差動位相シフト量子デジタル署名の提案

Differential Phase Shift Quantum Digital Signature

阪大工[1]，NTT 物性基礎研[2]　○井上　恭[1]，本庄　利守[2]

Osaka Univ.[1], NTT Basic Research Lab.[2], ○Kyo Inoue[1], Toshimori Honjo[2]

E-mail: kyo@comm.eng.osaka-u.ac.jp

[まえがき] デジタル署名は送信データが正規のものであることを証明する技術であり、そのために送信者は認証鍵を予め公開しておき、データ送信時に署名鍵を添付する。署名鍵と認証鍵が整合していれば正規のデータと認定される。このシステムでは、認証鍵からは署名鍵が偽造されないことが要となる。この機能を量子力学的に実現するのが量子デジタル署名（QDS）である。これまでいくつかの QDS 方式が提案されているが、実装性や操作性に課題があった。本発表では、従来よりも装置構成・鍵配布手順が簡便な、差動位相シフト（DPS）QDS を提案する。

[プロトコル] Fig. 1 に提案方式のシステム構成を示す。説明のため、送信者 1 名、受信者 2 名の 3 者構成としている。送信者は{0, π}で位相変調されたコヒーレントパルス列を平均光子数 1 未満/パルスとして同報送信する。受信者はこれを遅延マッハツェンダ干渉計(MZI)を通して光子検出受信し、光子検出時間スロットと検出器を記録する。そして、その一部をテストビットとして、送信者と照合してビット誤り率（BER）を見積もり、さらに受信間でビット照合し、残りを認証鍵とする。一方、送信者はテストビットパルスを除いた全送信パルスの位相値を署名鍵とする。データ受信時には、受信者は添付された署名鍵から認証鍵ビットに対応するビットを抽出・照合し、署名鍵の真偽を判定する。

生成した鍵の安全性は、微弱コヒーレントパルス列を用いていることにより保障される。この場合、光子検出は稀かつランダムなので、受信者の認証鍵は送信者及び他の受信者も含めて外部には分からない。また、送信パルスの全ては測定できないので、署名鍵の偽造も不可である。

[システムパラメータ] 受信者は、認証鍵と署名鍵の照合の際に、システム BER 及び部分盗聴から作成された偽造署名鍵である可能性を考慮して閾値 s_a を設け、不整合率が s_a 以下であれば正規のものと判断する。この s_a は、正規鍵が否認される確率 P_{ha} 及び偽造鍵が承認される確率 P_f が、無視できるほどに十分小さいように設定される。Fig. 2 は、[文献]の実験パラメータ及び連続インターセプト・リセンド攻撃[2]を想定して計算した、P_{ha} 及び P_f の上限が 10^{-4} となる s_a である（伝送距離 100km）。色付け領域のパラメータ値、例えば｛認証鍵長＝200、閾値＝0.175｝、とすれば QDS として機能する。

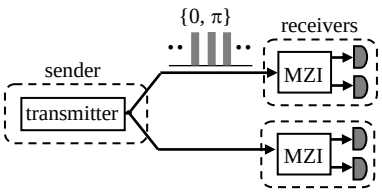

Fig. 1. System setup.

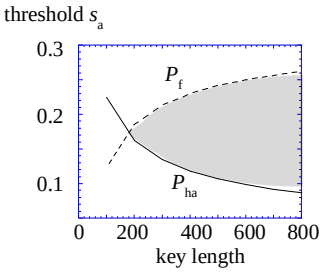

Fig. 2. Authentication threshold.

[1] R. Collins 他, Sci. Rep. **7**, 3235 (2017). [2] T. Tsurumaru, PRA **75**, 062319 (2007).