Optimal individual attack on BB84 quantum key distribution using single-photon two-qubit quantum logic

Optimal individual attack on BB84 quantum key distribution using single-photon two-qubit quantum logic

Raúl García-Patrón, Franco N. C. Wong, Jeffrey H. Shapiro

Research Laboratory of Electronics, MIT, Cambridge, MA 02139, USA

ABSTRACT

We propose the use of single-photon two-qubit quantum logic to physically simulate the optimal individual attack on Bennett-Brassard 1984 quantum key distribution protocol. The experimental setup does not require a quantum memory due to the physical simulation character of the proposal.

Keywords: Quantum information, quantum key distribution, BB84, single-photon two-qubit quantum logic

1. INTRODUCTION

The Bennett-Brassard 1984 (BB84) quantum key distribution (QKD) protocol[1,2] permits two remote partners, Alice and Bob, to create a shared secret key. Its security against wiretapping attacks is guaranteed by quantum physics, namely, the no-cloning theorem,[3] which holds that it is impossible to perfectly copy non-orthogonal quantum states. Thus, by randomly encoding their key in two incompatible bases, Alice and Bob prevent an eavesdropper (Eve) from generating a perfect copy.

The enormous importance of secure communications has prompted many theoretical security studies of BB84 QKD, with a variety of assumptions about the protocol's operating conditions and equipment, as well as the eavesdropper's capabilities.[4–7] There are two kinds of attacks on a QKD system, *attacks on the line* between Alice and Bob, and *hardware attacks*. The latter take advantage of loopholes in specific implementations and include trojan horses, faked-state, time-shift, and backflashing attacks. In this manuscript, however, we will restrict our attention to attacks on the line, specifically those that can be physically simulated with current technology.

There have also been experimental studies of several eavesdropping attacks and strategies for thwarting them, e.g., the decoy-state method.[8,9] For example, some of us have recently performed a physical simulation of the entangling-probe attack on BB84 QKD using single-photon two-qubit (SPTQ) quantum logic.[10,11] Our experiment was a physical simulation because Bob and Eve's measurements must be made jointly in that their qubits reside on the same photon carrier. The entangling-probe attack maximizes Eve's information about Alice and Bob's error-free sifted bits for a given disturbance that her eavesdropping creates. However, BB84 QKD *requires* Alice and Bob to perform error correction (via authenticated classical communication that Eve can monitor but not modify), and the entangling-probe attack neglects the information that Eve can glean from this error-correction step. Hence, it is *not* the optimal individual attack on BB84 QKD.[12] The focus of the present paper is to show that the same SPTQ technique can perform a physical simulation of the optimal individual attack on BB84 QKD.

In Sec. II, we briefly review BB84 QKD. We devote Sec. III to the feasible attacks that an eavesdropper can implement. In Sec. IV, we propose a physical simulation of the economical cloning machine as the optimal individual attack on BB84 QKD. We conclude, in Sec. V, with a look at the feasibility of physically simulating this attack.

2. REVIEW OF BB84

The standard BB84 protocol is divided into two steps: (i) quantum communication, in which Alice and Bob generate a correlated bit string; and (ii) classical post-processing, in which they distill a secret key from that bit string. The usual implementation of BB84 is called *prepare and measure*, as Alice prepares random quantum states that are later measured by Bob, see Fig. 1. Here, before she transmits each photon, Alice generates two random bits (r, a). Alice uses r to choose the basis (computational $\{|0\rangle, |1\rangle\}$, or conjugate $\{|+\rangle = (|0\rangle +$

Quantum Information and Computation VIII, edited by Eric J. Donkor, Andrew R. Pirich, Howard E. Brandt,
Proc. of SPIE Vol. 7702, 77020C · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.849478

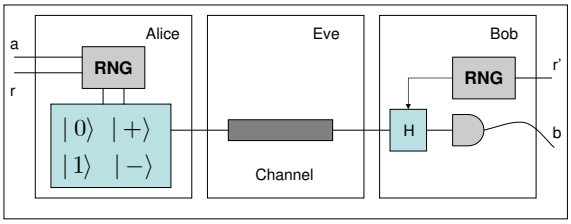

Figure 1. Schematic of the prepare-and-measure quantum communication step in single-photon BB84 QKD. Using a random number generator (RNG), Alice generates two random bits (r, a) that determine the state $(\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$ she will send to Bob through the quantum channel. Bob uses his random bit r' to control a Hadamard gate (H) that sets the basis (computational or conjugate) in which he will measure Alice's state. Any decoherence or loss incurred by Alice's state in its passage through the channel is assumed to be due to eavesdropping.

$|1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$) she will use to encode the bit a $(0 = \{|0\rangle, |+\rangle\}, 1 = \{|1\rangle, |-\rangle\})$. She does that encoding in an agreed-upon internal degree of freedom of the photon, such as polarization encoding (for free-space implementations) or time-bin encoding (for fiber implementations), and sends it to Bob over a quantum channel on which Eve may be eavesdropping. For each received photon, Bob randomly chooses to measure in either the computational or the conjugate basis (depending on the value of his own random bit r') obtaining the outcome b. Repeating this process many times (n realizations), Alice and Bob finally share a long string of correlated data.

After completing the quantum communication step, Alice and Bob initiate their classical post-processing. First, Bob informs Alice of the bits for which he detected a photon, thus accounting for loss incurred in the channel. Then Alice and Bob reject the detected bits for which their basis choices differed $(r \neq r')$. To accomplish this *sifting*, Alice employs an authenticated public classical channel to send Bob her string of basis choices. Sifting is followed by *direct error correction* *, in which Alice sends Bob a message through the authenticated public channel that allows him to correct the errors in his sifted data. The message must be as short as possible, in order to reveal the least amount of information to Eve, but sufficiently long to allow Bob to correct all of his errors. The error-correction protocol also enables Alice and Bob to estimate the channel's attenuation and noise levels, which, in turn, permits them to place an upper bound on Eve's information about their initial correlated bit string. Having that upper bound, Alice and Bob proceed to *privacy amplification*, using an algorithm such as hashing,[13] to distill a secret key from their perfectly correlated data.

There is an *entanglement-based* implementation of BB84 QKD[14] that is equivalent to the prepare-and-measure protocol described above. In the entanglement-based version, Alice generates a pair of photons in the Bell state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one to Bob through the quantum channel. Then both partners randomly and independently choose bases (computational or conjugate) in which they measure their respective photons. Interestingly, one can exploit the properties of quantum mechanics to obviate the need for random number generators by letting the quantum system do the random basis selection itself, as explained in Sec. IV. These measurements leave Alice and Bob with a correlated bit string on which they perform the classical post-processing to obtain the secret key. Both BB84 implementations (prepare-and-measure and entanglement-based) being equivalent, security analysis is generally done in the entanglement-based description.

2.1 Unconditional Security

To prove that BB84 is unconditionally secure, we need to guarantee security against Eve's most powerful attack, viz., the *coherent attack*. In this attack Eve has unlimited quantum computational power, complete control over the quantum channel, and can monitor without modifying the public communication (authenticated channel) between Alice and Bob. The only physical restriction on Eve is forbidding her access to Alice and Bob's equipment. Interestingly, it was shown by Renner[15] that in order to prove unconditional security it suffices to have security against a weaker attack called the *collective attack*. In a collective attack, each of Eve's ancilla interact

*Error correction is said to be *direct error correction* when the error-correcting communication is from Alice to Bob. When that communication goes from Bob to Alice it is called *reverse error correction*.

individually with a single photon sent by Alice and is then stored in a quantum memory. In the entanglement-based description of BB84, this means that Alice-Bob-Eve's tripartite quantum state before Eve's collective measurement is in a tensor product of n identical states ($\rho_{ABE}^{\otimes n}$). After listening to the public communication between Alice and Bob during the classical post-processing, Eve applies the optimal collective measurement to her ensemble of stored ancillae to gain the most information she can about Alice and Bob's key.

It is easy to see that Eve's optimal attack gives the following density matrix for Alice and Bob's state, ρ_{AB},[16]

$$\rho_{AB} = \lambda_1[\phi^+] + \lambda_2[\psi^+] + \lambda_3[\phi^-] + \lambda_4[\psi^-]. \tag{1}$$

This state is diagonal in the Bell basis, which consists of the four states $|\psi^\pm\rangle = [|01\rangle \pm |10\rangle]/\sqrt{2}$ and $|\phi^\pm\rangle = [|00\rangle \pm |11\rangle]/\sqrt{2}$, with $[\psi]$ denoting the projector $|\psi\rangle\langle\psi|$. During the error-correction process, Alice and Bob calculate the bit-flip error rate $Q_X = \lambda_2 + \lambda_4$ and the phase-flip error rate $Q_Z = \lambda_3 + \lambda_4$ incurred on their sifted initial data. Knowing the values of Q_X and Q_Z they can infer the secret key rate,

$$K = 1 - H(Q_X) - H(Q_Z), \quad \text{bits/sifted-photon.} \tag{2}$$

Realistic channels usually have the same error rates for bit flips and phase flips, i.e., the quantum bit error rate (QBER) obeys $Q = Q_X = Q_Z$. The secret key rate from (2) then reduces to the result of Shor and Preskill's security proof,[4]

$$K = 1 - 2H(Q), \quad \text{bits/sifted-photon.} \tag{3}$$

Most BB84 implementations do not distinguish between bit-flip and phase-flip errors, as they only calculate their average. In such cases, the concavity of the entropy shows that (3) gives a lower bound on the secret key rate when $Q_X \neq Q_Z$.

In realistic fiber-optic implementations, the unavoidable photon losses in the channel reduce the secret key rate, measured in bits/sec, by a factor α that decreases exponentially with increasing fiber length.[2] Experimental imperfections, such as dark counts in Bob's detector or degraded quantum-interference visibility in Bob's time-bin interferometer, contribute to the QBER.[2] In this manuscript we will assume the ideal situation in which error correction and privacy amplification are perfectly efficient, and we will consider the limit of an infinite number of transmitted photons. For a realistic implementation, with a finite number of photons and inefficient post-processing protocols, we have to take into account the deviations from the ideal case.[17]

3. FEASIBLE ATTACKS

Because high-capacity, high-fidelity, long-storage-time quantum memories are beyond current technological capabilities, the implementation of a collective attack by Eve is well beyond the current state of the art. Therefore, analyzing the security of a protocol against weaker classes of attacks is very relevant to near-term QKD applications.

If Eve cannot use a quantum memory, then her best approach is to apply an optimum positive operator-valued measurement (POVM) to her ancillae—one by one—to extract as much information about Alice's state as she can for a particular QBER. We call such a restricted attack, a *measurement attack*, of which the entangling-probe attack (also called the Slutsky-Brandt attack or the Fuchs-Peres-Brandt attack)[10,18] is an example. In 2007, some of us implemented a physical simulation of the entangling-probe attack,[11] using SPTQ quantum logic. As noted above, however, this attack ignores information that Eve might gain from Alice and Bob's error-correction process.[12] The class of measurement attacks has not received much attention to date, despite its practical interest. For example, it is not known if the entangling-probe attack is the best of this class.

Between the powerful collective attacks and the measurement attacks, ranges the class of *individual attacks*. In an individual attack, Eve has a quantum memory to store her ancillae, but she makes a measurement on each ancilla individually, doing so after sifting has occurred but before error correction takes place. Although such an individual attack requires a quantum memory, its measurement burden is lighter than that of the collective attack.

3.1 Optimal Individual Attack

Optimal individual eavesdropping can be achieved using a cloning machine, as shown in Ref. 19. For the BB84 protocol, the optimal individual attack employs the asymmetric Fourier-covariant cloning machine (AFCCM), which optimally and uniformly copies the states in the computational and conjugate bases.[20] The "asymmetric" designation means that the two copies of the input state—the one Eve sends to Bob and the one she retains—have different fidelities. Both fidelities satisfy a tradeoff relation between the amount of information that Eve gleans versus the QBER she creates on the quantum channel. The secret key rate corresponding to this attack is

$$K = H(Q_E) - H(Q), \quad \text{bits/sifted-photon}, \tag{4}$$

where Q_E is the error rate Eve incurs in her measurement of Alice's information, given by

$$Q_E = \frac{1}{2}\Big[1 - 2\sqrt{Q(1-Q)}\Big]. \tag{5}$$

A simpler version of the optimal individual attack against BB84 QKD was proposed in Ref. 21. This simpler attack is called the *economical cloner*, because Eve only uses one ancillary qubit, as shown in Fig. 2, whereas the AFCCM requires two ancillae. The economical cloner is indistinguishable from the AFCCM when Bob and

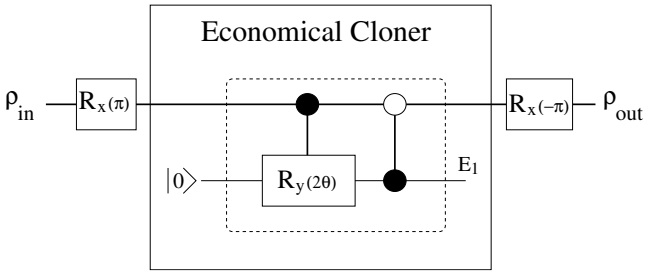

Figure 2. Quantum circuit diagram for the economical cloner. Eve prepares her ancilla in the state $|0\rangle$. Eve converts a Fourier-economical cloner into a Phase-economical cloner by applying a π-rad rotation about the Bloch-sphere's x axis to the input qubit and the inverse rotation to the output qubit. In between these rotations, she interacts her ancilla with Alice's state through a controlled rotation of 2θ ($\cos\theta = 1 - 2Q$) about the Bloch-sphere's y axis followed by a CNOT. Once the cloning is finished, Eve sends the outgoing qubit to Bob.

Eve's measurements are restricted to the computational and conjugate basis, as they are in BB84 QKD. This proves that the economical cloner provides an optimal individual attack on that protocol when Alice and Bob use direct error correction. In the following section we explain how to implement a physical simulation of the economical cloner based on SPTQ logic that was previously used to simulate the entangling-probe attack.[11]

4. PROPOSED EXPERIMENTAL IMPLEMENTATION OF ECONOMICAL CLONING

The main obstacles to implementing the economical cloning machine include the need for a universal two-qubit interaction and the need for high-fidelity quantum memory. In order to have any two-qubit operation carried out efficiently, Eve's ancilla qubit must be matched to Alice's qubit in space, time, and frequency, and the interaction between these qubits must be sufficiently strong to effect the desired operation. A quantum memory with high storage and retrieval efficiencies is also essential in this scheme, because Eve must delay her basis choice until Alice and Bob perform their sifting operation.

Both of these problems can be circumvented by implementing a physical simulation of the economical cloner in SPTQ logic, which exploits two independent photonic degrees of freedom to encode two qubits onto a single photon carrier. Some of us have previously demonstrated deterministic linear optics implementations of SPTQ CNOT[22] and SWAP[23] gates. Together with easily-implemented single qubit rotations, these give us a universal gate set for SPTQ-based quantum information processing.

One drawback of SPTQ logic is that with Bob and Eve's qubits residing on a single photon carrier the lack of viable quantum non-demolition measurements implies that both qubits must be measured simultaneously. This defect can be turned to our advantage, however, if we implement a physical simulation of the economical cloner attack—in which Bob and Eve share the measurement apparatus, but *not* their separate measurement results—because Eve no longer needs a quantum memory. As a result, a physical simulation based on SPTQ quantum logic allows us to study the characteristics of the economical cloning attack with real apparatus that includes the non-idealities of physical resources while eliminating the need for the as yet unavailable high-capacity, high-fidelity, long-storage-time quantum memory. In what follows, after reviewing the structure of SPTQ gates, we present the three parts of the economical cloner attack's physical simulation: (1) Alice's source; (2) Eve's cloning attack; and (3) Bob and Eve's simultaneous measurements.

4.1 SPTQ Logic

In SPTQ photonics, the two distinct qubits are the polarization and the momentum degrees of freedom of a single photon. Spontaneous parametric downconversion in a nonlinear optical crystal is used to generate pairs of photons, called signal and idler.[24] Detection of an idler photon heralds the presence of a single signal photon. The heralded single photon output is usually collimated so that the momentum qubit is equivalent to a spatial qubit, with a basis choice of left ($|L\rangle$) and right ($|R\rangle$). For SPTQ quantum logic, four different types of gates are required to form a universal gate set: (1) polarization rotation; (2) momentum rotation; (3) polarization-controlled NOT (P-CNOT);[22] and (4) momentum-controlled NOT (M-CNOT).[22] By cascading P-CNOT and M-CNOT gates we can implement a SWAP gate, which is particularly useful in SPTQ photonics.[23]

Single qubit rotation in the polarization degree of freedom is easily accomplished using half-wave plates (HWPs) and quarter-wave plates (QWPs). As an example, we show in Fig. 3 how to implement the π-rad rotation about the Bloch-sphere's x axis at the input of the economical cloner. On the other hand, in the

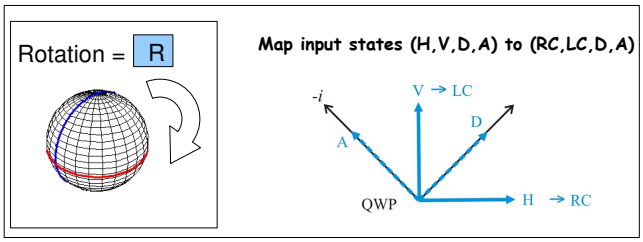

Figure 3. The π-rad rotation about the Bloch-sphere's x axis uses a quarter-wave plate (QWP) with its slow axis aligned with the antidiagonal polarization to transform the states H, V, D, A into RC, LC, D, A, where H denotes horizontal, V vertical, D diagonal, A antidiagonal, RC right-circular, and LC left-circular polarization. The inverse rotation R^{-1} is accomplished by aligning the QWPs slow axis with the diagonal polarization.

momentum (spatial) degree of freedom, it is much harder to apply an arbitrary rotation. Instead, it is most convenient to use a SWAP gate to exchange the values of the polarization and momentum qubits, apply the single-qubit rotation in the polarization space, and then use the SWAP gate to swap the qubit values again. In this way, the polarization qubit remains unchanged, and single-qubit rotation of the momentum qubit is easily achieved.

The momentum-controlled NOT, in which the momentum is the control qubit and the polarization the target qubit, can be realized with a HWP oriented at 45° relative to the horizontal polarization and acting only on one of the two beams, as shown in Fig. 4. The polarization-controlled NOT, in which the polarization is the control qubit and the momentum is the target qubit, consists of a polarization-Sagnac interferometer containing a dove prism whose base is oriented at 45° relative to the horizontal plane, as shown in Fig. 4. The input polarizing beam splitter (PBS) directs horizontally (vertically) polarized input light to travel in a clockwise (counterclockwise) direction. The dove prism orientation is different for the two counter-propagating directions, such that the transformation of the input spatial image differs for the horizontal (H) and vertical (V) polarizations.

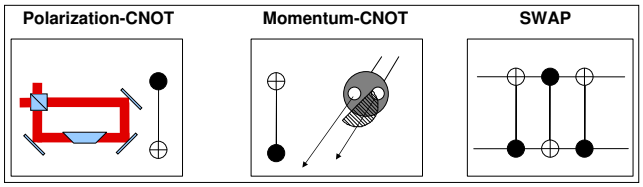

Figure 4. SPTQ logic controlled NOT gates and SWAP gate: (a) The polarization-controlled NOT consists of a polarization-Sagnac interferometer containing a dove prism whose base is oriented at 45° relative to the horizontal plane. The input polarizing beam splitter directs horizontally (vertically) polarized input light to travel in a clockwise (counterclockwise) direction. The dove prism orientation is different for the two counter-propagating directions, such that the transformation of the input spatial image differs for the horizontal (H) and vertical (V) polarizations. Specifically, the right-left (RL) sections of the input beam are mapped onto the top-bottom (TB) sections of the output beam for H-polarized light but onto the BT sections for V-polarized light.[22] (b) The momentum-controlled NOT can be realized with a HWP oriented at 45° relative to the horizontal polarization acting only on one of the two beams.[22] (c) By cascading P-CNOT and M-CNOT gates, we can implement a SWAP gate that is particularly useful in SPTQ photonics.[23]

4.2 Alice's Source

Alice may use either of two alternative implementations for her source: the prepare-and-measure and the entanglement-based schemes, as shown in Fig. 5.

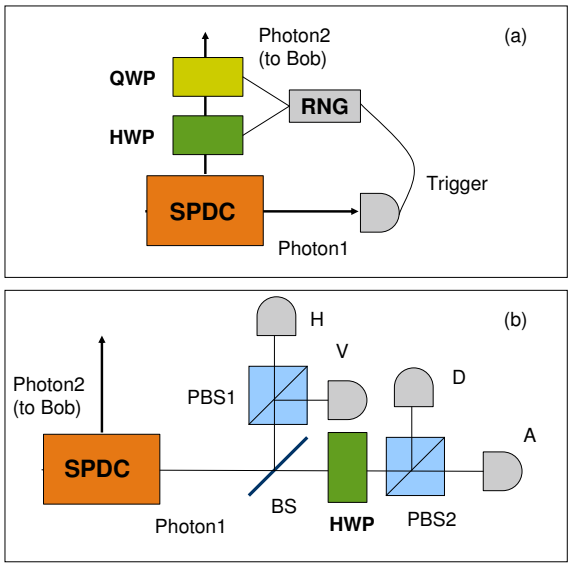

Figure 5. (a) Prepare-and-measure scheme: a pair of photons is generated by a SPDC source. Photon 1 is used as a trigger to herald photon 2 as a single-photon pulse for the BB84 protocol. Conditioned on the detection of photon 1, Alice applies a random polarization rotation to the heralded photon, using a HWP and a QWP, in order to encode her qubit in one of the four states H, V, D, A. (b) Entanglement-based scheme: Alice sends photon 2 to Bob and measures photon 1 in either the computational (H, V) or the conjugate basis (D, A). Photon 1 impinges on a 50-50 beam splitter (BS) that sends photon 1 to PBS1 or PBS2 with equal probability. PBS1 measures the computational basis, and, with the help of a HWP that rotates linear polarization states by 45°, PBS2 measures the conjugate basis.

In the prepare-and-measure scheme (Fig. 5(a)), we start with a pair of photons generated by a spontaneous parametric down conversion (SPDC) source. Photon 1 is used as a trigger to herald photon 2 as a single-photon pulse for the BB84 protocol. Conditioned on the detection of photon 1, Alice applies a random polarization

rotation using an electronically commanded HWP and QWP, in order to encode her qubit in one of the four states H, V, D, A.

In the entanglement-based scheme (Fig. 5(b)), Alice sends photon 2 to Bob and measures photon 1 in the computational (H, V) or the conjugate basis (D, A). First, photon 1 impinges on a 50-50 beam splitter (BS) which sends it to either PBS1 or PBS2 with equal probability. PBS1 measures the computational basis (H, V), whereas, with the help of a HWP that rotates the linear polarization states by 45°, PBS2 measures the conjugate basis. Interest in entanglement-based BB84 derives from the fact that quantum physics—rather than random-number generators—supplies Alice and Bob's basis choices and Alice's random key bits.

4.3 Cloning Interaction

Figure 6 shows the quantum circuit diagram for our SPTQ implementation of the economical cloner. Alice's qubit at the input is in one of four linear polarization states H, V, D, A under the standard BB84 protocol. We first map the input states H, V, D, A into RC, LC, D, A to simplify the SPTQ implementation of the economical cloner. The mapping is accomplished by use of a QWP with its fast and slow axes aligned with the D and A polarization axes, as shown in Fig. 3. The first step of the economical cloner is a $|\psi_A\rangle$-controlled rotation of

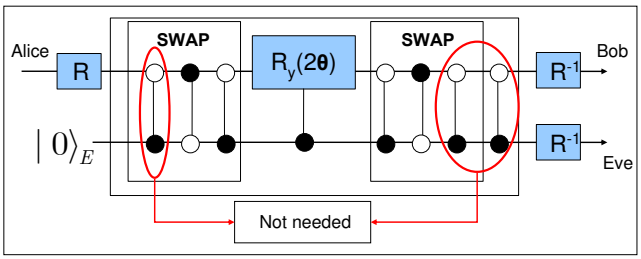

Figure 6. Quantum circuit diagram for SPTQ implementation of the economical cloner. Polarization and momentum qubits are represented by the upper and lower rails, respectively. Initial rotation R of Alice's qubit puts it on the equator of the Bloch sphere, while a subsequent inverse rotation R^{-1} restores the original orientation prior to Bob and Eve's measurements. The economical cloner is implemented using two SWAP gates and a controlled rotation $R_y(2\theta)$. The initial M-CNOT gate is not needed because Eve's input is in the state $|0\rangle$, and the last two M-CNOT gates cancel each other.

Eve's qubit $|\psi_E\rangle$, where $|\psi_A\rangle$ is the state of Alice's qubit after the polarization mapping by the rotation R, and $|\psi_E\rangle = |0\rangle = |L\rangle$. Linear polarization rotation $R_y(2\theta)$ about the y-axis of the Bloch sphere with an arbitrary angle θ for any linear polarization is more easily accomplished in polarization space, where two HWPs will do the trick, rather than in the momentum space. So, we implement the controlled rotation of Eve's qubit by first swapping the polarization and momentum qubits, then performing the controlled rotation, and finally applying another SWAP operation to return the qubits to their original spaces, as shown in Fig. 6. The first SWAP gate produces the state $|\psi_1\rangle = |H\rangle(\alpha'_A|L\rangle + \beta'_A|R\rangle)$, where α'_A, β'_A are the coefficients of Alice's qubit after the rotation R. To implement the controlled rotation $R_y(2\theta)$, we note that the control qubit is a momentum qubit and the desired action corresponds to a rotation of θ in the polarization space applied only for the right path $(|R\rangle = |1\rangle)$. Because the initial state of Eve's qubit is $|0\rangle$ (Eve's qubit being $|H\rangle$ after the SWAP), the rotation can be accomplished by a single HWP with its fast axis oriented at an angle $\theta/2$ relative to H such that the output polarization H' is rotated by θ from the initial orientation H, as shown in Fig. 7. The controlled rotation is completed with a SWAP operation to return Alice's qubit to the polarization space and Eve's qubit to the momentum space. The final CNOT gate cancels with part of the SWAP gate, simplifying the implementation as shown in Fig. 6. After the economical cloner is implemented, the reverse mapping R^{-1} is applied to return Bob and Eve's output qubits to the BB84 polarization bases. Because we are implementing a physical simulation, the R^{-1} operation can be delayed to the measurement stage without loss of generality, which again simplifies the implementation.

4.4 Measurement

In an individual attack, Eve and Bob measure in the same basis after sifting. This translates, in our physical simulation, to Bob and Eve's measuring the same basis simultaneously. In BB84 QKD, Bob randomly selects

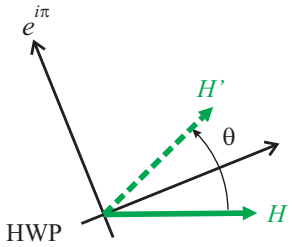

Figure 7. Implementation of controlled rotation $R_y(2\theta)$. For an initial state $|H\rangle$, the rotation is implemented using a half-wave plate (HWP) with its fast axis aligned at an angle $\theta/2$ from the H polarization axis, thus rotating it by an angle θ.

his measurement basis for each photon. This is achieved in Fig. 8(a) by implementing HWP1 and HWP2 using electro-optical modulators controlled by a random number generator (RNG). Depending on the output from the RNG, these HWPs do not apply a polarization rotation—so that Bob's measurement is in the computational basis—or they do apply the rotations necessary for Bob's measurement to be in the conjugate basis. For Bob and Eve's joint measurement in the computational basis, HWP1 and HWP2 have no effect on the qubits and after the SWAP gate Bob's qubit is in the L-R basis and Eve's qubit is in the H-V basis. For the conjugate-basis joint measurement, HWP1 converts the D-A basis into the H-V basis so that Bob's qubit can be analyzed in the computational basis. Then the SWAP gate swaps the qubits between Bob and Eve, so that Bob's qubit along the D and A polarization axes is now in the L and R paths, respectively. Once Bob's qubit is in the momentum space, HWP2 will have no effect on it. On the other hand, Eve's qubit, along L_+ or L_-, where $|L_\pm\rangle = (|L\rangle \pm |R\rangle)/\sqrt{2}$, becomes D or A after the SWAP gate, which is then converted into H or V by HWP2. As noted earlier, the reverse rotations R^{-1} can be delayed until the measurement stage, if desired, by preceding HWP1 and HWP2 with one QWP each.

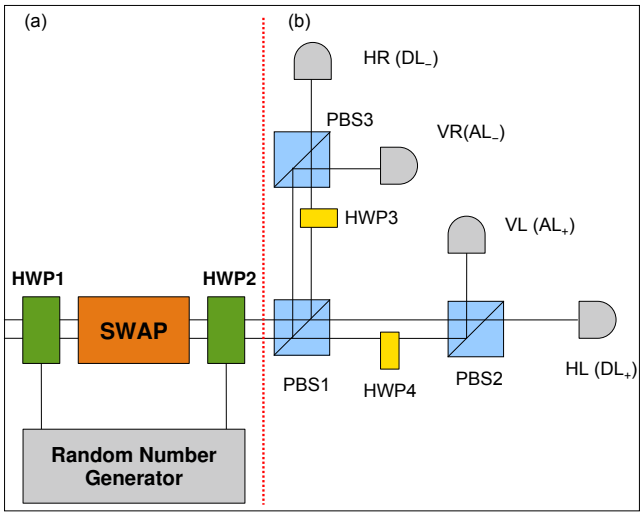

Figure 8. (a) Apparatus for swapping Bob and Eve's qubits for joint measurement in the computational basis (no rotation by HWP1 and HWP2) and the conjugate basis. (b) Apparatus for Bob and Eve's SPTQ measurements. Detectors are labeled to indicate the projected state of the joint measurement in the computational basis and the conjugate (in parentheses) basis. See text for details. PBS, polarizing beam splitter; HWP, half-wave plate.

Regardless of whether the joint measurement is performed in the computational or conjugate basis, Bob and Eve's qubits after the SWAP apparatus of Fig. 8(a) are in the L-R and H-V basis, respectively, and therefore we can use the same joint measurement apparatus of Fig. 8(b). The simplest way for Eve to distinguish H from V is

by means of a PBS, which transmits H-polarized light and reflects V-polarized light. After polarization analysis at PBS1, HWP4 in the R path rotates the transmitted H-polarized light into V-polarized light, but the light in the L path remains H polarized. Then PBS2 separates L from R and directs them to separate single-photon counters. Similarly, the combination of HWP3 and PBS3 in the reflected beams of PBS1 also separates Bob's qubit in the L and R basis. A click in any one of the four detectors then projects Bob and Eve's qubits into one of the four desired combinations, as labeled in Fig. 8(b) for their joint measurement in the computational basis. The labels in parentheses are for the conjugate-basis joint measurement.

As noted earlier for the entanglement-based source, Bob can use quantum physics—rather than a random-number generator—to supply his basis choices. To do so, he places a 50-50 beam splitter at the entrance to his receiver, sending Alice's photon to computational or conjugate basis measurement setups with equal probability. The advantage of such a scheme is that Bob no longer needs a random number generator. The price he pays is a doubling of the optical components (beam splitters and single-photon detectors) in his detection setup.

5. CONCLUSION

We have shown that the economical cloner is the optimal individual eavesdropping attack on BB84 QKD when Alice and Bob use direct error correction, and that it can be physically simulated using single-photon two-qubit quantum logic. We have already applied SPTQ photonics to physically simulate the entangling-probe attack on BB84, obtaining very good agreement between theory and experiment. In that work we used a P-CNOT gate and a SWAP gate for the implementation. The SWAP gate contains a P-CNOT gate and two M-CNOT gates, where the difficulty of implementing a P-CNOT gate is significantly higher than that for an M-CNOT gate. The application of SPTQ logic to physically simulate the economical cloner requires at most three P-CNOT gates, two of which are required for implementing the economical cloner, as shown in Fig. 6. The third P-CNOT gate is needed in the qubit measurement apparatus (for measurement in the conjugate basis). Thus, physical simulation of the economical cloner will be more difficult than what we did for the entangling-probe attack. Nevertheless, based on that earlier experience, we believe that physically simulating the optimal individual attack is well within the experimental state of the art. The ability to implement optimal individual attacks should provide the QKD community with experimentally realistic data for testing BB84 eavesdropping vulnerability and learning about the interplay between security and post-processing protocols.

ACKNOWLEDGMENTS

This research was supported by W. M. Keck Foundation Center for Extreme Quantum Information Theory.

REFERENCES

[1] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, pp 175-179 (1984).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145-195 (2002).

[3] W. K. Wootters and W. H. Zurek, A single quantum cannot be clonned, Nature 299, 802-803 (1982).

[4] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. 85, 441-444 (2000).

[5] D. Mayers, Unconditional security in quantum cryptography, J. ACM 48, 351-406 (2001); H.-K. Lo, A Simple Proof of the Unconditional Security of Quantum Key Distribution, J. Phys. A 34, 6957-6969 (2001).

[6] C. H. Bennett et al., Experimental Quantum Cryptography, J. Cryptology 5, 3-28 (1992); C. H. Bennett et al., Generalized Privacy Amplification, IEEE Trans. Inf. Theory 41, 1915-1923 (1995).

[7] B. Slutsky et al., Effect of channel imperfection on the secrecy capacity of a quantum cryptographic system, J. Mod. Opt. 44, 953-961 (1997); G. Brassard, N. Ltkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. 85, 1330-1333 (2000); G. Gilbert and M. Hamrick, Practical Quantum Cryptography: A Comprehensive Analysis (Part One), e-print quant-ph/0009027; V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. 52, 691-705 (2005).

[8] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. 91, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. 94, 230504 (2005).

[9] Y. Zhao et al., Experimental Quantum Key Distribution with Decoy States, Phys. Rev. Lett. 96, 070502 (2006); D. Rosenberg et al., Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber, Phys. Rev. Lett. 98, 010503 (2007); Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Unconditionally secure one-way quantum key distribution using decoy pulses," Appl. Phys. Lett. 90, 011118 (2007).

[10] J. H. Shapiro and F. N. C. Wong, Attacking quantum key distribution with single-photon two-qubit quantum logic, Phys. Rev. A 73, 012315 (2006).

[11] T. Kim, I. S. G. Wersborg, F. N. C. Wong, and J. H. Shapiro, Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol, Phys. Rev. A 75, 042327 (2007).

[12] I. M. Herbauts, S. Bettelli, H. Hbel, and M. Peev, On the optimality of individual entangling-probe attacks against BB84 quantum key distribution, Eur. Phys. J. D 46, 395-406 (2008).

[13] G. Van Assche, [Quantum Cryptography and Secret-Key Distillation], Cambridge University Press, Cambridge (2006).

[14] R. Ursin et al., Entanglement-based quantum communication over 144 km, Nature Physics 3, 481-486 (2007).

[15] R. Renner, [Security of quantum key distribution], ETH, Zrich (2005).

[16] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A 72, 012332 (2005).

[17] V. Scarani and R. Renner, Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing, Phys. Rev. Lett. 100, 200501 (2008).

[18] C. A. Fuchs and A. Peres, Quantum-state disturbance versus information gain: Uncertainty relations for quantum information, Phys. Rev. A 53, 2038-2045 (1996); B. A. Slutsky et al., Security of quantum cryptography against individual attacks, Phys. Rev. A 57, 2383-2398 (1998); H. E. Brandt, Quantum-cryptographic entangling probe, Phys. Rev. A 71, 042312 (2005).

[19] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, Phys. Rev. Lett. 88, 127902 (2002); N. J. Cerf, Asymmetric quantum cloning machines in any dimension, J. Mod. Opt. 47, 187-209 (2000).

[20] N. J. Cerf and J. Fiurasek, Optical quantum cloning, Progress in Optics 49, 455-545 (2006).

[21] C.-S. Niu, R. B. Griffiths, Two-qubit copying machine for economical quantum eavesdropping, Phys. Rev. A 60, 2764-2776 (1999).

[22] M. Fiorentino and F. N. C. Wong, Deterministic Controlled-NOT Gate For Single-Photon Two-Qubit Quantum Logic, Phys. Rev. Lett. 93, 070502 (2004).

[23] M. Fiorentino, T. Kim, and F. N. C. Wong, Single-photon two-qubit SWAP gate for entanglement manipulation, Phys. Rev. A 72, 012318 (2005).

[24] F. N. C. Wong, J. H. Shapiro, and T. Kim, Efficient generation of polarization-entangled photons in a nonlinear crystal, Laser Phys. 16, 1517-1524 (2006).