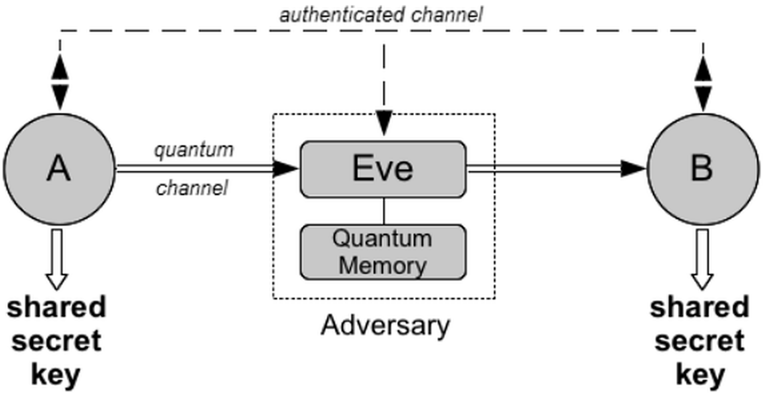
Fully device independent quantum key distribution

Thomas Vidick, Umesh Vazirani

Presented by: Hasan Iqbal

July 11, 2020

What is Quantum Key Distribution(QKD)



QKD in Practice

IDQuantique, Switzerland

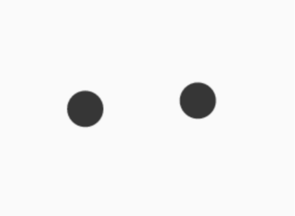
Toshiba, Japan

Qubittek, USA

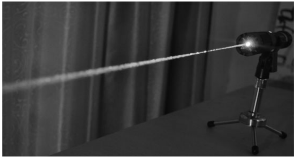
Why Device Independence (DI)

Practical implementation creates vulnerability, which are hard to defend against. Example:

Photon number splitting attack



Laser damage attack



DI Assumptions

- Alice and Bob can not signal to each other.
- They have access to a trusted RNG.
- Communication channel between them is authenticated.
- Quantum physics is correct.

Note that, the devices are fully uncharacterized. If asked to measure in Z basis, it may very well measure in the X basis.

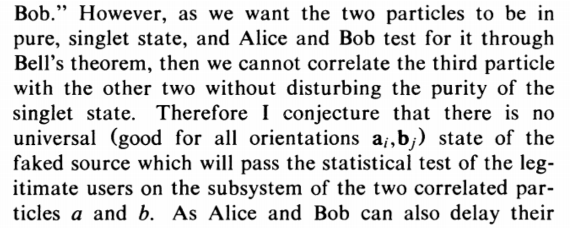
(Mayers and Yao, 98) [1]

DI Challenge

Can security be guaranteed by the input-output behavior of the devices alone?

Hint of an answer

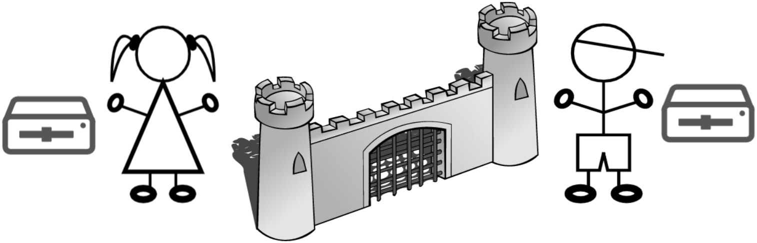
Ekert's E91 paper [2] had the following:

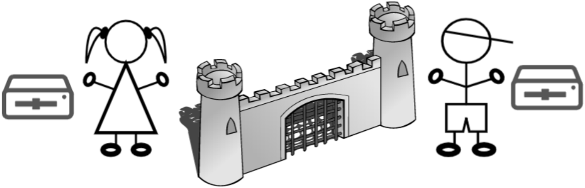


Bob." However, as we want the two particles to be in pure, singlet state, and Alice and Bob test for it through Bell's theorem, then we cannot correlate the third particle with the other two without disturbing the purity of the singlet state. Therefore I conjecture that there is no universal (good for all orientations $\mathbf{a}_i, \mathbf{b}_j$) state of the faked source which will pass the statistical test of the legitimate users on the subsystem of the two correlated particles a and b. As Alice and Bob can also delay their

Complete answer

After a series of papers, Vazirani and Vidick in 2014 proved the general security on a variant of E91 protocol [3].





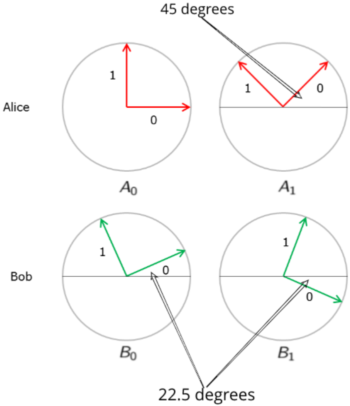
x	y	a	b	$x \wedge y$	$a \oplus b$
0	0			0	
0	1			0	
1	0			0	
1	1			1	

$$a \oplus b = x \wedge y$$

x	y	a	b	$x \wedge y$	$a \oplus b$
0	0	0	0	0	0
0	1	0	0	0	0
1	0	0	0	0	0
1	1	0	0	1	0

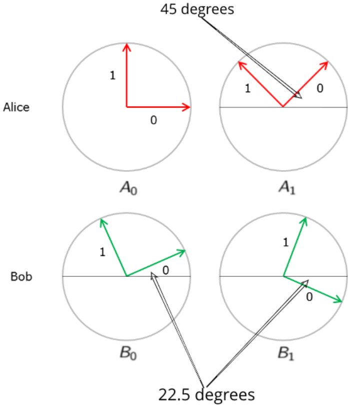
$$a \oplus b = x \wedge y$$

Deterministic strategy: win 75% of the times



$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$p(B_0 = 0|A_0 = 0) = cos^2(22.5) = .8536$$
$$p(B_0 = 1|A_0 = 0) = cos^2(90 + 22.5) = .1464$$
$$p(B_0 = 0|A_0 = 1) = cos^2(90 - 22.5) = .1464$$
$$p(B_0 = 1|A_0 = 1) = cos^2(22.5) = .8536$$
$$p(A_0 = 0) = p(A_0 = 1) = .5$$



$$|EPR\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

x	y	A	B	x∧y	a ⊕ b
0	0	A_0	B_0	0	$a_0 \oplus b_0$
0	1	A_0	B_1	0	$a_0 \oplus b_1$
1	0	A_1	B_0	0	$a_1 \oplus b_0$
1	1	A_1	B_1	1	$a_1 \oplus b_1$

$$a \oplus b = x \wedge y$$

Measurement based strategy: win $\approx$ 85% of the times

$$
\begin{aligned}
\text{Expected value of } A_0, B_0 = \langle A_0 B_0 \rangle = \langle EPR | A_0 \otimes B_0 | EPR \rangle \\
p(B_0 = 0 | A_0 = 0) p(A_0 = 0)(+1) + \\
p(B_0 = 1 | A_0 = 0) p(A_0 = 0)(-1) + \\
p(B_0 = 0 | A_0 = 1) p(A_0 = 1)(-1) + \\
p(B_0 = 1 | A_0 = 1) p(A_0 = 1)(+1) \\
= .5(.8536 - .1464 + .8536 - .1464) \\
= .7071
\end{aligned}
$$

Note that, this is also the probability that they win minus the probability that they lose given $x = 0$ and $y = 0$.

Similarly:

$$\langle A_0 B_1 \rangle = \langle A_1 B_0 \rangle = .7071$$
$$\langle A_1 B_1 \rangle = -.7071 (\text{mismatch wins here, so, OK})$$

So, the following operator:

$$\frac{1}{4}\Big(\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \Big) = \frac{2\sqrt{2}}{4},$$

gives the probability that they win minus the probability that they lose in a single round. Let's define $CHSH := 2\sqrt{2}$. Notice that,

$$p(win) = \frac{1}{2}(1 + \frac{2\sqrt{2}}{4}) = .8536,$$

as mentioned before.

Let $\{A_0, B_0, A_1, B_1\} \in \{\pm 1\}$. Local hidden variable model says:

$$\mathbb{E}(A_0(\lambda)B_0(\lambda)) = \int_\lambda p(\lambda)A_0(\lambda)B_0(\lambda)d\lambda.$$

Then,

$$\mathbb{E}(A_0(\lambda)B_0(\lambda) + A_0(\lambda)B_1(\lambda) + A_1(\lambda)B_0(\lambda) - A_1(\lambda)B_1(\lambda)) = \tag{1}$$

$$= \int_\lambda \Big(A_0(\lambda)B_0(\lambda) + A_0(\lambda)B_1(\lambda)$$
$$+ A_1(\lambda)B_0(\lambda) - A_1(\lambda)B_1(\lambda)\Big)p(\lambda)d\lambda.$$

But notice that, because $\{A_0, B_0, A_1, B_1\} \in \{\pm 1\}$, either,

$$B_0(\lambda) + B_1(\lambda) = 0 \text{ or } B_0(\lambda) - B_1(\lambda) = 0,$$

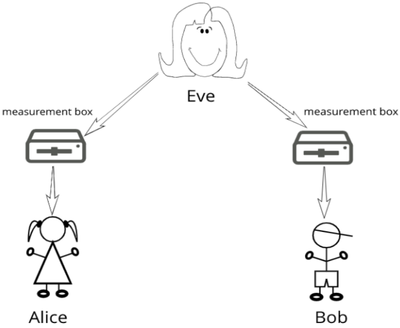
and the other is ± 2. So, equation (1) becomes:

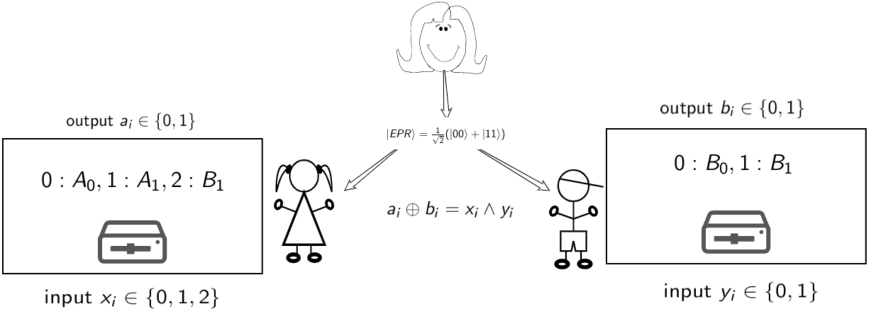
$$\begin{aligned}
&\mathbb{E}(A_0(\lambda)B_0(\lambda) + A_0(\lambda)B_1(\lambda) + A_1(\lambda)B_0(\lambda) - A_1(\lambda)B_1(\lambda)) = \\
&= \int_{\lambda \in \Lambda} \Big(A_0(\lambda)\big(B_0(\lambda) + B_1(\lambda)\big) \\
&+ A_1(\lambda)\big(B_0(\lambda) - B_1(\lambda)\big)\Big) p(\lambda) d\lambda \\
&\leq 2.
\end{aligned}$$

With equality, we see that,

$$p(win) = \frac{1}{2}(1 + \frac{2}{4}) = .75,$$

as seen in the classical case.


Eve
measurement box
measurement box
Alice
Bob



output $a_i \in \{0,1\}$

$0 : A_0, 1 : A_1, 2 : B_1$

input $x_i \in \{0,1,2\}$

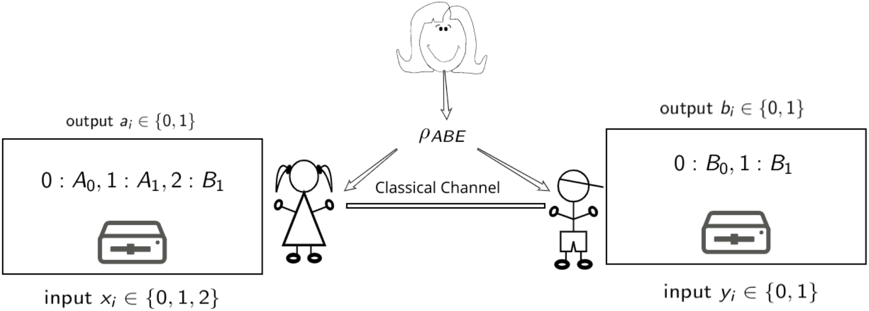
$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$a_i \oplus b_i = x_i \wedge y_i$

output $b_i \in \{0,1\}$

$0 : B_0, 1 : B_1$

input $y_i \in \{0,1\}$



output $a_i \in \{0,1\}$

$0 : A_0, 1 : A_1, 2 : B_1$

input $x_i \in \{0,1,2\}$

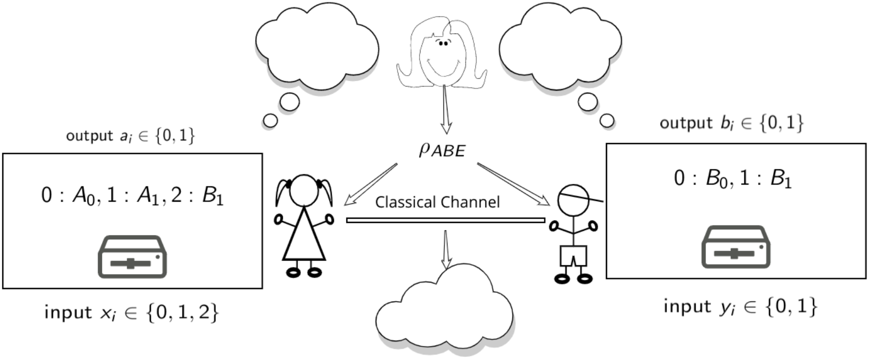
ρ_{ABE}

Classical Channel

output $b_i \in \{0,1\}$

$0 : B_0, 1 : B_1$

input $y_i \in \{0,1\}$



output $a_i \in \{0,1\}$

$0 : A_0, 1 : A_1, 2 : B_1$

input $x_i \in \{0,1,2\}$

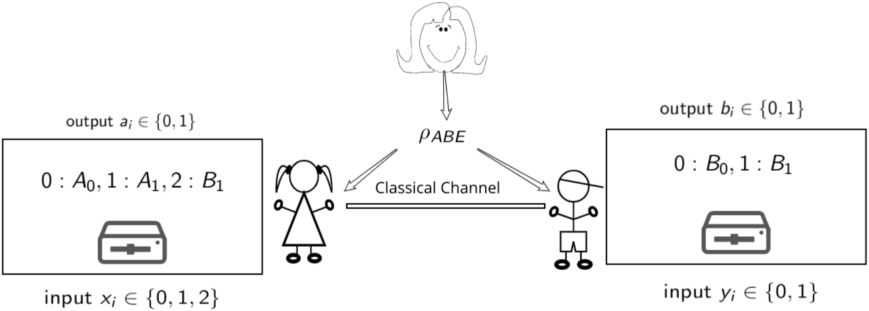
ρ_{ABE}

Classical Channel

output $b_i \in \{0,1\}$

$0 : B_0, 1 : B_1$

input $y_i \in \{0,1\}$



output $a_i \in \{0,1\}$

$0 : A_0, 1 : A_1, 2 : B_1$

input $x_i \in \{0,1,2\}$

ρ_{ABE}

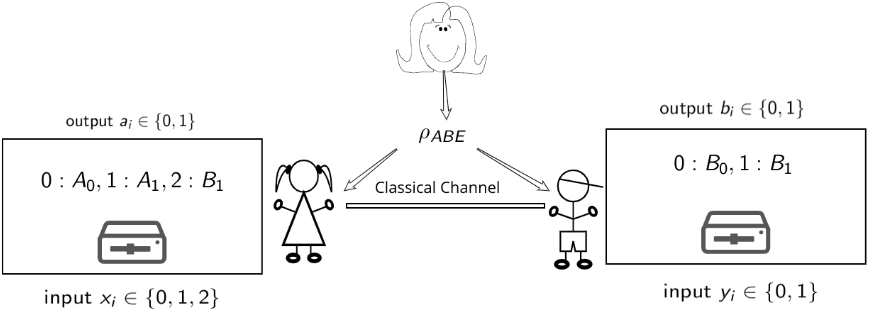
Classical Channel

output $b_i \in \{0,1\}$

$0 : B_0, 1 : B_1$

input $y_i \in \{0,1\}$

n : # of total rounds, $\boldsymbol{B} \subseteq \{1...n\}$:Bell-test rounds. Check the percentage of winning in $\boldsymbol{B}$ is $\geq .8536 - \eta$, otherwise, abort.



ρ_{ABE}

Classical Channel

output $a_i \in \{0, 1\}$

$0 : A_0, 1 : A_1, 2 : B_1$

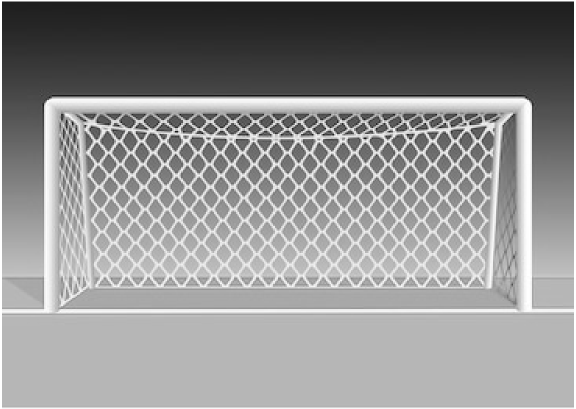
input $x_i \in \{0, 1, 2\}$

output $b_i \in \{0, 1\}$

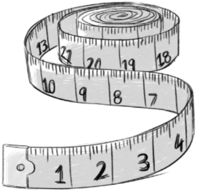
$0 : B_0, 1 : B_1$

input $y_i \in \{0, 1\}$

$\boldsymbol{C} = \{i : (x_i, y_i) = (2, 1)\}$. Select a subset, check frequency of $a_i = b_i$. If $\geq 1 - \eta$, continue with information reconciliation and privacy amplification, otherwise, abort.



The Goal



Key-rate Computation

Why higher CHSH value is better for key-rate? Pironio et.al. [4] showed that for collective attacks, Eve's information could be upper bounded by:

$$\chi(B:E) \leq h\left(\frac{1+\sqrt{(CHSH/2)^2-1}}{2}\right)$$

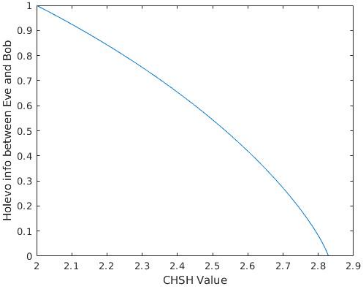
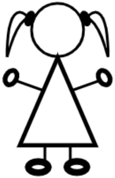


Figure 1: Eve's knows less as CHSH value goes higher

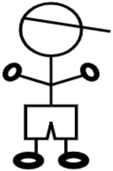
Information Reconciliation



$$A, B \in \{0, 1\}^k$$

$$\varepsilon > 0$$

$$l \leq H^{\varepsilon}_{max}(B|A)_{\rho} + \log(2/\varepsilon)$$



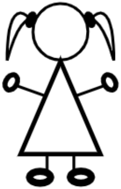
A = Alice's string, B = Bob's string, and the smooth max-entropy:

$$H^{\varepsilon}_{\max}(B|A)_{\rho} := \inf_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} H_{\max}(B|A)_{\rho'}$$

$$H_{\max}(B \mid A)_{\rho} = \log q_{\text{decpl}}(B \mid A)_{\rho}$$

$$q_{\text{decpl}}\,(B \mid A)_{\rho} := d_B \max_{\sigma_A} F\left(\rho_{AB}, \tau_A \otimes \sigma_B\right)^2$$

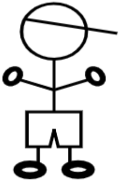
q_{decpl} = decoupling accuracy, F = fidelity function, $\mathcal{B}^{\varepsilon}(\rho)$ = ε-ball of density operators of ρ.



$$A, B \in \{0,1\}^k$$

$$\varepsilon > 0$$

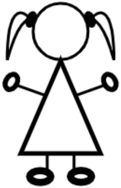
$$l \leq H_{max}^{\varepsilon}(B|A)_\rho + \log(2/\varepsilon)$$



$$H_{\max}^{\varepsilon'}(B_{\boldsymbol{C}}|A_{\boldsymbol{C}}) \leq H(1.1\eta)|\boldsymbol{C}|$$

$$\varepsilon' = 2e^{-\gamma|\boldsymbol{C}|/400}$$

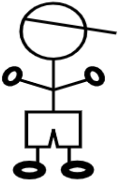
Privacy Amplification



l =leakage in IR

$\varepsilon > 0$

∃PA s.t. key-rate $\geq H^{\varepsilon}_{min}(B_{\boldsymbol{C}}|\mathcal{E}') - l - 2log(1/\varepsilon)$

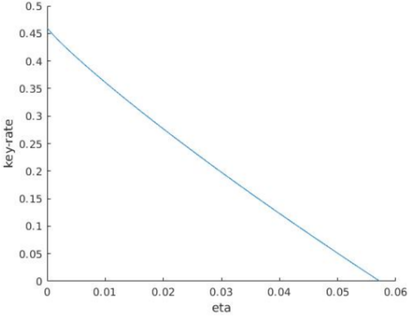


$$H^{\varepsilon}_{min}(B|E)_{\rho} := \max_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} H^{\varepsilon}_{min}(B|E)_{\rho'}$$

$$H_{\min}(B|E)_{\rho} := -\inf_{\sigma_B} \inf_{\lambda} \{\lambda \in \mathbb{R} : \rho_{BE} \leq 2^{\lambda}\sigma_B\}$$

$$\begin{aligned}\text{key-rate } r &= \frac{\text{number secret bits}}{\text{size of raw key}} \\ &\geq -\frac{11}{3} log(\frac{11}{12} + \frac{2}{3}\eta) - h(\frac{\eta}{\sqrt{2}})\end{aligned}$$

where $h(x)$ is the binary entropy function.



- CHSH Game ensures secrecy.
- Higher violation of Bell's inequality is better for Alice and Bob.
- Fully DIQKD is possible against coherent attacks.

Proof of Secrecy

The following three conditions can not hold simultaneously.

- The devices violate CHSH inequality in the test rounds.
- Eve can predict Bob's output in the key rounds.
- No-signalling property is satisfied among all parties in all rounds.

A 'Rare' Round

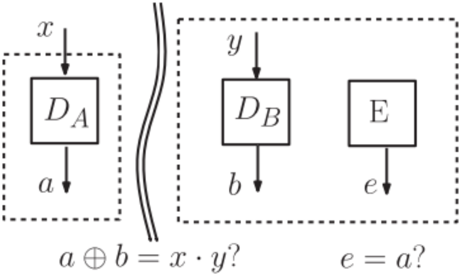
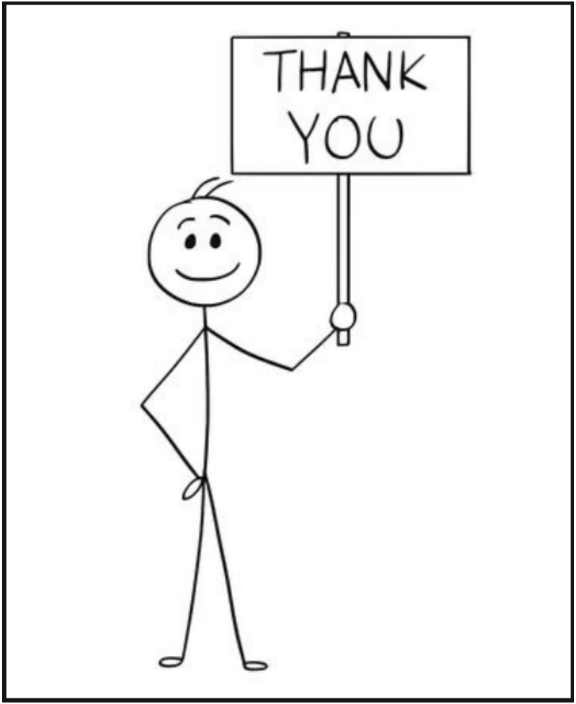


Figure 3: Contradiction of (a), (b) with (c)



THANK YOU

- Dominic Mayers and Andrew Yao.
  Proceedings of the 39th annual symposium on foundations of computer science (focs98).
  1998.

- Artur K Ekert.
  Quantum cryptography based on bell's theorem.
  Physical review letters, 67(6):661, 1991.

- Umesh Vazirani and Thomas Vidick.
  Fully device-independent quantum key distribution.
  Physical Review Letters, 113(14):Art–No, 2014.

- Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani.
  Device-independent quantum key distribution secure against collective attacks.
  New Journal of Physics, 11(4):045021, 2009.