

## Certified randomness from a two-level system in a relativistic quantum field

Thin, Le Phuc; Bancal, Jean Daniel; Martín-Martínez, Eduardo

**DOI**

[10.1103/PhysRevA.94.022321](https://doi.org/10.1103/PhysRevA.94.022321)

**Publication date**

2016

**Document Version**

Final published version

**Published in**

Physical Review A

**Citation (APA)**

Thin, L. P., Bancal, J. D., & Martín-Martínez, E. (2016). Certified randomness from a two-level system in a relativistic quantum field. *Physical Review A*, *94*(2), Article 022321. <https://doi.org/10.1103/PhysRevA.94.022321>

**Important note**

To cite this publication, please use the final published version (if applicable). Please check the document version above.

**Copyright**

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

**Takedown policy**

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

**Certified randomness from a two-level system in a relativistic quantum field**Le Phuc Thinh,<sup>1,2</sup> Jean-Daniel Bancal,<sup>1</sup> and Eduardo Martín-Martínez<sup>3,4,5</sup><sup>1</sup>*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*<sup>2</sup>*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*<sup>3</sup>*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*<sup>4</sup>*Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*<sup>5</sup>*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada N2L 2Y5*

(Received 14 April 2016; revised manuscript received 27 May 2016; published 17 August 2016)

Randomness is an indispensable resource in modern science and information technology. Fortunately, an experimentally simple procedure exists to generate randomness with well-characterized devices: measuring a quantum system in a basis complementary to its preparation. Towards realizing this goal one may consider using atoms or superconducting qubits, promising candidates for quantum information processing. However, their unavoidable interaction with the electromagnetic field affects their dynamics. At large time scales, this can result in decoherence. Smaller time scales in principle avoid this problem, but may not be well analyzed under the usual rotating wave and single mode approximation (RWA and SMA) which break the relativistic nature of quantum field theory. Here, we use a fully relativistic analysis to quantify the information that an adversary with access to the field could get on the result of an atomic measurement. Surprisingly, we find that the adversary's guessing probability is not minimized for atoms initially prepared in the ground state (an intuition derived from the RWA and SMA model).

DOI: [10.1103/PhysRevA.94.022321](https://doi.org/10.1103/PhysRevA.94.022321)**I. INTRODUCTION**

Randomness is a fundamental resource for tasks as varied as numerical simulations, cryptography, algorithms, or gambling [1,2]. It is known that quantum systems can be used to generate truly unpredictable outcomes. While measurements on entangled states allow one to certify this randomness under a small set of assumptions [3], measurements on single systems can already produce certified randomness if a higher “level of characterization” is taken into consideration [4]. Here, we consider the randomness that can be certified by measuring a single atom in the latter case.

Atoms do not exist isolated: They always, and unavoidably, interact with the electromagnetic field. If we want to use an atomic system as a source of randomness, for example by preparing a state in one basis and then measuring in a mutually unbiased basis, one has to consider that between the time of preparation ( $t = 0$ ) and the time of measurement ( $t = T$ ), the atom interacts with the field, thus effectively sharing some information with the field. If this information can be retrieved by an adversary having access to the field at a later time, it may compromise the unpredictability of the atom's measurement result.

When the time between preparation and measurement is large decoherence may leave the atom in a mixed state, thus significantly impacting the efficiency of an atomic random number generator. One could hope to circumvent this problem by considering a short time between preparation and measurement. However, certifying randomness in this regime requires special care since relativistic effects are expected to influence the leading order contributions to the correlations between the atom and the field in this situation, in a similar manner as in the case of entanglement harvesting [5–8].

It has been discussed in the context of relativistic quantum information that atomic probes which interact with the electromagnetic field become, in general, entangled with these fields.

This is true even when the dynamics of the atom-field system is dominated by vacuum fluctuations [7,8]. These correlations are neglected in quantum optics when working under the usual rotating wave approximation (RWA) and the single mode approximation (SMA) [9] – two approximations which break the Lorentz covariance of the interaction theory and allow for causality violations and superluminal signaling [10]. However, since such correlations could be used by an adversary to guess the result of the atomic measurement, neglecting them potentially results in an underestimate of the adversary's power.

In this paper, we focus on the regime of short time between preparation and measurement, and take into account the fully relativistic<sup>1</sup> light-matter interaction model. Our analysis applies for instance to the case of an atomic probe in an optical cavity or free space, or to a superconducting qubit coupled to a transmission line.

We show that, even for atoms in the ground state in the presence of vacuum, the field fluctuations drive the creation of field-atom entanglement at a significant level. This implies, perhaps contrary to intuition, that reducing the time from preparation to measurement generally does not spare a decrease in the randomness extractable from the atom, even for extremely short time scales. We hence conclude that relativistic effects need to be taken into account in the short-time regime.

We also show that, even for relatively long waiting times between preparation and measurement, the ground state of the atom together with the vacuum state of the field is not the optimal state for randomness extraction when all relativistic considerations are factored in. This contradicts the intuition

<sup>1</sup>By relativistic, we mean here that the detector is locally coupled to a Lorentz covariant field. This excludes any possibility of superluminal signaling (present within the SMA and RWA) [10] and guarantees a proper description of high-frequency modes relevant at short times.

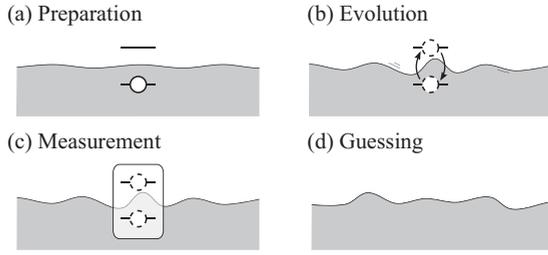


FIG. 1. Certifying randomness of an atomic measurement after interacting with a field. (a) Preparation: A two-level atom is prepared in some state (here the ground state) and starts interacting with an empty field. (b) Evolution: the atom and the field evolve for a time  $T$ . (c) Atomic measurement: a random outcome is obtained by measuring the state of the atom in an appropriate basis. (d) Guessing: the adversary can access the field (possibly at a later time) to try to guess the result of the atomic measurement.

stemming from the SMA and RWA according to which, if an atom starts in its ground state and the field is not excited, then the atom would not get entangled with the field, and so it would share no information with the field. Thus, our results demonstrate that the actual behavior is really different from the one given by these usual approximations. Quantitatively, for typical time scales and coupling regimes of strong and ultrastrong coupling in quantum optics and superconducting qubits in transmission lines, we estimate that the use of the SMA and RWA leads to an overestimation of the amount of randomness that can reach magnitudes of the order of 10%.

## II. QUANTIFYING THE RANDOMNESS EXTRACTABLE FROM AN ATOMIC DETECTOR

We consider the situation in which a user wants to generate random bits by performing a quantum measurement on an atom. For this purpose, he prepares the atom in a pure state  $|\psi_A\rangle$ , and then performs an *optimal* von Neumann measurement on it (e.g., in a complementary basis).<sup>2</sup> Since the measurement is not performed simultaneously with the state preparation, this leaves some time  $T$  for the atom to interact with the electromagnetic field between its preparation and measurement (cf. Fig. 1). In particular, this interaction modifies the optimal measurement to be performed at time  $T$  with respect to the initial mutually unbiased measurement.

Typically, this joint evolution results in the state of the atom and the field being partially entangled. After this interaction, the field thus contains some information about the outcome observed by the user upon measurement of the atom. Assuming that the field is not fully under control of the user, but can eventually be accessed by someone interested in guessing the outcome of the atom measurement (i.e., an adversary), one must evaluate how much information about the atom's state was shared with the field during this interaction time  $T$  in order

to certify the amount of randomness that can be extracted from the atom's measurement.

Throughout this paper, unless otherwise stated, we use natural units ( $\hbar = c = 1$ ) and work in the interaction picture. Let us consider a two-level atom and a massless scalar field  $\phi(x, t)$  in  $1 + 1$  dimensions initially prepared in the state  $\rho_i = |\psi_A\rangle\langle\psi_A| \otimes |0\rangle\langle 0|$ . The free Hamiltonian of such a system is given by  $H_0 = H_0^{\text{atom}} + H_0^{\text{field}}$ . If we write the Hamiltonian that generates translations with respect to the laboratory frame, which is also the field quantization frame, the free Hamiltonians of the atom and the field are given by the well-known expressions

$$H_0^{\text{atom}} = \Omega\sigma^+\sigma^-, \quad (1)$$

where  $\Omega$  is the energy gap between the two atomic levels and  $\sigma^+$  and  $\sigma^-$  are SU(2) ladder operators, and

$$H_0^{\text{field}} = \frac{1}{2} \int_{-\infty}^{\infty} dx [\pi^2(x, t) + [\nabla\phi(x, t)]^2], \quad (2)$$

where  $\pi$  is the field's canonical conjugate momentum. We model the atom-field interaction via a derivative coupling given by the following interaction Hamiltonian in the interaction picture:

$$H_I(t) = \lambda \int_{-\infty}^{\infty} dx F(x - x_a)\chi(t)\mu(t)\partial_t\phi(x, t). \quad (3)$$

Here,  $\lambda$  is the coupling strength,  $F(x - x_a)$  is the spatial profile of atom positioned at  $x_a$  (henceforth assumed symmetric about  $x_a$ ),  $\chi(t)$  is the coupling switching function, and  $\mu(t) = (e^{i\Omega t}\sigma^+ + e^{-i\Omega t}\sigma^-)$  is the atom's monopole moment.

Let us make a few remarks about the choice of this Hamiltonian. First, this is a simplified version of the light-matter interaction [9]: it can be thought of as a polarization-insensitive direct coupling to the electric field which is the derivative of the vector potential in the Coulomb gauge  $\mathbf{E} = \partial_t\mathbf{A}$  in a one-dimensional (1D) cavity such as an optical fiber. The derivative coupling has been employed in the past to ameliorate the infrared (IR) behavior of the model in many different contexts [12–14]. In our case, the use of this model also allows us to minimize the impact of neglecting the zero-mode dynamics in case of the periodic cavity [15] [see Eqs. (17) and (18)]. Despite the simplicity, this family of Unruh-DeWitt detector models have been proved to capture some of the fundamental features of the light-matter interactions [16–18].

Second, observe that this model *assumes neither the RWA nor the SMA*, and as a consequence is a causally well-behaved theory [10]. This is crucial in the current context, where we expect vacuum correlations to play a role in the amount of randomness that can be extracted by measuring an atomic system in short times after preparation.

Last, the model assumes an instantaneous coupling to all points of the atomic distribution as seen from the laboratory frame. This may lead to the unsatisfactory consequence that the Hamiltonian is no longer explicitly Lorentz covariant. However, it has been proved that the Unruh-Dewitt detector model yields Lorentz invariant predictions for smooth switching functions with arbitrary atomic profile [19] and for sudden switching functions provided the atomic profile is smooth with no problems to relativistic causality or covariance [10,20]. In any case, in our setting we write the Hamiltonian in the

<sup>2</sup>We leave the question of performing more general positive operator-valued measures (POVMs) on possibly mixed initial states, perhaps by involving additional ancillas [4], for further study. This could potentially certify up to two bits of randomness per measurement [11].

laboratory frame and always make the reasonable hypothesis that the atoms are at rest with the laboratory frame (or moving at nonrelativistic speeds with respect to it). Nevertheless, the fact that all the points of the atom are coupled simultaneously to the field calls for some care in handling the claims made with this model: we will consider interaction times in the atom's frame much longer than the light-crossing times of the atomic radius (an almost pointlike atom, so that the atom does not interact with the field in spacelike separated points in times not enough for a signal to propagate through the full extension of the atom), yet too short for the rotating wave approximation to be fulfilled. For a further discussion about the covariance of the model we refer to Sec. III E.

We will discuss the relevance of taking particular choices of the switching function  $\chi(t)$  and the spatial profile  $F(x)$  in Sec. III E after we assume concrete forms for both functions; for now we are going to keep the analysis general.

After the interaction with the field, the global state is given by

$$\rho_{AF} = |\psi_{AF}\rangle\langle\psi_{AF}| = U\rho_i U^\dagger,$$

$$U = \mathcal{T} \exp\left(-i \int_{-\infty}^{\infty} dt H_I(t)\right),$$

where  $\mathcal{T}$  represents time ordering.

After a time  $T$ , the atom is measured in some basis. The global pure state of the atom and field then effectively ‘‘collapses’’ into a state of the form  $\rho_{XF}^x = |x\rangle\langle x| \otimes \tau_F^x$  with probability  $p_X(x)$ . Here,  $x$  is the result of the measurement and  $\tau_F^x = \text{Tr}_A(P_x|\psi\rangle_{AF}\langle\psi|)/\text{Tr}(P_x|\psi\rangle_{AF}\langle\psi|)$  is the state in which the *field* is left when the measurement result is  $x$ , for a von Neumann measurement  $\{P_x\}$ . This part of the state is the one that an adversary Eve could get in contact with, and eventually measure in order to infer the value of  $x$ .

The amount of randomness that can be extracted from the outcome of the measurement performed at time  $T$  with respect to an adversary having access to the quantum field can be quantified by the conditional min-entropy

$$H_{\min}(X|F)_{\rho_{XF}} = -\log_2 P_g(X|F)_{\rho_{XF}}, \quad (4)$$

where  $P_g(X|F)_{\rho_{XF}}$  is the probability that the outcome (random variable)  $X$  is guessed correctly given the state of the quantum field  $F$ , and  $\rho_{XF} = \sum_x p_X(x)\rho_{XF}^x$ . Note that from a mathematical standpoint, the infinite dimensionality of the quantum field as side information may *a priori* require some special care [21]. The interpretation of the min-entropy in this context as well as its characterizing properties remain however intact. Using the invariance of the conditional min-entropy under local isometries [21, Lemma 1] and the fact that the atom under consideration can only be excited in a finite number of levels, we can effectively treat the quantum field  $F$  as a finite-dimensional system. To see this, we consider the state  $|\psi_{AF}\rangle$  of the atom and field just before the von Neumann measurement. By the Schmidt decomposition [22], there exists orthonormal field states  $\{|f_0\rangle, |f_1\rangle\}$  in which this state can be written as  $|\psi\rangle_{AF} = \sqrt{\lambda_0}|0, f_0\rangle + \sqrt{\lambda_1}|1, f_1\rangle$ , where  $\lambda_0$  and  $\lambda_1$  are the eigenvalues of the reduced atomic state  $\rho_A$ . For the purpose of the computation, we are not required to know explicitly the field modes  $|f_0\rangle$  and  $|f_1\rangle$  (although they can be identified by the Schmidt decomposition algorithm); it is

the job of the adversary Eve if she wants to optimally guess  $X$  given the field  $E$ . An isometry can be set up between the field  $F$  and an arbitrary qubit  $E$  of Eve so that all the information relevant for the min-entropy between  $A$  and  $F$  can be transferred to  $|\psi\rangle_{AE} = \sqrt{\lambda_0}|0,0\rangle + \sqrt{\lambda_1}|1,1\rangle$ . We can thus compute the min-entropy on  $\rho_{XE} = \sum_x p_X(x)|x\rangle\langle x| \otimes \tau_E^x$  where  $\tau_E^x = \text{Tr}_A(P_x|\psi\rangle_{AE}\langle\psi|)/\text{Tr}(P_x|\psi\rangle_{AE}\langle\psi|)$  is the *qubit* state hold by Eve whenever the atom is projected into outcome  $x$ .

To arrive at an analytic expression for the min-entropy, we recall two facts. First, the guessing probability  $P_g$  for classical-quantum states (cq) [23] can be interpreted as the optimal success probability for Eve to distinguish the (normalized) ensemble of states  $\{\tau_E^x\}$ :

$$P_g(X|E)_{\rho_{XE}} = \max_{\mathcal{E}} \sum_x p_X(x)\langle x|\mathcal{E}(\tau_E^x)|x\rangle$$

$$= \max_{\Pi_x} \sum_x p_X(x)\text{Tr}(\Pi_x \tau_E^x),$$

where optimizing over TPCPMs  $\mathcal{E}$  is equivalent to optimizing over POVMs  $\{\Pi_x = \mathcal{E}^\dagger(|x\rangle\langle x|)\}$ . Second, the optimal success probability for distinguishing an ensemble consisting of only two states is given by the Holevo-Helstrom theorem. Hence we find that the conditional min-entropy is given by

$$H_{\min}(X|E) = -\log_2 \left[ \frac{1}{2} + \frac{1}{2} \left| |p_X(0)\tau_E^0 - p_X(1)\tau_E^1| \right| \right].$$

The measurement providing the largest amount of randomness from the atom can be found by optimization over all von Neumann measurements, namely  $H_{\min}^*(X|E) = \max_{\{P_x\}} H_{\min}(X|E)_{\rho_{XE}}$ . One can check that the result of this optimization can be expressed in terms of the purity  $\text{Tr}(\rho_A^2)$  of the reduced density matrix  $\rho_A$  only as

$$H_{\min}^*(X|E) = -\log_2 \left[ \frac{1}{2} + \sqrt{\frac{1 - \text{Tr}(\rho_A^2)}{2}} \right]. \quad (5)$$

To see this, note that given the assumed form of  $|\psi\rangle_{AE}$  and orthogonal projection  $P_0 := |m_0\rangle\langle m_0|$ ,  $P_1 := |m_1\rangle\langle m_1|$  with  $|m_0\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$ ,  $|m_1\rangle = \sin\theta|0\rangle - e^{i\phi}\cos\theta|1\rangle$ , the operators  $p_X(0)\tau_E^0 = |e_0\rangle\langle e_0|$  and  $p_X(1)\tau_E^1 = |e_1\rangle\langle e_1|$  can be explicitly computed

$$|e_0\rangle = \sqrt{\lambda_0}\langle m_0|0\rangle|0\rangle + \sqrt{\lambda_1}\langle m_0|1\rangle|1\rangle,$$

$$|e_1\rangle = \sqrt{\lambda_0}\langle m_1|0\rangle|0\rangle + \sqrt{\lambda_1}\langle m_1|1\rangle|1\rangle,$$

which gives

$$\left| |p_X(0)\tau_E^0 - p_X(1)\tau_E^1| \right|_1 = \sqrt{1 - 4|\langle e_0|e_1\rangle|^2}.$$

Finally, it is useful to note that the fidelity between  $|e_0\rangle$  and  $|e_1\rangle$  reaches its maximum at  $(\lambda_0 - \lambda_1)^2/4 = \text{Tr}(\rho_A^2)/2 - 1/4$ .

The computation of the conditional min-entropy thus reduces to a computation of the reduced atomic state after the interaction with the quantum field. This is the subject of the next subsections.

### A. Final atomic state from perturbation theory

For small enough values of the coupling strength  $\lambda$ , the time-evolved density matrix is well approximated by the

following perturbative expansion:

$$\rho \simeq \rho_i + \rho^{(1)} + \rho^{(2)}, \quad (6)$$

where  $\rho^{(1)} = U^{(1)}\rho_i + \rho_i U^{(1)\dagger}$  and  $\rho^{(2)} = U^{(1)}\rho_i U^{(1)\dagger} + U^{(2)}\rho_i + \rho_i U^{(2)\dagger}$  are the first- and second-order perturbation terms in  $\lambda$ , and

$$\begin{aligned} U^{(1)} &= -i \int_{-\infty}^{\infty} dt H_I(t), \\ U^{(2)} &= - \int_{-\infty}^{\infty} dt \int_{-\infty}^t dt' H_I(t) H_I(t'). \end{aligned} \quad (7)$$

Since we are going to consider three different boundary condition scenarios (free space, Dirichlet (reflective) cavities, and periodic cavities), we will give the full detail of the calculations for the continuum case and skip directly to the final results for periodic and Dirichlet cavities.

For the case of a field in free space (e.g., an open optical fiber or open transmission line) the field can be expanded in plane-wave modes as

$$\phi(x,t) = \int_{-\infty}^{\infty} \frac{dk}{\sqrt{4\pi\omega_k}} (a_k^\dagger e^{i(\omega_k t - kx)} + \text{H.c.}) \quad (8)$$

$$\rho_A = \begin{pmatrix} a^2 & a\sqrt{1-a^2} \\ a\sqrt{1-a^2} & 1-a^2 \end{pmatrix} + \begin{pmatrix} (1-a^2)J_{--} + 2a^2 \text{Re}(X_{++}) & a\sqrt{1-a^2}(J_{-+} + X_{++} + X_{--}^*) \\ a\sqrt{1-a^2}(J_{+-} + X_{++}^* + X_{--}) & a^2 J_{++} + 2(1-a^2) \text{Re}(X_{--}) \end{pmatrix}, \quad (11)$$

where we define for  $r, s \in \{+, -\}$

$$\begin{aligned} X_{r,s} &= -\lambda^2 \int_{-\infty}^{\infty} dk \frac{\omega_k}{4\pi} \tilde{F}(k)^2 \int_{-\infty}^{\infty} dt \int_{-\infty}^t dt' \chi(t) \chi(t') e^{-i(\omega_k + r\Omega)t} e^{i(\omega_k + s\Omega)t'} \\ J_{r,s} &= \lambda^2 \int_{-\infty}^{\infty} dk \frac{\omega_k}{4\pi} \tilde{F}(k)^2 \int_{-\infty}^{\infty} dt \int_{-\infty}^{\infty} dt' \chi(t) \chi(t') e^{i(\omega_k + r\Omega)t} e^{-i(\omega_k + s\Omega)t'} \end{aligned} \quad (\text{free space}). \quad (12)$$

For atoms inside a cavity of length  $L$ , the field modes are no longer continuous but discrete. More specifically, for periodic boundary conditions (e.g., a closed optical fiber loop) we can make the following replacements:

$$k \rightarrow k_n = \frac{2\pi n}{L}, \quad \omega_k \rightarrow \omega_n = \frac{2\pi |n|}{L}, \quad (13)$$

$$\int_{-\infty}^{\infty} \frac{dk}{\sqrt{4\pi\omega_k}} \rightarrow \sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{2\omega_n L}}, \quad (14)$$

while for Dirichlet cavity (e.g., reflective walls)

$$k \rightarrow k_n = \frac{\pi n}{L}, \quad \omega_k \rightarrow \omega_n = \frac{\pi n}{L}, \quad (15)$$

$$\int_{-\infty}^{\infty} \frac{dk}{\sqrt{4\pi\omega_k}} \rightarrow \sum_{n=1}^{\infty} \frac{1}{\sqrt{\omega_n L}}. \quad (16)$$

Moreover, we make the physical assumption that the atom is much smaller than the size  $L$  of the cavity, allowing us to

so that the interaction Hamiltonian becomes

$$i\lambda\chi(t)\mu(t) \int_{-\infty}^{\infty} dk \sqrt{\frac{\omega_k}{4\pi}} \tilde{F}(k) (a_k^\dagger e^{i(\omega_k t - kx_a)} - \text{H.c.}),$$

where  $\tilde{F}(k) = \int dx f(x) e^{ikx}$  is the Fourier transform of the atomic spatial profile. We trace out the field to obtain the time-evolved state of the atom. The first-order contribution to the time-evolved density matrix is traceless on the field for our initial state, therefore for an initial detector state given by

$$|\psi\rangle_A = a|g\rangle + \sqrt{1-a^2}|e\rangle \quad (9)$$

and choosing a matrix representation such that

$$|\psi\rangle_A = \begin{pmatrix} a \\ \sqrt{1-a^2} \end{pmatrix}, \quad (10)$$

the second-order contributions in (6) are given by

$$\begin{aligned} \text{Tr}_F(U^{(2)}\rho_i) &= \begin{pmatrix} a^2 X_{++} & a\sqrt{1-a^2} X_{++} \\ a\sqrt{1-a^2} X_{--} & (1-a^2) X_{--} \end{pmatrix}, \\ \text{Tr}_F(U^{(1)}\rho_i U^{(1)\dagger}) &= \begin{pmatrix} (1-a^2) J_{--} & a\sqrt{1-a^2} J_{-+} \\ a\sqrt{1-a^2} J_{+-} & a^2 J_{++} \end{pmatrix}. \end{aligned}$$

Thus, the final state of the atom up to second order in perturbation theory is

simplify

$$\begin{aligned} &\int_{-L/2}^{L/2} dx F(x - x_a) e^{\pm ik_n x} \\ &= e^{\pm ik_n x_a} \int_{-L/2-x_a}^{L/2-x_a} dx F(x) e^{\pm ik_n x} \\ &\approx e^{\pm ik_n x_a} \int_{-\infty}^{\infty} F(x) e^{\pm ik_n x} = e^{\pm ik_n x_a} \tilde{F}(k_n) \end{aligned}$$

for a periodic cavity and similarly

$$\begin{aligned} &\int_0^L dx F(x - x_a) \sin(k_n x) \\ &\approx [e^{ik_n x_a} \tilde{F}(k_n) - e^{-ik_n x_a} \tilde{F}(-k_n)] / 2i \\ &= \tilde{F}(k_n) \sin(k_n x_a) \end{aligned}$$

for a Dirichlet cavity.

The form of the final state up to second-order perturbation remains unchanged, and  $X$  and  $J$  now take the

following form:

$$X_{r,s} = -\lambda^2 \sum_{n=1}^{\infty} \frac{\omega_n}{L} \tilde{F}(k_n)^2 \int_{-\infty}^{\infty} dt \int_{-\infty}^t dt' \chi(t) \chi(t') e^{-i(\omega_n+r\Omega)t} e^{i(\omega_n+s\Omega)t'} \quad (\text{periodic}) \quad (17)$$

$$X_{r,s} = -\lambda^2 \sum_{n=1}^{\infty} \frac{\omega_n}{L} \tilde{F}(k_n)^2 \sin^2(k_n x_a) \int_{-\infty}^{\infty} dt \int_{-\infty}^t dt' \chi(t) \chi(t') e^{-i(\omega_n+r\Omega)t} e^{i(\omega_n+s\Omega)t'} \quad (\text{Dirichlet}),$$

$$J_{r,s} = \lambda^2 \sum_{n=1}^{\infty} \frac{\omega_n}{L} \tilde{F}(k_n)^2 \int_{-\infty}^{\infty} dt \int_{-\infty}^{\infty} dt' \chi(t) \chi(t') e^{i(\omega_n+r\Omega)t} e^{-i(\omega_n+s\Omega)t'} \quad (\text{periodic}) \quad (18)$$

$$J_{r,s} = \lambda^2 \sum_{n=1}^{\infty} \frac{\omega_n}{L} \tilde{F}(k_n)^2 \sin^2(k_n x_a) \int_{-\infty}^{\infty} dt \int_{-\infty}^{\infty} dt' \chi(t) \chi(t') e^{i(\omega_n+r\Omega)t} e^{-i(\omega_n+s\Omega)t'} \quad (\text{Dirichlet}).$$

### B. For comparison: Final atomic state under the single mode and rotating wave approximations

When the coupling strength  $\lambda$  is small, it is frequent in quantum optics to simplify the interaction Hamiltonian (3) to the Jaynes-Cummings model where the single mode (SMA) and rotating wave (RWA) approximations are carried out when the atomic frequency is close to resonance with one of the cavity modes [9]. We discussed in the Introduction that these two approximations yield nonrelativistic models for light matter interaction. In this paper we will compare the predictions of extracted randomness of the fully relativistic calculation with the prediction of the usual RWA-SMA prediction in the Jaynes-Cummings model.

One may wonder why in this paper we do not analyze the SMA and RWA separately, and that perhaps only performing one of these two approximations could lead to valid results in the regimes that we are studying. However, we note that these two approximations are not independent, and in fact they derive from the same assumption: long evolution time as compared to the inverse of the atomic frequency gap. Moreover, in both approximations we neglect terms which are of the same order of magnitude, so it would be inconsistent to consider either of them individually (see the Appendix). Therefore, it makes sense to either do both approximations jointly (as we do in this section) or none of them (as we did in the previous section).

For the purpose of the comparison we suppose that the atom is on resonance with the  $m^{\text{th}}$  ( $m > 0$ ) mode of the cavity, namely  $\Omega = 2\pi m/L$  for the periodic cavity and  $\Omega = \pi m/L$  for the Dirichlet cavity (which can be obtained by controlling the cavity's length). With  $b_m = \frac{1}{\sqrt{2}}(a_m e^{ik_m x_a} + a_m e^{-ik_m x_a})$ ,  $k_m = \Omega$  as the resonant standing-wave mode of the periodic cavity, the interaction Hamiltonian under RWA and SMA becomes

$$H_I = i\lambda\chi(t)\sqrt{\frac{\Omega}{L}}\tilde{F}(k_m)(-\sigma_+ b_m + \sigma_- b_m^\dagger)$$

for a periodic cavity, and

$$H_I = i\lambda\chi(t)\sqrt{\frac{\Omega}{L}}\tilde{F}(k_m)\sin(k_m x_a)(-\sigma_+ a_m + \sigma_- a_m^\dagger)$$

for a Dirichlet cavity. This model can be solved exactly for all times, yielding the final state

$$\rho_A^m = \begin{pmatrix} a^2 + (1-a^2)\sin^2(\Theta) & a\sqrt{1-a^2}\cos(\Theta) \\ a\sqrt{1-a^2}\cos(\Theta) & (1-a^2)\cos^2(\Theta) \end{pmatrix},$$

where

$$\Theta = \begin{cases} \frac{\lambda\Omega}{\sqrt{2\pi m}}\tilde{F}(\Omega)T & (\text{periodic}) \\ \frac{\lambda\Omega}{\sqrt{\pi m}}\tilde{F}(\Omega)\sin(\Omega x_a)T & (\text{Dirichlet}) \end{cases}$$

and therefore the predictions of the SMA-RWA Jaynes-Cummings model can be compared with the fully relativistic model within the perturbative regime. More precisely, we use the following second-order expansion of the previous final state:

$$\rho_A^m = \begin{pmatrix} a^2 + (1-a^2)\Theta^2 & a\sqrt{1-a^2}\left(1 - \frac{\Theta^2}{2}\right) \\ a\sqrt{1-a^2}\left(1 - \frac{\Theta^2}{2}\right) & (1-a^2)(1-\Theta^2) \end{pmatrix}, \quad (19)$$

in the comparison.

## III. SIMULATION RESULTS

### A. Concrete simulation model

Between the instant the atom is prepared in the state  $|\psi\rangle_A$  and its measurement, the atom interacts with the field for a duration  $T$  in a manner that can be captured by the sharp switching function

$$\chi(t) = \begin{cases} 0 & \text{if } t \leq 0 \\ 1 & \text{if } 0 < t \leq T \\ 0 & \text{if } t > T. \end{cases} \quad (20)$$

We assume that the atom has the following simple spatial profile:

$$F(x) = \frac{1}{\sigma\sqrt{\pi}}e^{-x^2/\sigma^2}, \quad \tilde{F}(k) = e^{-\sigma^2 k^2}. \quad (21)$$

where  $\sigma$  gives the characteristic length scale of the atomic species [see Sec. III E below for further details about these

choices of  $\chi(t)$  and  $F(x)$ ]. Under these conditions, we have

$$\begin{aligned}
 X_{\pm,\pm} &= -\lambda^2 \int_0^\infty dk \frac{k}{2\pi} \tilde{F}(k)^2 \left[ \frac{T}{i(k \pm \Omega)} - \frac{1}{(k \pm \Omega)^2} (e^{-i(k \pm \Omega)T} - 1) \right] && \text{(free space)} \\
 X_{\pm,\pm} &= -\lambda^2 \sum_{n=1}^\infty \frac{2\pi n}{L^2} \tilde{F}\left(\frac{2\pi n}{L}\right)^2 \left[ \frac{T}{i(\frac{2\pi n}{L} \pm \Omega)} - \frac{1}{(\frac{2\pi n}{L} \pm \Omega)^2} (e^{-i(\frac{2\pi n}{L} \pm \Omega)T} - 1) \right] && \text{(periodic)} \\
 X_{\pm,\pm} &= -\lambda^2 \sum_{n=1}^\infty \frac{\pi n}{L^2} \tilde{F}\left(\frac{\pi n}{L}\right)^2 \sin^2\left(\frac{\pi n x_a}{L}\right) \left[ \frac{T}{i(\frac{\pi n}{L} \pm \Omega)} - \frac{1}{(\frac{\pi n}{L} \pm \Omega)^2} (e^{-i(\frac{\pi n}{L} \pm \Omega)T} - 1) \right] && \text{(Dirichlet),} \\
 J_{\pm,\pm} &= \lambda^2 \int_0^\infty dk \frac{2\tilde{F}(k)^2 k}{\pi(k \pm \Omega)^2} \sin^2\left(\frac{(k \pm \Omega)T}{2}\right) && \text{(free space)} \\
 J_{\pm,\pm} &= \lambda^2 \sum_{n=1}^\infty \frac{8\pi n}{L^2} \tilde{F}\left(\frac{2\pi n}{L}\right)^2 \frac{1}{(\frac{2\pi n}{L} \pm \Omega)^2} \sin^2\left(\frac{(\frac{2\pi n}{L} \pm \Omega)T}{2}\right) && \text{(periodic)} \\
 J_{\pm,\pm} &= \lambda^2 \sum_{n=1}^\infty \frac{4\pi n}{L^2} \tilde{F}\left(\frac{\pi n}{L}\right)^2 \sin^2\left(\frac{\pi n x_a}{L}\right) \frac{1}{(\frac{\pi n}{L} \pm \Omega)^2} \sin^2\left(\frac{(\frac{\pi n}{L} \pm \Omega)T}{2}\right) && \text{(Dirichlet),} \\
 J_{\pm,\mp} &= \lambda^2 \int_0^\infty dk \frac{\tilde{F}(k)^2 k}{2\pi(k^2 - \Omega^2)} [1 + e^{\pm 2i\Omega T} - 2 \cos(kT) e^{\pm i\Omega T}] && \text{(free space)} \\
 J_{\pm,\mp} &= \lambda^2 \sum_{n=1}^\infty \frac{2\pi n}{L^2} \tilde{F}\left(\frac{2\pi n}{L}\right)^2 \frac{1}{(\frac{2\pi n}{L})^2 - \Omega^2} \left[ 1 + e^{\pm 2i\Omega T} - 2 \cos\left(\frac{2\pi n}{L} T\right) e^{\pm i\Omega T} \right] && \text{(periodic)} \\
 J_{\pm,\mp} &= \lambda^2 \sum_{n=1}^\infty \frac{\pi n}{L^2} \tilde{F}\left(\frac{\pi n}{L}\right)^2 \sin^2\left(\frac{\pi n x_a}{L}\right) \frac{1}{(\frac{\pi n}{L})^2 - \Omega^2} \left[ 1 + e^{\pm 2i\Omega T} - 2 \cos\left(\frac{\pi n}{L} T\right) e^{\pm i\Omega T} \right] && \text{(Dirichlet),}
 \end{aligned}$$

where the notation  $X_{\pm,\pm}$  refers to either the upper  $X_{+,+}$  or the lower  $X_{-,-}$  combination of signs to be taken on the right-hand side (the same for the others). Given these expressions, the final state after the interaction (11) can be numerically approximated with high accuracy by performing the numerical integration or numerical summation up to a cutoff  $N_c/\sigma$ . Here, we normalize the numerical cutoff  $N_c$  by the atomic size  $\sigma$ . Since the Fourier transform of the spatial profile is a Gaussian centered at zero with standard deviation proportional to  $\sigma^{-1}$ , taking  $N_c \simeq 6$  already gives an extremely precise numerical approximation, independently of the atom's size.

### B. Randomness certification in free space

From the final states computed in the previous sections, one can compute the number of random bits that can be extracted per atom measurement using Eq. (5). In Fig. 2 we report the result of this computation for the free field case [i.e., using Eqs. (11) and (12)].

A first clear observation from Fig. 2 is that for most initial states, the randomness rate quickly decreases from 1 as soon as  $T > 0$  (see also solid line in Fig. 3). This shows that high-frequency terms play an important role in the evolution of the state for short times, and therefore they cannot be neglected.

One expected result that is verified in Fig. 2 is that preparing the atom in an excited state ( $a = 0$ ) always gives less randomness, at all interaction times within the limits of perturbation theory, than preparing it in the ground state. The

reason for this behavior is clear: an atom in the excited state can be deexcited by the rotating wave terms in the interaction Hamiltonian with an elevated probability by emitting real field quanta. For short times, these field quanta are therefore correlated with the state of the atom, giving away information about the atomic state to an adversary having access to the

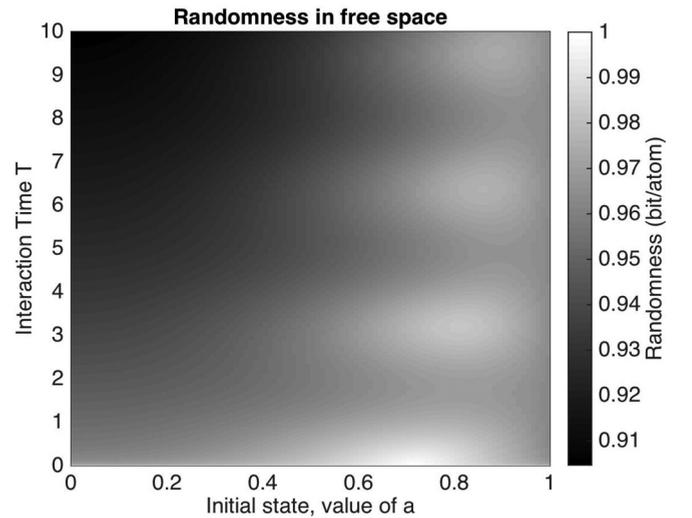


FIG. 2. Randomness in the free space scenario for different initial states at different measurement time after preparation, with chosen parameters  $\lambda = 0.01$ ,  $\sigma = 0.001$ ,  $\Omega = 1$ , and  $N_c = 6$ . Notice the use of natural units throughout.

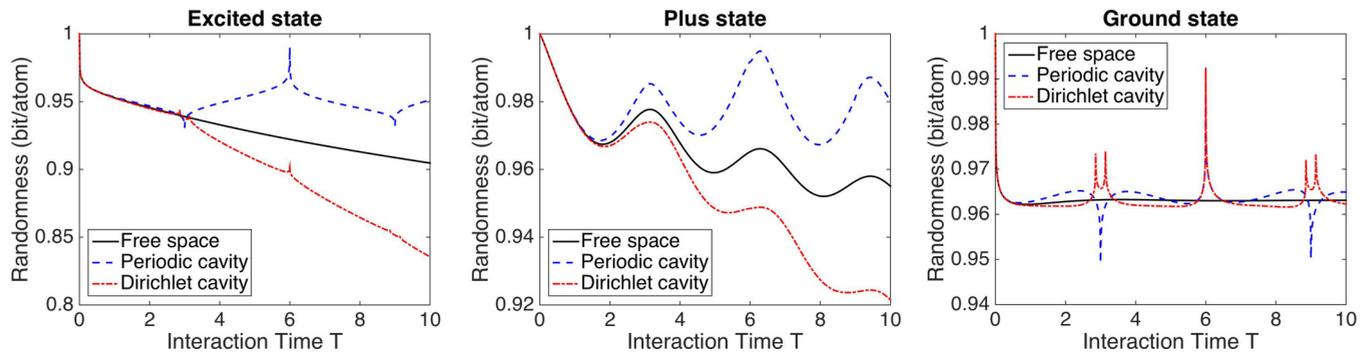


FIG. 3. Randomness for (from left to right)  $|e\rangle$ ,  $|+\rangle$ , and  $|g\rangle$  states at different measurement time after preparation, with chosen parameters  $\lambda = 0.01$ ,  $\sigma = 0.001$ ,  $\Omega = 1$ ,  $N_c = 6$ ,  $L = 3$ , and  $x_a = \pi L/6$ . Notice the use of natural units throughout. As the length  $L$  of the cavities increases, we observed that the cavity curves (blue dashed and red dot-dashed) converge to the free space curve (black solid). Note that the position of the atom in the Dirichlet cavity is chosen to be the default position  $x_a = \pi L/6$  which is roughly in the middle of the cavity. The peaks correspond to the light-crossing time of the cavity: The perturbation caused by the introduction of the atom returns to the atom after scattering with the Dirichlet or periodic boundaries of the cavities.

quantum field. Conversely, an atom in the ground state ( $a = 1$ ) can only be correlated with the field via the counter-rotating part of the Hamiltonian. Even though in that case the atom also gets correlated with the field through vacuum fluctuations, the excited state is always less secure. This behavior is indeed expected from the nonrelativistic intuition that an excited atom may emit a photon that an adversary can capture and learn about the state of the atom.

However, Fig. 2 also reveals a less intuitive effect. Namely, the ground state is not always the optimal state to extract randomness: depending on the other parameters, most notably the lag time between preparation and measurement  $T$ , it may be better to prepare the atom in a superposition of ground and excited states (see also solid line in Fig. 3).

It is clear that the ground state cannot be fully secured, because it is not an eigenstate of the interaction Hamiltonian. Therefore the interaction introduces correlations between the atom and the field even when starting from the ground state. These correlations can later be used by an adversary (that does not need to be in light contact with the first atom) to learn about the result of a measurement on the original atom. An example of how an adversary can gain information about the outcome of measurements even without receiving any energy from it is the “quantum collect calling” (virtual-photon mediated timelike communication) [24–26].

It is worth noting that the randomness certified when starting from the ground state, after rapidly decreasing, seems to attain an asymptotic value (see Fig. 3). While it is out of the scope of the present paper, it may constitute an interesting followup work to check whether this is still the case in the long-time regimes, or whether nonperturbative effects may still significantly change the purity of the reduced state of the atom  $\rho_A$  for long times.

In Fig. 4, we study the effect of the atomic size on the certified randomness. One observes that more randomness is certified in the presence of large atoms. The reason for this is that the bigger the atom gets the less the atom couples to the highest frequencies of the field, so the less the initial state is affected. Notice that the single mode approximation is recovered here when the atom is taken to be infinitely large and, thus, couples to a single frequency. This case,

of course, breaks the relativistic approach (the single mode approximation strongly violates causality [24]) which is not surprising since the atom sees the field at all points in space at the same time. In this case, the amount of certified randomness is essentially uniform over all states.

### C. Randomness extraction in cavity

Atoms inside cavities are a more realistic experimental scenario compared to atoms in free space [27–32]. There are two main differences when atoms are put inside a cavity. First, the cavity only supports a countable infinite number of modes, as opposed to the continuously many modes in free space. Second, although there are fewer modes to interact, the interaction may be made stronger than in free space [33–36].

The resulting effect of these two differences on the guessing probability is presented in Fig. 3. The periodic and Dirichlet curves in this graph were obtained by computing Eq. (5) with Eqs. (11), (17), and (18). Notice that the length of the cavity in this case is three orders of magnitude larger than the size of the atom, so our physical assumption of a small atom in a large cavity is met. This figure also compares the randomness rate with respect to the one obtained in the free field case. The peaks in Fig. 3 correspond to the light-crossing time of the cavity (the perturbation caused by the switching of the interaction bounces back on the boundary of the cavity and returns to the atom).

One would expect that for larger and larger cavities, the two cavity results converge to the free space one. This is verified in Fig. 5.

Also, in a Dirichlet cavity, the randomness output depends explicitly on the position of the atom, unlike in a periodic cavity. Figure 6 shows that this dependence is negligible.

Finally, in Fig. 7 we analyze the role of the coupling strength on the randomness rate. We observe that the behavior is the same for all the boundary condition scenarios. This can be understood because we know from Eq. (5) that the min-entropy only depends on the *purity* of the final state  $\text{Tr} \rho_A^2$ , and from (3), (6), and (7), we see that the purity of the atomic state scales as  $1 - \lambda^2$  for any set of boundary conditions.

#### D. Comparison with the rotating wave approximation

In order to compare the above results with predictions of the RWA model, we introduce the difference ratio

$$R = \frac{H_{\min}^{\text{RWA}} - H_{\min}^{\text{full}}}{H_{\min}^{\text{RWA}}}, \quad (22)$$

where  $H_{\min}^{\text{full}}$  is the randomness computed according to the method presented in the precedent paragraphs, i.e., from the state (11) with the terms described in Sec. III A, and  $H_{\min}^{\text{RWA}}$  stands for the randomness computed directly from the state (19).

Since the RWA randomness is computed under the assumption that the atom is resonant with some  $m^{\text{th}}$  mode of the cavity, throughout this section, the length of the cavity is always fixed based on the chosen resonant mode  $m$  according to  $L = 2\pi m / \Omega$  for periodic cavity and  $L = \pi m / \Omega$  for Dirichlet cavity. Note that for the sake of numerical simulation,  $m$  cannot be chosen too small relative to  $\sigma$  because this violates the assumption of a relatively big cavity with respect to the atom's size which we have made before.

As seen in Fig. 8, the randomness obtained from the fully relativistic calculation is *lower* than the randomness computed from the rotating wave approximation model (i.e.,  $R \geq 0$ ). We interpret this as coming from the fact that nonrelativistic approximations (SMA and RWA) neglect all the correlations created between the atomic probe and the remaining field modes. Indeed, the shorter the interaction, the larger the bandwidth of the field modes that get perturbed by the interaction (this can be thought of as a consequence of a time-energy uncertainty).

#### E. Discussion on the switching function and the spatial profile

In the previous subsections we have made choices for the switching function [in Eq. (20)] and the spatial profile [in Eq. (21)]. In this section we are going to discuss the relevance of these choices.

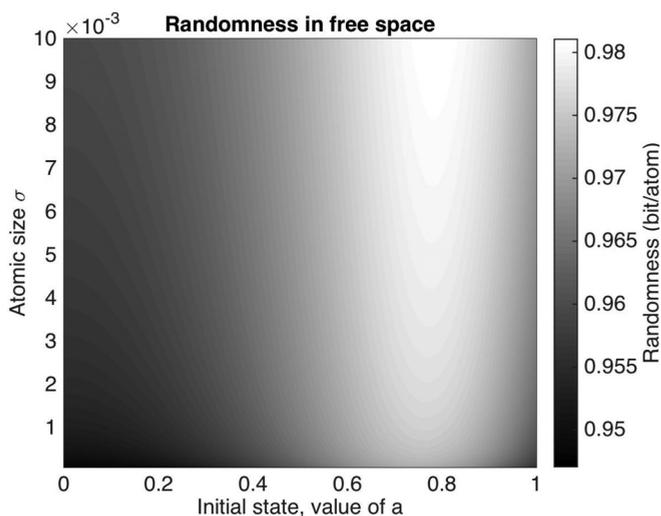


FIG. 4. Randomness for different initial states and atomic sizes, with chosen parameters  $\lambda = 0.01$ ,  $\Omega = 1$ ,  $T = 1$ , and  $N_c = 6$ . Notice the use of natural units throughout.

First of all, we have taken in (20) a sudden switching function. There are several reasons why this is a physically meaningful choice:

(i) As a first example, consider a device that prepares the state of an atom at the entrance of an optical cavity. The device would carry out a projective measurement on the atom in its free energy eigenbasis such that it ends up prepared in the ground state (i.e., we measure with optical means, and postselect only on ground states). Then the atom enters the cavity transversely (or forming some angle with the axis of the mirrors). If the atom is fast enough, a sudden switching is a good approximation to the description of the setup.

(ii) Alternatively, we could consider an atom sitting at a given position of a cavity, and at time  $t_0$  we prepare the atom in a free eigenstate, same as before, and at a time  $T$ , a measurement on the atom (with the goal to extract randomness) is performed. This case is again another example of a sudden switching function.

(iii) Consider now a different setup where an atom is trapped in a very short cavity (of near atomic size) so that the IR cutoff is well above the energy gap of the atom. That atom would be highly off resonance with the first cavity mode, and its effective interaction with the field inside the cavity would be “frozen.” The cavity is acting as a Faraday cage for the atom with respect with the EM field outside the cavity. Now imagine that we release the atom so that it starts interacting with the field. The switching function would be physically represented by the speed with which those walls are removed.

(iv) In microwave cavities with superconducting qubits, it is possible to control the strength of the coupling of a superconducting qubit with the quantum electromagnetic field inside a microwave guide as a function of time, and to make it vary either smoothly or sharply following any desired profile (see, e.g., [36]).

Note, from purely relativistic considerations, that the moment we make a choice of a finite interaction time scale, we need to specify in what reference frame this time scale is fixed. This puts constraints on the choice of the switching function and makes the Hamiltonian not explicitly Lorentz covariant as it would take different forms in different reference frames. However, the full interaction is still Lorentz covariant in this case. The details of this, as well as the details of how to write the Hamiltonian after a given switching function choice in different reference frames, can be seen in [37]. However note that we always consider the atom to be either comoving with the cavity or moving with a speed much smaller than the speed of light with respect to the cavity, and therefore the reference frame of the atom and the cavity can safely be considered the same.

As for the spatial profile, we have chosen a Gaussian spatial profile in (21) to endow the atom with some finite length scale and make our analysis more general. Indeed, the spatial profile function can be thought of as coming from the spatial probability density of an atom.

As shown in detail in [18], for realistic atoms, the spatial profile is proportional to the conjugate product of the excited and the ground-state orbital wave functions associated to the excited and the ground atomic states.

Given that the atomic wave functions have an exponential decay with the distance from the atomic center, which

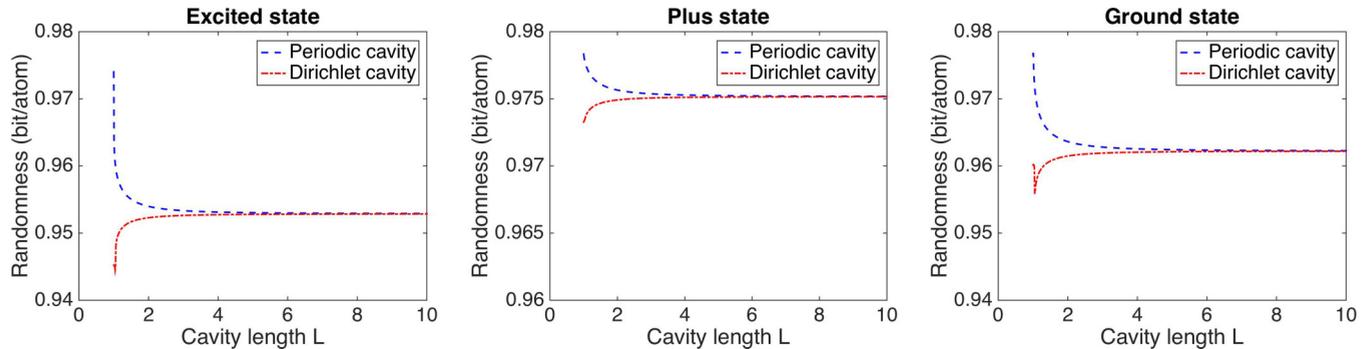


FIG. 5. Randomness for various cavity lengths assuming the atom was prepared in the state  $|e\rangle$ ,  $|+\rangle$ , or  $|g\rangle$ , with chosen parameters  $\lambda = 0.01$ ,  $\sigma = 0.001$ ,  $\Omega = 1$ ,  $T = 1$ ,  $N_c = 6$ , and  $x_a = \pi L/6$  in natural units. Dirichlet (periodic) cavity randomness converges up (down) to free space randomness.

is actually slower than a Gaussian (they are proportional to  $e^{-|x|/\sigma}$ ), their Fourier transform would be a Lorentzian function, and that means that the tails of the profile  $\tilde{F}(k)$  in momentum space will be thicker (polynomially decaying) than in the Gaussian profile case. This in turns means that under equal values of all the rest of the parameters, the single mode approximation would be even worse fulfilled for the more realistic case of an atomic orbital profile since the effect of higher frequencies would be stronger, and therefore the impact on the randomness extraction would be even more marked. This makes the choice of the Gaussian profile (which greatly simplifies the mathematical analysis) a more conservative assumption than the realistic atomic profile.

Additionally, several relativistic phenomena in the light-matter interaction have been studied with different smearing functions (compare for instance the results on entanglement harvesting and the response of particle detectors in [8] with the results in [18]). These studies showed that the qualitative behavior is not significantly altered whether we consider a Gaussian profile or a realistic atomic profile.

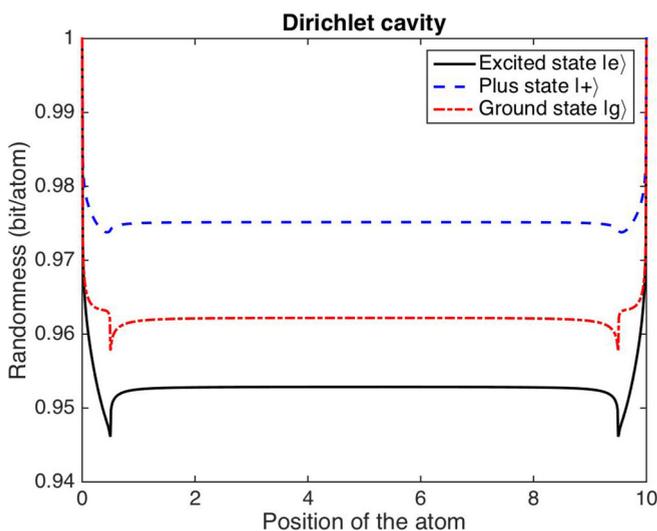


FIG. 6. Randomness vs position of atom in Dirichlet cavity, with chosen parameters  $\lambda = 0.01$ ,  $\sigma = 0.001$ ,  $\Omega = 1$ ,  $T = 1$ ,  $L = 10$ , and  $N_c = 6$ . Notice the use of natural units throughout.

Last, let us briefly discuss the assumptions made on the physical system regarding the covariant nature of the fundamental theory when we choose a spatial profile.

As discussed in [17,38], a reasonable hypothesis for a physical atomlike detector is that it has to keep internal coherence. This means that the internal forces that keep the atom together (electromagnetic interaction) will prevent it from being further smeared due to relativistic effects up to some reasonable acceleration regimes. That means that, effectively, every point of the detector will accelerate with a different acceleration in order to keep up with the rest of its points. For accelerating detectors, the rigorous analysis of a rigid atomiclike detector in terms of Fermi-Walker coordinates is analyzed in [38].

Note again that the atoms considered in this study are inertial, and moreover, moving with speeds always much slower than the speed of light, so all these considerations are not crucial for our study.

#### IV. CONCLUSIONS

In this paper we considered an atom coupled for a short time with the electromagnetic field. By taking into account the full relativistic description of the atom-field interaction, we studied the amount of information shared as a result of this interaction by the atom and the field beyond the rotating-wave and single mode approximations, as quantified by the guessing probability. We showed that small waiting times between preparation and measurement do not rid the atomic system from the problem of starting to share information with the quantized electromagnetic field to which the atom is unavoidably coupled. This is in stark contrast to what the usual approximated models of light-matter interaction predict.

In particular, the Jaynes-Cummings model under the single mode approximation and the rotating-wave approximation would predict that the optimal way to proceed to reduce this entanglement—and thus increase the randomness extractable from the atomic probe—would be to prepare the ground state of the atom and the field. This is easy to understand already from a classical intuition: If the atom is in the ground state and the field is not excited, the atom would remain in the ground state and thus it would not get correlated with the field. This intuition carries over to quantum optics under RWA and SMA. However, contrary to this intuition, we show that vacuum fluctuations

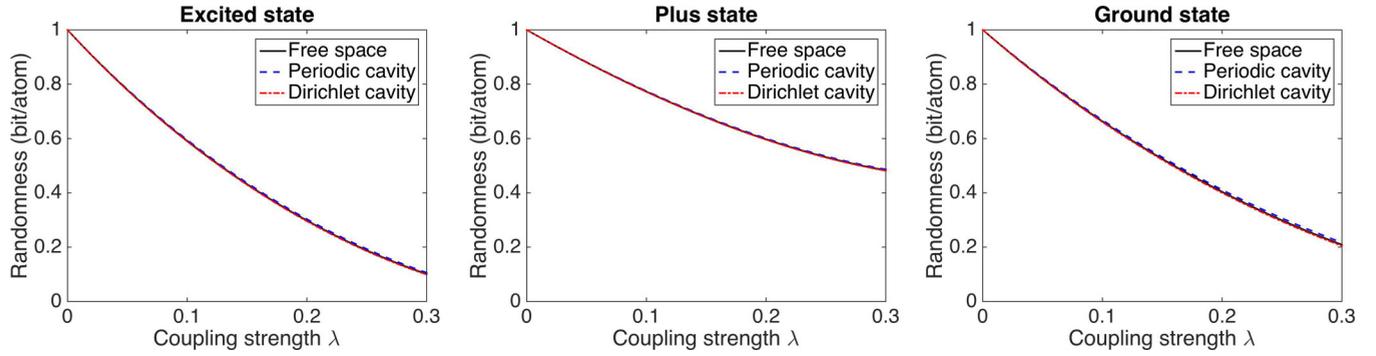


FIG. 7. Randomness vs coupling strength, with chosen parameters  $\sigma = 0.001$ ,  $\Omega = 1$ ,  $T = 1$ ,  $N_c = 6$ ,  $L = 3$ , and  $x_a = \pi L/6$ . Notice the use of natural units throughout.

entangle the atom with the field even in this case, and that this entanglement has significant consequences on the amount of certifiable randomness.

Also contrary to the classical intuition, we showed that the optimal amount of randomness is obtained for initial atomic states other than the ground state of the atom. This shows that the employment of the RWA and SMA in quantum optics does not provide a reliable lower bound on the amount of randomness that one can extract from an atomic probe.

As illustrative examples, we have analyzed the randomness loss due to these effects for the typical time scales and coupling regimes of strong and ultrastrong coupling in quantum optics and superconducting qubits in transmission lines, showing that the relative misestimation of the RWA and SMA models can indeed have a non-negligible magnitude. The time scales for these effects can be obtained by changing from natural units to dimensionful units. In the case of superconducting qubits coupled to transmission lines, the frequency gap can range from  $\Omega \sim 1$  MHz to 10 GHz [33,34,39]. This means that the time scales analyzed here are in the range of  $T \sim 10\Omega^{-1} \approx 100$  ms to 1 ns.

As a next step, it would be interesting to study quantitatively how the exchange of angular momentum may affect the randomness extracted from a quantum field when the RWA and SMA are not fulfilled. Finally, our analysis suggests that the guessing probability as a function of the time of interaction converges to a constant value in some circumstances. If this result also carries to nonperturbative regimes this could allow for randomness certification independently of the interaction time. This is an interesting open question in its own right, and it will be studied elsewhere.

#### ACKNOWLEDGMENTS

We thank V. Scarani, J. Kaniewski, and N. Sangouard for helpful discussions and correspondence. E.M.-M. gratefully acknowledges V. Scarani for his hospitality during his visit to NUS-CQT. This work was funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and by the National Research Foundation of Singapore. E.M.-M. acknowledges funding from the NSERC-Discovery program.

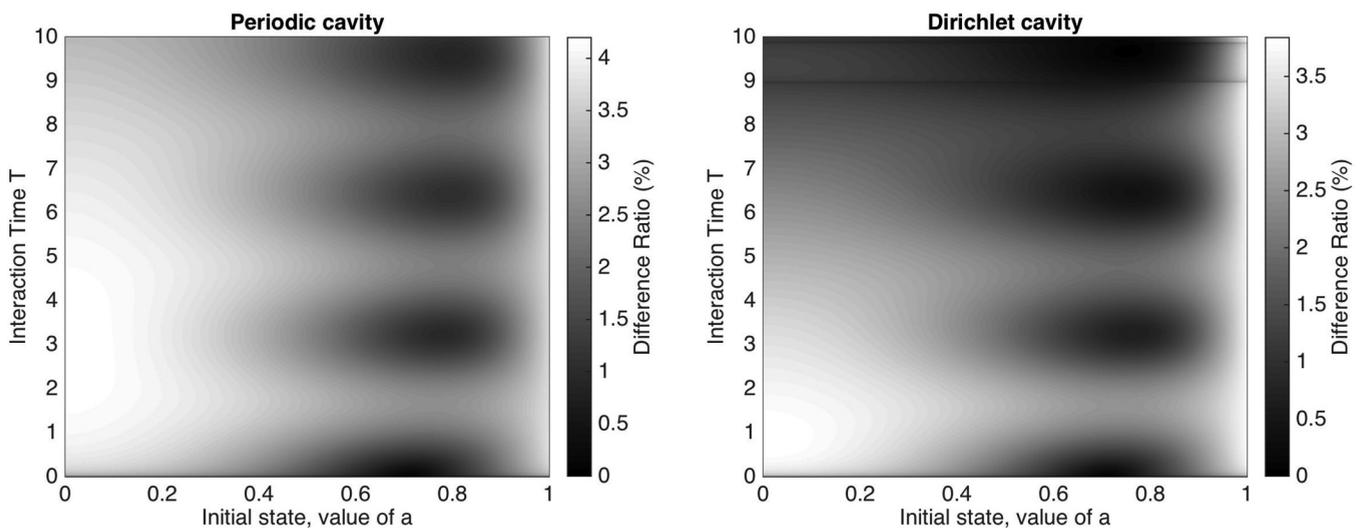


FIG. 8. Comparison between randomness computed for the full model and for the simplified RWA model in cavities, with chosen parameters  $\lambda = 0.01$ ,  $\sigma = 0.001$ ,  $\Omega = 1$ ,  $m = 3$ ,  $N_c = 6$ , and  $x_a = \pi L/6$ . Notice the use of natural units throughout. Observe the horizontal peaks in the figure on the right at the cavity light-crossing time due to the perturbation introduced by the switching returning to the original position of the atom after scattering with the boundaries. Note that  $m = 3$  corresponds to a Dirichlet cavity of length  $L = 3\pi$ .

**APPENDIX: RELATION BETWEEN THE SMA AND RWA**

In this appendix, we discuss that the terms neglected by the SMA and RWA are of the same order. Therefore, both approximations are related.

Recall that we have a two-level atom interacting, according to Eq. (3), with a quantized quantum field in periodic or Dirichlet cavity with the form of  $\phi(x, t)$  given by Eq. (8) with the appropriate replacement rules. In this case, the dynamics is completely governed by the unitary time evolution operator which in the small coupling ( $\lambda \ll \Omega$ ) is determined by Eq. (7). Let us assume further that the atom is on resonant with the cavity mode  $\Omega = \omega_m$  for some fixed  $m$ .

For illustration, the first-order perturbation  $U^{(1)}$  depends on terms of the form

$$\int_{-\infty}^{\infty} dt \chi(t) e^{\pm i(\Omega \pm \omega_n)t}, \quad (\text{A1})$$

where the terms with  $e^{\pm i(\Omega - \omega_n)t}$ , corresponding to interaction terms of the form  $a_n \sigma_+$  and  $a_n^\dagger \sigma_-$ , are usually called the rotating

contributions, and the other terms where  $e^{\pm i(\Omega + \omega_n)t}$  are called the counter-rotating contributions. Let us consider a constant interaction strength in some time interval  $[t_{\text{start}}, t_{\text{stop}}]$ . Namely  $\chi(t) = 1$  in some  $\Delta T = t_{\text{stop}} - t_{\text{start}}$  and 0 elsewhere. The contribution of the resonant mode  $m$  to the qubit's dynamics grows with  $\Delta T$  while the off-resonant modes  $n \neq m$  contribution stays bounded  $\sim (\Omega - \omega_n)^{-1}$ . The counter-rotating mode contributions are also always bounded  $\sim (\Omega + \omega_n)^{-1}$ .

Thus if one makes the assumption of SMA, namely dropping all contributions from off-resonant modes (because their contributions stay bounded while that of the resonant mode grows with interaction time  $\Delta T$ ), then for consistency one must drop the contributions from the counter-rotating terms since they are smaller, i.e., doing RWA as well.

For both approximations to be faithful already at leading order in perturbation theory we need to demand that

- (i) there is a resonant mode,
- (ii) the interaction times are much larger than  $\Omega^{-1}$ .

Since the requirement  $T \gg \Omega^{-1}$  is the same for both approximations, it is not a consistent approach (in these simple light-matter interaction models) to consider one and not the other without any further hypotheses.

---

[1] N. Metropolis and S. Ulam, *J. Am. Stat. Assoc.* **44**, 335 (1949).  
 [2] R. Motwani and P. Raghavan, *Randomized Algorithms* (Cambridge University Press, New York, 1995).  
 [3] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Nature (London)* **464**, 1021 (2010).  
 [4] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, *J. Phys. A: Math. Theor.* **47**, 424028 (2014).  
 [5] A. Valentini, *Phys. Lett.* **A153**, 321 (1991).  
 [6] B. Reznik, *Found. Phys.* **33**, 167 (2003).  
 [7] B. Reznik, A. Retzker, and J. Silman, *Phys. Rev. A* **71**, 042104 (2005).  
 [8] A. Pozas-Kerstjens and E. Martín-Martínez, *Phys. Rev. D* **92**, 064042 (2015).  
 [9] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, England, 1997).  
 [10] E. Martín-Martínez, *Phys. Rev. D* **92**, 104019 (2015).  
 [11] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, *Phys. Rev. A* **93**, 040102(R) (2016).  
 [12] P. C. W. Davies and A. C. Ottewill, *Phys. Rev. D* **65**, 104014 (2002).  
 [13] Q. Wang and W. G. Unruh, *Phys. Rev. D* **89**, 085009 (2014).  
 [14] B. A. Juárez-Aubry and J. Louko, *Class. Quantum Grav.* **31**, 245007 (2014).  
 [15] E. Martín-Martínez and J. Louko, *Phys. Rev. D* **90**, 024015 (2014).  
 [16] A. M. Alhambra, A. Kempf, and E. Martín-Martínez, *Phys. Rev. A* **89**, 033835 (2014).  
 [17] E. Martín-Martínez, M. Montero, and M. del Rey, *Phys. Rev. D* **87**, 064038 (2013).  
 [18] A. Pozas-Kerstjens and E. Martín-Martínez, [arXiv:1605.07180](https://arxiv.org/abs/1605.07180) [Phys. Rev. D (to be published)].  
 [19] A. Satz, *Class. Quantum Grav.* **24**, 1719 (2007).  
 [20] J. Louko and A. Satz, *Class. Quantum Grav.* **23**, 6321 (2006).  
 [21] M. Berta, F. Furrer, and V. B. Scholz, *J. Math. Phys.* **57**, 015213 (2016).  
 [22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).  
 [23] M. Tomamichel, [arXiv:1203.2142](https://arxiv.org/abs/1203.2142).  
 [24] R. H. Jonsson, E. Martín-Martínez, and A. Kempf, *Phys. Rev. A* **89**, 022330 (2014).  
 [25] R. H. Jonsson, E. Martín-Martínez, and A. Kempf, *Phys. Rev. Lett.* **114**, 110505 (2015).  
 [26] A. Blasco, L. J. Garay, M. Martín-Benito, and E. Martín-Martínez, *Phys. Rev. Lett.* **114**, 141103 (2015).  
 [27] J. M. Raimond, M. Brune, and S. Haroche, *Rev. Mod. Phys.* **73**, 565 (2001).  
 [28] S. Haroche, *Rev. Mod. Phys.* **85**, 1083 (2013).  
 [29] C. Guerlin, J. Bernu, S. Deleglise, C. Sayrin, S. Gleyzes, S. Kuhr, M. Brune, J.-M. Raimond, and S. Haroche, *Nature (London)* **448**, 889 (2007).  
 [30] S. Gleyzes, S. Kuhr, C. Guerlin, J. Bernu, S. Deleglise, U. B. Hoff, M. Brune, J.-M. Raimond, and S. Haroche, *Nature (London)* **446**, 297 (2007).  
 [31] M. Brune, S. Haroche, V. Lefevre, J. M. Raimond, and N. Zagury, *Phys. Rev. Lett.* **65**, 976 (1990).  
 [32] G. Nougues, A. Rauschenbeute, S. Osnaghi, M. Brune, J. M. Raimond, and S. Haroche, *Nature (London)* **400**, 239 (1999).  
 [33] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, *Phys. Rev. A* **69**, 062320 (2004).  
 [34] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf, *Nature (London)* **431**, 162 (2004).

- [35] I. Chiorescu, P. Bertet, K. Semba, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij, *Nature (London)* **431**, 159 (2004).
- [36] B. Peropadre, P. Forn-Díaz, E. Solano, and J. J. García-Ripoll, *Phys. Rev. Lett.* **105**, 023601 (2010).
- [37] E. G. Brown, E. Martín-Martínez, N. C. Menicucci, and R. B. Mann, *Phys. Rev. D* **87**, 084062 (2013).
- [38] S. Schlicht, *Class. Quantum Grav.* **21**, 4647 (2004).
- [39] K. Cicak, D. Li, J. A. Strong, M. S. Allman, F. Altomare, A. J. Sirois, J. D. Whittaker, J. D. Teufel, and R. W. Simmonds, *Appl. Phys. Lett.* **96**, 093502 (2010).