# Quantum enhancement of spoofing detection with squeezed states of light

Tomás P. Espinoza,[1,*] Sebastian C. Carrasco,[2,†] José Rogan,[1] Juan Alejandro Valdivia,[1] and Vladimir S. Malinovsky[2]
[1]*Departamento de Física, Facultad de Ciencias, Universidad de Chile, Santiago, Chile*
[2]*DEVCOM Army Research Laboratory, Adelphi, Maryland 20783, USA*

(Received 20 June 2024; accepted 21 October 2024; published 27 November 2024)

We employ quantum state discrimination theory to establish the ultimate limit for spoofing detection in electromagnetic signals encoded with random quantum states. Our analysis yields an analytical expression for the optimal bound, which we prove can be achieved using a pair of coherent states. Notably, the quantum enhancement persists regardless of photon number, thereby removing the previous constraint to single-photon sources. This breakthrough unlocks new experimental possibilities using standard laser sources. Furthermore, we explore the encoding of squeezed states and demonstrate that the detection probability approaches 100% when the spoofer's capability is restricted to coherent-state generation.

DOI: 10.1103/PhysRevResearch.6.043214

## I. INTRODUCTION

Quantum state discrimination theory [1,2] is a fundamental part of quantum mechanics and its technological applications [3,4], such as quantum computing [5], quantum sensing [6], and quantum information science [7–10]. It establishes that it is impossible to discriminate a set of nonorthogonal quantum states from each other with absolute precision [1,2]. At the most, one could successfully differentiate between states with a probability that depends on their overlap (in the case of pure quantum states). This has radical consequences. If quantum state discrimination were always perfect, it would imply impossibilities such as instantaneous communication via quantum entanglement [11,12] (contradicting the no-signaling principle) or cloning quantum states [13,14] (contradicting the no-cloning theorem). Thus, the impossibility of perfect quantum state discrimination is closely related to other fundamental results of quantum mechanics, and one can regard it as a fundamental, yet implicit, postulate of quantum theory [4].

These intriguing features have motivated applications of quantum mechanics in security and have given rise to new fields such as quantum cryptography [15,16]. In the past decade, it has been pointed out that those quantum effects can enhance spoofing detection with respect to the limitations that classical physics imposes [17–20]. More recently, Blakely and Pethel [21] showed that the most simple model of quantum spoofing exhibits enhancement in the probability of detecting spoofing. That enhancement comes from the impossibility of perfectly discriminating two nonorthogonal states, and its main application would be to detect the spoofing of a radar signal [21–23]. In radar, one party tries to gain information about the other's position, speed, and orientation, to name a few, by analyzing the reflection of an electromagnetic signal, while the other, the spoofer, could attempt to provide false information by creating a fictitious reflection. One limitation in the model of Ref. [21] is that the quantum advantage exists only within the limits of a low number of photons, thus limiting its applicability due to the difficulty of generating low photon pulses and distinguishing them from the background noise [24].

The model consists of a transmitter-receiver pair that chooses one of two nonorthogonal quantum states. Then the transmitter encodes the state in an electromagnetic signal. A third party, the spoofer, could intercept the signal and send a new one to the receiver. The spoofer has a delicate task if it wants to be undetected. It needs to know which state the transmitter-receiver pair chose. Thus, the spoofer must discriminate between the two possible quantum states, which the spoofer cannot do perfectly. The drawback is that the receiver must also measure the quantum state to check if it is the one agreed upon, which cannot be done faultlessly. In this model that interplay is what generates but also limits the quantum enhancement.

We extend the protocol of Ref. [21] to explore the fundamental quantum limits of spoofing detection, considering arbitrary quantum states as transmitter-receiver pairs. This generalization surpasses the binary-phase shift keying scenario of [21], enabling a more comprehensive analysis. Our key findings reveal that the success probability of spoofing detection solely depends on the overlap between the quantum states, allowing us to derive an upper bound for this probability. Furthermore, we identify the optimal coherent states for the transmitter-receiver, which achieve this bound at a critical photon number and demonstrate quantum enhancement over classical success probabilities. Notably, our approach eliminates the need for single-photon sources in proof-of-principle

*Contact author: tp.espinozam@gmail.com
†Contact author: seba.carrasco.m@gmail.com

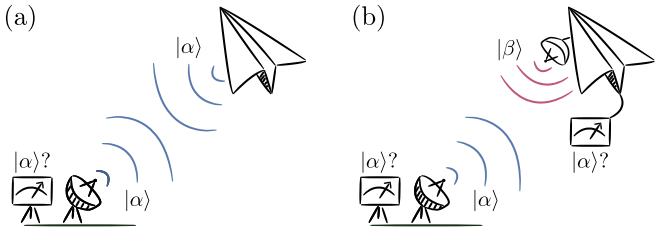


FIG. 1. Possible scenarios and quantum states. (a) shows the scenario where a quantum state $|\alpha\rangle$ is encoded in a signal and transmitted. Then an object (represented by an airplane) reflects the signal to the receiver. (b) shows the alternative scenario where a spoofer intercepts the transmitted signal and creates a false reflection. The quantum state encoded in the spoof signal depends on whether the spoofer concluded that the state was $|\alpha\rangle$ or $|\beta\rangle$. In the image the spoofer concluded that it was $|\beta\rangle$ and encoded it in the spoof signal. The receiver attempts to distinguish between both scenarios based on the received signal.

experiments; thus, it opens the door for a new regime for experimental demonstrations, paving the way for experimental advancements and further development of spoofing detection technology.

At first glance, our claim that advantages persist at higher photon numbers may appear counterintuitive, as experiments typically demonstrate that the probability of error in quantum state discrimination decreases with increasing photons [25–27]. However, these experiments usually involve discriminating between states with decreasing overlap as the photon number increases. In contrast, our approach optimizes quantum spoofing detection by identifying states with a specific optimal overlap value independent of photon number. As a result, the probability of successful discrimination remains constant, unaffected by the number of photons.

Our findings reveal that multiple pairs of quantum states, including nonclassical states, can saturate the bound. Although nonclassical states offer no advantage over coherent states in this context, their generation is significantly more challenging [28]. Therefore, we investigate a scenario where the transmitter-receiver pair has access to nonclassical states, while the spoofer is limited to coherent states. In this restricted scenario, we demonstrate that the success probability bound can be surpassed. As a specific example, we consider the transmitter-receiver pair utilizing squeezed states of light [28–30]. Our analysis shows that the probability of detecting spoofing approaches unity, limited only by the experimental capabilities of generating nonclassical states, such as squeezed states.

## II. QUANTUM LIMITS FOR SPOOFING TWO ARBITRARY QUANTUM STATES

Let us consider the scenario illustrated in Fig. 1(a). A transmitter randomly chooses a quantum state $|\alpha\rangle$ or $|\beta\rangle$ with equal probability. Next, the transmitter emits the coherent state encoded in an electromagnetic signal [31] [see Fig. 1(a)]. Then, the signal reflects from a target and goes to the receiver, which also knows the chosen quantum state. Upon arrival, the receiver can get information regarding the target position and speed by analyzing the arrival of the reflecting signal and the Doppler shift, among other properties. Nevertheless, there is a chance that the target chooses to spoof the signal by emitting a false signal, providing misleading information [see Fig. 1(b)].

The receiver can detect if the signal is a truly reflected pulse by checking if the quantum state of the received signal is the same as that transmitted originally. So, if the spoofer wants to go unnoticed, it has to create a pulse that is an exact copy of the original [as in Fig. 1(b)]. To create that copy, it must discriminate between the states $|\alpha\rangle$ or $|\beta\rangle$ that can be emitted by the transmitter. The measurement is able to successfully discriminate the states with probability

$$\gamma = \tfrac{1}{2} + \tfrac{1}{2}\sqrt{1 - |\tau|^2}, \tag{1}$$

where $\tau = \langle\alpha|\beta\rangle$. This is called the Helstrom bound [1].

When the reflected (or spoofed) pulse arrives at the receiver, the receiver must determine whether there has been spoofing. To do that, it has to choose between two hypotheses. The first one, $H_1$, is that the pulse is a true reflection of the original pulse, which we assume to be $|\alpha\rangle$. The density operator that describes this hypothesis is given by

$$\hat{\rho}_1 = |\alpha\rangle\langle\alpha|\,. \tag{2}$$

The second hypothesis, $H_2$, holds that the target side spoofed the pulse. The spoofer optimally discriminates the quantum state with probability $\gamma$. Therefore, the density operator representing this hypothesis is mixed and is described by

$$\hat{\rho}_2 = \gamma\,|\alpha\rangle\langle\alpha| + (1-\gamma)\,|\beta\rangle\langle\beta|\,. \tag{3}$$

If the prior probability of $H_2$ is $p$, the maximum probability of successfully discriminating a true reflection from a spoof is

$$P_s = \tfrac{1}{2} + \tfrac{1}{2}||p\hat{\rho}_2 - (1-p)\hat{\rho}_1||, \tag{4}$$

where $||\cdot||$ is the trace norm, which is defined as the sum of the absolute values of the eigenvalues.

The eigenvalues $\eta$ of $p\hat{\rho}_2 - (1-p)\hat{\rho}_1$ satisfy

$$\begin{vmatrix} p\gamma - (1-p) - \eta & [p\gamma - (1-p)]\,\langle\alpha|\beta\rangle \\ p(1-\gamma)\,\langle\beta|\alpha\rangle & p(1-\gamma) - \eta \end{vmatrix} = 0 \tag{5}$$

and are given by

$$\eta_\pm = \tfrac{1}{2} - p \pm \chi, \tag{6}$$

where $\chi = \sqrt{(1/2-p)^2 - p(1-\gamma)(p\gamma - 1 + p)(2\gamma-1)^2}$. The probability of success in detecting the spoofer is then

$$P_s = \tfrac{1}{2}(1 + |\eta_+| + |\eta_-|). \tag{7}$$

As $\eta_+$ is always positive, the probability of success depends on the sign of $\eta_-$. Indeed,

$$P_s(\gamma) = \begin{cases} \frac{1}{2} + \chi & \text{if } p < (1+\gamma)^{-1}, \\ p & \text{otherwise.} \end{cases} \tag{8}$$

If $p > (1+\gamma)^{-1}$, then $\eta_-$ is positive, and the probability of success is $P_s = p$, which matches the classical limit (where the states can be unambiguously discriminated, and $\gamma = 1$). If $p < (1+\gamma)^{-1}$, $\eta_-$ is negative and the probability of success $P_s$ differs from the classical limit.

To find the maximum value of the success probability, we need to optimize $\chi$ in Eq. (8), which is a function of $\gamma$. Taking $\partial\chi^2/\partial\gamma = 0$ (which shares the maximum we are looking for

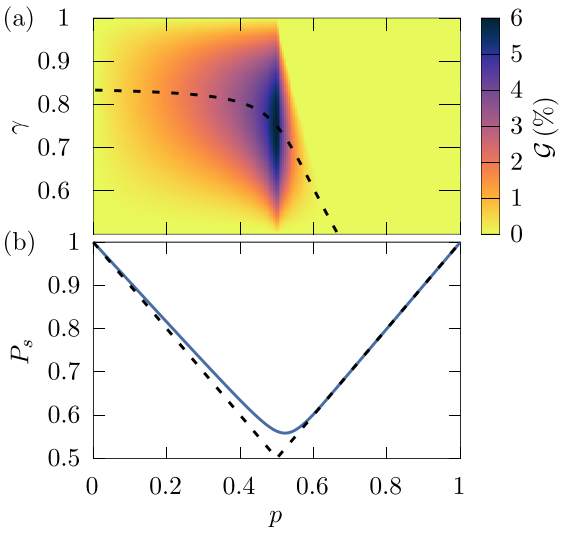


FIG. 2. Quantum spoofing results for a pair of arbitrary quantum states. (a) Quantum enhancement of the success probability in detecting the spoofer $\mathcal{G}$ as a function of the prior probability of spoofing $p$ and the probability of discriminating the two states $\gamma$. The dashed line shows the optimal value of $\gamma$. (b) Optimal bound for the success probability as a function of the prior probability $p$ for two arbitrary quantum states (solid line) and the classical limit (dashed line), where perfect state discrimination is possible, thus $\gamma = 1$.

with $\chi$), we obtain that the optimal value of $\gamma$ should satisfy the following equation:

$$16p\gamma^3 - 12(p+1)\gamma^2 + (16-6p)\gamma + 4p - 5 = 0. \quad (9)$$

Solving this equation, we find the optimal discrimination probability between two arbitrary states $|\alpha\rangle$ and $|\beta\rangle$ to be

$$\gamma_{\text{opt}} = \frac{p+3-\sqrt{33p^2-34p+9}}{8p}, \quad (10)$$

and therefore, according to Eq. (1), the optimal overlap is

$$|\tau_{\text{opt}}|^2 = \frac{26p-13p^2-9+3(1-p)\sqrt{33p^2-34p+9}}{8p^2}. \quad (11)$$

Equations (8), (10), and (11) are the main results of this work, which allow us to find all pairs of quantum states, maximizing the success probability of spoofing detection. Together, these equations define a universal bound for optimal quantum spoofing detection.

Figure 2(a) shows the quantum enhancement of the probability of detecting spoofing, given by the success probability increase with respect to the classical limit, $\mathcal{G} = P_s(\gamma) - P_s(\gamma = 1)$, as a function of $p$ and $\gamma$. In a dashed line we plot the optimal discrimination probability, $\gamma_{\text{opt}}$. We observe that our solution maximizes the quantum enhancement and that the maximum is surprisingly wide, demonstrating the solution robustness. In Fig. 2(b) we plot the optimal success probability of spoofing detection (solid line) as a function of the prior probability $p$ and compare it with the classical limit (dashed line). Using the expression for the optimal value of the successful discrimination probability, $\gamma_{\text{opt}}$, in Eq. (10) and the success probability in Eq. (8), we find that a quantum enhancement exists only if the prior probability $p < 2/3$. As we can see, the quantum advantage is maximum around $p \approx 1/2$.

## III. QUANTUM BOUND OF SPOOFING DETECTION: COHERENT-STATES CASE

To attain the bound, we modify the strategy of [21], where the states $|\alpha\rangle$ and $|-\alpha\rangle$ (binary-phase shift keying) were used by the transmitter-receiver. Here we propose to use the coherent states $|\alpha\rangle = |\sqrt{n}\exp(i\phi/2)\rangle$ and $|\beta\rangle = |\alpha^*\rangle$, where $n$ is the number of photons. The idea is that the phase $\phi$ will allow us to control the overlap,

$$|\tau|^2 = |\langle\alpha|\beta\rangle|^2 = \exp(-4n\sin^2\phi/2), \quad (12)$$

and consequently, the state discrimination probability $\gamma$ and the success probability of the spoofing detection $P_s$.

Using Eq. (12), we solve for the optimal phase given by

$$\phi_{\text{opt}} = 2\arcsin\left(\sqrt{-\frac{\log|\tau_{\text{opt}}|}{2n}}\right). \quad (13)$$

In the limit of a large number of photons, $\phi_{\text{opt}}$ scales proportionally to $1/\sqrt{n}$ due to the fact that the distribution width of a coherent state scales as $\sqrt{n}$. For small values of $n$, $\phi_{\text{opt}}$ becomes undefined according to Eq. (13), since the probability distributions of $|\alpha\rangle$ and $|\beta\rangle$ are too close to the origin in phase space and, thus, too close to each other. In this case, the optimal phase is $\phi_{\text{opt}} = \pi$, as it minimizes the overlap. For $p = 1/2$, the critical number of photons upon $\phi_{\text{opt}}$ ceases to be $\pi$ is $\log(4/3)/4 \approx 0.072$ (the minimum number of photons where Eq. (13) is well defined), as the optimal overlap in that case is $|\tau_{\text{opt}}|^2 = 3/4$.

We summarize our results for coherent states in Fig. 3. Figure 3(a) shows that given a prior probability, there is a critical number of photons upon which the case $\phi = \pi$ ceases to be optimal. Beyond that number of photons, the success probability saturates the bound defined by Eq. (8) when the phase is adjusted according to (13), and it becomes independent of the averaged number of photons, $n$.

Figure 3(b) shows the success probability as a function of the number of photons $n$ and the phase $\phi$. The solid line shows the optimal phase, which is $\pi$ for small values of $n$. For larger values of $n$, it starts decreasing as $1/\sqrt{n}$. As $n$ increases this becomes necessary to keep the overlap constant as Eq. (12) demands. Here it arises for similar reasons, as the minimum phase scale allows state discrimination. Figure 3(c) shows the comparison between the overlap obtained by optimizing the phase $\phi$ and the overlap obtained for $\phi = \pi$. The results are identical when the number of photons is below the critical value $n = 0.072$. When the number of photons surpasses the critical value, the overlap converges to the optimal value $|\tau_{\text{opt}}|^2 = 3/4$, which can be obtained from Eq. (11).

In summary, we show that it is possible to saturate the quantum bound for quantum spoofing detection using coherent states upon a certain number of photons.

## IV. DETECTING SPOOFING WITH SQUEEZED STATES

An alternative way to attain the maximum bound for the probability of success in detecting a spoofer is to utilize a pair of squeezed states. The only condition that needs to

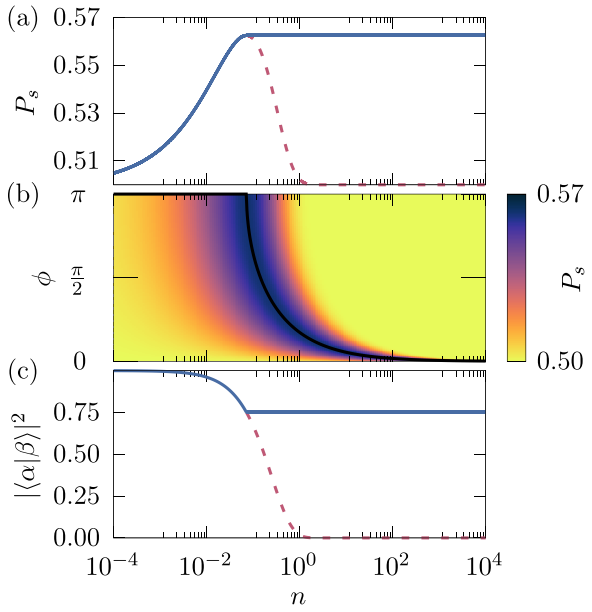


FIG. 3. Quantum spoofing results for a pair of coherent quantum states if the prior probability is $p = 0.5$ (spoofing is as likely as not spoofing). (a) Success probability of detecting spoofing as a function of the number of photons $n$. The dashed line corresponds to the case $\phi = \pi$, and the solid line demonstrates the proposed scenario when we adjust the state overlap by optimizing $\phi$. (b) Probability of detecting spoofing as a function of the phase $\phi$ and the number of photons $n$. The solid line shows the optimal phase, $\phi_{\text{opt}}$. (c) The coherent-state overlap squared vs the number of photons; the dashed line corresponds to $\phi = \pi$, and the solid line corresponds to the overlap generated by the optimal phase, $\phi_{\text{opt}}$.

be fulfilled is given by Eq. (11), which shows that the only requirement is to ensure the states have the optimal overlap. A squeezed state $|\Psi\rangle$ is defined as [3]

$$|\Psi(\alpha,\zeta)\rangle = \hat{D}(\alpha)\hat{S}(\zeta)\,|0\rangle\,, \tag{14}$$

where $\hat{D}(\alpha)$ is the displacement operator,

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^{\dagger} - \alpha^{*}\hat{a}), \tag{15}$$

and $\hat{S}(\zeta)$ is the squeezing operator,

$$\hat{S}(\zeta) = \exp\left(\tfrac{1}{2}(\zeta^{*}\hat{a}^{2} - \zeta\hat{a}^{\dagger 2})\right). \tag{16}$$

Here $\alpha = \sqrt{n}e^{i\phi/2}$ and $\zeta = re^{i\theta}$ are complex numbers, which define the position in phase space of the state $[\sqrt{2n}\cos(\phi/2), \sqrt{2n}\sin(\phi/2)]$, $r$ is the squeezing coefficient, and $\theta$ is the squeezing phase (related to the squeezing angle in phase space). The overlap between the two squeezed states can be adjusted by these parameters to be the optimal one.

Although squeezed states do not provide any advantage by themselves, they are harder to produce in an optical setup. For instance, if the spoofer is inside a moving object such as an airplane, it would not be that easy to have the necessary optics inside. Thus, it makes sense to consider the case where the spoofer cannot produce squeezed states. That changes the hypothesis previously discussed in the following way: after successfully discriminating between the two squeezed states $|\varphi\rangle = |\Psi(\alpha,\zeta)\rangle$ and $|\xi\rangle = |\Psi(\alpha^{*},\zeta^{*})\rangle$ with probability $\gamma$,

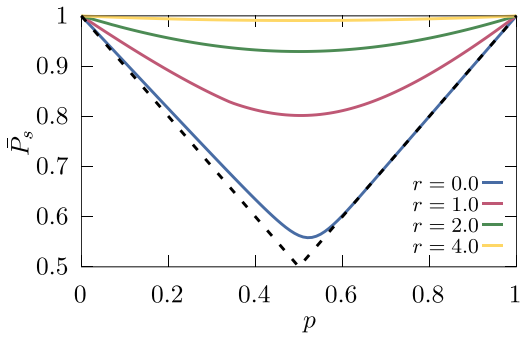


FIG. 4. Maximum success probability as function of the prior probability $p$ for $n = 100$ photons. The dashed line corresponds to the classical limit, and each solid line corresponds to different values of squeezing $r$.

the spoofer has to use the coherent states that maximize the overlap with the squeezed coherent state to respond.

Suppose the original state encoded in the pulse is $|\varphi\rangle$. The hypothesis $H_1$ is then represented by the density operator

$$\hat{\rho}_1 = |\varphi\rangle\langle\varphi|\,, \tag{17}$$

and the hypothesis $H_2$ is described by

$$\hat{\rho}_2 = \gamma\,|\alpha\rangle\langle\alpha| + (1-\gamma)\,|\alpha^{*}\rangle\langle\alpha^{*}|\,, \tag{18}$$

as the spoofer has probability $\gamma$ of concluding that the state encoded in the pulse was the squeezed state $|\varphi\rangle = |\Psi(\alpha,\zeta)\rangle$, and attempting to spoof with the state $|\alpha\rangle = |\Psi(\alpha,0)\rangle$, which maximizes the overlap with the squeezed states. Similarly, the spoofer has probability $1-\gamma$ to conclude that the state was $|\xi\rangle = |\Psi(\alpha^{*},\zeta^{*})\rangle$ and respond with $|\alpha^{*}\rangle = |\Psi(\alpha^{*},0)\rangle$.

These hypotheses and Eq. (4) give rise to a success probability $\bar{P}_s$ without the upper bound introduced in the previous section. The success probability can also be derived analytically, as shown in the Appendix. In Fig. 4 we corroborate this by plotting the success probability $\bar{P}_s$ as a function of the prior probability $p$ for fixed values of the squeezing coefficient $r$ and an average number of photons $n = 100$. By changing $\phi$ and $\theta$, we vary the position of the states in phase space and the direction of the squeezing in each calculation to maximize the success probability. We observe that the upper bound for $\bar{P}_s$ calculated in the previous section is broken when employing squeezed states. As we show, the higher the squeezing parameter, the higher the probability of detecting spoofing. Indeed, Fig. 4 demonstrates that there is no upper bound for the success probability $\bar{P}_s$, and it is possible to detect spoofing with absolute accuracy for a sufficiently high squeezing parameter.

It is constructive to consider a scenario where some spoofers can generate squeezing while others cannot. It turns out that it is possible to optimize the success probability for both cases simultaneously, independently of the ability of spoofers to generate squeezing. To demonstrate this, we plot in Fig. 5 the maximum success probability for both versions of the problem as a function of $r$ for different numbers of photons. To simultaneously optimize both cases, we vary $\phi$ and $\theta$ for each value $n$ and $r$. As Fig. 5(a) shows, $\bar{P}_s$ converges to the unity as the squeezing increases independently of the number of photons. Indeed, if the number of photons is high enough, the curves coincide. We observe differences between

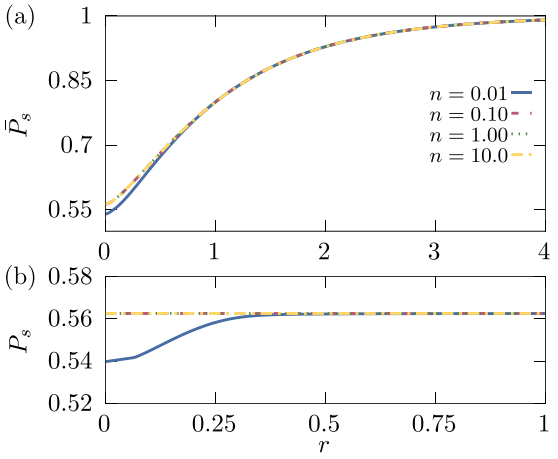


FIG. 5. Success probability as a function of the squeezing coefficient for various numbers of photons while the prior probability is $p = 0.5$. Here (a) shows the success probability when the spoofer can only generate coherent states, and (b) shows the results for the case where we remove that limitation on the spoofer capability. The states are optimized to simultaneously maximize the probability of success in both cases.

the curves for a small number of photons as they coincide with the results from the previous section where the coherent states, $r = 0$, were addressed. On the other hand, Fig. 5(b) shows that this can be done while still saturating the success probability bound for the scenario where the spoofer can generate squeezing (and thus, the overlap must be the optimal one). In the limit $r = 0$, the results coincide as well with those for coherent states discussed in the previous section. In particular, the success probability $P_s$ for $n = 0.01$ photons does not saturate to the optimal value, since the number of photons is below the critical value of 0.072. If the spoofer cannot generate squeezing, a squeezing coefficient of $r \approx 3.9$ is necessary to obtain $\bar{P}_s = 0.99$. That squeezing coefficient corresponds to 34 dB of squeezing, which is outside of the current experimental capabilities [32]. We estimate that current experimental capabilities allow for $\bar{P}_s \approx 0.9$, employing 15 dB of squeezing, which is a substantial improvement with respect to the classical case. We attribute this result to the fact that for a high enough squeezing parameter, the overlap between the squeezed states and the coherent states approaches zero, making it possible to discriminate them with high probability; therefore, the receiver can perfectly identify a spoofer.

## V. CONCLUSION AND OUTLOOK

We investigate a spoofing protocol that encodes arbitrary quantum states in an electromagnetic signal and derive the upper bound for spoofer detection probability. Our analysis reveals quantum enhancement in spoofing detection success probability, stemming from the impossibility of perfectly discriminating nonorthogonal quantum states. We demonstrate that a pair of coherent states can saturate this bound and determine the optimal states analytically. Furthermore, we show that this quantum enhancement persists for an arbitrarily large number of photons when using general coherent states for signal encoding. Notably, this result eliminates the strict requirement for single-photon sources, enabling a proof-of-principle experiment using standard laser sources to showcase quantum mechanics' role in improving spoofing detection [25–27].

Our work seeks to establish fundamental limits for quantum spoofing detection using the Helstrom bound framework, regarded as the most fundamental bound [25,26]. However, other suboptimal bounds, such as direct photon counting [25] or unambiguous state discrimination [14], may yield different limits for quantum spoofing detection.

Our results have significant implications for radar systems [21–23], particularly in scenarios where an airborne target emits spoof pulses to evade tracking by a ground-based radar. We investigate how the spoofer's ability to encode quantum states in the spoofing signal affects the probability of detection. For that purpose we analyze the benefits of using squeezed states. Assuming only the transmitter-receiver can generate nonclassical states like squeezed light [28–30], we show that the detection probability approaches unity, surpassing the coherent-state case. With current experimental capabilities [32], our estimate suggests achieving 90% spoofing detection probability is feasible. However, if the spoofer can also generate squeezing, the advantage of squeezed states over coherent states diminishes as the photon number increases. Nevertheless, exploring more complex entangled states or modifying the encoding protocol could potentially harness quantum correlations to enhance spoofing detection further.

## ACKNOWLEDGMENTS

This research was supported by DEVCOM Army Research Laboratory under Cooperative Agreement No. W911NF-24-2-0044 (S.C.C.). J.A.V. acknowledges support from AFOSR Project No. FA9550-20-1-0189. J.A.V. and J.R. acknowledge partial support from ANID/Fondecyt Grants No. 1240697 and No. 1240655, respectively. The authors thank Jonathan N. Blakely for his helpful discussions of this work.

## APPENDIX: EIGENVALUE CALCULATION FOR THE LIMITED QUANTUM RESOURCES SCENARIO

Analogously to Eq. (4), the success probability $\bar{P}_s$ depends on the eigenvalues of the operator:

$$p\hat{\rho}_2 - (1-p)\hat{\rho}_1 = p(\gamma\,|\alpha\rangle\langle\alpha| + (1-\gamma)\,|\beta\rangle\langle\beta|) - (1-p)\,|\varphi\rangle\langle\varphi|\,. \tag{A1}$$

Any eigenvector with a nonzero eigenvalue must be part of the subspace defined by $|\alpha\rangle$, $|\beta\rangle$, and $|\varphi\rangle$. Thus, we can represent the previously introduced operator as a matrix in this subspace. The eigenvalues $\eta$ of that matrix satisfy

$$\begin{vmatrix} p\gamma - \eta & p\gamma\,\langle\alpha|\beta\rangle & p\gamma\,\langle\alpha|\varphi\rangle \\ p(1-\gamma)\,\langle\beta|\alpha\rangle & p(1-\gamma) - \eta & p(1-\gamma)\,\langle\beta|\varphi\rangle \\ -(1-p)\,\langle\varphi|\alpha\rangle & -(1-p)\,\langle\varphi|\beta\rangle & -(1-p) - \eta \end{vmatrix} = 0,$$

or equivalently,

$$a_3\eta^3 + a_2\eta^2 + a_1\eta + a_0 = 0,$$

where

$$\begin{aligned}
a_3 &= -1,\\
a_2 &= 2p - 1,\\
a_1 &= p(-p\gamma + p\gamma^2 - p + 1) + p^2\gamma(1-\gamma)|\langle\alpha|\beta\rangle|^2\\
&\quad - p(1-\gamma)(1-p)|\langle\beta|\varphi\rangle|^2 - p\gamma(1-p)|\langle\alpha|\varphi\rangle|^2,\\
a_0 &= p^2\gamma(1-\gamma)(1-p)(|\langle\alpha|\beta\rangle|^2 + |\langle\beta|\varphi\rangle|^2 + |\langle\alpha|\varphi\rangle|^2\\
&\quad - 1 - 2\,\mathrm{Re}\{\langle\beta|\varphi\rangle\langle\varphi|\alpha\rangle\langle\alpha|\beta\rangle\}).
\end{aligned}$$

Finally, the overlap between squeezed coherent states can be evaluated using [33]

$$\begin{aligned}
&\langle\Psi(\alpha_1,\zeta_1)|\Psi(\alpha_2,\zeta_2)\rangle\\
&\quad = \frac{1}{\sqrt{\sigma_{21}}}\exp\left(\frac{\kappa_{21}\kappa_{12}^*}{2\sigma_{21}} + \frac{\alpha_2\alpha_1^* - \alpha_2^*\alpha_1}{2}\right),
\end{aligned}$$

where

$$\sigma_{kl} = \cosh r_k \cosh r_l - e^{i(\theta_k-\theta_l)}\sinh r_k \sinh r_l$$

and

$$\kappa_{kl} = (\alpha_k - \alpha_l)\cosh r_k + (\alpha_k^* - \alpha_l^*)e^{i\theta_k}\sinh r_k.$$


[1] C. W. Helstrom, Quantum detection and estimation theory, J. Stat. Phys. **1**, 231 (1969).

[2] H. Yuen, R. Kennedy, and M. Lax, Optimum testing of multiple hypotheses in quantum detection theory, IEEE Trans. Inform. Theory **21**, 125 (1975).

[3] P. R. Berman and V. S. Malinovsky, *Principles of Laser Spectroscopy and Quantum Optics* (Princeton University Press, Princeton, NJ, 2011).

[4] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, J. Phys. A: Math. Theor. **48**, 083001 (2015).

[5] S. Satyajit, K. Srinivasan, B. K. Behera, and P. K. Panigrahi, Nondestructive discrimination of a new family of highly entangled states in IBM quantum computer, Quantum Inf. Process. **17**, 212 (2018).

[6] Q. Zhuang, Z. Zhang, and J. H. Shapiro, Optimum mixed-state discrimination for noisy entanglement-enhanced sensing, Phys. Rev. Lett. **118**, 040801 (2017).

[7] J. Bergou, E. Feldman, and M. Hillery, Extracting information from a qubit by multiple observers: Toward a theory of sequential state discrimination, Phys. Rev. Lett. **111**, 100501 (2013).

[8] K. Nakahira, K. Kato, and T. S. Usuda, Generalized quantum state discrimination problems, Phys. Rev. A **91**, 052304 (2015).

[9] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, Quantum repeaters based on two species trapped ions, New J. Phys. **21**, 073002 (2019).

[10] D. Fields, J. A. Bergou, M. Hillery, S. Santra, and V. S. Malinovsky, Optimal unambiguous discrimination of Bell-like states with linear optics, Phys. Rev. A **106**, 023706 (2022).

[11] N. Gisin, Quantum cloning without signaling, Phys. Lett. A **242**, 1 (1998).

[12] J. Bae, W.-Y. Hwang, and Y.-D. Han, No-signaling principle can determine optimal quantum state discrimination, Phys. Rev. Lett. **107**, 170403 (2011).

[13] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[14] A. Chefles and S. M. Barnett, Quantum state separation, unambiguous discrimination and exact cloning, J. Phys. A: Math. Gen. **31**, 10097 (1998).

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

[16] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[17] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, Quantum-secured imaging, Appl. Phys. Lett. **101**, 241103 (2012).

[18] B. P. Williams, K. A. Britt, and T. S. Humble, Tamper-indicating quantum seal, Phys. Rev. Appl. **5**, 014001 (2016).

[19] J. Zhao, A. Lyons, A. C. Ulku, H. Defienne, D. Faccio, and E. Charbon, Light detection and ranging with entangled photons, Opt. Express **30**, 3675 (2022).

[20] C. Oh, L. Jiang, and B. Fefferman, Spoofing cross-entropy measure in boson sampling, Phys. Rev. Lett. **131**, 010401 (2023).

[21] J. N. Blakely and S. D. Pethel, Quantum limits to classically spoofing an electromagnetic signal, Phys. Rev. Res. **4**, 023178 (2022).

[22] D. C. Schleher, *Electronic Warfare in the Information Age*, 1st ed. (Artech House, Inc., USA, 1999).

[23] J. N. Blakely, S. D. Pethel, and K. Jacobs, Revealing spoofing of classical radar using quantum noise, Phys. Rev. Res. **6**, 013179 (2024).

[24] P. Senellart, G. Solomon, and A. White, High-performance semiconductor quantum-dot single-photon sources, Nat. Nanotechnol. **12**, 1026 (2017).

[25] R. L. Cook, P. J. Martin, and J. M. Geremia, Optical coherent state discrimination using a closed-loop quantum measurement, Nature (London) **446**, 774 (2007).

[26] C. Wittmann, M. Takeoka, K. N. Cassemiro, M. Sasaki, G. Leuchs, and U. L. Andersen, Demonstration of near-optimal discrimination of optical coherent states, Phys. Rev. Lett. **101**, 210501 (2008).

[27] A. R. Ferdinand, M. T. DiMario, and F. E. Becerra, Multi-state discrimination below the quantum noise limit at the single-photon level, npj Quantum Inf. **3**, 43 (2017).

[28] R. Schnabel, Squeezed states of light and their applications in laser interferometers, Phys. Rep. **684**, 1 (2017).

[29] D. F. Walls, Squeezed states of light, Nature (London) **306**, 141 (1983).

[30] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, Observation of squeezed states generated by four-wave mixing in an optical cavity, Phys. Rev. Lett. **55**, 2409 (1985).

[31] Z. J. Ou, *Quantum Optics for Experimentalists* (World Scientific Publishing Company, Singapore, 2017).

[32] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 db squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency, Phys. Rev. Lett. **117**, 110801 (2016).

[33] K. B. Møller, T. G. Jørgensen, and J. P. Dahl, Displaced squeezed number states: Position space representation, inner product, and some applications, Phys. Rev. A **54**, 5378 (1996).