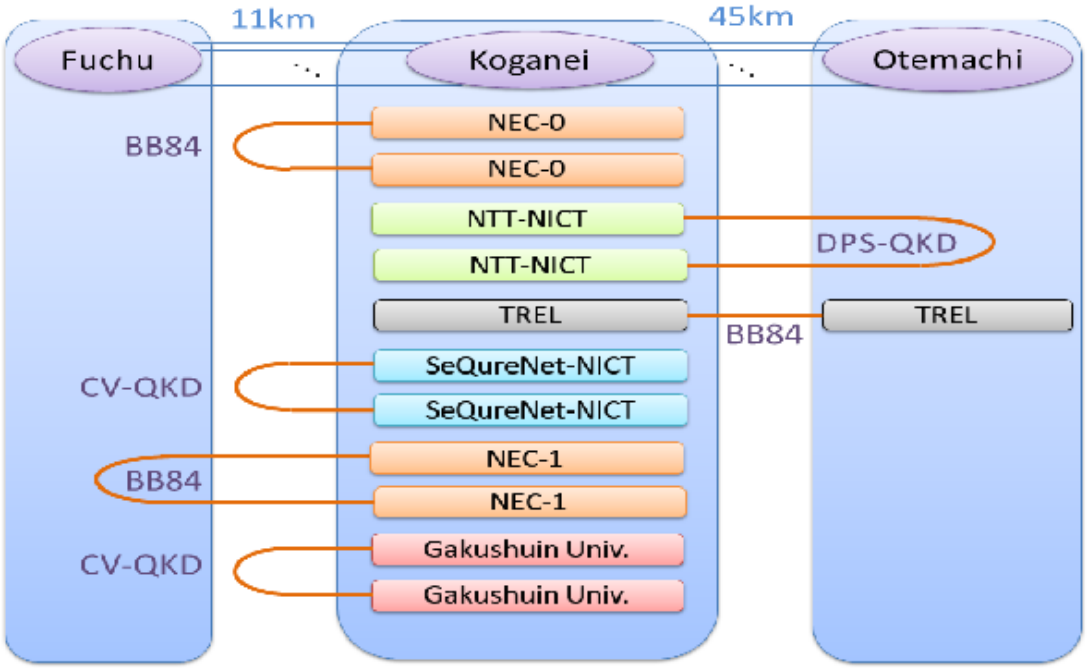


図 5.3.2 Tokyo QKD ネットワーク

5.4　量子鍵ネットワークにおける秘匿通信アプリケーション

本節では、QKD ネットワーク上での動作検証を行ったアプリケーション例について紹介する。まず、高速秘匿通信を目的として開発した QKD によって共有した鍵を advanced encryption standard (AES)暗号化の鍵として用いる QKD-AES ハイブリッドシステムについて紹介する。次に、複数携帯端末間の通信をサポートする秘匿スマートフォンシステムについて紹介する。これらアプリケーションを QKD ネットワークテストベッド Tokyo QKD ネットワークにおいて動作実証を行った。図 5.4.1 にそれぞれのアプリケーションの技術課題と施策をまとめた。以下でそれぞれについて説明する。

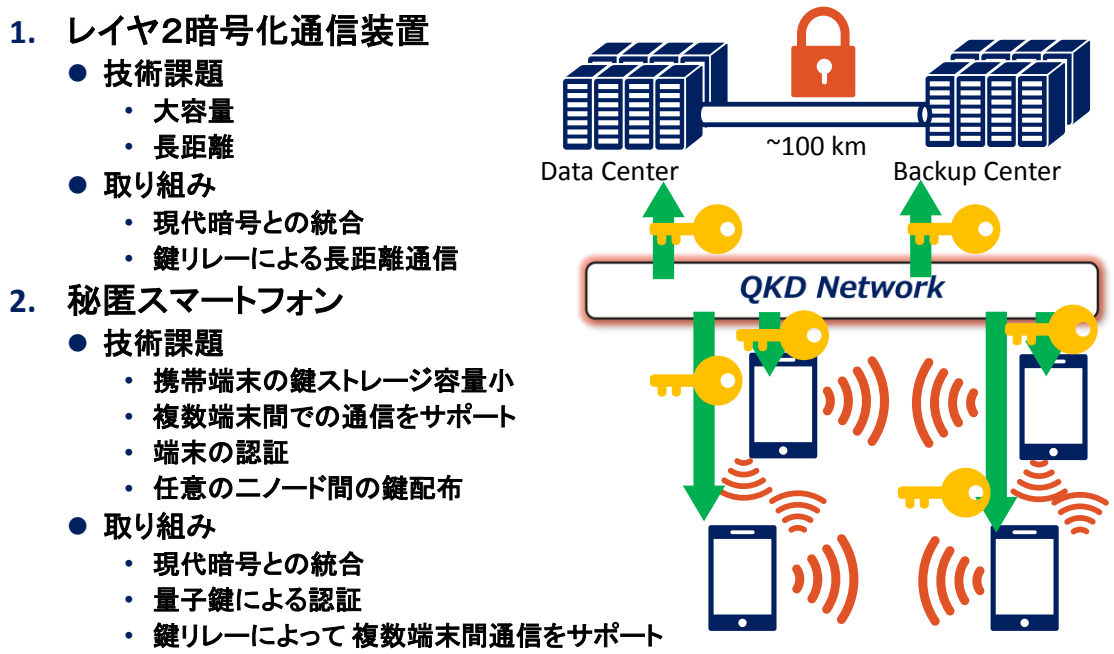


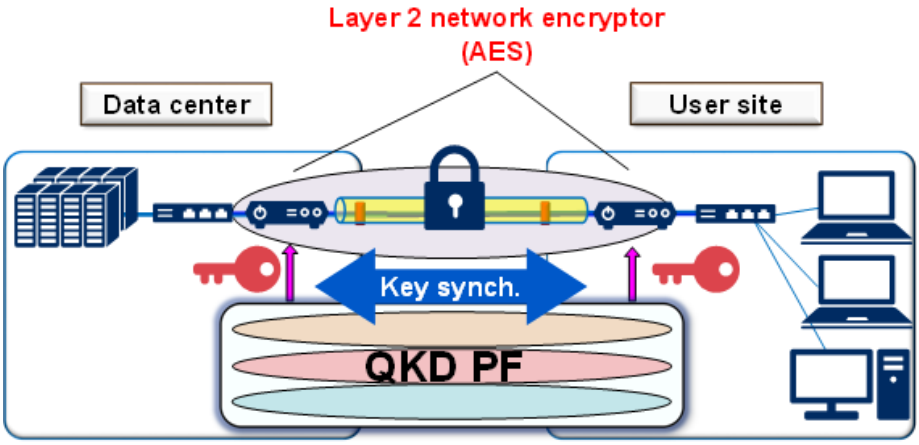
図 5.4.1　量子鍵ネットワークにおける秘匿通信アプリケーションの課題と施策

5.4.1　QKD-AES ハイブリッドシステム

データセンタとリモートバックアップセンター間の秘匿通信は、大容量かつ長距離(>100 km)が要求されることが多い。この要求を満たすために以下の二つのアプローチを組み合わせた。大容量化の秘匿通信を実現するために、必要な鍵量が少ない現代暗号を用いた。長距離化のためには、鍵リレーによる鍵共有を行った。図 5.4.2(a)は商用の Layer 2 ネットワーク暗号化通信装置[88]と QKD ネットワークを合わせた際のブロック図、(b)は装置全体の写真である。ここで Alice は送信側、Bob は受信側を表している。Layer 2 ネットワーク暗号化通信装置に安全鍵の受け取り機能、受け取った鍵の同期とチェック機能を追加した。このアプリケーションにおいて、Ethernet データは AES 暗号化され、その暗号化鍵は周期的に QKD ネットワークから供給されたものによって更新される。更新周期は最短で 1 秒、鍵の

同期機能は QKD ネットワークとは別に新規に開発した。暗号化されたデータの乱数性と鍵更新時に信号断のない連続したデータ通信とこの組み合わせで 21 週間の連続動作を確認(4.4.2(2)で説明)した。

(a)



(b)

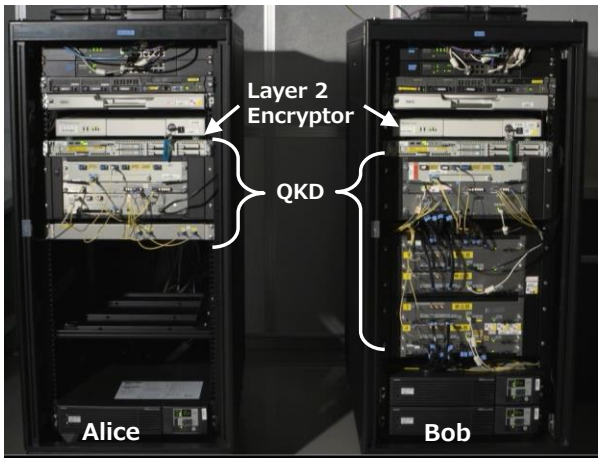
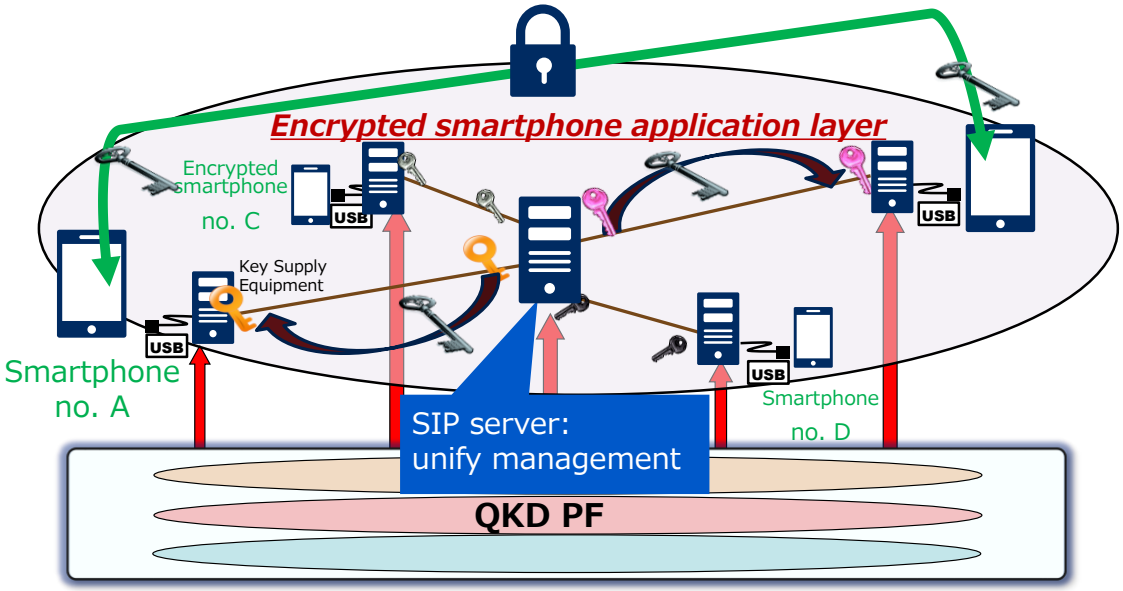


図 5.4.2 QKD-AES hybid system: (a) システム構成 (b) 装置写真

5.4.2　秘匿スマートフォン

次に、複数携帯端末間での通信をサポートする秘匿スマートフォンアプリケーションについて説明する。このアプリケーションでは、MPTP 通信をサポートする以外に、スマートフォンのような記憶容量が限られた端末を用いた通信、端末の認証、任意の二つのノードからの鍵供給の実現が技術課題である。それぞれの課題に対して、限られた記憶容量については、現代暗号を用いること、端末の認証については QKD ネットワークから供給された安全鍵を用いること、MPTP をサポートするために鍵リレーを用いることとした。図 5.4.3(a)にアプリケーションの概要を示す。Central session initiation protocol (SIP) サーバは呼制御と暗号化鍵配布の二つの役割を果たしている。安全な MPTP 通信を実現するために、通話セッションは AES 暗号化、量子鍵ネットワークから供給された鍵は端末認証と AES 暗号化鍵を SIP サーバから端末へ渡す際の One-time pad 暗号化に用いる。図 5.4.3(b)に示すような 5 ノードからなるネットワークにおいて、QKD ネットワークからスマートフォン、SIP サーバへの鍵供給と供給された鍵を用いたスマートフォンーサーバの認証、AES 鍵のスマートフォンーサーバの同期を確認した。また各スマートフォン間での e-mail 通信、信号落ちの無い明瞭な音声通信を確認した。

(a)



(b)

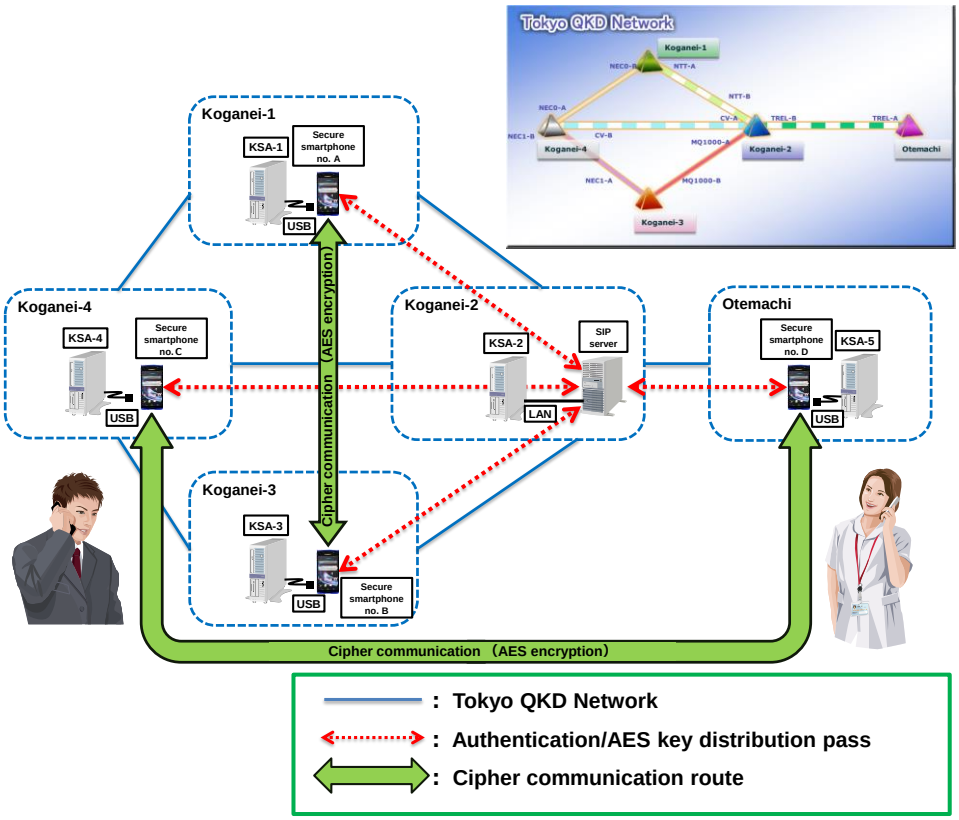


図 5.4.3 複数端末に対応した秘匿スマートフォンシステム: (a) 秘匿スマートフォンネットワーク, (b) デモシステム

６．まとめと展望

本論文では、量子セキュアネットワークの研究成果について述べた。まず、光子伝送から鍵抽出まで一気通貫のリアルタイム処理を行う量子鍵配送システムを考案し、さらに実使用環境での温度変動などの変動の影響を受けない安定化技術を開発し、商用光ファイバでの 14 日間連続リアルタイム量子鍵生成を世界で初めて達成した結果について述べた。これら成果により、それ以前は実験室でのフィジビリティスタディレベルだった量子鍵配送技術を、実フィールドファイバを用いた実使用環境下で使用可能なレベルまで引き上げることに成功した。さらにこのシステムを用いて 1:2 量子鍵生成・共有実験や異機種量子暗号システムの相互接続実験といった量子鍵配送ネットワークの初期検証を世界に先駆けて行った。

次に鍵生成速度の高速化に取り組み、独自の単一方向・偏波無依存型波長多重システム、高速光子検出技術、リアルタイム量子鍵抽出 H/W 技術を組み込んだ量子鍵配送システムを実現した。本システムを損失 13 dB のフィールド光ファイバ伝送路に接続し 30 日間連続運転に成功、世界最高レベルの鍵生成速度 100 kbps(8 波多重では 800 kbps)以上かつ低誤り率の誤り率 1.7%以下を達成した。また、システムを温度変動が大きい実使用環境設置し 21 週間の長期連続動作試験を達成したことについて述べた。これら成果により、システム設置条件のより厳しいサーバ室のような環境下においても、高速、低誤りかつ高信頼の鍵配送システムを実現することに成功した。

さらに、多様なアプリケーションへ量子鍵を配送する量子鍵配送ネットワークを実現するために、新たに量子鍵配送ネットワークアーキテクチャを提案し、提案したネットワークを Tokyo QKD ネットワークとして構築し、秘匿通信アプリケーション(QKD-AES Hybrid System、秘匿スマートフォン)を開発し Tokyo QKD ネットワークにおいて実証した。これら成果により、Point to point の量子鍵配送技術を、トポロジー、ノード数、規模の拡張性と可用性を有す鍵配送ネットワークにまで発展させることに成功した。

以上、これら研究成果により、従来暗号技術とは異なる安全性を持つ量子暗号の実現性から、実用性とその活用方法を示した。今後、潜在ユーザによる具体的な使用を想定した実証実験と並行して、現在議論されている実システムを実装した際の安全性について統一した指針とその評価方法が確立されること、相互接続性や利便性を向上させるアプリケーションインタフェースや鍵フォーマットの標準化を行っていくことで、本技術をベースとした秘匿通信ネットワークインフラストラクチャが実現されると考える。本技術を用いた秘匿通信ネットワークにより、情報通信ネットワークを利用するユーザは盗聴・解読などの危険から解放され通信の安全性が保証されたサービスを利用でき、ICT 社会がさらに発展し続けていくと信じる。

参考文献

[1] ITmedia NEWS ”誰が、なぜ？　史上最悪規模・ソニー個人情報流出事件を時系列順に整理,” URL: http://www.itmedia.co.jp/news/articles/1105/06/news052.html2011 (2011.5.).

[2] 日経ビジネス ONLINE “前代未聞　メガトン級の機密漏えい事件に迫る,” URL: http://business.nikkeibp.co.jp/article/world/20101215/217551/ (2919.12.).

[3] Luke Harding, “*The Snowden Files: The Inside Story of The World's Most Wanted Man,”* Vintage Books (2014.2.).

[4] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, “Photon level crosstalk between parallel fibers installed in urban area,” *Opt. Express,* Vol. **18,** No. 21, pp. 22199–207 (2010.10.).

[5] DATA ENCRYPTION STANDARD (DES), Federal Information Processing Standards Publication 46-2.

[6] ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197.

[7] 例えば KDDI 研究所, 九州大学ニュースリリース ”世界で誰にも解読されていない暗号問題を初めて解読！～スーパーコンピューターでも一万年以上かかる問題を、約 16 日間で解読に成功！～,” URL: http://www.kddi-research.jp/newsrelease/2016/071901.html (2016.7.).

[8] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public key distribution and coin tossing,” Proc. Int. Conf. Comput. Syst. Signal Processing, Bangalore, 1984, pp. 175–179.

[9] C. H. Bennett, “Quantum Cryptography Using Any Two Non-orthogonal States,” Phys. Rev. Lett., 68, pp. 3121-3124, 1992.

[10] C. E. Shannon, “Communication Theory of Secrecy Systems,” The Bell System Technical Journal, Vol. 28, Issue 4, pp. 656-715, (1949.10.).

[11] M. Peev and the SECOQC collaboration, “The SECOQC quantum key distribution network in Vienna,” New J. Phys. 11, 075001/1-37, (2009.7.).

[12] M. Sasaki and the Tokyo QKD Network collaboration, “Tokyo QKD Network and the evolution to Secure Photonic Network,” Proc. OSA/ CLEO 2011, JTuC1, (2011).

[13] Schneier on Security, “Switzerland Protects its Vote with Quantum Cryptography,” URL: https://www.schneier.com/blog/archives/2007/10/switzerland_pro.html (2007).

[14] IDQ, “Securing Your Data In Transit For The Long Term,“ URL: file:///C:/Users/0000010847283/Downloads/securing-your-data-in-transit-for-the-long-term-or-what-happens-when-rsa-encryption-is-finally-broken-by-mathematicians-or-quantum-computers.pdf (2014.10).

[15] 2010 FIFA World Cup South Africa ™, “Durban’s high tech stadium,” URL: http://www.fifa.com/worldcup/news/y=2010/m=5/news=durban-high-tech-stadium-1217593.html (2010.5.).
[16] W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication,” Phys. Rev. Lett. 91 057901 (2003).
[17] X.-B. Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography,” Phys. Rev. Lett. 94 230503 (2005).
[18] H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” Phys. Rev. Lett. 94 230504 (2005).
[19] C. H. Bennet, G. Brassard, C. Crepeau, and U. Maurer, “Generalized Privacy Amplification,” IEEE Trans. of Information Theory, vol. 41, No. 6, pp.1915-1923, (1995).
[20] P. D. Townsend, J. G. Rarity and P. R. Tapster, “Single Photon Interference in 10 km Long Optical Fibre Interferometer, “Electronics Letters. Vol. 29, No. 7, pp. 634-635, (1993.4.).
[21] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography with coherent states,” Phys. Rev. A 51, 1863, (1995.3.)
[22] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography,” Phys. Rev. Lett. 85, 1330, (2000.8.)
[23] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, “Quantum key distribution over 67 km with a plug and play sys-tem,” New J .of Physics, 4, 41.1-41.8, 2002.
[24] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura and K. Nakamura, “Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector,” Electron. Lett., Vol. 39, No. 16, pp. 1199–1201, 2003.
[25] G. Ribordy, J.-D. Gautier, H. Zbinden, and N. Gisin, “Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters,” Appl. Opt., Vol. 37, No. 12, pp. 2272–2277, 1998.
[26] A. Yoshizawa and H. Tsuchida, “A 1550 nm Single-Photon Detector Using a Thermoelecrically Cooled InGaAs Avalanche Photodiode,” Jpn. J. Appl. Phys. Vol. 40, Part 1, No. 1, pp. 200-201, (2001.1.).
[27] A. Tomita and K. Nakamura, “Balanced, gated-mode photon de-tector for quantum-bit discrimination at 1550 nm,” Opt. Lett. 27, pp. 1827–1829, (2002.10.).
[28] D. S. Bethune, W. P. Risk and G. W. Pabsta, “High-performance integrated single-photon detector for telecom wavelengths, “J. of Mod. Optics, Vol. 51, No. 9-10, pp. 1359 (2004).
[29] A. Yoshizawa, R. Kaji and H. Tsuchida, “10.5 km Fiber-Optic Quantum Key

Distribution at 1550 nm with a Key Rate of 45 kHz," Jpn. J. Appl. Phys. 43, No. 6A, pp. L735–L737, 2004.
[30] C. H. Bennet, F. Bessettem G. Brassard, L. Salvail and J. Smolin, "Experimental Quantum Cryptography," J. Cryptology, 5. pp. 3-28, (1992).
[31] P. D. Townsend, J. G. Rarity and P. R. Tapster, "Single Photon Interference in 10 km Long Optical Fibre Interferometer," Electronics Letters, Vol. 29, No. 7, pp. 634-635, (1993.4.).
[32] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N.Gisin, ""Plug and play" systems for quantum cryptography," Appl. Phys. Lett. 70 (1997) 793-795.
[33] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New Journal of Physics, No. 4, pp. 41.1–41.8, (2002.7.).
[34] T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "Field experiments of quantum cryptosystem in 96km installed fibers," CLEO/Europe-EQEC2005, EH3-4, Munich (2005).
[35] X.Mo, B.Zhu, Z.Han, Y.Gui, and G.Guo, "Faraday-Michelson system for quantum cryptography," Opt. Lett. Vol. 30, No. 19, pp. 2632-2634, (2005.10.).
[36] A. Tanaka, W. Maeda, A. Tajima, and S. Takahashi, "Fortnight quantum key generation field trial using QBER monitoring," The 18th Annual Meeting of Lasers and Electro-Optics Society (LEOS) 2005. pp. 557-558, Sydney, Australia (2005).
[37] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, and A. Tomita, "Practical Quantum Cryptosystem for Metro Area Applications," IEEE J. Selected Topics in Quantum Electronics 13 1031-1038, (2007.).
[38] T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, and K. Inoue, "Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors," Opt. Express 15 (2007) 13957-13964.
[39] S. Miki, M. Fujiwara, M. Sasaki, and Z. Wang, "NbN Superconducting Single-Photon Detectors Prepared on Single-Crystal MgO Substrates," IEEE Trans. Appl. Supercond. 17 (2007) 285.
[40] H. Takesue, S.-W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nature Photonics 1 (2007) 343-348.
[41] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," Quantum Information and Computation III, E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds., Proc. SPIE 5815, 138–149 (2005); arXiv:quant-ph/0503058v2.

[42] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, “High-rate quantum key distribution over 100 km using ultra-low-noise 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes,” Opt. Express 19(11), 10632–10639 (2011).
[43] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, “High speed single photon detection in the near infrared,” Appl. Phys. Lett. 91, 041114(2007).
[44] S. Takahashi, A. Tajima, and A. Tomita, “High-efficiency single photon detector combined with an ultra-small APD module and a self-training discriminator for high-speed quantum cryptosystems,” The13th Microoptics Conference, Takamatsu, Japan, PD-1 (2007) 2-3.This paper is now accessible at e-print arXiv: 0712.4179.
[45] Ken-ichiro Yoshino, Mikio Fujiwara, Akihiro Tanaka, Seigo Takahashi, Yoshihiro Nambu, Akihisa Tomita, Shigehito Miki, Taro Yamashita, Zhen Wang, Masahide Sasaki, and Akio Tajima, “High-speed wavelength-division multiplexing quantum key distribution system,” OPTICS LETTERS, Vol. 37, No. 2, pp. 223-–225 (2012).
[46] 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,” Optics Express Vol. 23, Issue 6, pp. 7583–7592, 2015.
[47] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima,. “Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days,”. Optics Express, Vol. 21, Issue 25, pp. 31395–31401, 2013.
[48] Tajima, Takashi Kondoh, Takao Ochi, Mikio Fujiwara, Ken-ichiro Yoshino, Hiromi Iizuka, Toshio Sakamoto, Akihisa Tomita, Ei Shimamura, Shione Asami and Masahide Sasaki, “Quantum key distribution network for multiple applications,” Quantum Science and Technology, vol. 2, 034003 (2017) .
[49] W. Maeda, A. Tajima, A. Tanaka, S. Takahashi, and T. Takeuchi, “High-speed QKD system synchronized by automatic phase-alignment mechanism,” Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC), 2005. OWI4, Anaheim, CA, USA (2005).
[50] R. J. Runser, T. E. Chapuran, P. Toliver, and M. S. Goodman, “Quantum Key Distribution for Reconfigurable Optical Network,” Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC), 2006. OFL1, Anaheim, CA, USA (2006).
[51] W. Maeda, A. Tanaka, S. Takahashi, and A. Tajima, “Automatic installation in QKD system using photon-counting optical power meter,” Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC) 2006, JThB21, Anaheim, CA, USA (2006).

[52] W.Maeda, A. Tanaka, A. Tajima, S. Takahashi, “Synchronization Technique in Quantum Key Distribution System,” IEICE Technical Report on Optical Communication Systems, vol. 105, no. 76, OCS2005-14, pp. 13-18 (2005.5).
[53] Synchronous Optical Network (SONET), The American National Standards Institute (ANSI), T1.105
[54] Synchronous Digital Hierarchy (SDH), The International Tele-communications Union (ITU), ITU-T G.707.
[55] 前田和佳子, 田中聡寛, 高橋成五, 田島章雄, ”量子暗号鍵配布システムにおけるフレーム同期技術,” 電子情報通信学会ソサイエティ大会, B-10-84 (2005).
[56] 田中聡寛, 前田和佳子, 田島章雄, 高橋成五, ”誤り率モニタを利用した量子暗号鍵配布システムの監視制御方法,” 電子情報通信学会ソサイエティ大会, B-10-85 (2005).
[57] A. Tanaka, A. Tomita, A. Tajima, T. Takeuchi, S. Takahashi, Y. Nambu, “Temperature Independent Q.K.D. System using Alternative-shifted Phase Modulation Method,” 30th European Conference on Optical Communication (ECOC), Tu4.5.3., Stockholm, Sweden (2004).
[58] A. Tomita, Y. Nambum A. Tajima, “Recent Progress in Quantum Key Transmission," NEC Journal of Advanced Technology, vol. 2, No. 1, pp. 84-91 (2005).
[59] N. Lutkenhaus, “Security against individual attacks for realistic quantum key distribution,” Phys. Rev., A61, pp. 052304 (2000).
[60] 高橋成五、田中聡寛、前田和佳子、田島章雄、竹内　剛、富田章久, “高速量子暗号通信システム用小型光子受信器,” 信学技報, vol. 105, no. 143, LQE2005-25, pp. 61-66 (2005.6).
[61] 田中聡寛、田島章雄、前田和佳子、高橋成五、竹内　剛, “高速量子暗号通信システムの開発(2) －バーストモードによる QKD－,” 電子情報通信学会総合大会, B-10-60, (2005)
[62] 田中聡寛、田島章雄、前田和佳子、高橋成五, “量子暗号鍵配布における光回路の温度無依存化、伝送路無依存化技術　～ 変調振幅一定制御及びバーストモード QKD ～,” 信学技報, vol. 105, no. 243, OCS2005-41, pp. 35-40 (2005.8).
[63] CompactPCI Overview, URL: https://www.picmg.org/openstandards/compactpci/
[64] 前田和佳子、田中聡寛、高橋成五、田島章雄, “光スイッチによる 1 対多量子暗号鍵配付ネットワーク,” 信学技報, vol. 106, no. 493, OCS2006-75, pp. 7-12 (2007.1).
[65] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, “Recent Progress in Quantum Key Distribution Network Technologies,” European Conference on Optical Communication (ECOC), Th2.6.2., Cannes, France (2006).
[66] 田島章雄、石塚裕一、萩原　学、田中聡寛、長谷川俊夫、今福健太郎、前田和佳子、西岡　毅、高橋成五、鶴丸豊広, “異機種量子暗号システムの相互接続実験,” 電子情報通信学会ソサイエティ大会, B-10-21, (2006)
[67] N. Namekata, S. Adachi, and S. Inoue, “1.5 GHz single-photon detection at

telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," Opt. Express 17 6275-6282 (2009).
[68] S. Miki, M. Fujiwara, M. Sasaki, and Z. Wang, "NbN Superconducting Single-Photon Detectors Prepared on Single-Crystal MgO Substrates," IEEE Trans. Appl. Supercond. 17 (2007) 285.
[69] Y. Nambu, K. Yoshino, and A. Tomita, "Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit," J. Mod. Optics 55, 1953-1970 (2008).
[70] K. Yoshino, A. Tanaka, Y. Nambu, A. Tajima, and A. Tomita, "Dual-mode Time-bin Coding for Quantum Key Distribution Using Dual-drive Mach-Zehnder Modulator," Technical Digest of ECOC2007, (Berlin, 2007)　paper 9.4.7.
[71] A. Tanaka, A. Tajima, A. Tomita, "Colourless Interferometric Technique for Large Capacity Quantum Key Distribution Systems by use of Wavelength Division Multiplexing," Technical Digest of ECOC2009, (Wien, 2009) paper 1.4.2.
[72] Akio Tajima, Akihiro Tanaka, Seigo Takahashi, Ken-ichiro Yoshino, and Yoshihiro Nambu, "High speed quantum key distribution system," IEICE Transactions on Fundamentals, Vol. E93-A, No. 5, pp. 889-896 (2010).
[73] S. Takahashi, A. Tajima, and A. Tomita, "High Efficiency Single Photon Detector Combined with an Ultra-small APD Module and a Self-training discriminator for high-speed quantum cryptosystems," 13th Microoptics Conference (MOC07), Post-deadline papers, PD-1, Takamatsu, Japan (2007).
[74] 田中聡寛、藤原幹生、富田章久、田島章雄, "量子鍵配送技術の高速化の為の鍵抽出高速化エンジンの開発," 信学技報, vol. 110, no. 392, OCS2010-103, pp. 25-30 (2012.1).
[75] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, and M. Sasaki, "Quantum Key Distribution Network for Multiple Applications," 16th Asian Quantum Information Science Conference (AQIS), pp. 229-230, Taipei, Taiwan (2016).
[76] Z. L. Yuan, A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," quant-ph/0501160 (2005).
[77] D. S. Bethune, W. P. Risk and G. W. Pabst, "A high-performance integrated single-photon detector for telecom wavelengths," J. of Mod. Optics, Vol. 51, No. 9-10, p.p. 1359 (2004).
[78] S. Takahashi, T. Takeuchi, A. Tajima, and A. Tomita, "An Ultra-compact Dual-APD Photon Receiver Module for Quantum Cryptosystem," Int. Symp. on Contemporary Photonic Technologies (CPT,) Tokyo, Japan, E-4 (2006).
[79] Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with

decoy method," Phys. Rev. A 76, 012329 (2007).
[80] M. Hayashi, "General theory for decoy-state quantum key distribution with an arbitrary number of intensities," New J. Phys. 9, 284 (2007).
[81] R. G. Gallager, “Low Density Parity-Check Codes,” MIT Press, Cambridge, MA (1963).
[82] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” Opt. Express, 16, pp. 11354–11360 (2008.July.).
[83] Advanced Telecom Computing Architecture,
URL: https://www.picmg.org/openstandards/advancedtca/
[84] NEC プレスリリース “NEC、「サイバーセキュリティ・ファクトリー」が本格稼働 ～ 官公庁や企業のサイバー攻撃対策向け支援を強化 ～,”
URL: http://jpn.nec.com/press/201406/20140616_01.html
[85] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection,” *Phys. Rev. A* **68** 042331 (2003).
[86] T. Sasaki, Y. Yamamoto, and M. Koashi, “Practical quantum key distribution protocol without monitoring signal disturbance,” Nature 509 475–78 (2014).
[87] M. Wegman, and L. Carter, “New Hash Functions And Their Use in Authentication And Set Equality,” J. of Computer and System Sciences 22 3 265-79 (1981).
[88] 回線暗号装置 COMCIPHER(AES)シリーズ,
URL: http://jpn.nec.com/access/prod/comcipher.html