Cwiczenia4

8 marca 2011
15:58

1 Intercept - Resend attack

1) E atakuje n-ty czesc fotonow. Jesli atakuje mierzy je z $p=\frac{1}{2}$ w bazie $\oplus$ lub $\otimes$

Wprowadza blad: $QBER = \frac{n}{4}$

Jaki jest blad E:

$$\varepsilon = \frac{n}{4} + \frac{1-n}{2}$$

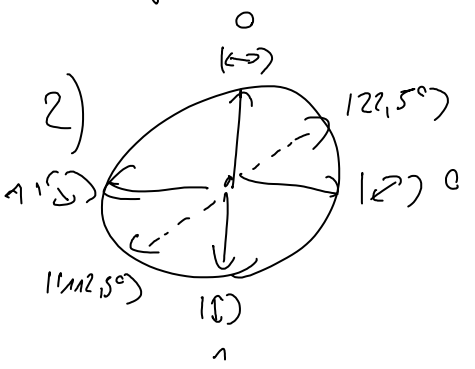
↑ jesli nie atakuje to musi zgadywac

czyli $\varepsilon = QBER + \frac{1-4QBER}{2}$ gdzie

$QBER < \varepsilon$ pod warunkiem, ze $QBER < 25\%$

Wynika sie wiec ze jestesmy bezpieczni jesli $QBER < 25\%$

2)

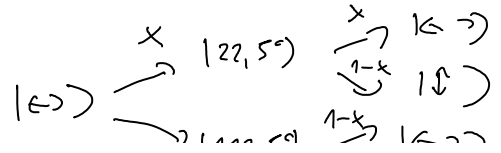


zamiast zmieniac baze E moze mierzyc w bazie $|22,5°\rangle, |112,5°\rangle$

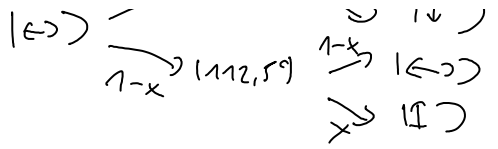
Jesli atakuje wysyla fotony to:

Nadal A wysyla $|\leftrightarrow\rangle$, oznaczmy $x = |\langle 22,5° | \leftrightarrow \rangle|^2 =$

A $\in$ B $= \cos^2 22,5° = \frac{\cos 45° + 1}{2} = \frac{2+\sqrt{2}}{4}$



$QBER = 2x(1-x) =$



$QBER = 2x(1-x) =$

$= 2 \cdot \frac{2+\sqrt{2}}{4} \cdot \frac{2-\sqrt{2}}{4} = \frac{1}{4} = 25\%$

$\varepsilon = 1 - x \approx \frac{2-\sqrt{2}}{4} \simeq 14,6\%$ $\quad \varepsilon < QBER$

Grzime ?

Przy jakim QBER bedzie bezpiecznie ?

Rozważmy atak gdzie E atakuje n-ta część fotonów:

$$QBER = \frac{n}{4}$$

$$\varepsilon = n\left(\frac{2-\sqrt{2}}{4}\right) + \frac{1-n}{2} = \frac{1}{2} - \frac{n\sqrt{2}}{4} = \frac{1}{2} - \sqrt{2}\,QBER$$

Warunek: $QBER < \varepsilon$

$$QBER < \frac{1}{2} - \sqrt{2}\,QBER$$

$$QBER < \frac{1}{2(1+\sqrt{2})} = 20,7\%$$

Widzimy, że mamy mocniejszy warunek.

Rozważając najbardziej ogólne atak uzyskuje się ograniczenie $QBER < 11\%$ które na pewno jest bezpieczne. (Może powiemy coś o tym później)

Bezpieczeństwo kryptografii kwantowej wiąże się ściśle z niemożliwością klonowania stanów kwantowych, ale o tym później....

2. Protokół B92

Wiemy że bezpieczeństwo kryptografii kwantowej wiąże się z niemożliwością klonowania stanów. Może więc istnieje protokół używający tylko

2 stanów nieortogonalnych.

A wysyła do B tylko dwa stany: $|\leftrightarrow\rangle$, $|\nearrow\!\!\swarrow\rangle$ (logiczne wartości 0, 1)
sformułuj stosowany protokół.

B mierzy losowo w bazie ✢ lub ✕
ale tym razem nie mogą ogłaszać bazy bo to jednoznacznie identyfikuje bit klucza.

Ale:
- jeśli B zmierzy $|\nwarrow\!\!\searrow\rangle$ wie że to musi pochodzić od $|\nearrow\!\!\swarrow\rangle$ = 0
- jeśli B zmierzy $|\updownarrow\rangle$ wie że to od $|\leftrightarrow\rangle$ = 1

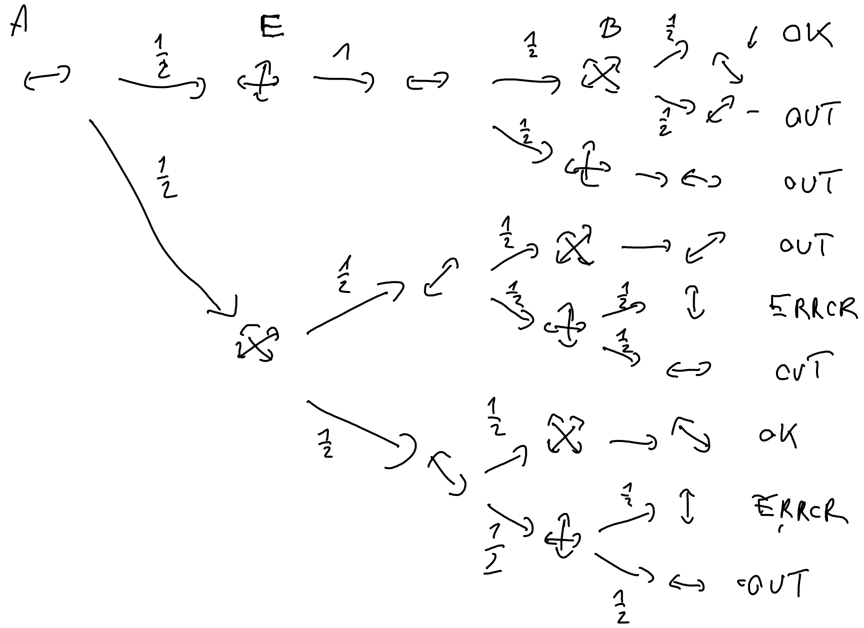
Zapisuje sobie w tych przypadkach bity logiczne.
Pozostałe przypadki odrzuca i informuje A żeby też je usunęła.

Jaką część bitów im zostanie?

$|\leftrightarrow\rangle$ z $p=\frac{1}{2}$ mierzy ✢ → ↔ odrzucane (OUT)
$\frac{1}{2}$ mierzy ✕ $\xrightarrow{\frac{1}{2}}$ ⤢ odrzucane (OUT)
$\frac{1}{2}$ → ⤡ zachowane (OK)

Zostanie im $\frac{1}{4}$ bitów (gorzej niż w BB84)

- Atak na B92
  - E mierzy ✢ lub ✕ z $p=\frac{1}{2}$, jeśli wyprowadzi QBER

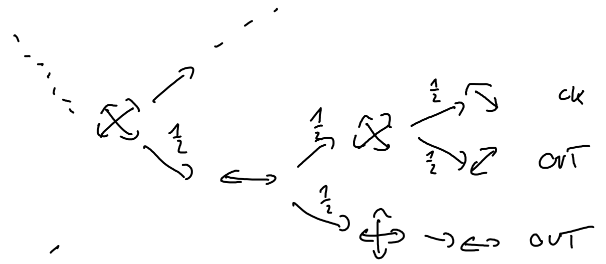


$P_{OK} = \frac{1}{8} + \frac{1}{8} = \frac{1}{4}$, $P_{OUT} = \frac{1}{8} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} = \frac{5}{8}$, $P_{ERROR} = \frac{1}{8}$

Taki atak zmienia [illegible] odrzuconych [illegible]. Tutaj do [illegible]

Taki atak zmienia odsetek odrzuconych czyli łatwy do wykrycia

- Głupio jest czytać ↘, lepsza strategia ↔



wtedy:

$p_{ok} = \frac{1}{8} + \frac{1}{16} = \frac{3}{16}$ $p_{OUT} = \frac{1}{8} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} + \frac{1}{8} = \frac{13}{16}$ $p_{ERROR} = \frac{1}{16}$

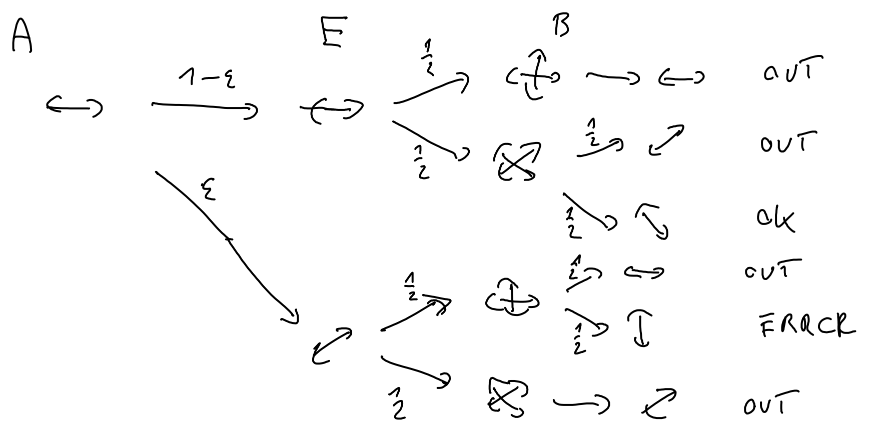
$QBER = \frac{1}{4}$

$\varepsilon = \frac{1}{4}$ czyli gdy $QBER < 25\%$ to jesteśmy bezpieczni ...

- Lepszy atak: $\{ \varepsilon = \frac{1}{2}\left(1 - \sqrt{1 - F(\psi_1, \psi_2)^2}\right)$

E przeprowadza optymalne rozróżnianie stanów

Gdy $\varepsilon = \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{2}}\right) \approx \frac{\sqrt{2}-1}{2\sqrt{2}} = \frac{2-\sqrt{2}}{4} \approx 14,6\%$



$P_{ok} = (1-\varepsilon)\cdot\frac{1}{4}$ $P_{OUT} = (1-\varepsilon)\cdot\frac{3}{4} + \varepsilon\cdot\frac{3}{4} = \frac{3}{4}$ $P_{ERROR} = \varepsilon\cdot\frac{1}{4}$

$QBER = \varepsilon$

Jeśli atakuje r-tą część fotonów to:

$QBER = r\cdot\frac{2-\sqrt{2}}{4}$ $\varepsilon = r\frac{2-\sqrt{2}}{4} + \frac{1-r}{2}$

bezpieczne gdy $QBER < \frac{2-\sqrt{2}}{4} \approx 14,6\%$

⌂ Pomyśleć o innych parach stanów w $\{|\leftrightarrow\rangle, |\swarrow\rangle\}$

3. Protokół 6S

Użyjmy 6 stanów |↔⟩, |↕⟩, |⤢⟩, |⤡⟩, |↻⟩, |↺⟩

Rośnie bezpieczeństwo, analizując dwa ataki intercept-resend

- losowo wybrana jedna z trzech baz
- ,,baza pośrednia''

Czy jest sens zwiększać jeszcze liczbę stanów...?