

# Informacja Kwantowa 1/2

## Seria 5

do oddania 05.04.2013

Rozważmy realistyczny model kwantowej dystrybucji klucza opartej o protokół BB84.  $A$  wysyła słabe impulsy laserowe o statystyce Poissonowskiej ze średnią liczbą fotonów na impuls:  $\bar{n}_0 = 0.01$ , z częstotliwością repetycji  $R_0 = 1\text{Ghz}$  przez światłowód o współczynniku tłumienia  $\alpha = 0.2\text{dB/km}$ .  $B$  do rejestracji impulsów używa detektorów o wydajności  $\eta = 10\%$  i częstotliwości ciemnych zliczeń  $\delta = 100\text{Hz}$ . Przyjmujemy, że jedynym źródłem błędów w uzyskanym przez  $A$  i  $B$  ciągu bitów są ciemne zliczenia.

Rozważ, atak podsłuchiacza oparty o tzw. photon number splitting attack (PNS), w którym podsłuchiacz: (i) sprawdza ile fotonów  $n_0$  zostało wysłane przez  $A$  (robi to tuż za laboratorium  $A$ ). (ii) Jeśli  $n_0 \geq 2$  to  $E$  zostawia sobie jeden foton i przechowuje go do momentu ujawnienia bazy, a pozostałe fotony jeśli chce, przesyła do  $B$ , przy czym przesyła je swoim idealnym bezstratnym światłowodem. (iii) Jeśli  $n_0 = 1$ ,  $E$  może impuls po prostu zablokować i nie przesyłać nic do  $B$ , puścić go swoim bezstratnym światłowodem do  $B$ , albo wykonać na tym fotonie intercept-resend attack używając, przypadkowo bazy  $\{| \leftrightarrow \rangle, | \updownarrow \rangle\}$  lub  $\{| \nearrow \rangle, | \searrow \rangle\}$  i taki foton po ataku również przesyła swoim bezstratnym światłowodem.

Celem zadania jest poszukiwanie optymalnego ataku podsłuchiacza, który prowadzi do obserwowanych przez  $B$  liczbę rejestrowanych zdarzeń na sekundę  $R$ , oraz obserwowanego przez  $A$  i  $B$  QBER (oczywiście jeśli podsłuchiacz może zdobyć maksymalną informację wprowadzając niższy QBER niż ten obserwowany przez  $A$  i  $B$  to tym lepiej dla podsłuchiacza. Możemy wtedy przyjąć, że mógł sztucznie dodać szum tak by się zgadzało z obserwowanym QBER)

- a) Zapisz wzór na prawdopodobieństwo  $p_B$  kliknięcia detektora u  $B$  na jeden wysłany impuls  $A$  (było na ćwiczeniach)
- b) Zapisz wzór na obserwowany przez  $A$  i  $B$  QBER (było na ćwiczeniach)
- c) Jakie jest prawdopodobieństwo  $p_{n_0 \geq 2}$ , że impuls wysłany przez  $A$  będzie zawierał więcej niż 1 foton (było na ćwiczeniach)
- d) Jaka jest optymalna strategia podsłuchiacza w przypadku gdy  $p_B \leq p_{n_0 \geq 2}$ . Przy jakiej długości światłowodu  $l$  powyższy warunek zachodzi i co w związku z tym można powiedzieć o bezpieczeństwie komunikacji w tym przypadku. (było na ćwiczeniach)
- e) Rozważmy teraz sytuację gdy  $p_B > p_{n_0 \geq 2}$ . Niech  $f$  oznacza fragment impulsów jednofotonowych od  $A$ , które *nie zostają* zablokowane przez  $E$ . Wyprowadź wzór na  $f$  w funkcji podanych parametrów i długości światłowodu  $l$ .
- f) Niech  $r$  oznacza *fragment niezablokowanych* impulsów na których  $E$  wykonuje atak intercept-resend poprzez pomiar w losowo wybranej bazie. Zapisz związek QBER z  $r$ , który pozwoli Ci wyznaczyć parametr  $r$  w funkcji podanych parametrów i długości światłowodu
- g) Zapisz wzór na  $\epsilon$  — poziom błędów  $E$  uzyskany w wyniku takiego ataku.
- h) Korzystając z warunku bezpieczeństwa:  $QBER < \epsilon$ , znajdź warunek na maksymalną odległość bezpiecznej komunikacji

- i) Oblicz tę odległość dla podanych w zadaniu parametrów. Porównaj z wynikami które uzyskał(a)byś zmieniając średnią liczbę fotonów w impulsie na  $\bar{n}_0 = 0.001, 0.1$ . Skomentuj jakościowo uzyskane wyniki.