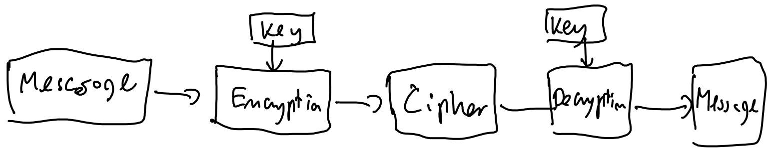
Wyklad5

17 maja 2011
13:00

Classical cryptography

General scheme:



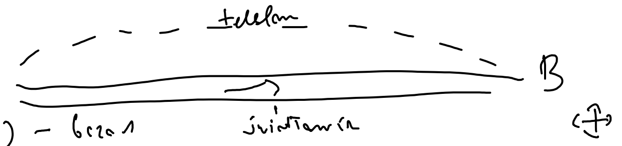
- CEASAR → DFBTBS
  only 26 keys easy to break
- general substitution cipher
  26! keys, but... frequency analysis
- Is there a 100% secure cipher
  yes: one-time pad.
  Key length = message length

If A and B have random bit sequence of the length of the message. A just adds mod 2 key to the message and B does the same for decoding.
Cipher is completely random.
Problem – key needs to be very long.
How to distribute the key? Very impractical

Quantum key distribution (Q. cryptography)

Ideas: - You cannot learn anything about a quantum state without disturbing it
– nonorthogonal states cannot be distinguished

- BB84



1. np. $|\leftrightarrow\rangle$, $|\updownarrow\rangle$ – baza 1 (0, 1)
   $|\nearrow\rangle$, $|\searrow\rangle$ – baza 2
2. po komunikacji zostają tylko te bity które zmierzone były w tej samej bazie

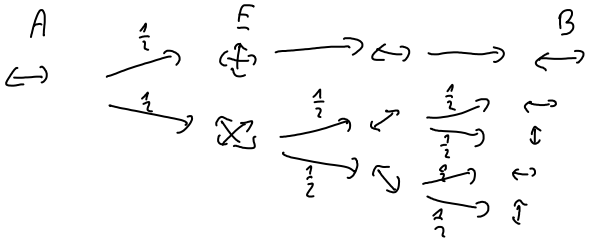
	0	~~0~~	1	~~1~~	1	1	~~0~~	~~0~~
A	↔	⤢	↕	↔	⤡	↕	↔	⤢
B	+	+	+	×	×	+	×	+
	0	0/1	1	0/1	1	1	0/1	0/1

3. następnie ujawniają może część aby sprawdzić czy poziom błędów jest dostatecznie mały
4. wtedy można stwierdzić że nikt nie mógł wyciągnąć

zbyt dużo informacji

W szczególności jeśli nie ma błędów mamy pewność że atakt nie mógł podsłuchać. Dlaczego?

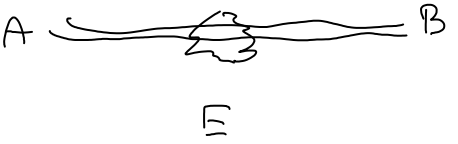
- Intercept & Resend attack
  - wykrywalne w połowie z nich QBER = 25%



Jeśli widzimy że nie ma błędów QBER=0 mamy pewność że atakt nie podsłuchał. Ale ....

W praktyce jednak zawsze są błędy wynikające z szumu. Czy jak widzimy poziom błędów < 25% to jesteśmy bezpieczni. Nie. Bo pewien mógł atakować niektóre bity. Jaki poziom błędów jest tolerowalny? Może jest inny typu ataku? Trzeba dokładniej zbadać ?

Im wyższy poziom błędów tym więcej informacji mógł zdobyć podsłuchiwacz. Assume for simplicity individual attacks !



A	00110100
B	0?1?0100
E	0?11?10?

After basis reconciliation there is a probability distribution describing correlation between bit values

$P(A,B,E)$: $p(a,b,e)$

$p(a,b) = \sum_e p(a,b,e)$ $\quad p(a,e) = \sum_b p(a,b,e)$

$a=0 \Rightarrow b=0 \; p=1-QBER$; $b=1 \; p=QBER$ $\quad a=0 \Rightarrow e=0 \; p=1-\varepsilon$; $e=1 \; p=\varepsilon$

$a=1 \Rightarrow b=1 \; p=1-QBER$; $b=0 \; p=QBER$ $\quad a=1 \Rightarrow e=1 \; p=1-\varepsilon$; $e=0 \; p=\varepsilon$

QBER - poziom błędów u B , ε - poziom błędów u E

Intuition if correlations between A and B are stronger (they share more information) then correlations between A and E:

$\sim$ $\quad QBER < \varepsilon$

it is possible to extract some secure key.

it is possible to extract some secure key by classical procedures of error-correction + privacy amplification. In niży QBER tym dalej mniej kwantowej wiemy że E nie wie więcej niż E..

Dla danego QBER musimy znaleźć optymalny atak (dający najmniejsze e) i policzyć wzór.

QBER < ε to możemy wysłać klucz

Potrzebujemy wielkości mówiących o ilości informacji jaką można poznać na temat A znając np. B

Shannon Entropy & Mutual information

- Shannon entropy: $H(X) = -\sum_x p(x)\log_2 p(x)$
  - miara przypadkowości zmiennej losowej X
- $x = 0,1$ $p(0) = \frac{1}{2}$ $p(1) = \frac{1}{2}$ $H(x) = 1$
- $p(0) = 1$ $p(1) = 0$ $H(x) = 0$

Jak dobrze można skompresować dane.

Example:

a, b, c, d $p(a) = \frac{1}{2}$ $p(b) = \frac{1}{4}$ $p(c) = p(d) = \frac{1}{8}$

How to encode to use on average the smallest number of bits

$a = 0$
$b = 10$ on average 1,75 bits
$c = 110$
$d = 111$

$H(X) = 1{,}75$.

If we chose a different encoding e.g. $a = 00$, $b = 01$, $c = 10$, $d = 11$ we would see that we more often use 2 than 1 - not optimal

Intuition:

If we have random variable X realized N times then for large N we will always have sequences in which symbol x appears $\simeq N p(x)$ times
- typical sequence.
- Law of large numbers.

probability of a given typical sequence

$$p^N_{typical} = \prod_x p(x)^{N p(x)} = 2^{N\sum_x p(x)\log_2 p(x)}$$

$$N_{\substack{typical\\sequences}} = \frac{1}{p^N_{typical}} = 2^{-N\sum_x p(x)\log_2 p(x)} = 2^{NH(X)}$$

So we need $N\,H(X)$ bits to label all sequences.
In this sense $H(x)$ is the compression rate.
Shannon source coding theorem.

- Shannon mutual information

- Shannon mutual information

X —— channel $p(y|x)$ —— Y

$p(x)$ — probability distribution for input symbols

— conditional entropy:

$$H(Y|x) = -\sum_y p(y|x) \log p(y|x)$$

on average:

$$H(Y|X) = \sum_x p(x) H(Y|x) = -\sum_{xy} p(x) p(y|x) \log p(y|x)$$

how random is Y if we know X

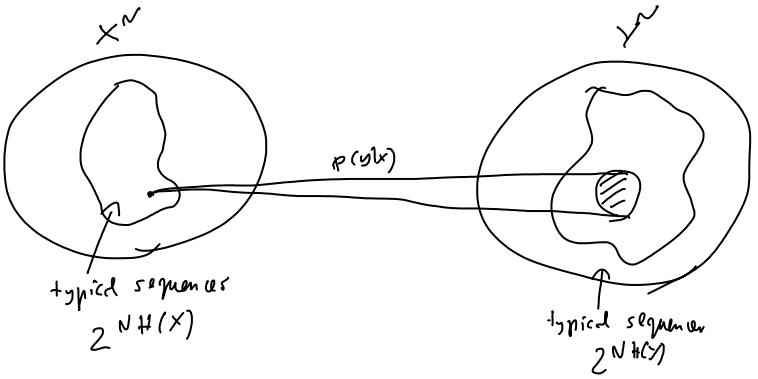
— mutual information

(how much do we learn about Y once we learn X)

$$I(X:Y) = H(Y) - H(Y|X) =$$
$$= H(X) + H(Y) - H(X,Y)$$

$$H(X,Y) = -\sum_{x,y} p(x,y) \log p(x,y) \quad !$$

Intuition



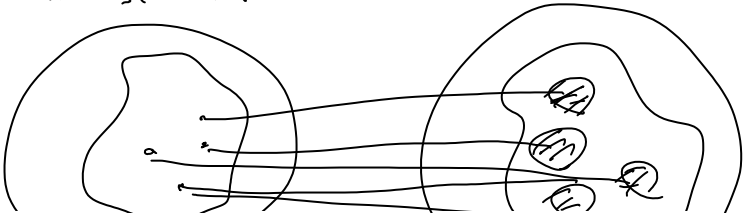
one typ.sequence in X^N will be transformed to

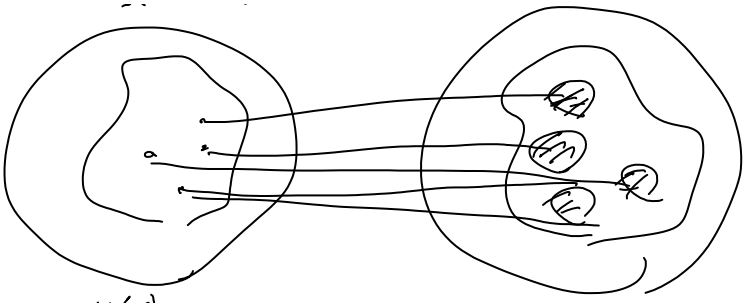
$2^{NH(Y|X)}$ =

$Np(x)$ very typ. x created probabilistically on $2^{Np(x)H(Y|x)}$ ways adding $Np(x)$ to some other knowledge x. many vice:

$2^{\sum_x Np(x)H(Y|x)} = 2^{NH(Y|X)}$ typ sequences

how many different input sequences can be used to send information:





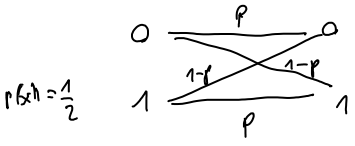
$$\frac{2^{NH(Y)}}{2^{NH(Y|X)}} = 2^{NI(X:Y)}$$

Mutual information tells us about channel capacity

- Shanno channel theorem:

$$C = \max_{p(x)} I(X:Y)$$

Example:

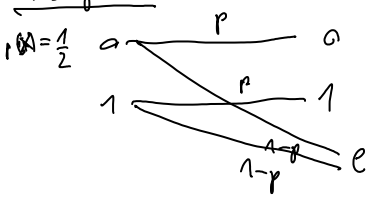


$$h(p) = -p\log_2 p - (1-p)\log_2(1-p)$$

$$I(X:Y) = 1 - h(p)$$

- $p = 100\%$ $\quad I(X:Y) = 1$
- $p = 50\%$ $\quad I(X:Y) = 0$
- for $p = 90\%$ $\quad I(X:Y) = 0{,}531$

Example:



$$H(Y) = -\frac{1}{2}p(\log_2 p - \frac{1}{2}p\log_2\frac{p}{2} - (1-p)\log(1-p)$$

$$H(Y|X) = 2\cdot\frac{1}{2}(-p\log p - (1-p)\log(1-p))$$

$$I(X:Y) = -p\log\frac{p}{2} + p\log p = p$$

Csiszar-Körner theorem

If three parties share N realization of random variables A, B, E distributed according to $p(a,b,c)$

Parties A and B are able to extract

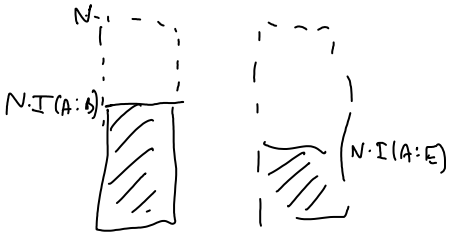
$$K \approx N(I(A:B) - I(A:E))$$

bits of which E knows nothing: $p'(a,b,c) \approx p'(a,b)\cdot p'(e)$

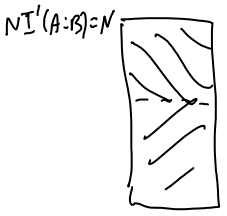
$$p'(a,b) = \frac{1}{2}\delta_{a,b}$$

secret key.

Idea:



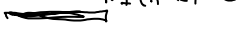
↓ Error correction
A and B exchange
arbitrarily $M = N(1 - I(A:B))$
bits to correct errors



– but this could also be used by E

↓ privacy amplification

we make use of the fact that E does still have some errors. A and B shorten their strings in order to make them completely random for E



$N'' = N\left[I(A:B) - I(A:E)\right]$ same bits

Error-Correction

- Interactive error correction protocol (1992, Bennett et al)

Iteration:

– A and B apply random permutation

– A and B divide their N bits in blocks of length n

$$N = k \cdot n$$

(the length of the block should be such that it is not very probable that there are more than 1 error)

– They check parities of bits in each subblock if it does not agree → bisection

– If all parity errors were corrected they repeat the iteration with larger block size ...

Privacy amplification

A and B share N perfectly correlated bits while E knows effectively $N - K$ bits

[after error-correction $K = N(I(A:B) - I(A:E))$]

A and B apply a random hashing function

the simplest example:

$$K' \text{ bits} \begin{bmatrix} \\ \\ \\ \end{bmatrix} = K' \begin{bmatrix} 1\,0\,0\,1\,1\,0\,1\,0\,1 \\ \vdots \\ \vdots \end{bmatrix}_{N} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} N$$

0 and 1 put randomly

1's will spread any error of E to a bits of the final key provided $K \leq K$

Main goal in Q. cryptography

Given QBER find the optimal attack by E, i.e. maximizing $I(A:E)$. Then we know what maximal knowledge E can have and we know how much we need to shorten the key during privacy amplification.

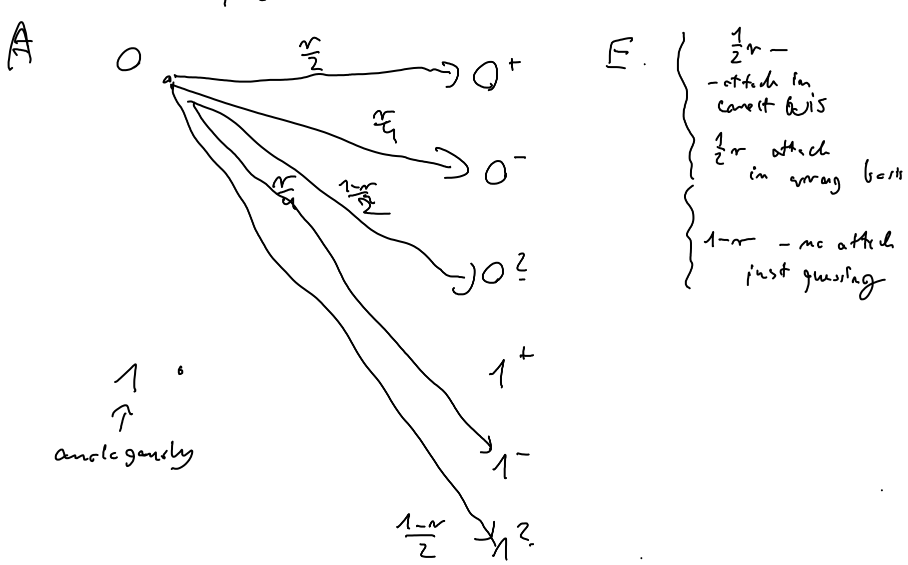
There is $QBER_{th}$ for which $I(A:B) = I(A:E)$. Above this threshold no key distribution is possible

Example: Intercept & Resend, attacking a fraction r of qubits. Using random basis for ...

$QBER = \frac{r}{4}$ $\qquad I(A:B) = 1 - h\left[\frac{r}{4}\right]$

$I(A:E)$: E guesses her bit correctly with $p = \left(\frac{1}{2} + \frac{1}{4}\right) + (1-r)\frac{1}{2} = \frac{1}{2} + \frac{r}{4}$

Error $e = \frac{1}{2} - \frac{r}{4}$ but be careful $I(A:E) \neq 1 - h[e]$, because E knows whether basis was correct or not



$p(0^+) = \frac{r}{4}$ $\quad p(0^-) = \frac{r}{4}$ $\quad p(0^?) = \frac{1-r}{2}$ $\quad p(1^+) = \frac{r}{4}$ $\quad p(1^-) = \frac{r}{4}$ $\quad p(1^?) = \frac{1-r}{2}$

$H(E) = -r \log \frac{r}{4} - (1-r) \log \frac{1-r}{2}$

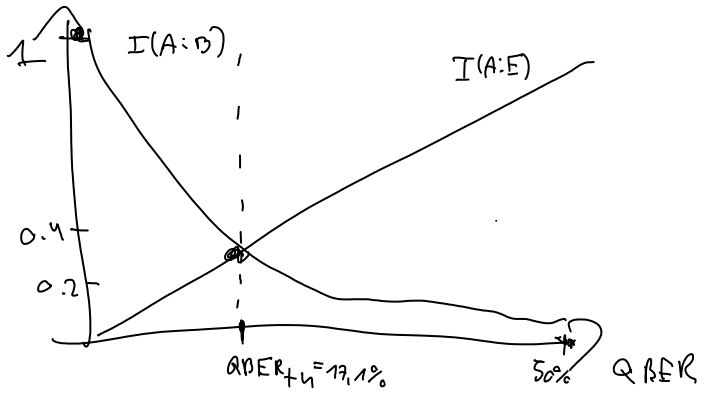
$H(E|A) = -\frac{r}{2} \log \frac{r}{2} - \frac{r}{2} \log \frac{r}{4} - (1-r) \log_2 \frac{1-r}{2}$

$$H(E) - H(E|A) = \frac{r}{2}\log\frac{r}{2} - \frac{r}{2}\log\frac{r}{4} \simeq \frac{r}{2} = I(A:E)$$

For what r we will have $I(A:B) = I(A:E)$?:

$$\frac{r}{2} \simeq 1 - h\left[\frac{r}{4}\right] \Rightarrow r = 0{,}6821$$

$$QBER_{th} = 0{,}1705 \approx 17{,}1\%$$



Assuming this was the optimal attack. If we detect $QBER < QBER_{th}$ we are sure that $I(A:B) > I(A:E)$ and we can distill secret key.

Actually the optimal attack (via optimal cloning) yields $QBER_{th} = \frac{2-\sqrt{2}}{4} \approx 14{,}6\%$

- In the attack we wait with the measurement until A & B announce the basis.

Pauli's attack:

To get some intuition consider the following attack

$$\begin{cases} |0\rangle_A \otimes |a\rangle_E \longrightarrow |0\rangle_B \otimes |0\rangle_E \\ |1\rangle_A \otimes |a\rangle_E \longrightarrow |1\rangle_B \otimes |\theta\rangle_E \end{cases} \qquad |\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

If $\theta = 0$, E gains no information, if $\theta = \frac{\pi}{2}$ E gains full information on $|0\rangle, |1\rangle_A$. In either case B state are undisturbed

How this operation acts on $|+\rangle, |-\rangle$

$$|+\rangle_A \otimes |0\rangle_E \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle_B \otimes |0\rangle_E + |1\rangle_B \otimes |\theta\rangle_E\right) = |\Psi^+\rangle_{BE}$$

$$|-\rangle_A \otimes |0\rangle_E \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle - |1\rangle \otimes |\theta\rangle\right) = |\Psi^-\rangle_{BE}$$

Let us look at reduced density matrices of B and E

$$|+\rangle_A\langle+| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$S_B^+ = Tr_E\left(|\Psi^+\rangle_{BE}\langle\Psi^+|\right) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| \cdot \underbrace{\langle\theta|0\rangle}_{\cos\theta} + \frac{1}{2}|1\rangle\langle 0| \underbrace{\langle 0|\theta\rangle}_{\cos\theta} + \frac{1}{2}|1\rangle\langle 1| =$$

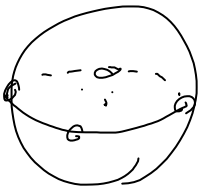
$$= \frac{1}{2}\begin{bmatrix} 1 & \cos\theta \\ \cos\theta & 1 \end{bmatrix}$$ – we are loosing coherence in particular for $\theta = \frac{\pi}{2}$ $S_B^+ = \frac{1}{2}\mathbb{1}$

$$S_B^- = \frac{1}{2}\begin{bmatrix} 1 & -\cos\theta \\ -\cos\theta & 1 \end{bmatrix} \qquad S_B^+ = \cos^2\frac{\theta}{2}|+\rangle\langle+| + \sin^2\frac{\theta}{2}|-\rangle\langle-|$$

$S_B^- = \cos^2\frac{\theta}{2}|-\rangle\langle -| + \sin^2\frac{\theta}{2}|+\rangle\langle +|$

The one E learns about B in $|0\rangle,|1\rangle$ basis the bigger disturbance it causes in $|+\rangle,|-\rangle$ basis.

Optymalne klonowanie dla stanu nr. BB84



Spróbujmy zrobić uogólnienie na rozmiar

$|0\rangle_1|0\rangle_2|0\rangle_A \to \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}(|01\rangle+|10\rangle)|1\rangle$

$|1\rangle|0\rangle|0\rangle \to \frac{1}{2}(|01\rangle+|10\rangle)|0\rangle + \frac{1}{\sqrt{2}}|111\rangle$

$|\psi\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + e^{i\psi}|100\rangle) \longrightarrow$

$\longrightarrow \frac{1}{2}|000\rangle + \frac{1}{2\sqrt{2}}(|01\rangle+|10\rangle)|1\rangle +$

$+ e^{i\psi}\frac{1}{2\sqrt{2}}(|01\rangle+|10\rangle)|0\rangle + e^{i\psi}\frac{1}{2}|111\rangle =$

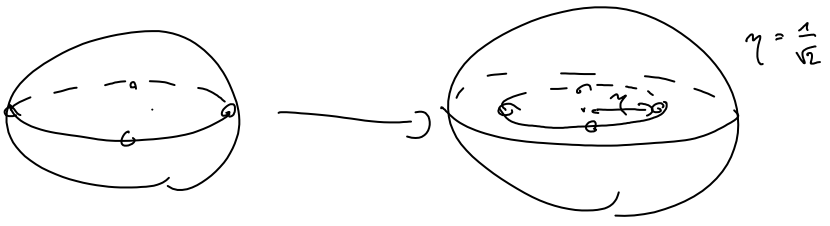
$= \left(\frac{1}{2}|0\rangle + \frac{1}{2\sqrt{2}}e^{i\psi}|1\rangle\right)|00\rangle + \frac{1}{2\sqrt{2}}|1\rangle|01\rangle$

$+ e^{i\psi}\frac{1}{2\sqrt{2}}|0\rangle|10\rangle + \left(\frac{1}{2\sqrt{2}}|0\rangle + \frac{1}{2}e^{i\psi}|1\rangle\right)|11\rangle$

$\rho_1 = \frac{1}{4}\begin{bmatrix} 1 & \frac{1}{\sqrt{2}}e^{-i\psi} \\ \frac{1}{\sqrt{2}}e^{i\psi} & \frac{1}{2}\end{bmatrix} + \frac{1}{4}\begin{bmatrix} \frac{1}{2} & \\ & \frac{1}{2}\end{bmatrix} + \frac{1}{4}\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}}e^{i\psi} \\ \frac{1}{\sqrt{2}}e^{i\psi} & 1\end{bmatrix} =$

$= \frac{1}{2}\begin{bmatrix} 1 & \frac{1}{\sqrt{2}}e^{-i\psi} \\ \frac{1}{\sqrt{2}}e^{i\psi} & 1\end{bmatrix} = \frac{1}{\sqrt{2}}|\psi\rangle\langle\psi| + \left(\frac{1}{2}-\frac{1}{2\sqrt{2}}\right)\mathbb{1}$

$F = \frac{1}{\sqrt{2}} + \frac{1}{2}\left(1-\frac{1}{\sqrt{2}}\right) = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \frac{\sqrt{2}+1}{2\sqrt{2}} = \frac{2+\sqrt{2}}{4}$ OK.



stany stają się bardziej zmieszane.

Załóżmy że np. klonowanie $|0\rangle$ dla ogóle: $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}|0\rangle\langle 1| + \frac{1}{4}|1\rangle\langle 1|$ $F = \frac{3}{4}$

cc — y ·

@ Atak na protokół BB84

E może użyć optymalnego klonowania
jako atak. Tzn. wtedy ma tam
samą jakość qubit co B czyli,
A i B nie mogą wykryć klona

Jakiem QBER odpowiada to sytuacja

$$\rho_1 = F|\varphi\rangle\langle\varphi| + (1-F)|\varphi+\pi\rangle\langle\varphi+\pi|$$

↑ bit

czyli $QBER = 1-F = \frac{2-\sqrt{2}}{4} = 14{,}6\%$

To jest najwyższy możliwy
atak na pojedynczy qubit ☞