# Simulation of a quantum key distribution scheme in view of a proof-of-principle implementation

**S. ZEBBOUDJ, S. CIALDI, S. OLIVARES & M. OMAR**

Doctoriales de Recherche Opérationnelle, le 12 et 13 Décembre 2018


## Abstract

**Although quantum key distribution schemes have been proven theoretically secure, they are based on assumptions about the devices that are not yet satisfied with today's technology. In this work, we present the experimental setup for a measurement device independent quantum key distribution scheme we have proposed as a part of my PhD research. Through simulations, we give the most appropriate parameters needed for the realisation of the scheme. We also see through simulations how an attack can introduce detectable errors in the distributed secret key.**


## Introduction

Cryptography is the science of encoding and decoding messages. The secrecy of the messages depends entirely on a secret key. In classical key distribution algorithms, the security lies in the assumption of unproven mathematical diffculties of certain problems such as the integer factorization and the discrete logarithm problem. However, in 1997, Peter W. Shor has discovered algorithms able to perform integer factorization and the discrete logarithm in polynomial time on a quantum machine [1]. Such algorithms would make a large number of private and secret keys, already used in industry, obsolete. Therefore, private information would be no longer protected. In contrast to the classical key distribution schemes, the security of Quantum Key Distribution (QKD) draws on laws of physics. Indeed, with Heisenberg's uncertainty principle and the quantum no-cloning theorem, QKD has been proven information theoretically secure i.e. no assumptions are made about the amount of resources available to an eavesdropper, Eve, for computing the secret key. In a previous work, we have proposed a quantum key distribution scheme able to achieve a relatively high secret key generation rate based on two-way quantum key distribution, that also inherits the robustness of the measurement device independent scheme against all detector side-channel attacks. In this work, we simulate the scheme to get the best parameters for a proof-of-principle realization.

## Original scheme

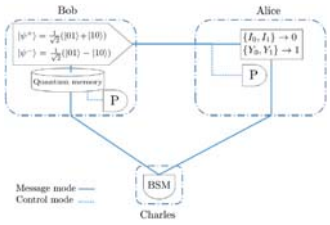


Figure 1. Deterministic measurement device independent QKD [2].

- Bob generates the states $|\psi^+\rangle$ and $|\psi^-\rangle$ with equal probabilities. He sends one qubit (travel qubit) of each pair to Alice and stores the other qubit (home qubit) in his quantum memory.
- Alice and Bob both switch to either message mode or control mode.
- In control mode, Alice measures the travel qubit and Bob measures the home qubit with the projectors $P = \{|v\rangle\langle v|, |H\rangle\langle H|, |V\rangle\langle V|\}$. The results are publicly announced and the probabilities of Alice receiving $|\hat{t}\rangle$ when the travel qubit is $|\hat{f}\rangle$ are shared in order to bound Eve's knowledge on the secret key.
- In message mode, if Alice chooses to encodes the classical bit "0", she performs the operation $I_0\{|v\rangle, |H\rangle, |V\rangle\} = \{|v\rangle, |H\rangle, |V\rangle\}$ or $I_1\{|v\rangle, |H\rangle, |V\rangle\} = \{|v\rangle, -|H\rangle, -|V\rangle\}$ on the travel qubit. Otherwise, she uses the operation $Y_0\{|v\rangle, |H\rangle, |V\rangle\} = \{|v\rangle, |H\rangle, -|V\rangle\}$ or $Y_1\{|v\rangle, |H\rangle, |V\rangle\} = \{|v\rangle, -|H\rangle, |V\rangle\}$ to encode the classical bit "1".
- Also in message mode, Bob and Alice send their qubits to Charles who performs a Bell State Measurement (BSM) and projects the two qubits in either $|\psi^+\rangle$ or $|\psi^-\rangle$. Charles publicly reveals his measurement results.
- For each received BSM result, Bob and Alice establish two bits of the secret key according to their preparation/encoding. The possible outcomes of the secret key are shown in Table 1.

| | $I_0$ | $I_1$ | $Y_0$ | $Y_1$ |
|---|---|---|---|---|
| $\|\psi^+\rangle$ | 00 | 00 | 10 | 10 |
| $\|\psi^-\rangle$ | 01 | 01 | 11 | 11 |

Table 1. Possible outcomes of the BSM.

## Experimental setup

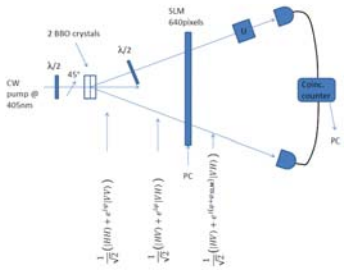


Figure 2. Experimental setup of [2].

- Entangled states of the form $|\phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + \exp^{i\phi}|VV\rangle)$ are generated with a poissonian distribution using two BBO crystals and a continuous wave laser at 405 nm.
- The state $|\psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + \exp^{i\phi}|VH\rangle)$ is obtained from $|\phi\rangle$ by placing a waveplate $(\lambda/2)$ in the path of one of the photons.
- A Spatial Light Modulator (SLM) made of 640 pixels is additionally used to act on the phase of the states and transform them to either $|\psi^+\rangle$ or $|\psi^-\rangle$. When taking into account the purity, $\mu$, the generated state is of the form :

$$\rho_{gen} = \mu\,|\psi_{gen}\rangle\langle\psi_{gen}| + \frac{1-\mu}{2}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|)\,,$$

- The encoding of classical bits "0" and "1", namely the phase shift, is performed with a phase gate. The operation on the travel qubit are represented by the identity matrix $\mathbb{I}$ for the encoding of classical bit "0" and the phase shift operator $\sigma_Z$ for encoding "1".

$$\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -\exp^{i\delta} \end{pmatrix},$$

where $\delta$ is an error introduced when performing the encoding operation.

- Two detectors aligned at 45° are connected to a coincidence counter with which, according to the number of detected events, we can distinguish between the two states.
- The performed measurement can be represented by the two following projectors $\pi^- = |-\rangle\langle -| \otimes |+\rangle\langle +|$ and $\pi^+ = \mathbb{1} - \pi^-$ where,

$$|\pm\rangle = \frac{1}{\sqrt{2}}|H\rangle \pm |V\rangle$$

## Simulation

- The number of photons within each pulse is R = 1000, and the mean number of detected photons are chosen to be $N_1 = Tr[\rho_+\pi^-] \times R \times \Delta t$ for detecting the state $|\psi^+\rangle$, and $N_2 = Tr[\rho_-\pi^-] \times R \times \Delta t$ for detecting the state $|\psi^-\rangle$.
- When $\Delta t$ = 0.08s, we can easily distinguish between $|\psi^+\rangle$ (Blue) and $|\psi^-\rangle$ (Red)

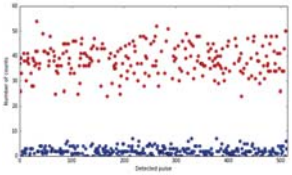

Figure 3. Number of counts in each pulse.

- We can calculate the probability of error as a function of the purity of the prepared state and the encoding error as shown in Figures 4 and 5.

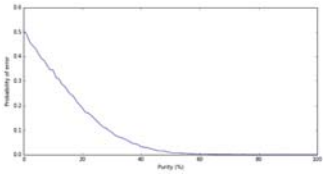

Figure 4. Probability of error as function of the purity.

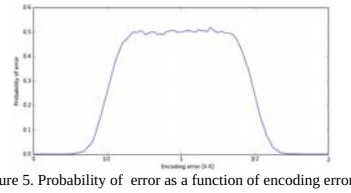

Figure 5. Probability of error as a function of encoding error $\delta$.

- We can also simulate an attack where Eve has to steel photons in order to recover the secret key. Figure 6 shows the probability of error introduced by such attack.

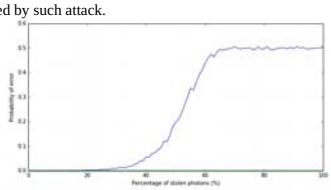

Figure 6. Probability of error as a function of the percentage of stolen photons.

- The overall Quantum Bit Error Rate (QBER) is :

$$QBER = \frac{P_{error} + P_{DC}}{P_{error} + P_{DC} + P_{OK}}$$

where:

- $P_{error}$ is the probability of error introduced by the measurement, and eventually, an attack.
- $P_{DC}$ is the probability of error introduced by dark counts.

$$P_{dc} = (1-\eta^2)^2 d_c^2 + 2(1-\eta^2) d_c \eta^2 \eta_d$$

## Conclusion

The implementation of QKD schemes has been challenged by loopholes in the devices, which have lowered their security level. We have thus initiated the work of implementing a deterministic and measurement device independent QKD scheme [2], we have previously proposed to remove all detector side-channel attacks. Our work aims at proving that our scheme allows us to obtain a higher and more practical final secret key generation rate.

## References


1. **P. SHOR (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM J. Comput. (1997)*, 26(5), 1484–1509.**
2. **S. ZEBBOUDJ & M. OMAR, Deterministic MDI QKD with two secret bits per shared entangled pair, Quantum Inf. Process (2018), 17(3), pp 10.**