Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080612

A Necessary Condition for the Security of Coherent-One-Way Quantum Key Distribution Protocol

Mhlambululi Mafu[1,*], *Adriana Marais*[1] *and Francesco Petruccione*[1,2]

[1] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001, Durban, South Africa
[2] National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa

Received: 13 Oct. 2013, Revised: 11 Jan. 2014, Accepted: 12 Jan. 2014
Published online: 1 Nov. 2014

Abstract: The coherent-one-way and the differential-phase-shift protocols are two of the most recent practical quantum key distribution protocols for quantum cryptography. These protocols belong to a class of so-called distributed-phase-reference quantum key distribution protocols. While security proofs for some limited attacks exist, the unconditional security proofs this class of protocol remain unrealised. The existing tools for proving security of protocols against the most general attacks fail to apply to this class of protocol in a straight forward way. One of the necessary conditions for a quantum key distribution protocol to be secure is the presence of noncommuting measurements. In this paper, the coherent-one-way protocol is formalised, and we describe Bob's measurements by non-commuting POVM elements, showing that this security condition is met.

Keywords: security; coherent one-way-protocol; quantum key distribution

1 Introduction

Quantum key distribution (QKD), one aspect of quantum cryptography, provides the only method proven to be physically secure for the transmission of a secret key between two distant parties, Alice and Bob [1]. The goal of QKD is to guarantee that a possible eavesdropper known as Eve, with access to the communication channel, is unable to obtain useful information about the generated key, which could then be used to encrypt the classical message [1,2]. Since the presentation of the first complete protocol i.e., BB84 protocol [3], several QKD protocols have been proposed. This has seen the development of the class of so-called distributed-phase-reference (DPR) QKD protocols, in which the coherence of the sequential pulses play an important role in security. Members of this class are the differential-phase-shift (DPS) protocol and coherent-one-way (COW) protocols [1].

The DPR protocols are tailored to work with weak coherent pulses at high bit rates and have been proven to be more practically implementable in the existing optical communication systems [1,4]. The DPS protocol was proposed by Inoue in 2002 [5] as a way to offer higher key creation efficiency as compared to the BB84 protocol. The COW QKD protocol was first proposed by Stucki in 2005 [4,6] and has been shown to be a simple high speed protocol which is easy to implement and yields even better rates than the class of so-called discrete variable protocols [1]. The COW protocol is also robust against reduced visibility [4] and against photon number splitting (PNS) attacks [8]. In 2005, Takesure reported an experimental implementation of the DPS protocol over 105km fiber [9]. In the same year, by using up-conversion detectors with 1GHz clock frequency, a successful generation of secure keys by using the DPS protocol for over 100km of fiber with a 166 bit/s key rate was reported by Diamanti [10]. This was followed by a security proof under the assumption that Eve is restricted to individual attacks by Waks in 2006 [11]. In the same year, Inoue [12] showed the robustness of DPS protocols against photon-number-splitting attacks. It was shown that the PNS attacks are not effective in the DPS and COW protocols because information is encoded in the phase difference between pulses, so any PNS attack will break the sequential coherent pulses which results in errors in Bob's measurements. The security for the DPS protocol against sequential attacks based on unambiguous discrimination and minimum error discrimination was

* Corresponding author e-mail: mhlambululi.mafu@gmail.com

shown in [13]. In the same year, security bounds for sequential attacks which can be more powerful than individual attacks were derived for the DPS protocol [14]. General security bounds against individual attacks and upper bounds for the error rates in the presence of coherent attacks were derived for both the COW and DPS protocols by Branciard in 2008 [15]. Again, security upper bounds for collective beam splitting attacks have been derived for the COW protocol [15]. Zero-error attacks have also been studied for the COW protocol [16]. In the same year, Zhao proved the security of the DPS protocol against weak coherent light source in the noiseless case [17]. Moreover, the effect of detector dead times on the evaluation of security for the DPS protocol against sequential attacks has been evaluated in [18]. Recently, lower bounds on the key generation rate for the COW protocol in the finite-size key scenario has been shown [19]. However, an unconditional security proof still remains elusive because there is no correspondence between the potential key bits and prepared states. Since these protocols rely on the mutual independence of all potential key bits therefore the present tools for proving the security of QKD protocols cannot be adopted to this class of protocols in a straightforward way.

The class of distributed-phase-reference QKD protocols use coherent sequences of signals which are not symmetric as opposed to qubits in other classes of protocols. These protocols move away from the symbol-per-symbol type of coding [15]. Since the formalism to be used to develop a full unconditional security proof still remains unsure for this class of protocols. Therefore, the efficiency and robustness as well as the practical communication advantages of the COW QKD protocol, together with the lack of an unconditional security proof for the protocol, motivate this study. Therefore, our goals here are to (i) motivate why the COW protocol is useful as a means of distributing a key, (ii) describe the operation and key extraction procedure of the COW protocol in the absence of a detailed explanation as presented in the original literature [4,6] and (iii) provide a formalism of Bob's measurement that is a step towards developing a full unconditional security proof, which includes describing Bob's measurements by non-commuting POVM elements. Such a description of Bob's measurement is a necessary condition for a QKD protocol to be secure [20]. However, such a description has not been explicitly worked out for complicated protocols as the COW protocol. Therefore, we hope that the approach in this paper may be used as a base on which to further develop an unconditional security proof for this protocol.

2 Operation of the COW protocol

According to Figure 1, Alice prepares a sequence of coherent pulses that are either empty or non-empty pulses. The non-empty pulses have a mean photon number $\mu < 1$ and a well defined time interval τ. Each logical bit of information is encoded in a sequence of two pulses, and Alice can also send decoy sequences. The decoy sequences are used to check for coherence in the data line and are then to be discarded in the public discussion. This is in contrast to the decoy states in the BB84 protocol which encode bit values [3]. So in each of $k = 1,...,N$ time intervals, Alice prepares the states $|\phi_0\rangle$ and $|\phi_1\rangle$ (which represent the logical states '0' or '1' respectively) or decoy states defined by:

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

where the index on the left hand side labels the time interval, $k = 1,...,N$, and the indices on the right hand side label the pulse index, $j = 1,...,2N$. In the case of a small mean photon number, the states $|\phi_0\rangle$ and $|\phi_1\rangle$ have a large overlap because of their vacuum component. There is also a phase coherence between any two non-empty pulses with a bit separation. 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, i.e., bit sequences '1-0' or decoy sequences, with the interferometer and detectors D_{M1} and D_{M2} as shown in Figure 1. The bit sequence is read from left to right as the bits arrive at Bob's detector. If D_{M2} fires, it means coherence is broken, and an error is recorded.

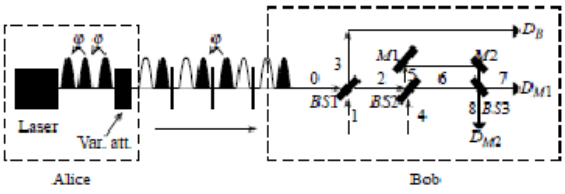


Fig. 1: Diagram for the COW Protocol. D_B represents the data detector, D_{M1} and D_{M2} are monitoring detectors, φ is the phase between successive non-empty pulses. The paths through Bob's interferometer are labelled 0-8. BS1 & BS2: symmetric beamsplitters, M1 & M2: mirrors, D: detector.

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

According to Figure 1, the signal entering Bob's interferometer in path '0' at time interval j can be described in terms of the creation operators $\hat{a}^{\dagger}_{0,j}$ and the

Table 1: Bob's detection events for the COW protocol. 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.

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

outgoing paths, $\hat{a}^\dagger_{3,j}$, $\hat{a}^\dagger_{7,j}$ and $\hat{a}^\dagger_{8,j}$, where the first index in the subscript is the spatial mode and the second is the temporal mode. In order to describe the signals entering Bob's interferometer, we follow the same approach used by Marais [21], since these protocols belong to the same class. The total action of the interferometer is derived to be

$$\hat{a}^\dagger_{0,j} \rightarrow \frac{1}{2\sqrt{2}}(\hat{a}^\dagger_{7,j} - e^{i\phi_3}\hat{a}^\dagger_{8,j} + 2\hat{a}^\dagger_{3,j} + \hat{a}^\dagger_{7,(j+1)} + e^{i\phi_3}\hat{a}^\dagger_{8,(j+1)}, \tag{2}$$

where ϕ_3 is a phase shift associated with symmetric BS3.

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

$$\begin{aligned}|\phi_0\rangle &= |\sqrt{\mu}\rangle_{0,(2k-1)}|0\rangle_{0,k} \\ &\xrightarrow{I} |\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{7,(2k-1)}|-e^{i\phi_3}\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{8,(2k-1)} \\ &\otimes |\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_{3,(2k-1)}|\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{7,k}|e^{i\phi_3}\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{8,k},\end{aligned} \tag{3}$$

where I is for the interferometer. Here, Bob gets a click in D_B which corresponds to a click in time slot $j-1$ with p_{click}=$1-e^{-\mu/8}$, which is the first of the slots constituting interval k, and records a '0'. Since D_{M1} and D_{M2} click with equal probability in slots $j-1$ and j, there is no test for coherence from $|0_k\rangle$ above.

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

$$\begin{aligned}|\phi_1\rangle_k &= |0\rangle_{0,(2k-1)}|\sqrt{\mu}\rangle_{0,k} \\ &\xrightarrow{I} |\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_{3,k}|\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{7,k}|\frac{-\sqrt{\mu}}{2\sqrt{2}}\rangle_{8,k} \\ &\otimes |\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{7,(2k+1)}|\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_{8,(2k+1)}.\end{aligned} \tag{4}$$

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 $k = 1,\ldots,N$ intervals, Bob records a '0'('1') when he gets a click in slot $2k-1$.

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

$$|\text{decoy}\rangle_k = |\sqrt{\mu}\rangle_{(2k-1)}|\sqrt{\mu}\rangle_k, \tag{5}$$

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

$$\begin{aligned}|\sqrt{\mu}\rangle_0^t|\sqrt{\mu}\rangle_0^{(t+1)} &\xrightarrow{I} |\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^t|\frac{\sqrt{\mu}}{2\sqrt{2}}\rangle_7^t|\frac{-\sqrt{\mu}}{2\sqrt{2}}\rangle_8^t|\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_3^{(t+1)} \\ &\otimes |\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_7^{(t+1)}|0\rangle_8^{(t+1)}|\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_7^{(t+2)}|\frac{\sqrt{\mu}}{\sqrt{2}}\rangle_8^{(t+2)}.\end{aligned}$$

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, $|\phi_0\rangle_k$ and $|\phi_1\rangle_k$, given in Equation (1), that arrive at his detector. As can be seen in Table 1, checks for coherence can be done via decoy states as well as 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.

3 Bob's measurements

We exploit the mathematical convenience of POVM's [22,23] as a tool for describing Bob's measurement statistics. The projectors constituting Bob's measurement in the time intervals $j \in \{1,...,2N\}$, where j is the superscript are written as

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

The $G_{i's}$ are projectors onto the basis of photon number states, $|n\rangle$. They represent all the possible outcomes for an implementation of the COW protocol with signals sent in $2N$ time intervals. The projector G_1

represent an implementation of the protocol when Bob measures a vacuum. Since Bob has a probability of detecting one or more photons (a click) or vacuum (no click) in each of the three detectors in $2N$ time intervals, there are 2^{6N} possible measurement outcomes corresponding to 2^{6N} POVM elements. This is represented as a projector $G_{2^{6N}}$.

The action of Bob's beamsplitter BS1, together with the interferometer are represented by the operator which maps the incoming state in path '0', '1' and '4' to the outgoing states in paths '3', '7' and '8'. The effects which we denote as E_j are the operators that act on the states in path '0'. This action can be represented as

$$E_j = {}_4\langle 0|_1\langle 0|\mathscr{U}^\dagger G_j \mathscr{U}|0\rangle_1|0\rangle_4. \tag{7}$$

The expectation value with respect to the vacuum in path '1' reduces the action of the operator $\mathscr{U}^\dagger G_j \mathscr{U}$ to the subspace of the states in path '0', similar to the partial trace.

The POVM element that corresponds to a click in Bob's detector D_B in $j = 1,...,5$ and vacuum everywhere else is given by

$$\begin{aligned}
E_2 &= \sum_{n=1}^{\infty} \frac{1}{2^n n!}(\hat{a}_{0,1}^\dagger)^n|0\rangle\langle 0|(\hat{a}_{0,1})^n,\\
E_3 &= \sum_{m=1}^{\infty} \frac{1}{8^m m!}(\hat{a}_{0,1}^\dagger + \hat{a}_{0,2}^\dagger)^m|0\rangle\langle 0|(\hat{a}_{0,1} + \hat{a}_{0,2})^m,\\
E_4 &= \sum_{n=1}^{\infty} \frac{1}{2^n n!}(\hat{a}_{0,2}^\dagger)^n|0\rangle\langle 0|(\hat{a}_{0,2})^n,\\
E_5 &= \sum_{m=1}^{\infty} \frac{1}{8^m m!}(\hat{a}_{0,2}^\dagger + \hat{a}_{0,3}^\dagger)^m|0\rangle\langle 0|(\hat{a}_{0,2} + \hat{a}_{0,3})^m,
\end{aligned} \tag{8}$$

If we consider a click in D_B in $j = 2$ and a click in D_{M1} in time interval $j = 3$, and vacuum everywhere else, the commutator is given by

$$[E_2, E_3] \neq 0, \tag{9}$$

since the operators $\langle 0|(\hat{a}_{0,1}^\dagger)^n(\hat{a}_{0,2}^\dagger)^m|0\rangle \neq 0$ act on different Hilbert spaces, the matrix elements do not cancel. Similarly, if we consider a click in D_B in $j = 2$ and a click in D_{M1} in time interval $j = 4$, and vacuum everywhere else, the commutator is given by

$$[E_2, E_4] = 0. \tag{10}$$

since $\langle 0|(\hat{a}_{0,1})^n(\hat{a}_{0,2})^m|0\rangle = 0$. We have shown in the case of the COW protocol that without clicks for checks of coherence, there is no security. This is easily seen since if we describe Bob's measurements by commuting operators, an eavesdropper could gain full knowledge of the key with a measurement that commutes with Bob's, thus remaining undetected. Therefore, it is important that some of the POVM elements describing Bob's measurements must be non-commuting.

Based on the above relations, one can observe that

$$\begin{aligned}
[E_j, E_{j+1}] &= {}_4\langle 0|_1\langle 0|\mathscr{U}^\dagger G_j \mathscr{U}, \mathscr{U}^\dagger G_{j+1} \mathscr{U}|0\rangle_1|0\rangle_4\\
&\neq 0,
\end{aligned} \tag{11}$$

and also that

$$\begin{aligned}
[E_j, E_{j+2}] &= {}_4\langle 0|_1\langle 0|\mathscr{U}^\dagger G_j \mathscr{U}, \mathscr{U}^\dagger G_{j+2} \mathscr{U}|0\rangle_1|0\rangle_4\\
&= 0.
\end{aligned} \tag{12}$$

Based on these generalizations, we note that if the effects come from consecutive time intervals, the POVM elements describing Bob's measurements do not commute and if the time intervals are not consecutive, the POVM elements commute. However, we note that if j is odd Equation (12) is not satisfied. This might look strange at first but this situation gives an inconclusive event because the clicks come from different time intervals. Therefore, we have 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. Recently it has been noted that nondisturbance is equivalent to commutativity on the condition that the second measurement has sufficiently many independent outcomes [24]. However, nondisturbance is inequivalent to commuting in general, hence such a description of Bob's measurement in terms of non-commuting POVM elements is an essential step in a potential proof of security against the most general kind of attack.

4 Conclusion

We have highlighted the practical advantages and efficiency of the COW QKD protocol, and as well as explicitly describing the implementation and key distribution procedure of the protocol. In spite of the challenges that come with showing the unconditional security of the COW QKD protocol, we have managed to provide a formalism for Bob's measurements that may be used as a base to develop an unconditional security proof for the COW QKD protocol. Specifically, from the above calculation, we can recognize that there exist non-commuting POVM elements in Bob's measurement. Thus, the COW protocol has been proven to satisfy an important necessary condition for security. Such a description of Bob's measurement is an essential element for a security proof against the most general kind of attack.

Acknowledgement

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.

References

[1] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Reviews of Modern Physics, **74**, 145-195 (2002)

[2] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Du sek, M., Lutkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys., **81**, 1301-1350 (2009)

[3] Bennett, C.H., Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, **175**, (1984).

[4] Stucki, D., Brunner, N., Gisin, N., Scarani, V., Zbinden, H.: Fast and simple one-way quantum key distribution. Applied Physics Letters, **87**, 194108-194108 (2005)

[5] noue, K., Waks, E., Yamamoto, Y.: Differential phase shift quantum key distribution. Phys. Rev. Lett., **89**, 037902 (2002).

[6] Stucki, D., Fasel, S., Gisin, N., Thoma, Y., Zbinden, H.: Coherent One-way Quantum Key Distribution. In: Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, **6583**, 18 (2007).

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

[8] Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A, **61**, 052304 (2000).

[9] Takesue, H., Diamanti, E., Honjo, T., Langrock, C., Fejer,M., Inoue, K., Yamamoto, Y.: Differential phase shift quantum key distribution experiment over 105 km fibre. New Journal of Physics, **7**, 232 (2005).

[10] Eleni Diamanti, C.L.M.M.F. Hiroki Takesue, Yamamoto, Y.: 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors. Optical Society of America, **14**, 13073-13082 (2006).

[11] Waks, E., Takesue, H., Yamamoto, Y.: Security of differential-phase-shift quantum key distribution against individual attacks. Phys. Rev. A, **73**, 012344 (2006).

[12] Inoue, K., Honjo, T.: Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. Phys. Rev. A, **71**, 042305 (2005)

[13] Curty, M., Zhang, L.-L., Lo, H.-K., Lutkenhaus, N.: Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. Quantum Information & Communication, 665-688 (2007)

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

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

[16] Branciard, C., Gisin, N., Lutkenhaus, N., Scarani, V.: Zeroerror attacks and detection statistics in the coherent one-way protocol for quantum cryptography. Quantum Information & Computation, **7**, 639 (2007).

[17] Zhao, Y.-B., Fung, C.-H.F., Han, Z.-F., Guo, G.-C.: Security proof of differential phase shift quantum key distribution in the noiseless case. Physical Review A, **78**, 042330 (2008).

[18] Curty, M., Tamaki, K., Moroder, T.: Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks. Physical Review A, **77**, 52321 (2008).

[19] Moroder, T., Curty, M., Lim, C.C.W., Zbinden, H., Gisin, N., : Security of distributed-phase-reference quantum key distribution. Physical Review Letters, **109**, 260501 (2012).

[20] Curty, M., Lewenstein, M., Lutkenhaus, N.: Entanglement as a precondition for secure quantum key distribution. Physical Review Letters, **92**, 217903 (2004).

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

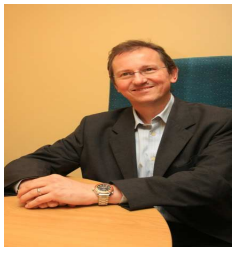
[22] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, (2000).

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

[24] Heinosaari, T., Wolf, M.M.: Nondisturbing quantum measurements. Journal of Mathematical Physics, **51**, 092201 (2010).

Mhlambululi Mafu completed his PhD in Physics at the Centre for Quantum Technology at the University of KwaZulu-Natal. His research interests are in the area of quantum information and communication, specifically in the security of quantum key distribution protocols and cryptographic devices.

Adriana Marais is currently completing her PhD in Physics at the Centre for Quantum Technology at the University of KwaZulu-Natal. After completing her MSc in the field of quantum cryptography, she is now doing research in the area of quantum biology, specifically investigating quantum effects in photosynthesis.



Francesco Petruccione was born in 1961 in Genova (Italy). He studied Physics at the University of Freiburg i. Br. and received his PhD in 1988. He got his “Habilitation” (Dr. rer. nat. habil.) from the same University in 1994. In 2004 he was appointed Professor of Theoretical Physics at the University of KwaZulu-Natal. In 2007 he was granted a South African Research Chair for Quantum Information Processing and Communication.