On the Robustness of Quantum Key Distribution with Classical Alice (photons-based protocol)

Michel Boyer

Département IRO
Université de Montréal, Canada
Email: boyer@iro.umontreal.ca

Tal Mor

Computer Science Department
Technion, Israel
Email: talmo@cs.technion.ac.il

***Abstract*—Quantum Key Distribution (QKD) with classical Bob, has been suggested and proven robust. Following this work, QKD with classical Alice was also suggested and proven robust. The above protocols are ideal in the sense that they make use of qubits. However, in the past, well-known QKD protocols that were proven robust and even proven unconditionally secure, when qubits are used, were found to be totally insecure when photons are used. This is due to sensitivity to photon losses (e.g., Bennett's two-state protocol) or sensitivity to losses combined with multi-photon states (e.g., the photon-number-splitting attack on the weak-pulse Bennett-Brassard protocol, BB84). Here, we prove that QKD with classical Alice is still robust when photon losses and even multi-photon states are taken into account. Our method can pave the road to robustness and security analysis of various other two-way QKD protocols.**

***Index Terms*—Cryptography; Quantum Mechanics.**

I. Introduction

A two-way Quantum Key Distribution (QKD) protocol in which one of the parties (Bob) uses only classical operations was recently introduced [1,2]. A very interesting extension in which the originator always sends the same state $|+\rangle = (|\mathtt{0}\rangle + |\mathtt{1}\rangle)/\sqrt{2}$ (where $\mathtt{0}$ and $\mathtt{1}$ are used to denote bits, to avoid confusion with the integers 0 and 1 used as occupancy numbers) while in [1] all four states, $|\mathtt{0}\rangle$, $|\mathtt{1}\rangle$, $|+\rangle$ and $|-\rangle = (|\mathtt{0}\rangle - |\mathtt{1}\rangle)/\sqrt{2}$, are sent, is suggested by Zou *et al.* [3]. In both "semi-quantum" key distribution (SQKD) protocols the qubits go from the originator Alice to (classical) Bob and back to Alice. Bob randomly either reflects a received qubit without touching its state (those are deemed CTRL bits), or measures it in the standard (classical) basis and sends back his result as $|\mathtt{0}\rangle$ or $|\mathtt{1}\rangle$ (those are deemed SIFT bits). These two operations, "doing nothing" or measure-resend in the standard (computation) basis, are called classical [1,2] for obvious reasons; in principle, semi-quantum protocols might be simpler to implement than fully quantum ones.

Following [4], we prefer to call the originator in [3] Bob (and not Alice), and to call the classical party Alice: usually in quantum cryptography, Alice is the sender of some non-trivial data, e.g., she is the one choosing the quantum states. The originator in [3] does not have that special role, as the state $|+\rangle$ is always sent (and we could even ask Eve to generate it). The classical person is then the one actually choosing a basis and knowing which of the three state ($|\mathtt{0}\rangle$, $|\mathtt{1}\rangle$, or $|+\rangle$) is sent back to the originator, thus it is natural to name that classical person Alice. We call the originator Bob, and we call the SQKD protocol of Zou et al "QKD with classical Alice". Note that QKD with classical Alice was also suggested, independently of [3], by Lu and Cai [5]. As proven in [4], QKD with Classical Alice (the protocol suggested in [3]) is completely robust against eavesdropping.

Here, we use Fock-space representation to extend the QKD with classical Alice protocol to the important case in which Alice and Bob use photons and not merely ideal qubits. We first extend the proof of robustness to include photon loss, and subsequently, also multi-photon states. To the best of our knowledge, such a general analysis has not yet been provided for any of the (many) two-way QKD protocols, including ping-pong protocols and (experimental and commerical) plug and play protocols, hence our approach and method may have major influence on future robustness and security analysis of QKD. A related (photonic) security analysis was recently done for a different two-way QKD protocol, see Section 4.2 in [6].

Such extensions from qubits to photons are far from trivial; on the contrary, often, robustness is actually lost when trying to deal with photons rather than qubits.

As a first example, in the two-state scheme (known as the Bennett'92 — B92 scheme), when qubits are assumed to be carried by photons, photon losses cause a severe problem: if Eve can replace a lossy channel by a lossless one, she might be able to get full information without causing errors at all, using an "un-ambiguous state discrimination" attack. As a second example, in the four-state scheme (known as the Bennett-Brassard'84 — BB84 scheme), when qubits are assumed to be carried by photons, photon losses combined with multi-photon pulses cause a severe problem: if Eve can replace a lossy channel by a lossless one, and can measure photon numbers (via a non-demolition measurement), she might be able to get full information without causing errors at all [7], using a "photon number splitting" attack.

II. The Fock space notations

The Fock space notations that serve as an extension of a qubit are as follows: in the standard (z) basis, the Fock basis vector $|0,1\rangle$ stands for a single photon in a qubit-state $|0\rangle$ and the Fock basis vector $|1,0\rangle$ stands for a single photon in a qubit-state $|1\rangle$. Naturally, the Hadamard (x) basis qubit-states are given by the superposition of those Fock states so that $[|0,1\rangle \pm |1,0\rangle]/\sqrt{2}$ stand for a single photon in a qubit-state $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The general state of this photonic qubit can then be written as $\alpha|0,1\rangle + \beta|1,0\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$.

This photonic qubit lies in a much larger space called Fock space. The first natural extension is $|0,0\rangle$ that describes the lack of photons (the vacuum state), a case of great practical importance, as it enables dealing properly with photon loss. The next extension of a very high practical importance is that $|2,0\rangle$ describes two (indistinguishable) photons in the same qubit-state $|1\rangle$, $|0,2\rangle$ describes two (indistinguishable) photons in the same qubit-state $|0\rangle$, and $|1,1\rangle$ describes two (in this case, distinguishable) photons, one in the qubit-state $|0\rangle$, and one in the qubit-state $|1\rangle$. This case (a six dimensional space, describing two or less photons) was found very important in the photon number splitting attack [7], as prior to that analysis, experimentalists assumed that the only impact of high loss rate is on the bit-rate and not on security.

In general, if a single photon can be found in two orthogonal states (these are called "modes" when discussing photons), then $|n_1, n_0\rangle$ represents n_1 (respectively n_0) indistinguishable photons in a qubit-state $|1\rangle$ (resp. $|0\rangle$). The numbers n_0 and n_1 are then called the occupation numbers of the two modes. From now on, the notations $|0\rangle \equiv |0,1\rangle$, $|1\rangle \equiv |1,0\rangle$, $|+\rangle = (|0,1\rangle + |1,0\rangle)/\sqrt{2}$ and $|-\rangle = (|0,1\rangle - |1,0\rangle)/\sqrt{2}$ will be used interchangeably. Similarly, since the single photon can also be found in $|0,1\rangle_x \equiv |+\rangle$ and $|1,0\rangle_x \equiv |-\rangle$ (namely, the x basis), then $|n_-, n_+\rangle$ represents n_- (resp. n_+) indistinguishable photons in qubit-state $|-\rangle$ (resp. $|+\rangle$).

More generally, one may consider more than two modes. For instance, the four modes $|n_{1b}, n_{1a}, n_{0b}, n_{0a}\rangle$ are the generalization of qu-quadrit (say a photon in one of two arms a or b, and one of two orthogonal polarizations, denoted 0 or 1).

III. The Classical Alice protocol, Dealing with Losses

The originator Bob sends Alice qubits in the state $|+\rangle$ and keeps in a quantum memory all qubits he received back from her. If Bob does not hold a memory to keep the qubits, he measures them upon reception at random in the standard (z) or the Hadamard (x) basis. Only CTRL bits measured in the x basis, and SIFT bits measured in the z basis, are used. That does not modify the conceptual proof (but in a security proof it would mean that they need to send more qubits to start with). When N qubits have been sent and received, (classical) Alice announces publicly which qubits she reflected (without disturbing them); the originator Bob then checks that he received $|+\rangle$ and not $|-\rangle$ on those positions (CTRL). For the (SIFT) qubits measured by Alice in the standard (classical) $\{|0\rangle; |1\rangle\}$ basis, a sample is chosen to be checked for errors (TEST). The remaining SIFT bits serve for obtaining a final, secure key, via error correction and privacy amplification, as in any conventional QKD protocol.

A. Defining the (limited) "photonic QKD with classical Alice" protocol

The qubits are embedded in the 3-dimensional, 2-mode Fock space containing the qubit states $|1,0\rangle$ and $|0,1\rangle$ and the vacuum state $|0,0\rangle$. The Hilbert space describing Alice+Bob states is (for now) the subspace

$$\mathscr{H}_{AB} = \mathrm{Span}\left(|0,1\rangle, |1,0\rangle, |0,0\rangle\right) \subseteq \mathscr{F} \qquad (1)$$

of the more general 2-mode Fock space ($\mathscr{F}$).

In this photonic protocol, Bob is always sending the $|+\rangle$ state. Losses or vacuum states are modeled by the state $|0,0\rangle$, and thus, we must define Alice's and Bob's operations when such states occur. Losses normally come from the interaction with the environment; as usual, the (worst case) analysis gives Eve total control on the environment. Classical Alice can either SIFT or CTRL [3,4]. In the SIFT mode, Alice's "measurement" is described (WLG) with the adjunction of a probe, extending $\mathscr{H}_{AB}$ to $\mathscr{H}_A \otimes \mathscr{H}_{AB}$, a unitary transformation and a measurement of her probe in the standard basis. Such a description is meant to match the general framework of measurements in quantum information, and may not correspond to the actual physical measurement performed by Alice. Using the Fock-space notations, it is assumed that Alice adds a two-mode probe in a state $|0,0\rangle_A$ to get the state $|0,0\rangle_A |+\rangle_{AB}$. Alice then performs one of the following two operations (with $|n_1,n_0\rangle_{AB}$ in the z, i.e., the standard basis):

$$U_{\text{CTRL}}\,|0,0\rangle_A\,|n_1,n_0\rangle_{AB} = |0,0\rangle_A\,|n_1,n_0\rangle_{AB} \qquad (2)$$

$$U_{\text{SIFT}}\,|0,0\rangle_A\,|n_1,n_0\rangle_{AB} = |n_1,n_0\rangle_A\,|n_1,n_0\rangle_{AB} \qquad (3)$$

then she measures her probe in the standard classical basis and sends Alice+Bob's state to Bob; in the case described by (2) (CTRL) she needs not measure, still the probe and its measurement are added there only to make the description uniform; Bob's original state ($|+\rangle_{AB}$) is reflected back to him, undisturbed. In the case described by (3) (SIFT), Alice gets the outcome $n_1 n_0$, and the state $|n_1,n_0\rangle_{AB}$ is sent to Bob. Note that, in order to analyze the enlarged space of the protocol, we *had to* add the definition of Alice's operation on the added state, $|0,0\rangle_{AB}$. Our choice of $U_{\text{SIFT}}\,|0,0\rangle_A\,|0,0\rangle_{AB} = |0,0\rangle_A\,|0,0\rangle_{AB}$ is the most natural way of extending Alice's SIFT operation, and it thus becomes part of our definition of the protocol "Photonic-QKD with classical Alice".

Naturally, when Bob measures in the classical (z) basis, he also measures the same three states as Alice, $|n_1,n_0\rangle$ with $n_0+n_1 \leq 1$. However, the space $\mathscr{H}_{AB}$ (1) is also spanned by the orthonormal basis $\{\,|+\rangle,\ |-\rangle,\ |0,0\rangle\}$, thus Bob (who is not limited to being classical) can perform a measurement in this generalized x basis of the qutrit.

B. Eve's attack on the (photonic) classical Alice protocol

Eve performs her attack in both directions; from Bob to Alice, Eve applies U; from Alice to Bob, Eve applies V. We may assume, WLG, that Eve is using a fixed probe space $\mathscr{H}_E$ for her attacks in both directions. The attack from Bob to Alice produces a state of the form $|E_{01}\rangle\,|0,1\rangle_{AB} + |E_{10}\rangle\,|1,0\rangle_{AB} + |E_{00}\rangle\,|0,0\rangle_{AB}$ (namely $\sum_{n_1,n_0\ |\ n_0+n_1\leq 1} |E_{n_1 n_0}\rangle\,|n_1,n_0\rangle_{AB} \in \mathscr{H}_E \otimes \mathscr{H}_{AB}$), where the $|E_{ij}\rangle$ are non normalized (and potentially non-orthogonal) vectors in $\mathscr{H}_E$. With Alice's probe attached we obtain

$$|\Psi\rangle = \sum_{n_1,n_0\ |\ n_0+n_1\leq 1} |E_{n_1 n_0}\rangle\,|0,0\rangle_A\,|n_1,n_0\rangle_{AB}\ , \qquad (4)$$

in $\mathscr{H}_E \otimes \mathscr{H}_A \otimes \mathscr{H}_{AB}$. In particular, if Eve does nothing then $|E_{10}\rangle = |E_{01}\rangle = |E_{00}\rangle \equiv |E\rangle$ and the state in Alice+Eve's hands, prior to Alice's operation, is $|E\rangle\,|0,0\rangle_A\,|+\rangle_{AB}$.

Going back to the general case, if Alice applies U_{CTRL}, then the state in Eve+Alice hands (after Alice's CTRL action) is still $|\Psi\rangle$. However, if Alice applies U_{SIFT}, the resulting global state in Eve+Alice's hands is

$$\sum_{n_1,n_0\ |\ n_0+n_1\leq 1} |E_{n_1 n_0}\rangle\,|n_1,n_0\rangle_A\,|n_1,n_0\rangle_{AB} \qquad (5)$$

and after Alice has measured her probe, she gets some output ($\{00,01,10\}$), and some (non normalized) residual state that she sends back to Bob.

Once Alice has performed her measurements and sent $|i,j\rangle_{AB}$ back to Bob via Eve, the resulting global state (fully in Eve's hands) is given by Table I, where the $|\psi_{ij}\rangle$ are not normalized, and where the $|E_{ij}\rangle$ were chosen by Eve. Eve now applies a unitary V on $\mathscr{H}_E \otimes \mathscr{H}_{AB}$ and then sends Bob his part of the resulting state.

TABLE I
GLOBAL STATE AFTER ALICE'S MEASUREMENT

Measurement	*State (non normalized)*
00	$\|\psi_{00}\rangle = \|E_{00}\rangle\,\|0,0\rangle_{AB}$
01	$\|\psi_{01}\rangle = \|E_{01}\rangle\,\|0,1\rangle_{AB}$
10	$\|\psi_{10}\rangle = \|E_{10}\rangle\,\|1,0\rangle_{AB}$
CTRL	$\|\psi\rangle = \|\psi_{00}\rangle + \|\psi_{01}\rangle + \|\psi_{10}\rangle$

C. A proof of robustness

For Eve to stay undetectable, if Alice measured $|0,0\rangle$ (namely, the outcome 00) in the SIFT mode, then Bob should have a probability zero of measuring 01 or 10, thus, a probability zero of receiving the states $|0,1\rangle$ or $|1,0\rangle$. Similarly if Alice measured 10 (01), then Bob should have a probability zero of measuring 01 (10); he could however get a loss, 00. The resulting (non normalized) Eve+Bob residual states thus take the form $|\psi'_{00}\rangle = V\,|\psi_{00}\rangle = |H_{00}\rangle\,|0,0\rangle_{AB}$ when a loss arrives, and otherwise,

$$|\psi'_{01}\rangle = V\,|\psi_{01}\rangle = |F_{01}\rangle\,|0,1\rangle_{AB} + |H_{01}\rangle\,|0,0\rangle_{AB} \qquad (6)$$

$$|\psi'_{10}\rangle = V\,|\psi_{10}\rangle = |F_{10}\rangle\,|1,0\rangle_{AB} + |H_{10}\rangle\,|0,0\rangle_{AB}\ . \qquad (7)$$

Finally, V being linear, the (normalized) residual state if Alice applied CTRL is $|\psi'\rangle \equiv V\,|\psi\rangle = |\psi'_{00}\rangle + |\psi'_{01}\rangle + |\psi'_{10}\rangle$.

In order to check CTRL bits, Bob measures $|\psi'\rangle$ in the x basis and checks if he gets a photon in the illicit state

ISBN: 978-1-61208-431-2

$|-\rangle$. To avoid that, Eve must make sure that the overlap between Eve-Bob's state $|\psi'\rangle$ and Bob's state $|-\rangle$ is zero. This results with another limitation on Eve's attack: the norm of ${}_{AB}\langle-\big|\big(|F_{01}\rangle\,|0,1\rangle_{AB}\big)+{}_{AB}\langle-\big|\big(|F_{10}\rangle\,|1,0\rangle_{AB}\big)$ must be 0; namely, $|F_{01}\rangle\langle- \mid 0,1\rangle + |F_{10}\rangle\langle- \mid 1,0\rangle = \big(|F_{01}\rangle - |F_{10}\rangle\big)/\sqrt{2} = 0$, i.e., $|F_{01}\rangle = |F_{10}\rangle = |F\rangle$ for some (non normalized) state $|F\rangle \in \mathscr{H}_E$. The final global states (6) and (7) if Alice measured 01 and 10 are thus (respectively)

$$|F\rangle\,|0,1\rangle_{AB} + |H_{01}\rangle\,|0,0\rangle_{AB} \tag{8}$$

$$|F\rangle\,|1,0\rangle_{AB} + |H_{10}\rangle\,|0,0\rangle_{AB}\ , \tag{9}$$

and if Bob does not get a loss, Eve's final state is $|F\rangle$ whether Bob measures $|0,1\rangle$, i.e., the bit 0, or $|1,0\rangle$, i.e., the bit 1. Eve's final probe is, thus, independent of all of Alice's and Bob's measurements, and is unentangled with their state.

Eve can thus get no information on the bits Alice and Bob agree upon without being detectable. That reasoning can be done inductively bitwise to get robustness with N qubits.

IV. The Classical Alice Protocol, Dealing with Losses and Multi-Photon Pulses

In practice, there are not just losses: when qubits are encoded using photon pulses, there may be more than one photon per pulse, giving the eavesdropper more tools to get information on the SIFT bits. We now allow the Hilbert space to contain all photonic states of the above-mentioned two modes. Namely, we consider all states $|n_1,n_0\rangle$ with $n_0+n_1 \geq 0$. As before, we *must* specify Alice's and Bob's operations on those states.

A. Defining the (full) "photonic QKD with classical Alice" protocol

If Alice and Bob can distinguish one from more than one photon, extending the results of the earlier section is rather trivial; in brief, Eve becomes limited to the same space as in the previous section, or else she will be noticed.

The interesting extension is when Alice and Bob are limited, and cannot tell a single photon pulse from a multi-photon pulse. It is conventional to say that they have "detectors" and not "counters". This, of course, is in contrast to Eve who has counters, and who can do whatever physics allows.

We now assume a specific realization of the Fock states, to make the limitation on the measurements more clear. We assume that the two classical states, $|0\rangle$ and $|1\rangle$, describe two pulses on the same arm, such that the photon can either be in one pulse, in the other, or in a superposition, such as the (non-classical) state $|+\rangle$. Measurements are applied onto the two modes separately, using two detectors, thus a state $|1,1\rangle$, as well as any state $|n_1,n_0\rangle$ with both $n_1 \geq 1$ and $n_1 \geq 1$, can be identified as an error. That will be enough to guarantee robustness.

As before, we assume that Alice's CTRL operation is given by (2), yet now, with n_0 and n_1 being any non-negative integers. Let $\hat{n}_1 = 1$ if $n_1 \geq 1$, else $\hat{n}_1 = 0$; similarly, $\hat{n}_0 = 1$ if $n_0 \geq 1$, else $\hat{n}_0 = 0$. To model properly the use of a detector that clicks when noticing one or more photons, it is assumed that in the SIFT mode Alice still attaches a probe in the $|0,0\rangle_A$ state. Now she applies the following transform, U_{SIFT}, on $\mathscr{H}_A \otimes \mathscr{H}_{AB}$ where $\mathscr{H}_A = \text{Span}\big(|0,0\rangle_A, |0,1\rangle_A, |1,0\rangle_A, |1,1\rangle_A\big)$ and $\mathscr{H}_{AB}$ is $\mathscr{F}$, Alice+Bob's 2-mode photonic space:

$$U_{\text{SIFT}}\,|0,0\rangle_A\,|n_1,n_0\rangle_{AB} = |\hat{n}_1,\hat{n}_0\rangle_A\,|n_1,n_0\rangle_{AB}\ . \tag{10}$$

Alice then measures her probe in the $|0,0\rangle_A$, $|0,1\rangle_A$, $|1,0\rangle_A$ and $|1,1\rangle_A$ basis; she cannot distinguish $|n_1,0\rangle$ with $n_1 \geq 2$ from $|1,0\rangle$, yet she can distinguish $|1,1\rangle$ from $|1,0\rangle$. When $n_1 \geq 1$ or $n_0 \geq 1$ she sees $\hat{n}_1 = 1$ or $\hat{n}_0 = 1$ (respectively); if both $n_1 \geq 1$ and $n_0 \geq 1$ then she measures her probe in a state $|1,1\rangle_A$; this is telling her that the state she received is illicit.

We need to *carefully* define Alice's operation on the states she receives, as the robustness analysis depends on the residual state after Alice's "measurement", which Alice sends back to Bob; we now consider two legitimate options for defining that state. In one, which we could call "the conventional measure-resend approach", we assume that depending on which detector clicks, the state $|0,1\rangle$ or the state $|1,0\rangle$ (or the state $|0,0\rangle$ if no detector clicked) is then sent back to Bob. However, now Eve could prepare the state $\big(|0,2\rangle + |2,0\rangle\big)/\sqrt{2}$ and send it to Alice; in CTRL mode the same state will return to Eve, while in SIFT mode only a single photon (or none) will be given back to Eve. Thus, Eve (who can measure the number of photons) will easily decode Alice's operation, and will be able to measure (and resend) in case of SIFT, or send the state $\big(|0,1\rangle + |1,0\rangle\big)/\sqrt{2}$ back to Bob in case of CTRL.

We thus stick here to a different way of defining the residual state after Alice's action: we simply assume that the state $|n_1,n_0\rangle$ is sent back to Bob in both (10) and (2). Incidently, that attack above is an example of a simple tagging attack. In a separate work (in preparation) we present a modified photonic classical Alice protocol that prevents many other tagging attacks, including the one suggested in [8] as an attack against QKD with classical Bob ([1]); see also [9].

B. Eve's attack on the (photonic) classical Alice protocol

Eve performs her attack in both directions using a fixed probe space $\mathscr{H}_E$; from Bob to Alice, Eve applies U; from Alice to Bob, Eve applies V. The attack from Bob to Alice produces a state of the form $\sum |E_{n_\imath n_\mathrm{o}}\rangle\,|n_\imath, n_\mathrm{o}\rangle_{AB} \in \mathscr{H}_E \otimes \mathscr{H}_{AB}$ where $\mathscr{H}_{AB} = \mathscr{F}$. With Alice's probe attached we obtain

$$|\Psi\rangle = \sum |E_{n_\imath n_\mathrm{o}}\rangle\,|0,0\rangle_A\,|n_\imath, n_\mathrm{o}\rangle \ , \tag{11}$$

in $\mathscr{H}_E \otimes \mathscr{H}_A \otimes \mathscr{H}_{AB}$. In particular, if Eve does nothing then $|E_{n_\imath n_\mathrm{o}}\rangle \equiv |E\rangle$ independently of $n_\imath$ and n_o, and the state in Alice+Eve's hands, prior to Alice's operation, is $|E\rangle\,|0,0\rangle_A\,|+\rangle_{AB}$.

Going back to the general case, if Alice applies U_{CTRL}, then the state in Eve+Alice hands (after Alice's CTRL action) is still $|\Psi\rangle$. However, if Alice applies U_{SIFT}, the resulting global state in Eve+Alice's hands is

$$\sum |E_{n_\imath n_\mathrm{o}}\rangle\,|\hat{n}_\imath, \hat{n}_\mathrm{o}\rangle_A\,|n_\imath, n_\mathrm{o}\rangle_{AB} \ ; \tag{12}$$

after Alice has measured her probe she gets some output ($\{00, 01, 10, 11\}$), and some complicated (non normalized) residual state (sent then back to Bob) that we soon analyze.

Eve now attacks that residual state on the way back from Alice to Bob using the unitary V acting on both her probe and the state sent by Alice to Bob (see below). Eve then sends Bob his part of the resulting state.

C. A proof of robustness

Alice's measuring abilities put a constraint on the state $|\Psi\rangle$ for Eve not to be detectable: Alice's probability of measuring $|1,1\rangle_A$ according to that model must be zero, or else Eve can be noticed. It is thus required that $|E_{n_\imath n_\mathrm{o}}\rangle = 0$ for $n_\imath \times n_\mathrm{o} \neq 0$. Therefore, Eve+Alice's state when Alice applies U_{SIFT} must take the form

$$\sum_{n_\mathrm{o} \geq 1} |E_{0 n_\mathrm{o}}\rangle\,|0,1\rangle_A\,|0, n_\mathrm{o}\rangle + \sum_{n_\imath \geq 1} |E_{n_\imath 0}\rangle\,|1,0\rangle_A\,|n_\imath, 0\rangle \tag{13}$$

$$+ \,|E_{00}\rangle\,|00\rangle_A\,|0,0\rangle \ . \tag{14}$$

Once Alice has performed her measurements and sent $|i,j\rangle_{AB}$ back to Bob via Eve, the resulting global state (fully in Eve's hands) is given by Table II where $|\psi_{ij}\rangle$ are not normalized, and where the $|E_{ij}\rangle$ were chosen by Eve. Eve now applies a unitary V on $\mathscr{H}_E \otimes \mathscr{H}_{AB}$ and then sends Bob his part of the resulting state.

TABLE II
THE STATE IN EVE'S HANDS AFTER ALICE'S MEASUREMENT WHEN LOSSES AND MULTI-PHOTON PULSES ARE ALLOWED

Measurement	*Residual state (in Eve's hands)*
00	$\lvert\psi_{00}\rangle = \lvert E_{00}\rangle\,\lvert 0,0\rangle_{AB}$
01	$\lvert\psi_{01}\rangle = \sum_{n_\mathrm{o} \geq 1} \lvert E_{0 n_\mathrm{o}}\rangle\,\lvert 0, n_\mathrm{o}\rangle_{AB}$
10	$\lvert\psi_{10}\rangle = \sum_{n_\imath \geq 1} \lvert E_{n_\imath 0}\rangle\,\lvert n_\imath, 0\rangle_{AB}$
CTRL	$\lvert\psi\rangle = \lvert\psi_{00}\rangle + \lvert\psi_{01}\rangle + \lvert\psi_{10}\rangle$

Recall that Eve attacks now using the unitary V acting on the residual state in $\mathscr{H}_E \otimes \mathscr{H}_{AB}$, and then she sends Bob his part of the resulting state. Bob's measuring abilities put more constraints on the state $|\psi\rangle$ for Eve not to be detectable. In case the SIFT bit is used for TEST, Bob's probability of measuring 11 must be zero, no matter what Alice measured. Furthermore, for Eve to stay undetectable, if Alice measured $|0,0\rangle$ (namely, the outcome 00) in the SIFT mode, then Bob should have a probability zero of measuring 01 or 10, thus, a probability zero of receiving the states $|1,0\rangle$ or $|0,1\rangle$. Similarly if Alice measured 10 (01), then Bob should have a probability zero of measuring 01 (10); he could however get a loss, 00. The resulting (non normalized) Eve+Bob residual states thus take the form $|\psi'_{00}\rangle = V\,|\psi_{00}\rangle = |H_{00}\rangle\,|0,0\rangle_{AB}$ when a loss arrives, and

$$\begin{aligned} |\psi'_{01}\rangle = V\,|\psi_{01}\rangle &= \sum_{n_\mathrm{o} \geq 1} |F_{0 n_\mathrm{o}}\rangle\,|0, n_\mathrm{o}\rangle_{AB} + |H_{01}\rangle\,|0,0\rangle_{AB} \\ |\psi'_{10}\rangle = V\,|\psi_{10}\rangle &= \sum_{n_\imath \geq 1} |F_{n_\imath 0}\rangle\,|n_\imath, 0\rangle_{AB} + |H_{10}\rangle\,|0,0\rangle_{AB} \end{aligned} \tag{15}$$

otherwise; V being linear, the (normalized) residual state if Alice applied CTRL is $|\psi'\rangle \equiv V\,|\psi\rangle = |\psi'_{00}\rangle + |\psi'_{01}\rangle + |\psi'_{10}\rangle$.

In order to check CTRL bits, Bob measures $|\psi'\rangle$ in the x basis and checks if he gets at least one photon in any illicit state, such as $|-\rangle$; more precisely, he measures $|\psi'\rangle$ in the Fock basis $|n_-, n_+\rangle_x$ corresponding to the x basis of single photon states, and aborts if he gets $n_- > 0$ (if the detector for $|-\rangle$ photons clicks). To avoid that, Eve must make sure that the overlap between Eve-Bob's state $|\psi'\rangle$ and each state of the form $|n_-, n_+\rangle_x$ with $n_- > 0$ is zero. This results with another limitation on Eve's attack.

Lemma 1. *If Bob has a zero probability of measuring any state* $|n_-, n_+\rangle_x$ *with* $n_- > 0$*, then* $|F_{01}\rangle = |F_{10}\rangle$*, and* $|F_{0n}\rangle = |F_{n0}\rangle = 0$ *for* $n > 1$.

Proof (sketch).
Let $|\psi'\rangle = \sum_{n_\mathrm{o} \geq 1} |F_{0 n_\mathrm{o}}\rangle\,|0, n_\mathrm{o}\rangle + \sum_{n_\imath \geq 1} |F_{n_\imath 0}\rangle\,|n_\imath, 0\rangle +$

$|H\rangle|0,0\rangle$ be the Eve+Bob residual state. Let $|e^{(n)}\rangle = \big(|0,n\rangle + |n,0\rangle\big)/\sqrt{2}$ and $|o^{(n)}\rangle = \big(|0,n\rangle - |n,0\rangle\big)/\sqrt{2}$; it then holds that $|e^{(n)}\rangle$ (resp. $|o^{(n)}\rangle$) is a superposition with non zero amplitudes of the states $|n_-,n_+\rangle_x$ with n_- even (resp. n_- odd) and that moreover $|F_{0n}\rangle|0,n\rangle + |F_{n0}\rangle|n,0\rangle$ is equal to

$$\left[\frac{|F_{0n}\rangle + |F_{n0}\rangle}{\sqrt{2}}\right]|e^{(n)}\rangle + \left[\frac{|F_{0n}\rangle - |F_{n0}\rangle}{\sqrt{2}}\right]|o^{(n)}\rangle \qquad (16)$$

For $n = 1$ the probability of measuring $|1,0\rangle_x$ must be 0. Since $\langle e^{(1)} \mid 1,0\rangle_x = 0$ (because 1 is odd) and $\langle o^{(1)} \mid 1,0\rangle_x \neq 0$, the probability of measuring $|1,0\rangle_x$ is zero iff $\big[|F_{01}\rangle - |F_{10}\rangle\big]/\sqrt{2} = 0$ i.e. $|F_{01}\rangle = |F_{10}\rangle$. For $n > 1$, the probabilities of measuring both $|n,0\rangle_x$ and $|n-1,1\rangle_x$ must be 0, implying that $|F_{0n}\rangle + |F_{n0}\rangle = 0$ and $|F_{0n}\rangle - |F_{n0}\rangle = 0$ and thus $|F_{n0}\rangle = |F_{0n}\rangle = 0$. More details are left for the full journal paper (see a preliminary version in [10, Appendix C], where is also provided the expansion of the x-basis Fock states $|n_-,n_+\rangle_x$ using the z-basis Fock states $|n_1,n_\circ\rangle$). □

Letting $|F\rangle = |F_{01}\rangle = |F_{10}\rangle$, Eve+Bob's final residual states given by (15), if Alice measured 01 and 10, are reduced to, strikingly, exactly the same states given (for the simpler case) by (8) and (15) (respectively). As before, if Bob measures in the z basis and gets a SIFT bit, Eve's final state $|F\rangle$ is the same whether Bob measured 0 or 1 and she thus can get no information on either Alice's measurement or Bob's result: the protocol is completely robust.

V. Conclusions

From the above analysis, we conclude that Bob must in the end, on CTRL bits, get either a loss or exactly the state $|+\rangle$, which he thinks he sent. This does not mean that Eve's attack is trivial (namely, she must send $|+\rangle$ to Alice, and do nothing on the way back). As the simplest non-trivial attack, Eve could prepare the state $|E\rangle[|0,2\rangle + |2,0\rangle]/\sqrt{2}$, and apply the transformation $V[|E\rangle|0,2\rangle] = |E\rangle|0,1\rangle; V[|E\rangle|2,0\rangle] = |E\rangle|1,0\rangle$ on the way back, without being noticed, but also, without gaining any information, as we proved here. It is important to combine our result with the use of decoy states, which is now the common practice in QKD. We believe that our result holds also if our analysis is applied to the recent practical implementation using a laser pulse train [11], but checking this is left for future work.

References

[1] M. Boyer, D. Kenigsberg, and T. Mor, “Quantum key distribution with classical Bob,” *Phys. Rev. Lett.*, vol. 99, no. 14, p. 140501, 2007.

[2] ——, “Quantum key distribution with classical Bob,” in *ICQNM 2007*, vol. 0. Los Alamitos, CA, USA: IEEE Computer Society, Jan. 2007, p. 10, URL: http://doi.ieeecomputersociety.org/10.1109/ICQNM.2007.18 [accessed: 2015:03:04].

[3] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, “Semiquantum-key distribution using less than four quantum states,” *Phys. Rev. A*, vol. 79, no. 5, p. 052312, 2009.

[4] M. Boyer and T. Mor, “Comment on ‘Semiquantum-key distribution using less than four quantum states’,” arXiv, 2010, URL: http://arxiv.org/abs/1010.2221 [accessed: 2015:03:04].

[5] H. Lu and Q.-Y. Cai, “Quantum key distribution with classical Alice,” *International Journal of Quantum Information (IJQI)*, vol. 6, no. 6, pp. 1195–1202, 2008.

[6] M. Lucamarini and S. Mancini, “Quantum key distribution using a two-way quantum channel,” *Theoretical Computer Science*, vol. 560, Part 1, no. 0, pp. 46 – 61, 2014.

[7] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, 2000.

[8] Y.-g. Tan, H. Lu, and Q.-y. Cai, “Comment on ‘Quantum key distribution with classical Bob’,” *Phys. Rev. Lett.*, vol. 102, no. 9, p. 098901, 2009.

[9] M. Boyer, D. Kenigsberg, and T. Mor, “Boyer, Kenigsberg, and Mor reply,” *Phys. Rev. Lett.*, vol. 102, no. 9, p. 098902, 2009.

[10] M. Boyer and T. Mor, “On the robustness of (photonic) quantum key distribution with classical Alice,” arXiv, 2010, URL: http://arxiv.org/abs/1012.2418/ [accessed: 2015:03:04].

[11] T. Sasaki, Y. Yamamoto, and M. Koashi, “Practical quantum key distribution protocol without monitoring signal disturbance,” *Nature*, vol. 509, no. 7501, pp. 475–478, 05 2014, ISBN: 0028-0836.