Cwiczenia5-jawne

13 marca 2011
21:45

1 Analiza bezpieczeństwa dla realistycznych modeli

Wysyłamy impulsy laserowe o średniej liczbie fotonów $\bar{n}_0$ z częstotliwością R_0, przez światłowód o długości L i współczynniku tłumienia α. Wydajność detektorów η a ciemne zliczenia S.

Czy kwantowych jest bezpieczna ?
(czy da się uzyskać bezpieczny kanał)

Przyjmujemy filozoficznie że wszystkie błędy pochodzą od podsłuchiwacza, nawet jeśli wiemy że są spowodowane niedoskonałością naszych urządzeń.

A & B mierzą QBER, oraz R - liczbę zarejestrowanych przez B sygnałów na sekundę.

Impuls dociera do B ma średnią liczbę fotonów $\bar{n} = \bar{n}_0 \, 10^{-\alpha \cdot L}$, po uwzględnieniu wydajności detektora $\bar{n}_d = \bar{n} \cdot \eta$

prawdop. że wysłany impuls spowoduje zliczenie u B:

$$P_{A \to B} = \left(1 - e^{-\bar{n}_d}\right) \approx \bar{n}_d = \bar{n}_0 \, \eta \cdot 10^{-\alpha \cdot L}$$

Czyli B będzie dostawał impulsy $R_0 \bar{n} \eta$ na sekundę

Ale pamiętamy, że B nie tylko ciemne zliczenia nawet gdy nic nie dotrze od A ani nikt coś

zarejestrowanie 2 $p_{dark} = \frac{\delta}{R_0}$

więc prawdop. kliknięcia w B

$p_{click} = p_{A \to B} + p_{dark} - \underbrace{p_{A\to B} \cdot p_{dark}}_{\text{to znacznie mniejsze pomijam}} \approx$

$\approx \quad \bar{n}_d \cdot \quad + \frac{\delta}{R_0}$

czyli $R = R_0 p_{click} \approx R_0 \cdot \bar{n}_0 \cdot 10^{-\alpha \cdot l} \cdot \eta + \delta$

Jeśli będzie poziom błędów w B. Przyjmijmy że światłowód nie wprowadza istotnych błędów i główne źródło błędów to ciemne zliczenia

$QBER = \frac{1}{2}\frac{\delta}{R}$ $\qquad QBER = \frac{\frac{1}{2} p_{dark}}{p_{click}} = \frac{\frac{1}{2}\frac{\delta}{R_0}}{\frac{R}{R_0}} = \frac{1}{2}\frac{\delta}{R}$

½ połowa ciemnych zliczeń da błędny bit.

Atak E

Przede wszystkim E może wykorzystać impulsy wielofotonowe: Jeśli $n > 1$, E zachowuje sobie 1 foton, pozostałe puszcza dalej do B, czeka na ogłoszenie baz przez A i B i może w dobrej bazie poznając bezbłędnie bit.

Co więcej może puścić pozostałe fotony swoim bezstratnym światłowodem do B, i może się okazać, że A i B nawet nie zauważą w związku z tym spadku R.

(Photon Number Splitting attack – PNS)

Prawdopodobieństwo że A wyśle impuls wielofotonowy

Prawdopodobieństwo że A wyśle impuls wielofotonowy

$p_{m\geq 2} \approx \frac{\tilde{\mu}_0^2}{2}$

- jeśli $p_{m\geq 2} \geq p_{click}$, E może postępować następująco:
  - robić PNS na stanach wielofotonowych i podstawić B pozostałe fotony, z
    (robi to na części $\frac{p_{click}}{p_{m\geq 2}}$ impulsów wielofotonowych a pozostałe blokuje)
  - blokować wszystkie sygnały jednofotonowe

w ten sposób E nie wzbudza żadnego QBER

- jeśli $p_{m\geq 2} < p_{click}$, E robi PNS na wszystkich wielofotonowych i podstawia B ale to za mało. Musi do B puścić też trochę stanów jednofotonowych. i na tych fotonach wykonuje atak np. intercept & resend na x-tej części fotonów w bazie $\oplus$ v $\otimes$. (lub częściej)

.... ciąg dalszy zdarzeń dowodu.