Experimental demonstration that qubits can be cloned at will, if encrypted with a single-use decryption key

Koji Yamaguchi,[1,*] Leon Rullkötter,[2,*] Ibrahim Shehzad,[3]
Sean J. Wagner,[4] Christian Tutschku,[2] and Achim Kempf[5,6,7,8]

[1] *Department of Informatics, Faculty of Information Science and Electrical Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan*
[2] *Fraunhofer Institute for Industrial Engineering (IAO), Nobelstraße 12, 70569 Stuttgart, Germany*
[3] *IBM Quantum, Thomas J. Watson Research Center, 1101 Kitchawan Rd, Yorktown Heights, NY 10598, USA*
[4] *IBM, Markham, ON L6G 1C7, Canada*
[5] *Department of Applied Mathematics, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[6] *Department of Physics, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[7] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[8] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

arXiv:2602.10695

Reminder (arXiv:2501.02757)

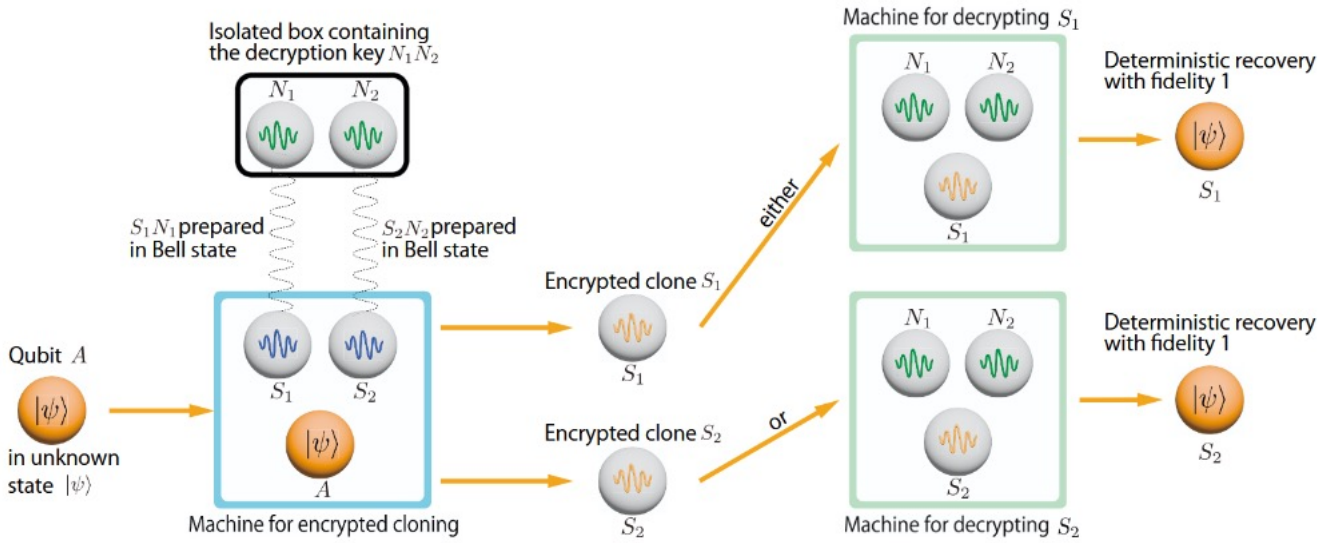
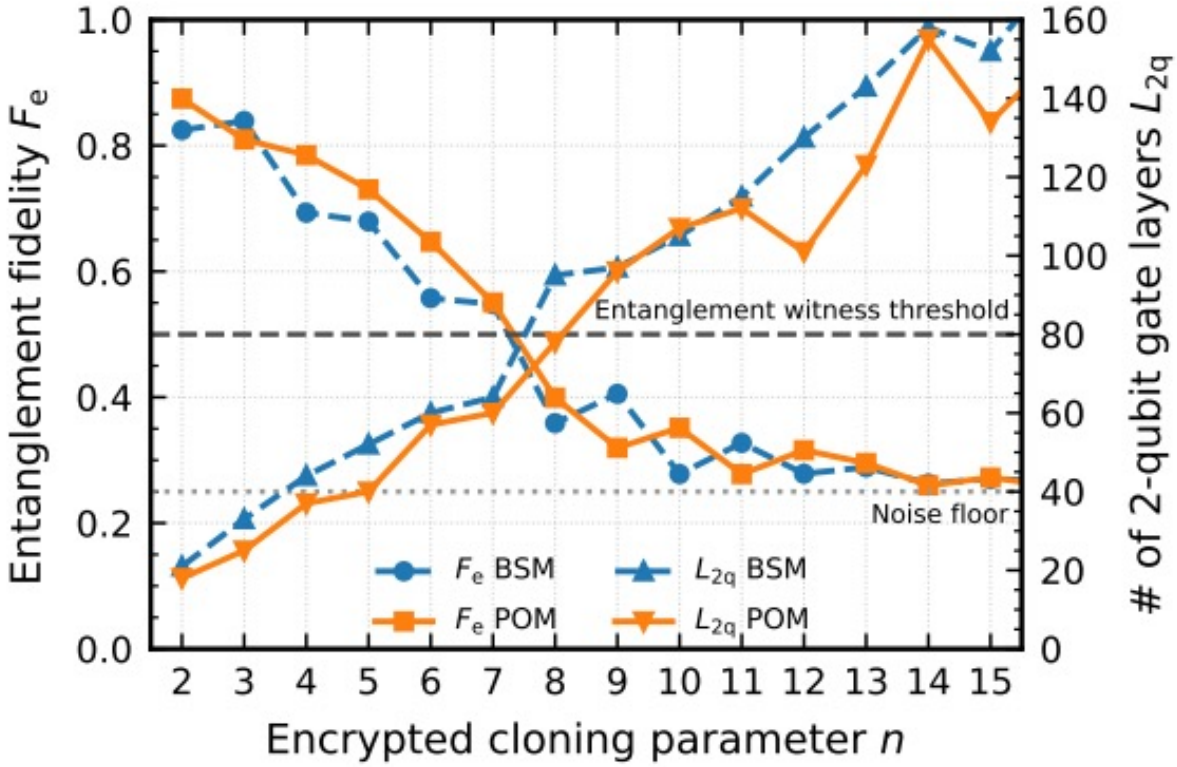


FIG. 1. The protocol for $n = 2$. Qubits whose reduced state is maximally mixed are represented by spheres displaying fluctuations. The initial maximal mixedness of S_1 and S_2, which stems from their being prepared in Bell states with N_1 and N_2 respectively, provides the quantum noise for the encryption.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

Experiment 1: Fidelity

IBM Heron R2



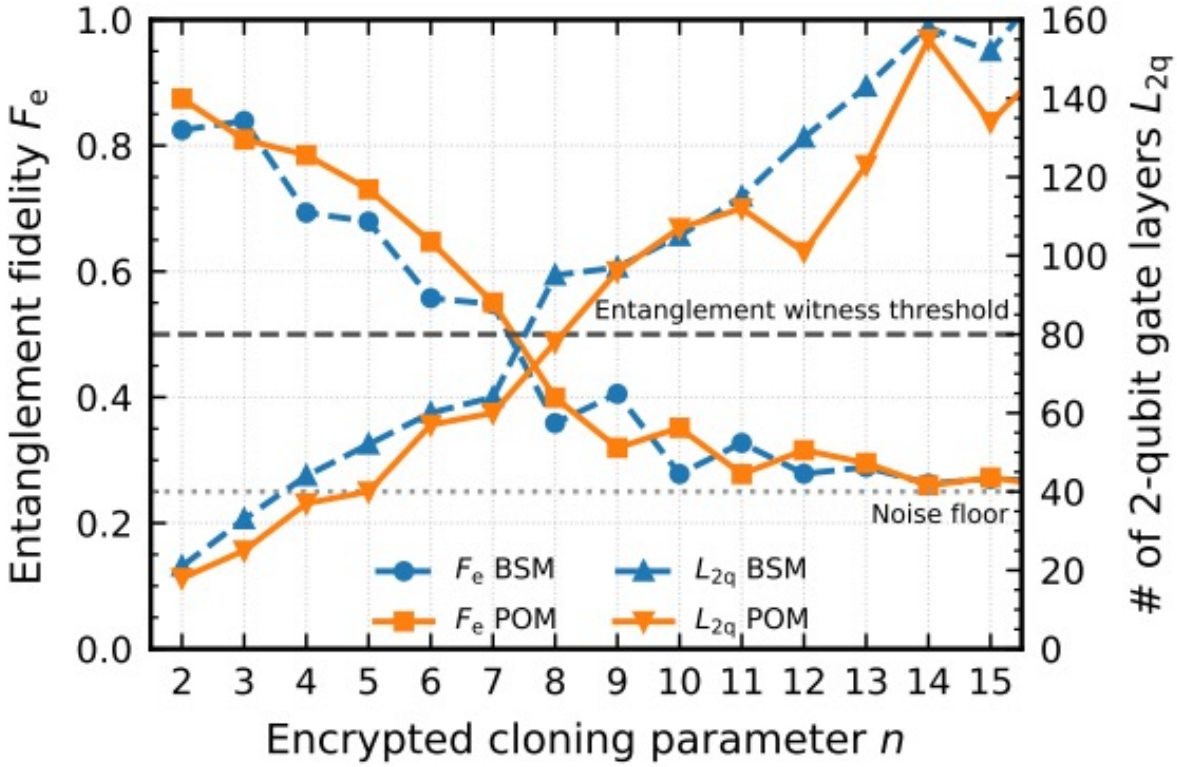
BSM: Bell State Measurement
POM: Parity Oscillations Method

Experiment 1: Fidelity

IBM Heron R2

F = 0.5 is the entaglement witness threshold *for a Bell pair*

- If F >= 0.5, there must be some entanglement
- See pg. 15 of arXiv: 0811.2803
  - maximal Schmidt coefficient of a Bell pair is $\frac{1}{\sqrt{2}}$



BSM: Bell State Measurement
POM: Parity Oscillations Method

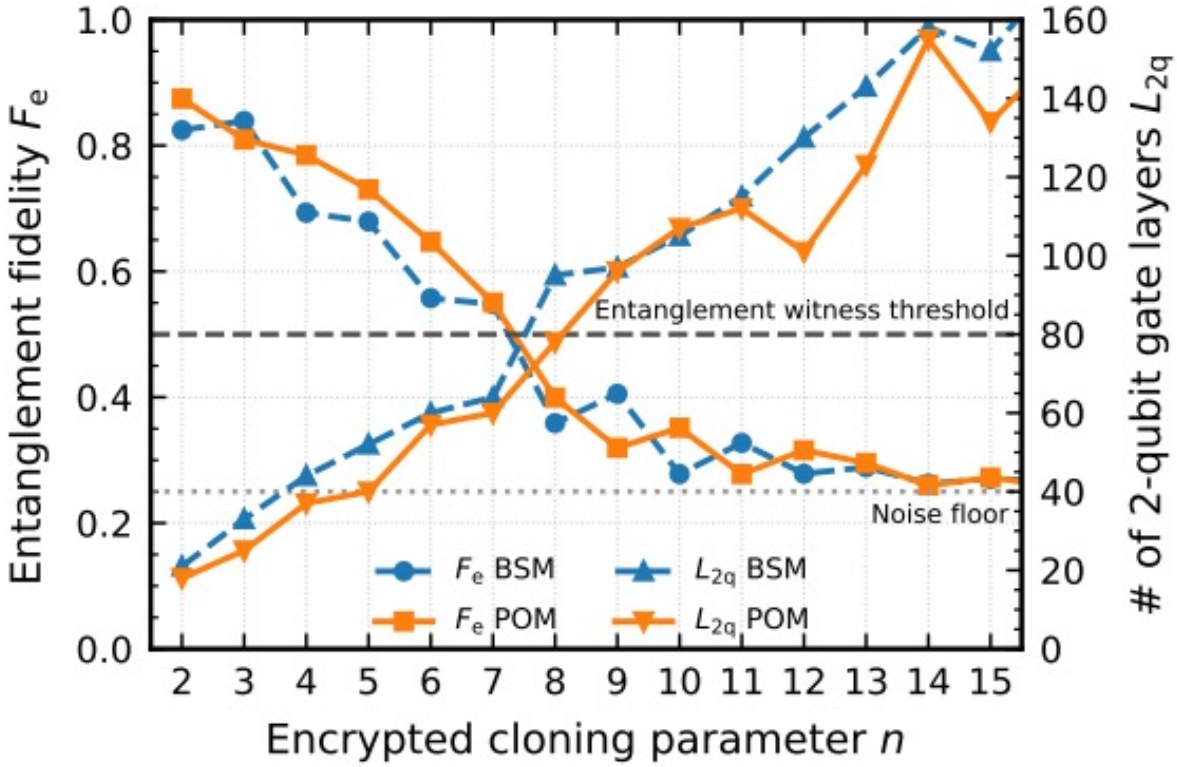
Experiment 1: Fidelity

IBM Heron R2

F = 0.5 is the entaglement witness threshold *for a Bell pair*

- If F >= 0.5, there must be some entanglement
- See pg. 15 of arXiv: 0811.2803
  - maximal Schmidt coefficient of a Bell pair is $\frac{1}{\sqrt{2}}$

Protocol works even on a NISQ machine, with fidelity dropping with gate depth



BSM: Bell State Measurement
POM: Parity Oscillations Method

Other experiments

- Experiment 2: Feasibility of interleaving encryption and decryption
  - Other operations can be done between encryption and decryption
  - Used measurement to demonstrate

Other experiments

- Experiment 2: Feasibility of interleaving encryption and decryption
  - Other operations can be done between encryption and decryption
  - Used measurement to demonstrate
- Experiment 3: Operation in series: Feasibility of iterating encrypted cloning
  - Ecrypt-clone one qubit, then encrypt-clone its clones, iterate
  - Using 154 qubits, they obtain 77 ecrypted clones, $F > 0.25$
  - For 27 encrypted clones, $F > 0.5$

Other experiments

- Experiment 2: Feasibility of interleaving encryption and decryption
  - Other operations can be done between encryption and decryption
  - Used measurement to demonstrate
- Experiment 3: Operation in series: Feasibility of iterating encrypted cloning
  - Ecrypt-clone one qubit, then encrypt-clone its clones, iterate
  - Using 154 qubits, they obtain 77 ecrypted clones, $F > 0.25$
  - For 27 encrypted clones, $F > 0.5$
- Experiment 4: Operation in parallel: Feasibility of encrypted cloning inside multipartite circuits
  - GHZ state, encrypt-clone one qubit at a time
  - Recovered state has $F > 0.5$ for up to a 4-qubit GHZ state