量子暗号通信で最長記録を達成

伝送距離100 km超の単一光子量子暗号システム

量子暗号は，どんな高性能計算機や装置を用いても，いかに巧妙なハッカーでも破ることのできない安全性を提供する，光ファイバ網上での通信手段です。その安全性は物理法則に由来するため，もっとも強力な暗号として知られています。

東芝欧州研究所では，標準光ファイバ上で世界で初めて伝送距離が100 kmを超す単一光子量子暗号システムの開発に成功しました。

量子暗号

量子暗号は，光ネットワーク上の二者間（通常アリスとボブと称する）で単一光子を用いて暗号鍵をやり取りする手法です。暗号鍵は，ユーザー間で秘密を保持したいデータやメッセージを暗号化するためのアルゴリズムとセットで用いられます。“ one-time pad ”と呼ばれるアルゴリズムを用いて，データの2値コードに単純に暗号鍵の2値情報を付加する暗号化手法を，**図1**に示します。情報の受け手は，暗号化されたデータに暗号鍵情報を付加することにより，元の情報を復元できます。“ one-time pad ”では暗号鍵が送信データと同じ長さでなければならないため，比較的短いメッセージのときにしか適用できませんが，量子暗号を“ one-time pad ”に適用すれば，少なくとも唯一絶対の安全性は保証することができます。一方，大きなデータの場合は，3DESやAESという対称暗号化手法を用いてデータを暗号化することができます。例えば，3DESでは112ビットの固定長の鍵を使用するので，一個の短い鍵で大量のデータを暗号化して送ることができます。

また，量子暗号では鍵の安全性をつどテストすることができます。第三者がハッキングによって鍵に関する情報を入手したとしても，量子力学の法則によって暗号鍵にエラーが発生するため，アリスとボブが鍵を比較して一定の割合で不一致が見つかれば，鍵が安全でなくなったことがわかります。ハッカーの存在がわかれば，別ルートで通信を行うか，単純に時間を置いて通信を再開するといった対策が立てられます。

システムの不完全性も共有鍵にエラーを引き起こすことがありますが，これは通常，誤り訂正ルーチンで取り除くことができます。システムの不完全性によって生じる鍵のエラーは，ハッカーによって生じるエラーと区別できません。しかし，エラー発生率があるしきい値（約15 %）以下であれば，“ プライバシー増幅処理 ”と呼ばれる盗聴の疑いのある暗号部分を排除して鍵を形成する方法が適用でき，これにより鍵の安全性は保証されます。

量子暗号プロトタイプシステム

われわれのシステムでは，**図2**に示すようにビット情報をマッハ－ツェンダー干渉計における位相遅れとして単一光子を符号化しています。発生源から検出器まで通過する光子は，アリス側の短い経路とボブ側の長い経路を通るか，あるいはアリス側の長い経路とボブ側の短い経路を通ります。二つの経路の長さは，アリス側設定で可変遅延ラインを用いてマッチングをとり，ボブ側の長経路に設置されたファイバ伸張器により微調整されます。

2 MHzで動作する1.55 μm帯DFBパルスレーザダイオードで80 ps幅の光パルスを生成した後，光強度を強く減衰させると，クロックサイクル当たり平均0.1個の光子を生成できます。ビット情報は二つの干渉ルートの位相変調器により光子に符号化されます。符号化された光子信号は，タイミング用1.3 μm帯クロックレーザから放出されるパルスに多重化され，光ファイバに送られます。また単一光子検出器として，InGaAsアバランシェダイオード（APD）と独自設計の駆動回路が使用されています。この検出器では，1.55 μmでの検出効率が約12 %のときに，典型的なダークカウントの確率は1 ns当たり10^{-7}です。これを使うと雑音等価パワーが$1.1\times10^{-17}\,WHz^{-1/2}$となり，今回の動作温度−100 ℃では現在報告されている中でもっとも低い値です。

システムは，双方の位相変調器の位相遅れを0 ℃に設定したとき，ボブ側検出器による光子数カウントが最小になるよう初期化されます。各クロックサイクルの間で，アリスとボブは，それぞれの位相変調器をランダムに0 ℃又は90 ℃にセットします。アリス側では0 ℃にbit＝0，90 ℃にbit＝1を，反対にボブ側では90 ℃にbit＝0，0 ℃にbit＝1を割り当てます。ボブとアリスが同じビットの値を（したがって異なる位相角を）セットしたときだけ，干渉による弱め合いが回避され，ボブ側検出器に光子が記録されます。光子検出時間に関する情報を共有することで，双方は二つのランダムビット列から共有鍵を取り出すことができます。

図3，**図4**にそれぞれ量子ビットエラー率（QBER）とビットレートの実測値を示します。ファイバ長が増大するにつれて，ビットレートは0.20 dB/kmの割合で減少しますが（図4），この値は標準の通信用シングルモードファイバにおける標準値とほぼ同じです。ファイバ長が101 kmであっても，数十秒で数百ビットの暗号鍵を転送するのに十分なビットレートがあります。ファイバ長が50 kmあたりまでは，QBERは約3.6 %程度の一定値を示します。この程度の距離までは，QBERは位相変調エラーに起因すると考えられます。一方，50 kmを超えると，QBERはファイバ長とともに増大しますが，これは検出器のダークカウント及び漏れ光に起因するカウントミスによるものです。図4の実線は変調エラーとカウントミス双方を含む理論計算結果を表しますが，実験値と良い一致を示すのがわかります。101 kmで2分の鍵転送に対する平均QBERは7.1 %ですが，これは15 %の上限値を下回っているため，誤り訂正とプライバシー増幅処理が可能であり，したがって鍵の安全性を保証することができます。

将来展望

得られたデータから，現在のシステムでは最高130 kmの光ファイバまで安全な鍵（QBER＜15 %）を送付できることがわかります。変調エラーを除去し，クロックレーザ光の信号チャネルへの漏れを改良し，より効率の高い量子暗号プロトコルを採用することで，システムの到達距離は174 kmまで延長可能です。しかし，これ以上距離を伸ばすには，受信側装置や単一光子検出技術の改善が必要です。将来的には，現在開発中の量子中継器の技術が，任意の光ファイバ長の鍵配布を可能にするでしょう。

A. J. シールズ
東芝欧州研究所　ケンブリッジ研究所グループ長
Z. L. ユアン
東芝欧州研究所　ケンブリッジ研究所
和訳：加藤　理一
東芝欧州研究所　ケンブリッジ研究所副所長

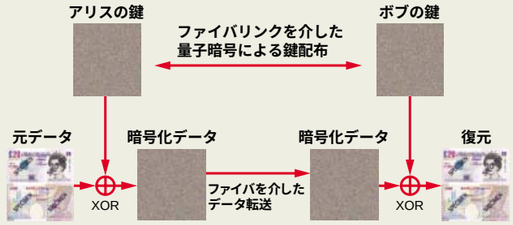

図1．“ one-time pad ”を量子暗号に使用した暗号通信の例 ― 量子暗号は，光ファイバにより結ばれたアリスとボブ間で暗号鍵を配布するために使用されます。アリスは図に鍵のコピーを排他的論理和（XOR）にて付加して暗号化し，通常の光通信ファイバにより送信します。ボブは受信データに暗号鍵のコピーを付加（XOR）すると元の図が復元されます。

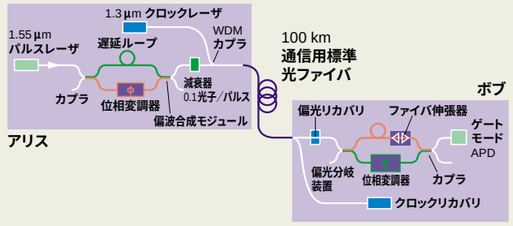

図2．量子鍵配布システムの概念 ― システムは本質的にはマッハ－ツェンダー干渉計です。干渉計は位相変調器と遅延ループにより構成され，検出器はゲートモードAPDと駆動回路から構成されます。

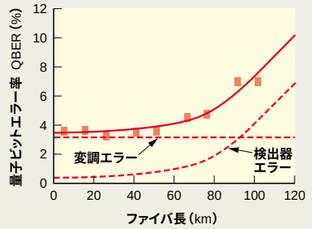

図3．ファイバ長の関数として測定されたQBER ― ■は実測値，破線は変調エラーと検出器エラーの寄与の理論計算結果，実線は両理論値の和を表します。

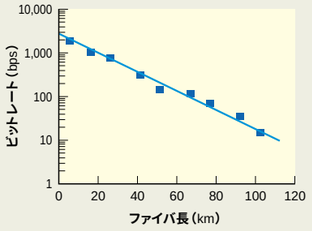

図4．異なる光ファイバ長に対するビット生成率 ― ■は実測値，実線は理論計算結果を表します。