Manuscript version: Published Version
The version presented in WRAP is the published version (Version of Record).

Persistent WRAP URL:
http://wrap.warwick.ac.uk/159323

How to cite:
The repository item page linked to above, will contain details on accessing citation guidance from the publisher.

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher’s statement:
Please refer to the repository item page, publisher’s statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk
Experimental accreditation of outputs of noisy quantum computers

Samuele Ferracini,1,2,* Seth T. Merkel,3,‡ David McKay,3,‡ and Animesh Datta2,†

1Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
2Department of Physics, University of Warwick, Coventry CV4 7AL, United Kingdom
3IBM Quantum, T. J. Watson Research Center, Yorktown Heights, New York 10598, USA

(Received 30 March 2021; accepted 17 September 2021; published 11 October 2021)

We provide and experimentally demonstrate an accreditation protocol that upper bounds the variation distance between noisy and noiseless probability distributions of the outputs of arbitrary quantum computations. We accredit the outputs of 24 quantum circuits executed on programmable superconducting hardware, ranging from depth-9 circuits on 10 qubits to depth-21 circuits on 4 qubits. Our protocol requires implementing the “target” quantum circuit along with a number of random Clifford circuits and subsequently postprocessing the outputs of these Clifford circuits. Importantly, the number of Clifford circuits is chosen to obtain the bound with the desired confidence and accuracy and is independent of the size and nature of the target circuit. We thus demonstrate a practical and scalable method of ascertaining the correctness of the outputs of arbitrary-sized noisy quantum computers—the ultimate arbiter of the utility of the computer itself.

DOI: 10.1103/PhysRevA.104.042603

I. INTRODUCTION

The utility of noisy quantum computers in simulation and optimization will be determined by our ability to ascertain whether the solutions provided are correct or close to correct. This is a challenging task for problems that are outside the complexity class NP. The current methods are based on evaluating single-valued metrics such as the cross entropy [1,2] and the quantum volume [3], which can be linked to the performance of the quantum hardware being used. These methods require simulating the relevant quantum circuits on classical computers. Although practical at present, they are not scalable and, consequently, are useless for problems that cannot already be simulated classically. On the contrary, the proposals based on quantum cryptography and interactive proof systems are scalable in principle but have an overhead in width (qubits) and depth (gates) that makes them impractical for the foreseeable future [4–11]. This calls for new methods that are both practical in the short term and scalable in the long term.

In this work we present and experimentally demonstrate an accreditation protocol (AP) that achieves this goal. This AP provides an upper bound on the variation distance (VD) between the probability distribution of the experimental outputs of a noisy quantum circuit \( p_{\text{exp}}(\sigma) \) and its ideal, noiseless counterpart \( p_{\text{ideal}}(\sigma) \), where \( \sigma \) denotes the bit strings that may be obtained as output. In our AP, the “target” quantum circuit, the correctness of whose outputs we wish to ascertain, is executed along with a number \( v \) of random Clifford circuits (the “traps”). The trap circuits have the same width and depth as the target circuit and are designed such that in the absence of noise they always return a fixed known output. This enables us, in the presence of noise, to measure the probability \( p_{\text{inc}} \) that a trap’s output is incorrect. Our AP guarantees that the VD \( V_D \) between \( p_{\text{exp}}(\sigma) \) and \( p_{\text{ideal}}(\sigma) \) is bounded as (see Sec. A1 for a proof)

\[
V_D := \frac{1}{2} \sum_\sigma |p_{\text{ideal}}(\sigma) - p_{\text{exp}}(\sigma)| \leq 2p_{\text{inc}}.
\]

The value \( 2p_{\text{inc}} \) is estimated experimentally with accuracy \( \theta \in (0, 1) \) and confidence \( \alpha \in (0, 1) \) chosen by the user. The number \( v \) of trap circuits is determined by the desired \( \theta \) and \( \alpha \) but is independent of the size and nature of the target circuit [Eq. (2)].

We implement our AP on ibmq_johannesburg and ibmq_paris, two two-dimensional arrays of superconducting transmon qubits. Figure 1 shows the bounds provided by our AP for 24 different circuits. Of these, 14 are structured circuits – 10 circuits to generate Greenberger-Horne-Zeilinger (GHZ) states [12] and 4 to perform the quantum Fourier transform (QFT) [13], both important primitives in quantum computation – and 10 are six-qubit random circuits of varying depths. The widest of these circuits has 10 qubits and depth 9; the deepest has 4 qubits and depth 21. The widths of our circuits compare favorably to that reached in the experimental demonstrations of some of the main protocols for noise characterization – 3 qubits in process tomography [14], 5 in randomized benchmarking [15], 7 in direct fidelity estimation [16], and 10 in cycle benchmarking [17].

Our AP is designed to ascertain the correctness of a noisy quantum computation rather than the performance of individual gates or families thereof. Thus, it can detect noise (such as location-dependent noise acting on the whole register of...
gate-independent noise, i.e., $E$ noise model; in Sec. III we present our AP; In Secs. IV and V the AP will supplant the protocols based on classical simulations showing that the bound provided by our AP is robust to noise weakly on the cycles of one-qubit gates (Sec. A2).

### III. ACCREDITATION PROTOCOL

Our AP takes as input the target circuit and two numbers, $\theta, \alpha \in (0, 1)$, which quantify the desired accuracy and confidence of the final bound. The target circuit must (i) take as input $q$ qubits in state $|0\rangle$, (ii) contain $2m$ cycles alternating between a cycle of one-qubit gates and a cycle of two-qubit gates, and (iii) end with measurements in the Pauli-$Z$ basis $[\theta, \alpha]$). Our AP requires that all two-qubit gates in the target circuit be Clifford gates, so that arbitrary noise processes can be transformed into Pauli errors via QOTP. Without loss of generality, we assume that all the two-qubit gates in the circuit are $cZ$ gates. Note that circuits containing different two-qubit Clifford gates (such as the $cX$ gates implemented by IBM Quantum devices and the Mølmer-Sørensen gate implemented by trapped-ion quantum computers [34]) can be efficiently recomposed in this form without increasing the depth, while circuits containing two-qubit non-Clifford gates (such as those implemented by Google Sycamore [2]) require a linear increase in depth.

Our AP requires executing $v + 1$ circuits sequentially, where $v = 2\ln[2/(1-\alpha)]/\theta^2$ and $\lceil \cdot \rceil$ is the ceiling function. One of these circuits (chosen at random) is the target circuit; the others are trap circuits. Each trap circuit is obtained by replacing the one-qubit gates in the target circuit with random one-qubit Clifford gates as per the following algorithm [Fig. 2(b)]:

1. For all $j \in [1, \ldots, m-1]$ and for all $i \in [1, \ldots, n]$:
   a. If the $j$th cycle of $cZ$ gates connects qubit $i$ to qubit $i'$, randomly replace $U_{i,j}$ with $S$ and $U_{i',j}$

![Diagram](image-url)
with $H$ or $U_{i,j}$ with $H$ and $U_{r,j}$ with $S$. Undo these gates after the cycle of $cZ$ gates.

(ii) If the $j$th cycle of $cZ$ gates does not connect qubit $i$ to any other qubit, randomly replace $U_{i,j}$ with $H$ or $S$. Undo this gate after the cycle of $cZ$ gates.

(2) Initialize a random bit $t \in \{0,1\}$. If $t = 0$, do nothing. If $t = 1$, append a cycle of Hadamard gates at the beginning and at the end of the circuit.

Since $(S^i \otimes H \otimes Z \otimes H) = cX$, the trap circuits apply a series of $cX$ gates to $n$ qubits in the state $|0\rangle$ (if $t = 0$) or $|+\rangle$ (if $t = 1$). Using $cX|00\rangle = |00\rangle$ and $cX|++\rangle = |++\rangle$, it can be seen that in the absence of noise all the trap circuits return the bit string $(0,0,\ldots,0)$.

After initializing the $v + 1$ circuits, we append a QOTP to each cycle of one-qubit gates in every circuit. This is done by appending a cycle of random Pauli gates after every cycle of one-qubit gates and by appending a second cycle of Pauli gates before the following cycle of one-qubit gates that undoes the first. This randomizes the noise to stochastic Pauli errors [4,10,24,35–37]. The trap circuits are designed to detect these Pauli errors, meaning that any Pauli error alters their outputs with a probability of at least 50% [24].

After appending the QOTP we recompile neighboring cycles of one-qubit gates into a single cycle. This ensures that all the circuits and subsequently estimate the probability $p_{\text{inc}}$ as the fraction $N_{\text{inc}}/v$ of traps that return an incorrect output. Since $v \geq 2\ln(2/(1-\alpha))/\theta^2$, Hoeffding’s inequality [38] guarantees that

$$\text{prob}\left[\left|p_{\text{inc}} - \frac{N_{\text{inc}}}{v}\right| \leq \frac{\theta}{2}\right] \geq \alpha.$$  

Finally, we calculate the bound on the VD as $2N_{\text{inc}}/v$, and we have $\text{prob}(2p_{\text{inc}} \leq 2N_{\text{inc}}/v \leq \theta) \geq \alpha$ by Hoeffding’s inequality.

The quantity $2p_{\text{inc}}$ grows linearly with the total probability $p_{\text{err}}$ that the target circuit is afflicted by errors. More formally, we have

$$p_{\text{err}} \leq 2p_{\text{inc}} \leq 2p_{\text{err}}.$$  

Here, the bound on the left-hand side (lhs) is proven in Sec. A1, while that on the right-hand side (rhs) is a consequence of the fact that in the absence of errors the traps always return the correct output. Since the VD is, at most, unity by construction, it follows that if $p_{\text{err}} \leq 50\%$, our AP always returns a nontrivial bound on the VD (i.e., below unity). Otherwise, it may return a trivial bound, indicating that the device is afflicted by such high levels of noise that its outputs are far enough from the ideal ones as to be unreliable.

As can be seen in Fig. 1, in our experiments we obtain nontrivial bounds for circuits with up to 10 qubits. Larger circuits yield trivial bounds. However, Eq. (3) shows that improvements in the hardware will extend the reach of the AP beyond 10-qubit circuits. Being fully scalable, in the future the AP will be able to accredit the outputs of quantum circuits that will be intractable for the protocols relying on classical simulations.

IV. EXPERIMENTAL ACCREDITATION

We implement our AP on two superconducting quantum computers, ibmq_johannesburg and ibmq_paris. These quantum computers consist of superconducting transmon qubits dispersively coupled according to the topology given in Fig. 3, where each edge denotes a $cX$ gate that can be implemented via the cross-resonance interaction. For a more comprehensive description of this architecture, see Ref. [39], and for specific details about ibmq_johannesburg and ibmq_paris, see Ref. [40].

We begin by conducting 14 experiments to accredit the outputs of QFT and GHZ circuits of different widths [Figs. 4(a) and 4(b)]. In every experiment we submit 40 jobs to the back end. Each job contains 450 trap circuits, each one chosen independently at random as described in Sec. III. At the end of each job we estimate $p_{\text{inc}}$, as illustrated in Fig. 5 for the preparation and measurement of the six-qubit GHZ state. (See [41] for more figures.) To demonstrate the AP, in each job we also implement 450 instances of the target circuit and compute the VD between the ideal and experimentally obtained probability distributions. In our experiments this can be done within a reasonable amount of time given the size of the target circuits.

In every job we find $V_D \approx p_{\text{inc}}$, but we observe fluctuations across different jobs. These fluctuations indicate that different jobs suffer different noise due to, e.g., automatic
FIG. 3. A graphical representation of the connectivity in (a) ibmq_johannesburg and (b) ibmq_paris. The circles represent qubits; the edges represent the available entangling gates.

FIG. 4. (a) Our largest GHZ circuit. After adding the QOTP, this circuit contains nine cycles of noncommuting gates. (b) Our largest QFT circuit. We apply the circuit to state $|+\rangle \otimes^4$. Each two-qubit gate is a controlled-phase gate, which we decompose into two $cZ$ gates interleaved by one-qubit gates [33]. After adding the QOTP, this circuit contains 21 cycles of noncommuting gates. (c) Our six-qubit depth-nine pseudorandom circuit. The various gates $V_{ij}$ are random one-qubit gates.

V. HARDWARE DIAGNOSIS USING AP

The trap circuits implement deterministic computations, designed to return the output $s = (0, \ldots, 0)$ in the absence of errors and some other output in the presence of errors. Importantly, different errors alter the traps’ outputs in different ways. Therefore, we expect the probability distribution of the traps’ outputs to contain information regarding the nature of the noise afflicting the device in use. To corroborate this, in this section we focus on the traps’ outputs collected in the experiments with six-qubit pseudorandom circuits. We show how these outputs can help identify the main sources of errors in circuits of different sizes implemented on ibmq_paris.

For ibmq_paris the error rates provided by the back end are around 0.05% for the one-qubit gates, 1.5% for the two-qubit gates, and 2.3% for single-qubit measurements [41], while errors in state preparation are expected to be negligible. Therefore, we expect measurement noise to be the dominant source of error in shallow circuits and gate noise in deep circuits. To verify this, let us consider a noise model in which the gates are recalibrated of the internal components of the device. $V_D \approx p_{\text{inc}}$ also suggests that the factor of 2 on the rhs of Eq. (1) may be unnecessary. However, this factor of 2 captures the effects of specific patterns of errors that are detected with probability 50% [such as single-cycle patterns afflicting a single qubit; see Fig. 6(a)]. Thus, it is necessary to ensure the validity of Eq. (1) for arbitrary types of noise. In general, multicycle patterns [Fig. 6(b)] as well as patterns afflicting more than one qubit (such as those afflicting today’s devices [22,37]) are detected with probability greater than 50% [24], and for these patterns we have $p_{\text{err}} > 2p_{\text{inc}}$.

Importantly, we find $V_D < 2p_{\text{inc}}$ for every job in each of our experiments [41]. This proves that in all the tests that we have conducted, our AP has correctly bounded the VD as expected from Eq. (1). Figure 1(a) shows the smallest value of $2p_{\text{inc}}$ obtained in the various experiments.

To study how $2p_{\text{inc}}$ varies with the circuit depth we conduct 10 more experiments on ibmq_paris. We target a set of six-qubit pseudorandom circuits of depths ranging from 1 to 19. These circuits alternate cycles of random one-qubit gates with cycles containing either two or three $cZ$ gates [Fig. 4(c)]. In every experiment we submit 20 jobs to the back end, each one containing 900 unique trap circuits. In Fig. 1(b) we show the smallest values of $2p_{\text{inc}}$ obtained across the 20 jobs for each experiment.
noiseless, while measurement errors flip each bit $s_i \in \mathcal{S}$ with probability $p_{\text{flip}}$. In this scenario, the probability that a trap returns an output $\mathcal{S}$ with Hamming weight $H_T = h \in \{0, \ldots, n\}$ is

$$P_{\text{trap}}(H_T = h) = \binom{n}{h} p_{\text{flip}}^h (1 - p_{\text{flip}})^{n-h}. \quad (4)$$

where the Hamming weight $H_T = \sum_{i \in \mathcal{S}} s_i$ is the number of bits equal to 1 in the output string $\mathcal{S}$.

Setting $p_{\text{flip}} = 2.3\%$, in Fig. 7(a) we compare the values of $P_{\text{trap}}(H_T = h)$ from our bit-flip noise model (striped bars) with the experimentally measured ones for pseudorandom circuits (solid bars). It can be seen that the bit-flip model accurately predicts the results obtained for shallow circuits (e.g., for circuits of depth 1 or 3), indicating that measurement noise dominates short-depth circuits. It can also be seen that the bit-flip model becomes progressively disparate as the depth increases, indicating that in deep circuits measurements are no longer the dominant contributor to noise.

The above inference may be challenged by positing that the measurement noise changes with the circuit’s depth. To rule this possibility out, in Fig. 7(b) we set $p_{\text{flip}} = 7.6\%$ such that the value of $P_{\text{trap}}(H_T = 0)$ calculated using the bit-flip model (leftmost bar) equals the value measured in the experiment with depth-19 random circuits. As can be seen in Fig. 7(b), the bit-flip model still remains largely disparate. Overall, measurement errors alone cannot explain the distribution of outputs of our deepest trap circuits, and gate noise can no longer be neglected.

This simple analysis builds upon the error rates provided by the back end and is thus device specific. It shows that the probability distribution of the traps’ outputs contains information regarding the noise afflicting ibmq_paris. Obvious questions regarding how much of this information can be retrieved and whether it can be retrieved in a device-agnostic manner remain open for future work.

VI. CONCLUSIONS

We have presented an accreditation protocol that uses random Clifford circuits to ascertain the correctness of the outputs of quantum computations implemented on existing hardware. We have experimentally demonstrated its present practicality and mathematically established its future scalability.

Presently, the factor of 2 on the rhs of Eq. (1) represents the main obstacle towards increasing the number of qubits in our experiments beyond $n = 10$. Indeed, for target circuits with $n > 10$ qubits we find $p_{\text{inc}} > 50\%$; hence, our AP returns a bound on the VD that exceeds unity. This is a trivial bound since the VD is below unity by construction [13]. Nevertheless, better devices will extend the reach of our AP beyond 10-qubit circuits. We anticipate that in the future our AP, being fully scalable, will replace the protocols based on classical
simulations of quantum circuits [1–3] and will become a standard routine to characterize the outputs of noisy quantum computers.

ACKNOWLEDGMENTS

S.F. and A.D. were supported by the U.K. Networked Quantum Information Technologies (NQIT) Hub (Grant No. EP/M013243/1) in the early stages of this work. The research of S.T.M. and D.M. was sponsored by the Army Research Office and was accomplished under Grants No. W911NF-14-1-0124 and No. W911NF-21-1-0002. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

APPENDIX

This Appendix is organized as follows: In Sec. A1 we provide a derivation of the bound on the VD provided by our AP, in Sec. A2 we show that our protocol is robust to noise processes that depend weakly on the choice of one-qubit gates, and in Sec. A3 we compare our AP with the AP in Ref. [24]. We refer the reader to Sec. II of the main text for the notation.

1. Derivation of the bound on the VD

In this section we derive the bound on the VD provided by our AP [Eq. (1)]. Before presenting the mathematical proof, we calculate the state of the system at the end of a noisy implementation of the kth circuit executed in our AP, with \( k \in \{1, \ldots, v + 1 \} \).

Under the assumptions that noise is Markovian and that the cycles of one-qubit gates suffer gate-independent noise, the state of the system at the end of a noisy implementation of circuit \( k \) is

\[
\tilde{\rho}^{(k)}_{\text{out}} = \mathcal{M} \cdot \mathcal{E}_{m} \cdot \mathcal{U}_{m}^{(k)} \cdot \mathcal{E}_{Z_{m-1}} \cdot \mathcal{E}_{Z_{m-2}} \cdot \mathcal{U}_{m-1}^{(k)} \cdot \ldots \cdot \mathcal{E}_{Z_{2}} \cdot \mathcal{E}_{Z_{1}} \cdot \mathcal{U}_{1}^{(k)} \cdot \mathcal{R}(0 \langle 0 \rangle^{\otimes n}),
\]

(A1)

where \( \mathcal{R} \) is the noise in state preparation, \( \mathcal{U}_{j}^{(k)} \) is the \( j \)th cycle of one-qubit gates (two-qubit gates), \( \mathcal{E}_{Z_{j}, l} \) is the noise due to \( cZ_{j} \mathcal{U}_{l}^{(k)} \) (which depends only on \( cZ_{j} \) and not on \( \mathcal{U}_{l}^{(k)} \)), and finally, \( \mathcal{M} \) is the round of measurements. To simplify the structure of the noise, a QOTP is appended to each cycle of one-qubit gates in all the circuits. This randomizes the noise into stochastic Pauli errors [4,10,24,35,36] and allows rewriting \( \tilde{\rho}^{(k)}_{\text{out}} \) as

\[
\tilde{\rho}^{(k)}_{\text{out}} = \sum_{P_{0}, \ldots, P_{m}} q_{0}(P_{0}) \cdots q_{m}(P_{m}) M \cdot P_{c} \cdot Z_{1} \mathcal{U}_{1}^{(k)} \cdot \mathcal{P}_{0}(0 \langle 0 \rangle^{\otimes n}) \cdot \mathcal{P}_{1} \cdots \mathcal{P}_{m} \mathcal{Z}_{m} \mathcal{U}_{m}^{(k)},
\]

(A2)

where \( q_{0}(P_{0}) \cdots q_{m}(P_{m}) \) is the probability that the “pattern of Pauli errors” \( P_{0}, \ldots, P_{m} \in \{I, X, Y, Z\}^{\otimes n} \) occurs.

Importantly, note that the cycles of two-qubit gates are identical in all the circuits (target and traps), as well as the input state and measurements. Therefore, under the assumption that the one-qubit gates suffer gate-independent noise, the probabilities \( q(P_{0}) \cdots q(P_{m}) \) are the same in all the circuits, and so is the total probability of error per circuit

\[
p_{\text{err}} = \sum_{P_{0}, \ldots, P_{m} \neq I, \ldots, I} q_{0}(P_{0}) \cdots q_{m}(P_{m}).
\]

(A3)

We can now establish the bound on the VD.

Proof of Equation (1). To prove the inequality we make use of the following two statements:

Statement 1. Suppose that a trap circuit is afflicted by a “single-cycle” pattern of errors, i.e., a pattern such that \( P_{j0} \neq I \) for some \( j_{0} \in \{0, \ldots, m\} \) and \( P_{j} = I \) for all \( j \neq j_{0} \). Then, summed over the random one-qubit gates in the trap, the trap returns an incorrect output with probability 50% or above. (The proof is given in Appendix B of Ref. [24].)

Statement 2. Let \( q_{\text{out}}(j) = \sum_{P_{j} \neq I} q_{j}(P_{j}) \) be the error rate of cycle \( j \in \{0, \ldots, m\} \). Denoting by \( p_{\text{canc}} \) the probability that errors in different cycles of a trap circuit cancel each other, we have \( p_{\text{canc}} \leq C \), where

\[
C = O\left( \sum_{j \neq j_{0}} q_{\text{out}}(j) q_{\text{out}}(j_{0}) \right).
\]

(A4)

(The proof is at the end of this section.)
Statements 1 and 2 ensure that the trap circuits can detect errors with probability greater than 50%. To see this, consider the state of the system at the end of a trap circuit [Eq. (A2)]. Since all the gates in the trap circuits are Clifford, we can map arbitrary patterns of errors into single-cycle patterns. That is, we can commute the errors with the various cycles and merge them into a single error \( Q_{(p_0,\ldots,p_m)} \) (which depends on the initial errors \( p_0,\ldots,p_m \)), obtaining

\[
\tilde{\rho}_{\text{out}}^{(k)} = \sum_{p_0,\ldots,p_m} q_0(p_0) \cdots q_m(p_m) \mathcal{M}_C Z_m U_m^{(k)} \ldots Q_{(p_0,\ldots,p_m)} C Z_1 U_1^{(k)} (|0\rangle) \langle 0 |) \tag{A5}
\]

for some \( j_0 \in \{0, \ldots, m\} \). In principle, the errors in the trap may cancel each other, yielding \( Q_{(p_0,\ldots,p_m)} = I \). In particular, denoting by \( p_{\text{canc}} \) the probability of error cancellation, we obtain \( Q_{(p_0,\ldots,p_m)} \neq I \) with probability \( p_{\text{err}} (1-p_{\text{canc}}) \).

Having mapped the original pattern into a single-cycle pattern, Statement 1 ensures that if errors do not cancel (i.e., if \( Q_{(p_0,\ldots,p_m)} \neq I \)), the trap circuit returns the incorrect output with probability greater than 50%. This proves that

\[
p_{\text{inc}} \geq \frac{p_{\text{err}} (1-p_{\text{canc}})}{2}, \tag{A6}
\]

where \( p_{\text{inc}} \) is the probability that a trap returns an incorrect output.

We can now use Eq. (A6) to upper bound the VD between ideal and experimental outputs of the target circuit. Labeling the target circuit with \( v_0 \in \{1, \ldots, u+1\} \), we rewrite the state of the system at the end of the target circuit [Eq. (A2)] with \( k = v_0 \) as

\[
\tilde{\rho}_{\text{out}}^{(v_0)} = (1-p_{\text{err}}) \tilde{\rho}_{\text{out}}^{(v_0)} + p_{\text{err}} \sigma^{(v_0)}, \tag{A7}
\]

where \( \tilde{\rho}_{\text{out}}^{(v_0)} \) is the state of the system at the end of an ideal implementation of the target circuit and \( \sigma^{(v_0)} \) is a state encompassing the effects of noise. This leads to

\[
V_D = \frac{1}{2} \sum_\tau |p_{\text{ideal}}(\tau) - p_{\text{exp}}(\tau)| \tag{A8}
\]

where \( D(\tau, \tau') = \text{Tr}[\rho - \sigma] / 2 \) is the trace distance between states \( \rho \) and \( \sigma \). This leads to

\[
D(\tilde{\rho}_{\text{out}}^{(v_0)}, \tilde{\rho}_{\text{out}}^{(v_0)}) \leq p_{\text{err}} \leq \frac{2p_{\text{inc}}}{1-p_{\text{canc}}}. \tag{A9}
\]

Relying on Statement 2, in the proof of Eq. (1) we used \( p_{\text{canc}} \leq C \), as well as \( C \ll 1 \). The latter can be corroborated empirically using calibration data. For example, our largest circuit [the 10-qubit GHZ circuit; Fig. 4(a)] contains five cycles of one-qubit gates with an error rate of \( \approx 0.1% \) [41] and four cycles of two-qubit gates. Since each two-qubit gate has an error rate of \( \approx 1.5% \) [41], we estimate an error rate of \( \approx 1.5% \) for the first cycle, \( \approx 3% \) for the second and the fourth, and \( \approx 6% \) for the third. One-qubit measurements have error rates of \( \approx 2% \) [41], from which we estimate an error rate of \( \approx 20% \) for the final cycle of measurements. Overall, using Eq. (A4) we estimate \( C \approx 3% \). With the same strategy we estimate values of \( C \) below 3% for all the other circuits.

As we point out at the end of this section, \( p_{\text{canc}} \leq C \) is a loose bound, and we expect that \( p_{\text{canc}} \) be well below \( C \) in practice.

We now provide a proof of Statement 2.

**Proof of Statement 2.** For simplicity, let us first consider the case where errors afflict two neighboring cycles, \( j \) and \( j+1 \), and no other cycle. In this case, error cancellation happens when \( P_{j+1} = c Z_j U_{j+1}(P) \). Therefore, indicating by \( Q(j, j+1) \) the probability of error cancellation, we have

\[
Q(j, j+1) = \sum_{P_{j+1} \neq I} q_j(P_j) q_{j+1}(c Z_j U_{j+1}(P_j)) \tag{A11}
\]

\[
\leq \sum_{P_{j+1} \neq I} q_j(P_j) q_{j+1}(P_{j+1}) \tag{A12}
\]

\[
= q_{tot}(j) q_{tot}(j+1) \tag{A13}
\]

where to obtain Eq. (A12) we use the fact that the probability of error cancellation is no more than the product of the probabilities of errors happening. With the same arguments we can upper bound the probability \( Q(j, j+1) \) of error cancellation for patterns afflicting any two cycles \( j \) and \( j+1 \) as

\[
Q(j, j+1) \leq q_{tot}(j) q_{tot}(j+1) \tag{A14}
\]

This proves that the probability of error cancellation for patterns afflicting two cycles is, at most, quadratic in the cycles’ error rates.

With the same strategy it can be shown that the probability of error cancellation for patterns afflicting \( K \geq 2 \) cycles \( j_1, j_2, \ldots, j_K \) is higher order in the cycles’ error rates. Specifically, indicating this probability by \( Q(j_1, j_2, \ldots, j_K) \), we find

\[
Q(j_1, j_2, \ldots, j_K) \leq q_{tot}(j_1) q_{tot}(j_2) \cdots q_{tot}(j_K). \tag{A15}
\]

This leads to

\[
p_{\text{canc}} = \sum_{K \geq 2, \{m+1\}} \left( \sum_{j_1, j_2, \ldots, j_K} Q(j_1, j_2, \ldots, j_K) \right) \tag{A16}
\]

\[
= O \left( \sum_{j_1, j_2, \ldots, j_K} Q(j_1, j_2) \right) \tag{A17}
\]

\[
= O \left( \sum_{j_1, j_2, \ldots, j_K} q_{tot}(j_1) q_{tot}(j_2) \right). \tag{A18}
\]

We conclude the section by pointing out that \( Q(j_1, j_2, \ldots, j_K) \leq q_{tot}(j_1) q_{tot}(j_2) \cdots q_{tot}(j_K) \), and consequently, \( p_{\text{canc}} \leq C \), is a loose bound. To see this, note that to upper bound the rhs of Eq. (A11) we use \( q_{j+1}(c Z_j U_{j+1}(P)) \leq q_{tot}(j+1) \). That is, we replace the probabilities of individual errors (including negligible probabilities) with the total probability of error in cycle \( j+1 \). Based on this observation, we expect \( p_{\text{canc}} \) to be well below \( C \).

### 2. Robustness to weak gate-dependent noise

In the proof of Eq. (1) we have assumed that the cycles of one-qubit gates suffer gate-independent noise. In practice this assumption may be too stringent. To relax this assumption, in this section we analyze how gate-dependent noise may affect the effectiveness of our AP.
Theorem 1. Let us consider a circuit implementing the operation
\[ C = \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m)cZ_{m}U_m \cdots cZ_1U_1, \]  
(A19)
where the cycles of one-qubit gates \( U_1, \ldots, U_m \) are chosen with probability \( p(U_1, \ldots, U_m) \). Let
\[ C_{gi} = \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m)C_{z_{m}, \ldots, z_1}U_m \cdots C_{z_{m}, \ldots, z_1}U_1 \]  
(A20)
be a noisy implementation of \( C \) with noise \( E_{cZ_{m}, \ldots, z_1} \) that depends only on the cycle of two-qubit gates \( cZ_j \) and on the index \( j \). Let
\[ C_{gi} = \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m)C_{z_{m}, \ldots, z_1}U_m \cdots C_{z_{m}, \ldots, z_1}U_1 \]  
(A21)
be a noisy implementation of \( C \) with noise \( E_{cZ_{m}, \ldots, z_1} \) that also depends on the cycle of one-qubit gates \( U_j \). Averaging over all possible choices of one-qubit gates, we have
\[ ||C_{gi} - C_{gd}||_o \leq \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m) ||E_{cZ_{m}, \ldots, z_1} - E_{cZ_{m}, \ldots, z_1}||_o, \]  
(A22)
where \( || \cdot ||_o \) is the diamond distance.

The above theorem shows that if the noise depends weakly on the choice of one-qubit gates (i.e., \( ||E_{cZ_{m}, \ldots, z_1} - E_{cZ_{m}, \ldots, z_1}||_o \) is small for all \( j \)), the outputs of a circuit affected by gate-dependent noise remain close to those of the same circuit affected by gate-independent noise. This theorem is valid for any circuit in which the one-qubit gates are selected at random. Applied to the target and trap circuits discussed in this paper, it guarantees our AP is robust to noise that depends weakly on the choice of one-qubit gates.

Proof of Theorem 1. Our proof follows the same arguments as those in Ref. [35]. Let
\[ F_j = E_{cZ_{j}, \ldots, Z_1}U_{j}, \]  
(A23)
\[ G_j = E_{cZ_{j}, \ldots, Z_1}U_{j} \]  
(A24)
and
\[ F_{j:1} = F_j \cdots F_1 \]  
(A25)
\[ G_{j:1} = G_j \cdots G_1. \]  
(A26)
By induction it can be proven that
\[ F_{m:1} - G_{m:1} = \sum_{j=1}^{m} F_{m:j+1}(F_j - G_j)G_{j:1}. \]  
(A27)
Noting that
\[ C_{gi} = \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m)F_{m:1}, \]  
(A28)
\[ C_{gd} = \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m)G_{m:1}, \]  
(A29)
we have
\[ ||C_{gi} - C_{gd}||_o \leq \sum_{U_1, \ldots, U_m} p(U_1, \ldots, U_m) ||F_{m:j+1}(F_j - G_j)G_{j:1}||_o. \]  
(A30)

3. Comparing the present AP with the AP in Reference [24]

In this section we compare the AP demonstrated in this paper (which we name "present AP") with the AP in Ref. [24] (which we name "original AP"), demonstrating that the present AP leads to a significantly tighter bound on the VD.

In the original AP the user implements the target circuit together with a \( v \) trap circuit, initialized in the same way as the trap circuits in the present AP. After implementing all the circuits, the output of the target circuit is accepted only if all the trap circuits return the correct output; otherwise, it is discarded. The main result proven in Ref. [24] is that the VD between the probability distribution of the accepted outputs \( \{p_{acc}^{\text{exp}}(\tau)\} \) and the ideal probability distribution \( \{p_{\text{ideal}}(\tau)\} \) can be bounded as
\[ 1/2 \sum_{\tau} |p_{\text{ideal}}(\tau) - p_{\text{acc}}^{\text{exp}}(\tau)| \leq \frac{\kappa}{(v+1)\text{prob}(\text{acc})}, \]  
(A35)
where \( \kappa \approx 1.7 \) is a constant and \( \text{prob}(\text{acc}) \) is the probability that the output of the target circuit is accepted (which can be measured by running the AP multiple times with the same target and the same number of traps). To prove that the present AP leads to a better bound than the original AP, we now rewrite the rhs of Eq. (A35) as a function of the total probability \( p_{\text{traps}} \) that a trap circuit returns an incorrect output. The probability that all the traps return the correct output is \( \text{prob}(\text{acc}) = (1 - p_{\text{traps}})^v \), which gives
\[ 1/2 \sum_{\tau} |p_{\text{ideal}}(\tau) - p_{\text{acc}}^{\text{exp}}(\tau)| \leq \frac{\kappa}{(v+1)(1 - p_{\text{traps}})^v}. \]  
(A36)
The rhs of the above inequality depends on the number \( v \) of traps. All the values obtained at different \( v \) are valid upper
and the bound provided by the refined AP \cite{rinc} as functions of $p_{\text{inc}}$.\footnote{M. Nielsen and I. Chuang, Quantum Computation and Quantum Inform. Proc., 5, 456 (2005).
[5] J. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation, Phys. Rev. A 96, 012303 (2017).
[6] B. W. Reichardt, F. Unger, and U. Vazirani, A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, Proceedings of the 4th conference on Innovations in Theoretical Computer Science ITCS ’13 (ACM, 2013).
[7] A. Broadbent, How to verify a quantum computation, Theory Comput. 14, 1 (2018).
[8] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. 115, 220502 (2015).
[9] Joseph F. Fitzsimons and M. Hajdušek, and T. Morimae, Post hoc Verification of Quantum Computation, Phys. Rev. Lett. 120, 040501 (2018).
[10] S. Ferracin, T. Kapourniotis, and A. Datta, Reducing resources for verification of quantum computations, Phys. Rev. A 98, 022323 (2017).
[11] U. Mahadev, Classical verification of quantum computations, arXiv:1804.01082.
[12] D. Greenberger, M. Horne, and A. Zeilinger, Going beyond Bell’s theorem, in Bell’s Theorem, Quantum Theory, and Conceptions of the Universe, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 69–72.
[13] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, 10th anniversary ed. (Cambridge University Press, New York, 2000).
[14] Y. Weinstein, T. Havel, J. Emerson, and N. Boulant, Quantum process tomography of the quantum Fourier transform, J. Chem. Phys. 121, 6117 (2004).
[15] T. Proctor, A. Carignan-Dugas, K. Rudinger, E. Nielsen, R. Blume-Kohout, and K. Young, Direct Randomized Benchmarking for Multiqubit Devices, Phys. Rev. Lett. 123, 030503 (2019).
[16] D. Lu, H. Li, D.-A. Trottier, J. Li, A. Brodutch, A. P. Krishmanich, A. Ghavami, G. I. Dmitrienko, G. Long, J. Baugh, and R. Laflamme, Experimental Estimation of Average Fidelity of a Clifford Gate on a 7-Qubit Quantum Processor, Phys. Rev. Lett. 114, 140505 (2015).
[17] A. Erhard et al., Characterizing large-scale quantum computers via cycle benchmarking, Nat. Commun. 10, 5347 (2019).
[18] S. Merkel, J. Gambetta, J. Smolin, S. Poletto, and A. Corcoles, Self-consistent quantum process tomography, Phys. Rev. A 87, 062119 (2013).
[19] R. Blume-Kohout, J. King Gamble, E. Nielsen, J. Mizrahi, J. Sterk, and P. Maunz, Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit, arXiv:1310.4492.
[20] R. Blume-Kohout, J. Gamble, E. Nielsen, K. Rudinger, J. Mizrahi, K. Fortier, and P. Maunz, Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography, Nat. Commun. 8, 14485 (2017).
[21] S. Flammia and K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. 106, 230501 (2011).
[22] R. Harper, S. Flammia, and J. Wallman, Efficient learning of quantum noise, Nat. Phys. 16, 1184 (2020).
[23] S. T. Flammia and J. J. Wallman, Efficient estimation of Pauli channels, ACM Trans. Quantum Comput. 1, 1 (2020).
[24] S. Ferracin, T. Kapourniotis, and A. Datta, Accrediting outputs of noisy intermediate-scale quantum computing devices, New J. Phys. 21, 113038 (2019).
[25] M. L. Dahlhauser and T. S. Humble, Modeling noisy quantum circuits using experimental characterization, Phys. Rev. A 103, 042603 (2021).
[26] I. L. Chuang and M. A. Nielsen, Prescription for experimental

bounds on the VD. The smallest value

$$\eta_{\text{best}} = \min_v \frac{\kappa}{(v + 1)(1 - p_{\text{inc}})^v}$$ \hspace{4cm} (A37)$$

corresponds to the best upper bound and can be calculated by implementing the AP many times for different values of $v$.

In Fig. 8 we plot the bounds provided by the present AP and original AP as functions of $p_{\text{inc}}$. As can be seen, for all the values of $p_{\text{inc}}$ the latter bound is larger than the former one by approximately a factor of 2. Moreover, the bound provided by the original AP exceeds unity for all $p_{\text{inc}} \geq 0.25$, while that provided by the present AP exceeds unity only for $p_{\text{inc}} \geq 0.5$.

While the present AP yields tighter bounds on the VD, the original AP has been proven to be robust to a more general noise model. Indeed, the noise model assumed in Ref. [24] encompasses arbitrary coupling between the system and environment, allowing for time-correlated noise. There is thus a trade-off between the generality of noise models captured and the tightness of the bounds obtained.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure8.png}
\caption{The best value provided by the original AP \cite{rinc} and the bound provided by the refined AP \cite{rinc} as functions of $p_{\text{inc}}$.}
\end{figure}
determination of the dynamics of a quantum black box, J. Mod. Opt. 44, 2455 (1997).

[27] D. Greenbaum, Introduction to quantum gate set tomography, arXiv:1509.02921.

[28] M. Da Silva, O. Landon-Cardinal, and D. Poulin, Practical Characterization of Quantum Devices without Tomography, Phys. Rev. Lett. 107, 210404 (2011).

[29] O. Moussa, M. Da Silva, C. Ryan, and R. Laflamme, Practical Experimental Certification of Computational Quantum Gates Using a Twirling Procedure, Phys. Rev. Lett. 109, 070504 (2012).

[30] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, Phys. Rev. A 77, 012307 (2008).

[31] E. Magesan, J. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, Phys. Rev. Lett. 106, 180504 (2011).

[32] K. Wright et al., Benchmarking an 11-qubit quantum computer, Nat. Commun. 10, 5464 (2019).

[33] G. Barron, F. A. Calderon-Vargas, J. Long, D. P. Pappas, and S. E. Economou, Microwave-based arbitrary CPHASE gates for transmon qubits, Phys. Rev. B 101, 054508 (2020).

[34] K. Mølmer and A. Sørensen, Multiparticle Entanglement of Hot Trapped Ions, Phys. Rev. Lett. 82, 1835 (1999).

[35] J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, Phys. Rev. A 94, 052325 (2016).

[36] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, Piscataway, NJ, 2009), pp. 517–526.

[37] A. Hashim et al., Randomized compiling for scalable quantum computing on a noisy superconducting quantum processor, arXiv:2010.00215.

[38] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Am. Stat. Assoc. 58, 13 (1963).

[39] P. Jurcevic et al., Demonstration of quantum volume 64 on a superconducting quantum computing system, arXiv:2008.08571.

[40] IBM Quantum Experience, https://quantum-computing.ibm.com/.

[41] S. Ferracin, S. Merkel, D. McKay, and A. Datta, Data and notebooks for Experimental accreditation of outputs of noisy quantum computers, 2021, doi:10.5281/zenodo.4592487.