Device-Independent Quantum Key Distribution (QKD) Secure Against Collective Attacks

Non-Locality and Contextuality
(2nd Semester - 2023/2024)
Técnico Lisboa, ULisboa

by

Rúben André Barreiro
ruben.andre.letra.barreiro@tecnico.ulisboa.pt

June 23, 2024

Contents

Introduction

Cryptography in the post-quantum era

- **Future quantum threats on cryptography include:**
  - Simon's, Grover's, Brassard-Høyer-Tapp (BHT), and Shor's Algorithms
- **Two new main approaches arise...**

	(Classical) Post-Quantum Cryptography	**Quantum Cryptography**
Foundation	(Still Believed) Hard Mathematical Problems	Quantum Mechanics and Physics
Type of Information	Classical	(Mainly) Quantum
Encoding	N/A	Discrete-Variables (DV) for qubits or Continuous-Variables (CV) for qumodes
Strategies	N/A	Prepare-and-Measure or Entanglement
Families	Lattice-based, Code-based, Hash-based, Isogeny-based, Multivariate, and Zero-Knowledge Proofs (ZKPs)	Quantum Key Distribution (QKD), Semi-Quantum Key Distribution (QKD), Quantum Conference Key Agreement (QCKA), Quantum Digital Signature Scheme (QDSS), Quantum Bit Commitment (QBC), Quantum Oblivious Transfer (QOT), and Quantum Multi-Party Computation (QMPC)
Popular Primitives	CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+, McEliece, HQC, and BIKE	BB84, B92, SSP, SARG04, E91, BBM92, KMB09, T12, Decoy State, Squeezed State, DPS, MSZ96, GG02

Table 1: Overview of the two main approaches for cryptography in the post-quantum era

What is a Quantum Key Distribution (QKD) protocol?

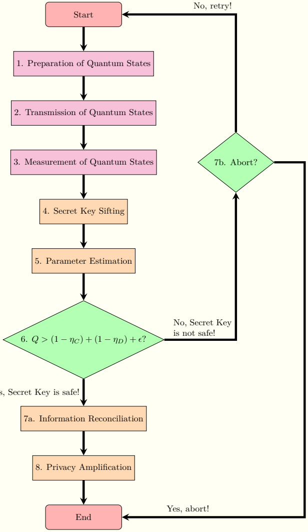

Figure 1: Flowchart of a QKD protocol

1. **Preparation of Quantum States**
2. **Transmission of Quantum States**
3. **Measurement of Quantum States**
4. **Secret Key Sifting**
   - Discard incompatible measurements
5. **Parameter Estimation**
   - Estimates Quantum Bit Error Rate (QBER), Holevo bounds, Key rates
6. (**Eavesdropping detected?**) $\Rightarrow Q > (1-\eta_C) + (1-\eta_D) + \epsilon$?

7a. Yes! $\Rightarrow$ **Information Reconciliation**
   - Cascade Protocol, Low-Density Parity Check (LDPC) Code

7b. No! $\Rightarrow$ Abort? (or Retry?)

8. **Privacy Amplification Estimation**
   - Toeplitz Hashing, Tabular Hashing

Attacks on QKD protocols

- ***Independent and identically distributed* (*i.i.d.*) rounds:**
  - The devices behave independently and in the same way
  - The quantum states distributed are always the same
- **There are three main attacks on QKD protocols:**
  - **Individual Attacks:**
    - The eavesdropper has no quantum memory
    - The eavesdropper can only attack each round individually
  - **Collective Attacks:**
    - The eavesdropper has no quantum memory
    - The eavesdropper can perform arbitrary global operations
  - **Coherent Attacks:**
    - The eavesdropper has quantum memory (trace of rounds)
    - The eavesdropper can perform arbitrary global operations
    - The parties' quantum states can be arbitrarily correlated

Problem

Can a QKD protocol with untrusted quantum devices be secure?

- **Considering Entanglement-based QKD protocols:**
  - The entangled particles are emitted from a common source
  - The parties measure each particle on a randomly chosen basis
  - Here, we assume that:
    - The locations of the parties (Alice and Bob) are secure
    - Alice and Bob trust their measuring devices
  - The source of the entangled particles:
    - Does not need to be trusted by Alice and Bob
    - Might be under the control of an eavesdropper (Eve)
- **And about untrusted quantum measurement devices?**
  - No guarantees on the expected measurement bases
  - No assumptions on the dimension of the Hilbert Space

Motivation

- **Device-Independent - Quantum Key Distribution (DI-QKD)** is a concept of security for QKD protocols that:
  - **Seeks to ensure the security of QKD protocols:**
    - **Without considering any details about the internal working of the quantum devices being used:**
      - The quantum devices can be imperfect, untrusted, or manipulated by a malicious party
    - **Based on the violation of Bell Inequalities:**
      - Quantum correlations between the quantum devices
      - The security is inferred directly from those quantum correlations observed on the outcomes
      - Do not exist any local hidden variables
  - **It is a "holy-grail" on Quantum Cryptography!**

- **Device-Independent - Quantum Key Distribution (DI-QKD)** requires the following basic assumptions:
  - **The physical locations of the parties are secure**
    - No unwanted information can leak out to the outside
  - **The parties have a Trusted Random Number Generator (TRNG), producing a classical random output**
    - Possibly, one derived from thermal noise or based on a Quantum Random Number Generator (QRNG)
  - **The parties have trusted classical devices**
    - Capable of storing and processing the classical data generated by their quantum devices
  - **The parties share a public authenticated classical communication channel**
    - The parties can start with a small shared secret
  - **Quantum Mechanics is correct (and well-defined)**

- **Some reasons lead the (usual) QKD protocols to be insecure in Device-Independent (DI) scenarios:**
  - **Sometimes they produce classical correlations**
    - We can reproduce them without quantum mechanics
    - We can generate them from a set of classical random data shared by the parties' systems
  - Those classical correlations can be written as:
    - $P(ab|XY) = \sum_{\lambda} P(\lambda) \times D(a|X,\lambda) \times D(b|Y,\lambda)$

    Where:
    - λ is a classical variable with probability distribution $P(\lambda)$, shared by the parties' quantum devices
    - $D(a|X,\lambda)$ is a function that completely specifies Alice's outputs once the input X and the variable λ are given
    - $D(b|Y,\lambda)$ is a function that completely specifies Bob's outputs once the input Y and the variable λ are given

- **Some reasons lead the (usual) QKD protocols to be insecure in Device-Independent scenarios:**
  - A copy of λ will give the full information about the outputs a and b to Eve, once the inputs X and Y are announced
  - However... The strategy for these correlations is not available to the eavesdropper **if the outputs** a **and** b**:**
    - **Are correlated in a non-local way**
    - **Violate a Bell Inequality**
  - Therefore, **the violation of a Bell Inequality is a key requirement for the security of DI-QKD protocols!**

Results

What are the ingredients of a DI-QKD protocol?

- **Let's consider the following QKD protocol:**
  - Alice and Bob share an entangled Werner quantum state
    - $\rho_{AB} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{I}}{4}$

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

      the term $\frac{\mathbb{I}}{4}$ represents white noise
  - They choose a measurement to apply to their particles for each round, resulting on binary outcomes, where:
    - Alice has three measurements choices: $X \in \{A_0, A_1, A_2\}$

      • $A_0 = \sigma_z$ • $A_1 = \frac{(\sigma_z+\sigma_x)}{\sqrt{2}}$ • $A_2 = \frac{(\sigma_z-\sigma_x)}{\sqrt{2}}$
    - Bob has two measurements choices: $Y \in \{B_0, B_1\}$

      • $B_1 = \sigma_z$ • $B_2 = \sigma_x$
    - The binary outcomes are denoted as $\{+1, -1\}$

What are the ingredients of a DI-QKD protocol?

- **Regarding this QKD protocol:**
  - The (initial) raw key is extracted from the resulting outcomes of the pair of measurements $\{A_0, B_1\}$:
    - For which the QBER Q is defined as follows:
      - $Q = P(a \neq b|01) = P(a \neq b|A_0, B_1) =$
        $= P(a = 0, b = 1|A_0, B_1) + P(a = 1, b = 0|A_0, B_1)$
    - In this context, the QBER Q is used for:
      - Estimating the amount of quantum correlations
      - Quantifying the amount of classical communication required for the Error Correction protocol/code

What are the ingredients of a DI-QKD protocol?

- **Regarding this QKD protocol:**
  - The measurements A_1, A_2, B_1, and B_2 are used on a subset of the particles to estimate the Clauser-Horne-Shimony-Holt (CHSH) polynomial:
    - $S = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle$

      - Where the correlators are defined as $\langle a_i b_j \rangle = P(a = b|i,j) - P(a \neq b|i,j)$
    - The CHSH polynomial is used by the parties to:
      - Bound Eve's potential partial information about the key
      - Define how much secret information leaked to Eve needs to be reduced during the Privacy Amplification step
  - **The parameters Q and S are used to estimate the information available to a potential eavesdropper**

What are the ingredients of a DI-QKD protocol?

- **Regarding this QKD protocol:**
  - The CHSH polynomial's correlations satisfy:
    - $Q = \frac{1}{2} - \frac{p}{2} \Leftrightarrow \frac{p}{2} = \frac{1}{2} - Q \Leftrightarrow p = 1 - 2Q$
    - $S = 2\sqrt{2}p = 2\sqrt{2}(1 - 2Q)$
  - Regarding the CHSH polynomial, we have:
    - Classically correlated data, for $p \leq \frac{1}{\sqrt{2}}$, and thus, $S \leq 2$
      - In this case, secure DI-QKD protocol is not possible
    - Maximal quantum violation, for $p = 1$, and thus, $S = 2\sqrt{2}$
      - No available information for the eavesdropper
    - **Now, we can interpolate for the range $\frac{1}{\sqrt{2}} < p \leq 2\sqrt{2}$!**
  - To bound the eavesdropper's information:
    - **No assumptions about:**
      - **Behaviour of quantum measurements choices X and Y**
      - **Dimension of the quantum systems ρ_{AB}**

How to prove the security of a DI-QKD protocol?

- **Let's consider some eavesdropping strategies:**
  - **For the most general attacks:**
    - The only data available to the parties to bound the eavesdropper's knowledge is:
      - The observed relation between the inputs and outputs
    - No assumptions on the type of quantum measurements and quantum physical systems used are made
    - Generally, we can model these attacks as a tripartite entangled quantum state $|\Psi\rangle_{ABE} \in \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E$

      - Where: n is the number of bits of the raw key
    - The size of the Hilbert Space of the parties' systems is:
      - Unknown to the parties
      - Fixed (and known) to the eavesdropper

How to prove the security of a DI-QKD protocol?

- **Let's consider some eavesdropping strategies:**
  - **Focusing on collective attacks:**
    - The eavesdropper applies the same attack to each quantum physical system of the parties
      - The quantum states are *i.i.d.*, and thus, $|\Psi\rangle_{ABE} = |\psi\rangle_{ABE}^{\otimes n}$
    - The quantum measurement devices
      - Have no memory register
      - Behave *i.i.d.* in every round of the QKD protocol
    - The (asymptotic) secret key rate r has a lower bound given by the Devetak-Winter key rate r_{DW} formula:
      - $r \geq r_{DW} = \underbrace{I(A_0 : B_1)}_{\text{Mutual information between Alice and Bob}} - \underbrace{\chi(B_1 : E)}_{\text{Holevo quantity between Eve and Bob}}$

How to prove the security of a DI-QKD protocol?

- **Let's consider some eavesdropping strategies:**
  - **Focusing on collective attacks:**
    - The mutual information between Alice and Bob is given as:
      - $I(A_0 : B_1) = \underbrace{H(A_0)}_{\substack{\text{Individual (binary)} \\ \text{Shannon entropy} \\ \text{for Alice}}} + \underbrace{H(B_1)}_{\substack{\text{Individual (binary)} \\ \text{Shannon entropy} \\ \text{for Bob}}} - \underbrace{H(A_0, B_1)}_{\substack{\text{Joint (binary)} \\ \text{Shannon entropy} \\ \text{for Alice and Bob}}}$
    - Since we assume uniform marginals, we also have:
      - $I(A_0 : B_1) = 1 - H(Q) \Big\} \substack{\text{Individual (binary)} \\ \text{Shannon entropy on QBER}}$
    - The Holevo quantity between Eve and Bob is given as:
      - $\chi(B_1 : E) = S(\rho_E) - \frac{1}{2} \sum_{b_1 = \pm 1} S(\rho_{E|b_1})$

      Where:

      - ρ_E denotes the Eve's quantum state after (partially) tracing out Alice and Bob's particles, i.e., $\rho_E = Tr_{AB} \left(|\psi\rangle_{ABE} \langle\psi|_{ABE} \right)$
      - $\rho_{E|b_1}$ denotes the Eve's quantum state when Bob has obtained the outcome result b_1 for the measurement setting $B_1 = \sigma_z$

How to prove the security of a DI-QKD protocol?

- **Let's consider some eavesdropping strategies:**
  - **Security against collective attacks:**
    - The optimal collective attack occurs when:
      - The tripartite entangled quantum state $|\psi\rangle_{ABE}$ is the purification of the (original) bipartite entangled quantum state ρ_{AB}
      - The Holevo quantity $\chi(B_1 : E)$ achieves its possible largest value (compatible with the parameters Q and S)
  - **When the parties symmetrize their uniform marginals:**
    - $\left.\chi(B_1 : E) \leq h\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2-1}}{2}\right)\right\}$ Theorem for DI-QKD
  - **Considering the optimal collective attack:**
    - We have to consider $\chi(B_1 : E) = h\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2-1}}{2}\right)$
      - Without violating the Bell Inequality (for $S \leq 2$), the Holevo bound will be $\chi(B_1 : E) \leq h\left(\frac{1}{2}\right) \Leftrightarrow \chi(B_1 : E) \leq 1$ (full information for Eve)
    - The key rate is given by $r \geq 1 - h(Q) - h\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2-1}}{2}\right)$

How QBERs Q impact the (usual) Entanglement-based QKD and DI-QKD protocols?

- **For Holevo bounds:**

- Greater Holevo bounds for the DI-QKD protocol
- We can easily detect the presence of an eavesdropper for the DI-QKD protocol, allowing to tolerate better the QBER
- For a QBER Q around 14%, the eavesdropper has all the information about the raw key in the DI-QKD protocol

- **For Devetak-Winter key rates:**

- Lower Devetak-Winter key rates for the DI-QKD protocol
- The noise introduced by the eavesdropper will have a greater impact on the DI-QKD protocol, reducing the key rate
- For a QBER Q around 7%, no extractable secure raw key will be possible in the DI-QKD protocol

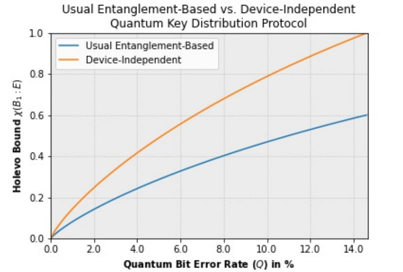

Figure 2: Holevo bounds with respect to QBER Q

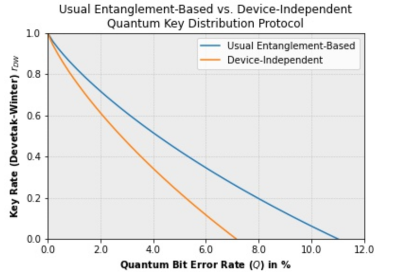

Figure 3: Devetak-Winter key rates with respect to QBER Q

Conclusion

Some possible directions and open questions

- **Possible directions:**
  - Consider other quantum cryptographic protocols:
    - Based on different Bell inequalities
    - Even under the assumption of collective attacks
  - Consider situations in which the eavesdropper may:
    - Have partial information about measurement settings
- **Open questions:**
  - **How is the security of the DI-QKD protocol modified for two-way Information Reconciliation techniques?**
    - Is a Bell inequality violation sufficient for security?
  - **Is de Finetti theorem extendable to the DI scenario?**
    - Does the security against collective attacks implies security against the most general type of attacks?

Thanks for your attention!