Experimentally feasible protocol for semiquantum key distribution

Michel Boyer,[1,*] Matty Katz,[2] Rotem Liss,[2,†] and Tal Mor[2,‡]
[1]*Département IRO, Université de Montréal, Montréal, Québec H3C 3J7, Canada*
[2]*Computer Science Department, Technion, Haifa 3200003, Israel*
(Received 17 August 2017; published 29 December 2017)

Quantum key distribution (QKD) protocols make it possible for two quantum parties to generate a secret shared key. Semiquantum key distribution (SQKD) protocols, such as "QKD with classical Bob" and "QKD with classical Alice" (that have both been proven robust), achieve this goal even if one of the parties is classical. However, existing SQKD protocols are not experimentally feasible with current technology. Here we suggest a protocol, "Classical Alice with a controllable mirror," that can be experimentally implemented with current technology (using four-level systems instead of qubits), and we prove it to be robust.

DOI: 10.1103/PhysRevA.96.062335

I. INTRODUCTION

Quantum key distribution (QKD) makes it possible for two legitimate parties, Alice and Bob, to generate an information-theoretically secure key [1], that is secure against any possible attack (of the adversary Eve) allowed by the laws of quantum physics. Alice and Bob use an insecure quantum channel and an authenticated classical channel.

Semiquantum key distribution (SQKD) protocols limit one of the parties to be classical, while still giving a secure key [2]. As explained in [2,3], such SQKD protocols are interesting from both the conceptual and the practical points of view; moreover, in a network of one quantum center and many classical "users," the classical users may even be oblivious to being involved in a quantum cryptographic protocol.

The use of SQKD protocols was introduced by [2], who also presented the "QKD with classical Bob" protocol; later, the "QKD with classical Alice" [4,5] protocol was suggested, as well as various other SQKD protocols (see, for example, [6–8]). Most of the SQKD protocols have been proven "robust": namely [2], any successful attack by an adversary necessarily induces some noise that the legitimate parties may notice. A few of them also have their full security analyzed [9].

However, to the best of our knowledge, all the currently existing SQKD protocols cannot be experimentally constructed in a secure way by using current technology, because, as explained below, one of the "classical" operations (SIFT) cannot be securely implemented.

We present a feasible SQKD protocol that can be experimentally constructed by using a "controllable mirror." It is based on "QKD with classical Alice" [4,5], but it is slightly more complicated, because it uses four-level systems instead of qubits (two-level systems), and because it requires Alice to choose one of four operations (instead of two). We prove this protocol to be robust.

In Sec. II we present the original "QKD with classical Alice" protocol, and in Sec. III we explain why this protocol and the other currently existing protocols are experimentally infeasible with current technology. In Sec. IV we present the "Classical Alice with a controllable mirror" SQKD protocol, and in Sec. V we prove it to be robust. We conclude in Sec. VI.

II. QUANTUM KEY DISTRIBUTION WITH CLASSICAL ALICE

In the "QKD with classical Alice" protocol [4] (the name is following [5]), in each round, the originator Bob sends to Alice the qubit state $|+\rangle$. Then, Alice randomly chooses one of two classical operations: CTRL—reflect the qubit to Bob—or SIFT—measure the qubit in the computational (i.e., the classical) basis $\{|0\rangle,|1\rangle\}$ and resend it to Bob. Bob then measures the qubit he receives from classical Alice, choosing randomly the measurement basis (the computational basis or the Hadamard basis $\{|+\rangle, |-\rangle\}$). After N qubits have been sent and received, Alice publicly announces her choice (CTRL or SIFT) for each round, and Bob publicly announces his basis choice for each round. Then, Alice and Bob check the error rates in the CTRL bits and in a random subset of the SIFT bits, aborting if they are too high. Finally, Alice and Bob perform error correction and privacy amplification on the remaining SIFT bits measured by Bob in the computational basis, so that they get a final identical key that is completely secret.

As proven in [5], "QKD with classical Alice" [4] is completely robust against eavesdropping. The proof of robustness was extended in [10] to include photonic implementations and multiphoton pulses.

III. THE EXPERIMENTAL INFEASIBILITY OF THE SIFT OPERATION IN SQKD PROTOCOLS

In the SQKD protocols (e.g., [2,4]), one of the classical operations is SIFT: measuring in the computational basis $\{|0\rangle,|1\rangle\}$ and then resending. In practical (photonic) implementations, and especially if limited to the existing technology, the SIFT operation is very hard to securely implement, because the generated photon will probably be at a different timing or frequency, thus leaking information to the eavesdropper; see details in [11] (which is a comment on [2]) and in the reply [12].

For example, let us look at the "QKD with classical Alice" protocol implemented with two *classical* modes, $|0\rangle$ and $|1\rangle$, describing two pulses (two distinct time bins) on a single arm. The photon can be either in one pulse, in the other, or in

*boyer@iro.umontreal.ca
†rotemliss@cs.technion.ac.il
‡talmo@cs.technion.ac.il

a superposition (a nonclassical state). In this case, the SIFT operation requires Alice to measure the two pulses, to generate a single photon in a state depending on the measurement outcome, and to resend it to Bob, while Alice can implement the CTRL operation simply by using a mirror (reflecting both pulses). In this case, it is indeed very difficult for Alice to regenerate the SIFT photon exactly at the right timing, so that it is indistinguishable from a CTRL photon.

Furthermore, in [11] it was shown that even if Alice could (somehow) have the machinery to perform SIFT with perfect timing, Eve would still be able to attack the protocol by taking advantage of the fact that Alice's detectors are imperfect: Eve's attack is modifying the *frequency* of the photon generated by Bob. Alice does not notice the change in frequency. If Alice performs SIFT, the photon she generates is in the original frequency; if she performs CTRL, the photon she reflects is in the frequency modified by Eve. Therefore, if Eve is powerful enough, she can measure the frequency and tell whether Alice used SIFT or CTRL. If Eve finds out that Alice used SIFT, she can copy the bit sent by Alice in the computational basis; if she finds out that Alice used CTRL, she shifts the frequency back to the original frequency. (A very similar attack works for other implementations, too, e.g., for polarization-based or phase-based implementations.) This "tagging" attack makes it possible for Eve to get full information on the key without inducing noise.

IV. THE CONTROLLABLE MIRROR PROTOCOL FOR QKD WITH CLASSICAL ALICE

We suggest an experimentally feasible SQKD protocol, similar to the infeasible protocol "QKD with classical Alice": in the original protocol of "QKD with classical Alice," Alice could choose only between two operations (CTRL and SIFT); in our protocol, Alice may choose between four operations (CTRL, SWAP-10, SWAP-01, and SWAP-ALL). This protocol avoids the need of using the infeasible operation SIFT. The two operations SWAP-10 and SWAP-01 correspond to two possible reflections of *pulses* by using a controllable mirror. Those operations cannot be described by qubit notations, so below we use four-level system notations. Our protocol is based on the Fock-space notations: in those notations, the state $|m_1,m_0\rangle$ represents m_1 indistinguishable photons in the mode of the qubit state $|1\rangle$ and m_0 indistinguishable photons in the mode of the qubit state $|0\rangle$. More details about the Fock-space notations are given in Appendix A.

This protocol is experimentally feasible and is safe against the "tagging" attack described in [11]. Moreover, we prove this protocol to be completely robust against an attacker Eve that can do anything allowed by the laws of quantum physics, including the possibility of sending multiphoton pulses (namely, assuming that Eve may use any quantum state consisting of the two modes $|0\rangle$ and $|1\rangle$, that is, any superposition of the Fock states $|m_1,m_0\rangle$).

We can describe the protocol in terms of photon pulses that correspond to two distinct time bins, and of a controllable mirror operated by Alice: in this case, the CTRL operation corresponds to operating the mirror on both pulses (reflecting both pulses back to the originator, Bob); the SWAP-10 operation corresponds to operating the mirror only on the $|0\rangle$ pulse while measuring the other pulse (and similarly for the SWAP-01 operation and the $|1\rangle$ pulse); and the SWAP-ALL operation corresponds to measuring all the pulses, without reflecting any of them.

For the experimental implementation, we note that a (very slow) mechanically moved mirror is trivial to implement; a much faster device can be electronically implemented by using standard optical elements (that are commonly used in QKD): a Pockels cell [that can change the polarization of the photon(s) in one of the pulses] and a polarizing beam splitter (that makes it possible to split the two different pulses into two paths, because they are now differently polarized). Like other (fast) QKD experimental settings, implementation is feasible but is not trivial.

Let Alice's initial probe be in the vacuum state $|0,0\rangle_A$, and let us assume that a single photon is arriving from Bob; thus, the system *as a whole* can be described as a four-level system (a single photon in four modes). Alice's operations are as follows.

I (CTRL): Do nothing:

$$I\,|0,0\rangle_A\,|m_1,m_0\rangle_B = |0,0\rangle_A\,|m_1,m_0\rangle_B. \tag{1}$$

S_1 (SWAP-10): Swap half of Alice's probe (the left mode) with the $|m_1\rangle_B$ half of Bob's state:

$$S_1\,|0,0\rangle_A\,|m_1,m_0\rangle_B = |m_1,0\rangle_A\,|0,m_0\rangle_B. \tag{2}$$

S_0 (SWAP-01): Swap half of Alice's probe (the right mode) with the $|m_0\rangle_B$ half of Bob's state:

$$S_0\,|0,0\rangle_A\,|m_1,m_0\rangle_B = |0,m_0\rangle_A\,|m_1,0\rangle_B. \tag{3}$$

S (SWAP-ALL): Swap the entire probe of Alice with the entire state $|m_1,m_0\rangle_B$ of Bob:

$$S\,|0,0\rangle_A\,|m_1,m_0\rangle_B = |m_1,m_0\rangle_A\,|0,0\rangle_B. \tag{4}$$

After each of the three SWAP operations, Alice measures her probe (the $|\cdot\rangle_A$ state) in the computational basis and sends to Bob the $|\cdot\rangle_B$ state. If there is no noise and no eavesdropping, and if we analyze the "ideal case" (in which exactly one photon is arriving from Bob to Alice), then each round is described by the four-dimensional Hilbert space $\mathrm{Span}\{|0,0\rangle_A\,|0,1\rangle_B, |0,0\rangle_A\,|1,0\rangle_B, |0,1\rangle_A\,|0,0\rangle_B, |1,0\rangle_A\,|0,0\rangle_B\}$, namely, by a four-level system; for our protocol, we use this four-level system instead of the qubit used by BB84 and by many other QKD schemes. In the most general "theoretical attack" (the attack analyzed by standard QKD security proofs), Eve attacks Alice's and Bob's states using any probe of her choice, but she cannot modify the four-dimensional Hilbert space of the protocol: she can only use those four levels. However, in practical attacks (as analyzed in our robustness analysis), Eve may use an extended Hilbert space (the entire Fock space).

While Eve is fully powerful, it is common to assume that Alice and Bob are limited to use only current technology. In particular, Alice and Bob are limited in the sense that they cannot *count* the number of photons in each mode, but can only check whether a detector corresponding to a specific mode clicks (detects at least one photon in that mode) or not (detects an empty mode). For our protocol to be practical (and for our robustness analysis to be stronger), we assume that Alice and Bob are indeed limited in that sense. Therefore, when Alice and

TABLE I. The four possible measurement results by Alice or Bob (measuring in the computational basis), depending on the state obtained by him or her (that is represented in the Fock-space notations).

Obtained state	Measurement result	Sum
$\|0,0\rangle$	00	0
$\|0,m_0\rangle$ $(m_0 > 0)$	01	1
$\|m_1,0\rangle$ $(m_1 > 0)$	10	1
$\|m_1,m_0\rangle$ $(m_1 > 0, m_0 > 0)$	11	2

TABLE III. Interpretations of Alice's and Bob's measurement results for SWAP-x states.

Alice's sum	Bob's sum	Interpretation
0	0	A loss
0	1	Alice and Bob share a bit
1	0	Alice and Bob do not share a bit
1	1	An error
0 or 1	2	An error
2		Impossible

Bob measure in the computational basis, their measurement results are denoted as $\hat{m}_1\hat{m}_0$, with $\hat{m}_0,\hat{m}_1 \in \{0,1\}$. Similarly, when Bob measures in the Hadamard basis, his measurement result is $\hat{m}_-\hat{m}_+$, with $\hat{m}_+,\hat{m}_- \in \{0,1\}$.

This limitation leads to the definition of "sum," as follows: let us look at a measurement result of Alice or Bob (that is 00, 01, 10, or 11). The sum of this measurement result is the number of distinct modes detected to be nonempty during the measurement (namely, the sum of the digits in the measurement result). This definition is summarized in Table I.

The protocol consists of the following steps.

(1) In each of the N rounds, Bob sends to Alice the state $|+\rangle_B$; Alice randomly chooses one of her four classical operations (CTRL, SWAP-10, SWAP-01, or SWAP-ALL) and sends the result back to Bob; Bob measures the state he receives, choosing randomly whether to measure in the computational basis or in the Hadamard basis.

(2) Alice reveals her operation choices [CTRL, SWAP-x ($x \in \{01,10\}$), or SWAP-ALL; Alice does *not* reveal her choices between SWAP-10 and SWAP-01, that she keeps as a secret bit string], and Bob reveals his basis choices. They discard all CTRL bits Bob measured in the computational basis and all SWAP-x bits he measured in the Hadamard basis.

(3) For each of the SWAP-x and SWAP-ALL states, Alice and Bob reveal the sums of their measurement results.

(4) Alice and Bob interpret their measurement results: they consider several types of measurement results as errors, losses, or valid results. See Tables II–IV for the details.

(5) For all the SWAP-x ($x \in \{01,10\}$) states, if Bob's sum is 1 and Alice's sum is 0, then Alice and Bob share a (secret) bit b, because Alice knows (in secret) what operation S_{1-b} she performed, and Bob knows (in secret) what mode $|b\rangle$ he detected. Each one of Alice and Bob keeps this sequence of bits b as his or her bit string.

(6) Alice and Bob reveal some random subset of their bit strings, compare them, and estimate the error rate (this is the error rate in the way from Alice back to Bob). They abort the protocol if the error rate in those bits, or any of the error rates measured in step 4, is above a specified threshold. They discard the revealed bits.

(7) Alice and Bob perform error correction and privacy amplification processes on the remaining bit string, yielding a final key that is identical for Alice and Bob and is fully secure from any eavesdropper.

Notice that Bob does not have a special role in the beginning: he always generates the same state, $|+\rangle$. It is even possible that the adversary Eve generates this state instead of him.

V. ROBUSTNESS ANALYSIS

To prove robustness, we will prove that for Eve's attack to be undetectable by Alice and Bob (namely, for Eve's attack not to cause any errors) it must not give Eve any information.

Eve's attack on a state can be performed in both directions: from the source (Bob) to Alice, Eve applies U; from Alice back to Bob, Eve applies V. We may assume, without limiting generality, that Eve uses a fixed probe space $\mathcal{H}_E$ for her attacks.

According to the definition of robustness, we will prove that if, during a run of the protocol, no error can be detected by Alice and Bob, then Eve gets no information on the raw key.

If Alice and Bob cannot find any error, the following conditions must be satisfied for all the measurement results that were not discarded due to basis mismatch.

(1) For all CTRL states, Bob's measurement result (in the Hadamard basis) must not be 10 or 11 (namely, Bob must never detect any photon in the $|-\rangle$ mode).

(2) For all SWAP-x states, Alice's sum and Bob's sum (in the computational basis) must not be both 1.

(3) For all SWAP-x states, Bob's sum (in the computational basis) must not be 2 (namely, Bob's measurement result must not be 11).

(4) For all SWAP-x states, no error (that may be detected during the protocol) can exist. In other words, (a) for all SWAP-

TABLE II. Interpretations of Bob's measurement results for CTRL states.

Bob's result	Interpretation
00	A loss
01 (i.e., $\|+\rangle$)	A legal result
10 (i.e., $\|-\rangle$)	An error
11	An error

TABLE IV. Interpretations of Alice's and Bob's measurement results for SWAP-ALL states.

Alice's result	Bob's result	Interpretation
00	00	A loss
01 or 10	00	A legal result
11	00	An error
	01, 10, or 11	An error

TABLE V. The (non-normalized) state of the Bob+Eve system after Alice's operation, given Alice's sum. Note that the states $|\varphi_{1,0}\rangle$, $|\varphi_{0,1}\rangle$, and $|\varphi_{0,0}\rangle$ are defined in Eqs. (7)–(9).

Operation	Alice	Bob+Eve state
CTRL		$\|\psi_{\text{CTRL}}\rangle \triangleq \|\varphi_{1,0}\rangle + \|\varphi_{0,1}\rangle + \|\varphi_{0,0}\rangle$
SWAP-10	0	$\|\psi^{(0)}_{\text{S-10}}\rangle \triangleq \|\varphi_{0,1}\rangle + \|\varphi_{0,0}\rangle$
SWAP-01	0	$\|\psi^{(0)}_{\text{S-01}}\rangle \triangleq \|\varphi_{1,0}\rangle + \|\varphi_{0,0}\rangle$
SWAP-10	1	$\rho^{(1)}_{\text{S-10}} \triangleq \sum_{m_1>0} \|0,0\rangle_{\text{B}}\langle 0,0\| \otimes \|E_{m_1,0}\rangle_{\text{E}}\langle E_{m_1,0}\|$
SWAP-01	1	$\rho^{(1)}_{\text{S-01}} \triangleq \sum_{m_0>0} \|0,0\rangle_{\text{B}}\langle 0,0\| \otimes \|E_{0,m_0}\rangle_{\text{E}}\langle E_{0,m_0}\|$
SWAP-ALL		$\rho_{\text{S-ALL}} \triangleq \rho^{(1)}_{\text{S-10}} + \rho^{(1)}_{\text{S-01}} + \|\varphi_{0,0}\rangle\langle\varphi_{0,0}\|$

10 states, Bob's measurement result (in the computational basis) must not be 10, and (b) for all SWAP-01 states, Bob's measurement result (in the computational basis) must not be 01.

(5) For all SWAP-ALL states, Alice's measurement result must not be 11.

(6) For all SWAP-ALL states, Bob's measurement result must not be 01, 10, or 11.

We now analyze each round of the protocol. After the round begins, the source (Bob) sends to Alice the state $|0,1\rangle_{x,B} \in \mathcal{H}_{\text{B}}$. Eve can now interfere: she attaches her own probe state (in the Hilbert space $\mathcal{H}_{\text{E}}$) and applies the unitary transformation U. The resulting Bob+Eve state (including Eve's probe) is of the form

$$|\psi_{\text{init}}\rangle \triangleq \sum_{m_1,m_0} |m_1,m_0\rangle_{\text{B}} |E_{m_1,m_0}\rangle_{\text{E}}, \tag{5}$$

where $|E_{i,j}\rangle_{\text{E}}$ are non-normalized vectors in $\mathcal{H}_{\text{E}}$.

Condition 5 means that $|E_{m_1,m_0}\rangle_{\text{E}} = 0$ for all m_1,m_0 satisfying $m_1 > 0$ and $m_0 > 0$. Therefore,

$$|\psi_{\text{init}}\rangle = |\varphi_{1,0}\rangle + |\varphi_{0,1}\rangle + |\varphi_{0,0}\rangle, \tag{6}$$

with

$$|\varphi_{1,0}\rangle \triangleq \sum_{m_1>0} |m_1,0\rangle_{\text{B}} |E_{m_1,0}\rangle_{\text{E}}, \tag{7}$$

$$|\varphi_{0,1}\rangle \triangleq \sum_{m_0>0} |0,m_0\rangle_{\text{B}} |E_{0,m_0}\rangle_{\text{E}}, \tag{8}$$

$$|\varphi_{0,0}\rangle \triangleq |0,0\rangle_{\text{B}} |E_{0,0}\rangle_{\text{E}}. \tag{9}$$

Alice now applies one of the four possible operations (CTRL $= I$, SWAP-10 $= S_1$, SWAP-01 $= S_0$, or SWAP-ALL $= S$) and destructively measures her probe state. The (non-normalized) state of the Bob+Eve system after Alice's operation (and measurement) is written in Table V.

Then, Eve applies a second unitary transformation V on the state sent from Alice to Bob (and on her own probe state). According to conditions 2, 3, and 6, the density matrices $V\rho^{(1)}_{\text{S-10}}V^\dagger$, $V\rho^{(1)}_{\text{S-01}}V^\dagger$, and $V\rho_{\text{S-}ALL}V^\dagger$ must only overlap with $|0,0\rangle_{\text{B}}$. It follows that there exists $|H_{0,0}\rangle_{\text{E}} \in \mathcal{H}_{\text{E}}$ such that

$$V|\varphi_{0,0}\rangle = |0,0\rangle_{\text{B}} |H_{0,0}\rangle_{\text{E}}. \tag{10}$$

Let $V|\varphi_{1,0}\rangle = \sum_{m_1,m_0} |m_1,m_0\rangle_{\text{B}} |F_{m_1,m_0}\rangle_{\text{E}}$. Let us look at a SWAP-01 state for which Alice's sum is zero. For this state, the Bob+Eve state after Eve's attack is

$$V|\psi^{(0)}_{\text{S-01}}\rangle = V|\varphi_{1,0}\rangle + V|\varphi_{0,0}\rangle = \sum_{m_1,m_0} |m_1,m_0\rangle_{\text{B}} |F_{m_1,m_0}\rangle_{\text{E}} + |0,0\rangle_{\text{B}} |H_{0,0}\rangle_{\text{E}}, \tag{11}$$

and following conditions 4(b) and 3 Bob must not detect a photon in the $|0\rangle$ mode (otherwise, the error may be detected during the protocol). Therefore, $|F_{m_1,m_0}\rangle_{\text{E}} = 0$ for all $m_0 > 0$. It follows that

$$V|\varphi_{1,0}\rangle = \sum_{m_1>0} |m_1,0\rangle_{\text{B}} |F_{m_1,0}\rangle_{\text{E}} + |0,0\rangle_{\text{B}} |F_{0,0}\rangle_{\text{E}}. \tag{12}$$

Similarly [following conditions 4(a) and 3],

$$V|\varphi_{0,1}\rangle = \sum_{m_0>0} |0,m_0\rangle_{\text{B}} |G_{0,m_0}\rangle_{\text{E}} + |0,0\rangle_{\text{B}} |G_{0,0}\rangle_{\text{E}}. \tag{13}$$

Now, Eqs. (10), (12), and (13) imply that if Alice applies CTRL the Bob+Eve state after Eve's attack is

$$V|\psi_{\text{CTRL}}\rangle = \sum_{m>0} [|m,0\rangle_{\text{B}} |F_{m,0}\rangle_{\text{E}} + |0,m\rangle_{\text{B}} |G_{0,m}\rangle_{\text{E}}] + |0,0\rangle_{\text{B}} |H\rangle_{\text{E}} \tag{14}$$

with $|H\rangle_{\text{E}} = |F_{0,0}\rangle_{\text{E}} + |G_{0,0}\rangle_{\text{E}} + |H_{0,0}\rangle_{\text{E}}$. Following condition 1, the probability of Bob getting a photon in the $|-\rangle$ mode must be zero.

We now use the following lemma, the proof of which is given in Appendix B.

Lemma 1. If $|\psi'\rangle = \sum_{m>0}[|m,0\rangle_{\text{B}} |F_{m,0}\rangle_{\text{E}} + |0,m\rangle_{\text{B}} |G_{0,m}\rangle_{\text{E}}] + |0,0\rangle_{\text{B}} |H\rangle_{\text{E}}$ is a bipartite state in $\mathcal{H}_{\text{B}} \otimes \mathcal{H}_{\text{E}}$, and if there is a zero probability that Bob gets a photon in the $|-\rangle$ mode, then $|F_{1,0}\rangle_{\text{E}} = |G_{0,1}\rangle_{\text{E}}$, and $|F_{m,0}\rangle_{\text{E}} = |G_{0,m}\rangle_{\text{E}} = 0$ for all $m > 1$.

Applying Lemma 1, we deduce that $|F_{m,0}\rangle_{\text{E}} = |G_{0,m}\rangle_{\text{E}} = 0$ for all $m > 1$, and that $|F_{1,0}\rangle_{\text{E}} = |G_{0,1}\rangle_{\text{E}} \triangleq |F\rangle_{\text{E}}$.

It follows that the Bob+Eve states after Eve's attack, when Alice performed SWAP-x and her sum is zero (those are the only states for which Alice and Bob may share a bit), are

$$V|\psi^{(0)}_{\text{S-10}}\rangle = |0,1\rangle_{\text{B}} |F\rangle_{\text{E}} + |0,0\rangle_{\text{B}}[|G_{0,0}\rangle_{\text{E}} + |H_{0,0}\rangle_{\text{E}}], \tag{15}$$

$$V|\psi^{(0)}_{\text{S-01}}\rangle = |1,0\rangle_{\text{B}} |F\rangle_{\text{E}} + |0,0\rangle_{\text{B}}[|F_{0,0}\rangle_{\text{E}} + |H_{0,0}\rangle_{\text{E}}]. \tag{16}$$

Therefore, the state of Eve's probe is independent of all Alice's and Bob's shared bits, and is equal to $|F\rangle_{\text{E}}$ whenever Alice and Bob share a bit. Eve can thus get no information on the bits shared by Alice and Bob without being detected.

VI. CONCLUSION

We have presented a semiquantum key distribution protocol, and have proved it robust (security analysis is left for the future). Unlike all the previous SQKD protocols, our protocol can be experimentally implemented in a secure way.

In this paper, we have suggested a solution for a practical security problem of SQKD protocols, that was discussed in Sec. III and in [11]. We note that QKD protocols have, too, some security weaknesses in their practical implementations, such as the "photon-number splitting" attack [13], the "bright illumination" attack [14], the "fixed apparatus" attack [15], and other practical attacks. While some of those security weak-

nesses can be mitigated, full security proofs for practical implementations are still out of reach. A future extension of this paper may check to what extent the practical implementations of the SQKD protocols discussed in this paper suffer from the same practical security problems as common QKD protocols, and whether insights from SQKD protocols (and the methods described in this paper) may help in solving practical security problems of both SQKD and fully quantum QKD protocols.

ACKNOWLEDGMENTS

The work of T.M. and R.L. was partly supported by the Israeli Ministry of Defense (MOD) Research and Technology Unit, and by the Gerald Schwartz and Heather Reisman Foundation.

APPENDIX A: FOCK-SPACE NOTATIONS

The Fock-space notations, that serve as an extension of the qubit space, are defined as follows: the Fock basis vector $|0,1\rangle$ represents a single photon in the $|0\rangle$ state, and the Fock basis vector $|1,0\rangle$ represents a single photon in the $|1\rangle$ state. The vectors $|0,1\rangle$ and $|1,0\rangle$ could, for example, be two polarization modes, two arm modes (e.g., arms entering an interferometer), or two time-bin modes on a single arm. The qubit space (representing a single photon in one of the two modes) can be extended to the entire two-mode Fock space:

$$\mathcal{F} = \mathrm{Span}\{|m_1,m_0\rangle \mid m_1 \geqslant 0, m_0 \geqslant 0\}, \tag{A1}$$

where the state $|m_1,m_0\rangle$ represents m_1 indistinguishable photons in the mode of the qubit state $|1\rangle$ and m_0 indistinguishable photons in the mode of the qubit state $|0\rangle$. In particular, the state $|0,0\rangle \in \mathcal{F}$ is used for describing absence of photons in both modes (the "vacuum state").

Similarly, a single photon in the $|+\rangle$ mode may be written as $|0,1\rangle_{\mathrm{x}}$ (and similarly for $|-\rangle$ and $|1,0\rangle_{\mathrm{x}}$), and the entire two-mode Fock space can be represented as

$$\mathcal{F} = \mathrm{Span}\{|m_-,m_+\rangle_{\mathrm{x}} \mid m_- \geqslant 0, m_+ \geqslant 0\}, \tag{A2}$$

where the state $|m_-,m_+\rangle_{\mathrm{x}}$ represents m_- indistinguishable photons in the mode of the qubit state $|-\rangle$ and m_+ indistinguishable photons in the mode of the qubit state $|+\rangle$.

In this paper, we shorten the term "the mode of the qubit state $|0\rangle$" to "the $|0\rangle$ mode", and similarly for $|1\rangle$, $|+\rangle$, $|-\rangle$.

APPENDIX B: PROOF FOR LEMMA 1

Proof. If there is a zero probability that Bob gets a photon in the $|-\rangle$ mode, then there is a zero probability of measuring any basis state $|m_-,m_+\rangle_{\mathrm{x},B}$ of $\mathcal{H}_{\mathrm{B}}$ with $m_- > 0$.

For $m = 1$, since $|0,1\rangle_{\mathrm{B}} = \frac{|0,1\rangle_{\mathrm{x},B}+|1,0\rangle_{\mathrm{x},B}}{\sqrt{2}}$ and $|1,0\rangle_{\mathrm{B}} = \frac{|0,1\rangle_{\mathrm{x},B}-|1,0\rangle_{\mathrm{x},B}}{\sqrt{2}}$, we get

$$\begin{aligned} &|1,0\rangle_{\mathrm{B}}|F_{1,0}\rangle_{\mathrm{E}} + |0,1\rangle_{\mathrm{B}}|G_{0,1}\rangle_{\mathrm{E}} \\ &\quad = \frac{|0,1\rangle_{\mathrm{x,B}}}{\sqrt{2}}[|G_{0,1}\rangle_{\mathrm{E}} + |F_{1,0}\rangle_{\mathrm{E}}] \\ &\qquad + \frac{|1,0\rangle_{\mathrm{x,B}}}{\sqrt{2}}[|G_{0,1}\rangle_{\mathrm{E}} - |F_{1,0}\rangle_{\mathrm{E}}]. \end{aligned} \tag{B1}$$

Since the probability of getting a photon in the $|-\rangle$ mode must be zero, it is necessary that $|F_{1,0}\rangle_{\mathrm{E}} = |G_{0,1}\rangle_{\mathrm{E}}$.

For $m > 1$, using the ladder operators a_0, a_1, a_+, and a_-, since $a_0 = \frac{a_+ + a_-}{\sqrt{2}}$ and $a_1 = \frac{a_+ - a_-}{\sqrt{2}}$, we get

$$\begin{aligned} |0,m\rangle_{\mathrm{B}} &= \frac{a_0^{\dagger m}|0,0\rangle_{\mathrm{B}}}{\sqrt{m!}} \\ &= \frac{1}{\sqrt{2^m m!}}\sum_{k=0}^{m}\binom{m}{k}a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}, \end{aligned} \tag{B2}$$

$$\begin{aligned} |m,0\rangle_{\mathrm{B}} &= \frac{a_1^{\dagger m}|0,0\rangle_{\mathrm{B}}}{\sqrt{m!}} \\ &= \frac{1}{\sqrt{2^m m!}}\sum_{k=0}^{m}\binom{m}{k}(-1)^k a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}. \end{aligned} \tag{B3}$$

From Eqs. (B2) and (B3) it follows that

$$\begin{aligned} &|m,0\rangle_{\mathrm{B}}|F_{m,0}\rangle_{\mathrm{E}} + |0,m\rangle_{\mathrm{B}}|G_{0,m}\rangle_{\mathrm{E}} \\ &\quad = |e^{(m)}\rangle_{\mathrm{B}}[|G_{0,m}\rangle_{\mathrm{E}} + |F_{m,0}\rangle_{\mathrm{E}}] \\ &\qquad + |o^{(m)}\rangle_{\mathrm{B}}[|G_{0,m}\rangle_{\mathrm{E}} - |F_{m,0}\rangle_{\mathrm{E}}], \end{aligned} \tag{B4}$$

with

$$|e^{(m)}\rangle_{\mathrm{B}} = \frac{1}{\sqrt{2^m m!}}\sum_{k\ \mathrm{even}}\binom{m}{k}a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}, \tag{B5}$$

$$|o^{(m)}\rangle_{\mathrm{B}} = \frac{1}{\sqrt{2^m m!}}\sum_{k\ \mathrm{odd}}\binom{m}{k}a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}, \tag{B6}$$

where $a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}$ is, up to a constant factor, the Fock state $|k,m-k\rangle_{\mathrm{x},B}$. The probability of finding a photon in the $|-\rangle$ mode must be zero; thus, the coefficient of $a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}$ for $k > 0$ must be zero. Substituting $|e^{(m)}\rangle_{\mathrm{B}}$ and $|o^{(m)}\rangle_{\mathrm{B}}$ by their values in Eq. (B4), the coefficient of $a_-^{\dagger k}a_+^{\dagger m-k}|0,0\rangle_{\mathrm{B}}$ is (up to a nonzero constant factor) $|G_{0,m}\rangle_{\mathrm{E}} + |F_{m,0}\rangle_{\mathrm{E}}$ for even k and $|G_{0,m}\rangle_{\mathrm{E}} - |F_{m,0}\rangle_{\mathrm{E}}$ for odd k. Since $k = m > 0$ and $k' = m - 1 > 0$ have different parities, this implies both $|G_{0,m}\rangle_{\mathrm{E}} + |F_{m,0}\rangle_{\mathrm{E}} = 0$ and $|G_{0,m}\rangle_{\mathrm{E}} - |F_{m,0}\rangle_{\mathrm{E}} = 0$, and thus $|F_{m,0}\rangle_{\mathrm{E}} = |G_{0,m}\rangle_{\mathrm{E}} = 0$. ∎

[1] C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).
[3] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, Phys. Rev. A **79**, 032341 (2009).
[4] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, Phys. Rev. A **79**, 052312 (2009).
[5] M. Boyer and T. Mor, Phys. Rev. A **83**, 046301 (2011).
[6] H. Lu and Q.-Y. Cai, Int. J. Quantum. Inform. **06**, 1195 (2008).
[7] Z.-W. Sun, R.-G. Du, and D.-Y. Long, Int. J. Quantum. Inform. **11**, 1350005 (2013).

[8] K.-F. Yu, C.-W. Yang, C.-H. Liao, and T. Hwang, Quant. Info. Proc. **13**, 1457 (2014).
[9] W. O. Krawec, in *2015 IEEE International Symposium on Information Theory (ISIT)* (IEEE, New York, 2015), pp. 686–690.
[10] M. Boyer and T. Mor, arXiv:1012.2418 (2010).
[11] Y.-g. Tan, H. Lu, and Q.-y. Cai, Phys. Rev. Lett. **102**, 098901 (2009).
[12] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **102**, 098902 (2009).
[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[15] M. Boyer, R. Gelles, and T. Mor, Phys. Rev. A **90**, 012329 (2014).