Practical Quantum Key Distribution Secure Against Side Channels

Álvaro Navarrete[1], Margarida Pereira[1], Marcos Curty[1] and Kiyoshi Tamaki[2]

[1]EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[2]Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

Universidade Vigo

UNIVERSITY OF TOYAMA

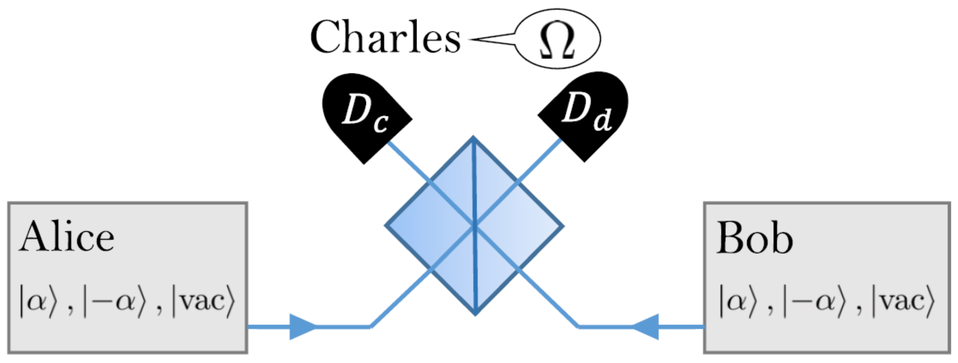
There is a large gap between theory and practice in quantum key distribution (QKD) because real devices do not satisfy the assumptions required by the security proofs. We close this gap by introducing a simple and practical measurement-device-independent-QKD type of protocol, based on the transmission of coherent light, for which we prove its security against any possible imperfection and/or side channel from the quantum communication part of the QKD devices. Our approach only requires to experimentally characterize an upper bound of one single parameter for each of the pulses sent, which describes the quality of the source. Moreover, unlike device-independent (DI) QKD, it can accommodate information leakage from the users' laboratories, which is essential to guarantee the security of QKD implementations.

1. Protocol description

I. Each round Alice (Bob) sends the state $|\nu\rangle$ ($|\omega\rangle$) to the untrusted node Charles with probability p_ν (p_ω), where $\nu, \omega \in \{\alpha, -\alpha, \text{vac}\}$. In particular, the state $|\alpha\rangle$ ($|-\alpha\rangle$) is a coherent state with amplitude α ($-\alpha$) and it is associated with the bit value 0 (1), while the vacuum state $|\text{vac}\rangle$ is only used for parameter estimation.

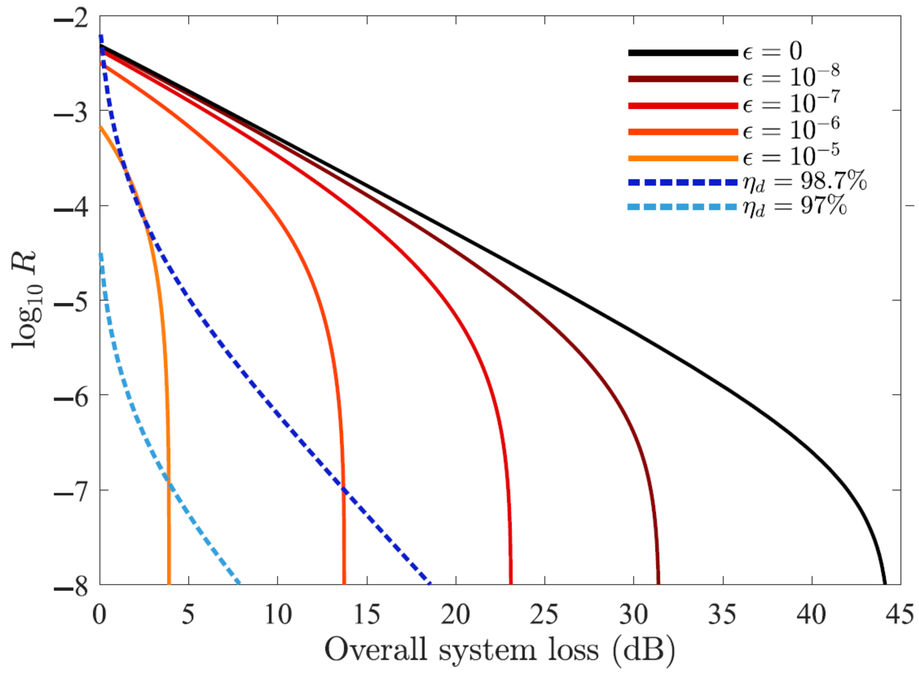
II. If Charles is honest, he causes the incoming pulses to interfere using a 50:50 beam splitter followed by two threshold detectors, and announces the measurement outcome Ω.

III. After N rounds, Alice and Bob reveal part of their state choices to estimate both the bit and the phase error rates. Finally, they perform standard error correction and privacy amplification techniques to obtain, with high probability, a secret key.



3. Numerical results

Below the rate-loss performance of the protocol is shown (solid lines) in the presence of side channels (for simplicity, we set $\epsilon_{\nu,\omega} = \epsilon$). The dark-count probability of Charles' detectors is $p_d = 10^{-8}$. For comparison purposes, the rate-loss performance of a highly optimistic CHSH-based DI-QKD protocol that uses parametric down-conversion sources, qubit amplifiers and photon-number-resolving detectors is also included (dashed lines).



2. Method

Transmitted states

For each particular round of the protocol, the joint state transmitted by Alice and Bob can always be written as

$$|\Psi_{\nu,\omega}\rangle_T = \sqrt{1-\epsilon_{\nu,\omega}}\,|\phi_{\nu,\omega}\rangle_T + \sqrt{\epsilon_{\nu,\omega}}\,|\phi^{\perp}_{\nu,\omega}\rangle_T,$$

where $\epsilon_{\nu,\omega} \in [0,1]$; $|\phi_{\nu,\omega}\rangle_T \coloneqq |\nu\rangle_a|\omega\rangle_b|\tau\rangle_E$ is the joint state *ideally* transmitted by Alice and Bob when they select ν and ω, respectively; $|\tau\rangle$ is a state that contains no information about ν and ω; and $|\phi^{\perp}_{\nu,\omega}\rangle_T$ is a state orthogonal to $|\phi_{\nu,\omega}\rangle_T$. That is, the previous equation represents the most general description of the transmitted states, which means that it allows us to characterize any potential state preparation flaw or information leakage about the internal settings of Alice and Bob.

Phase-error probability

In order to calculate the secret key rate, we first estimate, from the observed statistics, the phase-error probability for those rounds that are used for key generation. For this, we note that any of these rounds can be equivalently described by a fictitious scenario in which, instead, Alice and Bob prepare the entangled state

$$|\Psi^{\text{vir}}\rangle_{ABT} = \tfrac{1}{2}\textstyle\sum_{j,s=0,1}|j_z, s_z\rangle_{AB}\left|\Psi_{(-1)^j\alpha,(-1)^s\alpha}\right\rangle_T,$$

with $\{|0_z\rangle, |1_z\rangle\}$ being the computational basis for the ancilla systems A and B. Now, let $\widehat{\mathcal{D}}$ be the positive operator-valued measure element associated with Charles' successful announcement. Then, the phase error probability can be expressed as

$$\Gamma = \langle\Psi^{\text{vir}}|\widehat{\mathcal{D}}_{\text{ph}}|\Psi^{\text{vir}}\rangle,$$

where $\widehat{\mathcal{D}}_{\text{ph}} = (|0_x, 0_x\rangle\langle 0_x, 0_x| + |1_x, 1_x\rangle\langle 1_x, 1_x|) \otimes \widehat{\mathcal{D}}$, and $|j_x\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle + (-1)^j|1_z\rangle)$.

Reference States

In order to relate the phase-error probability to the observed statistics $Y_{\nu,\omega} = \langle\Psi_{\nu,\omega}|\widehat{\mathcal{D}}|\Psi_{\nu,\omega}\rangle$ we define a set of states $\{|\Phi_{\nu,\omega}\rangle\}$ called reference states[1]. These states are never prepared in the actual protocol (they are used just as a mathematical tool), and they should be similar to the ideally transmitted states. The key point is that the phase-error probability $\Gamma_{\text{ref}} = \langle\Phi^{\text{vir}}|\widehat{\mathcal{D}}_{\text{ph}}|\Phi^{\text{vir}}\rangle$ of these reference states (where $|\Phi^{\text{vir}}\rangle$ is analogous to $|\Psi^{\text{vir}}\rangle$ but for the reference states) can be easily related to the fictitious statistics $Y^{\text{ref}}_{\nu,\omega} = \langle\Phi_{\nu,\omega}|\widehat{\mathcal{D}}|\Phi_{\nu,\omega}\rangle$ that the users would have observe if they had used the reference states in the actual experiment. In particular, by choosing an appropriate set of reference states, one can obtain a linear relation as

$$\Gamma_{\text{ref}} = \mathbf{f}\,\mathbf{Y^{ref}},$$

where $\mathbf{f}$ is a row vector and $\mathbf{Y^{ref}}$ is a column vector containing the yields $Y^{\text{ref}}_{\nu,\omega}$.

Bounding deviations

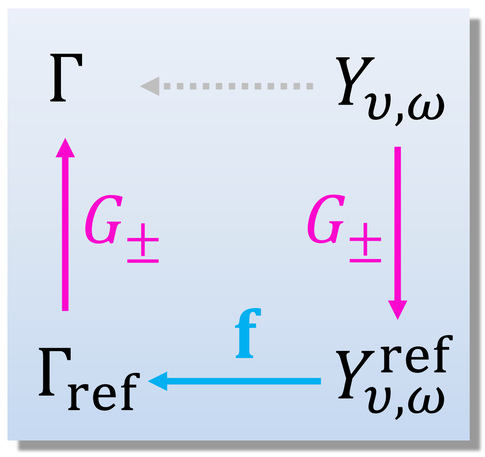
Since the reference states are similar to the actual states, one expects that $\Gamma \approx \Gamma_{\text{ref}}$ and $Y^{\text{ref}}_{\nu,\omega} \approx Y_{\nu,\omega}$. This can be exploited to estimate Γ from the observed statistics $Y_{\nu,\omega}$. In particular, one can upper bound the phase error probability as

$$\Gamma \leq G_+(\Gamma^{\text{U}}_{\text{ref}}, \delta^{\text{L}}_{\text{vir}}),$$

where G_+ is a known function, $\Gamma^{\text{U}}_{\text{ref}}$ is an upper bound on Γ_{ref}, and $\delta^{\text{L}}_{\text{vir}}$ is a lower bound on $\langle\Phi^{\text{vir}}|\Psi^{\text{vir}}\rangle$ that only depends on the quantities $\epsilon_{\nu,\omega}$.

Finally, $\Gamma^{\text{U}}_{\text{ref}}$ can be related to the actual yields $Y_{\nu,\omega}$ by using again some known functions G_+ and G_- that allow to bound the reference yields in $\mathbf{Y^{ref}}$ from the actual yields.

Importantly, we remark that the security of this protocol relies on the characterization of valid upper bounds on the quantities $\epsilon_{\nu,\omega}$ that account for the side-channel information.



[1] Pereira, M., Kato, G., Mizutani, A., Curty, M., & Tamaki, K. (2020). Quantum key distribution with correlated sources. *Science Advances*, *6*(37), eaaz4487.

Navarrete, Á., Pereira, M., Curty, M., & Tamaki, K. (2021). Practical Quantum Key Distribution That is Secure Against Side Channels. *Physical Review Applied*, *15*(3), 034072.