差動位相シフト量子鍵配送（DPS-QKD）実験

NTT物性科学基礎研究所では，オリジナルな量子鍵配送方式である差動位相シフト量子鍵配送（DPS-QKD）の研究開発に取り組んでいます．本稿では，本方式の概要，原理実証実験，プロトタイプシステムの開発および2010年10月に行われた東京QKDネットワークにおけるフィールド実験を紹介します．

本庄（ほんじょう） 利守（としもり） /都倉（とくら） 康弘（やすひろ）

NTT物性科学基礎研究所

差動位相シフト量子鍵配送

近年，究極の暗号通信を実現する方式として，量子力学の原理を利用した量子暗号（量子鍵配送）に注目が集められています．差動位相シフト量子鍵配送（DPS-QKD: Differential Phase Shift-Quantum Key Distribution）[1] は，2003年にNTTとスタンフォード大学との共同で提案されたオリジナルな量子鍵配送方式で，微弱な光パルス列のパルス間の位相差情報が原理的に一部しか読み出せないことを利用しています．本方式のセットアップとプロトコルを**図1**に示します．

まず送信者であるアリスは，コヒーレントな光パルス列を用意し，各光パルス間の位相差を0もしくはπのランダムに位相変調し，強度を1パルス当り1光子未満に減衰させてから，受信者であるボブに送付します．ボブは1

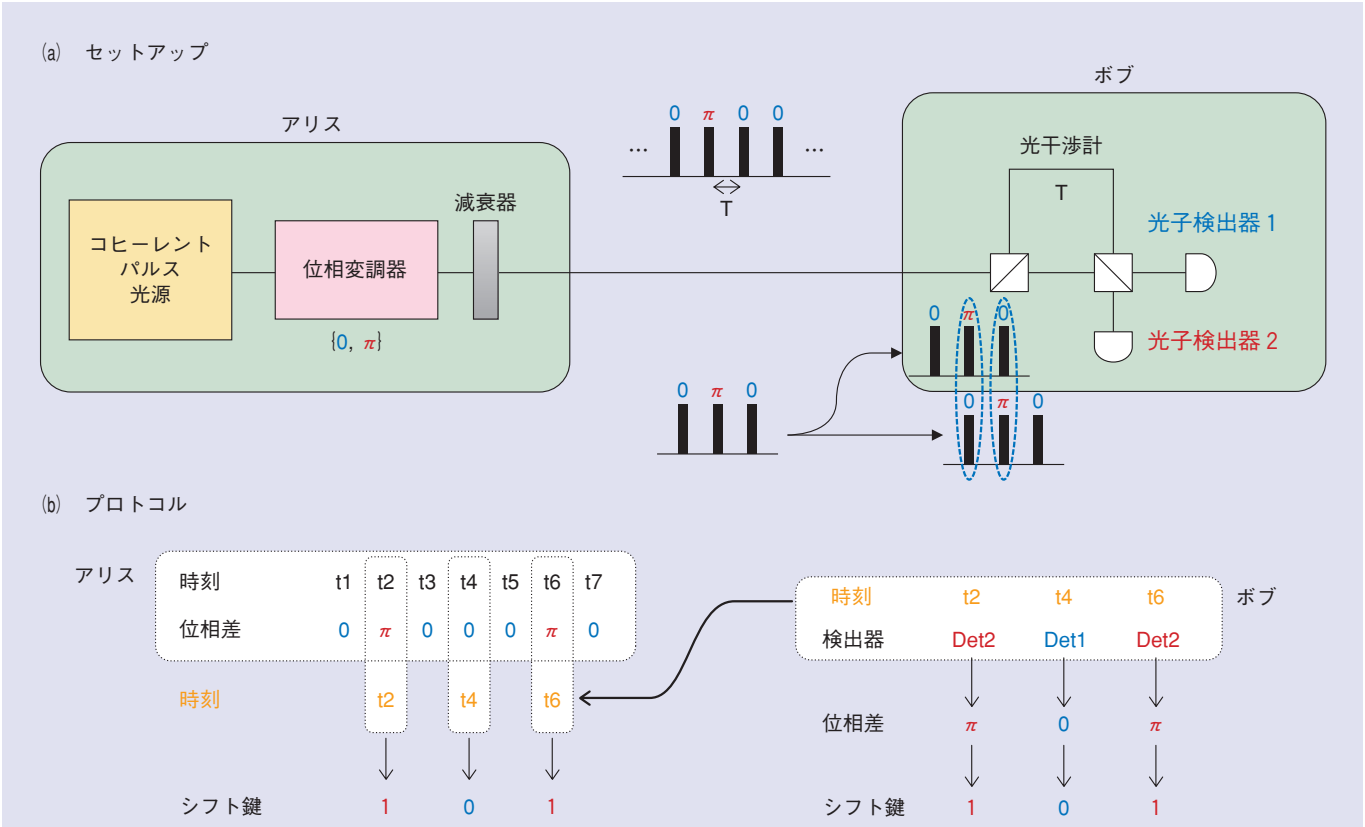

図1　DPS-QKD方式のセットアップとプロトコル

パルス遅延の干渉計を用いてパルスどうしを干渉させ，干渉計の出口に備えられた光子検出器からの出力により，パルス間の位相差の情報を読み出します．送出時点での光強度が弱いことから原理的に位相差情報の一部しか読み出せませんが，読めた個所に関しては，送信側の変調結果が反映されます．受信者であるボブは，光子が検出できた時刻（位相差の情報が読めた時刻）とどちらの検出器で検出されたかの情報（位相差の情報）を記録します．そして，位相差が0であった場合には，ビット0，位相差がπであった場合には，ビット1を割り当てることにより鍵を生成します．その後，検出できた時刻の情報のみをアリスに送り返します．アリスはこの情報と自ら位相変調した際の情報から鍵を生成します．この時点で生成された鍵をシフト鍵と呼びます．この後，エラー訂正および秘匿性増強と呼ばれる工程を経て，最終的に暗号通信で用いる安全鍵と呼ばれる鍵を生成します．

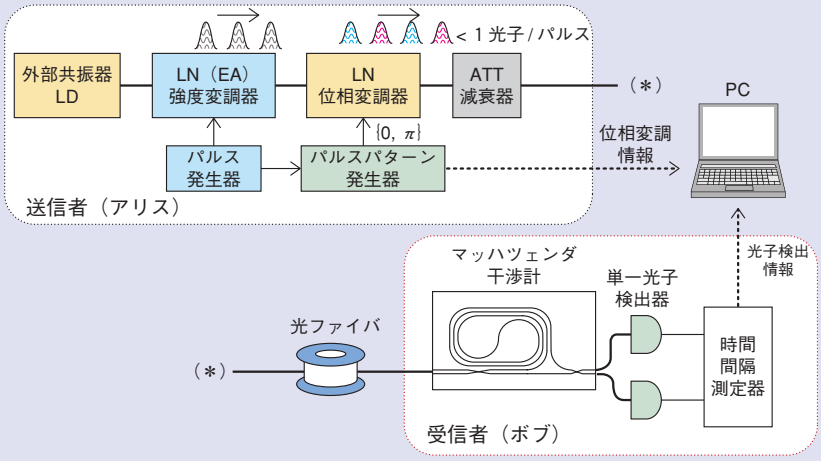

図2　DPS-QKD原理実証実験のセットアップ

原理実証実験

私たちはこれまでに本方式の原理実証実験を進めて，光ファイバ上での鍵配送距離および鍵配送速度を評価してきました．実験のセットアップを**図2**に示します．送信者であるアリス側では，レーザからの波長1 551 nmの光を，強度変調器で1 GHz繰り返しの光パルス列に変換し，パルスパターン発生器を用いて0もしくはπのランダムな位相変調を施します．そして，減衰器により，1パルス当り平均0.2光子まで減衰させてから，光ファイバに送出します．受信者であるボブ側では，アリスから送られてきた光パルス列を1パルス遅延の光干渉計に入れ，出力に設置された光子検出器により，光子を検出します．検出結果を時間間隔測定器により，光子の検出時刻と，どちらの検出器で検出したのかを記録します．この記録結果から前述のプロトコルにしたがってシフト鍵を生成し，鍵配送速度やエラーレートなどを評価します．

原理実証実験では，受信者であるボブ側の光干渉計の安定化と光子検出器の性能向上が課題となりました．そこで安定な光干渉を得るために，NTTで長年研究開発が進められてきた石英系ガラス導波路を用いた光集積回路であるプレーナ光波回路（PLC: Planar Lightwave Circuit）技術によるマッハツェンダ干渉計*を用いました[2]．本干渉計は通常の光通信で用いられるものに比べて光路差が10倍程度長く，安定化が難しいとされてきましたが，今回このPLCマッハツェンダ干渉計により，消光比20 dB以上（ビットエラーレート1 %以下に相当）を得ることに成功し，原理実証実験の実施につながりました．また光子検出器に関しては，その性能改善とともに，伝送可能距離を伸ばしてきました．2004年に，InGaAs（インジウムガリウムヒ素）のAPD（Avalanche Photo Diode）を用いた単一光子検出器を用いて，基本動作の実証実験に成功し，2006年には長波長帯の光子を短波長の光子に変換して，高効率高速なシリコンの単一光子検出器で検出する方式の採用により，100 kmの伝送に成功しました[3]．また，2007年には超伝導体を用いた単一光子検出器を用いて，200 km伝送実験に成功しました[4]．この実験では，繰り返し周波数を10 GHzまで上げることにも成功しました．

図1にあるプロトコルで説明したように本方式では大量の乱数列が必要となります．通常は計算機により生成された疑似乱数が用いられていますが，安全性向上のためには高速の物理乱数源が求められます．これについては最近，レーザ光のカオス的な揺らぎを用

＊マッハツェンダ干渉計：1つの光源から出た光を2つに分け，異なる経路を通過させた後，再び重ね合わせて干渉を起こさせる装置．

いた1 Gbit/sを超える生成レートを持つ乱数源が開発され[5]，これを用いたDPS-QKD実験も行いました．

プロトタイプシステム

これまでの原理実証実験によりDPS-QKDの実現性が見込めたことから，次のステップとしてプロトタイプシステムの開発に取り組みました．システムの外観を**図3**に示します．プロトタイプシステムの実装にあたり，新たにFPGA（Field Programmable Gate Array）を用いた高速信号発生およびその記憶装置を開発しました．これは送信者であるアリス側で位相変調のための信号発生およびその情報を鍵生成段階まで保持するためのハードウェアです．原理実証実験と同様に，アリス側ではレーザからの光を強度変調器により1 GHz繰り返しの光パルス列に変換し，FPGAボードからの位相変調信号を用いて，0もしくはπのランダムに位相変調を行います．そして減衰器により減衰させてから，ボブ側に送出します．ボブ側では，PLCマッハツェンダ干渉計と単一光子検出器を用いて位相差を測定します．光子検出器からの出力を時間間隔測定器により記録します．その情報をPCから連続的に読み出し，シフト鍵を生成します．同時に，アリス側に検出時刻の情報のみをネットワークを通じて送付します．アリス側ではその情報を基にFPGAボード上に蓄えられている位相変調の情報を読み出し，アリス側のシフト鍵を生成します．そして，それぞれで生成されたシフト鍵は，NECにより開発されたエラー訂正および秘匿性増強を行うハードウェア（鍵蒸留基板）に渡され，最終的に暗号通信で用いる安全鍵が生成されます．

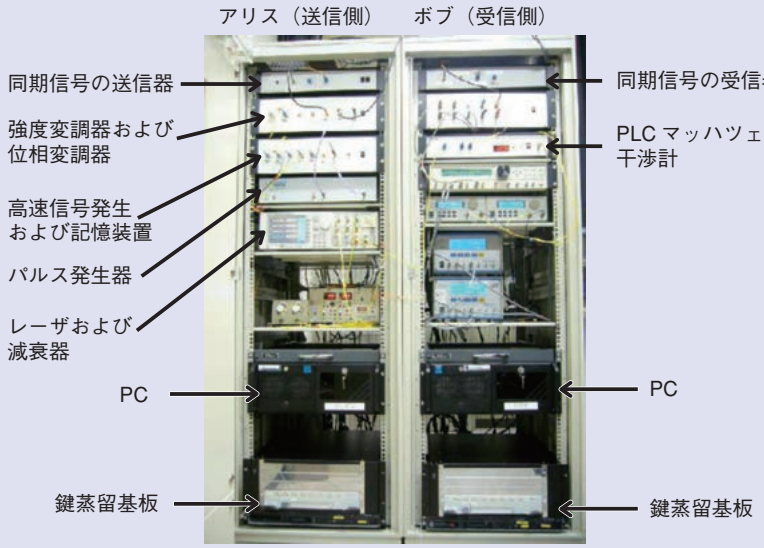

図3　DPS-QKDのプロトタイプシステム

フィールド実験

前述のプロトタイプシステムを用いて，私たちは㈱情報通信研究機構（NICT）主導による「東京QKDネットワーク」と呼ばれるテストベッドネットワーク実験に参加しました[6]．本実験には，NICTからの委託研究を受けているNEC，三菱電機，NTTに加えて，東芝，ヨーロッパの研究機関（Id Quantique，All Vienna）のチームが参加しました．本テストベッドネットワークは，NICTの保有するテストベッドネットワークJGN2plusの大手町，小金井，白山，本郷の各拠点間に敷設された光ファイバ上に構成されました．

伝送距離は大手町拠点を基点に，小金井拠点間約45 km，白山拠点間約12 kmおよび本郷拠点間約13 kmでした．小金井―大手町―白山区間には，複数の光ファイバが並走して敷設されており，さまざまな回線形態を構成しました．

今回の実験におけるネットワーク構成を**図4**に示します．下層はQKDレイヤと呼ばれ，各チームの装置がそれぞれ対向で配置され，6つのノードが形成されました．QKDにより生成された秘密鍵は，物理的に同じ場所に配置され，上位の鍵管理レイヤの鍵管理エージェントに吸い上げられます．そして鍵管理エージェントに保持された暗号鍵を用いて，TV電話や音声通信などの暗号化通信を行います．直接つながっていない拠点間の通信は，中間ノードで中継することにより，暗号通信を行うことができます．

NTTは，NICTと共同で本ネットワーク中の最長区間となる小金井―大手町間の往復90 kmの区間を担当しました．前述のプロトタイプシステムとNICT開発の超伝導単一光子検出器と組み合わせることにより，安定した鍵共有を実現しました．事前に行ったシフト鍵生成の安定性評価実験では，約8日間にわたり，安定したシフ

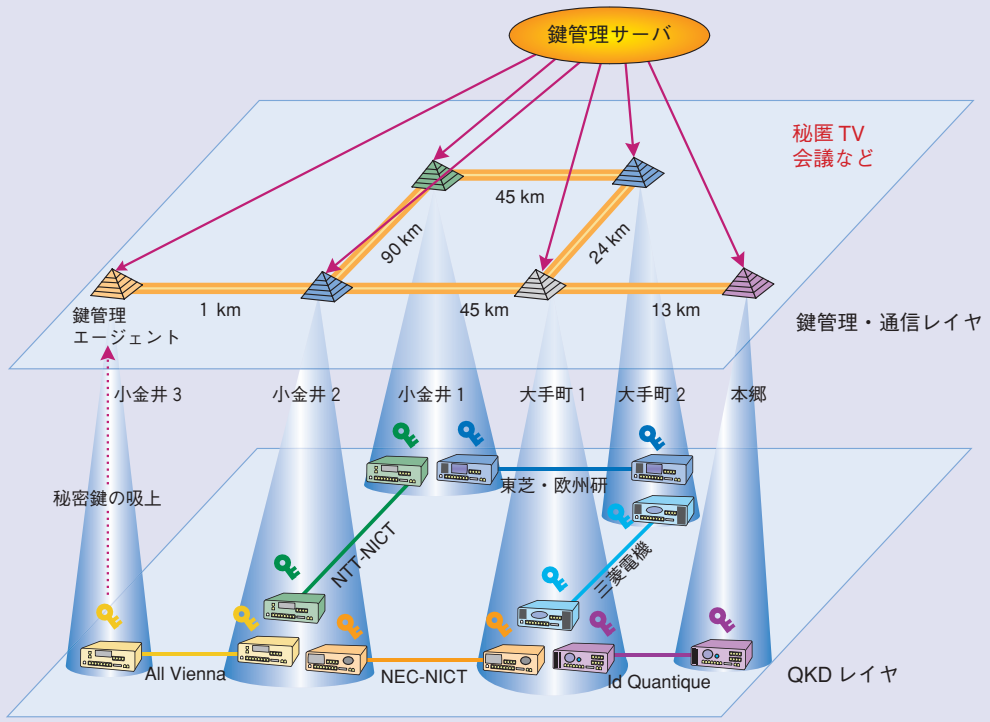

図 4　東京QKDネットワークの構成

ト鍵供給に成功しました．このときの平均鍵共有速度は18 kbit/sで，平均のビット誤り率は2.2 %でした．また，エラー訂正および秘匿性増強まで含めた安全鍵生成の安定性評価実験では，約 4 時間にわたり，安定した安全鍵供給に成功しました．このときの平均の安全鍵生成速度は，2.1 kbit/sでした．また，2010年10月に開催された国際会議UQCC（Updating Quantum Cryptography and Communications）2010[6] において，ライブデモンストレーションを行い，そこでは盗聴による盗聴検知およびその回避のための経路切替や，完全秘匿のTV会議などを行いました．

■参考文献

(1) K. Inoue, E. Waks, and Y. Yamamoto: “Differential-phase-shift quantum key distribution using coherent light,” Phys. Rev. A, Vol.68, No.2, 022317, 2003.

(2) 井上：“石英系プレーナ光波回路技術,” NTT技術ジャーナル, Vol.20, No.3, pp.58-62, 2008.

(3) E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto: “100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors,” Opt. Express, Vol. 14, No.26, pp.13073-13082, 2006.

(4) 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, pp.343-348, 2007.

(5) T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura: “Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers,” Opt. Express, Vol. 17, No.11, pp.9053-9061, 2009.

(6) http://www.uqcc2010.org/

（左から）都倉　康弘/ 本庄　利守

NTTではオリジナルな量子鍵配送方式であるDPS-QKDの研究開発を進めてきました．方式の提案および原理実証実験，プロトタイプシステムの開発，東京QKDネットワークにおけるフィールド実験を通じて，本方式のフィジビリティを示してきました．今後は，さらなる高性能化を目指して，研究開発を進めていきます．

◆問い合わせ先
NTT物性科学基礎研究所
量子光物性研究部
TEL　046-240-3340
FAX　046-270-2360
E-mail　tokura.yasuhiro@lab.ntt.co.jp