

Practical unclonable encryption with continuous variables

Arpan Akash Ray  and Boris Škorić 

Eindhoven University of Technology, Eindhoven, The Netherlands

 (Received 7 November 2025; revised 26 May 2026; accepted 15 July 2026; published 4 September 2026)

We propose the first continuous-variable (CV) unclonable encryption scheme, extending the paradigm of quantum encryption of classical messages to CV systems. In our construction, a classical message is first encrypted classically and then encoded using an error-correcting code. Each bit of the codeword is mapped to a CV mode by creating a coherent state which is squeezed in the q or p quadrature direction, with a small displacement that encodes the bit. The squeezing directions are part of the encryption key. We prove unclonability in the framework introduced by Broadbent and Lord, via a reduction of the cloning game to a CV monogamy-of-entanglement game. Furthermore, we demonstrate that our scheme can be readily implemented with current technology. By incorporating realistic imperfections such as channel noise and detector inefficiencies, we show that the protocol remains robust under these conditions.

DOI: [10.1103/kkzp-w2hc](https://doi.org/10.1103/kkzp-w2hc)

I. INTRODUCTION

The marriage of quantum information theory with cryptography has given rise to a wide array of protocols that exploit uniquely quantum phenomena, most notably the no-cloning principle [1–3], to achieve security properties that are unattainable in a classical setting. One such concept, *unclonable encryption*, harnesses the indivisibility of quantum states to prevent an adversary from copying an encrypted message.

The term unclonable encryption (UE) first appeared in 2003 in a paper by Gottesman [4]. Alice encrypts a classical message into a quantum state. A security definition was introduced that essentially states “If Bob decides that his decryption is valid, then Eve, given the key, has only negligible information about the plaintext.” The security definition was formulated in terms of the trace distance between encryptions of different messages and essentially encompasses tamper detection. In the same framework, Leermakers and Škorić devised an UE scheme with key recycling [5]. Broadbent and Lord [6] introduced the stronger notions of unclonability and unclonable indistinguishability, in which the splitting of the ciphertext is considered and both receiving partners are malicious. They constructed UE in the random oracle model. Several further UE schemes were introduced in [7–9] and results on the feasibility and limitations of UE were given in [10,11].

Until now, UE has been exclusively studied in discrete-variable (DV) quantum systems. However, in the field of quantum key distribution (QKD), continuous-variable (CV) quantum systems have emerged as an attractive alternative to DV [12–21]. A key advantage of CV-QKD over its DV

equivalent is its practicality; see, e.g., Ref. [22]. In broad terms, CV platforms are simpler to operate and exploit decades of progress in coherent optical-communication technology. DV protocols, by contrast, need single-photon detectors and sometimes single-photon sources as well. These components remain expensive and technically demanding, especially when photon-number resolution is required. CV schemes instead use homodyne or heterodyne detection, which is both cheaper and easier to deploy. Furthermore, today’s fiber-optic infrastructure is optimized for low-loss transmission at telecom wavelengths (1310 nm and 1550 nm); ideal single-photon emitters at these wavelengths have not yet been realized and frequency up-conversion introduces additional loss and error. Beyond QKD, the practical advantages hold more generally for other quantum information processing applications and this has fueled substantial interest in translating DV-based cryptographic ideas into the CV domain.

In this paper, we propose the first unclonable encryption scheme that works with continuous-variable states. We prove that our scheme is *unclonable secure*, in the UE framework of [6]. We note that this is strictly weaker than the more general notion of *unclonable indistinguishability*. Nevertheless, for the practical objective of a one-time encryption scheme, unclonable security already ensures that no adversary can duplicate or replay ciphertexts without detection, which suffices for our application. Furthermore, unclonable indistinguishability allows for the adversary to be entangled with the plaintext, which gives too much power to the adversary, since the plaintext is classical.

It turns out that bringing UE from discrete to continuous variables has a number of nontrivial aspects. On the construction side, the parameters of the scheme need to be tuned such that both decryptability and unclonability are satisfied. On the proof-technical side, we use a series of hybrids in order to connect the *cloning game*, which features in the UE security definition, to the *CV monogamy-of-entanglement game*, for which an upper bound on the winning probability has recently

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

TABLE I. Notation table for quick reference.

Notation	Meaning
α	Fixed displacement of the sq-vacuum state
β	Bit error probability
c	Codeword made from the ciphertext m'
ε_{DF}	Probability of decryption failure
$\phi \in \{0, 1\}^N$	Part of the key; selects the quadratures
$k \in \mathbb{R}^N$	Part of the key; random displacement
$m \in \{0, 1\}^n$	Plaintext message
n	Length of the plaintext
N	Number of modes in the cipherstate
r	Squeezing parameter
$s \in \{0, 1\}^z$	Symmetric-key classical encryption
t	Number of tolerated bitflips
z	Size of the key for classical encryption

been proven [23]. Furthermore, it is necessary to allow imperfect completeness in the CV case, as there is a nonzero probability of decryption failure caused by the probability tails of the CV measurements.

Beyond the immediate theoretical interest, a CV-based UE scheme has potential advantages for future practical quantum networks, especially where CV platforms are more readily integrated with existing optical infrastructure.

In line with this theme of practicality, we also show that our scheme is correct for experimentally feasible values of squeezing. Finally we analyze our protocol under noisy conditions and show robustness for realistic channel parameters.

The outline of the paper is as follows. In Sec. II we briefly review CV formalism and important definitions and results from the literature. In Sec. III we present our protocol and verify that it satisfies the definition of a quantum encryption. Section IV contains the unclonability proof. The main result is stated in Theorem 2. In Sec. V we discuss squeezing and robustness under channel and detector imperfections. In Sec. VI we summarize and discuss future work.

II. PRELIMINARIES

A. Notation

We use standard bra-ket notation for quantum states. Hilbert spaces are written as $\mathcal{H}$ with a subscript. For example, we write the Hilbert space of a single CV mode as $\mathcal{H}_1$. The notation $\mathcal{D}(\mathcal{H})$ stands for the set of density operators on $\mathcal{H}$. We use the abbreviation EB for entanglement based. The Hamming weight of a string s is written as $|s|$. Logarithms are in base 2 unless indicated otherwise. The binary entropy function is written as $h(p) = -p \log p - (1-p) \log(1-p)$. We denote the complementary error function by $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$. Other notation will be defined when they are first used throughout the paper. A quick reference notation chart (Table I) is also provided.

B. Continuous variables and Gaussian states

Continuous-variable (CV) quantum information uses quantum systems whose natural observables have a continuous spectrum. The basic example is a single optical mode, which

may be thought of as one harmonic oscillator associated with a fixed frequency, wave vector, and polarization of the electromagnetic field. Each mode has a creation operator $\hat{a}^\dagger$ and an annihilation operator $\hat{a}$. Instead of working directly with $\hat{a}$ and $\hat{a}^\dagger$, it is often more convenient to work with the two Hermitian quadrature operators

$$\hat{q} = \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}}, \quad \hat{p} = \frac{\hat{a} - \hat{a}^\dagger}{i\sqrt{2}}. \quad (1)$$

These operators satisfy the same commutation relation as the position and momentum of a harmonic oscillator,

$$[\hat{q}, \hat{p}] = i. \quad (2)$$

Thus a single optical mode can be represented by a two-dimensional phase space with coordinates (q, p) . In the protocols considered in this paper, measurements of these quadratures produce real-valued classical outcomes, which are then used as the classical variables appearing in the cryptographic description. Measuring one quadrature, for example $\hat{q}$, is called a *homodyne* measurement.

A particularly important family of CV states is the family of *Gaussian states*. These are states whose Wigner function is a Gaussian function on phase space [22]. The Wigner function is a phase-space representation of a quantum state; for Gaussian states it is completely specified by first and second moments of the quadratures. More precisely, for an N -mode system we collect the quadratures into the vector

$$\hat{x} = (\hat{q}_1, \hat{p}_1, \dots, \hat{q}_N, \hat{p}_N)^T. \quad (3)$$

An N -mode Gaussian state is fully characterized by a displacement vector $d \in \mathbb{R}^{2N}$ and a covariance matrix $\Gamma \in \mathbb{R}^{2N \times 2N}$. With the conventions used here, its Wigner function is

$$W(x) = \frac{1}{\pi^N \sqrt{\det \Gamma}} \exp[-(x-d)^T \Gamma^{-1} (x-d)], \quad (4)$$

where $x = (q_1, p_1, \dots, q_N, p_N)^T$ is a point in phase space. The displacement vector gives the mean values of the quadratures, while the covariance matrix describes their variances and correlations. In this normalization, the variance of a measured quadrature is one-half of the corresponding diagonal entry of Γ .

The class of Gaussian states contains many of the standard optical states used in CV quantum information, including the vacuum state, thermal states, coherent states, squeezed coherent states, and EPR states, also called two-mode squeezed vacuum states. A coherent state is the CV analog of a classical field with quantum noise. A squeezed state is a state in which the noise of one quadrature is reduced below the vacuum level, at the cost of increasing the noise of the conjugate quadrature. For example, a single-mode state squeezed in the q direction has covariance matrix

$$\Gamma_q = \begin{pmatrix} e^{-\zeta} & 0 \\ 0 & e^{\zeta} \end{pmatrix}, \quad (5)$$

where $\zeta \geq 0$ is the squeezing parameter. Similarly, a state squeezed in the p direction has covariance matrix

$$\Gamma_p = \begin{pmatrix} e^\zeta & 0 \\ 0 & e^{-\zeta} \end{pmatrix}. \quad (6)$$

Thus increasing ζ makes the state more sharply concentrated in one quadrature and more spread out in the other. Squeezing in intermediate phase-space directions is also possible, but will not be needed in this paper.

We will also use a two-mode entangled Gaussian state. Such a state can be prepared by mixing a q -squeezed vacuum state and a p -squeezed vacuum state on a 50 : 50 beam splitter. The resulting state is the two-mode squeezed state or EPR state. It has zero displacement and covariance matrix

$$\Gamma_{\text{EPR}} = \begin{pmatrix} \mathbb{I} \cosh \zeta & \sigma_z \sinh \zeta \\ \sigma_z \sinh \zeta & \mathbb{I} \cosh \zeta \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (7)$$

Here $\mathbb{I}$ denotes the 2×2 identity matrix. The off-diagonal blocks express the correlations between the two modes. Intuitively, for large squeezing, the two systems have strongly correlated q quadratures and strongly anticorrelated p quadratures.

In the entanglement-based version of our scheme, we use a displaced version of this EPR state. For instance, we may take the displacement vector to be

$$d = (\alpha, 0, \alpha, 0)^T. \quad (8)$$

This means that both modes are displaced in the q quadrature by the same amount α . If the q quadrature of the first mode is measured, the measurement outcome x_A is a real-valued Gaussian random variable with mean α and variance $\frac{1}{2} \cosh \zeta$. Conditioned on the value of this outcome, the second mode is projected onto a squeezed coherent state. Its displacement is $(\alpha + [x_A - \alpha] \tanh \zeta, 0)^T$ and its covariance matrix is

$$\Gamma_{B|x_A} = \begin{pmatrix} \frac{1}{\cosh \zeta} & 0 \\ 0 & \cosh \zeta \end{pmatrix}. \quad (9)$$

Thus, if x_A is known, the remaining mode is a known squeezed coherent state. If x_A is not known, then the displacement of the remaining mode must itself be treated as a Gaussian random variable. In that case, the random displacement $\alpha + [x_A - \alpha] \tanh \zeta$ has mean α and variance $\frac{1}{2} \cosh \zeta \tanh^2 \zeta$.

This last observation is the main reason these states are useful in the cryptographic construction: a homodyne measurement on one part of an entangled Gaussian state prepares, on the other part, a squeezed coherent state whose displacement is correlated with a classical Gaussian variable. The CV formalism describes the optical state and its measurement statistics, while the later game-based notation treats the measurement outcomes and classical choices as the random variables used in the security proof. For a comprehensive review of CV quantum information, we refer to Ref. [22].

C. Definitions and useful lemmas

In Sec. III we will introduce a scheme that encrypts a classical message into a quantum ciphertext (cipherstate),

using a classical key. For the formal description of such a scheme we follow the definition given in [6], with a small modification: we allow for a small probability of failure in the decryption.

Definition 1. Let $\lambda \in \mathbb{N}^+$ be a security parameter. Let $\mathcal{M}(\lambda)$ be the (classical) plaintext space. Let $\mathcal{K}(\lambda)$ be the (classical) key space. A quantum encryption of classical messages (QECM) scheme is a triplet of efficient quantum circuits ($\text{Key}_\lambda, \text{Enc}_\lambda, \text{Dec}_\lambda$) implementing CPTP maps of the form

$$\text{Key}_\lambda : \mathcal{D}(\mathcal{C}) \rightarrow \mathcal{D}(\mathcal{H}_{\mathcal{K}(\lambda)}), \quad (10)$$

$$\text{Enc}_\lambda : \mathcal{D}(\mathcal{H}_{\mathcal{K}(\lambda)} \otimes \mathcal{H}_{\mathcal{M}(\lambda)}) \rightarrow \mathcal{D}(\mathcal{H}_{T,\lambda}), \quad (11)$$

$$\text{Dec}_\lambda : \mathcal{D}(\mathcal{H}_{\mathcal{K}(\lambda)} \otimes \mathcal{H}_{T,\lambda}) \rightarrow \mathcal{D}(\mathcal{H}_{\mathcal{M}(\lambda)}), \quad (12)$$

where $\mathcal{H}_{\mathcal{K}(\lambda)}$ is the Hilbert space of the key, $\mathcal{H}_{\mathcal{M}(\lambda)}$ is the Hilbert space of the plaintext, and $\mathcal{H}_{T,\lambda}$ is the cipherstate space.

Let E_k denote the CPTP map $\rho \mapsto \text{Enc}_\lambda(|k\rangle\langle k| \otimes \rho)$ and let D_k stand for the CPTP map $\rho \mapsto \text{Dec}_\lambda(|k\rangle\langle k| \otimes \rho)$. For all $k \in \mathcal{K}(\lambda)$, $m \in \mathcal{M}(\lambda)$, it must hold that

$$\begin{aligned} \text{Tr}[|k\rangle\langle k| \text{Key}_\lambda(1)] &> 0 \\ \Rightarrow \text{Tr}[|m\rangle\langle m| D_k \circ E_k(|m\rangle\langle m|)] &\geq 1 - \varepsilon_{\text{DF}}, \end{aligned} \quad (13)$$

where ε_{DF} is the tolerated probability of decryption failure.

Unclonability of a QECM scheme is defined via a *cloning game*. A challenger prepares a cipherstate and gives it to Alice. Alice splits the cipherstate into two pieces; one piece goes to Bob and one to Charlie. Then Bob and Charlie receive the decryption key and must *both* produce the correct plaintext, without being allowed to communicate. A QECM scheme is considered to be secure against cloning if the three players ABC, acting together, have an exponentially small probability of winning the game. We follow the definitions of [6] for the cloning game and the security against cloning. For a schematic representation of a cloning game, see Fig. 1.

Definition 2. (Cloning attack). Let S be a QECM scheme, with Hilbert spaces $\mathcal{H}_{\mathcal{K}(\lambda)}$, $\mathcal{H}_{\mathcal{M}(\lambda)}$, $\mathcal{H}_{T,\lambda}$ as given in Definition 1. Let $\mathcal{H}_B$ and $\mathcal{H}_C$ be Hilbert spaces of arbitrary dimension. A cloning attack against S is a triplet of efficient quantum circuits ($\mathcal{A}, \mathcal{B}, \mathcal{C}$) implementing CPTP maps of the form

$$\mathcal{A} : \mathcal{D}(\mathcal{H}_{T,\lambda}) \rightarrow \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_C), \quad (14)$$

$$\mathcal{B} : \mathcal{D}(\mathcal{H}_{\mathcal{K}(\lambda)} \otimes \mathcal{H}_B) \rightarrow \mathcal{D}(\mathcal{H}_{\mathcal{M}(\lambda)}), \quad (15)$$

$$\mathcal{C} : \mathcal{D}(\mathcal{H}_{\mathcal{K}(\lambda)} \otimes \mathcal{H}_C) \rightarrow \mathcal{D}(\mathcal{H}_{\mathcal{M}(\lambda)}). \quad (16)$$

Definition 3. Consider the cloning attack according to Definition 2. Let $\mathcal{B}_k$ stand for the CPTP map $\rho \mapsto \mathcal{B}(|k\rangle\langle k| \otimes \rho)$ and analogously $\mathcal{C}_k$. Let $\mathcal{M}(\lambda) = \{0, 1\}^n$. A QECM scheme S is $\tau(\lambda)$ -unclonable secure if for all cloning attacks ($\mathcal{A}, \mathcal{B}, \mathcal{C}$) against S , there exists a negligible function η such that

$$\begin{aligned} \mathbb{E}_{m,k} \text{Tr}(|m\rangle\langle m| \otimes |m\rangle\langle m| (\mathcal{B}_k \otimes \mathcal{C}_k) \circ \mathcal{A} \circ E_k(|m\rangle\langle m|)) \\ \leq 2^{-n+\tau(\lambda)} + \eta(\lambda). \end{aligned} \quad (17)$$

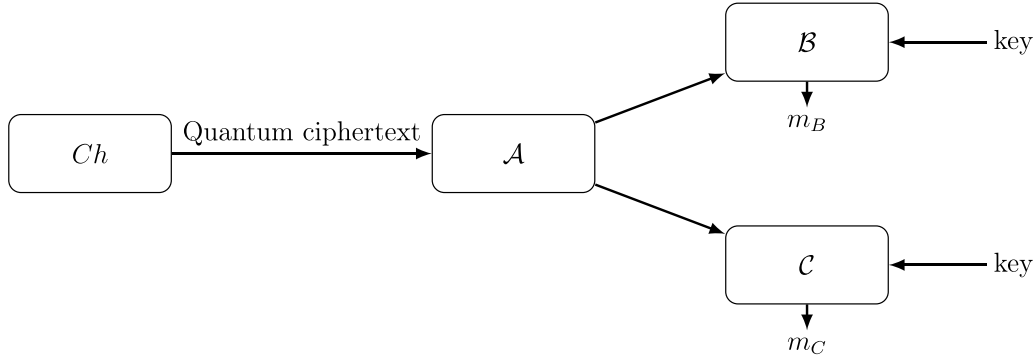


FIG. 1. Schematic representation of the unclonable encryption game.

Here the expectation $\mathbb{E}$ is over uniform m , and k distributed according to $\Pr[K = k] = \text{Tr}[|k\rangle\langle k| \text{Key}_\lambda(1)]$. If S is 0-unclonable secure, we simply say that it is unclonable secure.

Our security proof will make use of recent results on entanglement monogamy games for CV systems [23]. Such a game is played between Alice on one side and Bob and Charlie on the other. Bob and Charlie prepare a tripartite state ρ_{ABC} of their choice. Then Alice does an unpredictable measurement and Bob and Charlie have to show that they are both sufficiently entangled with Alice to guess Alice's outcome to some degree of accuracy. Below we present the coset monogamy game on $\mathbb{R}^N$ as introduced in Sec. 4 of [23]. In the original version, the measurement bases are continuous variable coset states of $\mathbb{R}^N$, given by $|P_{q,p}\rangle = \bigotimes_{i=1}^N \begin{cases} |q = q_i\rangle, & i \notin I, \\ |p = p_i\rangle, & i \in I. \end{cases}$ Here, I is a subset interval of N . We note that this is equivalent to performing a homodyne measurement in the q direction if $i \in I$, otherwise in the p direction. We refer to this game as the “partial” CV monogamy of entanglement game, since it requires Bob and Charlie to produce guesses for only one quadrature direction instead of two. In Sec. IVD we introduce a “full” version of the game.

Game 1: CV partial monogamy of entanglement game.

(1) *Initial-state preparation.* Bob and Charlie prepare an M -mode state ρ_{ABC} across three registers: one for Alice, one for Bob, and one for Charlie. After preparation, they are no longer allowed to communicate.

(2) *Alice's measurement choice and outcomes.* Alice chooses quadrature directions $(\theta_i)_{i=1}^M$, $\theta_i \in \{0, \frac{\pi}{2}\}$, such that $|i : \theta_i = 0| = M/2$, i.e., each direction is chosen exactly $M/2$ times. She then does homodyne detection of mode i in direction θ_i , getting outcomes that we denote as

$$q_i \quad \text{if } \theta_i = 0, \quad p_i \quad \text{if } \theta_i = \frac{\pi}{2}.$$

(3) *Announcement and responses.* Alice announces $(\theta_i)_{i=1}^M$. Bob outputs $q_B \in \mathbb{R}^{M/2}$ containing his guesses for Alice's q values. Charlie outputs $p_C \in \mathbb{R}^{M/2}$ containing his guesses for Alice's p values.

(4) *Winning condition.* Bob and Charlie win the game if

$$\|q - q_B\|_\infty < \delta, \quad \|p - p_C\|_\infty < \varepsilon. \quad (18)$$

The ∞ -norm in the winning condition means that all guesses $(q_B)_i$ and $(p_C)_i$ must be close to Alice's values.

As shown in [23], this game can be viewed as an *Abelian coset measure* monogamy game, where Bob and Charlie attempt to guess the measurement outcomes in each quadrature within error neighborhoods $(-\delta, \delta)^N$ and $(-\varepsilon, \varepsilon)^N$. The following upper bound was obtained on the winning probability.

Lemma 1. (Theorem 4.1 in [23]). In the CV partial monogamy of entanglement game (1), the winning probability w is upper bounded as

$$w \leq \frac{1}{\binom{N}{N/2}} \sum_{k=0}^{N/2} \binom{N/2}{k}^2 (2\sqrt{\delta\varepsilon})^k \leq \sqrt{e} \left(\frac{1}{2} + \sqrt{\delta\varepsilon}\right)^{\frac{N}{2}}. \quad (19)$$

III. PROTOCOL DESCRIPTION

We propose a QECM scheme that makes use of squeezed coherent states. The scheme encrypts a message $m \in \{0, 1\}^n$ to an N -mode cipherstate. First we apply a symmetric classical encryption scheme; this step ensures message confidentiality independent of the unclonability. We do not specify which symmetric cipher is used. We denote the encryption and decryption operations as $\text{Enc}_{\text{base}}(\cdot, \cdot)$ and $\text{Dec}_{\text{base}}(\cdot, \cdot)$.

Then the classical ciphertext gets encoded into an N -bit codeword c . The error correcting code is chosen such that it can correct t bit errors. The encoding and decoding algorithms are denoted as Encode , Decode .

We encode a bit message c_i into a CV mode by displacing a squeezed vacuum state over a distance $(-1)^{c_i}\alpha$, where $\alpha > 0$ is a constant. The displacement is in the “narrow” direction of the state. The underlying idea is that the squeezing direction is part of the encryption key; the attacker A , who does not know this direction, has trouble determining c and hence cannot create good clones. This encoding is similar to conjugate coding for qubits [24].

For proof-technical reasons, the squeezing directions are not chosen uniformly at random. We impose the constraint that exactly half the modes are squeezed in the q direction and one-half in the p direction. Hence the corresponding key space is not $\{0, 1\}^N$ but rather the set $\mathcal{L} = \{1, \dots, \binom{N}{N/2}\}$ of labels which uniquely enumerate the strings with Hamming weight $N/2$.

The QECM algorithms (Key, Enc, Dec) are given below.

ALGORITHM 1. Key generation (Key).

Input: $z(\lambda), N(\lambda), r(\lambda), \alpha(\lambda)$.
Output: a symmetric key $s \in \{0, 1\}^z$, a binary string $\phi \in \{0, 1\}^N$, and a real vector $k \in \mathbb{R}^N$.
1: Sample s uniformly from $\{0, 1\}^z$.
2: Sample label ℓ uniformly from $\{1, \dots, \binom{N}{N/2}\}$. Convert ℓ to a string $\phi \in \{0, 1\}^N$ with Hamming weight $N/2$.
3: **for** $i = 1$ to N **do**
4: Sample k_i from the normal distribution $\mathcal{N}(0, \frac{1}{2} \cosh r \tanh^2 r)$ truncated to the interval $(-\alpha \tanh r, \alpha \tanh r)$.
5: **end for**
6: $k = (k_1, \dots, k_N)$.
7: Output (s, ϕ, k) .

Note that the probability density function of k_i is proportional to $\exp(-\frac{k_i^2}{\cosh r \tanh^2 r})$, i.e., Gaussian form, but the support $k_i \in (-\alpha \tanh r, \alpha \tanh r)$ is quite narrow compared to the width of the Gaussian.

Theorem 1. Our construction is a QECM scheme with decryption failure parameter

$$\varepsilon_{\text{DF}} = \exp \left[-ND_{\text{KL}} \left(\frac{t+1}{N} \left\| \frac{1}{2} \text{erfc}(\alpha \sqrt{\cosh r}) \right\| \right) \right], \quad (20)$$

where D_{KL} stands for the binary Kullback-Leibler divergence, $D_{\text{KL}}(a||b) = a \ln \frac{a}{b} + (1-a) \ln \frac{1-a}{1-b}$, and erfc is the complementary error function.

Proof. It is trivial to see that the triplet (Key, Enc, Dec) fits the format of the CPTP maps in Definition 1. All that is left to show is that the protocol satisfies the correctness condition. A bit error in the codeword bit c_i occurs when $y_i - k_i$ has the wrong sign. Consider, without loss of generality, $c_i = 0$. Then the bit error probability is $\beta := \Pr[Y_i - k_i < 0]$. When k_i is known, the random variable $Y_i - k_i$ is Gaussian distributed with mean α and variance $1/(2 \cosh r)$. Hence

$$\beta = \frac{1}{2} - \frac{1}{2} \text{erf}(\alpha \sqrt{\cosh r}). \quad (21)$$

A decoding error can occur only when there are more than t bitflips; this occurs with probability $P = \sum_{j=t+1}^N \binom{N}{j} \beta^j (1-\beta)^{N-j}$.

ALGORITHM 2. Encryption (Enc).

Input: Key $(s, \phi, k) \in \{0, 1\}^z \times \{0, 1\}^N \times \mathbb{R}^N$; message $m \in \{0, 1\}^n$; parameters $\alpha, r \in \mathbb{R}^+$.
Output: Cipherstate $\rho \in \mathcal{D}(\mathcal{H}_1^{\otimes N})$.
1: Compute ciphertext $m' = \text{Enc}_{\text{base}}(s, m)$.
2: Compute codeword $c = \text{Encode}(m')$.
3: **for** $i = 1$ to N **do**
4: Prepare single mode squeezed state ρ_i with displacement d_i and covariance matrix Γ_i , where $d_i = [\alpha(-1)^{c_i} + k_i] \binom{\phi_i}{\phi_i}$ and

$$\Gamma_i = \begin{pmatrix} (\cosh r)^{2\phi_i-1} & 0 \\ 0 & (\cosh r)^{1-2\phi_i} \end{pmatrix}.$$

5: **end for**
6: $\rho = \rho_1 \otimes \dots \otimes \rho_N$.
7: Output ρ .

ALGORITHM 3. Decryption (Dec).

Input: Key $(s, \phi, k) \in \{0, 1\}^z \times \{0, 1\}^N \times \mathbb{R}^N$; cipherstate $\rho \in \mathcal{D}(\mathcal{H}_1^{\otimes N})$.
Output: Message $\hat{m} \in \{0, 1\}^n$.
1: **for** $i = 1$ to N **do**
2: Perform homodyne measurement on ρ_i in the $\phi_i \cdot \frac{\pi}{2}$ direction, resulting in outcome $y_i \in \mathbb{R}$.
3: $\hat{c}_i = \frac{1}{2} - \frac{1}{2} \text{sgn}(y_i - k_i)$.
4: **end for**
5: $\hat{c} = (\hat{c}_1, \dots, \hat{c}_N)$.
6: $\mu = \text{Decode}(\hat{c})$.
7: $\hat{m} = \text{Dec}_{\text{base}}(s, \mu)$.
8: Output $\hat{m}$.

$\beta)^{N-j} = \sum_{\ell=0}^{N-t-1} \binom{N}{\ell} \beta^{N-\ell} (1-\beta)^\ell$. Using a Chernoff bound on the binomial tail, we obtain $P \leq \exp[-ND_{\text{KL}}(\frac{t+1}{N}||\beta)]$.

Note that asymptotically N gets close to $\frac{n}{1-h(\beta)}$, where h is the binary entropy function.

IV. PROVING UNCLONABILITY

A. Game hopping

We prove that our scheme satisfies the security definition of Definition 3. We do this as follows. (i) We rewrite the state preparation from the original prepare-and-send form to the entanglement-based (EB) form. (ii) We show, in a series of “hops” (hybrids), that the cloning game that the security definition is based on is equivalent to a CV entanglement monogamy game. (iii) Finally we use Lemma 1, which upper bounds the winning probability in the CV entanglement monogamy game.

The sequence of games is as follows. (See Table II.) Note that this section does not discuss the decryption by the honest party (Algorithm 3), since it is unrelated to the proof of unclonability.

B. Entanglement-based version

The first hop is to replace (in the encryption algorithm) the drawing of k_i and the preparation of the single-mode state ρ_i by the following procedure. (1) Prepare a two-mode entangled state $\rho_{\text{ChA}}^{(i)}$. (2) Do a homodyne measurement on the “Ch” subsystem in the ϕ_i direction, yielding outcome u_i . Compute $k_i = [u_i - \alpha(-1)^{c_i}] \tanh r$.

The state $\rho_{\text{ChA}}^{(i)}$ must be such that it yields the correct distribution for k_i (truncated Gaussian) when the Ch system is measured in the ϕ_i direction and the state of the “A” subsystem gets projected to the correct squeezed coherent state. Without the truncation, $\rho_{\text{ChA}}^{(i)}$ would simply be given by the displaced EPR state mentioned in Sec. IIB. In order to reproduce the truncated k_i interval, however, the EPR state needs to be modified. The details are presented in the Appendix.

C. Unclonable encryption game

The cloning attack (Definition 2) can be represented as the game below, between the Challenger and the three players A,B,C.

TABLE II. Sequence of hybrids (games).

	Game	Brief description	Difference with respect to previous game
A	Unclonable encryption, prepare-and-send version	Ch prepares a q - or p -squeezed state displaced by $\alpha(-1)^{c_i} + k_i$. Alice splits the state between B and C, who then receive the key and must both recover the plaintext m .	–
A	Unclonable encryption, EB version	Ch prepares ρ_{ChA} and sends the A register to Alice. Alice splits her register. Ch homodynes his modes, derives k , and announces the complete key. B and C must both recover m .	The cipherstate is prepared using an entangled state and k is derived from Ch's homodyne outcomes.
B	EB intermediate unclonable encryption	Ch prepares ρ_{ChA} , sends the A register to Alice, and homodynes the retained register to obtain u . Alice splits. B and C output guesses u_B and u_C , which Ch converts into strings and decodes. Both u_B and u_C must yield correct decryption.	Bob and Charlie receive only ϕ and report u_B, u_C , rather than receiving the complete key and reporting m_B, m_C .
C	CV full monogamy of entanglement game	B and C prepare ρ_{ABC} . Alice measures half of her modes in q and half in p and announces her choices. B and C both guess all of her outcomes. All their guesses must be close.	State preparation is transferred to Bob and Charlie and winning is formulated directly in terms of closeness to Alice's homodyne outcomes.
	CV partial monogamy of entanglement game (Game 1)	B and C prepare ρ_{ABC} . Alice measures half of her modes in q and half in p and announces her choices. B guesses her q outcomes; C guesses her p outcomes. All their guesses must be close.	Bob and Charlie do not each guess all of Alice's outcomes: Bob reports only the q outcomes and Charlie reports only the p outcomes.

Game A: Unclonable encryption.

(1) *Initial-state preparation.* The challenger Ch picks a random message m .

Prepare-and-send: Ch runs Key (Algorithm 1) and obtains (s, ϕ, k) . He runs Enc (Algorithm 2) on m . He sends the resulting cipherstate to Alice.

Entanglement-based: Ch runs part of Algorithm 1 and obtains (s, ϕ) . He prepares an entangled state $\rho_{\text{ChA}} = \bigotimes_{i=1}^N \rho_{\text{ChA}}^{(i)}$, as explained in Sec. IVB. He sends the “A” part to Alice.

(2) *Distributing quantum information to co-players.* Alice (A) “splits” her quantum state and sends the two parts to her co-players, Bob (B) and Charlie (C) (see Fig. 1). After that, A, B, and C are no longer allowed to communicate.

(3) *Key opening and response.* Prepare-and-send: Ch announces the key (s, ϕ, k) . B and C respond with m_B and m_C , respectively.

Entanglement-based: Ch does homodyne measurements on his modes and computes k from the outcomes. Ch announces the key (s, ϕ, k) . B and C respond with m_B and m_C , respectively.

(4) *Winning condition.* The triplet of players ABC win the game if $m_B = m_C = m$.

Note that in this game the measurement by Ch has been postponed to step (3), as opposed to step (1) in the direct entanglement-based description of the preparation of A's state.

Game B: Entanglement-based intermediate unclonable encryption.

(1) *Initial-state preparation.* Ch prepares the entangled state ρ_{ChA} . He sends one-half of the state to Alice.

(2) *Distributing quantum information to co-players.*

(3) *Key opening (only ϕ) and response.* Ch measures u and announces ϕ . B and C respond with u_B and u_C , respectively. (Their guess for u .)

(4) *Winning condition.* For $i \in \{1, \dots, N\}$ Ch calculates $c_{Bi} = \frac{1}{2} - \frac{1}{2} \text{sgn}(u_{Bi} - \frac{k_i}{\tanh r})$ and $c_{Ci} = \frac{1}{2} - \frac{1}{2} \text{sgn}(u_{Ci} - \frac{k_i}{\tanh r})$. Then $m_B = \text{Dec}_{\text{base}}(s, \text{Decode}(c_B))$ and $m_C = \text{Dec}_{\text{base}}(s, \text{Decode}(c_C))$. The players ABC win if $m_B = m_C = m$.

Lemma 2. Winning the entanglement-based unclonable encryption game (Game A) is equivalent to winning the EB intermediate unclonable encryption game (Game B).

Proof. Consider the EB version of Game A. Given k_i , Bob and Charlie know that there are only two possible values for u_i , namely $u_i = \frac{k_i}{\tanh r} \pm \alpha$. Hence getting a bit c_i correct is equivalent to making the correct binary choice for u_i . From the fact that, by construction, $u_i \in (-2\alpha, 2\alpha)$, it follows that this in turn is equivalent to determining u_i with a resolution of α or better.

In Game B it is precisely such a resolution on the u axis that is required to guess c_i . ■

D. Monogamy of entanglement game

We introduce a version of the entanglement monogamy game that is closer to the encryption scheme than Game 1.

Game C: CV full monogamy of entanglement game.

(1) *Initial-state preparation.* Bob and Charlie prepare an M -mode state ρ_{ABC} across three registers: one for Alice, one for Bob, and one for Charlie. After preparation, they are no longer allowed to communicate.

(2) *Alice's measurement choice and outcomes.* Alice chooses quadrature directions $(\theta_i)_{i=1}^M$, $\theta_i \in \{0, \frac{\pi}{2}\}$, such that $|\{i : \theta_i = 0\}| = M/2$, i.e., each direction is chosen exactly $M/2$ times. She then does homodyne detection of mode i in direction θ_i , getting outcomes that we denote as

$$q_i \text{ if } \theta_i = 0, \quad p_i \text{ if } \theta_i = \frac{\pi}{2}.$$

(3) *Announcement and responses.* Alice announces $(\theta_i)_{i=1}^M$. Bob outputs a list $q_B \in \mathbb{R}^{M/2}$ containing his guesses for Alice's q values and a list $p_B \in \mathbb{R}^{M/2}$ containing his guesses for Alice's p values. Similarly, Charlie outputs q_C, p_C .

(4) *Winning condition.* Bob and Charlie win the game if

$$\begin{aligned} \|q - q_B\|_\infty < \delta, \quad \|p - p_B\|_\infty < \delta, \quad \|q - q_C\|_\infty < \varepsilon, \\ \|p - p_C\|_\infty < \varepsilon. \end{aligned} \quad (22)$$

Lemma 3. Let $w^{\text{UE}}(N, t)$ denote the winning probability for Game B. Let $w^{\text{full}}(N - 2t)$ be the winning probability for Game C with $\delta = \alpha$, $\varepsilon = \alpha$, and $M = N - 2t$. It holds that

$$w^{\text{UE}}(N, t) \leq 2^{N-n} w^{\text{full}}(N - 2t). \quad (23)$$

Proof. In Game B, getting a bit c_i correct is equivalent to getting u_i correct within a distance α . This corresponds to setting $\delta = \alpha$ and $\varepsilon = \alpha$ in Game C.

Next, in Game B it is required to get at least $N - t$ bits of c correct. Let $e \in \{0, 1\}^N$ denote an error pattern. Let w_e^{UE} be the probability of winning with precisely error pattern e . The bit errors can be arbitrarily distributed over the q part and the p part, which does not nicely fit the symmetric structure of the monogamy game. In order to obtain the symmetric structure we loosen our requirements a little and allow a surplus of bit errors in one block (if any) to be balanced by additionally allowed bit errors in the other block. In the worst case, all bit errors are located in one block; this leads to an allowed $2t$ errors. We write

$$\begin{aligned} w^{\text{UE}}(N, t) &= \sum_{e \in \{0, 1\}^N : |e| \leq t} w_e^{\text{UE}} \leq \sum_{e \in \{0, 1\}^N : |e| \leq t} w^{\text{full}}(N - 2t) \\ &= w^{\text{full}}(N - 2t) \left| \{e \in \{0, 1\}^N : |e| \leq t\} \right|. \end{aligned} \quad (24)$$

Finally we apply the Hamming bound for binary codes. ■

E. Main theorem

Theorem 2. Our QECM scheme is unclonable secure according to Definition 3, with

$$\tau(\lambda) = \frac{N}{2} + \left(\frac{N}{2} - t \right) \log(1 + 2\alpha) + t + \frac{1}{2} \log e. \quad (25)$$

Proof. The cloning attack in Definition 3 has a success probability equal to the winning probability in Game A. By Lemma 2, this equals the winning probability of Game B. Next, by Lemma 3 this is upper bounded by $2^{N-n} w^{\text{full}}(N - 2t)$. We use the fact that the full monogamy game C is harder (or equally hard) to win than the partial monogamy game 1. Thus we have $w^{\text{full}}(N - 2t) \leq \sqrt{e}(\frac{1}{2} + \alpha)^{\frac{N}{2}-t}$. ■

Remark. For $n \gg 1$, $\alpha \ll 1$ it holds that $\tau(\lambda) \approx \frac{N}{2}$. This is a large number; however, it still results in a winning probability that is exponentially small in n , which is the main objective for a QECM scheme.

We see from the result (25) that α needs to be smaller than approximately $\frac{1}{2}$; otherwise, the attackers' winning probability is not exponentially small in n . This is unsurprising, for the following reason. One obvious cloning attack on our scheme is to perform a *heterodyne* measurement on each cipherstate mode individually. This corresponds to mixing the squeezed state with the vacuum state using a 50:50 beam splitter. The effect is a deterioration of the signal-to-noise ratio: on the one hand, the signal power α^2 is reduced to $\alpha^2/2$. On the other hand, the noise power goes from $\frac{1}{2 \cosh r}$ to $\frac{1}{2}(\frac{1}{2} + \frac{1}{2 \cosh r})$ due to the averaging with the vacuum's shot noise, which has power $\frac{1}{2}$. The resulting signal-to-noise ratio in the heterodyne measurement is $2\alpha^2/(1 + \frac{1}{\cosh r}) \approx 2\alpha^2$. Hence at $\alpha = O(1)$ there is significant leakage about the codeword bits c_i , putting the unclonability at risk.

We consider the asymptotic case $n \rightarrow \infty$. In this limit the code rate approaches capacity and we write $n \approx N[1 - h(\beta)]$, where $h(\cdot)$ is the binary entropy function. From the security definition we have the requirement that $2^{-n+\tau}$ should be asymptotically small. Substituting $n \rightarrow N[1 - h(\beta)]$ in (25), the requirement $-n + \tau < 0$ can be rewritten as

$$h(\beta) - \left(\frac{1}{2} - \beta\right)[1 - \log(1 + 2\alpha)] < 0. \quad (26)$$

As β is a function of α and r (21), Eq. (26) specifies a region in the (α, r) plane where it is possible to achieve security asymptotically. This region is plotted in Fig. 2.

V. PRACTICAL CONSIDERATIONS

Since our main motivation for constructing CV-UE is to have a practically implementable scheme, we examine how the protocol behaves under realistic parameter choices and noise.

Generating highly squeezed light is experimentally challenging. We therefore restrict r to values that are reasonably close to the current state of the art. A 15 dB squeezed vacuum has been demonstrated [25] and 10 dB is common.¹

The bit error rate (BER) β is given by (21). We aim for a small BER, which in turn yields a small decryption-failure probability ε_{DF} (20). Figure 3(a) displays β as a function of r , at $\alpha = 0.4$.

As an example, consider $\alpha = 0.40$, $r = 3.4$, yielding $\beta = 0.014$. We take a ciphertext of size $N = 1000$ and we set $t = 35$ so that $t > N\beta$. Then (20) gives $\varepsilon_{\text{DF}} = 6.9 \times 10^{-6}$.

¹10 dB corresponds to $\cosh r = 10$, $r \approx 3$; 15 dB corresponds to $\cosh r = 10^{1.5} \approx 31.6$, $r \approx 4.15$.

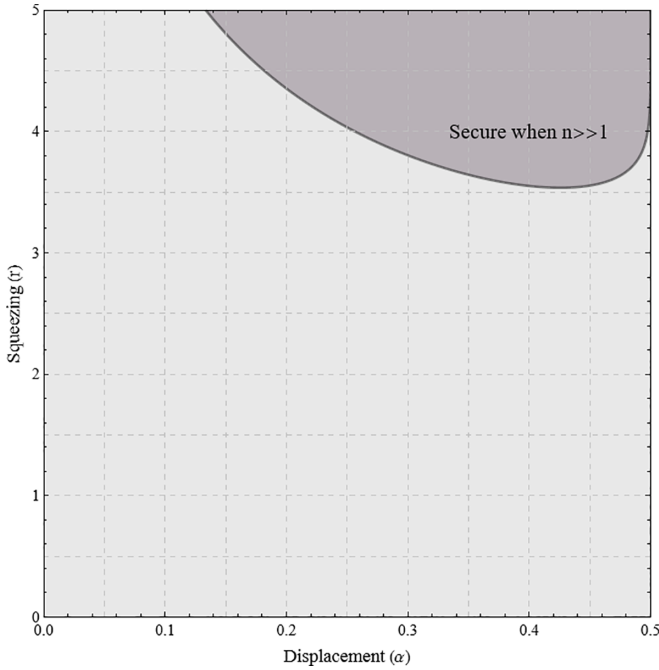


FIG. 2. Asymptotic condition (26) as a function of the squeezing r and displacement α .

Note that the actual message size in this case will be close to $N(1 - h(\beta)) \approx 892$. We will continue to use this relationship between N and n in the remainder of this section.

Robustness under noise

We model the optical channel by its transmittance $T \in [0, 1]$ and (input-referred) excess-noise power ξ in SNU [21]. In this model, the receiver's effective quadrature variance and displacement transform as

$$\frac{1}{\cosh r} \longrightarrow \frac{T}{\cosh r} + (1 - T) + T\xi, \quad \alpha \longrightarrow T\alpha, \quad (27)$$

which follows from the standard covariance-matrix transformation of a thermal-loss (attenuator) Gaussian channel and linear detection [20]. Detector inefficiency and electronics noise can be absorbed into the overall transmittance and noise budget in this framework [26]. Under the map (27), the BER becomes

$$\beta_{\text{noisy}} = \frac{1}{2} \operatorname{erfc} \left(\frac{T\alpha}{\sqrt{\frac{T}{\cosh r} + (1 - T) + T\xi}} \right). \quad (28)$$

This expression is plotted in Fig. 3(b) as a function of (T, ξ) for fixed (r, α) .

As an example, consider 5 km of standard single-mode optical telecom fiber at 1550 nm wavelength. The loss rate is 0.22 dB/km; at 5 km this corresponds to $T \approx 0.8$. At

12.63 dB squeezing ($r \approx 3.6$), Fig. 3(a) then gives a BER around 20%.² A BER of 20% is compatible with sufficiently low-rate binary error correction like the irregular LDPC codes [30,31]. A higher rate code could instead also be utilized if concatenated with a repetition code. This is the usual rate-versus-reliability trade-off for reducing the effective error probability before outer decoding [32].

Note that we assume that the adversaries are not using the noisy channel; they have $T = 1$ and $\xi = 0$. The channel properties hence need not enter the security analysis.

VI. DISCUSSION

We have introduced the first unclonable encryption scheme with continuous-variable states and have given a proof of unclonability in the game-based framework of [6]. We believe this analysis of an unclonable encryption protocol in the presence of realistic channel noise, marks a significant step toward practical quantum cryptography.

Making a meaningful comparison with prior work is difficult, since DV-CV performance cannot be fairly assessed by directly comparing the winning probabilities in the cloning game. The most informative benchmark is probably the DV analog of our scheme, which can be realized via Wiesner's conjugate coding [24]. Figure 4 plots the winning probability of our UE game as a function of message size, including also the UE game for conjugate coding into qubit states [6]. The conjugate coding scheme first one-time pads a message m and then bitwise encodes the ciphertext into the standard basis or the Hadamard basis. For experimentally feasible squeezing of $r = 3.6$ (≈ 15.6 dB), we observe exponentially decreasing probability of the adversaries winning only for longer message sizes in the order of 10^2 or greater. We emphasize that Fig. 4 is just an illustration for a single choice of parameters and is not intended as a comprehensive performance comparison.

We see several avenues for improvement. It is possible to get some extra tightness in the inequalities. The $\tau(\lambda)$ can be slightly improved by performing error correction on the q block and p block separately; this would change the $N - 2t$ in (23) to $N - t$.

It would be interesting to see if a tighter upper bound can be derived for the winning probability in Game C (full monogamy game). We have now used the upper bound for the *partial* game and we expect that this introduces a significant loss of tightness.

²The parameters used here are representative of current or near-current optical implementations. Standard commercial single-mode fiber at telecom wavelengths is commonly modeled with an attenuation of about 0.2 dB/km around 1550 nm and commercial G.652.D-compatible fibers such as Corning SMF-28 Ultra specify attenuation below this value, e.g., ≤ 0.18 dB/km at 1550 nm [27,28]. Thus using 0.22 dB/km is a conservative standard-fiber value; over 5 km it gives $T = 10^{-0.22 \times 5/10} \approx 0.776$. Strong squeezing at telecom wavelengths is also experimentally realistic: 3 dB squeezed vacuum at 1550 nm has been demonstrated with 12 mW pump power [29], while direct detection of 15 dB squeezed states has been reported [25].

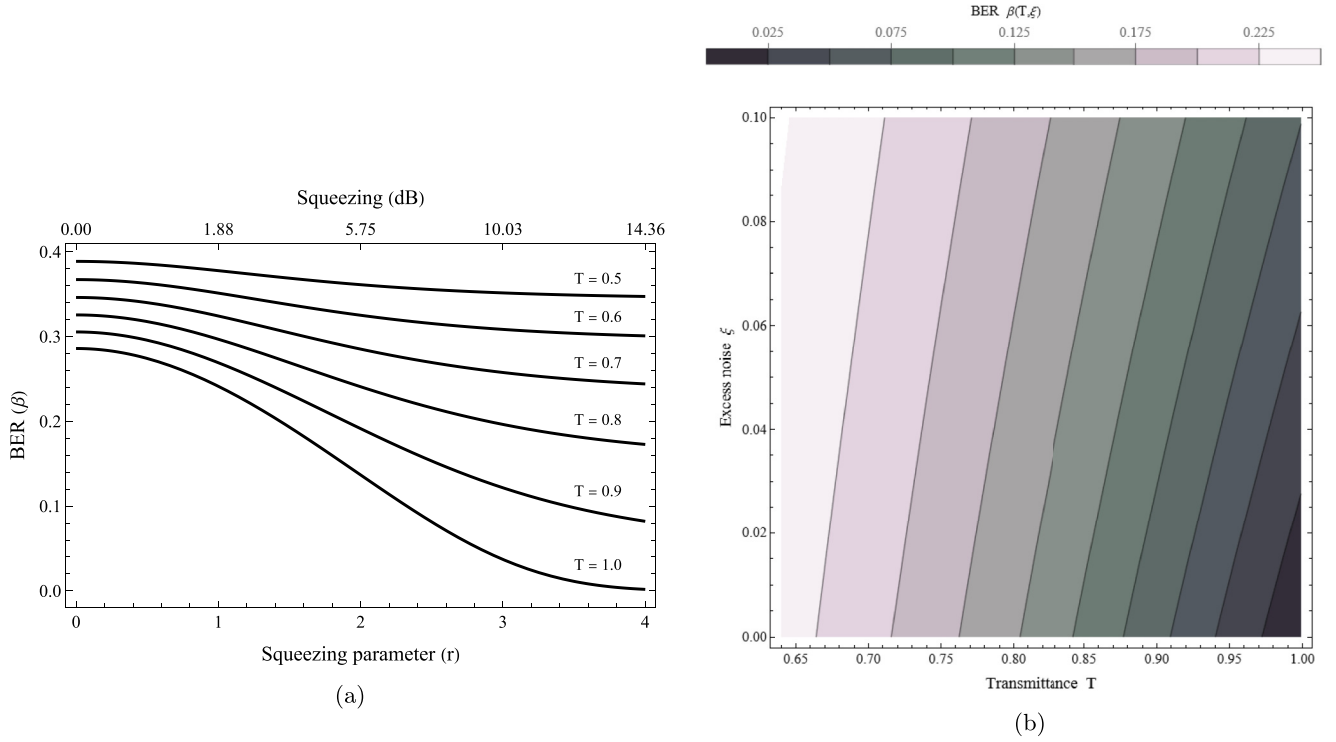


FIG. 3. Bit error rate (28) for different parameters (channel parameters in SNU). (a) β_{noisy} as a function of squeezing parameter r , at displacement $\alpha = 0.4$ plotted for various transmittance T . Excess noise $\xi = 0.001$ for all curves. (b) β_{noisy} as a function of channel transmittance T and excess noise ξ . Parameters: $r = 3.6$, $\alpha = 0.4$.

As discussed above, our results establish the security notion of *unclonability*, rather than the stronger guarantee of *unclonable indistinguishability*. Arguments based on monogamy of entanglement do not appear to yield guarantees beyond search security; establishing unclonable indistinguishability for CV protocols will likely require new proof techniques. We believe this is attainable and leave a full treatment to future work.

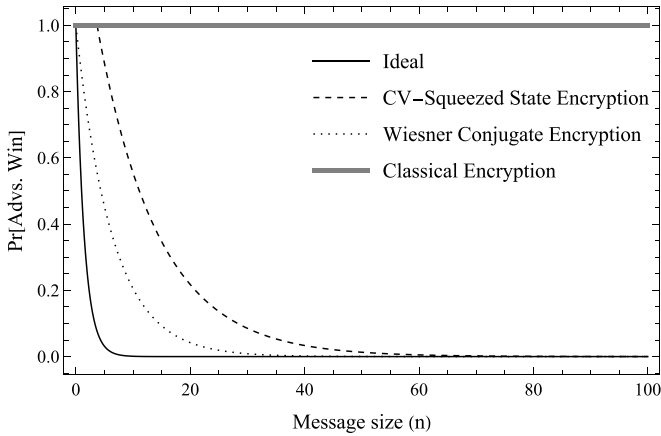


FIG. 4. Winning probabilities in the unclonability game for various schemes. The ideal curve is the simple guessing probability $(\frac{1}{2})^n$. The winning probability of the conjugate coding scheme is at most $(\frac{1}{2} + \frac{1}{2\sqrt{2}})^n$. For our CV scheme we plotted $2^{-n+\tau(\lambda)}$ (25) with parameters $r = 3.6$, $\alpha = 0.4$ and allow bit flips $t = 3.5\%$ of ciphertext size.

Furthermore, this work can pave the way for other schemes based on unclonability, for example, single-decryptor encryption [33] or revocable commitment.

ACKNOWLEDGMENT

The authors acknowledge that the work presented in this article was partially supported by the Nationaal Groeifonds Quantum Delta NL.

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

APPENDIX: ENTANGLED STATE

In the prepare-and-send scheme (Algorithm 2), we restrict k_i to the interval $(-\alpha \tanh r, \alpha \tanh r)$. To ensure compatibility with the EB version, the corresponding outcome u_i of the homodyne measurement on the Challenger's mode needs to be similarly restricted, $u_i - \alpha(-1)^{c_i} \in (-\alpha, \alpha)$. Consider the two-mode squeezed state without displacement:

$$|\text{EPR}_{r,\varphi}(0)\rangle = \frac{1}{\cosh \frac{r}{2}} \sum_{n=0}^{\infty} \left(-e^{i\varphi} \tanh \frac{r}{2} \right)^n |n, n\rangle. \quad (\text{A1})$$

In the position eigenbasis of both modes, the amplitude of this state can be represented using Hermite polynomials H_n . For

$\phi = 0$ we have

$$\langle x_1, x_2 | \text{EPR}_{r,0}(0) \rangle = \frac{e^{-\frac{1}{2}(x_1^2 + x_2^2)}}{\sqrt{\pi} \cosh \frac{r}{2}} \sum_{n=0}^{\infty} \frac{1}{n!} H_n(x_1) H_n(x_2) \left(\frac{1}{2} \tanh \frac{r}{2} \right)^n. \quad (\text{A2})$$

Using the identity $\sum_{n=0}^{\infty} \frac{1}{n!} H_n(x) H_n(y) \left(\frac{z}{2} \right)^n = \frac{1}{\sqrt{1-z^2}} \exp \left[\frac{2z}{1+z^2} xy - \frac{z^2}{1-z^2} (x-y)^2 \right]$, we can simplify the

expression to

$$\langle x_1, x_2 | \text{EPR}_{r,0}(0) \rangle = \frac{1}{\sqrt{\pi}} e^{-\frac{1}{4} e^r (x_1 - x_2)^2} e^{-\frac{1}{4} e^{-r} (x_1 + x_2)^2}. \quad (\text{A3})$$

Now we switch to the displaced EPR state, where both modes are translated over $\pm\alpha$ in the $\phi = 0$ direction,

$$\langle x_1, x_2 | \text{EPR}_{r,0}(\pm\alpha) \rangle = \frac{1}{\sqrt{\pi}} e^{-\frac{1}{4} e^r (x_1 - x_2)^2} e^{-\frac{1}{4} e^{-r} (x_1 + x_2 \mp 2\alpha)^2}. \quad (\text{A4})$$

Finally, we impose the restriction on the homodyne outcome by restricting the x_1 range,

$$|\text{EPR}_{r,0}(\pm\alpha)\rangle_{\text{restr}} \propto \int_{\pm\alpha-\alpha}^{\pm\alpha+\alpha} dx_1 |x_1\rangle \otimes \int_{-\infty}^{\infty} dx_2 |x_2\rangle \langle x_1, x_2 | \text{EPR}_{r,0}(\pm\alpha) \rangle \quad (\text{A5})$$

$$\propto \int_{\pm\alpha-\alpha}^{\pm\alpha+\alpha} dx_1 |x_1\rangle e^{-\frac{(x_1 \mp \alpha)^2}{2 \cosh r}} \otimes \int_{-\infty}^{\infty} dx_2 |x_2\rangle e^{-\frac{\cosh r}{2} [x_2 \mp \alpha - (x_1 \mp \alpha) \tanh r]^2} \quad (\text{A6})$$

$$= \int_{-\alpha}^{\alpha} dx |x \pm \alpha\rangle e^{-\frac{x^2}{2 \cosh r}} \otimes \int_{-\infty}^{\infty} dx' |x' \pm \alpha\rangle e^{-\frac{\cosh r}{2} [x' - x \tanh r]^2}. \quad (\text{A7})$$

It is not necessary to have a Gaussian-like distribution for the quadrature in the Challenger's mode. Here we specified an entangled state that resembles the standard TMS state, because it has a special property: the effect of

$|\text{EPR}_{r,\phi}(\pm\alpha)\rangle_{\text{restr}}$ can be obtained (although inefficiently) by taking the standard TMS state, homodyne measuring the Ch mode, and discarding if u_i does not lie in the right interval.

-
- [1] D. Dieks, Communication by EPR devices, *Phys. Lett. A* **92**, 271 (1982).
 - [2] J. L. Park, The concept of transition in quantum mechanics, *Found. Phys.* **1**, 23 (1970).
 - [3] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature (London)* **299**, 802 (1982).
 - [4] D. Gottesman, Uncloneable encryption, *Quantum Inf. Comput.* **3**, 581 (2003).
 - [5] D. Leermakers and B. Skoric, Qubit-based uncloneable encryption with key recycling *Quantum Inf. Comput.* **21**, 901 (2021).
 - [6] A. Broadbent and S. Lord, in *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, edited by S. T. Flammia, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 158 (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020), pp. 4:1–4:22.
 - [7] P. Ananth and F. Kaleoglu, in *Theory of Cryptography*, edited by K. Nissim and B. Waters (Springer International Publishing, Cham, 2021), pp. 299–329.
 - [8] D. Leermakers and B. Škorić, Two-way uncloneable encryption with a vulnerable sender, *Int. J. Quantum Inf.* **20**, 2150037 (2022).
 - [9] S. Kundu and E. Y.-Z. Tan, Device-independent uncloneable encryption, *Quantum* **9**, 1582 (2025).
 - [10] P. Ananth, F. Kaleoglu, X. Li, Q. Liu, and M. Zhandry, On the feasibility of uncloneable encryption, and more, *Cryptology ePrint Archive*, Paper 2022/884, 2022.
 - [11] C. Majenz, C. Schaffner, and M. Tahmasbi, Limitations on uncloneable encryption and simultaneous one-way-to-hiding, [arXiv:2103.14510](https://arxiv.org/abs/2103.14510).
 - [12] T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 010303(R) (1999).
 - [13] M. Hillery, Quantum cryptography with squeezed states, *Phys. Rev. A* **61**, 022309 (2000).
 - [14] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, *Phys. Rev. A* **62**, 062308 (2000).
 - [15] N. J. Cerf, M. Lévy, and G. van Assche, Quantum distribution of Gaussian keys using squeezed states, *Phys. Rev. A* **63**, 052311 (2001).
 - [16] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
 - [17] F. Grosshans, G. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature (London)* **421**, 238 (2003).
 - [18] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, *Quantum Inf. Comput.* **3**, 535 (2003).
 - [19] 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).
 - [20] R. Garcia-Patron Sanchez, Quantum information with optical continuous variables: From Bell tests to key

- distribution, Ph.D. thesis, Université libre de Bruxelles, 2007, <https://scispace.com/pdf/quantum-information-with-optical-continuous-variables-29lk8i20m.pdf>.
- [21] A. Leverrier, Theoretical study of continuous-variable quantum key distribution, Ph.D. thesis, Télécom ParisTech, 2009, <https://pastel.hal.science/tel-00451021/file/thesis.pdf>.
- [22] 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).
- [23] E. Culf, T. Vidick, and V. V. Albert, Group coset monogamy games and an application to device-independent continuous-variable QKD, [arXiv:abs/2212.03935](https://arxiv.org/abs/2212.03935).
- [24] S. Wiesner, Conjugate coding, *SIGACT News* **15**, 78 (1983).
- [25] 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).
- [26] S. Yamano, T. Matsuura, Y. Kuramochi, T. Sasaki, and M. Koashi, General treatment of Gaussian trusted noise in continuous variable quantum key distribution, <https://arxiv.org/abs/2305.17684>.
- [27] ITU-T Focus Group on Quantum Information Technology for Networks, Quantum key distribution network transport technologies, Tech. Rep. *FG QIT4N D2.4*, International Telecommunication Union, 2021.
- [28] Corning Incorporated, Corning SMF-28 Ultra optical fiber: Product information, 2025, product information sheet PI1424, <https://www.corning.com/opticalcommunications/worldwide/en/home/products/fiber.html>.
- [29] A. Schönbeck, F. Thies, and R. Schnabel, 13 dB squeezed vacuum states at 1550 nm from 12 mW external pump power at 775 nm, *Opt. Lett.* **43**, 110 (2018).
- [30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley-Interscience, New York, 2006).
- [31] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, Design of capacity-approaching irregular low-density parity-check codes, *IEEE Trans. Inf. Theory* **47**, 619 (2001).
- [32] G. D. Forney, *Concatenated Codes* (MIT Press, Cambridge, MA, 1966).
- [33] M. Georgiou and M. Zhandry, Unclonable decryption keys, *Cryptology ePrint Archive*, Paper 2020/877, 2020.