Article | Received 16 June 2026; Revised 14 August 2026; Accepted 2 September 2026; Published 21 September 2026
https://doi.org/10.55092/qr20260004

Supplementary data

Circuit-model blind quantum computation with key decoupling

Ting Xiang[1,†], Bingwen Feng[2,†] and Xiaoqian Zhang[3,*]

[1] School of Physics and State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou, China

[2] College of Cyber Security, Jinan University, Guangzhou, China

[3] College of Information Science and Technology, Jinan University, Guangzhou, China

† These authors contributed equally to this work.

* Correspondence author; E-mail: zhangxq64@jnu.edu.cn.

The supplementary material comprises two sections: Section 1 presents additional single-qubit circuit-model blind quantum computation (CMBQC) experiments on the International Business Machines Corporation (IBM) superconducting platform, while Section 2 provides the multi-qubit verification of the CMBQC protocol.

1. Additional single-qubit CMBQC experiments on the IBM superconducting system

The main text presents CMBQC experimental results for a single-qubit target gate $U_1^{(1)}$. Here, we provide additional experimental results for single-qubit target operations including $U_2^{(1)}$, H, S, and T. The experimental setting $\delta = 0.9$ is consistent with that described in Section 3 of the main text. The cheating operations V_{cheat} are chosen such that, in the target computation rounds, the resulting output states closely approximate those produced by the ideal operation V_{ideal}. We next present experimental results for four additional target quantum gates, shown in Figure S1.

As shown in Figure S1a, the $U_2^{(1)}$-gate CMBQC experiment is carried out over 16 rounds, with the 6th round designated as the target computation round and the 4th and 12th rounds randomly chosen as cheating rounds. The Pauli observables used in the 15 verification rounds are, in order, $Z,Y,X,X,Y,Y,Z,X,Z,X,X,Z,Y,Y,X$. The corresponding theoretical expectation values are -0.0134, 0.9699, -0.9105, -0.9695, 0.2449, -0.9770, 0.2111, -0.1806, -0.2111, 0.9105, 0.1806, 0.3382, 0.9699, 0.9770, -0.9105. The experimentally measured expectation values are -0.0361 ± 0.0317, 0.9426 ± 0.0277, -0.9158 ± 0.0189, -0.9733 ± 0.0249, 0.2100 ± 0.0271, -0.9706 ± 0.0181, 0.2376 ± 0.0273, -0.1632 ± 0.0405, -0.1684 ± 0.0309, 0.8726 ± 0.0200, 0.4286 ± 0.0281, 0.3071 ± 0.0308, 0.9923 ± 0.0070, 0.9388 ± 0.0197, -0.9276 ± 0.0315. The experiment is repeated 10^4 times to estimate the statistical uncertainty of the measured expectation values. For the cheating operations $V_{\text{cheat}}^{(4)}$ and $V_{\text{cheat}}^{(12)}$, the corresponding gate fidelities with respect to the ideal operation V_{ideal} are 0.8372 and 0.3413,

respectively. With the threshold set to 0.1, the deviation in round 4 is 0.0039 (theoretical value 0), which remains below the threshold and is therefore not flagged. In contrast, the deviation in round 12 reaches 0.2480 (theoretical value 0.4251), exceeding the threshold and thus being successfully detected. Overall, only one detectable deviation is observed among the 15 verification rounds, yielding $P_{\text{cheat}} \approx 0.053$ and hence $1 - P_{\text{cheat}} > 0.9$, indicating that the protocol passes the statistical test.

As shown in Figure S1b, the Hadamard-gate CMBQC experiment is carried out over 16 rounds, with the 10th round designated as the target computation round and the 4th and 6th rounds randomly chosen as cheating rounds. The Pauli observables used in the 15 verification rounds are, in order, $Y,Y,Z,Y,Z,X,Y,Z,X,Y,Z,Z,X,Y,Z$. The corresponding theoretical expectation values are 0.5933, -0.5933, -0.7168, 0.5933, -0.7168, 0.3662, -0.5933, -0.7168, -0.3662, -0.5933, 0.7168, 0.7168, 0.3662, 0.5933, -0.7168. The experimentally measured expectation values are 0.5852 ± 0.0368, -0.6015 ± 0.0242, -0.7237 ± 0.0285, 0.5457 ± 0.0481, -0.7426 ± 0.0221, -0.5041 ± 0.0348, -0.5950 ± 0.0324, -0.7157 ± 0.0169, -0.3201 ± 0.0377, -0.6723 ± 0.0094, 0.6803 ± 0.0175, 0.6795 ± 0.0168, 0.4038 ± 0.0429, 0.6323 ± 0.0236, -0.7452 ± 0.0229. For the cheating operations $V_{\text{cheat}}^{(4)}$ and $V_{\text{cheat}}^{(6)}$, the corresponding gate fidelities with respect to the ideal operation V_{ideal} are 0.3798 and 0.5610, respectively. With the threshold set to 0.1, the deviation in round 4 is 0.0476 (theoretical value 0.0289), which remains below the threshold and is therefore not flagged. In contrast, the deviation in round 6 reaches 0.8703 (theoretical value 0.8354), exceeding the threshold and thus being successfully detected. Overall, only one detectable deviation is observed among the 15 verification rounds, yielding $P_{\text{cheat}} \approx 0.053$ and hence $1 - P_{\text{cheat}} > 0.9$, indicating that the protocol passes the statistical test.

As shown in Figure S1c, the S-gate CMBQC experiment is carried out over 16 rounds, with the 11th round designated as the target computation round and the 7th and 16th rounds randomly chosen as cheating rounds. The Pauli observables used in the 15 verification rounds are, in order, $Y,X,Z,X,Y,X,Z,Y,Y,X,Z,X,X,Y,Y$. The corresponding theoretical expectation values are 0.4961, 0.7307, 0.4690, -0.7307, 0.4961, 0.7307, -0.4690, -0.4961, 0.4961, -0.7307, -0.4690, -0.7307, -0.7307, 0.4961, -0.4961. The experimentally measured expectation values are 0.4632 ± 0.0364, 0.6935 ± 0.0399, 0.5082 ± 0.0389, -0.7051 $\pm$ 0.0187, 0.4963 ± 0.0291, 0.7271 ± 0.0264, -0.2175 ± 0.0191, -0.5413 ± 0.0422, 0.5614 ± 0.0237, -0.7217 ± 0.0350, -0.4307 ± 0.0366, -0.7454 ± 0.0330, -0.7416 ± 0.0321, 0.4875 ± 0.0305, -0.1632 ± 0.0166. For the cheating operations $V_{\text{cheat}}^{(7)}$ and $V_{\text{cheat}}^{(16)}$, the corresponding gate fidelities with respect to the ideal operation V_{ideal} are 0.9827 and 0.8707, respectively. With the threshold set to 0.1, the deviations in rounds 7 and 6 are 0.2515 (theoretical value 0.2426) and 0.3329 (theoretical value 0.2902), respectively, both above the threshold and therefore detected. This yields $P_{\text{cheat}} \approx 0.1333$ and hence $1 - P_{\text{cheat}} < 0.9$, under which the protocol does not pass the statistical test.

As shown in Figure S1d, the T-gate CMBQC experiment is carried out over 16 rounds, with the 12th round designated as the target computation round and the 6th and 9th rounds randomly chosen as cheating rounds. The Pauli observables used in the 15 verification rounds are, in order, $Y,Z,X,X,Z,Z,X,Y,Y,Z,X,X,Y,X,X$. The corresponding theoretical expectation values are -0.0819, 0.2714, 0.9590, 0.0819, -0.2714, 0.2714, -0.9590, 0.0819, 0.0819, -0.2714, 0.9590, -0.0819, 0.0819, 0.9590, -0.0819. The experimentally measured expectation values are -0.0650 ± 0.0348, 0.2425

$\pm$ 0.0342, -0.9320 ± 0.0255, 0.1146 ± 0.0404, -0.2366 ± 0.0261, -0.6150 ± 0.0317, -0.9072 ± 0.0341, -0.0017 ± 0.0450, -0.0376 ± 0.0379, -0.2485 ± 0.0220, 0.8716 ± 0.0248, -0.0857 ± 0.0441, 0.0469 ± 0.0406, 0.9457 ± 0.0268, -0.1410 ± 0.0317. For the cheating operations $V_{\text{cheat}}^{(6)}$ and $V_{\text{cheat}}^{(9)}$,the corresponding gate fidelities with respect to the ideal operation V_{ideal} are 0.4058 and 0.3413, respectively. With the threshold set to 0.1, the deviations in rounds 6 and 9 are 0.8863 (theoretical value 0.8963) and 0.1195 (theoretical value 0.0650), respectively, both above the threshold and therefore detected. This yields $P_{\text{cheat}} \approx 0.1333$ and hence $1 - P_{\text{cheat}} < 0.9$, under which the protocol does not pass the statistical test.

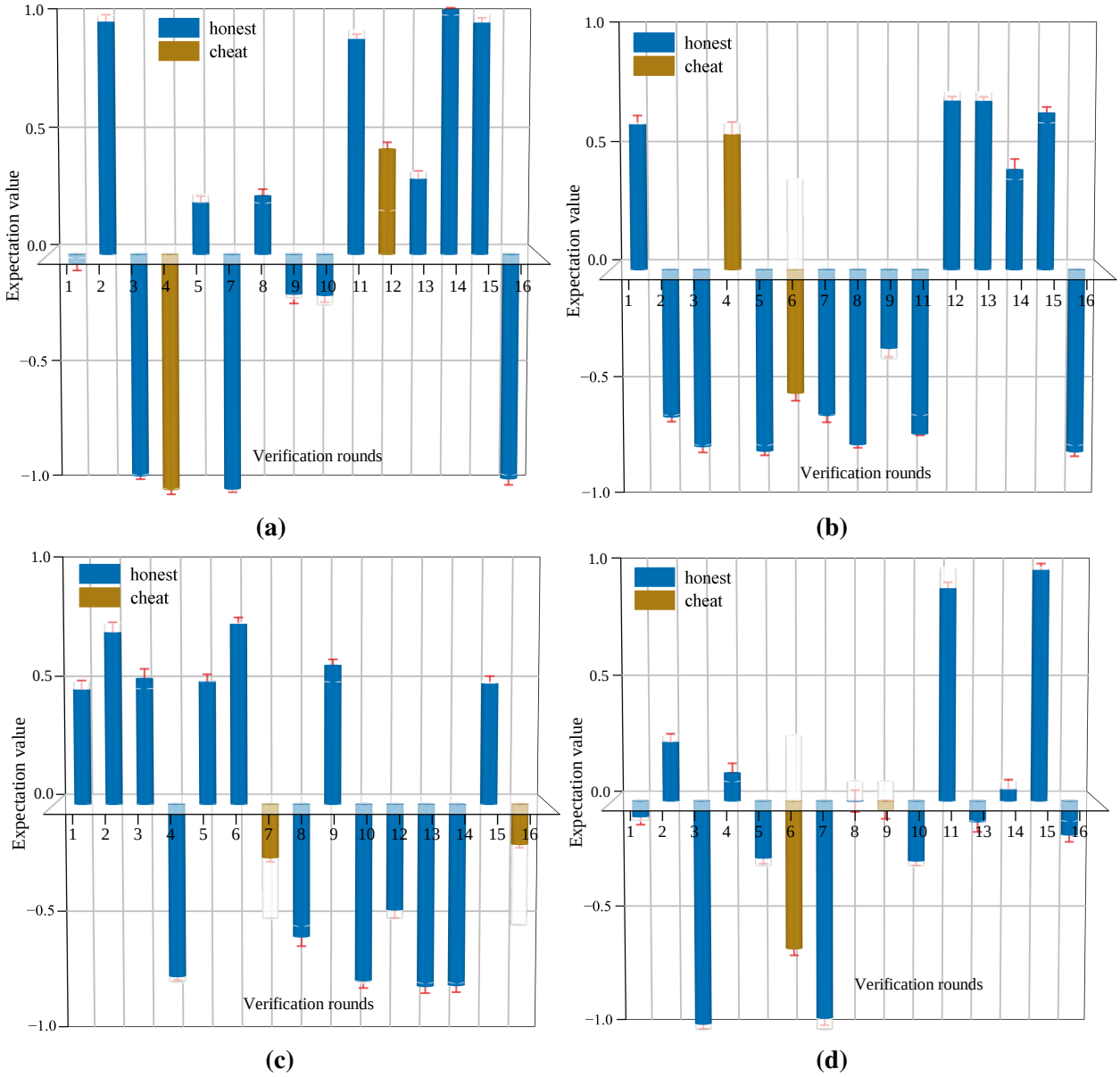

Figure S1. Experimental results of the single-qubit CMBQC protocol on the IBM superconducting quantum system. **(a)** Arbitrary single-qubit gate $U_2^{(1)}$ with cheating rounds in rounds 4 and 12, and the target computation in round 6; **(b)** Hadamard gate H with cheating rounds in rounds 4 and 6, and the target computation in round 10; **(c)** S gate with cheating rounds in rounds 7 and 16, and the target computation in round 11; **(d)** T gate with cheating rounds in rounds 6 and 9, and the target computation in round 12. Blue (brown) bars denote honest (cheating) executions.

2. Implementation of multi-qubit CMBQC verification

In n-qubit CMBQC, verification relies on finite-round random sampling rather than exhaustive coverage of the encryption key space. This is because the key space grows exponentially as 4^{2n}, rendering full coverage experimentally infeasible and statistically unnecessary. Thus, multi-qubit CMBQC security is characterized by the verification rounds N and the tolerated deviation fraction k/N. Each verification round employs a randomly chosen combination of Pauli observables as the measurement setting, enabling unbiased deviation detection. The multi-qubit verification results presented below are obtained from ideal, noiseless numerical simulations. State preparation, quantum operations, and measurements are assumed to be ideal, without including hardware noise such as gate errors, decoherence, or readout errors. Therefore, the simulations are intended to characterize the intrinsic statistical verification performance of the CMBQC protocol, with the observed deviations arising solely from the deliberately introduced cheating operations.

The verification results for two-qubit CMBQC under settings $N = 10, 20, 30, 40$, and 50, with acceptance thresholds $\varepsilon = 0.001$ and $\delta = 0.9$, are summarized in Table S1. For each setting N, the number of failing rounds m_{nopass} defines the statistical deviation-detection rate γ, which bounds the maximum number of cheating rounds as $k \lesssim (1-\delta)N/\gamma$. The corresponding boundary numbers of cheating rounds used in the weak-attack tests are $\lceil k \rceil = 1, 3, 4, 5$, and 6, respectively. We then verify the two-qubit CMBQC protocol on a representative set of quantum gates, including an arbitrary unitary $U_1^{(2)}$ as well as CH, CNOT, CS, CZ, iSWAP, $\sqrt{\text{iSWAP}}$, QFT, and SWAP. The tested gate sets are selected to cover representative multi-qubit operations with different structures and computational roles rather than to exhaust all possible gates. For two-qubit verification, the set contains an arbitrary unitary $U_1^{(2)}$, controlled gates CH, CNOT, CS, and CZ, exchange-type gates iSWAP, $\sqrt{\text{iSWAP}}$, and SWAP, and QFT as a representative algorithmic transformation. For three-qubit verification, we consider an arbitrary unitary $U_1^{(3)}$ together with the commonly used Toffoli, Fredkin, and CCZ gates. This selection allows us to assess whether the verification behavior remains consistent across different gate structures. The entries under the weak-attack setting denote the number of detected cheating rounds. As indicated by the bold values in Table S1, incomplete detection occurs in several cases, and the number of undetected cheating rounds is given by $\lceil k \rceil$ minus the corresponding bold value. For $N = 10$ ($\lceil k \rceil = 1$), cheating deviations are detected for all nine tested two-qubit gates. At $N = 20$ ($\lceil k \rceil = 3$), all cheating deviations are detected except for a single undetected instance associated with the CS gate. At $N = 30$ ($\lceil k \rceil = 4$), undetected instances are limited to one for $U_1^{(2)}$ and two for $\sqrt{\text{iSWAP}}$, with all remaining gates fully detected. At $N = 40$ ($\lceil k \rceil = 5$), only one undetected instance is observed for the CH gate and one for $\sqrt{\text{iSWAP}}$, while all other gates are detected. At $N = 50$ ($\lceil k \rceil = 6$), all tested two-qubit gates are detected without exception. Overall, these results indicate that a verification configuration of $N = 20$ already achieves an effective balance between detection capability and experimental overhead for two-qubit CMBQC verification.

Table S1. Statistical verification of two-qubit CMBQC.

		Strong Attack				**Weak Attack**							
N	m_{nopass}	γ	k	$\lceil k \rceil$	$U_1^{(2)}$	CH	CNOT	CS	CZ	iSWAP	$\sqrt{\text{iSWAP}}$	QFT	SWAP
10	10	1	1	1	1	1	1	1	1	1	1	1	1
20	19	0.95	2.11	3	3	3	3	**2**	3	3	3	3	3
30	28	0.93	3.21	4	**3**	4	4	4	4	4	**2**	4	4
40	38	0.95	4.21	5	5	**4**	5	5	5	5	**4**	5	5
50	46	0.92	5.43	6	6	6	6	6	6	6	6	6	6

For three-qubit CMBQC, the verification results are summarized in Table S2. The verification thresholds are fixed at $\varepsilon = 0.001$ and $\delta = 0.9$, giving bounds of $\lceil k \rceil = 1, 2, 4, 5$, and 5 for $N = 10, 20, 30, 40$, and 50, respectively. For an arbitrary three-qubit unitary $U_1^{(3)}$ and the Toffoli, Fredkin, and CCZ gates, cheating deviations are detected when the number of cheating rounds equals the corresponding bound $\lceil k \rceil$ at each tested N. These results establish that $N = 20$ verification rounds provide a practical trade-off between detection capability and experimental overhead for three-qubit CMBQC.

Table S2. Statistical verification of three-qubit CMBQC.

		Strong Attack				**Weak Attack**		
N	m_{nopass}	γ	k	$\lceil k \rceil$	$U_1^{(3)}$	Toffoli	Fredkin	CCZ
10	10	1	1	1	1	1	1	1
20	20	1	2	2	2	2	2	2
30	29	0.97	3.1	4	4	4	4	4
40	39	0.98	4.1	5	5	5	5	5
50	50	1	5	5	5	5	5	5