# Secure Quantum Pattern Communication

Cillian Harney* and Stefano Pirandola†
*Department of Computer Science, University of York, York YO10 5GH, United Kingdom*

(Received 12 April 2021; revised 22 October 2021; accepted 16 December 2021; published 19 January 2022)

We propose a multimode modulation scheme for continuous-variable (CV) quantum communications, which we call quantum pattern encoding. In this setting, classical information can be encoded into multimode patterns of discretely modulated coherent states, which form instances of a communicable image space. Communicators can devise arbitrarily complex encoding schemes that are degenerate and highly nonuniform, such that communication is likened to the task of pattern recognition. We explore initial communication schemes that exploit these techniques and that lead to an increased encoding complexity. We discuss the impact that this has on the role of a near-term quantum eavesdropper; formulating new realistic classes of attacks and secure communication rates.

DOI: 10.1103/PRXQuantum.3.010311

## I. INTRODUCTION

The rapid maturation of the field of quantum communications [1,2] promises to make it one of the first technologies to be featured in the upcoming quantum revolution. By exploiting quantum information-theoretic protocols [3–5], we can assure provably secure communication based on underlying physical principles. Protocols that utilize continuous-variable (CV) quantum systems [6–8] (such as bosonic modes) form a particularly promising area of research [9], due to their high performance, near-term practical feasibility, and potential for large-scale deployment using current telecommunication infrastructures.

There exist a wide variety of protocols derived from CV encodings, many of which rely on a continuous-modulation (Gaussian) of various Gaussian states [10–15]. Over the years, rigorous security proofs have been obtained for these protocols, alongside theoretical and/or experimental evidence of their efficacy [16–18]. However, the study of discretely modulated CV systems is also of significant interest, where finite-dimensional entities are embedded into infinite-dimensional Hilbert spaces [19–24]. Such discrete-modulation schemes present simplifications over Gaussian modulation with regard to state preparation and data processing.

*cth528@york.ac.uk
†stefano.pirandola@york.ac.uk



Alternative modulation schemes can be devised when considering multiple bosonic modes. The use of multimode technologies has been shown to be advantageous in a number of quantum communication settings [25–27], where communicable symbols are encoded into multiple modes, or via repeated channel usage. In Refs. [28–30], the authors study the utility of highly symmetric collections of multimode binary-modulated coherent states, the optimal discrimination of which is easier to obtain globally rather than locally. In this way, highly efficient communication schemes can be based on the packaging of $d$-ary variables into multimode coherent states.

Yet, multimode encoding invites a further abstraction. Let us define a *quantum pattern* as a $m$-mode coherent state undergoing local $k$-ary modulations. It is possible to construct a collection of quantum patterns that belong to a global *image space*, forming a subset of all $k^m$ possible patterns that exist. Each element of this image space can be endowed with a particular classification that encodes a communicable symbol; embedding information not into local modulations but into an abstract classification process associated with pattern features.

This marks a significant departure from any form of encoding used in standard communications. If information can be encoded into conceptual properties of a coherent-pattern space, it is possible to impose extreme classification degeneracies and nonlinearities, aligning the tasks of communication and pattern recognition very closely. Codes can be designed that exploit specific multimode technologies or embed extractable features into vast data sets. Furthermore, the recent integration of modern machine-learning tools within quantum hypothesis testing [31–34] further encourages an application of these methods to quantum communication.

The introduction of quantum pattern encoding also raises interesting questions about realistic eavesdroppers and security. While unconditional security must consider an eavesdropper with unlimited resources, perfect quantum memories and a full working knowledge of the protocol, these assumptions may not realistically hold in the presence of overwhelmingly complex (possibly data-driven) codes. Hence the application of versatile machine-learning enhanced encoders and/or receivers may be used to cast doubt on the knowledge of an attacker and improve communication rates. This makes it nontrivial to consider scenarios of information asymmetry between trusted parties and eavesdroppers. In this work, we explore this asymmetry by devising new weaker classes of eavesdropper attacks that may emerge within the pattern-communication regime.

This paper proceeds as follows. In Sec. II, we explicitly introduce coherent quantum patterns. In Sec. II C, we provide a general approach to studying secure communication, establishing a hierarchy of rates based on eavesdropper resources. In Sec. III, we devise two binary pattern-encoding schemes and illustrate their performance over pure-loss channels. Finally, we provide concluding discussions and possible future investigative paths.

## II. QUANTUM PATTERN COMMUNICATION

### A. Coherent quantum patterns

Let us formally introduce the concept of a *coherent quantum pattern*. This is a discrete ensemble of coherent states that undergo $k$-ary modulation. Let $\boldsymbol{i} = \{i_1, i_2, \ldots, i_m\}$ denote an $m$-length string, where each element of the string is a random variable that can occupy $k$ unique values, $i_j \in \{0, \ldots, k-1\}$. This string (or pattern) can be used to generate a corresponding coherent-pattern state given by

$$|\alpha_{\boldsymbol{i}}\rangle := |\alpha_{i_1}\rangle \otimes |\alpha_{i_2}\rangle \otimes \ldots \otimes |\alpha_{i_m}\rangle = \bigotimes_{j=1}^{m} |\alpha_{i_j}\rangle \,,$$
$$\text{where } |\alpha_{i_j}\rangle \in \{|\alpha_0\rangle, |\alpha_1\rangle, \ldots, |\alpha_{k-1}\rangle\}. \tag{1}$$

For example, if $k = 2$, then we are employing a binary modulation on each local mode. In this case, one can utilize binary-phase-shift keying (BPSK) so that each local coherent state $|\alpha_{i_j}\rangle$ will take the form $|\alpha_{i_j}\rangle \in \{|\sqrt{N_S}\rangle, |-\sqrt{N_S}\rangle\}$; or binary amplitude modulation (BAM), where $|\alpha_{i_j}\rangle \in \{|0\rangle, |\sqrt{N_S}\rangle\}$, where $N_S$ denotes the mean number of photons transmitted in each state [7].

A coherent-pattern state $|\alpha_{\boldsymbol{i}}\rangle$ represents a single state generated by the pattern $\boldsymbol{i}$. However, our goal is to create a basis for quantum communication and we therefore require much more than just a single $\boldsymbol{i}$. To this end, we define *an image space* as a collection of many $k$-ary patterns, which are used to generate a potentially vast collection of coherent-pattern states. More precisely, an $N$-element image space can be used to generate a corresponding collection of coherent-pattern states,

$$\mathcal{U} := \{\boldsymbol{i}_1, \boldsymbol{i}_2, \ldots, \boldsymbol{i}_N\} \to \{|\alpha\rangle_{\boldsymbol{i}}\}_{\boldsymbol{i}\in\mathcal{U}}. \tag{2}$$

This collection of states can then be used to create a basis for quantum communications. For $m$-mode patterns undergoing $k$-ary local modulations, the set of all possible patterns contains $k^m$ elements.

Crucially, coherent patterns can be used to formulate a mapping between a $d$-dimensional alphabet $\mathcal{A} = \{1, \ldots, d\}$, which contains symbols used to construct secret keys, and an image space $\mathcal{U}$. Each pattern $\boldsymbol{i} \in \mathcal{U}$ can be used to represent a symbol from the alphabet, which is the same as assigning a specific classification $c \in \mathcal{A}$ to each pattern. The formal mapping between an image space and an alphabet is described by a code book $\mathcal{C}$, which formally takes the form

$$\mathcal{C} := \left\{ \left(c(\boldsymbol{i}); |\alpha_{\boldsymbol{i}}\rangle\right) \middle| c(\boldsymbol{i}) \in \mathcal{A}, \boldsymbol{i} \in \mathcal{U} \right\}, \tag{3}$$

where $c(\boldsymbol{i}) = c \in \mathcal{A}$ is the classification of a pattern $\boldsymbol{i}$. The alphabet and code book thus completely characterize the pattern-modulation scheme; a sender (Alice) may transmit pattern states to a receiver (Bob) who must then discriminate the incoming pattern and its classification can be inferred by consulting with the shared code book. We may refer to a pattern-encoding setup using the alphabet-and-code-book tuple $(\mathcal{A}, \mathcal{C})$.

The construction of an image space $\mathcal{U}$ is incredibly flexible. It is by no means compulsory that the alphabet and image space are of the same dimension $|\mathcal{A}| = |\mathcal{U}|$, i.e., the encoding need not be a one-to-one mapping between patterns $\boldsymbol{i} \in \mathcal{U}$ and symbols $c \in \mathcal{A}$. In general, each symbol maps to a subset of the image space, $c \mapsto \{\boldsymbol{i} \in \mathcal{B}(c)\} \subset \mathcal{U}$, meaning that an image space can be decomposed according to class-equivalent subsets,

$$\mathcal{U} = \bigcup_{c\in\mathcal{A}} \mathcal{B}(c), \; \mathcal{B}(c) = \{\boldsymbol{i} \in \mathcal{U} | c(\boldsymbol{i}) = c\}. \tag{4}$$

Each subset $\mathcal{B}(c)$ is filled with many potential code words of varying forms; however, they should all possess abstract features that allow them to be classified as belonging to the class $c$. Furthermore, these subsets do not necessarily have a well-defined size but in reality we must possess a finite set of samples from which classifiers can draw expertise. For a $d$-dimensional alphabet, if each class of pattern state is transmitted with equal *a priori* probability $p_c = 1/d$, then the probability of transmitting any single pattern is $p_{c(\boldsymbol{i})} = 1/(d|\mathcal{B}(c(\boldsymbol{i}))|)$. An encoding of this form is called degenerate and is explored in subsequent sections.

### B. Practical aspects

We may consider two realizations of quantum pattern transmissions, corresponding to one-dimensional (1D) and two-dimensional (2D) patterns. This depends entirely on the spatiotemporal configuration in which one is interested. A 1D pattern transmission corresponds to single-shot multimode communications: Alice encodes information into quantum states that are simultaneously transmitted over $m$ spatial modes to Bob. Hence, any symbol is transmitted via the single use of each spatial mode. However, this may be quite restrictive, as the use of large pattern encodings leads to a potentially unfeasible number of spatial modes.

Instead, Alice may perform 2D pattern transmissions, achieved by introducing temporal extensions of each spatial mode; corresponding to multishot communications. Alice and Bob now communicate over a fixed time period of $T$ seconds, discretizing this period into time bins. Alice transmits information sequentially over $m'$ spatial modes and $m''$ temporal modes, such that each transmission point in space and time corresponds to a $k$-ary variable. This allows Alice to construct an $m = (m' \times m'')$ length pattern.

Importantly, any 2D pattern using identical $m'$ spatial modes and $m''$ temporal modes can always be expanded to a 1D pattern with exclusively $m$ spatial modes and vice versa. This is provided through an assumption of uniform channels; if the multichannel is not uniform, then degenerate channels can be pooled together or expanded in a similar way.

### C. Pattern-modulated CV QKD, communication rates, and security

Standard discretely modulated continuous-variable quantum key distribution (CV QKD) uses phase- and/or amplitude-encoded coherent states that form a constellation. Alice randomly generates and transmits coherent states from this constellation to Bob, followed by parameter estimation, privacy amplification, error correction, etc. in order to establish a secret key. In this protocol, the mapping between each discretely modulated coherent state and its binary presentation is *public*. This means that if an attacker (Eve) intercepts a state and correctly discriminates it as a particular coherent state from the constellation, she can correctly extract its binary representation use for key generation.

Quantum pattern communication is a generalized modulation scheme where we possess a mapping between an abstract image space of coherent-pattern states $\{\alpha_i\}_{i\in\mathcal{U}}$ and a set of corresponding symbols, contained in the code book $\mathcal{C}$. The relationship between a quantum pattern and its symbol in the code book may be highly nonlinear and degenerate, as it is encoded into global multimodal features. This produces a communication basis that is used for key distribution, i.e., Alice randomly generates quantum patterns from the image space that are transmitted and discriminated by Bob, followed by the standard CV-QKD steps in order to establish a secret key.

Like many other discretely modulated bosonic communication schemes, evaluating the efficacy (secure communication rate) of pattern-based protocols can be very demanding. In a best-case scenario, we would study information transmission over thermal-loss channels. However, the addition of thermal noise to the already non-Gaussian ensemble of discretely modulated coherent states requires treatment in an infinite-dimensional multimode Fock space that is computationally infeasible. For this reason, we restrict our studies to bosonic pure-loss channels $\mathcal{E}_\eta$, with transmissivity $\eta$ as an initial step in the study of this topic. For the transmission of $m$-mode pattern states, we assume that these channels are uniform, such that $\mathcal{E}_\eta^m := \bigotimes_{j=1}^m \mathcal{E}_\eta$ [35]. Here, we study secure quantum communication rates assuming the use of CV QKD in direct reconciliation. Thus we focus on a one-way sender (Alice) to receiver (Bob) scheme, subject to an eavesdropper (Eve).

Consider the use of an encoding scheme $(\mathcal{A}, \mathcal{C})$ using Eq. (3) over uniform pure-loss channels. In the asymptotic regime of many exchanged signals, we may quantify the performance of a communication protocol through the following secure transmission rate [36,37]:

$$R := I_{AB} - I_{AE}, \tag{5}$$

where $I_{AB}$ is the mutual information between the parties Alice and Bob, while $I_{AE}$ measures Eve's ability to extract information from the protocol (we also assume ideal reconciliation of data for Alice and Bob). The form of $I_{XY}$ for the respective parties depends on multiple factors; in particular, Eve's performance depends directly on the level of threat that she poses.

The maximum amount of classical information accessible to Bob or Eve is upper bounded by their Holevo information. Assuming that all symbols are transmitted with equal *a priori* probability $p_{c(\boldsymbol{i})}$ and defining $\alpha_{\boldsymbol{i}}^\eta := |\eta\alpha_{\boldsymbol{i}}\rangle\langle\eta\alpha_{\boldsymbol{i}}|$, we may write

$$I_{AB} \leq \chi_{AB}(\eta),\ I_{AE} \leq \chi_{AE}(1-\eta), \tag{6}$$

$$\chi(\eta) := S\left(\sum_{\boldsymbol{i}\in\mathcal{U}} p_{c(\boldsymbol{i})}\alpha_{\boldsymbol{i}}^\eta\right) - \sum_{\boldsymbol{i}\in\mathcal{U}} p_{c(\boldsymbol{i})} S(\alpha_{\boldsymbol{i}}^\eta), \tag{7}$$

where $S(\cdot)$ denotes the von Neumann entropy. Eve's maximum potential threat is safely quantified by the Holevo bound $\chi_{AE}$, making communication unconditionally secure provided that $I_{AB} \geq \chi_{AE}$. This bound assumes that Eve applies a beam-splitter attack, followed by perfect storage of the stolen modes in a quantum memory prior to information extraction (an entangling-cloner attack). While this is compulsory to ensure unconditional security, it is not always a realistic assumption on behalf of near-term quantum eavesdroppers.

Pattern encoding introduces a novel twist on traditional security assumptions. Typical quantum communication scenarios (discretely or continuously modulated) embed classical information in such a way that the mapping between quantum states and their classical symbols is either public or reliably inferred by an interceptor. For instance, if Eve intercepts the communications of a four-state phase-encoded protocol, even if *a priori* unknown, the encoding can be easily inferred over a number of transmissions.

If one utilizes pattern encoding, this inference is no longer a trivial assumption but an additional obstacle for Eve to overcome. Alice and Bob either (i) engage in a precommunication secure training protocol in order to construct an effective classifier for an encoding scheme [38,39] or (ii) share a preagreed precise code book to be used for communication. The increased complexity of the encoding scheme means that in a practical setting, it is extremely unlikely that Eve will have, or deduce, perfect knowledge of the code book. This invites a new class of weak but realistic attacks on a pattern-communication protocol, which we label *approximate attacks*. These attacks emerge from asymmetry between the predetermined encoding chosen by Alice and Bob $(\mathcal{A},\mathcal{C})$, and that to which Eve has access, $(\mathcal{A}_E,\mathcal{C}_E)$. In this way, we may establish a new hierarchy of eavesdropper threats, from approximate to collective attacks.

### D. Mutual information

Consider a pattern encoding $(\mathcal{A},\mathcal{C})$, where $\mathcal{C}$ is constructed from some appropriate image space $\mathcal{U}$. Alice transmits a pattern $\boldsymbol{i}_A$ with classification $c(\boldsymbol{i}_A)$. Bob has full knowledge of the encoding scheme and can therefore optimize his (generally quantum) measurements such that any incoming noisy pattern $\boldsymbol{i}_B$ is classified according to a set of optimized positive operator-valued measures (POVMs) $\tilde{\boldsymbol{\Pi}} := \left\{\tilde{\Pi}_{c(\boldsymbol{i})}\right\}_{c(\boldsymbol{i})\in\mathcal{A}}$. Measurements of this form $\tilde{\boldsymbol{\Pi}}$ are designed in such a way that discrimination of the pattern $\boldsymbol{i}\in\mathcal{U}$ and classification $c(\boldsymbol{i})\in\mathcal{A}$ are combined in a cohesive process and may be achieved via fully coherent quantum algorithms. That is, an input pattern would be processed by an optimized quantum circuit followed by some projective measurement onto the assigned class. For highly complex or nonlinear encodings, this task is best addressed by quantum machine learning [40,41].

Yet, in the absence of fully coherent class measurements, this task can be more simply split into quantum pattern discrimination $\boldsymbol{\Pi} := \{\Pi_{\boldsymbol{i}}\}_{\boldsymbol{i}\in\mathcal{U}}$ followed by classical postprocessing via a classifier $\tilde{c}$, such that $\tilde{c}(\boldsymbol{i})\in\mathcal{A}$ denotes the class prediction of a pattern $\boldsymbol{i}$ according to this classifier. Indeed, this classification process aligns itself with near-term realistic resources, providing access to powerful modern pattern-recognition tools. The goal of communication is to maximize the probability that the classifier's prediction of the received pattern is equal to the class of the initial pattern, i.e., $\tilde{c}(\boldsymbol{i}_B)\approx c(\boldsymbol{i}_A)$. Imposing a choice of classifier $\tilde{c}$, the conditional probabilities take the form

$$p_{\tilde{c}}(c_B|c_A) = \sum_{\boldsymbol{i}_A\in\mathcal{B}(c_A),\boldsymbol{i}_B\in\mathcal{B}(c_B)} p_{\tilde{c}}(c_B|\boldsymbol{i}_B)\mathrm{Tr}\left[\Pi_{\boldsymbol{i}_B}\alpha^{\eta}_{\boldsymbol{i}_A}\right], \quad (8)$$

$$p_{\tilde{c}}(c_A|c_B) = \frac{p_{\tilde{c}}(c_A,c_B)}{p_{\tilde{c}}(c_B)} = \frac{p_{\tilde{c}}(c_B|c_A)}{\sum_{c_A\in\mathcal{A}}p_{\tilde{c}}(c_B|c_A)}, \quad (9)$$

where the second line follows from Bayes theorem.

Assuming that a pattern class is transmitted with a probability equal to that of any other class, the mutual information between Alice and Bob then takes the form

$$I^{\boldsymbol{\Pi},\tilde{c}}_{AB}(\eta) = \log(|\mathcal{A}|) + \sum_{c_A,c_B\in\mathcal{A}} p_{\tilde{c}}(c_A,c_B)\log[p_{\tilde{c}}(c_A|c_B)]. \quad (10)$$

Throughout this work, log is taken as base 2. This quantifies Alice's and Bob's information retrieval given Bob's perfect knowledge of the encoding and the split measurement-classification process using the POVM set $\boldsymbol{\Pi}$ and the statistical classifier $\tilde{c}$. It also provides an alternative way to upper bound the mutual information in the absence of coherent class measurements,

$$I_{AB} \le \max_{\boldsymbol{\Pi},\tilde{c}}\left(I^{\boldsymbol{\Pi},\tilde{c}}_{AB}\right) \le \max_{\tilde{\boldsymbol{\Pi}}}\left(I^{\tilde{\boldsymbol{\Pi}}}_{AB}\right) \le \chi_{AB}. \quad (11)$$

When a one-to-one encoding is used, pattern classifications and the patterns themselves are equivalent and, therefore, Eq. (10) simplifies without the need for a classifier.

### E. Security hierarchy

We are now in a position to develop a security hierarchy. Consider communication such that Alice and Bob utilize an encoding $(\mathcal{A},\mathcal{C})$, achieving the realistic transmission rate in Eq. (10). We now introduce an eavesdropper with a (potentially different) encoding $(\mathcal{A}_E,\mathcal{C}_E)$. Enhanced security hinges on the asymmetry between these and we discuss this hierarchy in order of decreasing threat.

As discussed, unconditional security is guaranteed through the assumption of Eve's access to quantum memories and perfect knowledge of the encoding such that $(\mathcal{A}_E,\mathcal{C}_E)=(\mathcal{A},\mathcal{C})$. In this general setting of collective attacks and perfect knowledge, the rate can be lower bounded according to

$$R_{\mathrm{coll}} = I^{\boldsymbol{\Pi},\tilde{c}}_{AB}(\eta) - \chi_{AE}(1-\eta). \quad (12)$$

Hence, under collective attacks, communication is only secured via high transmissivity, $\eta > 0.5$ [1]. A more realistic rate for near-term technologies (but less secure) is achieved by removing Eve's ability to extract the accessible information. Granting Bob and Eve identical measurement apparatus and classifiers $(\mathbf{\Pi}_B, \tilde{c}_B) = (\mathbf{\Pi}_E, \tilde{c}_E) = (\mathbf{\Pi}, \tilde{c})$, then we may consider a rate proposed by individual attacks,

$$R_{\text{ind}} = I_{AB}^{\mathbf{\Pi},\tilde{c}}(\eta) - I_{AE}^{\mathbf{\Pi},\tilde{c}}(1-\eta) \geq R_{\text{coll}}. \tag{13}$$

Bob's and Eve's performances are symmetric with respect to transmissivity; therefore, secure communication is limited to $\eta \geq 0.5$ [1].

We may consider weaker classes of attacks by removing this symmetry. There exist scenarios where Eve will not possess perfect knowledge of the encoding scheme, $(\mathcal{A}_E, \mathcal{C}_E) \neq (\mathcal{A}, \mathcal{C})$, due to the complexity of the pattern-communication regime. This can be hugely detrimental to Eve, as even minute inaccuracies in her code book or alphabet can have a significant impact on her information retrieval. Generally, Eve's ignorance of the correct encoding leads to a code book of the form

$$\mathcal{C}_E = \left\{ \left[ c(\boldsymbol{i}); |\alpha_{\boldsymbol{i}}\rangle \right] \middle| c(\boldsymbol{i}) \in \mathcal{A}_E, \boldsymbol{i} \in \mathcal{U}_E \right\}, \tag{14}$$

where $\mathcal{U}_E \neq \mathcal{U}$ is a suboptimal image space of *potential* pattern states and may be larger or smaller than $\mathcal{U}$, depending on the scenario. We define an *approximate attack* as an individual attack by an eavesdropper who possesses only partial knowledge of the encoding. We denote approximate attack rates using $\tilde{R}$ and once more progress in order of decreasing threat.

Consider a degenerate encoding scheme $(\mathcal{A}, \mathcal{C})$ and an approximate attack in which Eve is aware of the alphabet-to-code-book mapping but possesses a suboptimal image space of potential patterns. That is, $\mathcal{A}_E = \mathcal{A}$, but for the image space

$$\mathcal{U}_E = \bigcup_{c \in \mathcal{A}} \mathcal{B}_E(c), \exists c \in \mathcal{A} \text{ s.t } |\mathcal{B}_E(c)| < |\mathcal{B}(c)|, \tag{15}$$

where $\mathcal{B}(c)$ are subspaces of class-equivalent patterns as in Eq. (4). That is, Eve is missing potential elements of the degenerate image space. In the limit of maximum ignorance, Eve possesses only one example of each class code word $|\mathcal{B}_E(c)| = 1, \forall c \in \mathcal{A}$. Since Eve is still knowledgeable of the encoding, she may optimize her measurement apparatus $(\mathbf{\Pi}_E = \mathbf{\Pi})$. But the diminished image space renders her classifier $\tilde{c}_E$ inferior with respect to Bob's, since there is less expertise to draw from the reduced image space $\mathcal{U}_E$. More formally, Eve's expected error rate of classification over a set of pattern transmissions $\boldsymbol{i} \in \mathcal{V}$ may be substantially worse than Bob's:

$$\mathbb{E}_{\mathcal{V}} \left\{ p \left[ c(\boldsymbol{i}) | \boldsymbol{i}, \mathcal{U}_E \right] \right\} < \mathbb{E}_{\mathcal{V}} \left[ p \left( c(\boldsymbol{i}) | \boldsymbol{i}, \mathcal{U} \right) \right]. \tag{16}$$

We label this as a *diminished approximate attack*, leading to the new rate

$$\tilde{R}_{\text{dim}} = I_{AB}^{\mathbf{\Pi},\tilde{c}}(\eta) - I_{AE}^{\mathbf{\Pi},\tilde{c}_E}(1-\eta) \geq R_{\text{ind}}. \tag{17}$$

To summarize, this is a form of individual attack in which Eve's resources limit her ability to optimize a classifier. For one-to-one pattern encodings, there exists only one example of each class code word anyway; hence this attack is no longer approximate and $\tilde{R}_{\text{dim}} = R_{\text{ind}}$.

The previous attack assumes that Eve still retains knowledge of the code word to symbol mapping; however, for larger code spaces and alphabets, it is possible to construct pattern embeddings that are close to indistinguishable from other codes. This makes code-book and/or alphabet inference extremely difficult. Consider an approximate attack such that Eve is in possession of suboptimal image space that is larger than Alice's and Bob's $\mathcal{U} \subset \mathcal{U}_E$ and must use this to infer the correct encoding to retrieve any information. Since $\mathcal{U}_E$ is larger than $\mathcal{U}$, it contains potentially invalid patterns, meaning that $\mathbf{\Pi}_E$ and $\tilde{c}_E$ will also become suboptimal. Furthermore, the attack is now probabilistic, since there is a chance that she will infer an incorrect encoding. Given that Eve can successfully learn $(\mathcal{A}, \mathcal{C})$ with some probability $p_{\text{dec}}$, we obtain the rate

$$\tilde{R}_{\text{pr}} = I_{AB}^{\mathbf{\Pi},\tilde{c}}(\eta) - p_{\text{dec}} \left[ I_{AE}^{\mathbf{\Pi}_E,\tilde{c}_E}(1-\eta) \right] \geq R_{\text{ind}}. \tag{18}$$

This is a *probabilistic approximate attack* and it describes a situation in which code-word-to-alphabet mappings cannot be trivially obtained by an eavesdropper. For large multimode encodings, $p_{\text{dec}}$ can be made extremely small, depending on how much encoding information has been leaked to Eve. This formulates our weakest class of attack for pattern communications, allowing for the hierarchy

$$R_{\text{coll}} \leq R_{\text{ind}} \leq \tilde{R}_{\text{dim}} \leq \tilde{R}_{\text{pr}}. \tag{19}$$

## III. PATTERN-ENCODING SCHEMES

In this section, we offer a pair of simple introductory examples of binary-pattern-modulated quantum communications, setting $k = 2$ and utilizing BPSK to construct our coherent-pattern bases. That is, we construct $m$-mode coherent quantum patterns $|\alpha_{\boldsymbol{i}}\rangle = \bigotimes_{j=1}^m |\alpha_{i_j}\rangle$ using a local binary modulation on each mode, such that each local coherent state is attributed to a *background state* so that $i_j = 0$ and $|\alpha_0\rangle = |-\sqrt{N_S}\rangle$, or a *target state* so that $i_j = 1$ and $|\alpha_1\rangle = |\sqrt{N_S}\rangle$. We illustrate how the abstraction to global encoding can severely impact the threat of a near-term eavesdropper, studying the hierarchy of rates depicted in Eq. (19).

### A. Localized-TPF pattern modulation

It is known that the discrimination of ensembles of quantum states with geometrical uniform symmetry (GUS) can be enhanced through the use of joint quantum measurements [42]. An ensemble of quantum states $\{p_i;\rho_i\}_{i=1}^n$ (a collection of states $\rho_i$, each of which occurs with probability $p_i$) possesses GUS if $p_i = 1/n$ and there exists a set of symmetry unitaries $\{S_i\}_{i=1}^n$ that can transform each state $\rho_i$ into another state from the ensemble, $\rho_i = S_i\rho_0 S_i^\dagger$ and $S_0 = I$, where $I$ is the identity. In the case of GUS ensembles of pure coherent states, "pretty good measurements" (PGMs) have been proven to be optimal discriminatory measurements [30]. This means that GUS ensembles of coherent states transmitted through pure-loss channels (which retain the purity of input states $\mathcal{E}_\eta(|\alpha\rangle\langle\alpha|) = |\eta\alpha\rangle\langle\eta\alpha|$) can be optimally discriminated via PGMs.

Motivated by this fact, and inspired by the channel-position-finding (CPF) formalism developed for quantum channel discrimination [43], here we introduce the concept of $k$-target position finding ($k$-TPF). This is an encoding scheme based on the use of image spaces $\mathcal{U}_{\text{TPF}}^{m,k}$ that describe the set of all $m$-length binary patterns that possess exactly $k$-target modulated states. For example, if $k = 1$, then the image space $\mathcal{U}_{\text{TPF}}^{m,1}$ denotes the ensemble of $m$-mode coherent states with a single target state, against a backdrop of $(m-1)$ background states. For an explicit example, take $m = 3$; we could then construct the image spaces

$$\mathcal{U}_{\text{TPF}}^{3,1} := \{\{1,0,0\},\{0,1,0\},\{0,0,1\}\}, \tag{20}$$

$$\mathcal{U}_{\text{TPF}}^{3,2} := \{\{1,1,0\},\{1,0,1\},\{0,1,1\}\}. \tag{21}$$

This form of image space can be used to generate GUS coherent-pattern ensembles for communication between Alice and Bob, as explored in Ref. [28].

#### *1. Pattern-modulation scheme*

We may now outline a potential pattern-modulation scheme over uniform $m$-length multichannels. Alice and Bob wish to globally encode information onto their $m$-mode patterns by means of two characteristics; locality and TPF properties (number of target modes). Any $m$-mode coherent pattern can be divided into an $n$-partite locality structure that identifies particular regions of the pattern state that will have specific characteristics. This partitioning can be described by a disjoint partition set $\mathcal{S}$ that collects specific modes within the pattern. More precisely, we can construct this disjoint partition set as

$$\mathcal{S} = \{\boldsymbol{s}_1,\boldsymbol{s}_2,\ldots,\boldsymbol{s}_n\} = \bigcup_{j=1}^{n}\{\boldsymbol{s}_j\}, \tag{22}$$

$$1 \le |\boldsymbol{s}_j| \le m, \text{ and } \boldsymbol{s}_j \cap \boldsymbol{s}_k = \varnothing,\ \forall j \ne k. \tag{23}$$

Importantly, $\{1,\ldots,m\} \subseteq \mathcal{S}$, meaning that all $m$ modes are accounted for in the locality structure. Meanwhile, Eq. (24) ensures that only mode labels from 1 to $m$ are considered and that all subcollections of modes $\boldsymbol{s}_j$ are pairwise disjoint.

Concurrently, Alice and Bob can assign a $k$-TPF property to each subcollection of modes. They may construct a $k$-TPF partition set $\mathcal{K}$ that informs them of how many target modulated states are permitted within any particular subregion of the quantum pattern state specified by $\mathcal{S}$. This partition set takes the form

$$\mathcal{K} = \{k_1,\ldots,k_j,\ldots,k_n\},\quad k_j \in \{1,\ldots,|\boldsymbol{s}|_j - 1\}. \tag{24}$$

This then ensures that a given subpattern $\boldsymbol{s}_j$ will contain exactly $k_j$ target modes. Note that $k_j \in \{1,\ldots,|\boldsymbol{s}|_j - 1\}$ ensures that at least a binary variable is encoded into each subpattern. Finally, Alice and Bob can impose a cardinality condition on their choice of target numbers in each subregion. Letting $C_n^k = n!/k!(n-k)!$ be the binomial coefficient, then they may impose the condition

$$C_{|\boldsymbol{s}_1|}^{k_1} \times C_{|\boldsymbol{s}_2|}^{k_2} \times \ldots \times C_{|\boldsymbol{s}_n|}^{k_n} = \prod_{j=1}^{r} C_{|\boldsymbol{s}_j|}^{k_j} = \Sigma, \tag{25}$$

to ensure that they can communicate exactly $\Sigma$ bits per global transmission.

A global image space can thus be constructed according to

$$\mathcal{U}_{\text{TPF}}^{\mathcal{S},\mathcal{K}} = \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}|_1,k_1} \cup \ldots \cup \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}|_n,k_n} = \bigcup_{j=1}^{n} \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}|_j,k_j}, \tag{26}$$

as a concatenation of all the $k_j$-TPF image spaces of each subpattern. Hence, we can define a one-to-one encoding in conjunction with these partition sets, with a $\Sigma$-dimensional alphabet $\mathcal{A} = \{1,\ldots,\Sigma\}$ and the following code book:

$$\mathcal{C} = \left\{\left(c;|\alpha_{\boldsymbol{i}}\rangle\right)\middle| c \in \mathcal{A}, \boldsymbol{i} \in \mathcal{U}_{\text{TPF}}^{\mathcal{S},\mathcal{K}}\right\}. \tag{27}$$

We label this a *localized-target position-finding* (LTPF) encoding scheme. Given this information, Bob can *always* optimize his measurement apparatus using optimal POVMs over specific subpatterns of the global message, in order to discriminate and decode the transmission. Let us define $\{\Pi_{\boldsymbol{i}}^{m,k}\}_{\boldsymbol{i}\in\mathcal{U}_{\text{TPF}}^{k}}$ as the optimal set of PGMs for discriminating an $m$-mode $k$-TPF pure-state ensemble. Then, for an $(\mathcal{S},\mathcal{K})$ encoding scheme, we utilize the following

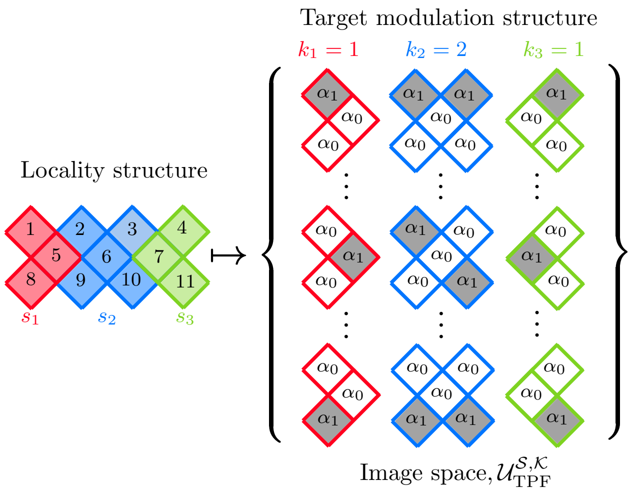


FIG. 1. The LTPF modulation scheme using $m$-mode coherent quantum patterns. This illustrates an example for $m = 11$, where the locality structure is described by a disjoint collection of modes $\mathcal{S} = \{\{1, 5, 8\}, \{2, 3, 6, 9, 10\}, \{4, 7, 11\}\}$ and an associated $k$-TPF property assigned to each collection of modes, where $\mathcal{K} = \{1, 2, 1\}$. This means that the subset $\boldsymbol{s}_1$ will always have $k_1 = 1$ target modulated states within its pattern region, $\boldsymbol{s}_2$ will have $k_2 = 2$, and $\boldsymbol{s}_2$ will have $k_3 = 1$. An image space $\mathcal{U}_{\mathrm{TPF}}^{\mathcal{S},\mathcal{K}}$ can then be generated according to these properties. The vast space of possible configurations puts Eve at a disadvantage if she cannot determine the precise modulation scheme.

set of optimal POVMs:

$$\boldsymbol{\Pi}^{\mathcal{S},\mathcal{K}} = \{\Pi_{\boldsymbol{i}}\}_{\boldsymbol{i} \in \mathcal{U}_{\mathrm{TPF}}^{\mathcal{S},\mathcal{K}}}, \; \Pi_{\boldsymbol{i}}^{\mathcal{S},\mathcal{K}} = \bigotimes_{j=1}^{n} \Pi_{\boldsymbol{i}^{s_j}}^{|\boldsymbol{s}_j|,k_j}, \tag{28}$$

where $\boldsymbol{i}^{s_j}$ denotes the subpattern corresponding to the modes contained in the $j^{\text{th}}$ partition, $\boldsymbol{s}_j$ [for an example of this communication setup, see Fig. 2(a)].

As an example, let us consider Fig. 1(a). This depicts an $m = 11$ mode coherent-pattern space with a specific tripartite locality structure $\mathcal{S} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3\}$, where $|\boldsymbol{s}_1| = |\boldsymbol{s}_3| = 3$ and $|\boldsymbol{s}_2| = 5$. We can attribute a $k$-TPF property to each of these subregions, which will inform Bob how many target modulated modes he should expect within each subregion. If this information can be concealed from Eve, then secure rates can be enhanced by encoding information asymmetry.

### 2. Secure rates

Measurement outcome probabilities can be assessed for PGMs by means of Gram matrices. Here, we define $G[\mathcal{U}]$ as the Gram matrix of an ensemble of lossy coherent-pattern states that form the image space $\mathcal{U}$:

$$G[\mathcal{U}]_{\boldsymbol{i},\boldsymbol{i}'} = \langle \eta\alpha_{\boldsymbol{i}} | \eta\alpha_{\boldsymbol{i}'} \rangle, \; \boldsymbol{i}, \boldsymbol{i}' \in \mathcal{U}. \tag{29}$$

The square root of the Gram matrix of a pure-state ensemble can be used to derive conditional probabilities of PGM measurement outcomes. For local subpatterns of transmission states,

$$p(\boldsymbol{i}_B^{s_j} | \boldsymbol{i}_A^{s_j}) = \left\{ \left[ \sqrt{G(\mathcal{U}_{\mathrm{TPF}}^{|s_j|,k_j})} \right]_{\boldsymbol{i}_A^{s_j} \boldsymbol{i}_B^{s_j}} \right\}^2. \tag{30}$$

Using Bayes theorem to find the converse conditional probabilities $p(\boldsymbol{i}_A^{s_j} | \boldsymbol{i}_B^{s_j})$, the conditional probability of Alice having transmitted a global pattern $\boldsymbol{i}_A$ given that Bob reconstructed the global pattern $\boldsymbol{i}_B$ is given by

$$p(\boldsymbol{i}_A | \boldsymbol{i}_B) = p\left( \bigcap_{j=1}^{n} \boldsymbol{i}_A^{s_j} \middle| \bigcap_{j=1}^{n} \boldsymbol{i}_B^{s_j} \right) = \prod_{j=1}^{n} p(\boldsymbol{i}_A^{s_j} | \boldsymbol{i}_B^{s_j}). \tag{31}$$

The mutual information can then be computed as

$$I_{AB}^{\boldsymbol{\Pi}^{\mathcal{S},\mathcal{K}}} := \log \Sigma + \sum_{\boldsymbol{i}_A, \boldsymbol{i}_B \in \mathcal{U}_{\mathrm{TPF}}^{\mathcal{S},\mathcal{K}}} p(\boldsymbol{i}_A, \boldsymbol{i}_B) \log [p(\boldsymbol{i}_A | \boldsymbol{i}_B)]. \tag{32}$$

This allows us to write the secure communication rates from Eqs. (12) and (13), under collective and individual

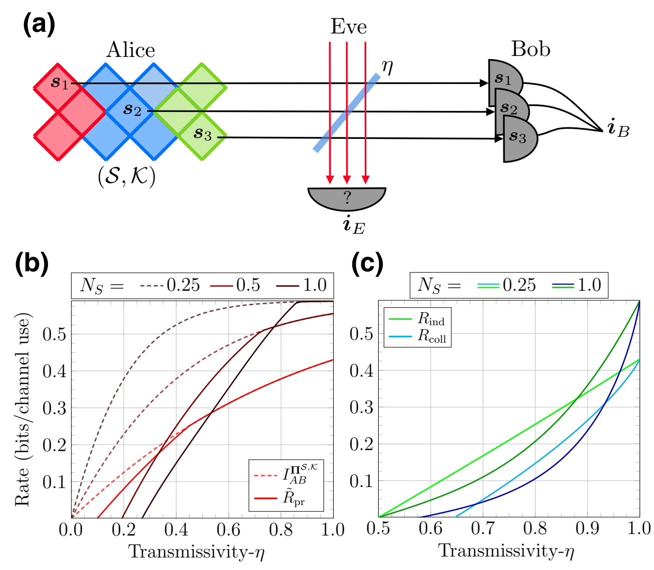


FIG. 2. (a) An illustration of LTPF pattern communication using the encoding scheme $(\mathcal{S}, \mathcal{K}) = (\{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3\}, \{1, 2, 1\})$ described in Fig. 1. (b) A description of the behavior with respect to transmissivity of the optimized mutual information between Alice and Bob (dashed) and the secure communication rate under probabilistic attacks $\tilde{R}_{\mathrm{pr}}$ (solid). (c) A description of secure communication rates from Eqs. (33)–(34) considering nonapproximate attacks, in which Eve possesses information and resources that are as good or better than those of Alice and Bob.

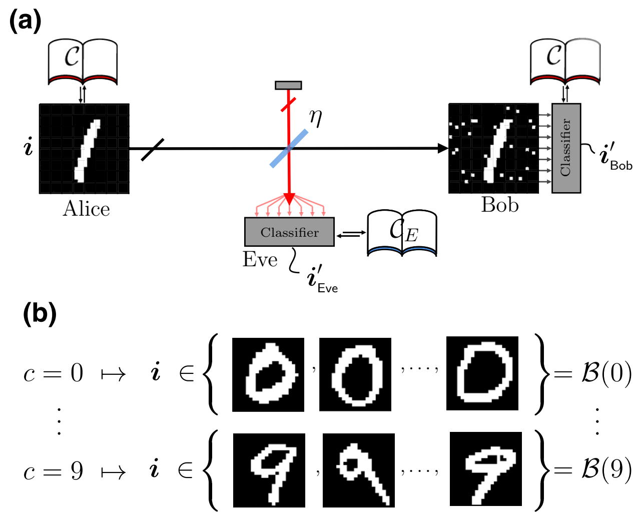


FIG. 3. (a) A description of pattern communication using a degenerate code book. Alice and Bob possess some degenerate code book $\mathcal{C}_{AB}$, while Eve possesses a potentially inferior code book $\mathcal{C}_E \subseteq \mathcal{C}_{AB}$. Local measurements are employed in conjunction with a classifier. (b) An example of degenerate coding using the MNIST handwritten-digit data set, with $d \in \{0, \ldots, 9\}$ symbols encoded into coherent patterns that explicitly "draw" these digits.

attacks, respectively:

$$R_{\text{coll}} = I_{AB}^{\mathbf{\Pi}^{\mathcal{S},\mathcal{K}}}(\eta) - \chi_{AE}(1-\eta), \tag{33}$$

$$R_{\text{ind}} = I_{AB}^{\mathbf{\Pi}^{\mathcal{S},\mathcal{K}}}(\eta) - I_{AE}^{\mathbf{\Pi}^{\mathcal{S},\mathcal{K}}}(1-\eta). \tag{34}$$

These rates assume that Eve has full knowledge of the encoding scheme $(\mathcal{S}, \mathcal{K})$ and can be seen in Fig. 2(c) for the specific encoding $(\mathcal{S}, \mathcal{K}) = (\{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3\}, \{1, 2, 1\})$. These rates are, of course, secure for $\eta \gtrsim 0.5$.

When considering a large number of modes $m$, there is a superexponentially increasing number of ways in which $\mathcal{S}$ and $\mathcal{K}$ can be chosen (see Appendix B2). Therefore, it is nontrivial to consider a scenario in which Eve is not in full possession of this code book, due to its highly degenerate characteristics.

The most threatening approximate attack is probabilistic and is a situation in which Eve has deduced $\mathcal{S}$ (the locality structure) but is unaware of $\mathcal{K}$ (the TPF of each subpattern). In this case, Eve must optimize her measurement apparatus in order to comply with $\mathcal{S}$ but without imposing any bias on $\mathcal{K}$. If she is biased, then she risks utilizing an image space that is missing essential code words from the real code book. Therefore, her best strategy is to utilize a larger potential image space that is compliant with $\mathcal{S}$; then Eve should assume that the number of target states that she measures in each subpattern is consistent with the real $\mathcal{K}$. That is, Eve must infer $\mathcal{K}$ directly from her measurements. Hence, Eve constructs an image space that is a concatenation of all $\mathcal{S}$-locality adhering patterns:

$$\mathcal{U}_{\text{TPF}}^{\mathcal{S}} = \bigcup_{j=1}^{n} \left( \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,1} \cup \ldots \cup \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,|\boldsymbol{s}_j|-1} \right). \tag{35}$$

Eve's image space (and thus the coherent-state ensemble) no longer satisfies GUS since the $k$-TPF properties of each pattern region are now variable. However, she may still use PGMs, as the requirement that the $k$-TPF property of each pattern region falls within $k_j \in \{1, \ldots, |\boldsymbol{s}_j| - 1\}$ means that she can rule out *some* invalid patterns, allowing her to outperform local measurements. Eve's measurement operators are thus

$$\mathbf{\Pi}^{\mathcal{S}} = \{\Pi_{\boldsymbol{i}}\}_{\boldsymbol{i} \in \mathcal{U}_{\text{TPF}}^{\mathcal{S}}}, \quad \Pi_{\boldsymbol{i}}^{\mathcal{S}} = \bigotimes_{j=1}^{n} \Pi_{\boldsymbol{i}^{\boldsymbol{s}_j}}^{|\boldsymbol{s}_j|,\{1,\ldots,|\boldsymbol{s}_j|-1\}}. \tag{36}$$

To analyze Eve's maximum mutual information, we can use Gram matrices in accordance with the suboptimal image space from Eq. (35), such that

$$I_{AE}^{\mathbf{\Pi}^{\mathcal{S}}} := \log \Sigma + \sum_{\boldsymbol{i}_A \in \mathcal{U}_{\text{TPF}}^{\mathcal{S},\mathcal{K}}, \boldsymbol{i}_E \in \mathcal{U}_{\text{TPF}}^{\mathcal{S}}} p(\boldsymbol{i}_A, \boldsymbol{i}_E) \times \log [p(\boldsymbol{i}_A | \boldsymbol{i}_E)]. \tag{37}$$

Eve's unbiased strategy means that she may still discriminate patterns that do not exist within the correct code book, leading to the inferior conditional entropy term above.

Furthermore, Eve will only obtain this information $I_{AE}^{\mathbf{\Pi}^{\mathcal{S}}}$ probabilistically, since it relies on her ability to correctly infer the $k$-TPF properties of the pattern space, $\mathcal{K}$. The probability of successful inference can also be computed via the Gram matrices of all the potential $k$-TPF subpattern ensembles, which we label $p_{\text{dec}}^{\mathcal{K}|\mathcal{S}}$ (see Appendix A). Ultimately, her approximate attack results in the following secure communication rate:

$$\tilde{R}_{\text{pr}} = I_{AB}^{\mathbf{\Pi}^{\mathcal{S},\mathcal{K}}}(\eta) - p_{\text{dec}}^{\mathcal{K}|\mathcal{S}} \left[ I_{AE}^{\mathbf{\Pi}^{\mathcal{S}}}(1-\eta) \right]. \tag{38}$$

Note that Eve's nonbiased approach is much more effective than any guessing-type scheme, since the number of ways in which Eve could choose $\mathcal{K}$ for large $m$ would quickly force $p_{\text{dec}}^{\mathcal{K}|\mathcal{S}} \to 0$.

Results for $\tilde{R}_{\text{pr}}$ are shown in Fig. 2(b). The undesirable contribution of invalid pattern states in $\mathcal{U}_{\text{TPF}}^{\mathcal{S}}$ clearly degrades Eve's information retrieval, resulting in a secure rate over much larger transmissivity intervals. These secure regions may be as low as $\eta \sim 0.1$ for signal energies $N_S = 0.25$. As the mean photon number $N_S$ is increased, Eve's inference abilities improve, causing the protocol to once more become less secure at lower transmissivities.

### B. Degenerate encoding and pattern recognition

The previous pattern-modulation-scheme example utilizes a one-to-one encoding, attempting to exploit information asymmetry between Bob and Eve in order to obtain superior discriminatory measurements. In the following, we take a data-driven approach in which information is packaged through classifiable degenerate patterns. It is then meaningful to consider a diminished approximate attack, such that overwhelming amounts of data have forced Eve into a limited resource position.

#### *1. Pattern-modulation scheme*

As an example, we use the MNIST data set to construct a degenerate pattern-encoding method. This contains a data set of $m = 28 \times 28$ pixel images $\boldsymbol{i}$, which can be classified as a decimal handwritten digit, formulating a ten-symbol alphabet $\mathcal{A} = \{0, \ldots, 9\}$. The typical data set is gray scale but the images can be polarized so as to represent the modulation of a binary-coherent-state basis. Here, we utilize the MNIST training set $\mathcal{T} = \{c_j; \boldsymbol{i}_j\}_j$ to formulate our code book, which contains an image space of $|\mathcal{T}| = 60\,000$ patterns, each of which has been prelabeled with an exact classifier, $c$. Clearly, $|\mathcal{T}| \gg \mathcal{A}$, leading to a vastly degenerate code book:

$$\mathcal{C} = \left\{ \left( c(\boldsymbol{i}); |\alpha_{\boldsymbol{i}}\rangle \right) \middle| [c(\boldsymbol{i}]; \boldsymbol{i}) \in \mathcal{T} \right\}. \tag{39}$$

The modulation scheme proceeds as follows. Symbols can be encoded by "drawing" a handwritten digit using binary-modulated coherent states. Alice can randomly generate and transmit these patterns to Bob through multimode pure-loss channels, who then uses a set of measurements $\boldsymbol{\Pi}$ to generate a noisy reconstruction of the pattern. Bob can consult with his code book $\mathcal{C}$ and a (possibly pretrained) classifier $\tilde{c}_{\mathcal{T}}$ (the efficiency of which is dependent on the quality of $\mathcal{T}$) in order to decode the pattern. Simultaneously, we may consider an eavesdropper who applies a global beam-splitter attack to steal information and may offer a variety of security threats based on her resources.

The large number of modes $m = 784$ and the nonuniformity of MNIST patterns makes it very difficult to determine optimal measurements. This, of course, motivates the use of local receivers assisted by statistical classifiers. Hence, we assume that Bob performs local Helstrom measurements (e.g., via a Dolinar receiver [44]), denoting the associated POVM as $\boldsymbol{\Pi}^{\otimes} := \bigotimes_{j=1}^{m} \Pi_{i_j}$. Noisy patterns can be simulated by performing single-pixel bit flips on each mode in a transmitted pattern with probability,

$$p_{\text{err}}^{\text{mode}} = \frac{1 - \sqrt{1 - e^{-\kappa \eta N_S}}}{2}, \tag{40}$$

where $\kappa = 4$ ($\kappa = 1$) for BPSK (BAM).

There is a plethora of potential classifiers that can be used in this communication setting, ranging from simple nearest-neighbor classifiers to more sophisticated convolutional neural networks (CNNs). In this work, we utilize shallow CNNs that act as neural decoders. CNNs are a very popular tool for image processing and pattern recognition, due to their high-performance classification accuracies even amidst noisy inputs, and therefore pose as an excellent model classifier for Bob and/or Eve [31].

#### *2. Secure rates*

The MNIST data set also contains an evaluation set $\mathcal{V} = \{c_k; \boldsymbol{i}_k\}_k$ with $|\mathcal{V}| = 10\,000$ patterns and their precise classification. Importantly, these are completely independent samples from the training set, $\mathcal{V} \cap \mathcal{T} = \varnothing$, and can therefore be used to empirically simulate and evaluate communication over $|\mathcal{V}|$ transmissions.

Let $c_A$ and $c_B$ denote the class of Alice's transmission and the class inferred by Bob's classification procedure, respectively: $c_A, c_B \in \{0, \ldots, 9\}$. The conditional probability of having transmitted a message with classification $c_A$, given that Bob has used a classifier $\tilde{c}$ to infer $c_B$, can be approximated using $\mathcal{V}$:

$$p(c_A|c_B) = \frac{p(c_A, c_B)}{p(c_B)} \approx \frac{\sum_{(c(\boldsymbol{i});\boldsymbol{i}) \in \mathcal{V}} \delta[c(\boldsymbol{i}), c_A] \delta[\tilde{c}_{\mathcal{T}}(\boldsymbol{i}), c_B]}{\sum_{(c(\boldsymbol{i});\boldsymbol{i}) \in \mathcal{V}} \delta[\tilde{c}_{\mathcal{T}}(\boldsymbol{i}), c_B]}, \tag{41}$$

where $\delta$ is a Kronecker delta function $\delta(c_j, c_k) = 1$ if and only if the classifications $c_j = c_k$. Using these approximate probability distributions, we may compute the mutual information between Alice and Bob:

$$I_{AB}^{\boldsymbol{\Pi}^{\otimes}, \tilde{c}_{\mathcal{T}}} \approx \log 10 - \sum_{c_A, c_B \in \mathcal{A}} p(c_A, c_B) \log [p(c_A|c_B)]. \tag{42}$$

This approximates their average mutual information over $|\mathcal{V}|$ transmissions and can be seen in Fig. 4(a).

The role of an eavesdropper can now be investigated. Once again, in a worst-case scenario, Eve may capture and store her share of all incident modes in a quantum memory and extract the accessible information via an optimal collective attack. For such a large degenerate ensemble of quantum states, this is an expensive and potentially unrealistic tactic (certainly for near-term technologies). Furthermore, computation of the Holevo information in this context is extremely demanding for the same reasons and thus we leave this security consideration to future studies [45].

Alternatively, we may consider the impact of individual attacks. In an informationally symmetric setting, Eve is aware of the code-word-to-alphabet mapping and possesses an identical code book $\mathcal{C}_E = \mathcal{C}$. The secure

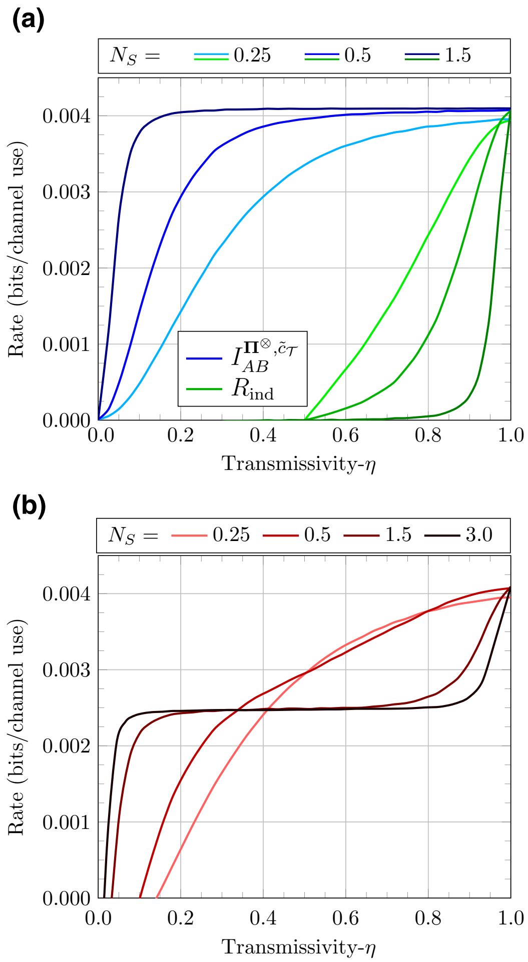


FIG. 4. MNIST degenerate-pattern communication. (a) The simulated mutual information (blue) and symmetric rate from Eq. (43) (green). (b) A computation of the rate under minimum approximate attacks given in Eq. (44). Both Bob and Eve employ the use of CNN decoders and we consider communication of patterns with $N_S \in \{0.25, 0.5, 1.5, 3.0\}$, with simulated communication rates computed over $|\mathcal{V}| = 10\,000$ transmissions and averaged over 20 simulations.

communication rate will thus follow Eq. (13)

$$R_{\text{ind}} = I_{AB}^{\Pi^{\otimes},\tilde{c}_{\mathcal{T}}}(\eta) - I_{AE}^{\Pi^{\otimes},\tilde{c}_{\mathcal{T}}}(1-\eta). \tag{43}$$

This symmetric rate is shown in Fig. 4(a), which follows the typical behavior for communication in direct reconciliation and only admits security for $\eta \geq 0.5$.

However, for a code book of this magnitude, it is not trivial to assume that an arbitrary eavesdropper can obtain perfect encoding knowledge. Indeed, it is nontrivial to consider scenarios such that (i) Eve does not possess the same resources as Bob $\mathcal{T}_E \neq \mathcal{T}$ or (ii) Eve does not possess the code book at all. We may simulate rates based on the assumption in (i) and outline a generic adaptive protocol for Eve's worst-case scenario in (ii).

The assumption that Eve possesses the code-book mapping but only partial resources leads to a diminished approximate attack, where Eve's training set may now be considered as a subset $\mathcal{T}_E \subset \mathcal{T}$. This separation in training-set quality will render Eve's classifier $\tilde{c}_{\mathcal{T}_E}$ inferior with respect to Bob's $\tilde{c}_{\mathcal{T}}$, especially when $|\mathcal{T}| \gg |\mathcal{T}_E|$. This results in a rate described by

$$\tilde{R}_{\text{dim}} = I_{AB}^{\Pi^{\otimes},\tilde{c}_{\mathcal{T}}}(\eta) - I_{AE}^{\Pi^{\otimes},\tilde{c}_{\mathcal{T}_E}}(1-\eta). \tag{44}$$

For an eavesdropper who is solely aware of the code-word mapping, he or she will only possess single examples of each code word such that $|\mathcal{B}(c)| = 1, \forall c$, and their training set $|\mathcal{T}_E| = 10$. This defines a *minimum approximate attack*, since this is the minimum amount of information Eve needs to apply a deterministic attack. Results for this rate are shown in Fig. 4(b). As expected, Eve's restricted resources lead to a dramatically more secure protocol, allowing Alice and Bob to communicate securely at much lower transmissivities. As the mean photon energy $N_S$ is increased, the rate begins to plateau with respect to transmissivity; improvements in Eve's single-mode discrimination are incapable of boosting her classification performance until $\eta \sim 0$. This lets Alice and Bob achieve a near-constant nonzero rate within a large window of transmissivities.

Finally, one can consider the strategy of a completely ignorant eavesdropper. Now Eve knows nothing about the encoding and must construct her own code book in order to extract any information at all. To do so, Eve must observe transmissions from the evaluation set and try to infer an approximate alphabet $\tilde{\mathcal{A}}$ and its respective code-word mappings. This can be achieved (albeit with some difficulty when transmissions are particularly noisy) by means of a data-clustering algorithm over the span of many transmissions and can then be used to devise an approximate code book and classifier. This will result in a probabilistic form of Eq. (44) with a decoding error associated with alphabet inference. In the limit of many transmissions, this strategy may have some success but will still result in a very secure rate for Alice and Bob.

## IV. DISCUSSION AND CONCLUSIONS

We investigate a multimode modulation scheme for bosonic quantum communications. We show that is possible to encode information into multimode coherent states that are discretely modulated according to specific structures, which we name quantum patterns. Likening the task of communication with pattern recognition, we study abstract encodings based on collections of coherent quantum patterns that may possess extreme degeneracies and nonlinearities. From this, interesting questions regarding practical and/or realistic security emerge. We elucidate these general arguments with some example pattern encodings, one of which exploits eavesdropper ignorance to obtain superior quantum measurements, while the other employs degenerate coding in order to capitalize on an eavesdropper's limited resources.

These methods and results are informative to the fact that multimode encoded information can be used to introduce serious complications for eavesdroppers. In particular, the versatility of trainable classifiers in cooperation with arbitrarily complex (even adaptive) coding schemes could be used to introduce novel layers of security in quantum communication protocols.

There are clearly many immediate possible developments, such as the explicit investigation of $k$-ary modulated patterns and the extension to reverse reconciliation protocols. It would also be valuable to better understand the abilities of an eavesdropper when exposed to a large degenerate code. If an attacker's resources for pattern inference can be securely limited, then their threat can be minimized, even when in possession of a quantum memory. This would require an upper bound on Eve's classification power via generally quantum resources, given that she has extracted the accessible information. Analyses from Refs. [40,41] may be of use for this.

In this work, we focus on the use of quantum patterns constructed from coherent states. This is carried out as an expedient translation from the most common and practical CV-QKD protocols. Furthermore, coherent-state discrimination and its error rates are well understood. Yet, in general, quantum pattern states can be constructed using any kind of locally modulated states, such as thermal states, squeezed states, etc. To this end, it would be interesting to explore the incorporation of *entangled* quantum pattern states, which would exploit nonlocal modulations to construct global patterns. Entanglement assistance is well known to be a powerful resource for quantum communications [46–49] and in this setting it might be possible to introduce further complications for eavesdroppers.

Most importantly, the use of pattern encoding in order to enhance secure protocols against collective attacks (rather than individual) offers the greatest reward. Devising a secure training protocol for the classifiers of trusted parties would allow for the benefits of approximate attacks to be realized within this stricter framework. The covert incorporation of information asymmetry between users and eavesdroppers in QKD could be of great benefit to security, representing a fascinating future investigative path.

## ACKNOWLEDGMENTS

C.H. acknowledges funding from the Engineering and Physical Sciences Research Council (EPSRC) via a Doctoral Training Partnership (EP/R513386/1). S.P. acknowledges funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No. 862644 (Quantum readout techniques and technologies, QUARTET).

## APPENDIX A: DISCRIMINATION VIA PGMS

Consider an ensemble of coherent-pattern states through a uniform lossy multichannel $\{p_i; \alpha_i^{\eta}\}_{i\in\mathcal{U}}$, where $\mathcal{U}$ is an image space and assuming equal *a priori* probabilities for each pattern to occur $p_i = 1/|\mathcal{U}|$ for all $\boldsymbol{i} \in \mathcal{U}$. Since the ensemble consists of pure states $|\alpha_i^{\eta}\rangle$, we can use its Gram matrix in order to study the effectiveness of discrimination using PGMs, the elements of which take the form

$$G[\mathcal{U}]_{i,i'} = \langle \eta\alpha_i | \eta\alpha_{i'} \rangle . \tag{A1}$$

The average error probability of discrimination is then given by

$$p_{\mathrm{err}}[\mathcal{U}] := 1 - \frac{1}{|\mathcal{U}|}\left(\sum_{i=1}^{|\mathcal{U}|} \lambda_i^{\frac{1}{2}}\right)^2 , \tag{A2}$$

where $\{\lambda_i\}_{i=1}^{|\mathcal{U}|}$ are the eigenvalues of the Gram matrix. This represents the average error probability of discriminating any pattern $\boldsymbol{i} \in \mathcal{U}$ from all the other patterns in this image space.

## APPENDIX B: DECODING LTPF MODULATION SCHEMES

In this appendix, we derive important quantities used in the study of LTPF encoding schemes. In particular, we derive Eve's decoding probability of the $k$-TPF partition set $\mathcal{K}$ given that she has knowledge of $\mathcal{S}$, used in the main text to compute Alice's and Bob's secure rate under probabilistic attack. Furthermore, we discuss the degeneracy of LTPF encodings, which preclude (or make difficult) effective inference methods of $\mathcal{S}$ or $\mathcal{K}$.

### 1. Probability of inferring $\mathcal{K}$ given $\mathcal{S}$

Consider LTPF pattern communication as in the main text, where the modulation scheme is completely characterized by a locality partition set $\mathcal{S}$ (which describes how Alice and Bob choose regions within the pattern states to encode information) and a $k$-TPF partition set $\mathcal{K}$ (which describes how many target modes and background modes will be present within any given subregion of the pattern states). If Eve has knowledge of $\mathcal{S}$ but not $\mathcal{K}$, then her information retrieval is disadvantaged, as she cannot fully optimize her discriminatory measurements. But worse than this, Eve must deduce the properties of the $\mathcal{K}$ if she is to steal any information at all, as it is required to properly decode any encoded classical information from her collected states.

Let us consider Eve's scenario. Alice generates $m$-mode coherent-pattern states according to the modulation scheme $(\mathcal{S},\mathcal{K})$, which Eve intercepts. Since Eve has knowledge of $\mathcal{S}$, she knows that she should apply $|\boldsymbol{s}_j|$-mode PGMs over each subpattern of the global state that she recovers from the beam splitter. The problem is that she is unable to fully optimize these measurements because she does not know the precise number of target modulated modes $k_j$ within each subpattern state. As discussed in Sec. III A, we know that valid target numbers in a pattern region $\boldsymbol{s}_j$ belong to the set of values $\boldsymbol{k} = \{1,\ldots,|\boldsymbol{s}|_j - 1\}$ to ensure that at least a binary variable is encoded in each subpattern. Hence, Eve must utilize measurements that account for a variable amount of target modes at each subpattern. This nonbiased approach means that she must consider her output ensemble to be generated by the image space

$$\mathcal{U}_{\text{TPF}}^{\mathcal{S}} = \bigcup_{j=1}^{n} \bigcup_{k=1}^{|\boldsymbol{s}_j|-1} \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,k}, \tag{B1}$$

as in Eq. (35) in the main text. This image space contains $\Sigma(\boldsymbol{s}_j) := \sum_{i=1}^{|\boldsymbol{s}_j|-1} C_{|\boldsymbol{s}|_j}^{i}$ potential output states at each subpattern.

Eve performs these measurement to discriminate the pattern states. However, she must further infer $k_j$ over each subregion $\boldsymbol{s}_j$ in order to decode the transmissions into their binary representations. In the absence of prior knowledge of $\mathcal{K}$, we consider Eve's strategy to be direct inference of $k_j$ from her discrimination. That is, if Alice transmits a subpattern $\boldsymbol{i}_A^{\boldsymbol{s}_j}$ with $k_j$ target modulated modes that Eve discriminates as $\boldsymbol{i}_E^{\boldsymbol{s}_j}$ with $\tilde{k}_j$ target modulations, she must infer that $\tilde{k}_j$ is the correct value in the encoding scheme. This allows Eve to build up an approximate $k$-TPF partition set $\tilde{\mathcal{K}} = \{\tilde{k}_1,\ldots,\tilde{k}_N\}$ associated with each transmission.

The question is thus: What is the probability that Eve correctly infers $\tilde{\mathcal{K}} = \mathcal{K}$? This is equivalent to asking: What is the probability that Eve discriminates her intercepted pattern state as belonging to the correct image space $\mathcal{U}_{\text{TPF}}^{\mathcal{S},\mathcal{K}}$? Consider a single subpattern $\boldsymbol{s}_j$ with a true number of target modulations $k_j$. The average error probability of Eve inferring a target modulation $\tilde{k}_j$ is equal to

$$p(\tilde{k}_j|k_j,\boldsymbol{s}_j) = \sum_{\boldsymbol{i}_A^{\boldsymbol{s}_j} \in \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,k_j}} \sum_{\boldsymbol{i}_E^{\boldsymbol{s}_j} \in \mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,\tilde{k}_j}} \frac{p(\boldsymbol{i}_E^{\boldsymbol{s}_j}|\boldsymbol{i}_A^{\boldsymbol{s}_j})}{|\mathcal{U}_{\text{TPF}}^{|\boldsymbol{s}_j|,k_j}|}. \tag{B2}$$

Since we are using PGMs and coherent pattern states transmitted through pure-loss channels, we can replace the conditional probability $p(\boldsymbol{i}_E^{\boldsymbol{s}_j}|\boldsymbol{i}_A^{\boldsymbol{s}_j})$ with its computable value

$$p(\boldsymbol{i}_E^{\boldsymbol{s}_j}|\boldsymbol{i}_A^{\boldsymbol{s}_j}) = \text{Tr}\left[\Pi_{\boldsymbol{i}_E^{\boldsymbol{s}_j}} \alpha_{\boldsymbol{i}_A^{\boldsymbol{s}_j}}^{1-\eta}\right], \tag{B3}$$

$$= \left[\left(\sqrt{G[\mathcal{U}_{\text{TPF}}^{\mathcal{S}}]}\right)_{\boldsymbol{i}_A^{\boldsymbol{s}_j} \boldsymbol{i}_E^{\boldsymbol{s}_j}}\right]^2. \tag{B4}$$

Therefore, the average success probability of Eve inferring $k_j$ can be computed by summing the error probabilities $p(\tilde{k}_j|k_j,\boldsymbol{s}_j)$ over all the values that she believes $\tilde{k}_j$ could possibly take. More precisely,

$$p_{\text{dec}}^{k_j|\boldsymbol{s}_j} := 1 - \sum_{\tilde{k}_j=1}^{|\boldsymbol{s}_j|-1} p(\tilde{k}_j|k_j,\boldsymbol{s}_j). \tag{B5}$$

Since she has to do this for all subpatterns, we can then finally compute the successful decoding probability of inferring $\mathcal{K}$ directly from her measurements:

$$p_{\text{dec}}^{\mathcal{K}|\mathcal{S}} := \prod_{j=1}^{n} p_{\text{dec}}^{k_j|\boldsymbol{s}_j}. \tag{B6}$$

Hence, $p_{\text{dec}}^{\mathcal{K}|\mathcal{S}}$ is the success probability of inferring $\mathcal{K}$ through PGM measurements that are nonbiased to the number of target modes in each subregion $\boldsymbol{s}_j$, given that the locality structure $\mathcal{S}$ is already known. There may exist more sophisticated methods that Eve can employ to more accurately infer the partition set $\mathcal{K}$. Nonetheless, this offers an insightful inspection into the effects that information asymmetry has on communicators and attackers.

### 2. Degeneracy of LTPF encoding schemes

Here, we briefly summarize the degeneracy properties of LTPF encoding schemes and the number of ways in which a specific $(\mathcal{S},\mathcal{K})$ pair can be chosen over $m$ mode patterns. A partition of $m \in \mathbb{N}$ into $n$ parts is defined as an ordered vector $\boldsymbol{x} = \{x_1,\ldots,x_n\}$, where $x_j \in \mathbb{N}$, $x_1 \geq \ldots \geq x_n > 0$ and $\sum_{j=1}^{n} x_j = m$. We denote this as $\boldsymbol{x} \vdash_n m$. Given the multinomial coefficient

$$M_m^{\boldsymbol{x}} = M_m^{x_1\ldots,x_n} := \prod_{j=1}^{n} C_{m-\sum_{k=1}^{j} x_k}^{x_j}, \tag{B7}$$

we define a modification that discards permutations that are invariant under the shuffling of subpatterns [50]:

$$\tilde{M}_m^{\boldsymbol{x}} = \frac{M_m^{\boldsymbol{x}}}{\prod_{l=1}^{\max(\boldsymbol{x})}\left[\sum_{k=1}^{r}\delta(x_k,l)\right]!}, \tag{B8}$$

where $\delta(x,y)$ is an integer Kronecker delta function.

The number of ways in which one may choose a locality partition set $\mathcal{S}$ over $m$ modes may be calculated using the above formalism, summing over all possible combinations and partitions. A simpler computation is given by the associated Stirling numbers of the second kind, which count the number of ways to partition $m$ modes into $n$ parts with minimum subset size $k$. These numbers obey the recurrence relation

$$S_k^m(n) = nS_k^{m-1}(n) + C_{m-1}^{k-1} S_k^{m-k}(n-1). \tag{B9}$$

Restricting subpattern dimensions to $2 \leq |\mathbf{s}_j| \leq m$ (to ensure that all subpatterns can encode at least 1 bit), then the degeneracy of $\mathcal{S}$ is

$$\mathcal{G}_{\mathcal{S}} := \sum_{n=1}^{\lfloor m/2 \rfloor} S_2^m(n) = \sum_{n=1}^{\lfloor m/2 \rfloor} \sum_{\mathbf{x} \vdash_n m} \tilde{M}_m^{\mathbf{x}}. \tag{B10}$$

The parallel freedom of locality and TPF-partition sets expands the space of encodings even further. For each subpattern $\mathbf{s}_j \in \mathcal{S}$, there will exist $\prod_{j=1}^{n}(|\mathbf{s}_j| - 1)$ choices of $k_j$ target modulations, with the constraints of $2 \leq |\mathbf{s}_j| \leq m$ and $k \in \{1, \ldots, |\mathbf{s}_j| - 1\}$. The total degeneracy of all possible schemes is then given by

$$\mathcal{G}_{\mathcal{S},\mathcal{K}} := \sum_{n=1}^{\lfloor m/2 \rfloor} \sum_{\mathbf{x} \vdash_n m} \tilde{M}_m^{\mathbf{x}} \prod_{j=1}^{n} (x_j - 1). \tag{B11}$$

It is also useful to determine conditional degeneracies, $\mathcal{G}_{\mathcal{S}|\mathcal{K}}$ and $\mathcal{G}_{\mathcal{K}|\mathcal{S}}$, based on some leaked information that Eve may have obtained. If Eve is aware of $\mathcal{K} = \{k_1, k_2, \ldots, k_n\}$ only, she can still glean some information about $\mathcal{S}$. Due to $\mathcal{K}$, Eve can infer the number of subpatterns $n$ and also the minimum size of the $j^{\text{th}}$ subpattern, $x_{\min}(j) = k_j + 1$. Alternatively, if Eve is only aware of $\mathcal{S}$, then she can significantly narrow the space of possible $\mathcal{K}$. She knows that it consists of $n$ elements and she is aware of the maximum and minimum target numbers of each subpattern. We can then summarize the conditional degeneracies:

$$\mathcal{G}_{\mathcal{S}|\mathcal{K}} := \sum_{\substack{\mathbf{x} \vdash_n m, \\ x_j \geq k_j + 1, \forall j}} \tilde{M}_m^{\mathbf{x}}, \quad \mathcal{G}_{\mathcal{K}|\mathcal{S}} := \prod_{j=1}^{n} (|\mathbf{s}_j| - 1). \tag{B12}$$

In general, $\mathcal{G}_{\mathcal{S}|\mathcal{K}} \gg \mathcal{G}_{\mathcal{K}|\mathcal{S}}$; hence it is always more secure to keep $\mathcal{S}$ secret. Regardless, one can always choose a locality structure $\mathcal{S}$ that maximizes this degeneracy. Interestingly, one finds that constraining the number of subpattern sizes as $|\mathbf{s}_j| \in \{4, 5\}$ and maximizing the number of subpatterns with $|\mathbf{s}_j| = 5$ produces the desired result. Defining the function

$$g_{\mathcal{K}|\mathcal{S}}(m) := \begin{cases} m-1, & \text{if } 2 \leq m \leq 7, \\ 4^{m/5}, & \text{if } (\frac{m}{5} \in \mathbb{N}) \wedge (m > 7), \\ 4^{\lceil m/5 \rceil} \left(\frac{3}{4}\right)^{5-(m \bmod 5)}, & \text{otherwise}, \end{cases} \tag{B13}$$

we can write

$$\mathcal{G}_{\mathcal{K}|\mathcal{S}} \leq \max_{\mathcal{S}} \mathcal{G}_{\mathcal{K}|\mathcal{S}} = g_{\mathcal{K}|\mathcal{S}}(m). \tag{B14}$$


[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, and J. L. Pereira, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[2] S. Pirandola and S. L. Braunstein, Physics: Unite to build a quantum internet, Nature **532**, 169 (2016).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, USA, 2011), 10th ed.

[4] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).

[5] A. S. Holevo, *Quantum Systems, Channels, Information* (De Gruyter, Berlin-Boston, 2019).

[6] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Taylor & Francis Group, 2017).

[7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[8] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[9] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[10] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[12] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[13] N. J. Cerf, M. Lévy, and G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

[14] R. Filip, Continuous-variable quantum key distribution with noisy coherent states, Phys. Rev. A **77**, 022310 (2008).

[15] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Quantum Cryptography Approaching the Classical Limit, Phys. Rev. Lett. **105**, 110501 (2010).

[16] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[17] Y. Zhang, Z. Chen, C. Weedbrook, S. Yu, and H. Guo, Continuous-variable source-device-independent quantum

key distribution against general attacks, Sci. Rep. **10**, 6673 (2020).

[18] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[19] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Quantum cryptography using pulsed homodyne detection, Phys. Rev. A **68**, 042331 (2003).

[20] A. Leverrier and P. Grangier, Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, Phys. Rev. Lett. **102**, 180504 (2009).

[21] D. Sych and G. Leuchs, Coherent state quantum key distribution with multi letter phase-shift keying, New J. Phys. **12**, 053019 (2010).

[22] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels, Phys. Rev. A **98**, 012340 (2018).

[23] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X **9**, 021059 (2019).

[24] P. Papanastasiou and S. Pirandola, Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks, Phys. Rev. Res. **3**, 013047 (2021).

[25] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates, Phys. Rev. A **94**, 012322 (2016).

[26] Q. Zhuang, Z. Zhang, and J. H. Shapiro, High-order encoding schemes for floodlight quantum key distribution, Phys. Rev. A **98**, 012323 (2018).

[27] K. Noh, S. Pirandola, and L. Jiang, Enhanced energy-constrained quantum communication over bosonic Gaussian channels, Nat. Commun. **11**, 457 (2020).

[28] N. Dalla Pozza and N. Laurenti, Adaptive discrimination scheme for quantum pulse-position-modulation signals, Phys. Rev. A **89**, 012339 (2014).

[29] G. Cariolaro and G. Pierobon, Theory of quantum pulse position modulation and related numerical problems, IEEE Trans. Commun. **58**, 1213 (2010).

[30] N. Dalla Pozza and G. Pierobon, Optimality of square-root measurements in quantum state discrimination, Phys. Rev. A **91**, 042334 (2015).

[31] M. A. Nielsen, *Neural Networks and Deep Learning* (Determination Press, San Francisco, 2015).

[32] K. P. Murphy, *Machine Learning: A Probabilistic Perspective* (The MIT Press, Cambridge, Massachusetts, 2012).

[33] L. Banchi, Q. Zhuang, and S. Pirandola, Quantum-Enhanced Barcode Decoding and Pattern Recognition, Phys. Rev. Appl. **14**, 064026 (2020).

[34] C. Harney, L. Banchi, and S. Pirandola, Ultimate limits of thermal pattern recognition, Phys. Rev. A **103**, 052406 (2021).

[35] This assumption is strong when considering a small number of spatial modes.

[36] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1996).

[37] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Akademiai Kiado, Budapest, 1997).

[38] Q. Liao, G. Xiao, H. Zhong, and Y. Guo, Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution, New J. Phys. **22**, 083086 (2020).

[39] W. Song, Y. Lim, H. Kwon, G. Adesso, M. Wieśniak, M. Pawłowski, J. Kim, and J. Bang, Quantum secure learning with classical samples, Phys. Rev. A **103**, 042409 (2021).

[40] L. Banchi, J. Pereira, and S. Pirandola, Generalization in quantum machine learning: A quantum information perspective, ArXiv:2102.08991 (2021).

[41] H.-Y. Huang, R. Kueng, and J. Preskill, Information-Theoretic Bounds on Quantum Advantage in Machine Learning, Phys. Rev. Lett. **126**, 190505 (2021).

[42] Y. C. Eldar and G. D. Forney, On quantum detection and the square-root measurement, IEEE Trans. Inf. Theory **47**, 858 (2001).

[43] Q. Zhuang and S. Pirandola, Entanglement-enhanced testing of multiple quantum hypotheses, Commun. Phys. **3**, 103 (2020).

[44] S. J. Dolinar, Research Laboratory of Electronics (RLE) at the Massachusetts Institute of Technology (MIT), Technical Report, RLE_QPR_111_VII (1973).

[45] Nonetheless, it would be interesting to investigate security conditions granted that Eve utilizes *imperfect* quantum memories and realistic data-processing times.

[46] C. H. Bennett and S. J. Wiesner, Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett. **69**, 2881 (1992).

[47] A. S. Holevo, On entanglement-assisted classical capacity, J. Math. Phys. **43**, 4326 (2002).

[48] Q. Zhuang, E. Y. Zhu, and P. W. Shor, Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement, Phys. Rev. Lett. **118**, 200503 (2017).

[49] P. L Guo, T. Li, and Q. Ai, Self-error-rejecting quantum state transmission of entangled photons for faithful quantum communication without calibrated reference frames, EPL **127**, 60001 (2019).

[50] For example, it is clear that the locality structures $\{\{1,2\},\{3,4\},\{5,6,7,8\}\}$ and $\{\{3,4\},\{1,2\},\{5,6,7,8\}\}$ are the same, as subsets have just been relabeled.