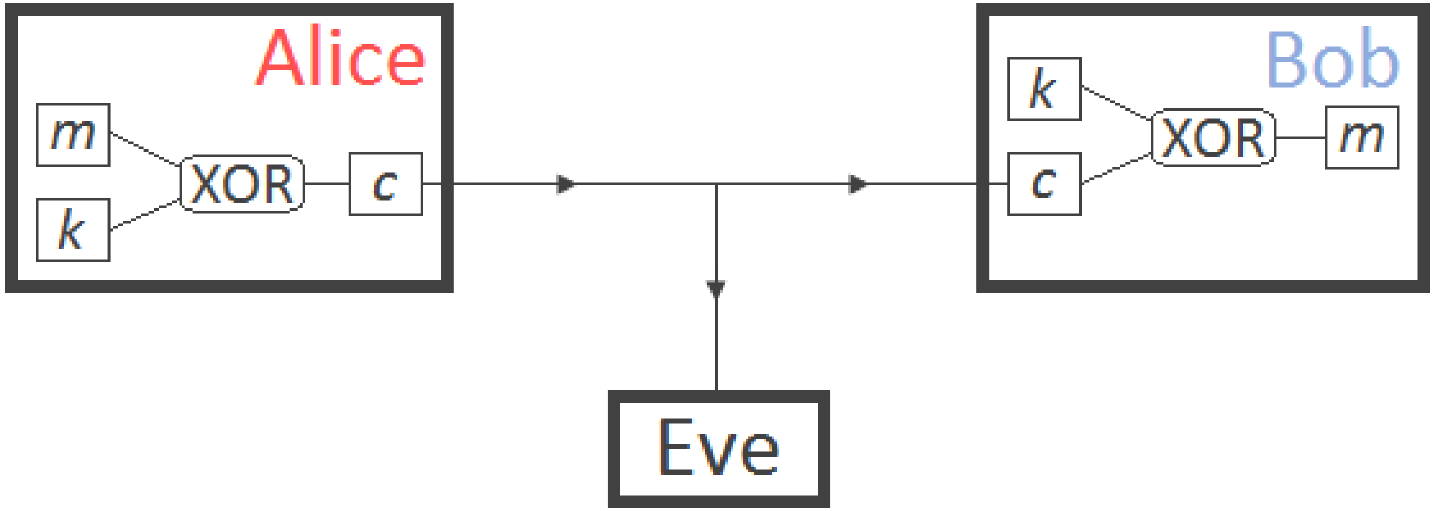
Introduction to Quantum Information and Quantum Machine Learning

Project - class 3

Dr Gustaw Szawioła, docent PUT
D. Sc. Eng. Przemysław Głowacki

1. Protocol E91

Alice want to sent a message to Bob
The information has to be encrypted (plaintext -> ciphertext).



where

$m=(m_1\dots m_n)$ binary string of **plaintext**

$c=(c_1\dots.c_n)$ binary string of **ciphertext**

$k=(k_1\dots k_n)$ binary string of **key**

Question: The main problem – how to distribute the **key?**

Answer: The E91 quantum key distribution protocol.

Quantum entanglement

Entaglement singlet state (one of Bell states):
Two electrons A and B can be prepared in such a state,
Vector $|0\rangle$ and $|1\rangle$ describe the states of each electron with the bit state projection along the positive and negative direction of the *z* axis of Bloch sphere coordination system.

$$\boxed{|\psi\rangle_s = \sqrt{\frac{1}{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right) = \sqrt{\frac{1}{2}}\left(|01\rangle - |10\rangle\right)}$$

The observable of the projection of the bit state onto the direction $\vec{\boldsymbol{n}}$

$$\vec{\boldsymbol{n}} \cdot \vec{\boldsymbol{\sigma}} = \boldsymbol{n_x X} + \boldsymbol{n_y Y} + \boldsymbol{n_z Z},$$

where $\vec{\boldsymbol{\sigma}} = (\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$

$$\boldsymbol{X} = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{1} \\ \boldsymbol{1} & \boldsymbol{0} \end{pmatrix}, \boldsymbol{Y} = \begin{pmatrix} \boldsymbol{0} & -\boldsymbol{i} \\ \boldsymbol{i} & \boldsymbol{0} \end{pmatrix}, \boldsymbol{Z} = \begin{pmatrix} \boldsymbol{1} & \boldsymbol{0} \\ \boldsymbol{0} & -\boldsymbol{1} \end{pmatrix}$$ - Pauli matrices

$$\left\langle (\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})_A \otimes (\vec{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}})_B \right\rangle_{\psi_s} = -\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{b}} \qquad \textbf{(eq. 1)}$$

For two qubits A and B, the observable $(\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})_A \otimes (\vec{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}})_B$ describes the joint measurements of the qubit state projections onto the directions $\vec{\boldsymbol{a}}$ and $\vec{\boldsymbol{b}}$

Alice and Bob measure the qubit state projections of the electron A and B onto the same direction, they will obtain the opposite results. Alice obtain ±1, then Bob get result ∓1, i.e. the results will be perfectly **anticorrelated.** We use ±1 intiger number instead of 0,1 since ±1 are equal to eigenvectors of $\vec{\boldsymbol{n}} \cdot \vec{\boldsymbol{\sigma}}$ matrices.

The formula $\left\langle (\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})_A \otimes (\vec{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}})_B \right\rangle_{\psi_s} = -\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{b}}$ represents expectation value of $(\vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})_A \otimes (\vec{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}})_B$ measurement

CHSH inequality

$$S = \langle \hat{X} \otimes \widehat{W} \rangle \text{-} \langle \hat{X} \otimes \hat{V} \rangle + \langle \hat{Z} \otimes \widehat{W} \rangle + \langle \hat{Z} \otimes \hat{V} \rangle = -2\sqrt{2}$$

Compatible measurements types

Alice Bob

$\vec{a}_2 = \vec{b}_1$ $\widehat{W} \otimes \widehat{W}$

$\vec{a}_3 = \vec{b}_2$ $\hat{Z} \otimes \hat{Z}$

Incompatible measurement types

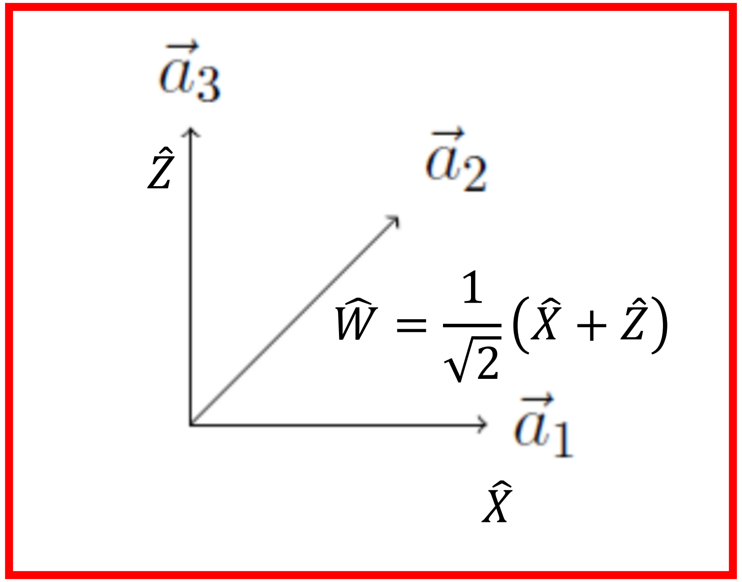
Alice Bob

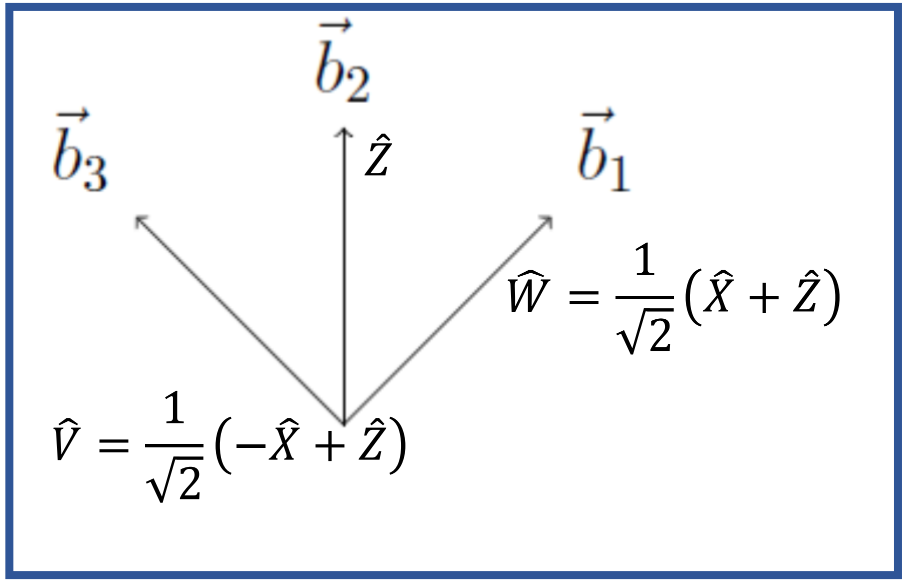
$\vec{a}_1 = \vec{b}_1$ $\hat{X} \otimes \widehat{W}$ $\vec{a}_3 = \vec{b}_1$ $\hat{Z} \otimes \widehat{W}$

$\vec{a}_1 = \vec{b}_3$ $\hat{X} \otimes \hat{V}$ $\vec{a}_3 = \vec{b}_3$ $\hat{Z} \otimes \hat{V}$

$\vec{n}_A \in \{ \vec{a}_1 , \vec{a}_2 , \vec{a}_3\},$

$\vec{n}_B \in \{ \vec{b}_1 , \vec{b}_2 , \vec{b}_3\}$




$\vec{b}_2$
$\vec{b}_3$
$\hat{Z}$
$\vec{b}_1$
$\widehat{W} = \frac{1}{\sqrt{2}}(\hat{X} + \hat{Z})$
$\hat{V} = \frac{1}{\sqrt{2}}(-\hat{X} + \hat{Z})$

$$\langle \hat{X} \otimes \widehat{W} \rangle_{\psi_s} = -\frac{1}{\sqrt{2}}$$

$$\langle \hat{X} \otimes \hat{V} \rangle_{\psi_s} = \frac{1}{\sqrt{2}}$$

$$\langle \hat{Z} \otimes \widehat{W} \rangle_{\psi_s} = -\frac{1}{\sqrt{2}}$$

$$\langle \hat{Z} \otimes \hat{V} \rangle_{\psi_s} = -\frac{1}{\sqrt{2}}$$

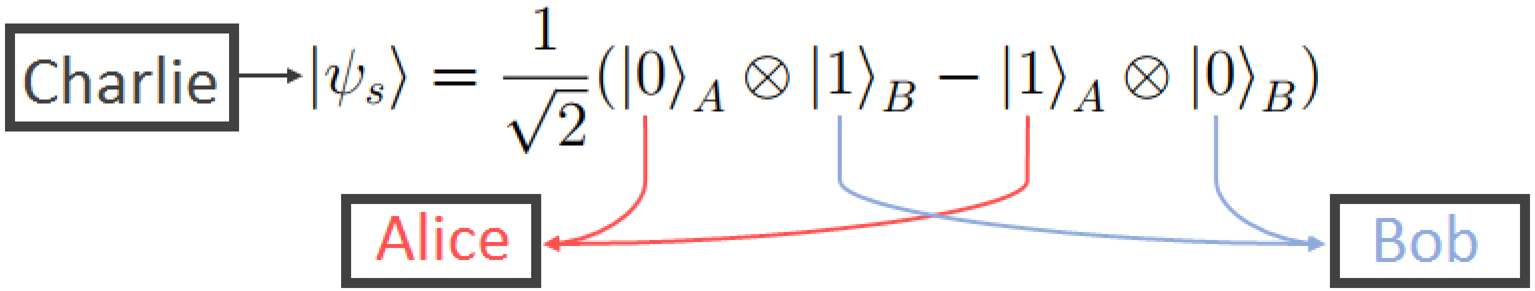
(eq.2)

CHSH inequality

$$S = \langle \hat{X} \otimes \widehat{W} \rangle \text{-} \langle \hat{X} \otimes \hat{V} \rangle + \langle \hat{Z} \otimes \widehat{W} \rangle + \langle \hat{Z} \otimes \hat{V} \rangle = -2\sqrt{2} \qquad \textbf{(eq. 3)}$$

The E91 protocol:

1. Charlie creates N-copies of entangled states $|\psi\rangle_S$ and sent qubits A to Alice and qubits B to Bob



$$|\psi_s\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

The E91 protocol:

2. Alice and Bob generate strings b=(b$_1$…b$_n$) and b’=(b’$_1$ … b’$_n$), where b$_i$, b’$_j$ =1,2,3.

b$_i$=1:	$\vec{a}_1 = (1,0,0)$	**(X observable)**	**b’$_j$=1:**	$\vec{b}_1 = (\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$	**(W observable)**
b$_i$=2:	$\vec{a}_2 = (\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$	**(W observable)**	**b’$_j$=2:**	$\vec{b}_2 = (0,0,1)$	**(Z observable)**
b$_i$=3:	$\vec{a}_3 = (0,0,1)$	**(Z observable)**	**b’$_j$=3:**	$\vec{b}_3 = (-\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$	**(V observable)**

The measurement of the observables $(\vec{a}_i\cdot\vec{\sigma})_A \otimes (\vec{b}_j\cdot\vec{\sigma})_B$ for each singlet state create by Charlie

The E91 protocol:

3. Alice and Bob record the results of their measurements as elements of strings
$a = (a_1 \ldots a_N)$ and $a' = (a'_1 \ldots a'_N)$, respectively where a_i, $a'_j = \pm 1$.
The results of measurements with a quantum computer give us 0 or 1 instead of +1, -1.

4. Alice and Bob using the classical channel compare their strings
$b = (b_1 \ldots b_N)$ and $b' = (b'_1 \ldots b'_N)$.

Alice and Bob tell each other which measurements they have performed during the step 2.
If Alice and Bob have measured the spin projections of the m-th entangled pair of qubits onto the same direction
(ie. $\overrightarrow{a_2}/\overrightarrow{b_1}$ or $\overrightarrow{a_3}/\overrightarrow{b_2}$) they are sure that they obtained opposite results i.e. a_m=-a'_m (see eq. 1 on page 4)
(in binary representation $a_{m,\ binary}=1 \oplus a'_{m,\ binary}$)

Thus, for the *l*-th bit of the key strings $k = (k_1 \ldots k_N)$, $k' = (k'_1 \ldots k'_N)$, Alice and Bob can write $k_l = a_m$, $k'_l = -a'_m$ (see the figure on the next page).

The E91 protocol:

4. Alice and Bob using the classical channel compare their strings *$b = (b_1 \ldots b_N)$ and $b' = (b'_1 \ldots b'_N)$. (continued)*

b=1 $(\hat{X})$

b=2 $(\hat{W})$

b=3 $(\hat{Z})$

$\overrightarrow{a_2}/\overrightarrow{b_1}$ ---> b=2 and b'=1
or
$\overrightarrow{a_3}/\overrightarrow{b_2}$ ---> b=3 and b'=2

b'=1 $(\hat{W})$

b'=2 $(\hat{Z})$

b'=3 $(\hat{V})$

binary k=1 --> 0, k=-1 -->1

Alice

k			-1						1	1					-1
a	1	1	-1	-1	-1	-1	-1	-1	1	1	-1	1	1	-1	-1
b	1	2	2	1	3	2	2	1	3	3	1	1	2	2	3

$(\vec{a}_1 \cdot \vec{\sigma})$

$(\vec{b}_2 \cdot \vec{\sigma})$

Bob

b'	2	3	1	2	3	2	2	3	2	2	1	2	2	3	2
a'	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	-1	1
k'			1						1	1					-1

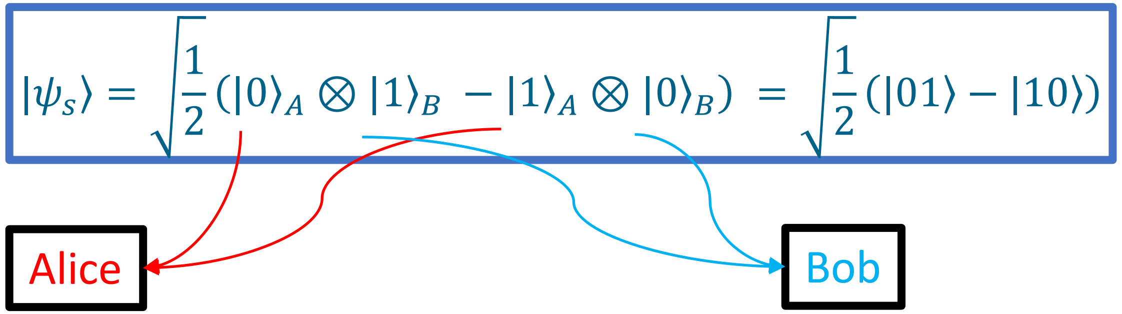
binary k'=1 --> 0, k'=-1 -->1

The E91 protocol:

5. Using the results obtained after measuring the qubit state projections onto the $\overrightarrow{a_1}/\overrightarrow{b_1}$, $\overrightarrow{a_1}/\overrightarrow{b_3}$, $\overrightarrow{a_3}/\overrightarrow{b_1}$ and $\overrightarrow{a_3}/\overrightarrow{b_3}$ directions (observables eq.2 page 5), Alice and Bob calculate the CHSH correlation value (eq.3 page 6).

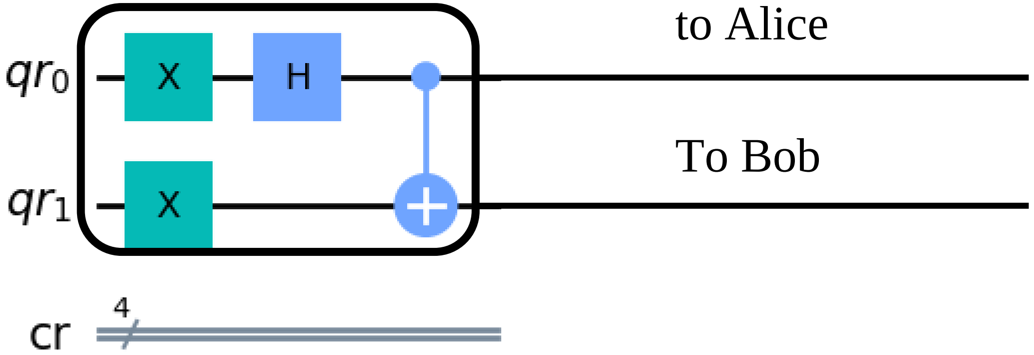
If $S = -2\sqrt{2}$, then Alice and Bob can be sure that the states they had been receiving from Charlie were entangled indeed. This fact tells the participants that there was no interference in the quantum channel.

Task 1. Charlie creates singlet states $|\psi_s\rangle$, qubits q_0 and q_1 are now entangled, and sent q_0 to Alice and q_1 to Bob, (shots=1, N_{singlets}=1024)

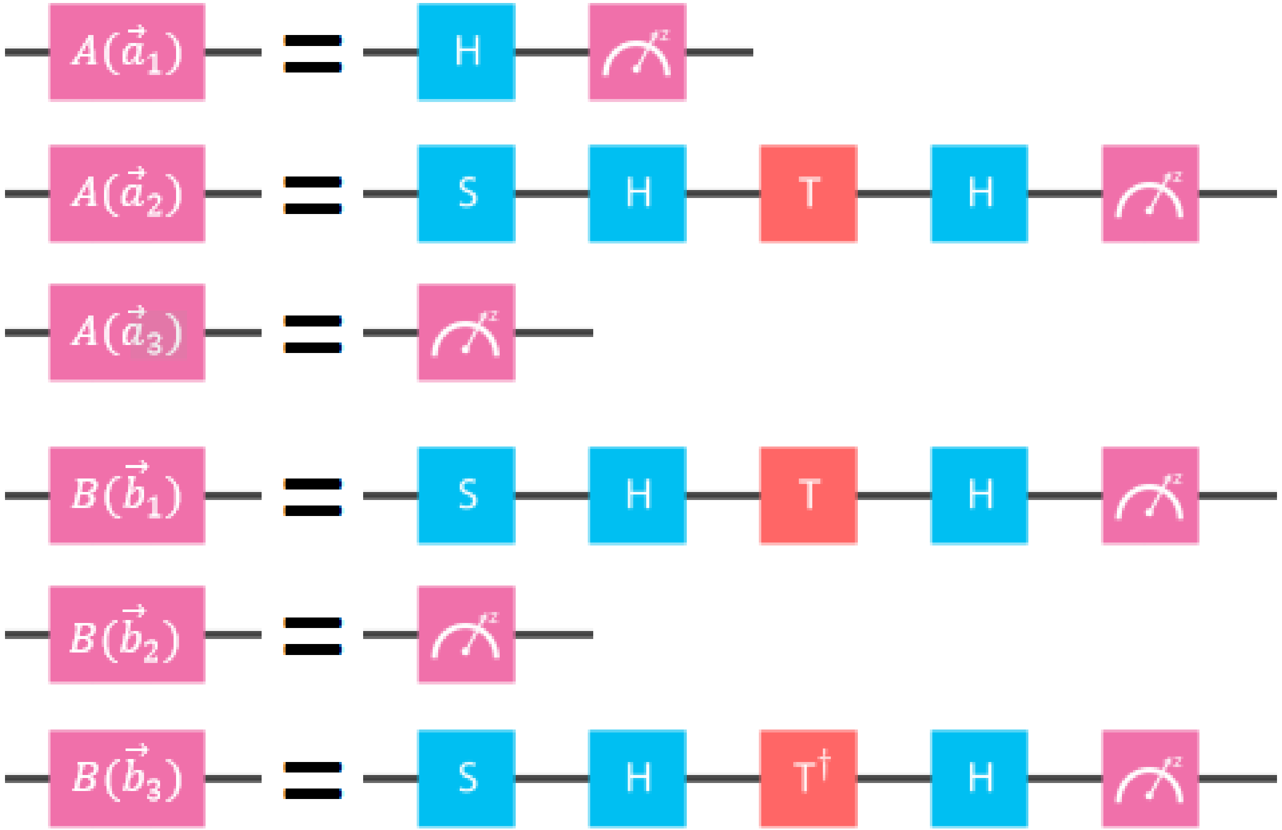


$$|\psi_s\rangle = \sqrt{\frac{1}{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right) = \sqrt{\frac{1}{2}}\left(|01\rangle - |10\rangle\right)$$

Charlie’s singlet
Preparation device



Task 2. Measuring



b

$\hat{X}$ 1

$\hat{W}$ 2 Alice

$\hat{Z}$ 3

$\hat{W}$ 1

$\hat{Z}$ 2 Bob

$\hat{V}$ 3

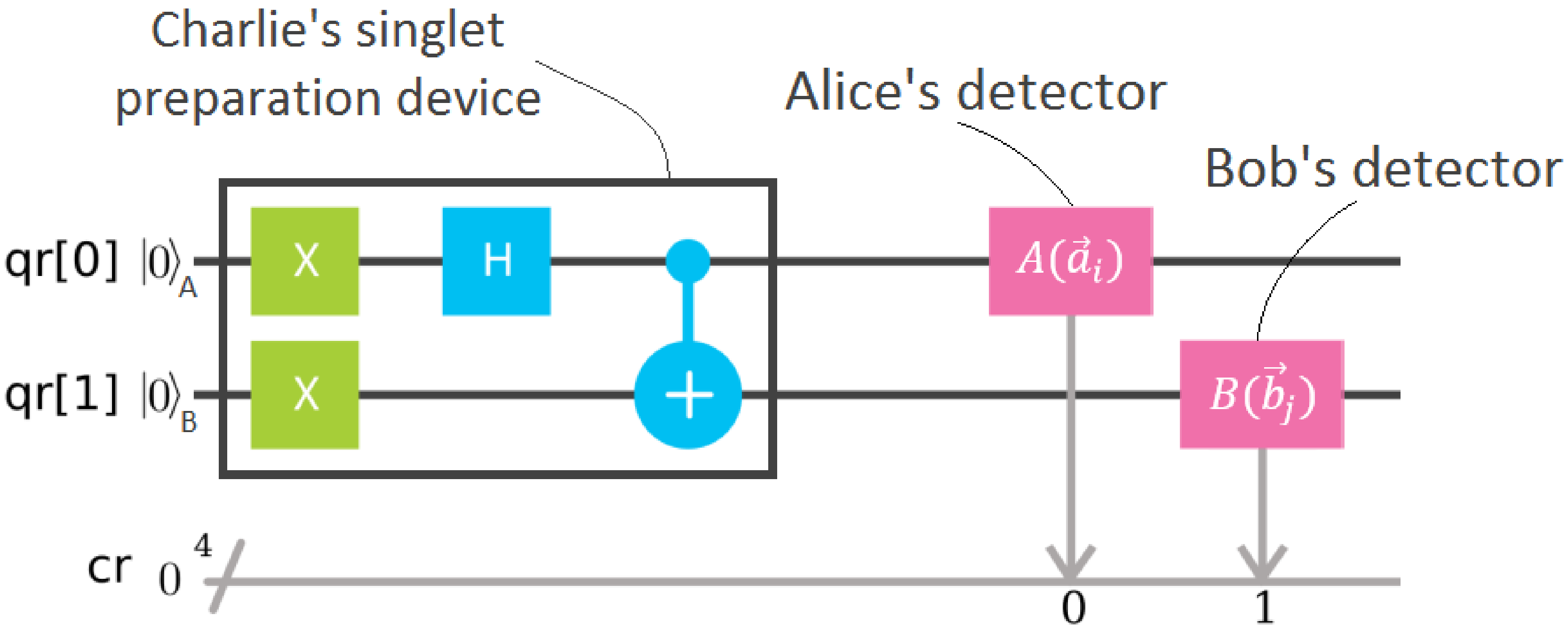
b’

Task 2. Measuring (continued)

Alice and Bob want to generate a secret key using N (=1024) singlet states prepared by Charlie

Alice and Bob create the strings *b* and *b’* with randomly generated elements.

You need to combine Charlie’s device and Alice’s and Bob’s detectors into one circuit.



The idea is to model every act of the creation of the singlet state, the distribution of its qubits among the participants and the measurement of the spin projection onto the chosen direction in the E91 protocol by executing each circuit from the *circuits* list with one shot.

Task 3. Recoding the results

cr[3210]

1. Example of result after execute the first measurement {’0011’: 1}

It consists of four digits. Recall that Alice and Bob store the results of the measurement in classical bits *cr[0]* and *cr[1]* (two digits on the right). Since we model the secret key generation process without the presence of an eavesdropper, the classical bits *cr[2]* and *cr[3]* are always 0.

Alice and Bob record the results of their measurements as bits of the strings *a* and *a’*.

Task 4. Revealing the bases

1. Now the participants compare their strings *b* and *b'* via the public classical channel.

If Alice and Bob have measured the spin projections of their qubits of the *i*-th singlet onto the same direction, then Alice records the result a_i as the bit of the string *k*, and Bob records the result $-a_i$ as the bit of the string *k'* (see eq. (1) page4).

It is important for Alice and Bob to have the same keys, i.e. strings *k* and *k'* must be equal.
It is good to check the number of mismatches bits in the keys (supposed to be zero)

Task 5. CHSH correlation value test

Alice and Bob have to calculate the CHSH correlation value (eq. 3) using the results obtained after the measurements of spin projections onto the $\overrightarrow{a_1}/\overrightarrow{b_1}$, $\overrightarrow{a_1}/\overrightarrow{b_3}$, $\overrightarrow{a_3}/\overrightarrow{b_1}$ and $\overrightarrow{a_3}/\overrightarrow{b_3}$ directions. Recall that it is equivalent to the measurement of the observables X⊗W, X⊗V, Z⊗W and Z⊗V respectively.

$$\langle A \otimes B \rangle_{\psi_s} = \sum_{j,k} a_j b_k P_\psi\left(A\middle|= a_j, B\middle| = b_k\right) = \sum_{j,k} a_j b_k P_\psi\left(a_j, b_k\right) \qquad \textbf{(eq. 4)}$$

Note that if A and B are the bit state projection observables, then the corresponding eigenvalues are a_j, b_k *=±1, so*

$$\langle A(a_i) \otimes B(b_k) \rangle = P(-1,-1) - P(1,-1) - P(-1,1) + P(1,1) \qquad \textbf{(eq. 5)}$$

$$P(a_i, b_k) = \frac{n_{a_i,b_k}(A \otimes B)}{N(A \otimes B)} \qquad \textbf{(eq. 6)}$$

Since Alice and Bob revealed their strings *b* and *b'*, they know what measurements they performed and what results they have obtained. With this data, participants calculate the expectation values (**eq.2** page5) using (**eq.5**) and (**eq.6**).

Task 5. CHSH correlation value test (continued)

To get quantum key

$\overrightarrow{a_2}/\overrightarrow{b_1}$ ---> b=2 and b’=1

$\overrightarrow{a_3}/\overrightarrow{b_2}$ ---> b=3 and b’=2

Check CHSH

$\overrightarrow{a_1}/\overrightarrow{b_1}$ ---> b=1 and b’=1

$\overrightarrow{a_1}/\overrightarrow{b_3}$ ---> b=1 and b’=3

$\overrightarrow{a_3}/\overrightarrow{b_1}$ ---> b=3 and b’=1

$\overrightarrow{a_3}/\overrightarrow{b_3}$ ---> b=3 and b’=3

binary k=1 --> 0, k=-1 -->1

Alice

$(\vec{a}_1 \cdot \vec{\sigma})$

k			-1						1	1					-1
a	1	1	-1	-1	-1	-1	-1	-1	1	1	-1	1	1	-1	-1
b	1	2	2	1	3	2	2	1	3	3	1	1	2	2	3
b’	2	3	1	2	3	2	2	3	2	2	1	2	2	3	2
a’	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	-1	1
k’			1						1	1					-1

$(\vec{b}_2 \cdot \vec{\sigma})$

Bob

binary k’=1 --> 0, k’=-1 -->1

Task 5. CHSH correlation value test (continued)

Measur. type	Measur. type	N_{jk} (of 1024)	(a,a')	$n_{jk}(a,a')$	$p_{jk}(a,a')=n_{jk}(a,a')/N_{jk}$	$p_{jk}(a,a')*(a*a')$	$\langle \hat{A} \otimes \hat{B} \rangle = \sum_{a,a'} p_{jk}(a,a')*(a*a')$
$\vec{a}_j = \vec{b}_k$							
$\vec{a}_1 = \vec{b}_1$	$\hat{X} \otimes \widehat{W}$	123	(1,1) (1,-1) (-1,1) (-1,-1)	9 54 52 8	9/123 54/123 52/123 8/123	(9/123)*(1*1) (54/123)*(1*(-1)) (52/123)*((-1)*1) (8/123)*((-1)*(-1))	9/123 – 54/123 – 52/123 +8/123
$\vec{a}_1 = \vec{b}_3$	$\hat{X} \otimes \hat{V}$	104	(1,1) (1,-1) (-1,1) (-1,-1)				
$\vec{a}_3 = \vec{b}_1$	$\hat{Z} \otimes \widehat{W}$	122	(1,1) (1,-1) (-1,1) (-1,-1)				
$\vec{a}_3 = \vec{b}_3$	$\hat{Z} \otimes \hat{V}$	111	(1,1) (1,-1) (-1,1) (-1,-1)				

Task 6. Results

1) Obtain the list of secret key by Alice list(a) and Bob list(a’), number of elements in each list has to be the same
2) Check if the list(a) and list(a’) possess some mismatching bits (if there is low noise in the system No of mismatching bits=0)
3) make the CHSH test:

   $\langle \hat{X} \otimes \hat{W} \rangle$,$\langle \hat{X} \otimes \hat{V} \rangle$, $\langle \hat{Z} \otimes \hat{W} \rangle$,$\langle \hat{Z} \otimes \hat{V} \rangle$

   1) make a list of the type of measurements (b,b’): (1,1), (1,3), (3,1), (3,3)
   2) Check the number of results for each type of measurements (b,b’): there are (a,a’): (1,1), (1,-1),(-1,1) and (-1,-1)
   3) Calculate $\langle \hat{X} \otimes \hat{W} \rangle = \sum_{a,a'} p_{jk}(a,a')*(a*a')$ *for each type of measurements*
   4) calculates CHSH correlation value : S=$\langle \hat{X} \otimes \hat{W} \rangle$- $\langle \hat{X} \otimes \hat{V} \rangle$+ $\langle \hat{Z} \otimes \hat{W} \rangle$ + $\langle \hat{Z} \otimes \hat{V} \rangle$=$-2\sqrt{2}$

POLITECHNIKA POZNAŃSKA
POZNAN UNIVERSITY OF TECHNOLOGY

THE END