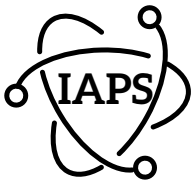
Lecture 18

QUANTUM CRYPTOGRAPHY. PART 3 - Quantum key distribution

of the course "Fundamentals of Quantum Computing"

(by IAPS *and* QUANTERALL*)*

Stoyan Mishev



INSTITUTE *for* ADVANCED
PHYSICAL STUDIES

NEW
BULGARIAN
UNIVERSITY

October 14, 2022

Plan

Encryption basics

Quantum encryption without entanglement

Quantum encryption with entanglement

Qiskit code

The Nobel Prize in Physics 2022

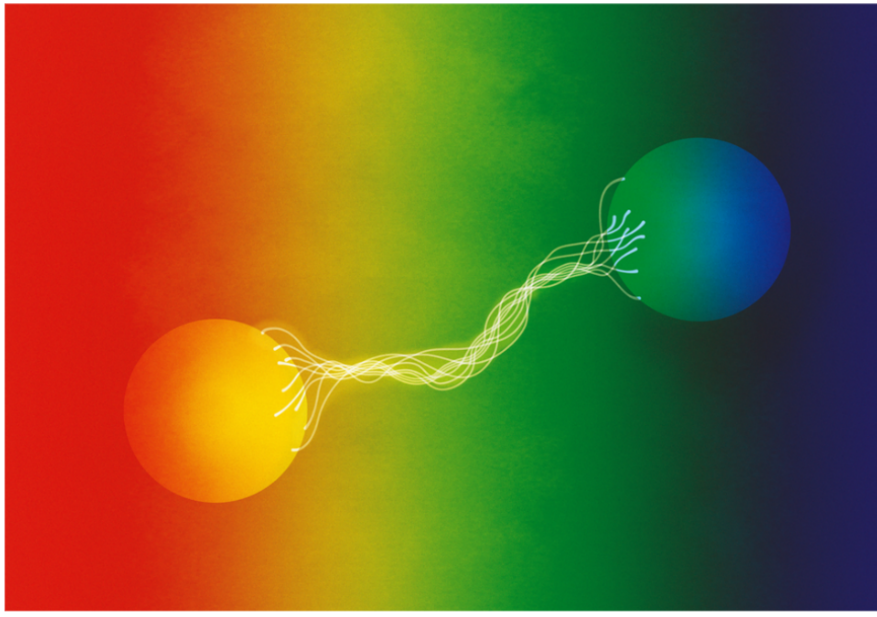
How entanglement has become a powerful tool

Using groundbreaking experiments, Alain Aspect, John Clauser and Anton Zeilinger have demonstrated the potential to investigate and control particles that are in entangled states. What happens to one particle in an entangled pair determines what happens to the other, even if they are really too far apart to affect each other. The laureates' development of experimental tools has laid the foundation for a new era of quantum technology.

Related articles

Press release: The Nobel Prize in Physics 2022
Popular information: How entanglement has become a powerful tool

https://www.nobelprize.org/prizes/physics/



if K is a **key** and M is a **message**, encryption can be seen as

if K is a **key** and M is a **message**, encryption can be seen as

$$e : K \times M \to C$$

where C is the encrypted message.

if K is a **key** and M is a **message**, encryption can be seen as

$$e : K \times M \to C$$

where C is the encrypted message.
Decryption will then be:

$$d : K \times C \to M$$

if K is a **key** and M is a **message**, encryption can be seen as

$$e : K \times M \to C$$

where C is the encrypted message.
Decryption will then be:

$$d : K \times C \to M$$

Notes

- if K is the same for encr. and decr. the cipher is **symmetric**

if K is a **key** and M is a **message**, encryption can be seen as

$$e : K \times M \to C$$

where C is the encrypted message.
Decryption will then be:

$$d : K \times C \to M$$

Notes

- if K is the same for encr. and decr. the cipher is **symmetric** and **asymmetric** otherwise;
- $d(k, e(k, m)) = m$.

Example - VERNAN crypting code

A message m can be presented by a series of digits m_j:

$$m = \sum_{j=0}^{n_M - 1} m_j 2^j.$$

Example - VERNAN crypting code

A message m can be presented by a series of digits m_j:

$$m = \sum_{j=0}^{n_M - 1} m_j 2^j.$$

The VERNAN encryption is

$$e(k, m) = (k_{n-1} \overset{2}{\oplus} m_{n-1}, ..., k_0 \overset{2}{\oplus} m_0)$$

Example - VERNAN crypting code

A message m can be presented by a series of digits m_j:

$$m = \sum_{j=0}^{n_M-1} m_j 2^j.$$

The VERNAN encryption is

$$e(k,m) = (k_{n-1} \overset{2}{\oplus} m_{n-1}, ..., k_0 \overset{2}{\oplus} m_0)$$

Encryption	Message	$m =$	0	0	1	0	1	1	0	1
			$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$
	Key	$k =$	1	0	0	1	1	0	0	0
	Ciphertext	$c = e(k,m) =$	1	0	1	1	0	1	0	1
Decryption	Ciphertext	$c =$	1	0	1	1	0	1	0	1
			$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$
	Key	$k =$	1	0	0	1	1	0	0	0
	Message	$m =$	0	0	1	0	1	1	0	1

Example - VERNAN (de)crypting code

Encryption	Message	$m =$	0	0	1	0	1	1	0	1
			$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$
	Key	$k =$	1	0	0	1	1	0	0	0
	Ciphertext	$c = e(k,m) =$	1	0	1	1	0	1	0	1
Decryption	Ciphertext	$c =$	1	0	1	1	0	1	0	1
			$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$	$\overset{2}{\oplus}$
	Key	$k =$	1	0	0	1	1	0	0	0
	Message	$m =$	0	0	1	0	1	1	0	1

The VERNAN decryption is

$$
\begin{aligned}
& d(k, e(k,m)) = \\
& = (k_{n-1} \overset{2}{\oplus} k_{n-1} \overset{2}{\oplus} m_{n-1}, \ldots, k_0 \overset{2}{\oplus} k_0 \overset{2}{\oplus} m_0) \\
& = (m_{n-1}, \ldots, m_0) \equiv m
\end{aligned}
$$

$(k_j \overset{2}{\oplus} k_j = 0)$

Quantum encryption without entanglement

Theoretical Computer Science 560 (2014) 7–11

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum cryptography: Public key distribution and coin tossing ☆

Charles H. Bennett [a], Gilles Brassard [b]

[a] *IBM Research, Yorktown Heights NY 10598, USA*
[b] *Département IRO, Université de Montréal, Montréal, QC, H3C 3J7 Canada*

C.H. Bennett, G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (New York, 1984)

No spies!

- generate a random bit sequence (the key) which is only known to Alice and Bob
- A. and B. can tell if the key was listened to (eavesdropped).

No spies!

- generate a random bit sequence (the key) which is only known to Alice and Bob
- A. and B. can tell if the key was listened to (eavesdropped).

A. has many qubits and she *randomly* applies σ_z or σ_x to them.

No spies!

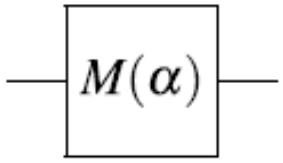
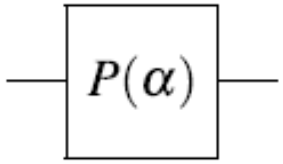
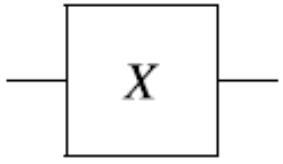
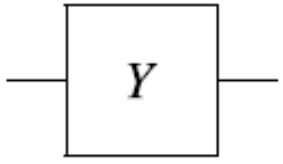
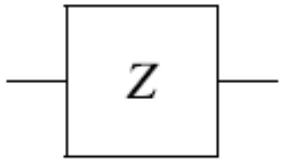
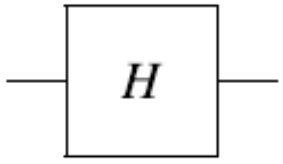
- generate a random bit sequence (the key) which is only known to Alice and Bob
- A. and B. can tell if the key was listened to (eavesdropped).

A. has many qubits and she *randomly* applies σ_z or σ_x to them. A. sends the qubits to B. who also *randomly* applies σ_z or σ_x to them.

No spies!

- generate a random bit sequence (the key) which is only known to Alice and Bob
- A. and B. can tell if the key was listened to (eavesdropped).

A. has many qubits and she *randomly* applies σ_z or σ_x to them.
A. sends the qubits to B. who also *randomly* applies σ_z or σ_x to them.
A. and B. exchange info via *a public channel* for (the indices of) the qubits measured with the same operator, i.e. the same corresponding σ_z and σ_x which should give the same eigenvalues. They exchange a subset of same- and not same-operator measured results and compare. If they the results are consistent then the transmission is not eavesdropped:

Identity		$\mathbf{1}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Phase-factor		$M(\alpha) := \mathrm{e}^{\mathrm{i}\alpha}\mathbf{1}$	$\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\alpha} \end{pmatrix}$
Phase-shift		$P(\alpha) := \|0\rangle\langle 0\| + \mathrm{e}^{\mathrm{i}\alpha}\|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\alpha} \end{pmatrix}$
PAULI-X or Q-NOT		$X := \sigma_x$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
PAULI-Y		$Y := \sigma_y$	$\begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$
PAULI-Z		$Z := \sigma_z$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
HADAMARD		$H := \frac{\sigma_x+\sigma_z}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

For qubit no.	1	2	3	4	5	6	7	8	9	10	11	12	...
	Alice chooses randomly one of the observables σ_z or σ_x. Suppose she measures												
Alice's observable	σ_x	σ_x	σ_x	σ_z	σ_x	σ_x	σ_x	σ_z	σ_z	σ_x	σ_x	σ_z	...
	and observes												
Alice's value	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	$+1$	$+1$	$+1$	$+1$	...
	The qubit is then in the												
qubit state	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	...
	Alice sends the qubits thus prepared to Bob. He chooses for each qubit												

Alice sends the qubits thus prepared to Bob. He chooses for each qubit randomly one of the observables σ_z or σ_x. Suppose he measures

Bob's observable	σ_z		σ_x		σ_z		σ_z		σ_x		σ_z		σ_z		σ_x		σ_x		σ_z		σ_z	$\ldots$

and observes

Bob's value	-1		-1		-1		$+1$		$+1$		-1		$+1$		-1		$+1$		$+1$		-1	$\ldots$

Alice and Bob publicly compare for which qubit they have measured which observable. But they do not reveal the outcome of the measurement, that is, the observed value. They thus divide the qubits into a set where they chose either the same observable or different ones. Measured

observables were	$\neq$		$=$		$\neq$		$=$		$\neq$		$=$		$\neq$		$=$		$\neq$		$=$		$\neq$	$\ldots$

observables were	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$\ldots$

If they have chosen the same observable, their measured values have to agree. As a control they compare publicly every second of the observed values where they measured the same observable:

control-value Alice			$+1$			-1					$+1$	$\ldots$		
control-value Bob			$+1$			-1					$+1$	$\ldots$		

100% agreement in comparison of control values implies:
with a probability increasing with the number of control values the qubits have *not been read* between the measurements by Alice and Bob.
Use the observed values in the remaining cases where both measured the same observable as *joint, secret*, and *random*

bit sequence:	$\mathbf{-1}$			$\mathbf{-1}$					$\mathbf{+1}$			$\ldots$		

With spies!

The spy is called Eve (E.) .

For qubit no.	1	2	3	4	5	6	7	8	9	10	11	12	...
	Alice randomly selects one of the observables σ_z or σ_x and measures												
Alice's observable	σ_x	σ_x	σ_x	σ_z	σ_x	σ_x	σ_x	σ_z	σ_z	σ_x	σ_x	σ_z	...
	and observes												
Alice's value	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	$+1$	$+1$	$+1$	$+1$	...
	The qubit is then in the												
qubit state	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	...

Alice sends the thus prepared qubits to Bob. Eve intercepts the qubit,

With spies!

Alice sends the thus prepared qubits to Bob. Eve intercepts the qubit, but does not know, in which state it is. Thus, Eve measures

Eve's observable	σ_z	σ_x	σ_x	σ_z	σ_z	σ_x	σ_z	σ_x	σ_x	σ_x	σ_z	σ_z	$\ldots$

and observes

Eve's value	-1	-1	-1	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	$+1$	$+1$	$\ldots$

The qubit is then in the

qubit state	$\lvert\downarrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\downarrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{x}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\lvert\uparrow_{\hat{\mathbf{z}}}\rangle$	$\ldots$

and is passed on from Eve to Bob. He randomly selects one of the observables σ_z or σ_x and measures

Bob's observable	σ_z	σ_x	σ_z	σ_z	σ_z	σ_x	σ_z	σ_z	σ_x	σ_x	σ_z	σ_z	$\ldots$

He observes

Bob's value	-1	-1	-1	$+1$	-1	-1	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$\ldots$

With spies!

He observes

Bob's value	-1	-1	-1	$+1$	-1	-1	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	…

Alice and Bob publicly compare for which qubit they have measured which observable. But they do not reveal the outcome of the measurement, that is, the observed value. They thus divide the qubits into a set where they chose either the same observable or different ones. Measured

observables were	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	$\neq$	$=$	…

If they have chosen the same observable, their measured values have to agree and as a control they compare publicly every second of the observed values where they measured the same observable:

control-value Alice			$+1$				-1					$+1$	…
control-value Bob			$+1$				$+1$					$+1$	…

33% disagreement in the control values implies eavesdropping.
Discard all qubits sent and start all over with a new sequence.

Quantum encryption with entanglement

A. Ekert, Phys. Rev. Lett. 67, 661 (1991)

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \;=\; \frac{1}{\sqrt{2}}(|\uparrow_{\hat{\mathbf{n}}}\rangle \otimes |\downarrow_{\hat{\mathbf{n}}}\rangle - |\downarrow_{\hat{\mathbf{n}}}\rangle \otimes |\uparrow_{\hat{\mathbf{n}}}\rangle)$$

One of the qubits belongs to Alice and the other one belongs to Bob. They need to exchange a crypting key. Alice measures $\sum_{n^A}^{A} = n^A.\sigma$ where n^A is one of the directions $\{n^1, n^2, n^4\}$ $\{n^1, n^2, n^4\}$. For each qubit she applies a randomly chosen n^i.

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|\uparrow_{\hat{\mathbf{n}}}\rangle \otimes |\downarrow_{\hat{\mathbf{n}}}\rangle - |\downarrow_{\hat{\mathbf{n}}}\rangle \otimes |\uparrow_{\hat{\mathbf{n}}}\rangle)$$

One of the qubits belongs to Alice and the other one belongs to Bob. They need to exchange a crypting key. Alice measures $\sum_{n^A}^{A} = n^A.\sigma$ where n^A is one of the directions $\{n^1, n^2, n^4\}$ $\{n^1, n^2, n^4\}$. For each qubit she applies a randomly chosen n^i. Bob does the same but applies randomly $\{n^2, n^3, n^4\}$ to $\sum_{n^B}^{B} = n^B.\sigma$.

$$\hat{\mathbf{n}}^i = \begin{pmatrix} \cos \nu_i \\ 0 \\ \sin \nu_i \end{pmatrix} \in S^1_{\mathbb{R}^3} \quad \text{for } i \in \{1, \ldots, 4\}$$

$$\nu_1 = \frac{3\pi}{4} \qquad \nu_2 = \frac{\pi}{2} \qquad \nu_3 = 0 \qquad \nu_4 = \frac{\pi}{4}$$

B. and A. inform each other via a public channel which directions n^A and n^B they used. However, they keep the observed values, that is, the measurement results, secret!

qubit-pair no.	Alice measures $\Sigma^A_{\hat{\mathbf{n}}^A}$ in direction $\hat{\mathbf{n}}^A =$ $\hat{\mathbf{n}}^1$	$\hat{\mathbf{n}}^2$	$\hat{\mathbf{n}}^4$	Bob measures $\Sigma^A_{\hat{\mathbf{n}}^B}$ in direction $\hat{\mathbf{n}}^B =$ $\hat{\mathbf{n}}^3$	$\hat{\mathbf{n}}^2$	$\hat{\mathbf{n}}^4$
1			+1			−1
2		−1			+1	
3	+1				−1	
4			−1		−1	
5		+1			−1	
6	−1					−1
7	+1				−1	
8			+1			−1
9	−1					+1
10			−1			+1
11		+1		+1		
12	−1			−1		
13	−1				+1	
14			+1			−1
15	+1				−1	
16	−1			−1		
17	−1				+1	
18	+1			−1		
19	+1				+1	
20	−1			−1		
21		−1			+1	
22			+1	−1		
23		+1				−1
24		−1		−1		
25	−1					+1
26			−1	+1		
27			+1	−1		
28		−1				−1
29			−1	+1		
30	+1			+1		
31		−1			+1	
32			−1		+1	
33			+1		−1	
34		−1		+1		
35	+1			+1		
36	−1					−1
37			−1		+1	
38		+1			−1	
39			−1	+1		
40			−1	−1		
41			+1			−1
42		+1			−1	
43			−1		+1	
44			+1	−1		
45	+1					−1
46	−1					−1
47		−1				+1
48		+1		+1		
49		−1				+1
50			+1		−1	
51		+1				−1
52		−1			+1	
53			−1			+1
54		+1		−1		
55	+1				−1	
56	−1					+1
57		−1		−1		
58			+1		−1	
59		−1		+1		
60		+1				−1
61		+1				−1
62			+1			−1
63	+1			+1		

Two sets of measurements depending on the directions

- one set, where they happened to have measured in the same direction $n^A = n^2 = n^B$ or $n^A = n^4 = n^B$. In this case A. and B. will have opposite values of the measurements.
- a set, where they happened to have measured in different directions $n^A \neq n^B$. In this case not only the directions but also the values $s^X_{n_i}$ ($X \in \{A, B\}$ and $n_i \in \{1, ..., 4\}$) are exchanged.

In case of eavesdropping the composite system will be in a separable state $|\phi\rangle \otimes |\psi\rangle$ before Alice and Bob perform their measurements.

In case of eavesdropping the composite system will be in a separable state $|\phi\rangle \otimes |\psi\rangle$ before Alice and Bob perform their measurements. In such a state the following statement holds:

Proposition 4.8 *In any separable state* $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ *the expectation values of spin-observables* $\Sigma^A_{\hat{\mathbf{n}}^i} \otimes \Sigma^B_{\hat{\mathbf{n}}^i}$ *in arbitrary spin-directions* $\hat{\mathbf{n}}^i$ *with* $i \in \{1,\ldots,4\}$ *satisfy the CHSH variant of the* BELL *inequality, that is,*

$$\left| \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} - \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} \right| \leq 2$$

In case of eavesdropping the composite system will be in a separable state $|\phi\rangle \otimes |\psi\rangle$ before Alice and Bob perform their measurements. In such a state the following statement holds:

Proposition 4.8 *In any separable state* $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ *the expectation values of spin-observables* $\Sigma^A_{\hat{\mathbf{n}}^i} \otimes \Sigma^B_{\hat{\mathbf{n}}^i}$ *in arbitrary spin-directions* $\hat{\mathbf{n}}^i$ *with* $i \in \{1,\ldots,4\}$ *satisfy the CHSH variant of the* BELL *inequality, that is,*

$$\left| \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} - \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} \right| \leq 2$$

$$\overline{\Sigma^A_{\hat{\mathbf{n}}^i} \Sigma^B_{\hat{\mathbf{n}}^j}} = \frac{1}{N^{A,B}_{i,j}} \sum_{l \in M^{A,B}_{i,j}} s^A_{\hat{\mathbf{n}}^i}(l) s^B_{\hat{\mathbf{n}}^j}(l)$$

In case of eavesdropping the composite system will be in a separable state $|\phi\rangle \otimes |\psi\rangle$ before Alice and Bob perform their measurements. In such a state the following statement holds:

Proposition 4.8 *In any separable state* $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ *the expectation values of spin-observables* $\Sigma^A_{\hat{\mathbf{n}}^i} \otimes \Sigma^B_{\hat{\mathbf{n}}^i}$ *in arbitrary spin-directions* $\hat{\mathbf{n}}^i$ *with* $i \in \{1,\ldots,4\}$ *satisfy the CHSH variant of the* BELL *inequality, that is,*

$$\left| \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} - \left\langle \Sigma^A_{\hat{\mathbf{n}}^1} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^2} \right\rangle_{\varphi\otimes\psi} + \left\langle \Sigma^A_{\hat{\mathbf{n}}^4} \otimes \Sigma^B_{\hat{\mathbf{n}}^3} \right\rangle_{\varphi\otimes\psi} \right| \leq 2$$

$$\overline{\Sigma^A_{\hat{\mathbf{n}}^i} \Sigma^B_{\hat{\mathbf{n}}^j}} = \frac{1}{N^{A,B}_{i,j}} \sum_{l \in M^{A,B}_{i,j}} s^A_{\hat{\mathbf{n}}^i}(l) s^B_{\hat{\mathbf{n}}^j}(l)$$

If $\left| \overline{\Sigma^A_{\hat{\mathbf{n}}^1} \Sigma^B_{\hat{\mathbf{n}}^2}} - \overline{\Sigma^A_{\hat{\mathbf{n}}^1} \Sigma^B_{\hat{\mathbf{n}}^3}} + \overline{\Sigma^A_{\hat{\mathbf{n}}^4} \Sigma^B_{\hat{\mathbf{n}}^2}} + \overline{\Sigma^A_{\hat{\mathbf{n}}^4} \Sigma^B_{\hat{\mathbf{n}}^3}} \right| \approx 2\sqrt{2} \quad \Rightarrow \quad$ exchange is secure,

if $\left| \overline{\Sigma^A_{\hat{\mathbf{n}}^1} \Sigma^B_{\hat{\mathbf{n}}^2}} - \overline{\Sigma^A_{\hat{\mathbf{n}}^1} \Sigma^B_{\hat{\mathbf{n}}^3}} + \overline{\Sigma^A_{\hat{\mathbf{n}}^4} \Sigma^B_{\hat{\mathbf{n}}^2}} + \overline{\Sigma^A_{\hat{\mathbf{n}}^4} \Sigma^B_{\hat{\mathbf{n}}^3}} \right| \leq 2 \quad \Rightarrow \quad$ eavesdropping has occurred.

https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html

NEXT LECTURE

OCTOBER 21, 2022

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!