Device-Independent Quantum Key Distribution Secure Against Collective Attacks

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

by

Rúben André Barreiro

June 19, 2024

Contents

Introduction

Cryptography in the post-quantum era

- Some future quantum threats are expected to impact modern classical cryptography we use today
  - Grover's Algorithm
    - Unstructured searches, with a complexity of $O(\sqrt{N})$
    - Brute-force attacks on cryptographic key spaces
    - Halves the security strength of Advanced Standard Encryption (AES)
    - AES-128 and AES-192 are no longer secure!
  - Simon's Algorithm
    - Queries to black boxes, with complexity of $O(N)$
    - Brute-force attacks on cryptographic key spaces
    - Not clear yet how can affect the security strength of Advanced Standard Encryption (AES)

Cryptography in the post-quantum era

- Some future quantum threats are expected to impact modern classical cryptography we use today (cont.)
  - Brassard-Høyer-Tapp (BHT) Algorithm
    - Also known as Quantum Birthday Attack
    - Combination of Grover's algorithm and Birthday Paradox
    - Collision searches, with a complexity of $O(\sqrt[3]{N})$
    - Reduces the security strength of Secure Hash Algorithm 3 (SHA-3) by $\frac{1}{3}$
    - SHA-3-224 and SHA-3-256 are no longer secure!
  - Shor's Algorithm
    - Solves factorization, discrete logarithm, and period finding problems, with a complexity of $O(\log(N)^2 \times \log(\log(N)) \times \log(\log(\log(N))))$
    - Completely breaks Rivest-Shamir-Adleman (RSA), Finite Field Diffie-Hellman (FF-DH), and Elliptic Curve Cryptography (ECC)!

Cryptography in the post-quantum era

- **New cryptographic primitives are needed! Specially:**
  - Asymmetric public-key cryptography
  - Key exchange protocols
- **Two new main approaches arise:**
  - (Classical) Post-Quantum Cryptography
    - Relies on mathematical problems (still believed) to be hard on both classical and quantum contexts
    - Uses classical information
    - Several cryptographic families:
      - Lattice-based, Code-based, Hash-based, Isogeny-based, Multivariate, and Zero-Knowledge Proofs (ZKPs)
    - New standards already chosen include:
      - Lattice-based: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON
      - Hash-based: SPHINCS^{+}

Cryptography in the post-quantum era

- **Two new main approaches arise (cont.):**
  - Quantum Cryptography
    - Relies on quantum mechanics and physics
    - Uses (mainly) quantum information
    - Based on Discrete-Variable (DV) for qubits
    - Based on Continuous-Variables (CV) for qumodes
    - Applies Prepare-and-Measure or Entanglement strategies
    - Popular cryptographic primitives include:
      - Quantum Key Distribution (QKD)
      - Semi-Quantum Key Distribution (SQKD)
      - Quantum Conference Key Agreement (QCKA)
      - Quantum Digital Signature Scheme (QDSS)
      - Quantum Bit Commitment (QBC)
      - Quantum Oblivious Transfer (QOT)
      - Quantum Multi-Party Computation (QMPC)

What is a Quantum Key Distribution (QKD) protocol?

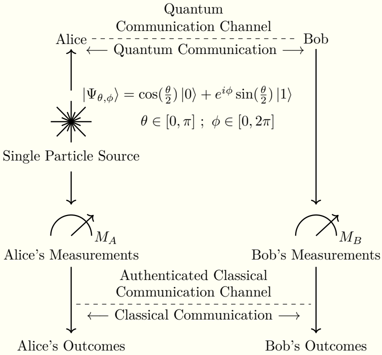

Figure 1a: Schematic of a Prepare-and-Measure QKD protocol

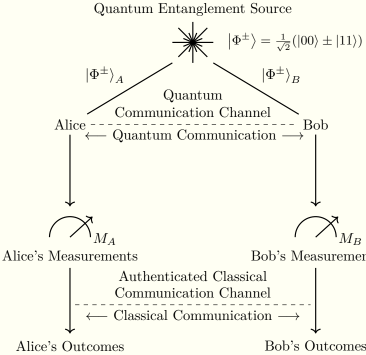

Figure 1b: Schematic of an Entanglement-based QKD protocol

What is a Quantum Key Distribution (QKD) protocol?

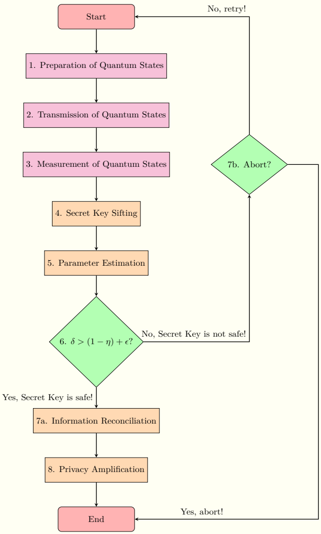

Figure 2: Flowchart of a QKD protocol

1. Preparation of Quantum States
   - Single Particles, Entangled Particles, Coherent States, Fock States, etc.
2. Transmission of Quantum States
   - Uses a quantum communication channel with a certain efficiency η_C
   - “Flying” quantum states can be eavesdropped, with noisy effects ϵ
3. Measurement of Quantum States
   - Uses quantum measurement devices with a certain efficiency η_D
   - Composes a raw key
4. Secret Key Sifting
   - Identifies which protocol rounds can be used to compose a sifted key

What is a Quantum Key Distribution (QKD) protocol?

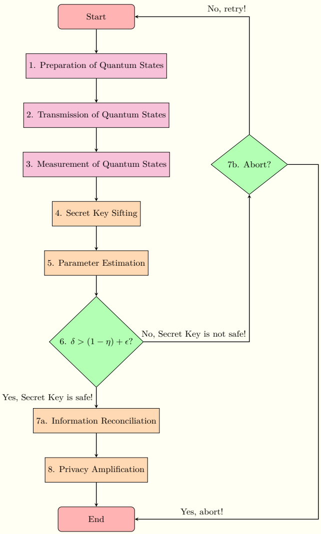

Figure 2: Flowchart of a QKD protocol

5. Parameter Estimation
   - Samples and evaluates the Quantum Bit Error Rate (QBER) δ of the quantum communication channel
   - Estimates the key rate
   - Estimates the secure mutual information between Alice and Bob
6. (Eavesdropping detected?)

   $\Rightarrow \delta > (1-\eta_C) + (1-\eta_D) + \epsilon$?

   7a. Yes! $\Rightarrow$ Information Reconciliation
   - Applies an Error Correction Code (ECC) to correct the sifted into an error-free key
   - These ECC algorithms include:
     - Cascade protocol, Winnow protocol, and Low-Density Parity-Check (LDPC) codes
   - Can be accelerated by classical software and hardware (e.g., OpenMP, CUDA, etc.)

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

What is a Quantum Key Distribution (QKD) protocol?

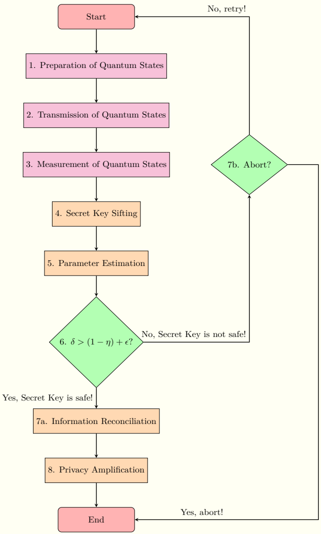

Figure 2: Flowchart of a QKD protocol

8. Privacy Amplification Estimation
   - Applies a Universal Hash Function on the error-free key, composing the final (and amplified) secret key
   - This Universal Hash Function can be a Toeplitz Hashing procedure, usually applied using a random seed as well
   - Can be accelerated by classical software and hardware (e.g., OpenMP, CUDA, etc.)

- The Secret Key Sifting, Parameter Estimation, Information Reconciliation, and Privacy Amplification steps require an authenticated and interactive exchange of classical information
  - We can achieve it with a Carter-Wegman Message Authentication Code (CW-MAC), requiring an initial small secret defined *a priori*

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
  - The measurement outcomes:
    - Are kept private and secret
    - Compose the (initial) raw key
  - Here, we assume that:
    - The locations of the parties (Alice and Bob) are secure
    - The parties (Alice and Bob) trust their measuring devices
  - The source of the entangled particles:
    - It is not trusted by the parties (Alice and Bob)
    - Might be under the control of an eavesdropper (Eve)

Can a QKD protocol with untrusted quantum devices be secure?

- Considering Entanglement-based QKD protocols:
  - The source of the entangled particles is **not trusted**:
    - Example:
      - The eavesdropper could replace the original source of entangled particles by a new one
      - This new source of entangled particles produces quantum states that give it useful information about the parties' measurement outcomes
    - However, the parties (Alice and Bob) can...
      1. Perform measurements in well-chosen bases on a random subset of particles
      2. Compare their measurement results
      3. Estimate the quantum states they receive from the eavesdropper
      4. Decide whether a secret key can be extracted from those quantum states

Can a QKD protocol with untrusted quantum devices be secure?

- Considering Entanglement-based QKD protocols:
  - And about the cases that even the measuring devices are **not trusted**?
    - Examples:
      - The measurement directions may drift with time due to manufacture imperfections
      - A malicious party might have fabricated them
    - In those cases, the parties (Alice and Bob)...
      - Have no guarantee that the actual measurement bases correspond to the expected ones
      - Cannot even make assumptions about the dimension of the Hilbert Space defined in those physical apparatuses
- QKD protocols can often ensure unconditional security
  - If combined with One-Time Pad (OTP)
  - But... They can be susceptible to side-channel attacks!

Motivation

What is a Device-Independent - Quantum Key Distribution (DI-QKD) protocol?

- 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
      - Therefore, guarantees the security of a QKD protocol even when the quantum devices are imperfect, untrusted, or manipulated by a malicious party
    - Based on the violation of Bell Inequalities, ensuring that:
      - There are quantum correlations between the quantum devices being used
      - The security is inferred directly from those quantum correlations observed on the outcomes from the quantum measurement devices
      - Do not exist any local hidden variables
  - It is considered a “holy-grail” on Quantum Cryptography!

- Device-Independent - Quantum Key Distribution (DI-QKD) is a concept of security for QKD protocols that:
  - However... Needs basic assumptions to be ensured:
    - 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)

- How can DI-QKD protocols possibly be secure?
  - Some reasons lead the (usual) QKD protocols to be insecure in Device-Independent scenarios:
    - Sometimes they produce classical correlations
      - We can reproduce them without invoking quantum mechanics at all
      - 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

- How can DI-QKD protocols possibly be secure?
  - Some reasons lead the (usual) QKD protocols to be insecure in Device-Independent scenarios:
    - A copy of the variable λ will give the full information about the parties' outputs a and b to an eavesdropper (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 of the parties' quantum devices
      - 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:
  - The parties (Alice and Bob) share a quantum communication channel between them
    - Consisting of common source of entangled particles
      - Producing 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
  - The parties choose a measurement to apply to their particles for each round, resulting on binary outcomes
    - Alice has three measurements choices: $X \in \{A_0, A_1, A_2\}$
      - Where: $A_0 = \sigma_z, A_1 = \frac{(\sigma_z+\sigma_x)}{\sqrt{2}}, A_2 = \frac{(\sigma_z-\sigma_x)}{\sqrt{2}}$
    - Bob has two measurements choices: $Y \in \{B_0, B_1\}$
      - Where: $B_1 = \sigma_z, B_2 = \sigma_x$
    - The binary outcomes are denoted as $\{+1, -1\}$

What are the ingredients of a DI-QKD protocol?

- Let's consider the following QKD protocol:
  - Recall that:

- $$\rho_{AB} = \begin{bmatrix} \frac{(1+p)}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{(1-p)}{4} & 0 & 0 \\ 0 & 0 & \frac{(1-p)}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{(1+p)}{4} \end{bmatrix}$$

- $A_0 = B_1 = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- $A_1 = \frac{(\sigma_z + \sigma_x)}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$
- $B_2 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $A_2 = \frac{(\sigma_z - \sigma_x)}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$

What are the ingredients of a DI-QKD protocol?

- Let's consider the following QKD protocol:
  - The (initial) raw key is extracted from the resulting outcomes of the pair of measurements $\{A_0, B_1\}$
    - The Quantum Bit Error Rate (QBER) is defined as:
      - $Q = P(a \neq b|01) = P(a \neq b|A_0, B_1) =$
        $= P(a = 0, b = 1|A_0, B_1) + P(a = 1, b = 0|A_0, B_1)$

      - Estimates the amount of quantum correlations between the parties, using the same measurement
      - Quantifies the amount of classical communication required for the Error Correction protocol/code during the Information Reconciliation step

What are the ingredients of a DI-QKD protocol?

- Let's consider the following 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 the eavesdropper's potential partial information about the (weak) error-free key
      - Define how much secret information available to a potential eavesdropper 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?

- Let's consider the following QKD protocol:
  - The CHSH polynomial's correlations satisfy:
    - $Q = \frac{1}{2} - \frac{p}{2} \Leftrightarrow \frac{p}{2} = \frac{1}{2} - Q \Leftrightarrow p = 1 - 2Q$
    - $S = 2\sqrt{2}p = 2\sqrt{2}(1 - 2Q)$
  - In order to bound the potential eavesdropper's available information, the parties do not need to assume that:
    - They perform the measurements A_0, A_1, A_2, B_1, and B_2
    - The quantum systems ρ_{AB} are of dimension 2
  - 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, $S = 2\sqrt{2}$
      - In this case, the potential eavesdropper has
      has no available information about the secret key
    - Now, we can interpolate for the range $\frac{1}{\sqrt{2}} < p \leq 2\sqrt{2}$
      to prove the security of the DI-QKD protocol

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

- Let's consider the following 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 d of the Hilbert Space of the parties' quantum physical 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 the following eavesdropping strategies:
  - Focusing on collective attacks:
    - The eavesdropper applies the same attack to each quantum physical system of the parties
      - The respective quantum states are *independent and identically distributed* (*i.i.d.*), and thus, $|\Psi\rangle_{ABE} = |\psi\rangle_{ABE}^{\otimes n}$
    - The quantum measurement devices
      - Have no memory register
      - Behave *independent and identically distributed* (*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 the following 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:
      - $I(A_0 : B_1) = 1 - H(Q) \Big\}$ Individual (binary) 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 the following 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:
    - $\chi(B_1 : E) \leq h\left(\frac{1+\sqrt{(\frac{S}{2})^2-1}}{2}\right)$ } Theorem for DI-QKD
  - Considering the optimal collective attack:
    - We have to consider $\chi(B_1 : E) = h\left(\frac{1+\sqrt{(\frac{S}{2})^2-1}}{2}\right)$
    - The key rate is given by $r \geq 1 - h(Q) - h\left(\frac{1+\sqrt{(\frac{S}{2})^2-1}}{2}\right)$

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

- Simplifying the calculations for the DI-QKD protocol...
  - Recall that for the CHSH polynomial, we have:
    - $S = 2\sqrt{2}(1 - 2Q)$
  - We can simplify the (maximum) Holevo bound $\chi(B_1 : E)$ and Devetak-Winter key rate r_{DW} for the DI-QKD protocol:
    - $\chi(B_1 : E) = h\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2-1}}{2}\right) = h\left(\frac{1+\sqrt{\left(\frac{2\sqrt{2}(1-2Q)}{2}\right)^2-1}}{2}\right)$
    - $r \geq r_{DW} = 1 - h(Q) - h\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2-1}}{2}\right) =$

$$= 1 - h(Q) - h\left(\frac{1+\sqrt{\left(\frac{2\sqrt{2}(1-2Q)}{2}\right)^2-1}}{2}\right)$$

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

- Simplifying the calculations for the (usual) Entanglement-based QKD protocol...
  - Recall that for the CHSH polynomial, we have:
    - $S = 2\sqrt{2}(1 - 2Q)$
  - The respective Holevo bound is given as follows:
    - $\chi(B_1 : E) \leq h\left(Q + \frac{S}{2\sqrt{2}}\right)$
  - We can simplify the (maximum) Holevo bound $\chi(B_1 : E)$ and the Devetak-Winter key rate r_{DW} for the (usual) Entanglement-based QKD protocol:
    - $\chi(B_1 : E) = h\left(Q + \frac{S}{2\sqrt{2}}\right) = h\left(Q + \frac{2\sqrt{2}(1-2Q)}{2\sqrt{2}}\right) = \\ = h\left(Q + (1 - 2Q)\right) = h\left(1 - Q\right)$
    - $r \geq r_{DW} = 1 - h(Q) - h\left(Q + \frac{S}{2\sqrt{2}}\right) = \\ = 1 - h(Q) - h\left(Q + \frac{2\sqrt{2}(1-2Q)}{2\sqrt{2}}\right) \\ = 1 - h(Q) - h\left(Q + (1 - 2Q)\right) = 1 - h(Q) - h(1 - Q)$

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

What are the differences between 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 better tolerate a QBER, in comparison to the Entanglement-Based QKD protocol
- 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 greater impact on the DI-QKD protocol, reducing more the key rate, compared to the Entanglement-Based QKD protocol
- For a QBER Q around 7%, no extractable secure raw key will be possible in the DI-QKD protocol

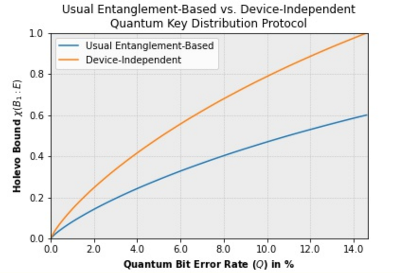

Figure 3: Holevo bounds with respect to QBER Q

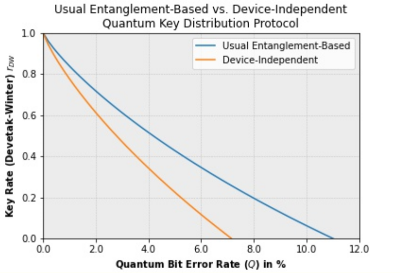

Figure 4: Devetak-Winter key rates with respect to QBER Q

Conclusion