世界最速の光ファイバー量子暗号通信

究極的な安全を保障する暗号通信技術の実用化に向けて

産総研光技術研究部門では高速動作時に発生する雑音を効果的に抑える独自の光子検出法を考案し、光ファイバー通信波長1550nm帯で動作周波数10MHzの光子検出装置を開発した。この光子検出装置を用いて光ファイバー長10.5kmでの量子暗号通信による鍵配布実験で世界最高となる鍵生成率45kビット/秒を達成した。

量子暗号通信を利用すれば原理的に盗聴・解読が不可能な究極の暗号通信を実現することができる。但し、量子暗号通信は光子1個につき1ビットの情報を載せて多数の光子を送ることで鍵配布を行うため、鍵生成率の高い量子暗号通信には光子検出装置の高速化が必要不可欠である。

究極の暗号通信における量子暗号の役割

専用回線を利用した政府間の外交等の機密文書の暗号通信に限らず、インターネットなどの情報ネットワークでも文書（平文）を第三者に盗聴されないように暗号が利用されている。暗号化と復号化には鍵が必要である。このとき、鍵を知らない盗聴者が暗号文を解読しようとしても現在の技術水準では解読に莫大な時間を要するため、事実上、暗号は解読不可能であるとみなされている。但し、コンピュータの性能は年々上昇しその安全性は永遠ではない。さらに、効率良く暗号を解読する方法が発見される恐れもある。これは計算量的困難さを安全の根拠にしている現代暗号の宿命と言える。唯一の例外がVernam暗号である。これは平文と同じ長さの秘密鍵を一度で使い捨てるもので、絶対安全性が保障されているが、平文と同じ長さの秘密鍵を常に用意する必要がある。量子暗号通信はこの秘密鍵を安全に効率よく配布する技術として期待されている。量子暗号通信は光子1個につき1ビットの情報を載せて多数の光子を送ることで鍵配布を行うが、盗聴を検知できる点に特徴がある。間違って1ビットに対して2個以上の光子を送ると、盗聴者は1個を盗ってビット値を測定し、残りを受信者に送ることで検知を回避できる。但し、光子は分割できないので1ビットにつき確実に1個なら盗聴は必ず検知できる。また、コピーを保管するために盗聴者がオリジナルのコピーを作るとその痕跡が残る。実は、盗聴者が伝送中の光子に触れるだけで痕跡が残る。従って、何をやっても盗聴が発覚するため盗聴がうまくいかないという意味で量子暗号通信は究極的な安全性を保障する。図1に暗号通信の模式図を示す。手順は以下の通りである。

1) 量子暗号通信で平文と同じ長さの秘密鍵を送受信者間で共有する。
2) 盗聴の有無を確認。盗聴を検知すれば量子暗号通信をやり直す。盗聴を検知しなければ送信者側でVernam暗号による暗号化を行う。
3) Vernam暗号による暗号文はインターネットなどの情報ネットワーク経由で受信者側に届く。
4) 受信者側は共有している秘密鍵で復号化する。
5) 安全のため使用済みの秘密鍵を廃棄する。

量子暗号通信では盗聴を検知されてしまうので盗聴者は秘密鍵を知ることはできない。そこで、盗聴者はインターネット上を流れる暗号文を入手することになるが、平文と同じ長さの秘密鍵で暗号化すれば、鍵を知らない限り絶対に暗号解読できないことが、情報理

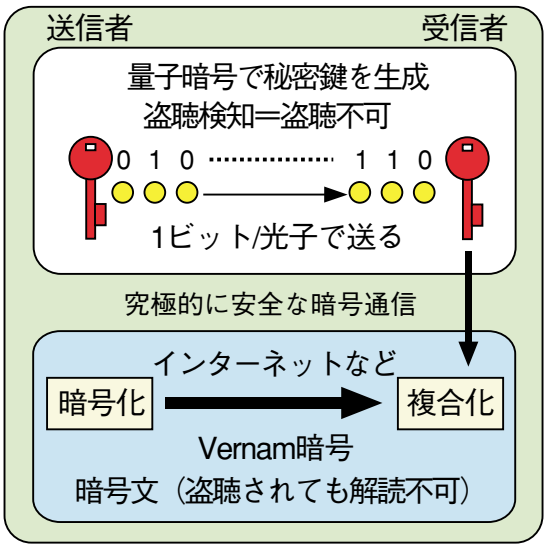


図1　暗号通信の模式図。Vernam暗号の秘密鍵配布の手段として量子暗号通信が利用される。

論上、証明されている。但し、現代暗号（例えば、共通鍵暗号）は秘密鍵が平文より圧倒的に短く、複雑な計算アルゴリズムを利用して鍵を拡張している。この場合、永遠の安全性は保障されない。量子暗号通信は計算アルゴリズムを利用せず、平文と同じ長さの秘密鍵を生成するための手段である。但し、使用済みの秘密鍵を再利用すると安全性が低下するので、常に新しい秘密鍵を生成し続けなければならない。従って、鍵生成率の高い量子暗号通信が望ましい。量子暗号通信とVernam暗号を併用することで究極的に安全な暗号技術が完成する。

光子検出装置の課題

波長1550nm帯は光ファイバーの伝送損失が最低となるため、量子暗号通信の長距離化に適している。但し、通常、0.2 dB/km 程度の伝送損失がある。このとき、100km伝送した場合の伝送損失は20dBであるから、99%の光子は受信側に到着せず、鍵生成率は10ビット/秒前後と極めて低いのが現状である。これに対し、量子暗号通信を用いない現代暗号では鍵生成率が100Mビット/秒前後であるが、この場合、平文と同じ長さの秘密鍵が生成されても永遠の安全性は期待できない。このため、量子暗号通信の鍵生成率を改善することが究極的な安全性を保障する暗号技術の開発に必要不可欠と考えられる。しかし、光ファイバーの伝送損失はレイリー散乱と赤外吸収によるものであり、石英ガラスを使用する限り0.14dB/km程度が限界である。従って、将来、最高品質の光ファイバーが商用化されたとしても、100km伝送した場合の伝送損失は14dB程度にしかならない。伝送損失が20dBから14dBに改善されても、鍵生成率の改善は4倍にとどまる。そこで、隣り合う光子の間隔をできるだけ狭くして、短時間に多数の光子を伝送・検出する必要がある。間隔を1/10にできれば鍵生成率は10倍改善するが、10倍速く動作する光子検出装置が必要になる。光子検出装置の高速化は量子暗号通信の鍵生成率を改善するために重要な課題である。

検出器の高速化による鍵生成率の改善

波長1550nm帯光子一個一個を検出できる高感度のアバランシェフォトダイオードを受光素子とする光子検出装置では、これまでガイガーモードと呼ばれるなだれ電流増幅を利用した光子検出法が用いられていた。しかしながら、なだれ電流を増幅するとアフターパルスと呼ばれる雑音が動作周波数1MHz付近で急激に増加するため、1MHzを超えるような繰り返し動作は困難であった。産総研では、光子検出過程でなだれ電流増幅を必要としない新しい光子検出法を開発し、アフターパルス発生を大幅に抑えることに成功した。この結果、動作周波数10MHzという光子検出装置を実現した。図2に電気回路を示す。アフターパルスの発生はなだれの規模に比例するため、アバランシェフォトダイオード印加電圧をガイガーモードより低めに設定する。図2左上にアバランシェフォトダイオードの等価回路を示すが、アバランシェフォトダイオードは光子を検出しない場合、コンデンサーとして機能する。光

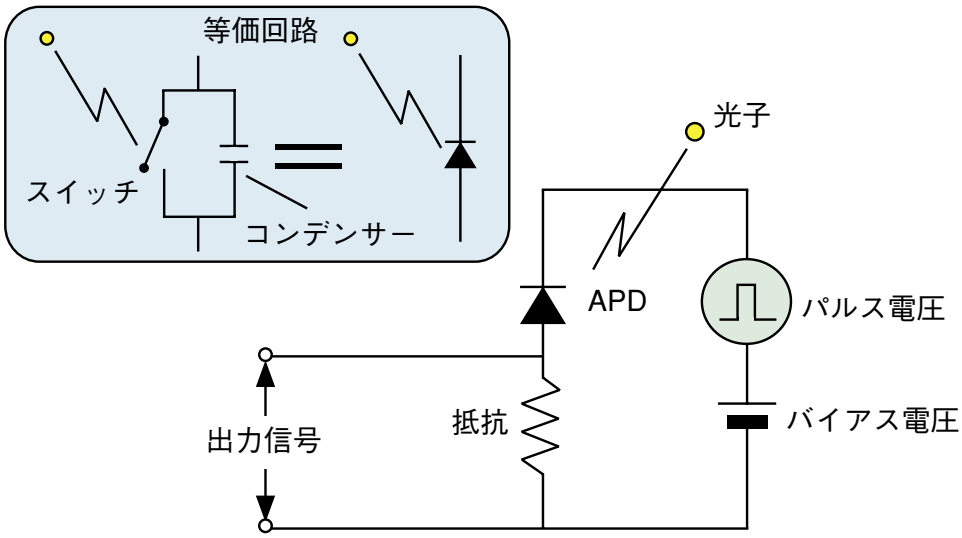


図2　光子検出装置の電気回路とアバランシェフォトダイオード（APD）の等価回路

子吸収があるとスイッチが閉じられコンデンサーとして機能が失われるので、コンデンサーとしての機能を判定することで光子を検出できる。この光子検出過程では電流増幅の必要性を排除するのでアフターパルス雑音を抑圧できる。この結果、動作周波数を10MHzまで改善することに成功した。手順は以下の通りである。

1) 降伏電圧よりわずかに小さな直流バイアス電圧をアバランシェフォトダイオードに印加する。
2) 電圧パルスを重畳して降伏電圧よりわずかに大きな電圧をアバランシェフォトダイオードに印加する。アバランシェフォトダイオードはコンデンサーとして電圧パルスの立ち上がり時に充電され、正の電圧パルスが抵抗両端に発生する。
3) 光子吸収によりコンデンサーとしての機能が失われる。もしくは、光子検出が無くコンデンサーとしての機能を維持する。
4) アバランシェフォトダイオードがコンデンサーとして機能していれば電圧パルスの立ち下がり時に放電し、負の電圧パルスが抵抗両端に発生する。コンデンサーとしての機能が失われていると負の電圧パルスは発生しない。
5) 放電パルス（負の電圧パルス）の有無で光子検出を判定する。
6) 電圧パルスの印加が終了し、スイッチが開放される。手順1の状態に戻る。

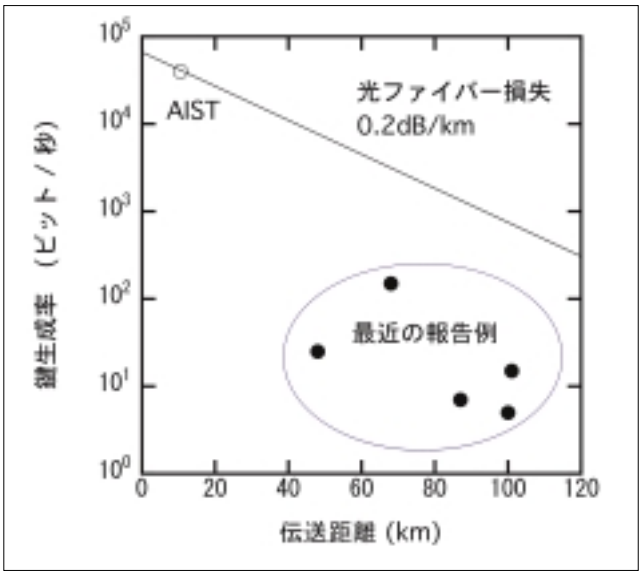
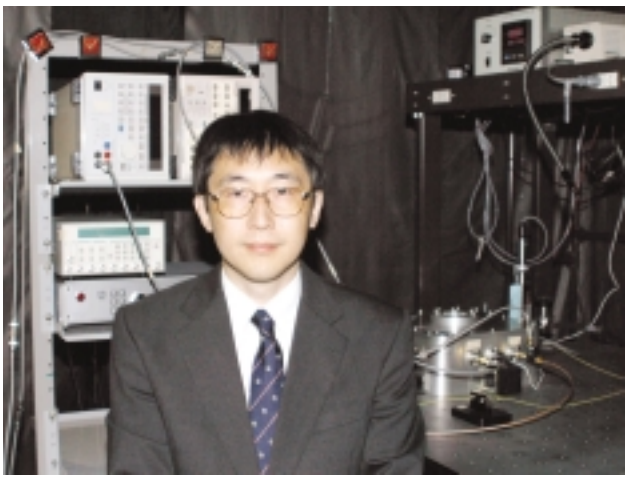


図３　量子暗号通信の伝送距離と鍵生成率
最近報告された他研究機関の量子暗号通信の伝送距離と鍵生成率のデータ（●）と産総研のデータ（○）。単純な比較はできないが、仮に、光ファイバーの伝送損失を0.2dB/kmとすれば、産総研の成果を利用することで実線のような関係が期待できるため、従来の鍵生成率に100倍程度の改善が見込まれる。



光技術研究部門　情報通信フォトニクスグループ
主任研究員　吉澤　明男

手順1から6を繰り返して周期的に光子検出を行う。図2に示した電気回路はガイガーモードと同一である。つまり、従来のガイガーモードで用いられてきた電気回路を変更することなく、なだれ電流増幅を抑えるためにアバランシェフォトダイオードに印加するバイアス電圧をガイガーモードより低めに設定するだけで高速繰り返し動作が可能になることが光子検出法の特徴である。この光子検出装置を利用してB92と呼ばれる鍵配布プロトコルの量子暗号通信を行った結果、光ファイバー長10.5kmに対して現時点で世界最速となる鍵生成率45kビット／秒を達成した。図3の「○」が、今回の研究成果である。

今後の技術展望

今回の実験では光ファイバー長が短く、今後、これを100km程度に延長し、10MHz以上で動作する光子検出装置を開発する予定である。単純な比較はできないが、仮に、光ファイバーの伝送損失を0.2 dB/kmとすれば、産総研の光子検出装置を使用することで図3の実線で示した実線のような関係が期待できるため、鍵生成率に100倍程度の改善が見込まれる。

◆関連情報
・プレス発表，平成16年5月12日: http://www.aist.go.jp/aist_j/press_release/pr2004/pr20040512/pr20040512.html

●問い合わせ
独立行政法人 産業技術総合研究所
光技術研究部門
情報通信フォトニクスグループ　主任研究員　吉澤　明男
E-mail : yoshizawa-akio@aist.go.jp
〒305-8568
茨城県つくば市梅園 1-1-1 中央第２