Fault-tolerant verification of quantum supremacy & Accreditation of NISQ devices

Animesh Datta

Department of Physics, University of Warwick, UK

Samuele Ferracin, Theodoros Kapourniotis

June 10, 2019

Quantum Information and String Theory 2019, Kyoto

EPSRC Engineering and Physical Sciences Research Council

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Us

arXiv.org > quant-ph > arXiv:1703.09568

Search...

Quantum Physics

Nonadaptive fault-tolerant verification of quantum supremacy with noise

Theodoros Kapourniotis, Animesh Datta

(Submitted on 28 Mar 2017 (v1), last revised 27 Feb 2019 (this version, v3))

arXiv.org > quant-ph > arXiv:1811.09709

Search...

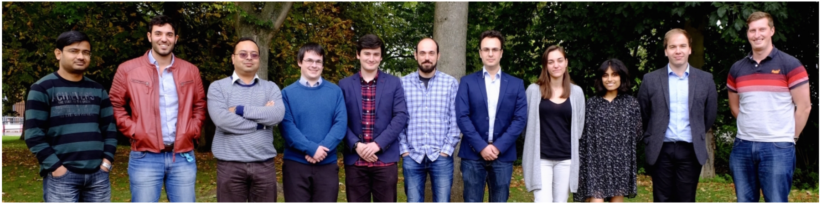
Quantum Physics

Accrediting outputs of noisy intermediate-scale quantum computing devices

Samuele Ferracin, Theodoros Kapourniotis, Animesh Datta

(Submitted on 23 Nov 2018 (v1), last revised 30 May 2019 (this version, v2))

Papers



- Dominic Branford
- Samuele Ferracin
- Jamie Friel
- Evangelia Bisketzi
- Aiman Khan
- Andrew Jackson
- Theodoros Kapourniotis
- Max Marcus
- Francesco Albarelli

Quantum supremacy

Quantum supremacy

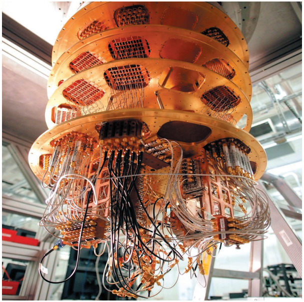
Why quantum supremacy? It used to be ...

1. quantum simulator — Manin/Feynman (1980/82)
2. quantum computer — Shor (1994)
3. quantum 'supreme' device — Aaronson/Arkhipov (2013)

It may look like the promise of quantum information is shrinking

The slide down from computation to supremacy is because

- Experiments are hard!
- All of DiVincenzo's criteria need fulfilling



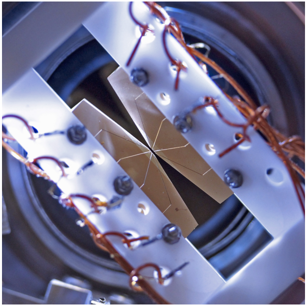


Figure: Experimental advances have been enormous (Google, UMD)

We still don't have a big enough system with low enough noise

If we had a universal QC, we wouldn't be talking about supremacy

Theoretical shortcomings

- Many examples of exponential improvement in QIP
- Simon's algorithm (oracle separation between BPP & BQP)
- Shor's algorithm (compared to best known classical algorithm)
- ✗ Hofstadter butterfly @ Google (provably polynomial)
- ...

No theoretical impossibility of classical polynomial algorithms

Tang, 1807.04271

No proof QC is exponentially stronger than classical

If we had a proven exponential gap of QC, we wouldn't be talking about supremacy

So, we've settled for

Quantum supremacy

- Theoretical proof of exponential gaps (with conjectures)
- Sub-universal (typically sampling) problems

- The idea has been around for a long time

  Knill/Laflamme, DQC1, 1998- | Terhal/DiVincenzo, Fermionic QC, 2002-

- Revived interest after complexity-theoretic hardness proofs (sampling problems with conjectures)

  Bremner/Jozsa/Shepherd/Montanaro, IQP, 2010- | Aaronson/Arkhipov, BosonSampling, 2013-

  Morimae/Fujii/Fitzsimons, $DQC1_k$ 2014- | Fefferman/Umans, FourierSampling, 2015-

  Farhi/Harrow, QAOA, 2016- | Google, RandomSampling, 2016-

  Gao/Wang/Duan, IsingSampling, 2016

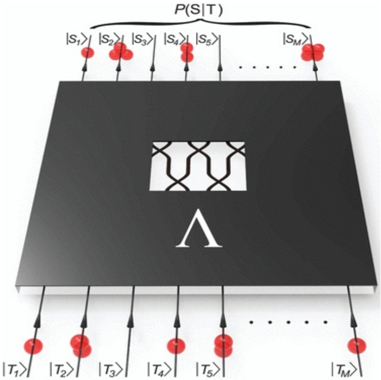
- Some performed/proposed experiments

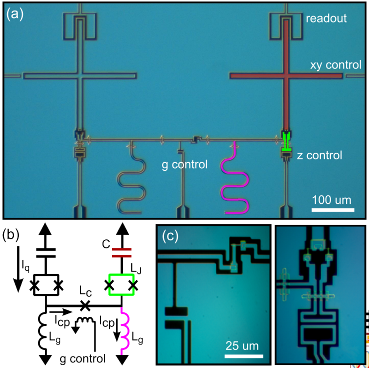
  Oxford, Vienna, Rome, Brisbane, Shanghai, Google, IBM, ...

Quantum supremacy experiments

What do quantum supremacy experiments prove?

Figure: Boson sampling (Oxford), Random sampling(Google)





Is quantum supremacy <u>really</u> easier than quantum computation?

All experiments are imperfect and noisy

- Can imperfect/noisy experiments ‘show’ quantum supremacy?

All experiments are imperfect and noisy

- Can imperfect/noisy experiments 'show' quantum supremacy?

- Physical system must be quantum (non-classical)

  Rahimi-Keshari/Ralph/Caves, PRX, **6**, 021039, (2016)

  [need low(er) noise/imperfection]

- Computational task must be supreme (super-classical)

  DWave | Neville *et al.* Nat. Phys. 13, 1153 (2017) | Google/IBM

  [need large(r) system]

All experiments are imperfect and noisy

- Can imperfect/noisy experiments 'show' quantum supremacy?
- But even with better and larger systems ...

Noise

- Is the problem still hard?
- Otherwise experiments useless (for quantum supremacy)

Imperfections

- Is the solution correct?
- Not solving decision problems

The two fundamental issues are

- Proofs of hardness of sampling (with noise)
- Verification of quantum supremacy (with imperfections)

Aaronson/Chen, 1612.05903

Harrow/Montanaro, Nature 549, 203 (2017)

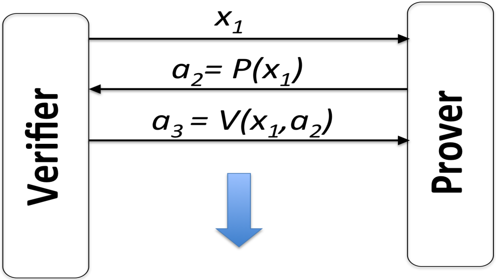
Why do we care?

- Is quantum supremacy easier than quantum simulation?
- Is quantum supremacy easier than quantum computation?
- If so, by how much?

Verification of quantum computation

I. Direct certification, benchmarking (Hardware solution)
   Certify a small system, hope it stills holds for a big one

II. Interactive proof system: verification (Software solution)



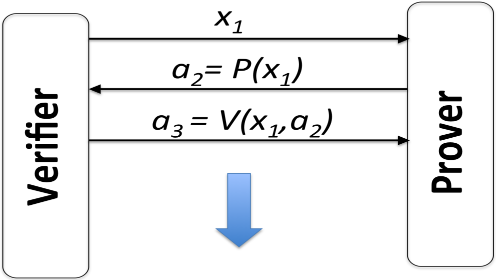
Aharonov, Ben-Or, Broadbent, Fitzsimmons, Hayashi, Kashefi, Morimae, Vazirani, Vidick, ...

To verify, must trust

Our work: 'Prepare-and-send' protocol

Verification of quantum computation

II. Interactive proof system: verification (Software solution)



- Hide easy 'trap' computations within hard computation
- Check the correctness of the 'traps'
- Bound the correctness of the overall computation
- Also useful in adverserial setting

Aharonov, Ben-Or, Broadbent, Fitzsimmons, Hayashi, Kashefi, Morimae, Vazirani, Vidick, ...

To verify, must trust

Our work: 'Prepare-and-send' protocol

Verification scheme for quantum supremacy

New definition of verifiability over i.i.d. repetitions based on

$$\text{var} \equiv \frac{1}{2} \sum_{\boldsymbol{x}} |q^{\text{exc}}(\boldsymbol{x}) - q^{\text{nsy}}(\boldsymbol{x})|,$$

Fitzsimmons/Kashefi, PRA 96, 012303 (2017)

(1) Takes as input a verification protocol, $M \in \mathbb{N}, l \in [0, 1]$

(2) Outputs a string and a bit.

(3) The bit determines if the string is accepted or rejected.

(4) After running M i.i.d repetitions of (1) it outputs one of the M output strings at random. Accept if at least a fraction l of the protocols accept and reject otherwise.

Verifiability

Definition (Verifiability)

A scheme is verifiable if its output is

- $(\delta', \delta)-$complete: For an honest prover having only bounded noise, the scheme accepts at least with probability δ', and

$$\mathrm{var} \leq 1 - \delta$$

  for the output string.
- $(\varepsilon', \varepsilon)-$sound: For any, including adversarial, prover if the scheme accepts then

$$\mathrm{var} \leq \varepsilon$$

  with confidence ε'.

Kapourniotis/AD, arXiv:1703.09568

Blindness is a necessary ingredient in our verification scheme

Verifiability

Definition (Verifiability)

A scheme is verifiable if its output is

- $(\delta', \delta)-$complete: For an honest prover having only bounded noise, the scheme accepts at least with probability δ', and

$$\mathrm{var} \leq 1 - \delta$$

  for the output string.

- $(\varepsilon', \varepsilon)-$sound: For any, including adversarial, prover if the scheme accepts then

$$\mathrm{var} \leq \varepsilon$$

  with confidence ε'.

Kapourniotis/AD, arXiv:1703.09568

Blindness is a necessary ingredient in our verification scheme

Our work: Trap-based verification of Ising sampling problem

Ising sampler

- Translationally-invariant, nonadaptive, Ising spin model

$$\mathcal{H} = -\sum_{\langle i,j \rangle} J Z_i Z_j + \sum_i B_i Z_i$$

- The probability $p_{\boldsymbol{x}}$ of measuring bit string $\boldsymbol{x}$ from partition function $\mathcal{Z}_{\boldsymbol{x}}$

$$p_{\boldsymbol{x}} = \frac{\left|\mathrm{Tr}\left(e^{-i(\mathcal{H}+\frac{\pi}{2}\sum_i x_i Z_i)}\right|^2}{2^{2mn}} \equiv \frac{|\mathcal{Z}_{\boldsymbol{x}}|^2}{2^{2mn}}$$

Gao/Wang/Duan, PRL, **118**, 40502 (2017)

- Partition function at imaginary temperatures insightful

Lee/Yang, Phys. Rev. **87**, 410 (1952)

Fujii/Morimae, NJP **19**, 033003 (2017)

Goldberg/Guo, Computational Complexity **26**, 765 (2017)

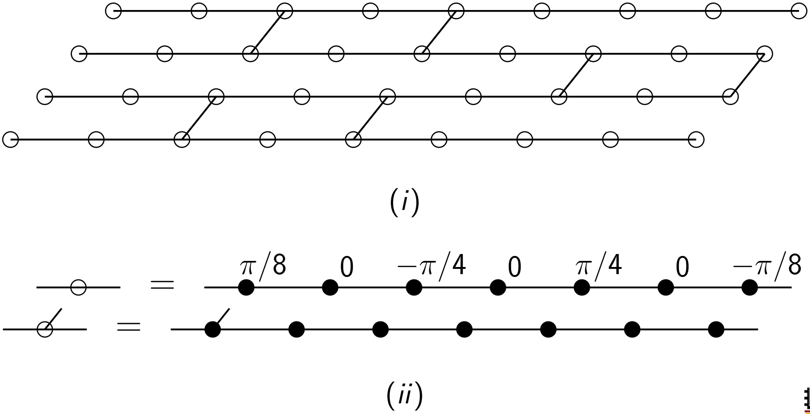


Figure: Avoids Multi-instanceness (unlike IQP, BS, RSC)

Gao/Wang/Duan, PRL, **118**, 40502 (2017)

Traps

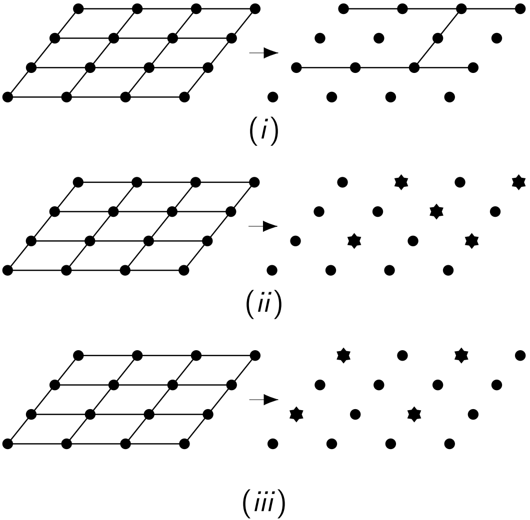


Figure: Verifier chooses a random ordering of $2\kappa + 1$ graph states. Single qubit traps.

Kapourniotis/AD, arXiv:1703.09568

Noise model

- 'Prepare-and-send' protocol
- Blindness (Quantum one-time pad)

$$\mathcal{N}_j = (1 - \epsilon_{V,P})\mathcal{I} + \mathcal{E}_j$$

where

- $\epsilon_V = ||\mathcal{E}_j||_\diamond$ for preparation noise [Verifier]
- $\epsilon_P = ||\mathcal{E}_j||_\diamond$ for entangling/measurement noise [Honest Prover]

Theorem (Non-fault tolerance verification scheme)

There exists a verification scheme with

$$M = \frac{\log(1/\beta)}{2\kappa^2 N^2(\epsilon_V + \epsilon_P)^2},$$

$$I = 1 - \kappa N(2\epsilon_V + 4\epsilon_P)$$

that is

$$\left(1-\beta, 1-\sqrt{N(\epsilon_V + 3\epsilon_P)}\right) - \textit{complete}$$

and

$$\left(1-\beta, \sqrt{\kappa N(3\epsilon_V + 5\epsilon_P) + \Delta_\kappa}\right) - \textit{sound},$$

where $\Delta_\kappa = \kappa!(\kappa+1)!/(2\kappa+1)! \sim 2^{-\kappa}$.

Kapourniotis/AD, arXiv:1703.09568

Recall

Definition (Verifiability)

A scheme is verifiable if its output is

- $(\delta', \delta)-$complete: For an honest prover having only bounded noise, the scheme accepts at least with probability δ', and
$$\text{var} \leq 1 - \delta$$
for the output string.
- $(\varepsilon', \varepsilon)-$sound: For any, including adversarial, prover if the scheme accepts then
$$\text{var} \leq \varepsilon$$
with confidence ε'.

Kapourniotis/AD, arXiv:1703.09568

Problem

For verifiable quantum supremacy, we need

$$N(\epsilon_V + 3\epsilon_P) \quad \text{const.}$$

and

$$\kappa N(3\epsilon_V + 5\epsilon_P) + \Delta_\kappa \qquad \downarrow$$

Impossible in large systems(N) with constant noise($\epsilon_{P,V}$)

Want to verify quantum supremacy for large N and constant $\epsilon_{P,V}$

Solution: Quantum fault tolerance

- Use FT (3D cluster state) encoding for universal QC

✗ RHG encoding require adaptive operations (gate distillation)

Raussendor/Harrington/Goyal, NJP 9, 199 (2007)

- On target computation, use free postselection due to Fujii

1610.03632

- Trap computation is Clifford, so nonadaptive

Solution: Quantum fault tolerance

✗ RHG encoding require adaptive operations (gate distillation)

Raussendor/Harrington/Goyal, NJP 9, 199 (2007)

- On target computation, use free postselection due to Fujii

1610.03632

- Trap computation is Clifford, so nonadaptive
- FT thresholds

RHG error-correction in traps

$$\epsilon_{\text{thres}} = 0.75\%$$

Less than $\epsilon_{\text{thres}} = 2.84\%$ for unverified quantum supremacy

1610.03632

RHG error-detection in traps

$$\epsilon_{\text{thres}} = 1.97\%$$

Extend Fujii 1610.03632 to additive errors

Kapourniotis/AD, arXiv:1703.09568

FT thresholds for verifiable quantum supremacy

Supremacy easier than universal QC

$$\epsilon_{\text{thres}} = 1.97\%$$

- Replace error correction with error detection
- Works as isolated trap qubits isolated can be retransmitted individually
- Same completeness & soundness with κ replaced by $M\kappa$

ϵ	$\epsilon_{\text{thres}}/20$	$\epsilon_{\text{thres}}/50$	$\epsilon_{\text{thres}}/100$
M	3×10^8	2863	54

✓ M independent of problem size

- Improved by judicious braiding or other topological code
- Larger ϵ_{thres} with simpler problem specific code

Kapourniotis/AD, arXiv:1703.09568

Blindness and fault tolerance

✗ Leaking logical measurement angles in magic state distillation

✗ For distillation, need to reveal information about state distilled

Ising Sampler and Trap Computations MBQC
(Logical layer)

Protected topology using defects

Blind 3D cluster-state MBQC
(Physical layer)

Kapourniotis/AD, arXiv:1703.09568

On target computation, use free postselection due to Fujii

$$\mathrm{var}^{\mathrm{Post}} \equiv \frac{1}{2}\sum_{\boldsymbol{x}} |q^{\mathrm{exc}}(\boldsymbol{x}|y=0) - q^{\mathrm{nsy}}(\boldsymbol{x}|y=0)|$$

Definition (Verifiability of a scheme for post-selected distribution)

A scheme is verifiable conditioned on the post-selection register being zero, if its output is

- $(\delta', \delta)-$complete: For an honest prover having only bounded noise, the scheme accepts at least with probability δ', and

$$\mathrm{var}^{\mathrm{Post}} \leq 1-\delta$$

  for the the output string.

- $(\varepsilon', \varepsilon)-$sound: For any, including adversarial, prover if the scheme accepts, then

$$\mathrm{var}^{\mathrm{Post}} \leq \varepsilon$$

  with confidence ε'.

Kapourniotis/AD, arXiv:1703.09568

Our results (Long term aim of experiments)

Theorem (Fault-tolerant verification scheme)

There exists a verification scheme with

$$M = \log(1/\beta)/(2\epsilon''^2)$$

and

$$l = (1 - 2\epsilon''),$$

that is

$$(1-\beta, 1-\sqrt{\epsilon''}) - \textit{complete}$$

and

$$(1-\beta, \sqrt{3\epsilon'' + \Delta_\kappa}) - \textit{sound}$$

where $\Delta_\kappa = \kappa!(\kappa+1)!/(2\kappa+1)!$.

- Milestone towards FT QC

Kapourniotis/AD, arXiv:1703.09568

Conjecture (Average-case hardness)

For $0 \leq \alpha_1, \beta_1 \leq 1$, *approximating the probability distribution of the Ising sampler by* $p^{\mathrm{apx}}(\boldsymbol{x}|y=0)$ *up to multiplicative error*

$$|p^{\mathrm{apx}}(\boldsymbol{x}|y=0) - q^{\mathrm{exc}}(\boldsymbol{x}|y=0)| \leq \alpha_1 q^{\mathrm{exc}}(\boldsymbol{x}|y=0)$$

in time poly$(|\boldsymbol{x}|, 1/\alpha_1, 1/\beta_1)$ *is* $\#P$*-hard for at least a fraction* β_1 *of* $\boldsymbol{x}$ *instances.*

Conjecture (Anti-concentration)

There exist some $0 \leq \alpha_2, \beta_2 \leq 1$, $1/\alpha_2 \in \mathrm{poly}(1/\beta_2)$ *such that for all* x

$$\mathrm{prob}\left(q^{\mathrm{exc}}(\boldsymbol{x}|y=0) \geq \frac{\alpha_2}{2^N}\right) \geq \beta_2$$

More general than Bremner/Montanaro/Shepherd, PRL 117, 080501 (2016)

Theorem (Fault-tolerant hardness)

Assume that the two Conjectures hold. Then sampling from the output distribution of the experimental Ising sampler $q^{\mathrm{nsy}}(\boldsymbol{x}, y)$ *with a classical machine, assuming a* $(\varepsilon', \varepsilon)$*-sound verification scheme accepts with*

$$\varepsilon \leq \frac{(\beta_1 + \beta_2 - 1 - 2^{-N})\alpha_1\alpha_2}{2},$$

implies, with confidence ε'*, a collapse in the polynomial hierarchy to the third level.*

Kapourniotis/AD, arXiv:1703.09568

First FT verification of quantum supremacy

FT supremacy verification milestone for FT QC

Kapourniotis/AD, arXiv:1703.09568

We still need

- bespoke FT thresholds for verifying specific supremacy models
- bespoke error correcting codes for specific supremacy models
- verification schemes for specific architectures
- to use verification schemes in experiments
  - short term (Thm 1)
  - long term (Thm 2/3)
  - But we want everything now. NISQ devices...

NISQ devices have a credibility problem

If/when a NISQ device solves a hard problem (not in NP), how do we know its done so correctly?

- ✗ NISQ devices are noisy and imperfect
- ✗ Cannot check efficiently on a classical computer

"Quantum Accreditation"

To build big (intermediate) systems, start with small ones

- State tomography
- Process tomography
- Measurement (Detector) tomography

Numerous references ...

Too many parameters for NISQ devices

Good gate fidelities are not enough

- Randomised benchmarking
- Gate set tomography

Knill *et. al.*, PRA 77, 012307 (2008)

Blume-Kohout *et. al.*, Nat. Comm. 8, 14485 (2017)

Makes unrealistic assumptions

Average fidelity ϵ is a poor bound

Sanders *et. al.*, NJP 18 012002 (2016)

$$1 - \epsilon \lesssim \epsilon_G = ||G - G^{\mathrm{ideal}}||_\diamond \lesssim \sqrt{1 - \epsilon}$$

Verification of quantum supremacy

PHYS: Statistical methods (e.g., cross entropy)

Inadequate | Bouland *et al.*, Nat. Phys. (2018)

TCS: Interactive proof system

Childs, Aharonov, Ben-Or, Broadbent, Eisert, Fitzsimmons, Hayashi, Kashefi, Mahajan

Morimae, Vazirani, Vidick, Zhu, Us ....

- Hide easy 'trap' computations within hard computation
- Check the correctness of the 'traps'
- Bound distance between ideal (p_{id}) and actual (p_{act}) output

Exorbitant overheads (due to MBQC)

- Even constant overheads are impractical

CS meets experiments: Scalable *vs* practical

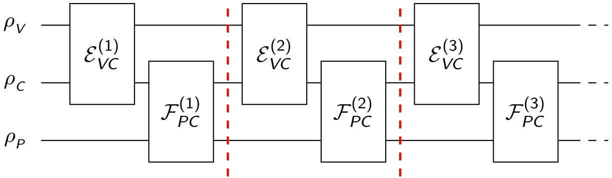
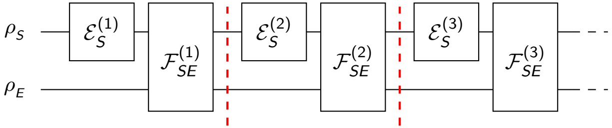


Figure: CS: Verifier, prover, and a shared register C.

Figure: Experiments: System and environment.



- In the circuit model

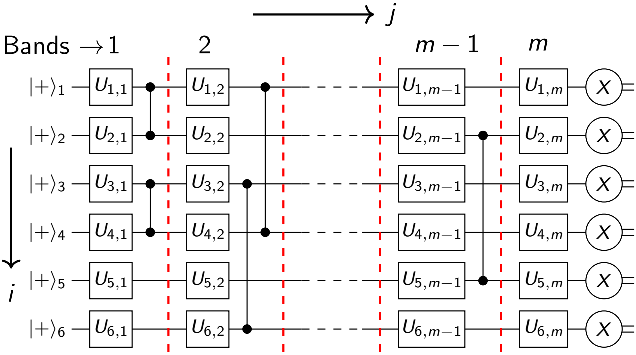


Figure: A six-qubit example of target circuit.

- Several ($v > 1$) trap circuits
- Traps designed to capture all noise
- Trap and target circuits of same size

Our work

Ferracin/Kapourniotis/AD, 1811.09709

- In the circuit model
- Different trust assumptions (noise model)

N1: Noise in state preparation, entangling gates, measurements is arbitrary CPTP map encompassing system & environment

$$\rho_{\text{out}} = \mathrm{Tr}_E \left[\circ_{p=1}^{q} \mathcal{N}_{SE}^{(p)} (\mathcal{E}_S^{(p)} \otimes \mathcal{I}_E)(\rho_S \otimes \rho_E) \right]$$

and is unbounded in diamond norm;

N2: Single qubit gates are trusted

Single qubit gates are the best component in leading architectures

Different from 'prepare & send' or 'receive & measure'

Accreditation Protocol - One run

$$\rho_{\text{out}} = \mathrm{Tr}_E\left[\,\circ_{p=1}^{q}\,\mathcal{N}_{SE}^{(p)}(\mathcal{E}_S^{(p)} \otimes \mathcal{I}_E)(\rho_S \otimes \rho_E)\right]$$

Protocol $\{\mathcal{E}_S^{(p)}\}_{p=1}^{q}$ accredits outputs in presence of $\{\mathcal{N}_{SE}^{(p)}\}_{p=1}^{q}$ if

$$\begin{aligned}\rho_{\text{out}} &= b\,\tau'^{\,\text{tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| \\ &+ (1-b)\left(l\,\sigma^{\text{tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-l)\tau^{\text{tar}}_{\text{out}} \otimes |\text{rej}\rangle\langle\text{rej}|\right),\end{aligned}$$

where
$\sigma^{\text{tar}}_{\text{out}}$ ($\tau'^{\,\text{tar}}_{\text{out}}$) is target circuit state after noiseless (noisy) protocol,
$\tau^{\text{tar}}_{\text{out}}$ is an arbitrary state for the target circuit,
$|\text{acc}\rangle$ is the state of the flag indicating acceptance,
$|\text{rej}\rangle = |\text{acc} \oplus 1\rangle$,
$0 \leq l \leq 1$, $0 \leq b \leq \varepsilon$ and $\varepsilon \in [0,1]$.

$1-\varepsilon$ is the *credibility* of the accreditation protocol.

Accreditation Protocol - One run

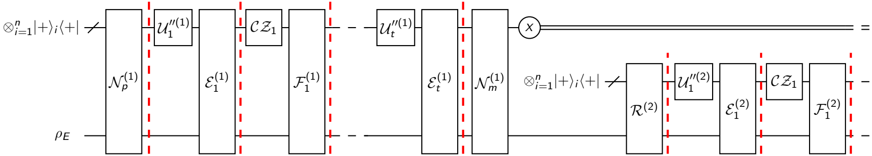


Figure: One target computation and v trap computations.

Correlated noise across all $v+1$ circuits - in space and time.

- Use $U'_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j}$, $\alpha_{i,j}, \alpha'_{i,j} \in \{0,1\}$ are random bits
- Pauli twirl decomposes noise into combination of local Paulis
- Traps designed to capture all local Pauli noise

Accreditation Protocol - Many runs

- After d protocol runs (with same target and v different traps),
- If all runs are affected by i.i.d. noise,
- then, with confidence $1 - e^{-2d\theta^2}$, $\theta \in (0, N_{\text{acc}}/d)$

$$\frac{1}{2} \sum_{\bar{s}} \left| p_{\text{noiseless}}(\bar{s}) - p_{\text{noisy}}(\bar{s}) \right| \leq \frac{\varepsilon}{N_{\text{acc}}/d - \theta} ,$$

for all $N_{\text{acc}} \in [0, d]$ protocol runs ending with $|\text{acc}\rangle$ flag bit.

Results

Theorem

Suppose that all single-qubit gates are <u>noiseless</u>.
For any number $v \geq 3$ of trap circuits, our protocol can accredit the outputs of a noisy quantum computer affected by noise of the form N1 with

$$\varepsilon = \frac{\kappa}{v+1} \; ,$$

where $\kappa = 3(3/4)^2 \approx 1.7$.

Ferracin/Kapourniotis/AD, 1811.09709

Noisy single qubit gates

- Different trust assumptions (noise model)

N1: Noise in state preparation, entangling gates, measurements is arbitrary CPTP map encompassing system & environment

$$\rho_{\text{out}} = \mathrm{Tr}_E\big[\circ_{p=1}^{q}\, \mathcal{N}_{SE}^{(p)}(\mathcal{E}_S^{(p)} \otimes \mathcal{I}_E)(\rho_S \otimes \rho_E)\big]$$

and is unbounded in diamond norm;

N2: Noise in single-qubit gates is arbitrary (inc. gate-dependent) CPTP map encompassing system & environment

$$\widetilde{\mathcal{U}}_j = \mathcal{N}_j^{(k)}(\mathcal{U}_j \otimes \mathcal{I}_E) \;\; \text{with} \;\; ||\mathcal{N}_j^{(k)} - \mathcal{I}_{SE}||_\diamond \leq r_j^{(k)}$$

and $0 \leq r_j^{(k)} < 1$ (bounded in diamond norm).

Results

Theorem

Our protocol with $v \geq 3$ of trap circuits can accredit the outputs of a noisy quantum computer affected by noise of the form N1 *and* N2 *with*

$$\varepsilon = g\frac{\kappa}{v+1} + \left(1 - g\right), \tag{1}$$

where $\kappa = 3(3/4)^2 \approx 1.7$ *and* $g = \prod_{j,k}(1 - r^{(k)}_{\text{max},\ j})$.

Ferracin/Kapourniotis/AD, 1811.09709

$$\frac{1}{2}\sum_{\bar{s}}\left|p_{\text{noiseless}}(\bar{s}) - p_{\text{noisy}}(\bar{s})\right| \le \frac{\varepsilon}{N_{\text{acc}}/d - \theta}\ ,$$

Since N_{acc}/d is an estimate of prob(acc) (and if prob(acc)$\geq \delta$.)

$$\frac{1}{2}\sum_{\bar{s}}\left|p_{\text{noiseless}}(\bar{s}) - p_{\text{noisy}}(\bar{s})\right| \le \frac{\varepsilon}{\mathrm{prob(acc)}} \le \frac{\varepsilon}{\delta}.$$

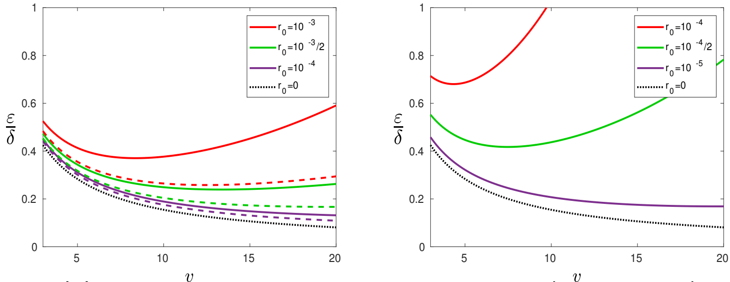


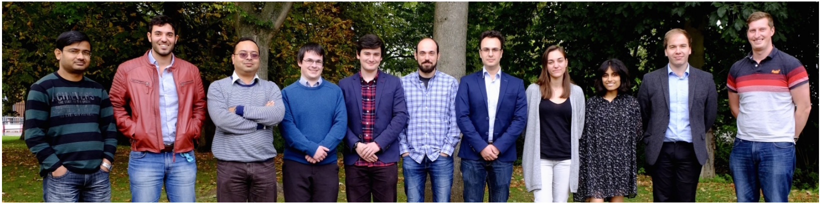
Figure: **(a)** Preparing GHZ states, with $n = m = 7$ (dashed lines) and $n = m = 10$ (solid lines). **(b)** Google RCS supremacy with $n = 62$ qubits and circuit depth $m = 34$.

So, Accreditation

- is practical (and scalable)
- is inspired by trap-based verification schemes
- is different from verification
- combines best features from physics & CS
- inspires new mesothetic (verifier-in-the-middle) verification scheme

Ferracin/Kapourniotis/AD, 1811.09709

Us



- Dominic Branford
- Samuele Ferracin
- Jamie Friel
- Evangelia Bisketzi
- Aiman Khan
- Andrew Jackson
- Theodoros Kapourniotis
- Max Marcus
- Francesco Albarelli

Thank you!

www.warwick.ac.uk/qinfo