

Suitability versus fidelity for rating single-photon guns

George M. Hockney, Pieter Kok, and Jonathan P. Dowling

*Quantum Computing Technologies Group, Section 367, Jet Propulsion Laboratory, California Institute of Technology
Mail Stop 126-347, 4800 Oak Grove Drive, Pasadena, California 91109*

(Version: June 17, 2002)

The creation of known quantum states is important for most, if not all, applications in quantum computation and communication. The quality of the state preparation is therefore an essential ingredient in any assessment of a quantum-state gun. We show that the fidelity, under the standard definitions is not sufficient to assess quantum sources, and we propose a new measure of suitability that necessarily depends on the application for the source. We consider the performance of single-photon guns in the context of quantum key distribution (QKD) and interferometric quantum computation. Single-photon sources for QKD need radically different properties than sources for quantum computing. Furthermore, the suitability for single-photon guns is discussed explicitly in terms of experimentally accessible criteria.

PACS numbers: 03.67.-a, 03.65.Wj, 03.67.Dd, 03.67.Hk

One of the requirements for quantum computation and communication is the ability to faithfully produce certain input states [1]. For quantum computers in general, this means that we have to be able to initialize the registers in some $|0\rangle$ state. Quantum communication involves the transmission of quantum states, and the quality of the state preparation determines in part the success of the communication.

Optical implementations of quantum communication and computation such as cryptography, teleportation, optical quantum computers, interferometric quantum non-demolition measurements, and many other applications often rely on good single-photon sources [2]. There are many proposals for single-photon guns, ranging from semiconductor quantum dots and the manipulation of individual molecules to parametric down-conversion [3], but the suitability of these sources has not yet been sufficiently addressed. Whereas attenuated coherent states might be a good approximation to a single-photon state for some applications, its two-photon contribution renders it unsuitable for cryptography [4]. Any measure of suitability therefore has to take the intended purpose of the state into account.

One possible choice for the suitability of a source would be the fidelity f_{AB} of the input state ρ_A with respect to the desired state ρ_B : $f_{AB} \equiv \{\text{Tr}[(\sqrt{\rho_A} \rho_B \sqrt{\rho_A})^{1/2}]\}^2$ [5]. This fidelity satisfies $0 \leq f_{AB} \leq 1$, and most importantly, $f_{AB} = 1 \Leftrightarrow \rho_A = \rho_B$. When one of the systems is in a pure state $|\psi\rangle$ and the other system is in a mixed state ρ , this measure reduces to $\text{Tr}(\rho|\psi\rangle\langle\psi|)$. However, f_{AB} is generally *not* a good measure for the suitability of a state preparation device (such as a single-photon gun) given a specific application. The reason is that several different input states may be equally suitable for a specific application. When two distinct states ρ_X and ρ_Y are both useful states for a specific application, a state ρ_A might have a large f_{XA} , but a small f_{YA} . Similarly, a state ρ_B might have a small f_{XB} , but a large f_{YB} . Both ρ_A

and ρ_B are suitable for the application, but the fidelity acknowledges only one of them.

In this paper we propose a general definition for the suitability S_{GT} of a source gun G given a target application T . The suitability satisfies $0 \leq S_{GT} \leq 1$, and is a good measure of how well a candidate gun will work in a given target application. We will first give an example where the fidelity breaks down as a performance measure of the single-photon gun, and subsequently we define the general suitability S_{GT} . We then use this formalism to describe single-photon guns in quantum key distribution (QKD) and demonstrate how a source highly suitable for QKD is not at all suitable for quantum teleportation.

To understand why conventional definitions of the fidelity are problematic, consider the QKD protocol associated with the 1984 cryptographic scheme by Bennett and Brassard [6]. In this application, Alice chooses a random string from a set of four pair-wise orthogonal polarization states $\mathcal{S} = \{|H\rangle, |V\rangle, |L\rangle, |R\rangle\}$. She then prepares and sends these states to Bob. In order to ensure security, it is important that the states only contain a single photon [4]. However, it is *not* important that the state's frequency or exact timing within a window is controlled (as long as this is not correlated with the polarization). Pure states with some spread in time and frequency are as suitable for key distribution as a mixed state, provided the polarization is definite and the state contains exactly one photon.

Suppose for simplicity that the unknown and unimportant part of the state can be in only three (pure) states $|A\rangle$, $|B\rangle$, or $|C\rangle$. When Alice wishes to send the state $|\psi\rangle \in \mathcal{S}$ to Bob, it does not matter whether the state she produces is actually $|\psi\rangle \otimes |A\rangle$, $|\psi\rangle \otimes |B\rangle$, $|\psi\rangle \otimes |C\rangle$ or a combination of these. Although one could require Alice to create the state $|\psi\rangle \otimes |A\rangle$, this is overly restrictive. In a real system this would be equivalent to requiring the input gun to have no time jitter or any other irrelevant mixing. It only matters that $|\psi\rangle$ is the correct polar-

ization and has only one photon. When we define Alice's target state as $\rho_T = \frac{1}{3}|\psi, A\rangle\langle\psi, A| + \frac{1}{3}|\psi, B\rangle\langle\psi, B| + \frac{1}{3}|\psi, C\rangle\langle\psi, C|$, $\text{Tr}(\rho_G \rho_T)$ is always smaller than $1/3$ and yields different values for equally useful input states. Using instead the fidelity $f_{AB} = \{\text{Tr}[(\sqrt{\rho_A} \rho_B \sqrt{\rho_A})^{1/2}]\}^2$ also fails, since fidelity is a only measure of how much two states are alike. f_{AB} is unity only if the input state is exactly ρ_T , but any of several other states are equally suitable.

The solution is to define a procedure for writing a target state ρ_T , a gun state ρ_G , and an expression $S(\rho_T, \rho_G)$ that has the desired property of being close to one if and only if the gun is suitable for the target. We define ρ_G as the state that is produced by the gun and ρ_T as the target state. That is, first determine the set of states that are equally suitable. Then we select a complete set of N suitable states $|\phi_i\rangle$ and define the target density matrix as $\rho_T \equiv N^{-1} \sum_i |\phi_i\rangle\langle\phi_i|$. In the above example, this leads to Alice's target state $\rho_T = \frac{1}{3}|\psi, A\rangle\langle\psi, A| + \frac{1}{3}|\psi, B\rangle\langle\psi, B| + \frac{1}{3}|\psi, C\rangle\langle\psi, C|$. To define the suitability of a quantum source, let $F_{AB} \equiv \text{Tr}(\rho_A \rho_B)$ for any two normalized density matrices ρ_A and ρ_B . Given two mixtures we have $F_{AB} \leq F_{AA}$. Note that F_{AB} is not a proper definition of fidelity, since $F_{AA} \neq 1$. F_{AA} is a measure for the mixedness of ρ_A .

We propose the following definition for the suitability S of a gun that purports to create a particular quantum state:

$$S_{GT} \equiv \frac{F_{GT}}{F_{TT}}, \quad (1)$$

where ρ_G is the output state of the gun and ρ_T is a mixture of all possible target states associated with a particular application. If there is one and only one pure target state, $F_{TT} = 1$ and $S_{GT} = f_{GT}$. This definition for S yields one for any input state that completely overlaps the requirement. This may be explicitly worked out for the three states mentioned in the QKD example above: $F_{TT} = \frac{1}{3}$ and $S_{GT} = 1$.

The triangle inequality on F leads to an important inequality on S_{GT} , namely

$$S_{GT} = \frac{F_{GT}}{F_{TT}} \leq \frac{F_{GG}}{F_{TT}}. \quad (2)$$

Since F_{GG} is only determined by the gun, this leads to an important measure of the quality of the gun. If the target application requires interference between the input state from the gun and an existing state in the system, then target state must be a pure state. That is, the input state must overlap the pre-existing state. However, for any pure state $F_{TT} = 1$ and S_{GT} reduces to F_{GT} , which must be less than F_{GG} . Therefore F_{GG} directly limits the suitability of a candidate gun for this class of targets.

So far, the formalism has been completely general, and we will now consider the important special case of single-photon guns. Naively, an ideal single-photon gun is a

device that emits one and only one photon with a particular frequency in a given spatial mode when triggered to do so. Such a device does not exist. According to Heisenberg's uncertainty relation in energy and time, it is not possible to fix both the photon number and the triggering time with infinite precision. This means that we have to admit a continuum of frequency modes if we keep the photon number fixed. The difficulties involving ideal single-photon guns are closely related to the fact that single photons do not have a well-defined wave function [7]. We therefore have to be careful when we define the single-photon states that are produced by the guns. In particular, the desired states differ from application to application.

For single-photon guns, we can modify F_{AB} such that we obtain $F_{AB}^{(1)} \equiv \text{Tr}(\rho_A |1\rangle\langle 1| \rho_B)$, where $|1\rangle\langle 1| \equiv \int d\vec{k} d\omega \hat{a}_{\vec{k}}^\dagger(\omega) |0\rangle\langle 0| \hat{a}_{\vec{k}}(\omega)$. Here, $\hat{a}_{\vec{k}}^\dagger(\omega)$ and $\hat{a}_{\vec{k}}(\omega)$ are the creation and annihilation operators satisfying $[\hat{a}_{\vec{k}}(\omega), \hat{a}_{\vec{k}'}^\dagger(\omega')] = \delta(\vec{k} - \vec{k}') \delta(\omega - \omega')$. Obviously, we have $F_{AB}^{(1)} \leq F_{AB}$. This does not change F_{GT} or F_{TT} , since ρ_T is already confined to the $|1\rangle\langle 1|$ subspace. However, $F_{GG}^{(1)}$ gives a better measure for the performance of single-photon guns than F_{GG} , since $F_{GG}^{(1)} \leq F_{GG}$, and therefore $S_{GT} \leq F_{GG}^{(1)}/F_{TT}$.

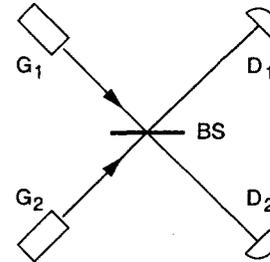


FIG. 1. The Hong-Ou-Mandel test: G_1 and G_2 are the single-photon guns and D_1 and D_2 are the photo-detectors. When the output modes of the guns are mixed in the beam splitter (BS), there should be no detector coincidences in D_1 and D_2 .

A good approximation of $F_{GG}^{(1)}$ can be measured using a Hong-Ou-Mandel (HOM) interferometer (see Fig. 1). In this measurement, the input of two identical single-photon guns G_1 and G_2 is directed toward a beam splitter and then detected by two photo-detectors D_1 and D_2 . Assuming the input state from each gun was a single photon in the same state, the output state after the beam splitter is $|2, 0\rangle + |0, 2\rangle$. However, if the input state is a mixed state or if the two guns are not identical, there will be contamination of $|1, 1\rangle$ states.

The ability to trigger the gun reproducibly is an important component of this test. If it is not possible to obtain a high $F_{GG}^{(1)}$, then the suitability of the candidate gun for any application requiring a pure state will be low. If the

application only requires a mixed state (in, for example, the case of quantum key distribution above), then the gun may still be suitable. This is a clear example where two different applications yield different suitabilities for the same single-photon gun.

It is illustrative to apply the suitability formalism to the HOM experiment itself, because it explains how to apply the concept of suitability when there are two inputs. Let the input state on the beam splitter be ρ_{in} and the output state ρ_{out} . The objective of the experiment is to obtain a high visibility in the interference, i.e., to maximize $v = 1 - \langle 1, 1 | \rho_{\text{out}} | 1, 1 \rangle$, where $|1, 1\rangle$ denotes the state that yields a detector coincidence in D_1 and D_2 .

We now want to find the target state ρ_T that is to be used in determining the suitability of the single-photon guns for the HOM experiment. In order to gain perfect visibility, the single-photon input state from G_1 must be identical to the input state from G_2 . The target state is given by

$$\rho_T = \int d\vec{k} d\omega h(\vec{k}, \omega) \hat{a}_{\vec{k}}^\dagger(\omega) \hat{b}_{\vec{k}}^\dagger(\omega) |0\rangle\langle 0| \hat{a}_{\vec{k}}(\omega) \hat{b}_{\vec{k}}(\omega), \quad (3)$$

where $\hat{a}_{\vec{k}}$ and $\hat{b}_{\vec{k}}$ are the annihilation operators associated with two input modes that overlap in the beam splitter, and $h(\vec{k}, \omega)$ is the normalized momentum and frequency window for which the beam splitter still works ($\int d\vec{k} d\omega h(\vec{k}, \omega) = 1$). Notice that F_{TT} is very small.

The input state $\rho_G = \rho_{G_1} \otimes \rho_{G_2}$ is the physical state produced when the experimenter pushes the button telling *both* guns to fire. The suitability $S_{GT} = F_{GT}/F_{TT}$ is now close to unity if and only if the state generated by the two guns overlaps with itself. The easiest way to do this, of course, is to have both guns individually generate the same pure state. Other suitable systems may involve either entangled or classical correlations between the two guns, such as in parametric down-conversion. All of the required information is always in the state ρ_G of the two-gun output.

As an example, the formalism developed above is used to design a QKD system using spontaneous parametric down-conversion in continuous wave operation (see Fig. 2a). A (nearly perfect) photodetector in the idler mode counts the number of photons per time interval. When the outcome is “1”, the same time interval in the signal mode then also contains exactly one photon in a known polarization. Alice will rotate this photon into one of the states $|\psi\rangle \in \mathcal{S}$ and send it to Bob (see Fig. 2b). The state sent to Bob will have a low $F_{GG}^{(1)}$ but high S_{GT} . The source will have high immunity to eavesdropping attacks, which means that it has a low suitability S_{GE} for the eavesdropper (where the target state ρ_E is constructed for maximum possible information gain by Eve). The state ρ_G is now a highly mixed state that contains only one photon (if D is nearly perfect) in the state $|\psi\rangle$, but crossed with a large subspace $\mathcal{R} = \{|A\rangle, |B\rangle, |C\rangle \dots\}$,

representing the unknown time of emission and uncertainty in frequency. This state has a small $F_{GG}^{(1)}$, as may be demonstrated experimentally in a Hong-Ou-Mandel experiment. The target state ρ_T required for QKD is the mixed state $|\psi\rangle\langle\psi| \otimes \rho_{\mathcal{R}}$, where $\rho_{\mathcal{R}} = \mathbb{1}/d$ is the identity operator on the subspace \mathcal{R} with dimension d . It is clear that $F_{GG}^{(1)} \approx 1/d$ but so are F_{TT} and F_{GT} . Therefore, this gun has $S_{GT} \approx 1$ and is suitable for QKD.

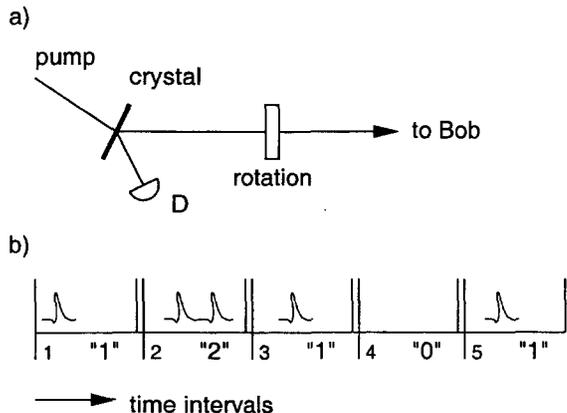


FIG. 2. Spontaneous parametric down-conversion in continuous-wave operation. a) The pump beam created photon pairs in two spatial modes, one of which is continuously monitored. b) The photon counts in the time windows. Only when one photon per time interval is counted by the detector D , we deem the creation of a “single-photon state” a success.

Let us now consider the suitability of the single-photon gun for an eavesdropper Eve. Since Eve does not know the polarization chosen by Alice, she must assign her own density matrix σ_G (i.e., her knowledge about the protocol) to the system she intercepts. For clarity, ρ is the state according to Alice, whereas σ is the state according to Eve. For example, Alice creates a state with definite polarization (say $\rho = |\psi\rangle\langle\psi|$), whereas Eve must describe it as a maximally mixed state in the polarization ($\sigma = \mathbb{1}/2$). Eve can gain information about the key when σ is no longer of this form.

The target density operator σ_E is then defined such that it allows Eve to obtain maximal information about the string of qubits that Alice sent to Bob. The quantity $S_{GE} = S(\sigma_G, \sigma_E)$ is the suitability of σ_G for eavesdropping. Perfect key distribution is defined as $S_{GE} = 0$. Notice that S_{GE} is not simply related to S_{GT} . For example, the source may sometimes fail to emit anything, which reduces both S_{GT} and S_{GE} . In this case a small S_{GT} does not necessarily mean that eavesdropping is possible. Suppose that in a practical system based on this scheme the main imperfection is the detector inefficiency (and not the possible correlations between \mathcal{S} and \mathcal{R}). Then it is easy to calculate how a given efficiency of D affects both S_{GT} and S_{GE} . Due to an imperfect detector, the state ρ_G acquires a contamination of two-photon states at a fraction ϵ , which would make $S_{GT} = 1 - \epsilon$ and $S_{GE} = \epsilon$. This

analysis would be completely different for other applications. Suppose that a pure target state were required for some protocol, for example in quantum teleportation. Since the continuous wave single-photon gun based on down-conversion has an unmeasureably small $F_{GG}^{(1)}$, it would be useless because $F_{TT} \simeq 1$ and $S_{GT} \leq F_{GG}^{(1)}$. The suitability of a single-photon gun therefore depends critically on the application.

In conclusion, we have shown that the performance of a quantum source must be evaluated in the context of some application. The suitability of a source cannot be defined as the fidelity of the output state with a target state. The reason is that there might be multiple distinct target states all equally suited for the application. We defined the suitability $S_{GT} = \text{Tr}(\rho_G \rho_T) / \text{Tr}(\rho_T \rho_T)$ instead, where ρ_G is the output state of the gun and ρ_T is an equal mixture of all suitable target states. In the case where ρ_T is pure the suitability reduces to the standard fidelity.

We explicitly investigated the case where the quantum source is a single-photon gun. It was shown that for QKD, a system using a continuously pumped SPDC crystal can provide the single-photon states needed to prevent eavesdropping even though this system would not be useful in applications where F_{TT} is close to unity. It is important to carefully understand whether a given application using single-photon quantum optics requires a pure state or can be run with any of a number of states. The requirements on the photon source are very different in these two cases. For many applications, an analysis similar to the one done for the Hong-Ou-Mandel visibility requirement must be done. This is because the apparatus uses several input photons in different places, and G is the combined state of *all* of them. In these applications it is tempting to require that all the guns emit maximally overlapping pure states. However, this is not necessary

if there is a correlation between the inputs.

This work was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The authors wish to thank Deborah Jackson for many useful discussions. P.K. acknowledges the United States National Research Council. Support was received from the Office of Naval Research, Advanced Research and Development Activity, National Security Agency, and the Defense Advanced Research Projects Agency.

-
- [1] D.P. DiVincenzo, Fortschr. Phys. **48**, 771 (2000); also in: *Scalable Quantum Computers*, S.L. Braunstein and H.-K. Lo (Eds.), pp. 1-13, Wiley-VCH (2001).
 - [2] D. Bouwmeester et al., Nature **390**, 575 (1997); E. Knill et al., Nature **409**, 46 (2001); P. Kok et al., quant-ph/0202046.
 - [3] A. Beveratos et al., Eur. Phys. J. D **18**, 191 (2002); Z.L. Yuan et al., Science **295**, 102 (2002); E. Moreau et al., App. Phys. Lett. **79**, 2865 (2001); K.O. Greulich and E. Thiel, Single Mol. **2**, 5 (2001); P. Michler et al., Science **290**, 2282 (2000); M. Lau, Mrs. Bull. **25**, 5 (2000); B. Lounis et al., J. Phys. IV **10**, 13 (2000); C.L. Foden et al., Phys. Rev. A **62**, 011803 (2000); C. Brunel et al., Cr. Acad. Sci. II B **326**, 911 (1998); K.M. Gheri et al., Phys. Rev. A **58**, R2627 (1998).
 - [4] G. Brassard, N. Lutkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
 - [5] Jozsa, R. J. Mod. Optics **41**, 2315-2323 (1994).
 - [6] C.H. Bennett and G. Brassard, Proc. IEEE Int. Conf. Comp., IEEE New York (1984).
 - [7] P.A.M. Dirac, Proc. R. Soc. London A **114**, 243 (1928); K.W. Chan, C.K. Law, and J.H. Eberly, Phys. Rev. Lett. **88**, 100402 (2002).