

Kvantna kriptografija kot namizna igra

Sergej Faletič, UL FMF

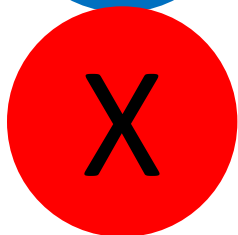
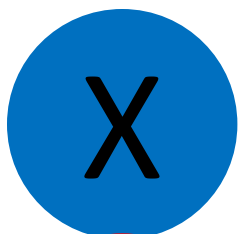
Viri

- Martin Laforest
QCrypto Coins
IQC Scientific Outreach team
iqc-outreach@uwaterloo.ca
University of Waterloo
<https://uwaterloo.ca/institute-for-quantum-computing/outreach-and-workshops/teacher-resources>
- Tim Lethen
Bit commitment as an introduction to quantum cryptography
European Journal of Physics 43(5), 2022
<https://doi.org/10.1088/1361-6404/ac78a7>
- Charles H. Bennett, Gilles Brassard
Quantum cryptography: public key distribution and coin tossing
International Conference on Computers, Systems & Signal Processing
Bangalore, India December 10-12, 1984
<https://doi.org/10.48550/arXiv.2003.06557>

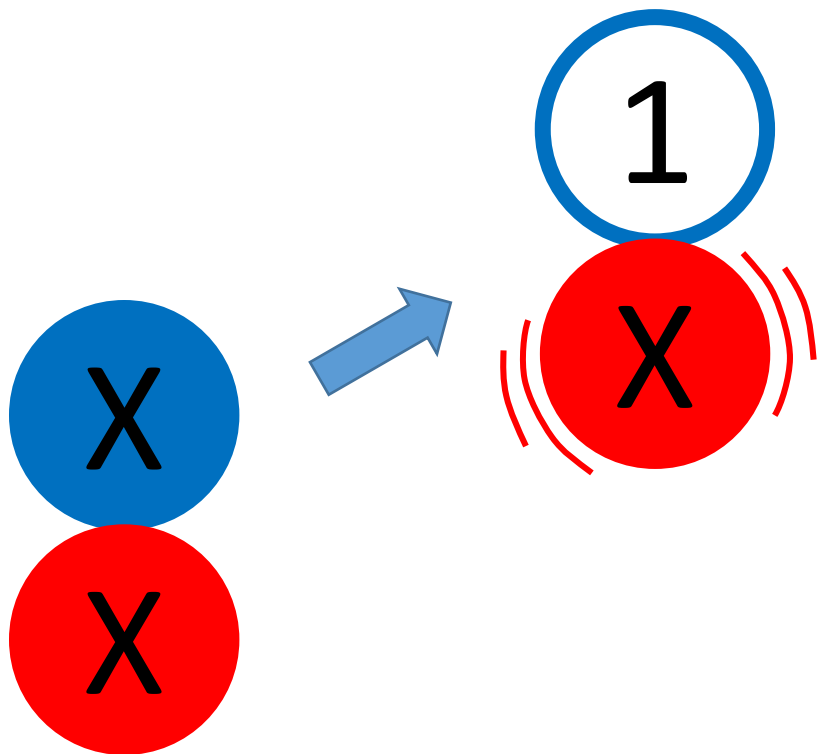
Oris

- BB84b
- BB84
- BB84 s prisluškovanjem

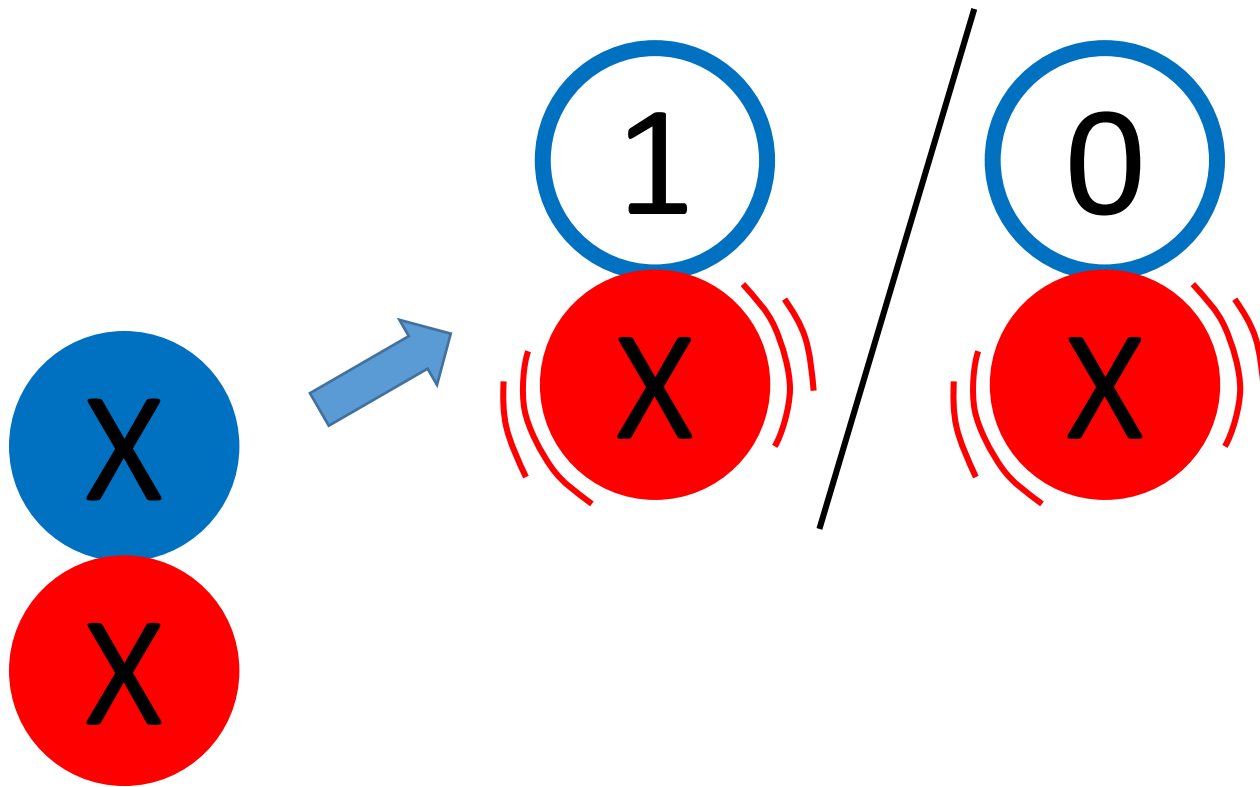
Edino pravilo



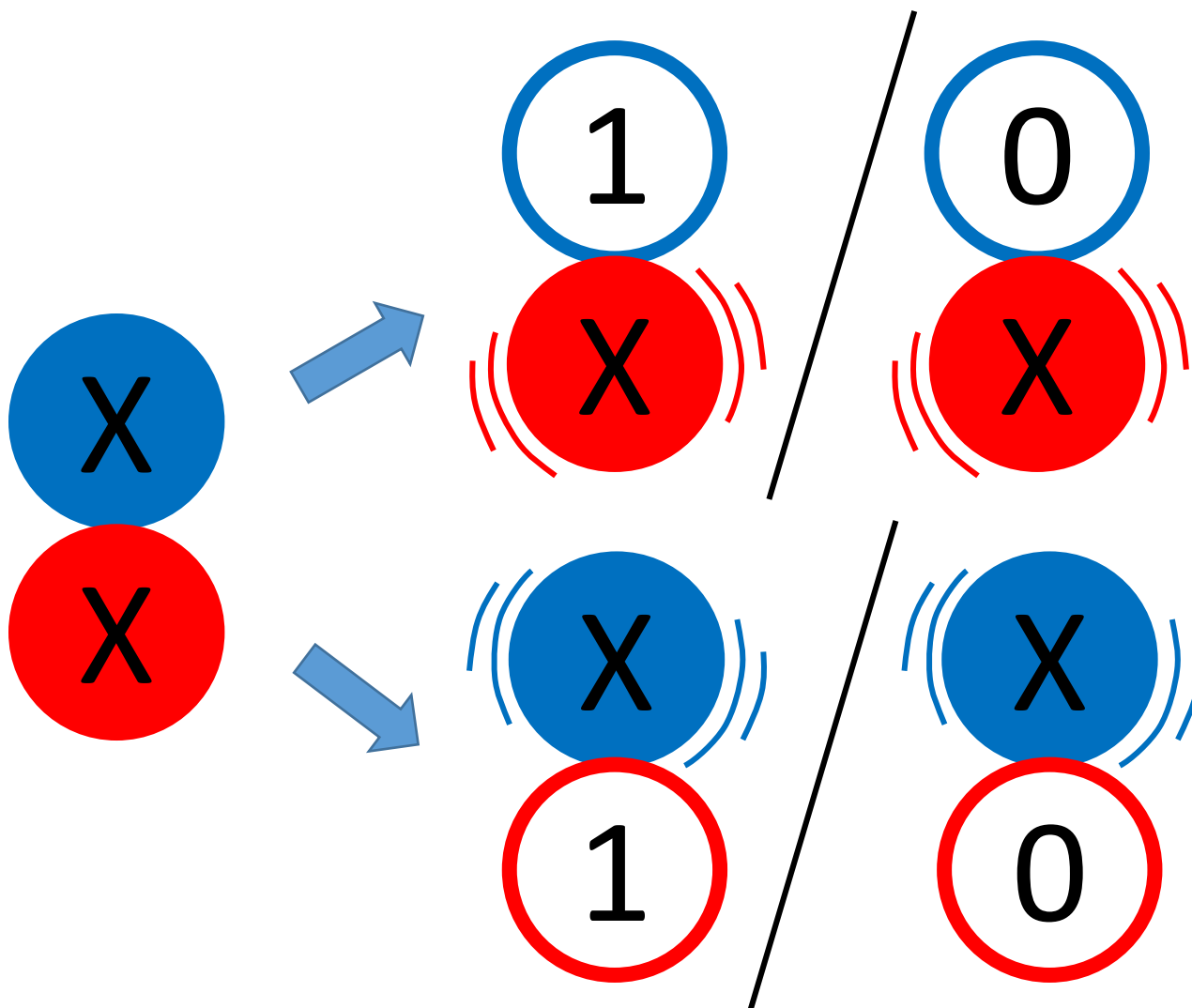
Edino pravilo



Edino pravilo



















Edino pravilo



BB84b – met kovanca na daljavo

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev |   |   |   |   |   |   |   |   |
| Alicejini qubiti: | | | | | | | | |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | 1 X | 0 X | 1 X | 1 X | 0 X | 1 X | 0 X | 0 X |
| Alicejini qubiti: | | | | | | | | |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev |   |   |   |   |   |   |   |   |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | 1 X | 0 X | 1 X | 1 X | 0 X | 1 X | 0 X | 0 X |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce |   |   |   |   |   |   |   |   |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|---|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| | X | X | X | X | X | X | X | X |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | 1 X | X 1 | 1 X | 1 X | 0 X | 1 X | 0 X | 0 X |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | 1 X | X 1 | X 0 | 1 X | 0 X | 1 X | 0 X | 0 X |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|--|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev |  |  |  |  |  |  |  |  |
| |  |  |  |  |  |  |  |  |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | 1 X | X 1 | X 0 | 1 X | X 0 | 1 X | 0 X | 0 X |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

















BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--|--|--|--|--|--|--|--|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | 1 X | X 1 | X 0 | 1 X | X 0 | 1 X | 0 X | X 1 |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|---|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | | | | | | | | |
| Alicejini qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|---|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|---|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|---|---|---|---|---|---|---|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | | | | | | | | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|----------------------|----|---|---|----|---|----|----|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | OK | | | OK | | OK | OK | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo









| | | | | | | | | |
|----------------------|----|---|---|----|---|----|----|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | OK | | | OK | | OK | OK | |
| Sodba | T | F | | | | | | |

BB84b – met kovanca na daljavo

| | | | | | | | | |
|------------------------|---|---|---|----|---|----|----|---|
| Alice izbere bazo | M | | | | | | | |
| Alice opravi meritev | Alice odpre škatle skladno z izbiro baze in druge strese. | | | | | | | |
| Alicejini qubiti: | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | Alice previdno nese škatle Bobu | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | M | R | R | M | R | M | M | R |
| Bob opravi meritev | Bob odpre škatle skladno z izbiro baze in druge strese. | | | | | | | |
| Bobovi qubiti | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| KLASIČNI PRENOS | Alice pove Bobu svojo bazo in qubite | | | | | | | |
| Alicejina baza | M | M | M | M | M | M | M | M |
| Alicejini qubiti | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Primerjava istih baz | OK | | | OK | | OK | OK | |
| Sodba | T | F | | | | | | |

BB84 – Prenos ključa

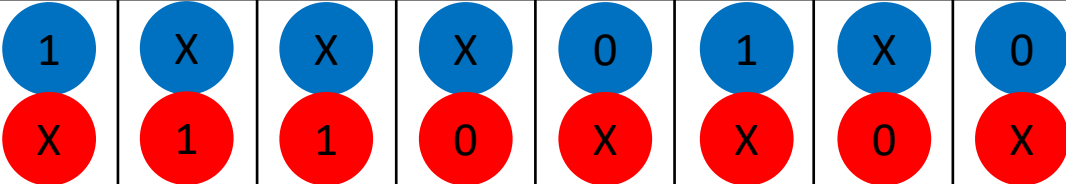
BB84 – Prenos ključa

| | | | | | | | | |
|----------------------------|---|---|--|---|---|---|---|---|
| Alice izbere baze | M | R | R | R | M | M | R | M |
| Alice opravi meritev |  |  |  |  |  |  |  |  |
| Alicejini qubiti: | | | | | | | | |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejine baze | | | | | | | | |
| Alicejini kontrolni qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Ključ: | | | | | | | | |

















BB84 – Prenos ključa

| | | | | | | | | |
|----------------------------|--|---|---|---|---|---|---|---|
| Alice izbere baze | M | R | R | R | M | M | R | M |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | 1 (blue), X (red) X (red), 1 (red) X (red), 1 (red) X (red), 0 (red) 0 (blue), X (red) 1 (blue), X (red) X (red), 0 (red) 0 (blue), X (red) | | | | | | | |
| Bob izbere baze | | | | | | | | |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejine baze | | | | | | | | |
| Alicejini kontrolni qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Ključ: | | | | | | | | |

















BB84 – Prenos ključa

| | | | | | | | | |
|----------------------------|--|---|---|---|---|---|---|---|
| Alice izbere baze | M | R | R | R | M | M | R | M |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce |  | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M |
| Bob opravi meritev | | | | | | | | |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejine baze | | | | | | | | |
| Alicejini kontrolni qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Ključ: | | | | | | | | |

BB84 – Prenos ključa

| | | | | | | | | |
|----------------------------|--|--|--|--|--|--|--|--|
| Alice izbere baze | M | R | R | R | M | M | R | M |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | | | | | | | | |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejine baze | | | | | | | | |
| Alicejini kontrolni qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Ključ: | | | | | | | | |

BB84 – Prenos ključa

| | | | | | | | | |
|----------------------------|--|--|--|--|--|--|--|--|
| Alice izbere baze | M | R | R | R | M | M | R | M |
| Alice opravi meritev | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| KVANTNI PRENOS | | | | | | | | |
| Bob dobi delce | | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M |
| Bob opravi meritev |   |   |   |   |   |   |   |   |
| Bobovi qubiti | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| KLASIČNI PRENOS | | | | | | | | |
| Alicejine baze | | | | | | | | |
| Alicejini kontrolni qubiti | | | | | | | | |
| Primerjava istih baz | | | | | | | | |
| Ključ: | | | | | | | | |

BB84 – Prenos ključa

| | | | | | | | | | | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alice opravi meritev | | | | | | | | | | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | ... |
| KVANTNI PRENOS | | | | | | | | | | | | | | | | | |
| Bob dobi delce | | | | | | | | | | | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M | R | M | M | R | R | M | R | M | ... |
| Bob opravi meritev | | | | | | | | | | | | | | | | | |
| Bobovi qubiti | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | ... |
| KLASIČNI PRENOS | | | | | | | | | | | | | | | | | |
| Alicejine baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alicejini kontrolni qubiti | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | | | | | | | | | |
| Primerjava istih baz | | 1 | | | | 1 | 0 | 0 | | | | | | | | | |
| Ključ: | | | | | | | | | | 1 | | 0 | | | 0 | 1 | |

BB84 – Prenos ključa

| | | | | | | | | | | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alice opravi meritev | | | | | | | | | | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | ... |
| KVANTNI PRENOS | | | | | | | | | | | | | | | | | |
| Bob dobi delce | | | | | | | | | | | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M | R | M | M | R | R | M | R | M | ... |
| Bob opravi meritev | | | | | | | | | | | | | | | | | |
| Bobovi qubiti | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | ... |
| KLASIČNI PRENOS | | | | | | | | | | | | | | | | | |
| Alicejine baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alicejini kontrolni qubiti | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | | | | | | | | | |
| Primerjava istih baz | | 1 | | | | 1 | 0 | 0 | | | | | | | | | |
| Ključ: | | | | | | | | | | 1 | | 0 | | | 0 | 1 | |

BB84 – Prenos ključa

| | | | | | | | | | | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alice opravi meritev | | | | | | | | | | | | | | | | | |
| Alicejini qubiti: | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | ... |
| KVANTNI PRENOS | | | | | | | | | | | | | | | | | |
| Bob dobi delce | | | | | | | | | | | | | | | | | |
| Bob izbere baze | R | R | M | M | R | M | R | M | R | M | M | R | R | M | R | M | ... |
| Bob opravi meritev | | | | | | | | | | | | | | | | | |
| Bobovi qubiti | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | ... |
| KLASIČNI PRENOS | | | | | | | | | | | | | | | | | |
| Alicejine baze | M | R | R | R | M | M | R | M | M | M | R | R | M | R | R | M | ... |
| Alicejini kontrolni qubiti | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | | | | | | | | | |
| Primerjava istih baz | | 1 | | | | 1 | 0 | 0 | | | | | | | | | |
| Ključ: | | | | | | | | | | 1 | | 0 | | | 0 | 1 | |

BB84 – Prenos ključa, prisluškovanje

BB84 – Prenos ključa, prisluškovanje

| | | | | | | | | | |
|-----------------------------------|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | ... |
| Alice pošlje qubite | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | ... |
| Eva dobi delce in izbere baze | R | R | M | M | R | M | R | M | ... |
| Eva opravi meritev in dobi qubite | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| KVANTNI PRENOS (nadaljevanje) | | | | | | | | | |
| Bob dobi delce in izbere baze | M | R | M | R | R | M | M | R | ... |
| Bob opravi meritev in dobi qubite | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | ... |
| KLASIČNI PRENOS | | | | | | | | | |
| Alicejine baze | M | R | R | R | M | M | R | M | ... |
| Alicejini kontrolni qubiti | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | |
| Eva primerja qubite istih baz | | 1 | | | | 1 | 0 | 0 | ... |
| Bob primerja qubite istih baz | 0 | 1 | | 0 | | 1 | | | ... |
| Ključ je v bitih naprej od črte | | | | | | | | | tu |

Kjer sta bazi enaki, bo vedno ujemanje.

BB84 – Prenos ključa, prisluškovanje

| | | | | | | | | | |
|------------------------------------|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | ... |
| Alice opravi meritev in dobi qbite | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | ... |
| KVANTNI PRENOS | | | | | | | | | |
| Eva dobi delce in izbere baze | R | R | M | M | R | M | R | M | ... |
| Eva opravi meritev in dobi qubite | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| KVANTNI PRENOS (prisluškovanje) | | | | | | | | | |
| Eva izbere baze | M | R | M | R | R | M | M | R | ... |
| Eva dobi qubite | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | ... |
| KLASIČNI PRENOS | | | | | | | | | |
| Alicejine baze | M | R | R | R | M | M | R | M | ... |
| Alicejini kontrolni qubiti | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | ... |
| Eva primerja qubite istih baz | | 1 | | | | 1 | 0 | 0 | ... |
| Bob primerja qubite istih baz | 0 | 1 | | 0 | | 1 | | | ... |
| Ključ je v bitih naprej od črte | | | | | | | | | tu |

A zaradi Evinega vmešavanja, ne nujno med Alice in Bobom (stolpec 1).

BB84 – Prenos ključa, prisluškovanje

| | | | | | | | | | |
|------------------------------------|---|---|---|---|---|---|---|---|-----|
| Alice izbere baze | M | R | R | R | M | M | R | M | ... |
| Alice opravi meritev in dobi qbite | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | ... |
| KVANTNI PRENOS | | | | | | | | | |
| Eva dobi delce in izbere baze | R | R | M | M | R | M | R | M | ... |
| Eva opravi meritev in dobi qubite | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| KVANTNI PRENOS (nadaljevanje) | | | | | | | | | |
| Bob dobi delce in izbere baze | M | R | M | R | R | M | M | R | ... |
| Bob opravi meritev in dobi qubite | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | ... |
| ... | | | | | | | | | |
| | M | R | R | R | M | M | R | M | ... |
| | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | |
| | | 1 | | | | 1 | 0 | 0 | ... |
| | 0 | 1 | | 0 | | 1 | | | ... |
| Ključ je v bitih naprej od črte | | | | | | | | | tu |

Lahko pa, če ima Eva srečo, da izbere iste baze kot Alice in Bob (stolpca 2 in 6) ali če je naključen rezultat slučajno enak kot Alicejin original (stolpec 4).

Kaj se izkustveno naučijo igralci?

Kaj se izkustveno naučijo igralci?

- Rezultat posamezne meritve je naključen (stohastičnost).
- Rezultat je lahko le eden (ekskluzivnost).¹
- Obstajajo taki pari količin, da ima meritev ene količine vedno za posledico naključno vrednost druge količine (nekompatibilnost/nekomutativnost/Heisenbergova nedoločenost).

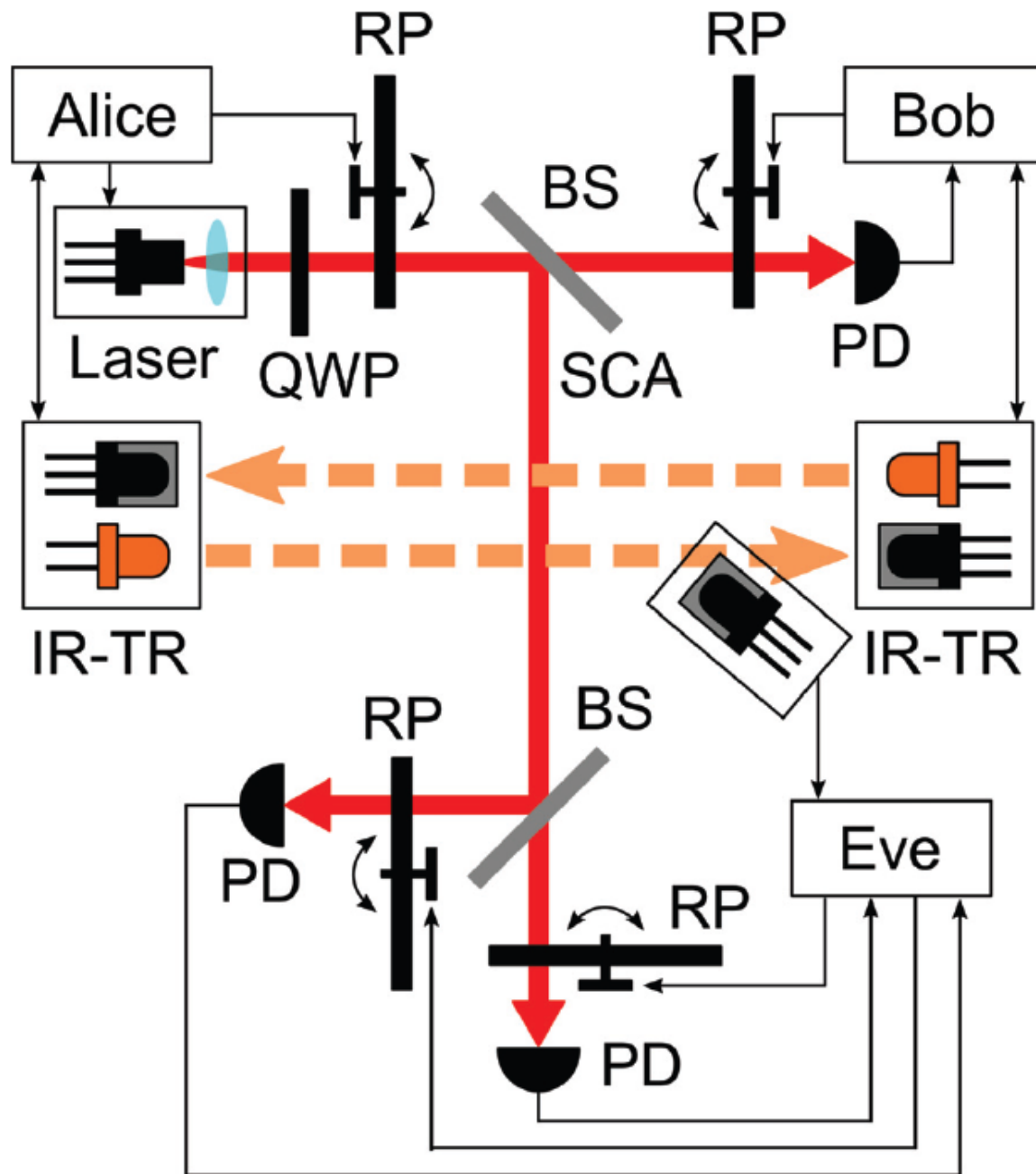
¹ Če se ploščice ne postavljajo na rob... bolje imeti kovance 😊

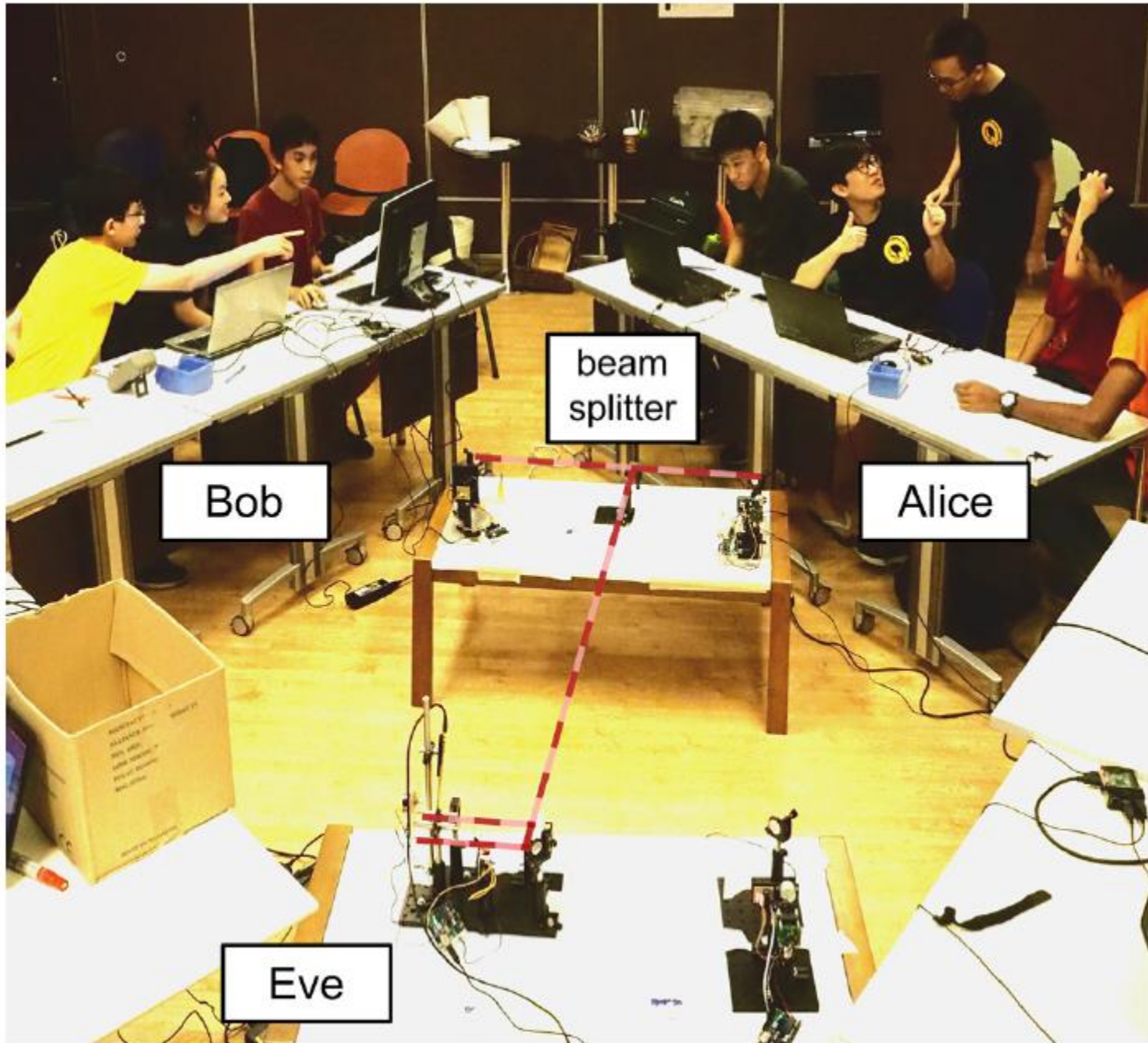
Hvala za igro!



Nekaj dodatkov na podlagi vprašanj

- Iz članka:
Adrian Nugraha Utama, Jianwei Lee and Mathias Alexander Seidler
A hands-on quantum cryptography workshop for pre-university students
American Journal of Physics 88, 1094, 2020
<https://doi.org/10.1119/10.0001895>





beam
splitter

Bob

Alice

Eve