Quantum Cyber Security
Lecture 11: Quantum Key Distribution IV

Petros Wallden

University of Edinburgh

27th February 2024

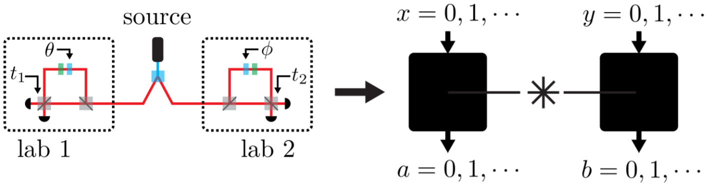
This Lecture: Device-Independent QKD and Non-Locality

1. Device-Independence (DI): definition, meaning, motivation
2. Non-Locality and Bell's Inequalities
3. E91 Protocol
4. Security for DI protocols
5. Loopholes and experimental challenges
6. Semi-device-independence (SDI)

Device-Independent Quantum Cryptography

Definition: Device-Independent Quantum Cryptography

Achieving a **cryptographic task** while treating the (quantum) **devices** used as **black-boxes** with classical input and output, where these **boxes are prepared by the adversary** in a possibly correlated or even entangled way



Motivation:

- **Higher level of security** (classically impossible)

Motivation:

- **Higher level of security** (classically impossible)
- No trust on devices means that the protocol **remains secure** when physical implementation does not meet exactly the theoretical specifications
  Non-ideal single-photon source, leakage of info on the measuring device setting (hacking/side-channel attacks), etc

Device-Independent Quantum Cryptography

Motivation:

- **Higher level of security** (classically impossible)
- No trust on devices means that the protocol **remains secure** when physical implementation does not meet exactly the theoretical specifications
  Non-ideal single-photon source, leakage of info on the measuring device setting (hacking/side-channel attacks), etc
- **No trust** required to the **manufacturer** (important for commercial applications)

Device-Independent Quantum Cryptography

Motivation:

- **Higher level of security** (classically impossible)
- No trust on devices means that the protocol **remains secure** when physical implementation does not meet exactly the theoretical specifications
  Non-ideal single-photon source, leakage of info on the measuring device setting (hacking/side-channel attacks), etc
- **No trust** required to the **manufacturer** (important for commercial applications)

Assumptions:

- Secure Labs: stop unwanted info between lab & other devices
- Reliable classical info processing
- Perfect local randomness source
- Classically authenticated channel

Non-Locality and Bell's Inequalities (CHSH)

- **DI** possible due to **quantum non-locality**
- Of most fundamental differences between classical and quantum theories

- **DI** possible due to **quantum non-locality**
- Of most fundamental differences between classical and quantum theories
- Locality: The state of a system cannot be influenced instantaneously by an action that is far away
- Appears essential to do science!

Non-Locality and Bell's Inequalities (CHSH)

- **DI** possible due to **quantum non-locality**
- Of most fundamental differences between classical and quantum theories
- Locality: The state of a system cannot be influenced instantaneously by an action that is far away
- Appears essential to do science!
- **John Bell** (1964) derived some inequalities that allowed to test if non-locality is present in quantum theory
- Technically proved that there is doesn't exist any **local hidden variables (LHV)** theory that agrees with the prediction of QT
- Along with the Einstein-Podolsky-Rosen argument this means that QT is non-local

Non-Locality and Bell's Inequalities (CHSH)

- **DI** possible due to **quantum non-locality**
- Of most fundamental differences between classical and quantum theories
- Locality: The state of a system cannot be influenced instantaneously by an action that is far away
- Appears essential to do science!
- **John Bell** (1964) derived some inequalities that allowed to test if non-locality is present in quantum theory
- Technically proved that there is doesn't exist any **local hidden variables (LHV)** theory that agrees with the prediction of QT
- Along with the Einstein-Podolsky-Rosen argument this means that QT is non-local
- **Experiments confirmed Quantum Theory**

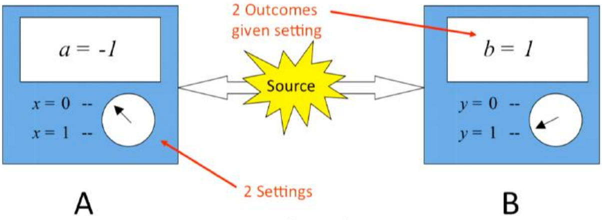
2022 Nobel for violation of Bell's inequalities

- Experimental validation of Quantum Theory got the **2022 Physics Nobel prize**
- **John F. Clauser** (first experiment AND simpler inequality)
- **Alain Aspect** (experiment with varying bases – first "conclusive" experiment)
- **Anton Zeilinger** (loophole free experiment 2015)

`www.nobelprize.org/prizes/physics/2022/summary/`

CHSH (Bell) inequalities

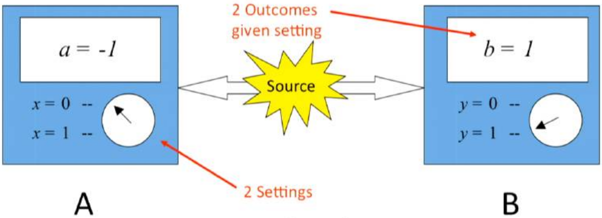
- Clauser, Horne, Shimony and Holt (CHSH) in 1969 proved a similar (and simpler) "Bell" inequality (which we will see)



$$P_{xy}(a, b)$$

CHSH (Bell) inequalities

- Clauser, Horne, Shimony and Holt (CHSH) in 1969 proved a similar (and simpler) "Bell" inequality (which we will see)

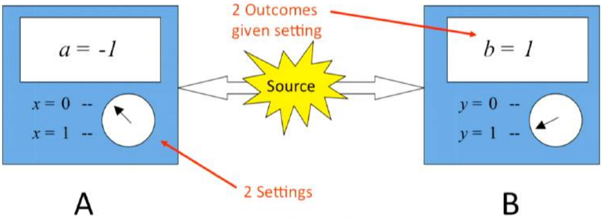


$$P_{xy}(a,b)$$

- Two parties (Alice, Bob), each can choose between two measurements, Alice $x = \{0, 1\}$, Bob $y = \{0, 1\}$. Each measurement can take two values $a_x = \{1, -1\}$, $b_y = \{1, -1\}$

CHSH (Bell) inequalities

- Clauser, Horne, Shimony and Holt (CHSH) in 1969 proved a similar (and simpler) "Bell" inequality (which we will see)



$$P_{xy}(a,b)$$

- Two parties (Alice, Bob), each can choose between two measurements, Alice $x = \{0,1\}$, Bob $y = \{0,1\}$. Each measurement can take two values $a_x = \{1,-1\}$, $b_y = \{1,-1\}$
- We have 4-different probability distributions (one for each different choice of measurement settings) $P_{00}(a,b), P_{01}(a,b), P_{10}(a,b), P_{11}(a,b)$

CHSH inequalities

- We define the correlator to be (expresses the correlation between the outcomes of different variables)
  $E_{xy} = \sum_{ab} abP_{xy}(ab)$, e.g.:
  $E_{01} = P_{01}(1,1) + (-1)P_{01}(1,-1) + (-1)P_{01}(-1,1) + (-1)(-1)P_{01}(-1,-1)$

CHSH inequalities

- We define the correlator to be (expresses the correlation between the outcomes of different variables)
  $E_{xy} = \sum_{ab} abP_{xy}(ab)$, e.g.:
  $E_{01} = P_{01}(1,1) + (-1)P_{01}(1,-1) + (-1)P_{01}(-1,1) + (-1)(-1)P_{01}(-1,-1)$
- We can easily see that $|E_{xy}| \leq 1$. We define the quantity β:

$$\beta := E_{00} - E_{01} + E_{10} + E_{11}$$

CHSH inequalities

- We define the correlator to be (expresses the correlation between the outcomes of different variables) $E_{xy} = \sum_{ab} abP_{xy}(ab)$, e.g.: $E_{01} = P_{01}(1,1) + (-1)P_{01}(1,-1) + (-1)P_{01}(-1,1) + (-1)(-1)P_{01}(-1,-1)$
- We can easily see that $|E_{xy}| \leq 1$. We define the quantity β:

$$\beta := E_{00} - E_{01} + E_{10} + E_{11}$$

- Given a local hidden variables model, we obtain the inequality

$$-2 \leq \beta \leq 2$$

- We define the correlator to be (expresses the correlation between the outcomes of different variables)
  $E_{xy} = \sum_{ab} abP_{xy}(ab)$, e.g.:
  $E_{01} = P_{01}(1,1) + (-1)P_{01}(1,-1) + (-1)P_{01}(-1,1) + (-1)(-1)P_{01}(-1,-1)$
- We can easily see that $|E_{xy}| \leq 1$. We define the quantity β:

$$\beta := E_{00} - E_{01} + E_{10} + E_{11}$$

- Given a local hidden variables model, we obtain the inequality

$$-2 \leq \beta \leq 2$$

- The assumption of local hidden-variables is given by:

$$E_{xy} = \int A(x,\lambda)B(y,\lambda)\rho(\lambda)d\lambda$$

  Each outcome depends on the local measurement only and is fixed given λ

  Correlations appear due $\rho(\lambda)$ where $\int \rho(\lambda)d\lambda = 1$

CHSH inequalities: Quantum Bound and Eavesdropping

- Given LHV, an eavesdropper (Eve) can **mimic all correlations** observed deterministically. Having access to λ, can reproduce all outcomes of both Alice, Bob in all bases.

- Variables still appear random for someone with no access to λ: e.g. $A(x) = \int A(x,\lambda)\rho(\lambda)d\lambda$

CHSH inequalities: Quantum Bound and Eavesdropping

- Given LHV, an eavesdropper (Eve) can **mimic all correlations** observed deterministically. Having access to λ, can reproduce all outcomes of both Alice, Bob in all bases.

- Variables still appear random for someone with no access to λ: e.g. $A(x) = \int A(x,\lambda)\rho(\lambda)d\lambda$

- In QT can achieve a max value of $\beta = 2\sqrt{2} > 2$ which proves **non-locality**, i.e. non existence of LHV

CHSH inequalities: Quantum Bound and Eavesdropping

- Given LHV, an eavesdropper (Eve) can **mimic all correlations** observed deterministically. Having access to λ, can reproduce all outcomes of both Alice, Bob in all bases.

- Variables still appear random for someone with no access to λ: e.g. $A(x) = \int A(x, \lambda)\rho(\lambda)d\lambda$

- In QT can achieve a max value of $\beta = 2\sqrt{2} > 2$ which proves **non-locality**, i.e. non existence of LHV

- **Example of max violation:** Alice and Bob share the state:

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

  Alice measures observables: $x = 0 \to Z$; $x = 1 \to X$
  Bob measures: $x = 0 \to \frac{1}{\sqrt{2}}(X + Z)$; $x = 1 \to \frac{1}{\sqrt{2}}(X - Z)$

CHSH inequalities: Quantum Bound and Eavesdropping

- To compute β need the correlators, e.g.:

$$E_{01}(\rho_{AB}) := \mathrm{Tr}\left((Z_A \otimes \frac{1}{\sqrt{2}}(X_B - Z_B))\rho_{AB}\right)$$

- Then compute $\beta = E_{00} - E_{01} + E_{10} + E_{11}$

  Which leads to $\beta = 2\sqrt{2} > 2$!

CHSH inequalities: Quantum Bound and Eavesdropping

- To compute β need the correlators, e.g.:

$$E_{01}(\rho_{AB}) := \mathrm{Tr}\left((Z_A \otimes \frac{1}{\sqrt{2}}(X_B - Z_B))\rho_{AB}\right)$$

- Then compute $\beta = E_{00} - E_{01} + E_{10} + E_{11}$

  Which leads to $\beta = 2\sqrt{2} > 2$!

- Whenever $\beta > 2$ system we know there was **no LHV that can reproduce the behaviour**, and it exhibits **non-locality**

- See tutorial for computing β for different states ρ.

The E91 QKD Protocol

- Proposed by: Ekert (1991)
- Difference to BBM92: Alice and Bob, measure in three bases in a way that they can violate the CHSH inequality. Security is based on this violation
- History:
  - Ekert did not realise that this protocol is device-independent
  - Concept first define 1998 by Mayers and Yao
  - first DI QKD protocol by Barrett, Hardy, Kent 2005 where stronger version of DI was obtained (alas not practically implementable)

The E91 QKD Protocol

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

The E91 QKD Protocol

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

Alice

- Measures randomly one of the **three** observables
  $x^{(i)} = 1 \to Z$; $x^{(i)} = 2 \to \frac{1}{\sqrt{2}}(X + Z)$; $x^{(i)} = 3 \to X$
- Obtains result $a^{(i)} \in \{1, -1\}$
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

Alice

- Measures randomly one of the **three** observables
  $x^{(i)} = 1 \to Z$; $x^{(i)} = 2 \to \frac{1}{\sqrt{2}}(X + Z)$; $x^{(i)} = 3 \to X$
- Obtains result $a^{(i)} \in \{1, -1\}$
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

Bob

- Measures randomly one of the **three** observables
  $y^{(i)} = 1 \to \frac{1}{\sqrt{2}}(X + Z)$; $y^{(i)} = 2 \to X$; $y^{(i)} = 3 \to \frac{1}{\sqrt{2}}(X - Z)$
- Obtains result $b^{(i)} \in \{1, -1\}$
- Stores string of pairs: $(b^{(1)}, y^{(1)}), (b^{(2)}, y^{(2)}), \cdots, (b^{(n)}, y^{(n)})$

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where they used the same basis $x^{(i)} = 2 \wedge y^{(i)} = 1$ or when $x^{(i)} = 3 \wedge y^{(i)} = 2$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)}\ \forall\ i$ of the raw key

The E91 Protocol

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where they used the same basis $x^{(i)} = 2 \wedge y^{(i)} = 1$ or when $x^{(i)} = 3 \wedge y^{(i)} = 2$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)}\ \forall\ i$ of the raw key

"Parameter Estimation"

- Instead of discarding results measured in different bases, they use them to compute $\beta = E_{11} - E_{13} + E_{31} + E_{33}$, where e.g. $E_{31} = \langle\tilde{\Psi}|\, X \otimes \frac{1}{\sqrt{2}}(X + Z)\, |\tilde{\Psi}\rangle$
- Small fraction of same bases are also used to compute D the symmetric **QBER** (not in original E91)

  $e_b = \frac{1}{2}\left(1 - \mathrm{Tr}\left((Z \otimes Z)\rho\right)\right)$ and $e_p = \frac{1}{2}\left(1 - \mathrm{Tr}\left((X \otimes X)\rho\right)\right)$
- Rate is derived wrt β, D and $\beta > 2$ to not abort
- **IR** and **PA** as usual

E91 security and Key Rate

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

  Due to **monogamy** of entanglement triv true for max violation

E91 security and Key Rate

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

  Due to **monogamy** of entanglement triv true for max violation

  It also holds for **any** violation since perfect correlation would imply existence of **local hidden variables**!

E91 security and Key Rate

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

  Due to **monogamy** of entanglement triv true for max violation

  It also holds for **any** violation since perfect correlation would imply existence of **local hidden variables**!
- For **i.i.d. adversaries** it holds:
  $S(A|E) \geq 1 - h\left(\frac{1}{2}(1 + \sqrt{(\beta/2)^2 - 1})\right)$
- **Non-iid** harder but reduces essentially to similar expression

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

  Due to **monogamy** of entanglement triv true for max violation

  It also holds for **any** violation since perfect correlation would imply existence of **local hidden variables**!

- For **i.i.d. adversaries** it holds:
  $S(A|E) \geq 1 - h\left(\frac{1}{2}(1 + \sqrt{(\beta/2)^2 - 1})\right)$

- **Non-iid** harder but reduces essentially to similar expression

- **Other DI QKD** no simple formula. Instead weakly bound $S(A|E)$ by min-entropy and numer methods (SDP)

E91 security and Key Rate

- Intuition: Eve cannot be (perfectly) correlated with Alice's string if there is non-locality ($\beta > 2$)

  Due to **monogamy** of entanglement triv true for max violation

  It also holds for **any** violation since perfect correlation would imply existence of **local hidden variables**!
- For **i.i.d. adversaries** it holds:
  $S(A|E) \geq 1 - h\left(\frac{1}{2}(1 + \sqrt{(\beta/2)^2 - 1})\right)$
- **Non-iid** harder but reduces essentially to similar expression
- **Other DI QKD** no simple formula. Instead weakly bound $S(A|E)$ by min-entropy and numer methods (SDP)
- Key Rate: $R \geq S(A|E) - H(A|B) = S(A|E) - h(D)$

  Smaller than BB84 but can be made viable ($\sim 7\%$). Major issue is the **high detection** required (see loopholes)

Loopholes

- There are ways to **mimic** Bell inequality **violation with LHV** if one is not sufficiently careful.

  Is crucial for Crypto, when fake violations may lead to wrong assumptions about the info that Eve has!

Loopholes

- There are ways to **mimic** Bell inequality **violation with LHV** if one is not sufficiently careful.

  Is crucial for Crypto, when fake violations may lead to wrong assumptions about the info that Eve has!

  - Detection Loophole: If an adversary can choose (adaptively) which qubits are detected, then she can achieve higher β on the post-selected, detected qubits
  - **Crucial for QKD** implies that **high detection rates** are essential!

Loopholes

- There are ways to **mimic** Bell inequality **violation with LHV** if one is not sufficiently careful.

  Is crucial for Crypto, when fake violations may lead to wrong assumptions about the info that Eve has!

  - Detection Loophole: If an adversary can choose (adaptively) which qubits are detected, then she can achieve higher β on the post-selected, detected qubits
  - **Crucial for QKD** implies that **high detection rates** are essential!
  - Locality Loophole: If the two parties are not far enough the basic assumption that observables depend only on their local measurement setting is violated (not big issue for photonic implementations)

Loopholes

- There are ways to **mimic** Bell inequality **violation with LHV** if one is not sufficiently careful.

  Is crucial for Crypto, when fake violations may lead to wrong assumptions about the info that Eve has!

  - Detection Loophole: If an adversary can choose (adaptively) which qubits are detected, then she can achieve higher β on the post-selected, detected qubits
  - **Crucial for QKD** implies that **high detection rates** are essential!
  - Locality Loophole: If the two parties are not far enough the basic assumption that observables depend only on their local measurement setting is violated (not big issue for photonic implementations)

- Only in 2015 loophole-free violation was observed!

Semi-Device Independent Quantum Cryptography

- Rates and detection efficiency makes DI very hard currently for practical applications

- Can have weaker (but more practical) variations:
  Semi-Device Independent

Semi-Device Independent Quantum Cryptography

- Rates and detection efficiency makes DI very hard currently for practical applications

- Can have weaker (but more practical) variations:
  Semi-Device Independent

- 1-side DI: Untrusted/black-box only the one-side (e.g. Bob's measuring device) but the other side is trusted

Semi-Device Independent Quantum Cryptography

- Rates and detection efficiency makes DI very hard currently for practical applications

- Can have weaker (but more practical) variations:
  Semi-Device Independent

- 1-side DI: Untrusted/black-box only the one-side (e.g. Bob's measuring device) but the other side is trusted

- Measurement-device independent: Protocol that does not require trust on any **measuring device**. Measuring-devices are liable to hacking attacks easier (e.g. "blinding-attack") so such protocols are useful

Semi-Device Independent Quantum Cryptography

- Rates and detection efficiency makes DI very hard currently for practical applications
- Can have weaker (but more practical) variations: **Semi-Device Independent**
- 1-side DI: Untrusted/black-box only the one-side (e.g. Bob's measuring device) but the other side is trusted
- Measurement-device independent: Protocol that does not require trust on any **measuring device**. Measuring-devices are liable to hacking attacks easier (e.g. "blinding-attack") so such protocols are useful
- Bounded dimension: Make a min assumption on **dimension** of systems that Alice's and Bob's devices process.