Towards the unconditional security proof for the Coherent-One-Way protocol

Mhlambululi Mafu, Adriana Marais, Francesco Petruccione

Quantum Research Group, School of Physics and National Institute for Theoretical Physics, University of KwaZulu-Natal

E-mail: mhlambululi.mafu@gmail.com, adrianamarais@gmail.com and petruccione@ukzn.ac.za

Abstract. Quantum Cryptography, one aspect of which is Quantum Key Distribution, provides the only physically secure and proven method for the transmission of a secret key between two distant parties, Alice and Bob. The goal of QKD is to guarantee that a possible eavesdropper (Eve), with access to the communication channel is unable to obtain useful information about the message. The Coherent-One-Way protocol is one of the most recent practical QKD protocols. However, its unconditional security proof still remains unrealized. We therefore present a necessary condition for the security of the COW protocol, and show that Bob's measurements are described by non-commuting POVM elements which satisfies this condition.

1. Introduction

The Coherent-One-Way (COW) Quantum Key Distribution (QKD) protocol was first proposed by Gisin et al. [1] and belongs to a class of the so-called distributed-phase-reference protocols [2]. Currently no lower bound is known for the unconditional security of this protocol. The existing tools for proving security of protocols against the most general attacks fail to apply to this protocol in a straight forward way. While security proofs for some limited attacks exist, the unconditional security proofs still remain unrealized. This paper presents an improvement in this direction for the COW QKD protocol by presenting a necessary security condition for the most general kind of attacks which is a step towards the unconditional security proof.

Various attacks have been studied for the COW QKD protocol. Security against intercept and resend attacks based on unambiguous state discrimination has been shown [4] as well as for general individual attacks [3]. Upper bounds for the error rates for the security of COW protocol in the presence of large collective attacks as well as collective beam splitting attacks [3] have also been derived [2]. Security against sequential attacks [5] based on unambiguous state discrimination have also been shown [4]. The security against the most general attacks is still elusive because the present tools for proving security of protocols in general cannot be adopted in a straightforward way.

In spite of these proofs against limited examples of kinds of attacks, it still remains unclear how the unconditional security proof can be realized. This is mainly because this class of protocols use coherent sequences of signals which are not symmetric as opposed to qubits in other classes of protocols. Again, these protocols move away from the symbol-per-symbol type of coding [7]. The notation and the formalism to be used to develop a full unconditional security proof is complicated for this class of protocols. Therefore, our goals in this paper is (i) to present why the COW protocol is useful as a means of distributing a key, (ii) to show how the operation of the COW protocol takes place in the absence of a detailed explanation of the protocol as presented in the original literature [1, 6] and illustrate explicitly how the two parties extract the key and (iii) to provide a notation and formalism that can be a necessary condition for the security of COW QKD protocol.

2. Operation of the COW protocol

Alice prepares states $|\phi_0\rangle$ and $|\phi_1\rangle$ which represent logical states '0' and '1' respectively and decoy states in each of $k = 1, ..., N$ time intervals in a two-pulse sequence consisting of a non-empty and an empty pulse:

$$\begin{aligned} |\phi_0\rangle_k &= |\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k}, \\ |\phi_1\rangle_k &= |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}, \\ |\text{decoy}\rangle_k &= |\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}, \end{aligned} \tag{1}$$

where $2k-1$ and $2k$ label the pulses in the pair. In the case of a small mean photon number, the states $|\phi_0\rangle_k$ and $|\phi_1\rangle_k$ have a large overlap because of their vacuum component and also they possess a phase coherence between any two non-empty pulses with a bit separation. The decoy sequences are used to check for coherence in the data line and they are then going to be discarded in the public discussion. Each logical bit of information is encoded in a sequence of two pulses. The key is obtained by measuring the time-of-arrival of photons on the data line, detector D_B. The presence of the eavesdropper is checked interferometrically in a monitoring line by randomly measuring the coherence between the successive non-empty pulses; bit sequences '1-0' or decoy sequences with the interferometer and detectors D_{M1} and D_{M2}. If coherence is broken D_{M2} fires, and an error is recorded.

Bob uses a detector D_B to unambiguously discriminate the non-orthogonal states $|\phi_0\rangle_k$ and $|\phi_1\rangle_k$. Since μ the average photon number is small Bob doesn't always get a click. But sometimes Bob gets a click in time interval k, and if the click corresponds to the first (second) pulse of the pair, he records a zero (one).

3. COW protocol as P&M scheme

Alice prepares a random sequence of predefined non-orthogonal coherent states $\bigotimes_{k=1}^{N} |\psi(s_k)\rangle$, where each coherent state $|\psi(s_k)\rangle = |\phi_0\rangle_k$ or $|\phi_1\rangle_k$ is defined according to Equation 1. These states are sent to Bob through an untrusted quantum channel. On the receiving side, Bob performs a POVM on the signal he receives.

We divide each time slot k into two and label with integers j, such that $j = 1, ..., 2N$ then, according to Figure 1, the signal entering Bob's interferometer in path '0' after each time interval j can be described in terms of the creation operators $\hat{a_0}^{\dagger j}$ and the outgoing paths, $\hat{a_3}^{\dagger j}$, $\hat{a_7}^{\dagger j}$ and $\hat{a_8}^{\dagger j}$. In order to describe the signals entering Bob's interferometer, we follow the same approach used by A. Marais et al. [9], since these protocols belong to the same class. The total action of the interferometer is derived to be

$$\hat{a_0}^{\dagger j} \rightarrow \frac{1}{2\sqrt{2}}(\hat{a_7}^{\dagger j} - e^{i\phi_3}\hat{a_8}^{\dagger j} + 2\hat{a_3}^{\dagger j} + \hat{a_7}^{\dagger (j+1)} + e^{i\phi_3}\hat{a_8}^{\dagger (j+1)}), \tag{2}$$

where the subscripts '0,. . .,8' refer to paths as labelled in Figure 1, and $\phi_1 + \phi_2 + \phi_3 = \phi_{\triangle t}$ are phase shifts associated with symmetric BS1, BS2, BS3 and the time delay, respectively.

When Alice prepares a $|\phi_0\rangle$, the input state is transformed to the output state as follows

$$\begin{aligned} |\phi_0\rangle_k &= |\sqrt{\mu}\rangle_0^{(j-1)}|0\rangle_0^j \\ &\xrightarrow{I} |\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^{j-1}|-e^{i\phi_3}\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_8^{j-1}|\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^{j-1}|\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^j|e^{i\phi_3}\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_8^j. \end{aligned} \tag{3}$$

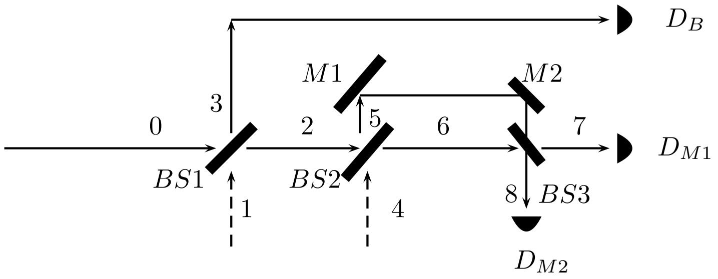

Figure 1. Schematic diagram of the QKD system for realizing the COW protocol. Key extraction takes place along the data-line, with detector D_B. Coherence between successive non-empty pulses is checked interferometrically in the monitoring line with detectors D_{M1} and D_{M2}. BS1, BS2 and BS3 are considered to be symmetric beamsplitters, M1 and M2 are mirrors and '0-8' are paths along which the coherent pulses travel.

$k=6$ ▲▲	$k=5$ △▲	$k=4$ ▲△	$k=3$ ▲△	$k=2$ ▲△	$k=1$ △▲	
	1	0	0	0	1	$\leftarrow c$
$\|\mu\rangle_{12}\|\mu\rangle_{11}$	$\|0\rangle_{10}\|\mu\rangle_9$	$\|\mu\rangle_8\|0\rangle_7$	$\|\mu\rangle_6\|0\rangle_5$	$\|\mu\rangle_4\|0\rangle_3$	$\|0\rangle_2\|\mu\rangle_1$	$\leftarrow b$
decoy	1	0	0	0	1	$\leftarrow a$

Table 1. An example of the implementation of the COW protocol for $k = 1, \ldots, 6$ where k labels pairs; a is the logical bit recorded by Bob; b represents the states received at detector D_B and c is the bit value sent by Alice.

Here, Bob gets a click in D_B which corresponds to a click in time slot $j-1$ with $p_{\text{click}}{=}1-e^{-\mu/8}$, which is the first of the slots constituting interval k, and records a '0'. Since D_7 and D_8 click with equal probability in slots $j-1$ and j, there is no test for coherence from $|0\rangle_k$ above.

When Alice prepares a $|\phi_1\rangle$, the output state is of the form

$$\begin{aligned} |\phi_1\rangle_k &= |0\rangle_0^{(j-1)}|\sqrt{\mu}\rangle_0^j \\ &\xrightarrow{I} |\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^j|\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^j|\tfrac{-\sqrt{\mu}}{2\sqrt{2}}\rangle_8^j|\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^{(j+1)}|\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_8^{(j+1)}. \end{aligned} \tag{4}$$

Here, Bob gets a click in slot j in D_B with $p_{\text{click}} = 1 - e^{-\mu/8}$ and records a '1' for the time interval k. Again, this follows for each of $k = 1, ..., N$ intervals, Bob records a '0'('1') when he gets a click in slot $j = 2k - 1 (j = 2k)$.

In order to check for coherence in the data line, Alice prepares and sends decoy states to Bob. A loss of coherence reveals the presence of an eavesdropper, which contributes to the error rate. When Alice prepares a decoy state, the output is of the form

$$|\text{decoy}\rangle_k = |\sqrt{\mu}\rangle^{(j-1)}|\sqrt{\mu}\rangle^j, \tag{5}$$

but states formed from $|\phi_1\rangle_k|\phi_0\rangle_{k+1}$ can also be used for the channel estimation, i.e., $|\phi_1\rangle_k|\phi_0\rangle_{k+1} = |0\rangle_0^{(j-1)}|\sqrt{\mu}\rangle_0^j|\sqrt{\mu}\rangle_0^{(j+1)}|0\rangle_0^{(j+2)}$. The state $|\sqrt{\mu}\rangle_0^t|\sqrt{\mu}\rangle_0^{(t+1)}$ transforms the interferometer as follows

$$|\sqrt{\mu}\rangle_0^t|\sqrt{\mu}\rangle_0^{(t+1)} \xrightarrow{I} |\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^t|\tfrac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^t|\tfrac{-\sqrt{\mu}}{2\sqrt{2}}\rangle_8^t|\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^{(t+1)}|\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_7^{(t+1)}|0\rangle_8^{(t+1)}|\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_7^{(t+2)}|\tfrac{\sqrt{\mu}}{\sqrt{2}}\rangle_8^{(t+2)}. \tag{6}$$

So, it can be seen that decoy states and $|\phi_1\rangle_k|\phi_0\rangle_{k+1}$ sequences do not contribute to the key since here D_B has a probability to click for both slots j in the pair k, so that Bob learns no key bit. But, if D_{M2} clicks, this is an indication of a loss of coherence since if the consecutive non-empty pulses have a constant relative phase, this detector has zero probability of clicking as seen above.

Table 1 shows how the bits sent by Alice correspond to the sent states. To obtain the bit value, Bob has to distinguish unambiguously between the two non-orthogonal states given in Equation (1), that arrive at his detector. According to Table 1, Alice can also send decoy states. Alternatively, checks for coherence can be done between two consecutive non-empty pulses for example across the pair in $k = 4$ and $k = 5$. Based on these states Bob can record each respective bit as shown in the example depicted by the same Table 1.

4. Bob's Measurements

We exploit the mathematical convenience of POVM's [10, 11] as a tool for describing Bob's measurement statistics. Since Bob has a probability of detecting one or more photons (a click) or vacuum (no click) in each of his detectors in $2N$ time intervals, there are 2^{6N} possible measurement outcomes corresponding to 2^{6N} POVM elements.

The projectors constituting Bob's measurement in the time intervals $j \in \{1, ..., 2N\}$ where j is the superscript, are written as

$$\begin{aligned}
G_1 &= |0\rangle\langle 0|, \\
G_2 &= \sum_{n=1}^{\infty} |n\rangle_3^1\langle n| \otimes |0\rangle\langle 0|, \\
G_3 &= |0\rangle_3^1\langle 0| \otimes \sum_{n=1}^{\infty} |n\rangle_7^1\langle n| \otimes |0\rangle\langle 0|, \\
G_4 &= |0\rangle_3^1\langle 0| \otimes |0\rangle_7^1\langle 0| \otimes \sum_{n=1}^{\infty} |n\rangle_8^1\langle n| \otimes |0\rangle\langle 0|, \\
G_5 &= |0\rangle_3^1\langle 0| \otimes |0\rangle_7^1\langle 0| \otimes |0\rangle_8^1\langle 0| \otimes \sum_{n=1}^{\infty} |n\rangle_3^2\langle n| \otimes |0\rangle\langle 0|, \\
&\ \ . \\
&\ \ . \\
&\ \ . \\
G_{2^{6N}} &= \sum_{n=1}^{\infty} |n\rangle\langle n|. \qquad (7)
\end{aligned}$$

The $G_{i's}$ are projectors onto the basis of photon number states, $|n\rangle$. They represent all possible outcomes for an implementation of the COW protocol with signals sent in $2N$ time intervals. The projectors G_1 and $G_{2^{6N}}$ represent an implementation of the protocol when Bob measures vacuum and one or more photons respectively, in all the time intervals.

The action of Bob's beamsplitter BS1, together with the interferometer are represented by the operator $\mathcal{U}$ which maps the incoming state in path '0' to the outgoing states in paths '3', '7' and '8'. Now the POVM's E_j (where $E_j = {}_4\langle 0|_1\langle 0|\mathcal{U}^\dagger G_j \mathcal{U}|0\rangle_1|0\rangle_4$) are the operators that act only on the states in path '0'. The expectation value with respect to the vacuum in path '1' reduces the action of the operator $\mathcal{U}^\dagger G_j \mathcal{U}$ to the subspace of the states in path '0', similar to the partial trace.

The effect that corresponds to a click on Bob's detector D_B in $j = 1; k = 1$ and vacuum in all other slots is given by

$$\begin{aligned} E_2 &= {}_{1,4}\langle 0|\mathcal{U}^\dagger G_2 \mathcal{U}|0\rangle_{1,4} \\ &= \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 1})^n |0\rangle\langle 0|(\hat{a}_0^1)^n. \end{aligned} \tag{8}$$

Similarly a click in D_B in $j = 3; k = 2$ and vacuum in all other slots becomes

$$\begin{aligned} E_3 &= {}_{1,4}\langle 0|\mathcal{U}^\dagger G_3 \mathcal{U}|0\rangle_{1,4} \\ &= \sum_{m=1}^{\infty} \frac{1}{2^m m!} (\hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^3)^m. \end{aligned} \tag{9}$$

The commutator is then given by

$$\begin{aligned} [E_2, E_3] &= \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 1})^n |0\rangle\langle 0|(\hat{a}_0^1)^n \sum_{m=1}^{\infty} \frac{1}{2^m m!} (\hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^3)^m \\ &- \sum_{m=1}^{\infty} \frac{1}{2^m m!} (\hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^3)^m \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 1})^n |0\rangle\langle 0|(\hat{a}_0^1)^n \\ &= 0, \end{aligned} \tag{10}$$

since $\langle 0|(\hat{a}_0^1)^n(\hat{a}_0^3)^m|0\rangle = 0$, i.e., the time intervals $j = 1$ and $j = 3$ belong to different Hilbert spaces. So without clicks for checks of coherence, it means that there is no security. Therefore, when we describe Bob's measurements by commuting operators, an eavesdropper could measure an observable which commutes with all of Bob's measurements, thus remaining undetected. Therefore, it is important that some of the POVM elements describing Bob's measurements must be non-commuting. This can be shown to be the case below. If we consider a click in D_B in time interval $j = 2$ and a click in D_{M1} in time interval $j = 3$, and vacuum everywhere else, we have

$$\begin{aligned} E_4 &= {}_{1,4}\langle 0|\mathcal{U}^\dagger G_4 \mathcal{U}|0\rangle_{1,4} \\ &= \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 2})^n |0\rangle\langle 0|(\hat{a}_0^2)^n, \\ E_5 &= {}_{1,4}\langle 0|\mathcal{U}^\dagger G_5 \mathcal{U}|0\rangle_{1,4} \\ &= \sum_{m=1}^{\infty} \frac{1}{8^m m!} (\hat{a}_0^{\dagger 2} + \hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^2 + \hat{a}_0^3)^m. \end{aligned} \tag{11}$$

The commutator is then given by

$$\begin{aligned} [E_4, E_5] &= \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 2})^n |0\rangle\langle 0|(\hat{a}_0^2)^n \sum_{m=1}^{\infty} \frac{1}{8^m m!} (\hat{a}_0^{\dagger 2} + \hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^2 + \hat{a}_0^3)^m \\ &- \sum_{m=1}^{\infty} \frac{1}{8^m m!} (\hat{a}_0^{\dagger 2} + \hat{a}_0^{\dagger 3})^m |0\rangle\langle 0|(\hat{a}_0^2 + \hat{a}_0^3)^m \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 2})^n |0\rangle\langle 0|(\hat{a}_0^2)^n. \\ &= \sum_{n=1}^{\infty} \frac{1}{2^n n!} (\hat{a}_0^{\dagger 2})^n |0\rangle n! \sum_{n=1}^{\infty} \frac{1}{8^n} \langle 0|(\hat{a}_0^2 + \hat{a}_0^3)^n \\ &- \sum_{n=1}^{\infty} \frac{1}{8^n n!} \langle 0|(\hat{a}_0^{\dagger 2} + \hat{a}_0^{\dagger 3})^n |0\rangle n! \sum_{n=1}^{\infty} \frac{1}{2^n} \langle 0|(\hat{a}_0^{\dagger 2})^n \end{aligned} \tag{12}$$

$$
\begin{aligned}
&= \sum_{n=1}^{\infty}\sum_{k=0}^{n}\binom{n}{k}\frac{1}{2^n 8^n n!}\{(\hat{a}_0^{\dagger 2})^n|0\rangle\langle 0|(\hat{a}_0^{2})^{n-k}(\hat{a}_0^{3})^k - (\hat{a}_0^{\dagger 2})^{n-k}(\hat{a}_0^{\dagger 3})^k|0\rangle\langle 0|(\hat{a}_0^{2})^n\} \\
&= \sqrt{n!}\sqrt{k!}\sqrt{(n-k)!}\left(|n\rangle_0^2\langle n-k|_0^2\langle k|_0^3 - |n-k\rangle_0^2|k\rangle_0^3\langle n|_0^2\right) \\
&\neq 0.
\end{aligned}
\tag{13}
$$

Since the operators $\hat{a}_0^{(\dagger)2}, \hat{a}_0^{(\dagger)3}$ act on different Hilbert spaces, the matrix elements do not cancel. Therefore, it has been shown that there exist non-commuting POVM elements in Bob's measurements, hence a precondition for the security of the COW protocol has been shown to be met.

5. Conclusion

From the above calculation, we can recognize that there exist non-commuting POVM elements in Bob's measurement in the P&M version of the COW protocol. Thus the COW protocol has been proven to satisfy an important necessary condition for security and such a description is an essential step in a potential proof for the most general kind of attacks..

6. Acknowledgments

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

7. References

[1] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. Fast and simple one-way quantum key distribution. Applied Physics Letters, 87(19):194108194108, 2005.

[2] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. Rev. Mod. Phys., 81(3):13011350, Sep 2009.

[3] C. Branciard, N. Gisin, and V. Scarani. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. New Journal of Physics, 10:013031, 2008.

[4] C. Branciard, N. Gisin, N. Lutkenhaus, and V. Scarani. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. arXiv:0609090, 2006

[5] T. Tsurumaru. Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol. Physical Review A, 75(6):62319, 2007.

[6] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden. Coherent one-way quantum key distribution. In Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, volume 6583, page 18, 2007.

[7] D. Stucki, N. Walenta, F. Vannel, R.T. Thew, N. Gisin, H. Zbinden, S. Gray, CR Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. New Journal of Physics, 11:075003, 2009.

[8] C.H. Bennett, G. Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175. Bangalore, India, 1984

[9] A. Marais, T. Konrad, and F. Petruccione. A necessary condition for the security of differential-phase-shift quantum key distribution. Journal of Physics A: Mathematical and Theoretical, 43:305302, 2010.

[10] M. A. Nielsen, I. Chuang, and L. K. Grover. Quantum Computation and Quantum Information. American Journal of Physics, 70:558, 2002.

[11] J. Audretsch. Entangled Systems: New Directions in Quantum Physics. Wiley-VCH, 2007.