Security of quantum key distribution with arbitrary individual imperfections

Øystein Marøy,* Lars Lydersen, and Johannes Skaar
Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway and University Graduate Center, NO-2027 Kjeller, Norway

(Received 23 March 2009; revised manuscript received 2 June 2010; published 30 September 2010)

We consider the security of the Bennett-Brassard 1984 protocol for quantum key distribution, with arbitrary individual imperfections simultaneously in the source and detectors. We provide the secure key generation rate and show that three parameters must be bounded to ensure security; the basis dependence of the source, a detector-blinding parameter, and a detector leakage parameter. The system may otherwise be completely uncharacterized and contain large losses.

DOI: 10.1103/PhysRevA.82.032337 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a method for distributing a secure key to two communicating parties, Alice and Bob. The most common QKD protocol, Bennett-Brassard 1984 (BB84) [1], has been proved secure by a number of approaches, some of which include different kinds of imperfections in the equipment [2–7]. The ultimate goal of QKD security analysis is to take all kinds of imperfections into account, at least those that cannot be eliminated completely by a suitable design of the setup. So far, most of the available security proofs for BB84 consider imperfections at the source or detector separately. An exception is the work by Gottesman *et al.* [5], which treats the security in the presence of source flaws and a squashing detector with certain limited imperfections. Also of interest is the article by Hayashi [8], which combines finite-length key analysis with photon number imperfections at the source. Proving security for a realistic system with arbitrary imperfections simultaneously in the source, channel, and detectors has so far been an open problem.

A particularly suitable approach for practical QKD is to limit the assumptions about the equipment. By considering entanglement-based protocols with detectors in both ends of the system [9], one can prove security in a rather general setting [10], assuming collective attacks and individual imperfections [11]. While these protocols and security proofs are promising, they do not necessarily provide security for realistic devices. All realistic systems have large losses due to the channel and limited detector efficiencies. An eavesdropper Eve may use imperfect detection efficiencies to effectively control Bob's basis choice [12,13]. Using this detection loophole, she may perform the identical measurement as Bob to obtain a perfect copy of the key.[1]

In this work we prove security for BB84 with any combination of individual imperfections, as well as channel losses. By individual imperfections we mean that the operation of the devices for a particular signal is independent of earlier signals. To obtain such generality, we describe the actual physics in the protocol rather than using, for example, squashing models with "tagging." Thus, the detectors are described as a basis-dependent quantum operation on the actual state space in front of a three-outcome measurement ("0", "1", and "vacuum"). Describing the detector in this way also enables an elegant solution to the problem of combining errors in the detectors and errors in the source.

To get around the detection loophole, we anticipate that at least two parameters must be known or bounded about the system; one for the source and one for the detectors. Our proof is formulated with two such parameters; the basis dependence of the source and a detector-blinding parameter. In addition to these parameters, we include a third parameter quantifying leakage from Bob's detectors. Once these parameters are bounded, the system may contain bit and basis leakage from Alice, multimode behavior, basis-dependent misalignments, losses, nonlinearities, basis-dependent threshold detectors with detector efficiency mismatch and information leakage, dark counts, etc. In that sense, our proof offers the generality of the entanglement-based scenarios [11], applies to realistic scenarios with loss, and provides universal composable security against the most general attacks.

II. PROTOCOL

Consider the following BB84-like protocol as the actual protocol. Alice chooses basis $a = Z$ or $a = X$ randomly according to some probability distribution and prepares the state $|\chi_a\rangle$, where

$$|\chi_Z\rangle = \sqrt{p_Z}|0\rangle|\beta_0\rangle + \sqrt{1-p_Z}|1\rangle|\beta_1\rangle, \tag{1a}$$

$$|\chi_X\rangle = \sqrt{p_X}|+\rangle|\beta_+\rangle + \sqrt{1-p_X}|-\rangle|\beta_-\rangle. \tag{1b}$$

Here p_Z and p_X are probabilities, $|0\rangle$,$|1\rangle$ are some orthonormal qubit basis states, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice measures the qubit in the a basis (this measurement can be delayed to the end of the protocol). She repeats the procedure to obtain a large number of "β states," which are sent via Eve to Bob. These β states include any system that is correlated to Alice's system and to which Eve has access. Note that Eve is free to send anything to Bob, including parts of β and/or any state of her own choice. Depending on Alice's source, the four different β states will differ in photon number statistics, polarization, wavelength, etc. Any

*oystein.maroy@iet.ntnu.no

[1]For any protocol, Bob's basis choice (or more generally, measurement setting) must be random and come from a trusted random-number generator; otherwise, Eve could perform the same measurement as Bob to obtain a perfect copy of his result.

leakage in nonphotonic side channels will also be included in these states. With no loss of generality, the β states are assumed to be pure; if they were mixed, we could simply purify them, sending the auxiliary, purifying system to Eve.

For each state received by Bob, he chooses a "basis" variable b according to some probability distribution and conducts measurements M_b. The measurements M_b have three outcomes: "0", "1", and "vacuum." When he obtains "0" or "1", he publicly acknowledges receipt. After transmission, Alice and Bob broadcast a and b. When $b = X$, they openly compare their measurement results to estimate the fraction q_X of nonvacuum events at Bob when $a = X$, the corresponding error rate δ_X, and the fraction q_{ph} of nonvacuum events when $a = Z$. After this estimation only the n states for which $a = b = Z$ are kept. Discarding all events where Bob detected "vacuum," Alice and Bob each end up with nq_Z bits. Alice's bits are the raw key.

We now summarize Koashi's generic framework for security proofs [14,15]. Imagine a virtual experiment where Alice measures her final nq_Z qubits (corresponding to the raw key) in the X basis instead of Z basis. In this virtual experiment, instead of measuring M_Z, Bob now tries to predict the outcome of Alice's measurement. To do this, he may do whatever is permitted by quantum mechanics, as long as he does not alter the information given to Eve. Let $H_{\text{virt}X}(A|B = \mu)$ denote the entropy of Alice's result, given measurement result μ in Bob's prediction. Let $H_{\text{virt}X}(A|B = \mu) \leqslant H$ for some constant H. Since the uncertainty after Bob's prediction is less than H, the entropic uncertainty relation [16] suggests that anyone (including Eve) cannot predict the outcome of a Z-basis measurement by Alice with less entropy than $nq_Z - H$. This indicates that Alice can extract $nq_Z - H$ bits of secret key. The quantity H is to be found from the estimated parameters q_X, δ_X, and q_{ph}.[2] The detailed proof [14] of the fact that Alice can extract $nq_Z - H$ bits of secret key is based upon the universal, composable security definition and considers the actual privacy amplification protocol by universal hashing.

To ensure that Bob has the identical key, we note that it does not matter to Eve what Bob does (as long as he gives the same receipt acknowledgment information); he can as well measure M_Z. Then Bob obtains the identical raw key from his measurement result and $nq_Z h(\delta_Z)$ extra bits of error correction information from Alice, consuming $nq_Z h(\delta_Z)$ of previous established secure key. Here $h(\cdot)$ is the binary Shannon entropy function, and the error rate δ_Z can be estimated by sacrificing a subset of the raw key (whose size we can neglect in the asymptotic limit $n \to \infty$). We therefore obtain the asymptotic net secure key generation rate

$$R_Z \geqslant 1 - H/nq_Z - h(\delta_Z). \tag{2}$$

[2]The Z-basis error rate δ_Z is not needed to ensure that Alice's key is secret; thus, there is no need to invoke the classicalization argument [17] regarding statistics of measurements involved in the simultaneous estimation of δ_X and δ_Z.

III. INDIVIDUAL IMPERFECTIONS IN THE DETECTORS

We first consider the situation where Alice's source is perfect ($|\chi_X\rangle = |\chi_Z\rangle$) and Bob's detectors can be subject to any kind of individual imperfections. With the understanding that Bob chooses his bit randomly for coincidence counts [3,5], his detectors can be modeled by a basis-dependent quantum operation ($\mathcal{E}_Z$ and $\mathcal{E}_X$) in front of a measurement with three possible outcomes: "0", "1", and "vacuum." Note that there is no need to require a squash model [5,18,19] in our proof as Bob's basis selector is included into the basis-dependent quantum operation.

In addition to the optical modes, there may also be other relevant degrees of freedom in the detector. For example, dark counts are caused by physical processes internally in the detector. Thus, we consider an extended state space consisting of the Fock space of all optical modes in addition to the state space associated with "electronic" degrees of freedom inside the detectors. Pessimistically, we let Eve control all degrees of freedom.

The quantum operations $\mathcal{E}_Z$ and $\mathcal{E}_X$ are decomposed as follows: First there is a basis-dependent quantum operation ($\mathcal{F}_Z$ and $\mathcal{F}_X$) acting on the Fock space associated with all optical modes. This operation contains Bob's basis selector. The operations $\mathcal{F}_Z$ and $\mathcal{F}_X$ are assumed to be passive in the sense that if vacuum is incident to all modes, there will also be vacuum at the output. Then there is another quantum operation $\mathcal{F}$ describing interaction between the photonic state and the internal degrees of freedom in the detectors (see Fig. 1). The quantum operation $\mathcal{F}$ may be active in the sense that even though vacuum is incident to all optical modes, there may be nonvacuum detections. When the optical modes contain the vacuum state, we can (pessimistically) assume that Eve has full control over Bob's detectors through $\mathcal{F}$; in other words, she controls the dark counts directly with the "electronic" modes. The quantum operation $\mathcal{F}$ is assumed to be independent of

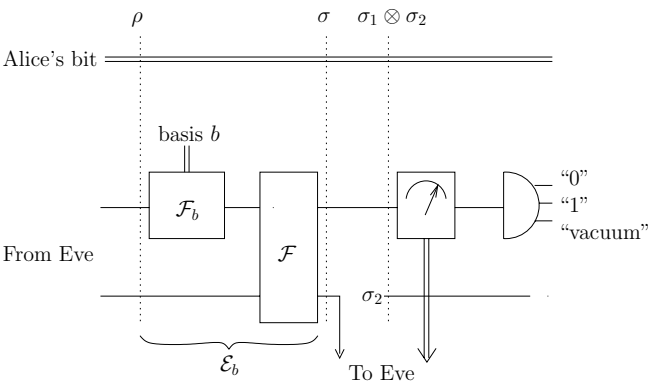

FIG. 1. Bob's detectors consist of a basis-dependent quantum operation ($\mathcal{E}_Z = \mathcal{F} \circ \mathcal{F}_Z$ and $\mathcal{E}_X = \mathcal{F} \circ \mathcal{F}_X$) in front of a three-outcome measurement. The fact that Eve gets arrival information from Bob is included through a dedicated vacuum measurement preceding Bob's three-outcome measurement. On the input side of $\mathcal{F}$, the lower line contains the electronic modes of the detector, while on the output side of $\mathcal{F}$, the lower line indicates the part of the Hilbert space leaked to Eve. Alice's classical bit, indicated in the upper part of the figure, is included in the state σ.

Bob's basis choice. This assumption is natural as Bob's basis choice does not influence internal degrees of freedom in the detector. In other words, when Eve emits the vacuum in all optical modes, Bob's basis choice will not affect the detection statistics.

To achieve a completely general detector model, we should not only let Eve control the detectors; in addition, we must let information return to Eve. Consider the case where Bob has chosen the Z basis. In the most general case, the information leakage is quantum; that is, a part of the total Hilbert space is given directly to Eve. Replacing this part of the Hilbert space with some standard state σ_2, we can quantify the leakage ϵ_Z by the trace distance $D(\cdot,\cdot)$ as follows:

$$\epsilon_Z = \min_{\sigma_2} \max_{\rho} D(\sigma, \sigma_1 \otimes \sigma_2). \tag{3}$$

Here ρ is any state at Bob's input (including Alice's part of the system; see Fig. 1), σ is the state of Alice and Bob before leakage, and $\sigma_1 = \mathrm{Tr}_2(\sigma)$ is the state of the remaining Hilbert space after leakage. Note that these density operators refer to a single signal, not the entire block of n signals. The parameter ϵ_Z measures the correlation between the leaked quantum state and the state of Alice and Bob, maximized over states sent by Eve. More precisely, ϵ_Z is the maximum probability that the actual state before leakage can be distinguished from the state where the leaked part is replaced by the standard state σ_2 [20]. Equation (3) has another very useful physical interpretation: Choose a fixed σ_2, dependent on $\mathcal{E}_Z$, but independent of the state coming from Eve. For any σ, the probability of a measurement result of $\sigma_1 \otimes \sigma_2$ deviates no more than ϵ_Z from the corresponding probability when measuring σ [20].

Although we now have a general detector model, we add one little feature. In the actual protocol, Eve gets to know whether a particular signal was detected. This can be included as an extra projective measurement with projectors P and $I - P$, where $I - P$ is a projector onto the subspace corresponding to detection result "vacuum" in Bob's measurement. Clearly, this addition does not disturb Bob's measurement statistics. The composed measurement consisting of $\mathcal{E}_Z$ followed by this projective measurement will be referred to as Eve's vacuum measurement. It can be described by some positive operator-valued measure (POVM) elements E and $I - E$, where $I - E$ corresponds to detection result "vacuum" at Bob. Including Eve's vacuum measurement separately, rather than absorbing it into the quantum leakage (3), leads to a better rate. The reason is that the information from the vacuum measurement is classical and available to Bob, as opposed to general, leaked quantum information.

Having described the model, we now turn to the security analysis. As before, Alice extracts the key in the Z basis. In Koashi's security proof, Bob wants to predict the outcome of a virtual X-basis measurement by Alice. In this virtual prediction there is only one important restriction: Bob is not allowed to alter the information going to Eve. Thus, Eve's vacuum measurement must be retained.

The setup used by Bob to perform the virtual X-basis prediction is depicted in Fig. 2. The state from Eve is incident to a first vacuum measurement, Bob's vacuum measurement,

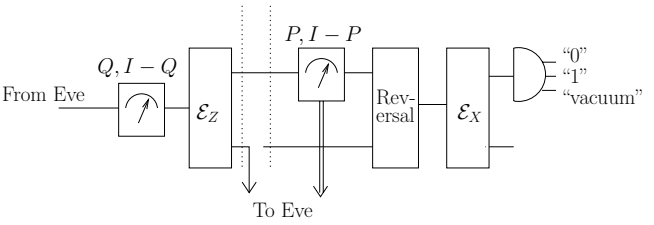

FIG. 2. Bob's setup for virtual X-basis prediction. The optical and electronic modes are denoted by a single line in this figure.

a projective measurement with certain projectors Q and $I - Q$, corresponding to results "nonvacuum" and "vacuum," respectively. Then it goes through the quantum operation $\mathcal{E}_Z$ and leaks partially back to Eve. The remaining part is measured by Eve's vacuum measurement and sent through a reversal operation. The goal of the reversal operation is to reverse the effect of the vacuum measurement so that the combined operation consisting of Eve's vacuum measurement and the reversal operation is identity, with a certain probability. Finally, the quantum operation $\mathcal{E}_X$ and Bob's three-outcome measurement are applied.

To analyze Bob's virtual prediction, we note the following observations. The quantum operation $\mathcal{E}_Z$ can be viewed as a unitary operation on an extended state space. Moreover, since Bob's reversal operation does not have to be realizable in practice (only in principle), we may assume that Bob has access to any extra degrees of freedom used to "unitarize" $\mathcal{E}_Z$. He does not have access to the quantum state leaked to Eve; however, the leakage disturbs the probabilities of Bob's prediction by no more than ϵ_Z. Therefore, for the moment we can ignore the leakage, taking it into account in the final expression for the key rate.

To proceed, we need the following results.

Lemma 1 (Koashi and Ueda [21]). Let E, acting on a Hilbert space $\mathcal{H}$, be a POVM element associated with some measurement M. If any state in some subspace $\mathcal{Q} \subseteq \mathcal{H}$ is measured with M, the measured state can be reversed to the original state, with maximum joint probability of outcome E and successful reversal $\inf_{|\Phi\rangle \in \mathcal{Q}, \langle \Phi|\Phi\rangle = 1} \langle \Phi|E|\Phi\rangle$. It is possible to know when the reversal is successful or not.

Lemma 2. The output of a quantum operation $\mathcal{E}_b$ is measured with projectors P_0, P_1, and $I - P_0 - P_1$, corresponding to detection results "0", "1", and "vacuum," respectively, or alternatively, with $P \equiv P_0 + P_1$ and $I - P$. Let $I - Q$ be a projector onto an input subspace of $\mathcal{E}_b$ that leads to detection result "vacuum" with certainty. The measurement statistics are not changed by the presence of a projective measurement $\{Q, I - Q\}$ before $\mathcal{E}_b$.

Proof. Lemma 2 is not as trivial as it may appear at first sight since states in the support of Q may also lead to detection result "vacuum." Thus, the measurement before $\mathcal{E}_b$ gives extra information. Nevertheless, the quantum operation $\mathcal{E}_b$ can be viewed as a unitary transformation on an extended Hilbert space, with a standard state as auxiliary input. Clearly, it does not matter if we measure the extra degrees of freedom at the output. This measurement can be constructed so that the total output measurement distinguishes between input states in the support

of Q or $I-Q$. Then, an input measurement $\{Q, I-Q\}$ is redundant.

More precisely, the unitary operator can be chosen such that the projective measurement at the output is implemented as a measurement of a single qutrit in the computational basis. Thus, it transforms

$$|0_1\rangle|0\rangle_{\text{aux}} \to |v\rangle|\psi_1\rangle, \tag{4a}$$

$$|0_2\rangle|0\rangle_{\text{aux}} \to |v\rangle|\psi_2\rangle, \tag{4b}$$

and

$$|1_1\rangle|0\rangle_{\text{aux}} \to |v\rangle|\phi_1^v\rangle + |0\rangle|\phi_1^0\rangle + |1\rangle|\phi_1^1\rangle, \tag{5a}$$

$$|1_2\rangle|0\rangle_{\text{aux}} \to |v\rangle|\phi_2^v\rangle + |0\rangle|\phi_2^0\rangle + |1\rangle|\phi_2^1\rangle, \tag{5b}$$

etc. Here $|0_i\rangle$ and $|1_i\rangle$ are bases for the support of $I-Q$ and Q, respectively; $|0\rangle_{\text{aux}}$ is the auxiliary standard state; and $|0\rangle\langle 0| = P_0$, $|1\rangle\langle 1| = P_1$, and $|v\rangle\langle v| = I - P_0 - P_1$. The ψ and ϕ vectors are (not necessarily normalized) states of the remaining part of the output state space. Since $\langle 1_i|0_j\rangle = 0$, we have $\langle\phi_i^v|\psi_j\rangle = 0$ for any i, j. Thus, by a measurement of the ψ or ϕ part of the output state space in addition to the qutrit, we can distinguish between the $|0_i\rangle$ states and $|1_i\rangle$ states. ■

We define the projector $I-Q$ so as to project onto vacuum in all photonic modes and onto the biggest subspace of the "electronic" modes that gives detection result "vacuum" in Eve's vacuum measurement. The orthogonal subspace, which is the support of Q, is denoted $\mathcal{Q}$. Lemma 2 ensures that Bob's vacuum measurement does not change the statistics of Eve's vacuum measurement. When Eve's vacuum measurement gives result "vacuum," or the reversal operation is not successful, the reversal operation is assumed to output a state in the support of $I-Q$. Thus, in these cases the output of Bob's virtual prediction is "vacuum" with certainty.

If the outcome of Bob's vacuum measurement is "vacuum," the outcome of Eve's vacuum measurement is "vacuum," and the reversal operation is successful with certainty. Suppose the outcome of Bob's vacuum measurement is "nonvacuum." According to Lemma 1, the maximum joint probability of result E in Eve's vacuum measurement and successful reversal is $\eta_Z = \inf_{|\Phi\rangle\in\mathcal{Q},\langle\Phi|\Phi\rangle=1}\langle\Phi|E|\Phi\rangle$. When result E and the reversal is successful (and Bob knows when it is), the statistics of Bob's measurement compared to Alice's virtual X-basis measurement will be identical to that of Alice's and Bob's ordinary parameter estimation in the X basis, except for any disturbance by Bob's vacuum measurement. According to Lemma 2 such disturbance does not exist. The number of detection events E in Eve's vacuum measurement is nq_Z; of these $nq_X\eta_Z$ is successfully reversed *and* detected as "0" or "1" in Bob's virtual prediction. Thus, we obtain $H \leqslant (nq_Z - nq_X\eta_Z) + nq_X\eta_Z h(\delta_X)$, which gives us the rate

$$R_Z \geqslant \eta_Z q_X/q_Z[1-h(\delta_X)] - h(\delta_Z). \tag{6}$$

The parameter $\eta_Z = \inf_{|\Phi\rangle\in\mathcal{Q},\langle\Phi|\Phi\rangle=1}\langle\Phi|E|\Phi\rangle$ is the minimum probability that a state in $\mathcal{Q}$ gives result E by Eve. This parameter has a clear physical interpretation. When vacuum is incident to the optical modes, recall that with no loss of generality we may assume that Eve has full control of the detectors through the "electronic" modes. Then there are no losses of her excitation in the "electronic" modes through the quantum operation $\mathcal{F}$. Thus, we identify η_Z as the minimum probability that a nonvacuum photonic state is detected by Bob. In other words, $1-\eta_Z$ is the maximum probability that a nonvacuum photonic state is absorbed in the detectors and detected as vacuum in the actual setup (Fig. 1).

So far we have ignored the effect of any quantum leakage from the detectors. Parametrizing the leakage by (3), ϵ_Z quantifies the maximum deviation of any measurement probabilities. In the absence of leakage, the probabilities of correct and incorrect predictions are $q_X\eta_Z(1-\delta_X)$ and $q_X\eta_Z\delta_X$, respectively, while the probability of vacuum result is $1-q_X\eta_Z$. When there is leakage, in the worst case these probabilities are changed to $q_X\eta_Z(1-\delta_X)-\epsilon_Z$, $q_X\eta_Z\delta_X+\epsilon_Z-\xi$, and $1-q_X\eta_Z+\xi$, respectively. Here ξ is an unknown parameter satisfying $0\leqslant\xi\leqslant\epsilon_Z$. Of the nq_Z nonvacuum results in Eve's vacuum measurement, there are $n(q_X\eta_Z-\xi)$ nonvacuum results in Bob's virtual prediction. This leads to

$$\begin{aligned} H &\leqslant nq_Z - n(q_X\eta_Z-\xi) \\ &\quad + n(q_X\eta_Z-\xi)h\left(\frac{q_X\eta_Z\delta_X+\epsilon_Z-\xi}{q_X\eta_Z-\xi}\right) \\ &\leqslant nq_Z - nq_X\eta_Z + nq_X\eta_Z h\left(\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\right). \end{aligned} \tag{7}$$

The last inequality in (7) can be found after some algebra using the facts that $h(u)-h(u-\Delta)\geqslant h'(u)\Delta$ for $\Delta\geqslant 0$ and $u\leqslant 1/2$, and $h'(u)(1-u)\geqslant 1$ for $u\leqslant 0.277$. Here we have set $u=\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}$.

This gives the rate

$$R_Z \geqslant \eta_Z\frac{q_X}{q_Z}\left[1-h\left(\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\right)\right] - h(\delta_Z) \tag{8}$$

for $\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\leqslant 0.277$. An expression for the rate, also valid for $0.277\leqslant\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\leqslant 0.5$, can be derived straightforwardly; however, this regime is only relevant for very small δ_Z and large δ_X and/or $\frac{\epsilon_Z}{q_X\eta_Z}$.

IV. INDIVIDUAL IMPERFECTIONS IN THE ENTIRE SYSTEM

From the previous section we note that when the reversal operation is successful (and Bob knows when it is), the measurement statistics in the prediction becomes identical to the statistics if Bob measured in the X basis. This makes it possible to consider simultaneous imperfections at the source and detector. We may then consider the case where Alice creates a general state ρ_a depending on the basis choice a. The basis dependence of the source is characterized by the fidelity $F(\rho_Z,\rho_X)\equiv\text{Tr}(\sqrt{\rho_Z}\rho_X\sqrt{\rho_Z})^{\frac{1}{2}}$. We let this dependence be bounded by a parameter Δ defined by $F\geqslant 1-2\Delta$. By Uhlmann's theorem there exist purifications, $|\chi_a\rangle$ of ρ_a, such that $\langle\chi_Z\mid\chi_X\rangle = 1-2\Delta$. We note that $|\chi_a\rangle$ can be expressed as in Eq. (1).

Again, we first ignore the detector leakage, taking it into account in the final expression for the rate. Since Bob wants to predict Alice's virtual X-basis measurement on $|\chi_Z\rangle$, the error rate δ_X and the transmission rate q_X in (6) must be replaced with δ_{ph} and q_{ph}, respectively. Here δ_{ph} is the error

rate when Alice measures her part of $|\chi_Z\rangle$ in the X basis and Bob measures his part using M_X.

In BB84 such a measurement is not actually performed, but $\delta_{\rm ph}$ can be bounded from the measured error and transmission rates. We expand the statistical argument from [14] to include "vacuum" as a possible measurement result. Assume that for the systems used in the random sampling Alice chooses her basis by measuring a quantum coin in the Z basis. Then these systems can be described by state $|\Psi\rangle = (|\chi_Z\rangle|0\rangle + |\chi_X\rangle|1\rangle)/\sqrt{2}$, with the last system being that of the quantum coin.

We then consider the situations where Alice and Bob both conduct X-basis measurements. For each measurement a variable t is assigned the value $t = 0$ if their results are the same, $t = 1$ if there is an error, and $t = 2$ if Bob gets no result. Alice then measures her quantum coin in the Z basis, getting the result c. We obtain the following conditional probabilities.

$$p(t = 0|c = 1) = q_X(1 - \delta_X), \tag{9a}$$
$$p(t = 0|c = 0) = q_{\rm ph}(1 - \delta_{\rm ph}), \tag{9b}$$
$$p(t = 1|c = 1) = q_X\delta_X, \tag{9c}$$
$$p(t = 1|c = 0) = q_{\rm ph}\delta_{\rm ph}, \tag{9d}$$
$$p(t = 2|c = 1) = 1 - q_X, \tag{9e}$$
$$p(t = 2|c = 0) = 1 - q_{\rm ph}. \tag{9f}$$

Assuming that the systems used to estimate error and transmission rates are randomly chosen, the probabilities given $c = 0$ are also valid for the systems used to extract the raw key.

Now assume that for some states Alice measures the coin in the X basis, getting measurement result $\bar{c}$. Note that

$$\sum_j p(t = j)p(\bar{c} = 1|t = j) = \Delta. \tag{10}$$

Using (9), (10), and the bound [22],

$$[1 - 2p(\bar{c} = 1|t = j)]^2 + [1 - 2p(c = 0|t = j)]^2 \leqslant 1,$$

we find

$$\begin{aligned} 1 - 2\Delta &\leqslant \sum_j \sqrt{p(t = j|a = Z)p(t = j|a = X)} \\ &= \sqrt{q_X(1 - \delta_X)q_{\rm ph}(1 - \delta_{\rm ph})} + \sqrt{q_X\delta_X q_{\rm ph}\delta_{\rm ph}} \\ &\quad + \sqrt{(1 - q_X)(1 - q_{\rm ph})}. \end{aligned} \tag{11}$$

$\delta_{\rm ph}$ can now be taken to be the maximal value for which the inequality is obeyed.

Similarly to the analysis in the previous section, we can include detector leakage by modifying the detection probabilities. As in (8), the leakage is accounted for by adding a term proportional to the leakage parameter ϵ_Z,

$$\tilde{\delta}_{\rm ph} \leqslant \delta_{\rm ph} + \frac{\epsilon_Z}{q_{\rm ph}\eta_Z}. \tag{12}$$

We have arrived at our main result.

Theorem 1. In BB84 the basis dependence of Alice's source is bounded by $F(\rho_X, \rho_Z) \geqslant 1 - 2\Delta$. Bob's detectors are modeled by a passive, basis-dependent quantum operation ($\mathcal{F}_Z$ and $\mathcal{F}_X$) acting on the multimode photonic state, followed by a basis-independent quantum operation ($\mathcal{F}$) describing interaction with internal degrees of freedom in the physical detector, followed by a measurement with three outcomes: "0", "1", and "vacuum." Suppose Eve controls the photonic modes and the internal degrees of freedom in the detectors and that a quantum state leaks back to Eve from the detectors. Then the asymptotic secure key generation rate for key extraction in the Z basis satisfies

$$R_Z \geqslant \eta_Z q_{\rm ph}/q_Z[1 - h(\tilde{\delta}_{\rm ph})] - h(\delta_Z), \tag{13}$$

provided $\tilde{\delta}_{\rm ph} \leqslant 0.277$. Here δ_Z is the estimated error rate in the Z basis, $\tilde{\delta}_{\rm ph}$ is given by (11) and (12), $1 - \eta_Z$ is the maximum probability that a nonvacuum photonic state is detected as "vacuum," and $q_{\rm ph}/q_Z$ is the ratio between the transmission rates for Bobs measurements M_X and M_Z given that Alice sends in the Z basis.

The rate (13) is valid for any kind of individual imperfection and loss. The parameters q_X, q_Z, $q_{\rm ph}$, δ_X, and δ_Z are estimated directly in the protocol, while Δ, η_Z, and ϵ_Z characterize the practical setup.

V. DISCUSSION OF RESULTS

In this discussion we assume that the quantum channel is symmetric with respect to loss; that is, $q_X = q_{\rm ph} = q_Z \equiv q$. This will be approximately true for most setups. We also assume no information returned to Eve from the detectors, $\epsilon_Z = 0$, anticipating that such errors could be avoided by modifying the setup.

In this case (11) reduces to

$$\frac{2\Delta}{q} \geqslant 1 - \sqrt{(1 - \delta_X)(1 - \delta_{\rm ph})} - \sqrt{\delta_X\delta_{\rm ph}} \tag{14}$$

and the estimated worst possible error rate is

$$\begin{aligned} \delta_{\rm ph} = \min\Bigg\{\frac{1}{2}\,,\ \delta_X + 8\frac{\Delta}{q}\Bigg[\left(1 - \frac{\Delta}{q}\right)(1 - 2\delta_X) \\ + \sqrt{\frac{\Delta}{q}\left(1 - \frac{\Delta}{q}\right)\delta_X(1 - \delta_X)}\Bigg]\Bigg\}. \end{aligned} \tag{15}$$

We see that errors in the source are more critical when the transmission is low. In fact, both the basis dependence of the source, Δ, and transmission rate, q, only appears in the equation in the form $\frac{\Delta}{q}$. If the source is perfect, $\Delta = 0$, loss in the channel does not affect the secret key rate. This relationship between the source error and the transmission rates is due to Eve's control of the channel, which let her pass to Bob only the systems where her operation has given her the most information for the least disturbance. The upper limit on the source error for which key gain is possible is $\frac{\Delta}{q} \leqslant \frac{\sqrt{2}-1}{2\sqrt{2}} \approx 0.146$. This is independent of the blinding parameter η_Z, as long as it is nonzero, but demands error rates equal to zero. For larger error rates the limit depends heavily on η_Z (Fig. 3).

Channel loss and imperfect sources only contributes to an increase in $\delta_{\rm ph}$. A better estimate of $\delta_{\rm ph}$ would increase the rate. This is related to the method of decoy states [23–25], where Alice instead of producing ρ_Z, sometimes produces a decoy state with a different mean photon number. From the

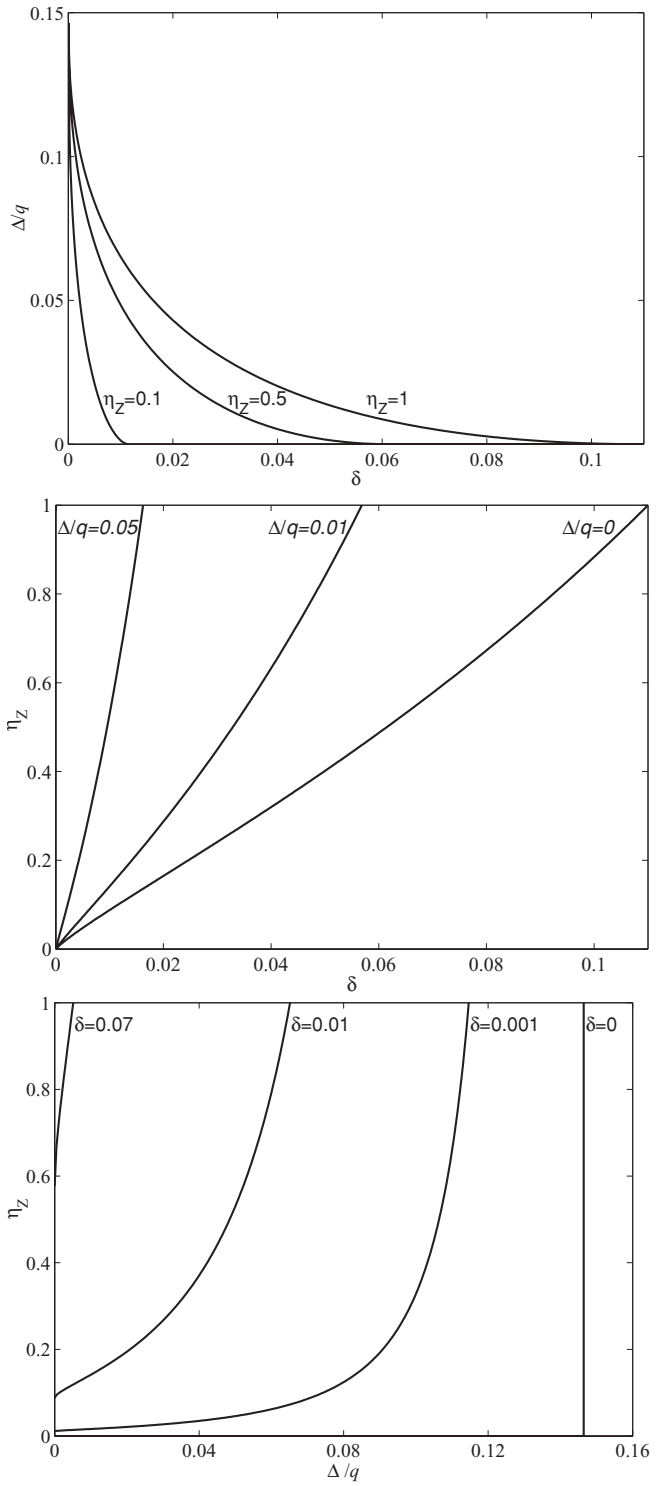

FIG. 3. Plots showing the security bounds $R_Z = 0$ for different values of the blinding parameter η_Z, the basis dependence of the source Δ, and the error and transmission rates δ and q. The security bound is found by setting $R_Z = 0$ in (13). Positive key gain is possible for parameter values to the left of the curves. We have assumed $\epsilon_Z = 0$, $\delta_X = \delta_Z = \delta$, and $q_X = q_{\text{ph}} = q_Z = q$.

transmission and error rates for this state, Alice and Bob are able to derive a stricter bound on δ_{ph}, effectively reducing R_Z's dependence of channel loss. To generalize this method, using decoy states where other properties of the signal state are varied might prove useful when operating with an imperfect source. However, creating such states may require the detailed output statistics of the source and might be experimentally difficult in general.

Considering the special case of a perfect source, our rate is larger than the rate proved for restricted detector flaws in previous literature [6,7]. Key gain is possible for $\eta_Z \leqslant \frac{h(\delta_Z)}{1-h(\delta_X)}$. Unlike previous results, our rate applies to all relevant, individual imperfections at the detectors, for example, mode coupling including misalignments and multiple reflections, nonlinearities, mode-dependent losses and detector efficiency mismatch, and any basis dependence of those effects. Moreover, it applies to threshold detectors with dark counts.

Note that the detector-blinding parameter η_Z is not supposed to contain the transmission efficiency of the channel. Generally, one should factorize $\mathcal{E}_Z = \tilde{\mathcal{E}}_Z \circ \mathcal{E}$ and $\mathcal{E}_X = \tilde{\mathcal{E}}_X \circ \mathcal{E}$ to put as much as possible of the imperfections into the basis-independent operation $\mathcal{E}$. By absorbing $\mathcal{E}$ into Eve and treating $\tilde{\mathcal{E}}_Z$ and $\tilde{\mathcal{E}}_X$ as the new imperfections, η_Z will be maximal. For example, for the case where reduced detector efficiencies can be described as beam splitters in front of ideal detectors, and if there is no coupling between modes associated with different logical bits, η_Z is the minimum ratio between the two detection efficiencies [7]. For detectors that cannot be modeled by beam splitters in front of ideal detectors, our security proof clearly shows the danger associated with the possibility of detector blinding [13]: If the detection probability of a nonvacuum state is zero, our proof predicts zero key rate. For the case where the detectors can only be partially blinded, our proof can predict positive rate.

Returning to the general case, the rate (13) is dependent on Δ, η_Z, and ϵ_Z, in addition to estimated parameters. For a specific QKD setup, Δ and ϵ_Z must be upper bounded, and η_Z must be lower bounded. How to deal with this in practice is an interesting question for future research.

VI. CONCLUSION

We have proved security for arbitrary, individual imperfections in a BB84 system. The detector model includes a basis-dependent quantum operation, possibly with quantum leakage back to Eve, followed by a three-outcome measurement with outcomes "0", "1", and "vacuum." Such a general detector model can describe detector efficiency mismatch, nonlinear blindable behavior, response to multiple modes, mode coupling and multiple reflections, misalignments, back-reflection leakage, nonoptical leakage, etc. By reversing the measurement which gives Eve information about whether a particular signal was detected (Eve's vacuum measurement), we show how to treat the general case with a lossy channel and general, individual imperfections at the source, combined with the flawed detector. The final rate is dependent on three parameters which describe the equipment, in addition to error and transmission rates. These parameters are the basis dependence of the source and a blinding parameter and a leakage parameter characterizing the detector.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984), p. 175.
[2] D. Mayers, in *Proceedings of Crypto '96*, edited by N. Koblitz (Springer, New York, 1996), Vol. 1109, p. 343.
[3] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[4] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[6] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).
[7] L. Lydersen and J. Skaar, Quantum Inf. Comput. **10**, 60 (2010).
[8] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[9] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[10] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[12] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).
[13] V. Makarov, New J. Phys. **11**, 065003 (2009).
[14] M. Koashi, New J. Phys. **11**, 045018 (2009); e-print quant-ph/0505108v1.
[15] M. Koashi, e-print quant-ph/0609180.
[16] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[17] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[18] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
[19] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[21] M. Koashi and M. Ueda, Phys. Rev. Lett. **82**, 2598 (1999).
[22] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[23] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[24] H.-K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[25] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).