Editors' Suggestion

Encrypted Qubits Can Be Cloned

Koji Yamaguchi[1,2,*,†] and Achim Kempf[1,3,4,5,‡]
[1]Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[2]Department of Communication Engineering and Informatics, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan
[3]Department of Physics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[4]Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[5]Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada

(Received 14 January 2025; revised 21 May 2025; accepted 14 November 2025; published 6 January 2026)

We show that encrypted cloning of unknown quantum states is possible. Any number of encrypted clones of a qubit can be created through a unitary transformation, and each of the encrypted clones can be decrypted through a unitary transformation. The decryption of an encrypted clone consumes the decryption key; i.e., only one decryption is possible, in agreement with the no-cloning theorem. Encrypted cloning represents a new paradigm that provides a form of redundancy, parallelism, or scalability where direct duplication is forbidden by the no-cloning theorem. For example, a possible application of encrypted cloning is to enable encrypted quantum multicloud storage.

DOI: 10.1103/y4y1-1ll6

The no-cloning theorem [1,2] shows that it is impossible to create an identical clone of an unknown quantum state, a fact that fundamentally limits the processing of quantum information. The theorem arises from the unitarity of quantum mechanics and shares a close relationship with the no-signaling principle [3–6]. The no-cloning theorem has spurred further related research, such as broadcasting of mixed states [7], imperfect cloning [8–12], and probabilistic cloning [13,14] (see, e.g., Refs. [15,16] for review). The implications of the no-cloning theorem are far reaching, spanning a wide array of research areas in both quantum information science and fundamental physics, including quantum communication [17–21], quantum error correction [22], quantum cryptography [23–27], quantum estimation [28,29], and black hole physics [30,31].

In this context, we here show that encrypted cloning of an unknown quantum state is possible. Crucially, this protocol generates multiple redundant, indirectly accessible encrypted copies, rather than multiple simultaneously accessible identical quantum states, thus strictly adhering to the no-cloning theorem.

To this end, we explicitly show that any number $n > 1$ of encrypted clones of a qubit A can be produced through a unitary transformation and that each of the encrypted clones can be decrypted through a unitary transformation. The decryption of an encrypted clone consumes the decryption key; i.e., only one decryption is possible, in agreement with the no-cloning theorem. The number of gate operations needed for the encryption and decryption scales linearly with the number of clones.

The new method of encrypted cloning (see Fig. 1) begins with the preparation of n pairs of maximally entangled qubits, (S_i, N_i), $i = 1, \ldots, n$, where we will refer to the S_i and N_i as signal qubits and noise qubits, respectively. The method of encrypted cloning then has A interact with all signal qubits $S_i, i = 1, \ldots, n$, through a unitary operator $U_{\text{enc}}^{(n)}$ that acts nontrivially only on qubit A and the signal qubits. Through this encoding operation, complete information about qubit A gets imprinted into each of the signal qubits S_i. At the same time, each of these imprints is encrypted due to the quantum noise in the S_i from their initial maximal entanglement with the N_i. We will call the imprinted signal qubits S_i the encrypted clones of the original state of A.

The noise qubits $N_i, i = 1, \ldots, n$, do not take part in the process of encrypted cloning; i.e., $U_{\text{enc}}^{(n)}$ acts as the identity on the Hilbert space of the N_i. Therefore, the N_i acquire neither classical nor quantum information about A. Instead, the role of the noise qubits is to keep a record of the quantum noise in the signal qubits so that, together, the set of all noise qubits $N_i, i = 1, \ldots, n$, forms the encryption key. By using and thereby consuming this key, any one and only one of the encrypted clones S_i can then be decrypted

*Present address: Department of Informatics, Faculty of Information Science and Electrical Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan.
†Contact author: koji.yamaguchi@inf.kyushu-u.ac.jp
‡Contact author: akempf@uwaterloo.ca

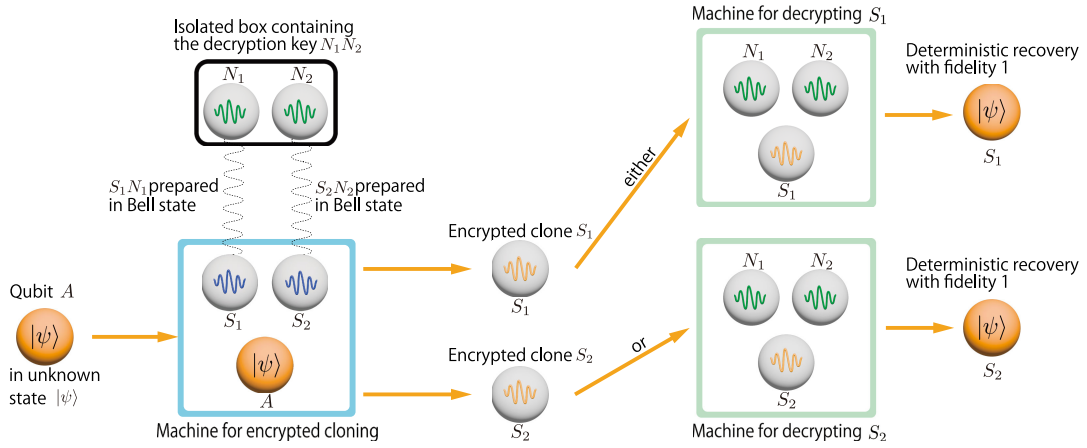

FIG. 1. The protocol for $n = 2$. Qubits whose reduced state is maximally mixed are represented by spheres displaying fluctuations. The initial maximal mixedness of S_1 and S_2, which stems from their being prepared in Bell states with N_1 and N_2, respectively, provides the quantum noise for the encryption. N_1 and N_2 keep a record of this quantum noise and can, therefore, later be used to denoise or decrypt either S_1 or S_2. Crucially, the decryption machine consumes N_1 and N_2, so that only one decryption can be performed. Therefore, only one unencrypted version of the original state of A can exist at a time, which enables consistency with the no-cloning theorem.

to reproduce the original state of qubit A. The decryption or "denoising" of an encrypted clone S_k is accomplished by a unitary $U_{\text{dec}}^{(n)}$ that acts nontrivially only on S_k and the noise qubits N_i, $i = 1, \ldots, n$, and it reproduces the original state of qubit A in qubit S_k.

Example application: Quantum encrypted multicloud storage—Let us consider a scenario in which the owner of quantum data requires for security reasons that these data are stored (a) off site, (b) redundantly in multiple quantum clouds to protect, e.g., from hardware failures, and (c) encrypted, with the key kept by the owner on site.

The new method of encrypted cloning can be used for this purpose. To this end, the owner of a qubit A creates n encrypted clones and distributes them to n quantum clouds for storage. The owner can then discard the original qubit A. The owner retains the n noise qubits, which together serve as the key. Condition (a) is fulfilled because on site are only the noise qubits and they do not carry information about qubit A. Condition (b) is fulfilled since the owner can decrypt (i.e., denoise) any one of the redundantly stored encrypted clones to recover qubit A, by using the noise qubits. Condition (c) is fulfilled since each of the encrypted clones that are hosted off site in one of the quantum clouds is maximally mixed and independent of the initial state of A.

The method of encrypted cloning—We consider n qubits S_i, $i = 1, \ldots, n$, called signal qubits, and n qubits N_i, $i = 1, \ldots, n$, called noise qubits with each pair (S_i, N_i) prepared in this maximally entangled state:

$$|\phi\rangle_{S_iN_i} := \frac{1}{\sqrt{2}}(|0\rangle_{S_i}|0\rangle_{N_i} + |1\rangle_{S_i}|1\rangle_{N_i}). \tag{1}$$

We denote the identity operator and the Pauli operators for the ith signal and noise qubits by $\{\sigma_\mu^{(S_i)}\}_{\mu=0,1,2,3}$ and $\{\sigma_\mu^{(N_i)}\}_{\mu=0,1,2,3}$, respectively, in their $\{|0\rangle, |1\rangle\}$ basis.

The owner of quantum data, say, Alice, possesses a qubit A and aims to create n encrypted clones of the state of qubit A. To this end, Alice lets her qubit A interact with the n signal qubits $\{S_i\}_{i=1}^n$ through the following unitary encrypted cloning operation:

$$U_{\text{enc}}^{(n)} := e^{-(\pi i/4)\sigma_1^{(A)}\otimes(\otimes_{i=1}^n\sigma_1^{(S_i)})}e^{-(\pi i/4)\sigma_3^{(A)}\otimes(\otimes_{i=1}^n\sigma_3^{(S_i)})}. \tag{2}$$

Here, the superscript of each Pauli operator denotes the subsystem that this Pauli operator acts on. The unitary $U_{\text{enc}}^{(n)}$ acts as the identity operator on the noise qubits' tensor factor of the Hilbert space. Therefore, when $U_{\text{enc}}^{(n)}$ is compiled into a succession of native gates of a quantum processor, no gates act on the noise qubits; i.e., the noise qubits are noninteracting ancillas that may as well be kept physically apart. Hence, the noise qubits carry neither classical nor quantum information about Alice's qubit.

Decryption: Proof of full recovery—After the process of encrypted cloning, Bob (which can also be Alice) attempts to recover the initial state of qubit A from a subset of the signal qubits and noise qubits. Correspondingly, we consider this quantum channel from Alice to Bob:

$$\mathcal{N}_{A\to B}^{(n)}(\rho_A) := \text{Tr}_{\bar{B}}\left\{U_{\text{enc}}^{(n)}\left[\rho_A \otimes \left(\bigotimes_{i=1}^n \phi_{S_iN_i}\right)\right]U_{\text{enc}}^{(n)\dagger}\right\}. \tag{3}$$

Here, we defined $\phi_{S_iN_i} := |\phi\rangle\langle\phi|_{S_iN_i}$. Also, we let B denote the qubit(s) that Bob chooses to use to try to reproduce the original state ρ_A of qubit A. We let $\bar{B}$ denote the complementary system to B. For example, if $B = S_1$, then $\bar{B} = AS_2\ldots S_nN_1\ldots N_n$. Our aim is to show that if Bob uses any one signal qubit, S_i, and all noise qubits, $N_1, \ldots, N_n$, then Bob can retrieve Alice's qubit perfectly, in the sense that the

channel from Alice to Bob is of full quantum capacity C_Q:

$$C_Q(\mathcal{N}^{(n)}_{A\to S_iN_1N_2\ldots N_n}) = 1. \tag{4}$$

We will see that the capacity drops to zero if Bob omits even only one noise qubit.

We prove Eq. (4) by explicitly constructing a decrypting operation (we provide an alternative proof using coherent information in Supplemental Material [32]). To this end, we show that Alice's initial state ρ_A is fully recovered from $S_1N_1N_2\ldots N_n$ by the decrypting operation $\mathcal{D}^{(n)}_{S_1N_1N_2\ldots N_n\to S_1}$ defined for $n > 1$ by

$$\mathcal{D}^{(n)}_{S_1N_1N_2\ldots N_n\to S_1}(\cdots) \coloneqq \mathrm{Tr}_{N_1N_2\ldots N_n}\left(U^{(n)}_{\mathrm{dec}}(\cdots)U^{(n)\dagger}_{\mathrm{dec}}\right),$$
$$U^{(n)}_{\mathrm{dec}} \coloneqq \sum_{\mu=0}^{3}\alpha_\mu\left(|\phi_\mu\rangle\langle\phi_\mu|_{S_1N_1}\right)\otimes\left(\bigotimes_{j=2}^{n}\sigma_\mu^{(N_j)\top}\right). \tag{5}$$

Here, $|\phi_\mu\rangle_{S_iN_i} \coloneqq \sigma_\mu^{(S_i)}\otimes\mathbb{I}^{(N_i)}|\phi\rangle_{S_iN_i}$, $\top$ denotes the transpose operation with respect to the computational basis $\{|0\rangle,|1\rangle\}$, and the coefficients are defined by $\alpha_0 \coloneqq 1$, $\alpha_1 = \alpha_3 \coloneqq \mathrm{i}$, and $\alpha_2 \coloneqq -\mathrm{i}^{n+1}$.

First, it is straightforward to check that $U^{(n)}_{\mathrm{dec}}$ is unitary by using the fact that $\{|\phi_\mu\rangle_{S_iN_i}\}_{\mu=0}^{3}$ forms an orthonormal basis of a two-qubit system and $|\alpha_\mu|^2 = 1$. Therefore, $\mathcal{D}^{(n)}_{S_1N_1N_2\ldots N_n\to S_1}$ is a quantum channel. Second, from Eq. (2), we find

$$\begin{aligned}U^{(n)}_{\mathrm{enc}} &= \left[\cos(\pi/4)\mathbb{I} - \mathrm{i}\sin(\pi/4)\sigma_1^{(A)}\otimes\left(\bigotimes_{i=1}^{n}\sigma_1^{(S_i)}\right)\right]\\ &\quad\times\left[\cos(\pi/4)\mathbb{I} - \mathrm{i}\sin(\pi/4)\sigma_3^{(A)}\otimes\left(\bigotimes_{i=1}^{n}\sigma_3^{(S_i)}\right)\right]\\ &= \frac{1}{2}\sum_{\mu=0}^{3}\alpha_\mu^{-1}\sigma_\mu^{(A)}\otimes\left(\bigotimes_{i=1}^{n}\sigma_\mu^{(S_i)}\right),\end{aligned} \tag{6}$$

where we have used $\sigma_1^{\otimes(n+1)}\sigma_3^{\otimes(n+1)} = (-\mathrm{i})^{n+1}\sigma_2^{\otimes(n+1)}$. Therefore, we get

$$\begin{aligned}&U^{(n)}_{\mathrm{enc}}\left[|\psi\rangle_A\otimes\left(\bigotimes_{i=1}^{n}|\phi\rangle_{S_iN_i}\right)\right]\\ &\quad= \frac{1}{2}\sum_{\mu=0}^{3}\alpha_\mu^{-1}\sigma_\mu^{(A)}|\psi\rangle_A\otimes\left(\bigotimes_{i=1}^{n}|\phi_\mu\rangle_{S_iN_i}\right),\end{aligned} \tag{7}$$

implying that

$$\begin{aligned}&\left(U^{(n)}_{\mathrm{dec}}\otimes\mathbb{I}_{AS_2S_3\ldots S_n}\right)U^{(n)}_{\mathrm{enc}}\left[|\psi\rangle_A\otimes\left(\bigotimes_{i=1}^{n}|\phi\rangle_{S_iN_i}\right)\right]\\ &\quad= \frac{1}{2}\left(\sum_{\mu=0}^{3}\sigma_\mu^{(A)}\otimes\sigma_\mu^{(S_1)}\otimes\mathbb{I}\right)|\psi\rangle_A\otimes\bigotimes_{i=1}^{n}(|\phi\rangle_{S_iN_i}),\end{aligned} \tag{8}$$

where we have used $\sigma_\mu^{(S_i)}\otimes\sigma_\mu^{(N_i)\top}|\phi\rangle_{S_iN_i} = |\phi\rangle_{S_iN_i}$. Since $\frac{1}{2}\sum_{\mu=0}^{3}\sigma_\mu^{(A)}\otimes\sigma_\mu^{(S_1)}$ is a SWAP operation between A and S_1 and since $\mathcal{N}^{(n)}_{A\to S_1N_1N_2\ldots N_n}(\cdots) = \mathrm{Tr}_{AS_2S_3\ldots S_n}[U^{(n)}_{\mathrm{enc}}(\cdots\bigotimes_{i=1}^{n}\phi_{S_iN_i})U^{(n)\dagger}_{\mathrm{enc}}]$, we conclude that

$$\mathcal{D}^{(n)}_{S_1N_1N_2\ldots N_n\to S_1}\circ\mathcal{N}^{(n)}_{A\to S_1N_1N_2\ldots N_n}(|\psi\rangle\langle\psi|_A) = |\psi\rangle\langle\psi|_{S_1} \tag{9}$$

holds for any initial pure state $|\psi\rangle_A$ of Alice's qubit. Therefore, Alice's initial state can be retrieved perfectly from $S_1N_1N_2\ldots N_n$. As one can also decrypt the same information from $S_iN_1N_2\ldots N_n$ due to the symmetry under exchanging the roles of S_1N_1 and S_iN_i in the decoding operation, Eq. (4) is proven for any i. Therefore, Bob can recover the original state of qubit A using one arbitrary signal qubit and all noise qubits. One signal qubit alone would not be sufficient to recover the original state of A, since otherwise it could also be recovered from the remaining signal qubits due to symmetry, thereby violating the no-cloning theorem. Indeed,

$$C_Q(\mathcal{N}^{(n)}_{A\to S_i}) = 0 \quad \text{(no cloning)}, \tag{10}$$

since $\mathcal{N}^{(n)}_{A\to S_i}$ is antidegradable due to the permutation symmetry among signal qubits, and the quantum capacity vanishes for any antidegradable channel [17–21]. We remark that the present results were inspired by our prior work [42,43] on classical and quantum denoising.

In conclusion, each signal qubit contains an encrypted but perfect clone of Alice's original qubit A. As we show in Supplemental Material [32], each clone is perfectly encrypted in the sense that it is noisy to the extent that each individually is in a maximally mixed state. Yet, each encrypted clone is also a perfect copy of the original state of A in the sense that the original state of A can be perfectly recovered from the encrypted clone by denoising or "decoding" or "decrypting"—we will here use these three terms interchangeably—using only the noise qubits which never interacted with A and, therefore, contain no classical or quantum information about A.

Let us clarify that consistency with the no-cloning theorem demands that, after decrypting one signal qubit, it is impossible to reuse the noise qubits to decrypt another signal qubit. Indeed, after decoding, as Eq. (8) shows, the state of the $(n-1)$ unused signal qubits and n noise qubits is independent of Alice's information. Of course, it would not violate no cloning if, after denoising one signal qubit, Bob runs the unitary decoding operation Eq. (5) in reverse and then chooses to denoise another signal qubit.

We remark that, trivially, the pair of encoding and decoding unitary operations, as in Eqs. (2) and (5), can be replaced by rotated versions. For example, $\sigma_3^{(A)}\otimes\left(\bigotimes_{i=1}^{n}\sigma_3^{(S_i)}\right)$ can be replaced with $\sigma_2^{(A)}\otimes$

$\left(\bigotimes_{i=1}^{n}\sigma_2^{(S_i)}\right)$ while, in the encoding operation in Eq. (2), the coefficients α_μ in Eq. (7) change into $\alpha_0 = 1$, $\alpha_1 = \alpha_2 = \mathrm{i}$, and $\alpha_3 = -(-\mathrm{i})^{n+1}$. Then, Alice's quantum information can be retrieved using the decoding operation (5) with these coefficients. More generally, the encoding and decoding unitaries of Eqs. (2) and (5) can be replaced by any of the infinitely many unitaries that act the same way on the initial states and on the encoded states, respectively. The choice of encoding and decoding unitaries can be important in practical applications, where the encoding and decoding unitaries need to be decomposed, i.e., compiled into the universal native one- and two-qubit gates of a given quantum processor [44–46]. As we also show in Supplemental Material [32], the number of two-qubit gates that is required to implement the copying and retrieval operations scales well, namely, by growing only linearly with n.

We here remark that, in recent experimental work in progress with Tutschku, Rullkötter, Wagner, and Shehzad, we successfully implemented encrypted cloning and the subsequent decryption for up to $n = 10$ on a quantum processor [47]. For variants of the protocol, see the Appendix in End Matter.

Relationship to other phenomena—

From classical one-time pads to quantum multitime pads: The encryption aspect of the new encrypted cloning method can also be understood in analogy to classical one-time pad (OTP) cryptography. This is because the quantum information that is imprinted on the signal qubits is perfectly masked by noise, as if from an OTP, the noise being here the quantum noise from the initial maximal entanglement between the signal and noise qubits. The noise qubits, therefore, represent an analog of a one-time pad, except that in the quantum case, the pad can actually be reused without compromising security. This is because the encrypted cloning method encrypts and decrypts without measurements, unitarily, in such a way that, after decryption, the n maximally entangled pairs are restored and are, therefore, available again for encryption.

Consistency with the no quantum summoning theorem: Quantum summoning [48–51] is an adversarial game played in spacetime. At an event X, player 1 gives player 2 a qubit A. Then, at some event Y_i from a preagreed upon set of events in the causal future of X, player 1 asks player 2 to produce qubit A. Player 2 is able to win this challenge if all events Y_i are timelike to another, because then player 2 can transport or teleport qubit A from one Y_i to the next until it is summoned by player 1. The no quantum summoning theorem states that player 2 cannot possess an always-winning strategy if some of the Y_i are spacelike to another, as this would contradict no cloning.

While encrypted cloning is clearly consistent with the no quantum summoning theorem, the application of encrypted cloning to quantum encrypted multicloud storage also shows that a variant of quantum summoning is possible also for spacelike separated Y_i: Player 2 deposits encrypted clones at each of the Y_i. Then, player 1 can summon qubit A at any Y_i of her choosing—even if some or all of the Y_i are spacelike separated from another—provided that player 1 brings the decryption key, i.e., the noise qubits. Recall that the noise qubits do not carry any classical or quantum information about A.

Consistency with quantum secret sharing: The new encrypted cloning method is consistent not only with the no-cloning theorem, but also with quantum secret sharing [52,53]. To see this, we need to consider what in quantum secret sharing is called the access structure, namely, the list of so-called authorized or unauthorized sets of parties (subsystems) from which a secret qubit can or cannot be recovered, respectively. In encrypted cloning, any subsystem containing one pair of signal and noise qubits and one half of each of the remaining $(n-1)$ pairs is authorized, while any subsystem of $(n-1)$ pairs or n noise qubits is unauthorized. As is easy to check, the two necessary and sufficient conditions required for quantum secret sharing [53], namely, (a) that the complement of any authorized set is unauthorized and (b) monotonicity, i.e., that any superset of an authorized set is authorized, are readily verified.

Since any quantum secret sharing scheme can correct erasure errors on the complementary system to an authorized set [52], encrypted cloning can, therefore, also be viewed as an error-correcting code. For example, after encrypted cloning, the original state of qubit A can be retrieved even if $(n-1)$ signal qubits are lost.

Consistency with entanglement monogamy: Let us assume that qubit A is initially maximally entangled with an ancilla qubit $\tilde{A}$. After the encrypted cloning, $\tilde{A}$ is, therefore, simultaneously maximally entangled with each set of qubits from which the original state of A can be recovered.

This fact does not violate entanglement monogamy [54], since the monogamy argument applies to only disjoint sets of subsystems, while in encrypted cloning every set of qubits from which the original state of A can be reconstructed overlaps with any other such set.

Relation to the Hayden-Preskill model: Similar to encrypted cloning, which assumes that initially we have a number of maximally entangled pairs of signal and noise qubits, in the case of black holes, the degrees of freedom of the black hole and the degrees of freedom of the Hawking radiation that it has emitted by the Page time can be assumed to be maximally entangled. Then, similar to the imprinting of a qubit A into the signal qubits in encrypted cloning, when sending a qubit A into a black hole, it may become imprinted into the degrees of freedom in the black hole through fast scrambling. In encrypted cloning, A can be recovered from even just a single one of the encrypted clones S_i. Similarly in spirit, in the Hayden-Preskill model [30], as soon as some more of the degrees of freedom (perhaps analogous to the imprinted signal qubits)

evaporate from the black hole, qubit A can be recovered with the help of all of the prior degrees of freedom of the Hawking radiation (analogous to the noise qubits).

Outlook—While technical tools used in encrypted cloning, such as the manipulation of multipartite entanglement, are also foundational in quantum error correction [55–58] and quantum secret sharing [52,53], the operational goals and applications differ. Encrypted cloning is not designed to protect against computational errors (as in quantum error correction) or to restrict information access among agents (as in quantum secret sharing). Instead, it enables the creation of encrypted yet decryptable clones of an unknown quantum state—a new functionality, relevant in contexts where classical copying is essential, but forbidden quantum mechanically by the no-cloning theorem. (And the encrypted cloning protocol achieves this entirely unitarily, without syndrome measurements or classical communication, and permits arbitrary selection of the decrypted clone.)

For example, as we discussed, the new encrypted cloning paradigm naturally enables quantum multicloud storage, and it will be very interesting to explore its extension to quantum multicloud parallel homomorphic, or "blind," computation.

More generally, the paradigm of encrypted cloning can also be seen as a method to evade a constraint imposed by unitarity, namely, in this case the no-cloning constraint. To this end, encrypted cloning enlarges the system with ancillas, thereby leaving the original system an open system. Quantum noise is then introduced through maximum entanglement with ancillas—but in such a way that later denoising is possible.

This is reminiscent of how unitarity also forces quantum linear amplifiers to introduce quantum noise [59,60]. It will be interesting, therefore, to explore whether an encrypted cloning-type approach can be used to develop new quantum amplifier architectures in which the necessary quantum noise is introduced through maximally entangled pairs—in such a way that halves of these pairs may later serve to at least partially denoise a quantum amplified signal. Similarly, also the no-programming theorem [61,62] arises from unitarity and an encrypted cloning approach may, therefore, provide a new perspective.

It should also be very interesting to explore an encrypted cloning approach for quantum sensing. Useful for sensing could also be the fact that, for large n, the ability to recover qubit A can be extremely sensitive to any interactions that a to-be-probed system may have with the n noise qubits.

Vice versa, in encrypted cloning we have enhanced robustness in the transmission of the signal qubits, in the sense that if n signal qubits are sent, it suffices that even just one arrives to achieve full recovery. For example, one may envision a quantum radar-type setup (see Ref. [63]), in which n noise qubits in photons are kept as idlers while n signal photons are emitted, of which only one signal photon needs to be received.

Finally, it will also be interesting to generalize encrypted cloning from qubits to qudits and to explore the corresponding scaling of the minimal resources needed.

Acknowledgments—K. Y. acknowledges support from the Japan Society for the Promotion of Science (JSPS) Overseas Research Fellowships and JSPS Grants-in-Aid for Scientific Research No. JP24KJ0085. A. K. acknowledges support through the Dieter Schwarz Foundation, a Discovery Grant of the National Science and Engineering Council of Canada (NSERC), an Applied Quantum Computing Challenge Grant from the National Research Council of Canada (NRC), a Discovery Project grant of the Australian Research Council (ARC), and support from Perimeter Institute which is supported in part by the Government of Canada through the Department of Innovation, Science and Industry Canada and by the Province of Ontario through the Ministry of Colleges and Universities.

Data availability—No data were created or analyzed in this Letter.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[3] N. Herbert, Found. Phys. **12**, 1171 (1982).
[4] N. Gisin, Phys. Lett. A **242**, 1 (1998).
[5] P. Navez and Nicolas J. Cerf, Phys. Rev. A **68**, 032313 (2003).
[6] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[7] H. Barnum, Carlton M. Caves, Christopher A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[8] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[9] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[10] D. Bruß, D. P. DiVincenzo, A. Ekert, Christopher A. Fuchs, C. Macchiavello, and John A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[11] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[12] M. Keyl and R. F. Werner, J. Math. Phys. (N.Y.) **40**, 3283 (1999).
[13] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[14] A. K. Pati, Phys. Rev. Lett. **83**, 2849 (1999).
[15] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).
[16] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, Phys. Rep. **544**, 241 (2014).
[17] Charles H. Bennett, D. P. DiVincenzo, and John A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).
[18] V. Giovannetti, S. Lloyd, L. Maccone, and Peter W. Shor, Phys. Rev. A **68**, 062323 (2003).
[19] V. Giovannetti, S. Lloyd, L. Maccone, and Peter W. Shor, Phys. Rev. Lett. **91**, 047901 (2003).
[20] F. Caruso and V. Giovannetti, Phys. Rev. A **74**, 062307 (2006).

[21] A. S. Holevo, Probl. Inf. Transm. **44**, 171 (2008).
[22] D. E. Gottesman, Stabilizer codes and quantum error correction, Ph.D. thesis, California Institute of Technology, 1997.
[23] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
[24] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[25] Nicolas J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[26] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[27] V. Scarani, H. Bechmann-Pasquinucci, Nicolas J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[28] D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).
[29] J. Bae and A. Acín, Phys. Rev. Lett. **97**, 030402 (2006).
[30] P. Hayden and J. Preskill, J. High Energy Phys. 09 (2007) 120.
[31] Samuel L. Braunstein, S. Pirandola, and K. Życzkowski, Phys. Rev. Lett. **110**, 101301 (2013).
[32] See Supplemental Material at http://link.aps.org/supplemental/10.1103/y4y1-1ll6 for further details, which includes Refs. [33–41].
[33] H. Barnum, E. Knill, and M. Nielsen, IEEE Trans. Inf. Theory **46**, 1317 (2000).
[34] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[35] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[36] P. Shor, in *Lecture Notes, MSRI Workshop on Quantum Computation* (2002), https://www.slmath.org/workshops/203/schedules/1181.
[37] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[38] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013).
[39] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England, 2010).
[41] N. Yu, R. Duan, and M. Ying, Phys. Rev. A **88**, 010304(R) (2013).
[42] K. Yamaguchi, A. Ahmadzadegan, P. Simidzija, A. Kempf, and E. Martín-Martínez, Phys. Rev. D **101**, 105009 (2020).
[43] A. Ahmadzadegan, P. Simidzija, M. Li, and A. Kempf, Sci. Rep. **11**, 21624 (2021).
[44] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[45] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[46] A. Barenco, Charles H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[47] K. Yamaguchi, L. Rullkötter, C. Tutschku, S. Wagner, I. Shehzad, and A. Kempf (in preparation)
[48] A. Kent, Classical Quantum Gravity **29**, 224013 (2012).
[49] A. Kent, Quantum Inf. Process. **12**, 1023 (2013).
[50] P. Hayden and A. May, J. Phys. A **49**, 175304 (2016).
[51] E. Adlam and A. Kent, Phys. Rev. A **93**, 062327 (2016).
[52] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[53] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[54] V. Coffman, J. Kundu, and William K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[55] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[56] J. Roffe, Contemp. Phys. **60**, 226 (2019).
[57] T. A. Brun, in *Oxford Research Encyclopedia of Physics* (Oxford University Press, New York, 2020).
[58] I. Georgescu, Nat. Rev. Phys. **2**, 519 (2020).
[59] H. A. Haus and J. A. Mullen, Phys. Rev. **128**, 2407 (1962).
[60] Carlton M. Caves, Phys. Rev. D **26**, 1817 (1982).
[61] M. A. Nielsen and Isaac L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[62] Y. Yang, R. Renner, and G. Chiribella, Phys. Rev. Lett. **125**, 210501 (2020).
[63] S. Lloyd, Science **321**, 1463 (2008).

End Matter

Appendix: Variants of the protocol—Let us consider the scenario where the owner of the quantum data, Alice, loses access to some of the n noise qubits but retains access to at least one noise qubit. In this case, the owner can still recover the original state of A from any subsystem composed of one pair of signal and noise qubits plus at least one half of each of the remaining $(n-1)$ pairs of signal and noise qubits. For example, the original state of A can be recovered using S_1S_2 and $N_1N_3N_4\ldots N_n$ by replacing $\sigma_\mu^{(N_2)\top}$ with $\sigma_\mu^{(S_2)}$ in Eq. (5). While, therefore, the loss of some noise or signal qubits can be compensated, the loss of even just one pair of signal and noise qubits makes it impossible to retrieve qubit A, and the channel capacity drops to zero. This is because the reduced state of $(n-1)$ pairs of signal and noise qubits is given by $\frac{1}{4}\sum_{\mu=0}^{3}|\phi_\mu\rangle\langle\phi_\mu|^{\otimes(n-1)}$ after the encoding, independently of $|\psi\rangle_A$, as seen in Eq. (7). However, in the case where Alice, the owner of the quantum data, is also the owner of the quantum clouds or is trusting the quantum cloud provider(s), the owner can enable an additional security feature that allows her to recover the original qubit A even in the case of a loss of all noise qubits. To enable this security feature, the owner sends not only the n copies to quantum clouds, but also the postencoding qubit A (which is maximally mixed) to a quantum cloud. Now even if Alice were to lose all of her noise qubits, she could still recover the original qubit A, namely, by running the encoding unitary in reverse on the collection of all signal qubits and the postencoding qubit A. In addition, if Alice maintains access to all n noise qubits, she can recover the original qubit A by using any one of the signal qubits or also by using the postencoding qubit A, at least if n is even, as we show in Supplemental Material [32]. In effect, at least if n is even, the postencoding

qubit A can serve as an encrypted clone as well. Finally, among possible variants, let us mention the possibility to create a large number of encrypted clones of A by repeatedly creating, say, two additional clones of A, by using the $n = 2$ encrypted cloning method. In this case, while the last created pair of encrypted clones requires all noise qubits for decryption, the first pair of encrypted clones requires only the first two noise qubits for decryption. Alternatively, a favorable scaling of the number of noise qubits required for decryption can be obtained, for example, by creating three encrypted clones (counting also A as an encrypted clone) using the $n = 2$ method and then creating three encrypted clones of each of these encrypted clones and so on, say, k times. This yields 3^k encrypted clones along with $2(1 + 3 + \cdots + 3^{k-1}) = 3^k - 1$ noise qubits. This means that, to create $m + 1 \coloneqq 3^k$ encrypted clones, m noise qubits are required, as in the original method for $n = m$ (counting also A as an encrypted clone). However, when using this iterated encrypted cloning method, each of the 3^k encrypted clone requires for its decryption merely $2k$ specific noise qubits.