3 Cwiczenia

21 października 2014
10:33

1 Intercept - Resend attack

1) E atakuje n-ty czesć fotonów. Jeśli atakuje mierzy je z $p=\frac{1}{2}$ w bazie $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$

Wprowadzi błąd: $QBER = \frac{n}{4}$

Jeśli jest błąd E:

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

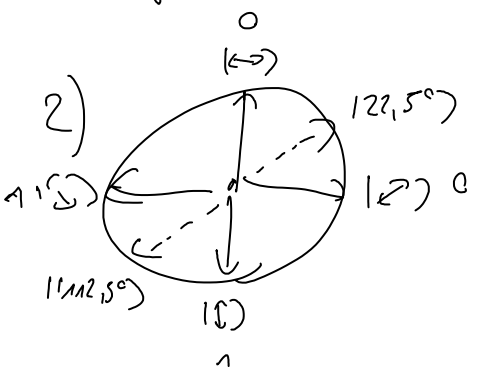
↑ jeśli nie atakuje to musi zgadywać

czyli $E = QBER + \frac{1-4QBER}{2}$ więc

$QBER < E$ pod warunkiem, że $QBER < 25\%$

Wydaje się więc że jesteśmy bezpieczni jeśli $QBER < 25\%$

2)

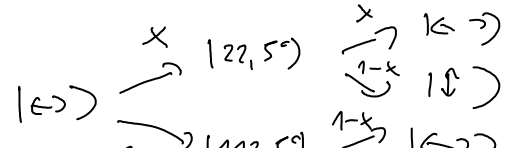


zamiast zmieniać bazy E może mierzyć w bazie $|22,5°\rangle, |112,5°\rangle$

Jeśli atakuje wysłane fotony to:

Niech A wysyła $|\leftrightarrow\rangle$, oznaczmy $X = |\langle 22,5° | \leftrightarrow \rangle|^2 =$

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



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

$1-x$ [illegible] $= 2 \cdot \frac{2+\sqrt{2}}{4} \cdot \frac{2-\sqrt{2}}{4} = \frac{1}{4} = 25\%$

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

Granice ?

Przy jakim QBER bardzo 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 atakui uzyskuje się ograniczenie $QBER < 11\%$ kiedy na pewno jest bezpiecznie (Może powiemy coś o tym później)

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

2. Protokół BB2

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

2 stanów nieortogonalnych.

logiczne wartości: 0, 1

A wysyła do B tylko dwa stany: $|\leftrightarrow\rangle$, $|\swarrow\!\nearrow\rangle$
sformułuj stosowny protokół.

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

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

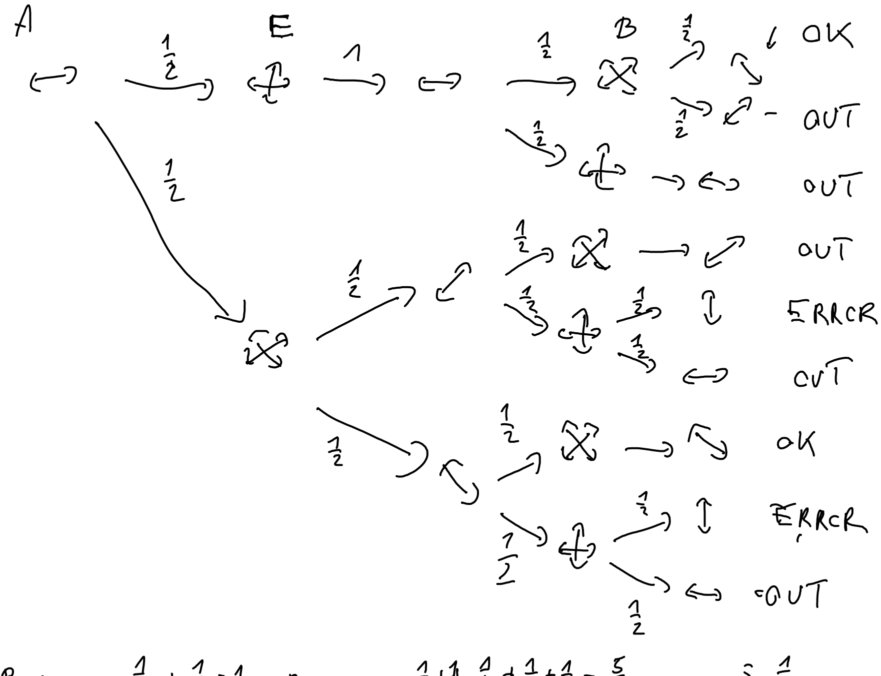
Zapisuje sobie w tych przypadkach bity logiczne.
Pozostałe przypadki odrzuca i informuje A żeby też je usunęła.

Jak dużo bitów im zostanie?

$|\leftrightarrow\rangle$ z $p=\frac{1}{2}$ mierzy ✣ → ↔ odrzucane (OUT)
$\frac{1}{2}$ mierzy ✕ $\frac{1}{2}$ → ⤢ 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

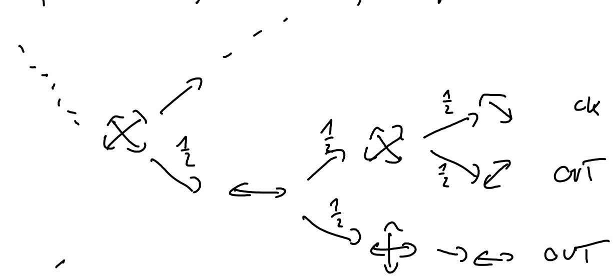


$P_{OK} = \frac{1}{8} + \frac{1}{8} = \frac{1}{4}$, $P_{OUT} = \frac{1}{8} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} = \frac{5}{8}$, $P_{ERROR} = \frac{1}{8}$

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

Taki atak zmienia odsetek odrzuconych czyli łatwy do wykrycia

– Głupio jest czyścić ↘, lepsza strategia ↔



wtedy:

$p_{OK} = \frac{1}{8} + \frac{1}{16} = \frac{3}{16}$ $p_{OUT} = \frac{1}{8} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} + \frac{1}{8} = \frac{12}{16}$ $p_{ERROR} = \frac{1}{16}$

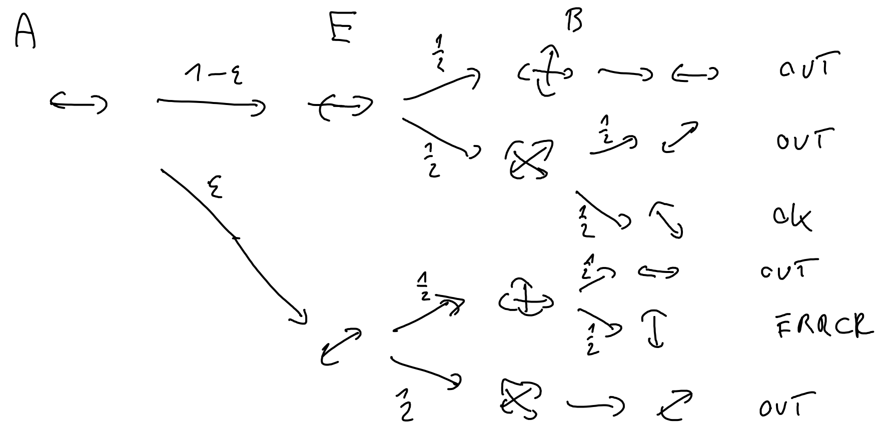
QBER $= \frac{1}{4}$

$\varepsilon = \frac{1}{4}$ czyli jeśli 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

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



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

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

⌂ Poczytać o innych parach stanów $\{|\leftrightarrow\rangle, |\nearrow\rangle\}$

3. Protokół 6S

Używamy 6 stanów $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nearrow\rangle, |\circlearrowright\rangle, |\circlearrowleft\rangle, |\circlearrowleft\rangle$

Rozważmy bezpieczeństwo, analizując dwa ataki intercept-resend

– losowo wybrana jedna z trzech baz

– „baza pośrednia"

Czy jest sens zwiększać jeszcze liczbę stanów...?

a) $\frac{1}{3}$ bitów (2p) opis

b) poziom błędów: E: 33%

poziom błędów A:B = 33% (3p)

c)

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2} e^{i\varphi}|1\rangle$$

„Symetryczna baza" : $\varphi = \frac{\pi}{4}$

$$\langle 0|\psi\rangle = \cos\frac{\theta}{2}$$

$$\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)|\psi\rangle = \frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2} e^{i\frac{\pi}{4}}\right)$$

$$|\ \ |^2 = \frac{1}{2}\left(\cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} + 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\cdot\frac{\sqrt{2}}{2}\right)$$

$$\left(1 + \sqrt{2}\cos\frac{\theta}{2}\sin\frac{\theta}{2}\right) = 2\cos^2\frac{\theta}{2}$$

$$1 + \frac{\sqrt{2}}{2}\sin\theta = 1 + \cos\theta$$

$$\operatorname{tg}\theta = \sqrt{2} \qquad \theta \approx 54^\circ$$

$$\underset{x}{\operatorname{tg}\theta} = \frac{\sin\theta}{\cos\theta} \qquad x^2\cos^2\theta = 1 - \cos^2\theta$$

$$\cos\theta = \sqrt{\frac{1}{1+x^2}}$$

$$\left(\langle 0|\psi\rangle\right)^2 = \frac{\cos\theta + 1}{2} = \frac{1}{2}\left(1 + \sqrt{\frac{1}{1+2}}\right) = \frac{1}{2}\left(1 + \frac{\sqrt{3}}{3}\right) \approx 0{,}79$$

Poziom błędów E: 21%

QBER: $2\,\frac{1}{2}\left(1+\frac{\sqrt{3}}{3}\right)\frac{1}{2}\left(1-\frac{\sqrt{3}}{3}\right) = \frac{1}{2}\cdot\left(1-\frac{3}{9}\right) = 33\%$

2p

$r\,\frac{1}{2}\left(1-\frac{\sqrt{3}}{3}\right)+(1-r)\frac{1}{2} = \frac{2r}{3}$

$r\left(1-\frac{2}{3}-1-\frac{\sqrt{3}}{3}\right) = -1$

$r = \frac{3}{2+\sqrt{3}}$ $\qquad QBER_{th} = \frac{1}{2+\sqrt{3}} \simeq 26{,}7\%$

2p