Encrypted Qubits can be Cloned

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, ON 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, ON N2L 3G1, Canada*
[4] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[5] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

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 multi-cloud storage.

https://arxiv.org/pdf/2501.02757

QARS
Alexandre Leblanc
10 février 2026

INSTITUT QUANTIQUE UDS

Key Result

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, ON 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, ON N2L 3G1, Canada*
[4] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[5] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

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 multi-cloud storage.

Method

- The protocol generates multiple redundant, indirectly accessible encrypted copies, rather than multiple simultaneously accessible identical quantum states, thus strictly adhering to the no-cloning theorem.

- Any number, $n > 1$, of encrypted clones of a qubit, A, can be produced and decrypted through a unitary transformation.

- The number of gate operations needed for the encryption and decryption scales linearly with the number of clones (n).

Method

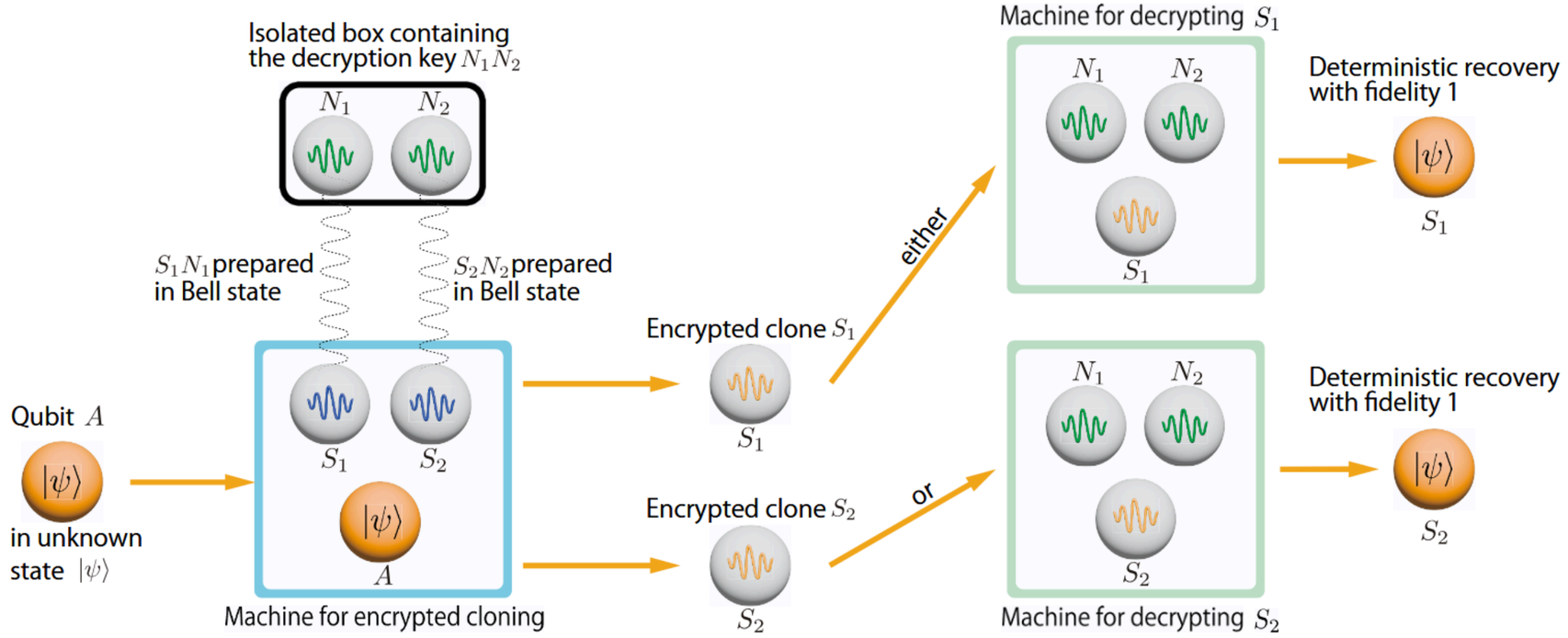

FIG. 1. The protocol for $n = 2$. Qubits whose reduced state is maximally mixed are represented by spheres displaying fluctuations. The initial maximal mixedness of S_1 and S_2, which stems from their being prepared in Bell states with N_1 and N_2 respectively, provides the quantum noise for the encryption. N_1 and N_2 keep a record of this quantum noise and can, therefore, later be used to de-noise 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.

Method

1. Start with n pairs of maximally entangled qubits labeled Signal (S_i) and Noise (N_i).
2. Encryption of the original qubit (A) with all signal qubits through U_{enc} .
3. Information about qubit A is inscribed on every signal qubits, but is masked by noise.
4. The noise qubits never interact with qubit A, they only serve as decryption key (denoising).

Method

Last important things to note:

- **They showed that any single signal qubit (S_i) plus the full set of noise qubits ($N_1 \ldots N_n$) allows for deterministic recovery with fidelity 1.**
- **Gate operations required for this process grow only linearly with the number of clones (n), making it computationally efficient.**

Applications

They proposed application such as:

- **Encrypted quantum multi-cloud storage (blind computation).**
- **Quantum sensing.**
- **Quantum radar.**

https://arxiv.org/pdf/2501.02757