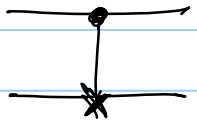
Podstawy w kryptografii.

Znamy bramki kwantowe.

Jednoqubitowa bramka Hadamarda.

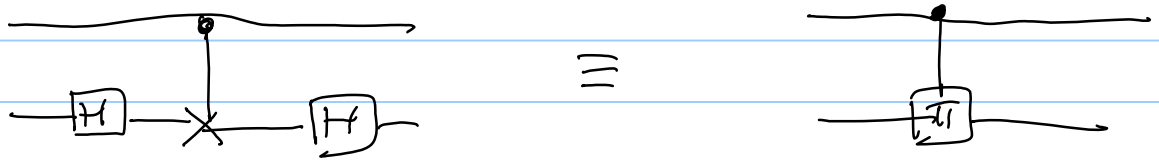
$$\equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Dwuqubitowa bramka C-NOT



$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix}$$

No to znamy inne bramki:



$$\equiv$$

$$|00\rangle \to \frac{1}{\sqrt{2}}|0\rangle(|0\rangle+|1\rangle) \longrightarrow \frac{1}{\sqrt{2}}|0\rangle(|0\rangle+|1\rangle) \to |00\rangle$$

$$|01\rangle \to \frac{1}{\sqrt{2}}|0\rangle(|0\rangle-|1\rangle) \longrightarrow \frac{1}{\sqrt{2}}|0\rangle(|0\rangle-|1\rangle) \to |01\rangle$$

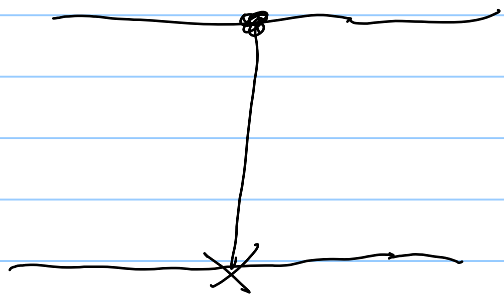
$$|10\rangle \to \frac{1}{\sqrt{2}}|1\rangle(|0\rangle+|1\rangle) \to \frac{1}{\sqrt{2}}|1\rangle(|0\rangle+|1\rangle) \to |10\rangle$$

$$|11\rangle \to \frac{1}{\sqrt{2}}|1\rangle(|0\rangle-|1\rangle) \to -\frac{1}{\sqrt{2}}|1\rangle(|0\rangle-|1\rangle) \to |11\rangle$$

"CONDITONAL SIGN GATE"

Alicja:

$|0\rangle$ lub $|1\rangle$



Ewa: $|0\rangle$

Na wyjściu:

$$|0\rangle_A|0\rangle_E \to |0\rangle_A|0\rangle_E$$

$$|1\rangle_A|0\rangle_E \to |1\rangle_A|1\rangle_E$$

Ewa mierząc swój qubit jest w stanie rozróżnić czy Alicja przygotowała $|0\rangle$ czy $|1\rangle$.

Czy jest jakaś "kara" za to?

Wygodniej z uwagi na notację będzie to przedyskutować dla C-π gate. Oczywiście jedyna różnica to inna baza dla Ewy.

Niech pierwszy qubit "kontrolny" będzie należał do Alicji, a drugi do Ewy.

Załóżmy, że Ewa przygotowała swój qubit w stanie

$$|\xi\rangle_E = \cos\frac{\xi}{2}|0\rangle_E + \sin\frac{\xi}{2}|1\rangle_E$$

Co się dzieje? Niech Alicja wysyła $|0\rangle_A$ lub $|1\rangle_A$.

$$|0\rangle_A|\xi\rangle_E \longrightarrow |0\rangle_A|\xi\rangle_E$$
$$|1\rangle_A|\xi\rangle_E \longrightarrow |1\rangle_A|-\xi\rangle_E$$

Jak dobrze Ewa może odróżnić stan $|0\rangle_A$ oraz $|1\rangle_A$ patrząc na swój qubit? To zależy od kąta ξ.

$$\langle -\xi|\xi\rangle_E = \cos^2\frac{\xi}{2} - \sin^2\frac{\xi}{2} = \cos\xi = V$$

Jeśli $\xi = \frac{\pi}{2}$ (czyli stan postaci $\frac{1}{\sqrt{2}}(|0\rangle_E + |1\rangle_E)$) to dobrze, jeśli $\xi = 0$ to słabo.

(Do tych rzeczy wrócimy mówiąc dojść patrząc na bramkę C-NOT).

Co się dzieje, jeśli Alicja przygotuje qubit w stanie $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

$$|\Psi_{AE}\rangle = |+\rangle_A |\xi\rangle_E = \frac{1}{\sqrt{2}}\left(\cos\frac{\xi}{2}|0\rangle_A|0\rangle_E + \cos\frac{\xi}{2}|1\rangle_A|0\rangle_E + \sin\frac{\xi}{2}|0\rangle_A|1\rangle_E - \sin\frac{\xi}{2}|1\rangle_A|1\rangle_E\right).$$

$$= \cos\frac{\xi}{2}|+\rangle_A|0\rangle_E + \sin\frac{\xi}{2}|-\rangle_A|1\rangle_E$$

Jak wygląda stan qubita Alicji po oddziaływaniu?

$$\hat{\rho}_A = Tr_E\left(|\Psi\rangle_{AE}\langle\Psi|\right) =$$

$$= \cos^2\frac{\xi}{2}|+\rangle_A\langle+| + \sin^2\frac{\xi}{2}|-\rangle_A\langle-|.$$

Dostaniemy $|+\rangle\langle+|$ jeśli $\xi = 0, 2\pi$, itd. To oznacza że Ewa nie wysłała żadnej informacji. Natomiast jeśli $\theta = \pi$, to

$$\hat{\rho}_A = \frac{1}{2}\left(|+\rangle_A\langle+| + |-\rangle_A\langle-|\right) = \frac{1}{2}\hat{1}_A$$

STAN CAŁKOWICIE MIESZANY.

A co dla ogólnego stanu? Weźmy:

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

$$|\psi\rangle_A|\xi\rangle_E = \left(\cos\frac{\theta}{2}|0\rangle_A + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle_A\right)\left(\cos\frac{\xi}{2}|0\rangle_E + \sin\frac{\xi}{2}|1\rangle_E\right)$$

$$= \left(\cos\frac{\theta}{2}|0\rangle_A + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle_A\right)\cos\frac{\xi}{2}|0\rangle_E$$

$$+ \left(\cos\frac{\theta}{2}|0\rangle_A - e^{i\varphi}\sin\frac{\theta}{2}|1\rangle_A\right)\sin\frac{\xi}{2}|1\rangle_E$$

$$\hat{\rho}_A = \cos^2\frac{\theta}{2}|0\rangle_A\langle 0| + \cos\xi\, e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|1\rangle_A\langle 0|$$

$$+ \cos\xi\, e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|0\rangle_A\langle 1| + \sin^2\frac{\theta}{2}|1\rangle_A\langle 1|$$

$$= \begin{pmatrix} \cos^2\frac{\theta}{2} & e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\cos\xi \\ e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\cos\xi & \sin^2\frac{\theta}{2} \end{pmatrix}$$

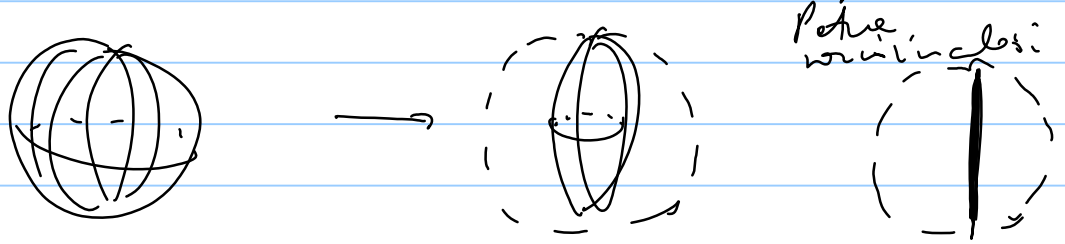
$$= \frac{1}{2}\begin{pmatrix} 1+\cos\theta & e^{-i\varphi}\sin\theta\cos\xi \\ e^{i\varphi}\sin\theta\cos\xi & 1-\cos\theta \end{pmatrix}$$

$$= \frac{1}{2}\Big(\mathbb{1} + \underbrace{\cos\xi\sin\theta\cos\varphi}_{s_x'}\,\hat{\sigma}_x + \underbrace{\cos\xi\sin\theta\sin\varphi}_{s_y'}\,\hat{\sigma}_y + \underbrace{\cos\theta}_{s_z'}\,\hat{\sigma}_z\Big)$$

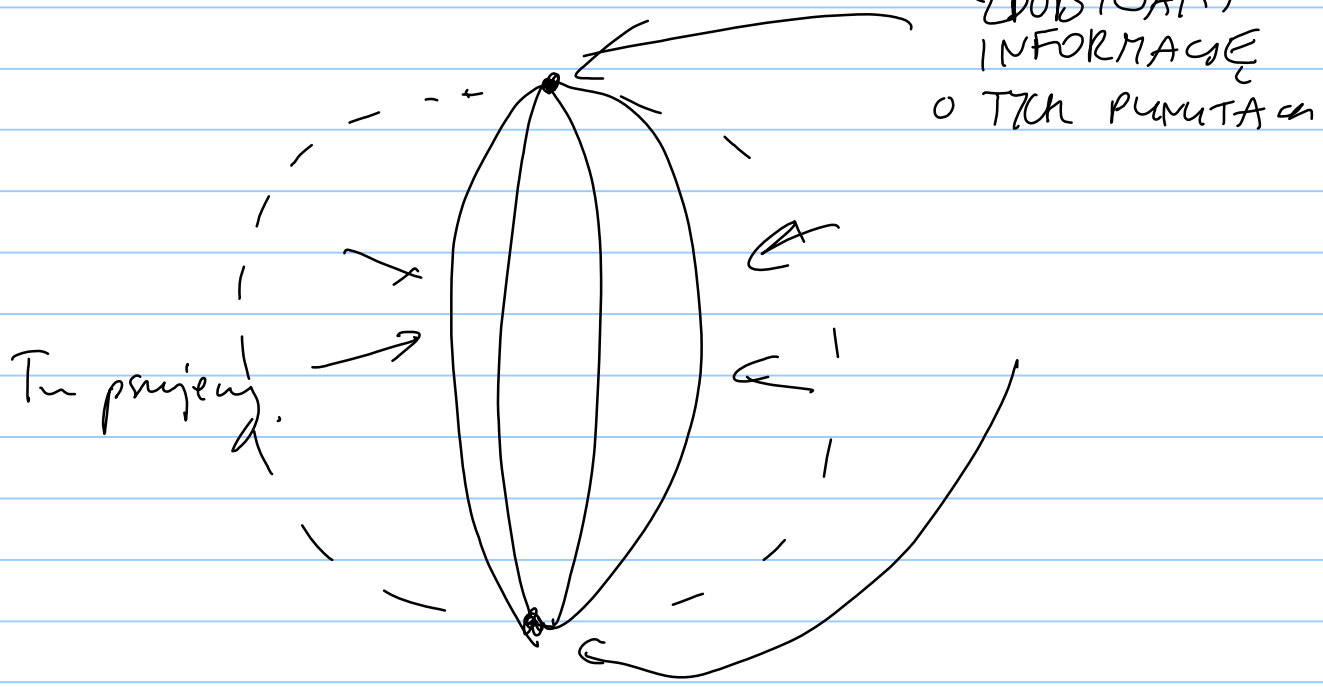
Wektor Blocha:

$$\vec{s}' = \begin{pmatrix} V \sin\theta \cos\varphi \\ V \sin\theta \sin\varphi \\ \cos\theta \end{pmatrix}$$

Utożsamienie $\begin{pmatrix} s_x \\ s_y \\ s_z \end{pmatrix} \to \begin{pmatrix} V s_x \\ V s_y \\ s_z \end{pmatrix}$

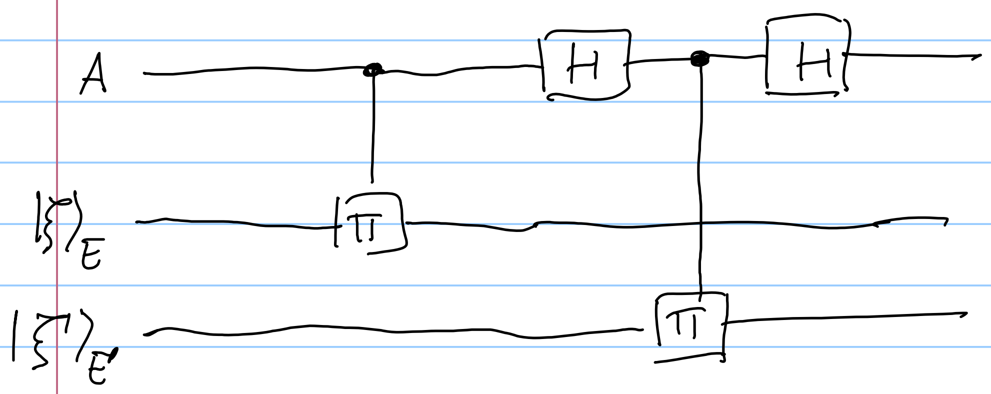


Popsuty sfery Blocha.



Teraz widzimy, dlaczego kryptografia kwantowa jest bezpieczna: testujemy, że nic złego się nie stało w dwóch kanałach.

Zaprojektujmy podsłuch, który byłby symetryczny w $\{|0\rangle, |1\rangle\}$ oraz $\{|+\rangle, |-\rangle\}$.



$$|0\rangle_A|\xi\rangle_E|\xi'\rangle_{E'} \rightarrow |0\rangle_A|\xi\rangle_E|\xi'\rangle_{E'}$$

$$\xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right)|\xi\rangle_E \cos\frac{\xi'}{2}|0\rangle_{E'} + \frac{1}{\sqrt{2}}\left(|0\rangle_A - |1\rangle_A\right)|\xi\rangle_E \sin\frac{\xi'}{2}|1\rangle_{E'}$$

$$\xrightarrow{H} \cos\frac{\xi'}{2}|0\rangle_A|\xi\rangle_E|0\rangle_{E'} + \sin\frac{\xi'}{2}|1\rangle_A|\xi\rangle_E|1\rangle_{E'}$$

$$|1\rangle_A|\xi\rangle_E|\xi'\rangle \rightarrow \cos\frac{\xi'}{2}|1\rangle_A|\xi\rangle_E|0\rangle_{E'} + \sin\frac{\xi'}{2}|0\rangle_A|\xi\rangle_E|1\rangle_{E'},$$

W tej bazie qubit E zbiera informacje, qubit E' wprowadza niepewność.

Tutaj by jeszcze policzyć, co się dzieje w drugiej bazie! Ale to mniej ważne

$$|+\rangle_A |\xi\rangle_E |\xi'\rangle_{E'} \to \cos\frac{\xi}{2}|+\rangle_A|0\rangle_E|\xi'\rangle_{E'} + \sin\frac{\xi}{2}|-\rangle_A|1\rangle_E|-\xi'\rangle_{E'}$$

$$|-\rangle_A |\xi\rangle_E |\xi'\rangle_{E'} \to \cos\frac{\xi}{2}|-\rangle_A|0\rangle_E|-\xi'\rangle_{E'} + \sin\frac{\xi}{2}|+\rangle_A|1\rangle_E|\xi'\rangle_{E'}$$

Z punktu widzenia Alicji i Boba:

$$|0\rangle\langle 0|_A \to \cos^2\frac{\xi}{2}|0\rangle\langle 0|_A + \sin^2\frac{\xi}{2}|1\rangle\langle 1|_A$$

$$|1\rangle\langle 1|_A \to \cos^2\frac{\xi}{2}|1\rangle\langle 1|_A + \sin^2\frac{\xi}{2}|0\rangle\langle 0|_A$$

$$|+\rangle\langle +|_A \to \cos^2\frac{\xi}{2}|+\rangle\langle +| + \sin^2\frac{\xi}{2}|-\rangle\langle -|$$

$$|-\rangle\langle -| \to \cos^2\frac{\xi}{2}|-\rangle\langle -| + \sin^2\frac{\xi}{2}|+\rangle\langle +|$$

$\sin^2\frac{\xi}{2}$ jest prawdopodobieństwem wpłynięcia błędu w bazie $0/1$, $\sin^2\frac{\xi}{2}$ - w bazie $+/-$

Zatem dla uproszczenia, że są takie same

$$QBER \equiv q = \sin^2\frac{\xi}{2} = \cos^2\frac{\xi}{2}.$$

Jak to wygląda z punktu widzenia Ewy? Po ogłoszeniu bazy przez Boba Ewa wie, na który qubit patrzeć. Ma rozróżnić pomiędzy $|\xi\rangle$ a $|-\xi\rangle$ dla E albo E'.

Twierdzenie z klasycznej teorii informacji: możemy wydestylować co najmniej [illegible]

$$K \geq I(A:B) - I(A:E)$$

bitów klucza.

$$I(A:B) = 1 - H(q) = 1 + q\log_2 q + (1-q)\log_2(1-q)$$

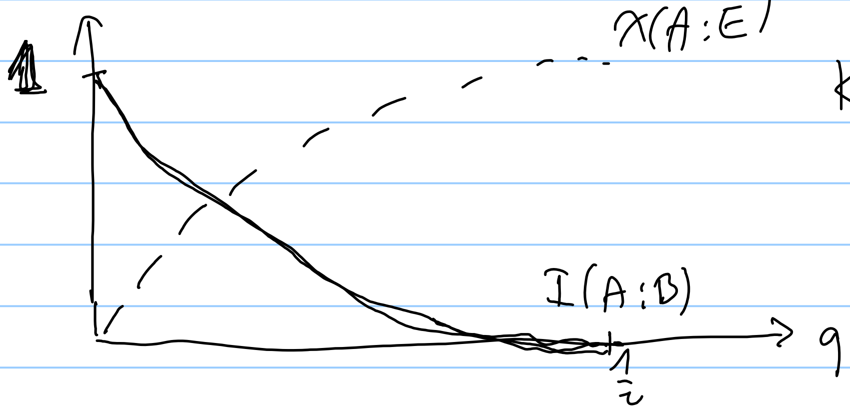
Prosta, A co z $I(A:E)$?

$$I(A:E) \leq \chi(A:E) =$$

$$= S\left(\frac{1}{2}|\xi\rangle\langle\xi| + \frac{1}{2}|-\xi\rangle\langle-\xi|\right)$$

$$\frac{1}{2}|\xi\rangle\langle\xi| + \frac{1}{2}|-\xi\rangle\langle-\xi| = \begin{pmatrix} \cos^2\frac{\xi}{2} & 0 \\ 0 & \sin^2\frac{\xi}{2} \end{pmatrix}$$

$$\chi(A:E) = H(q)$$



$$K \geq 1 - 2H(q).$$

Tracimy bezpieczeństwo, kiedy

$1 - 2H(q) = 0$ $\qquad q \approx 11\%$.

ĆWICZENIE Znaleźć definicję sfery Blocha, indukowaną przez naszą strategię podsłuchu.