Title: Brownian Circuits and Quantum Randomness

Speakers: Gregory Bentsen

Collection/Series: Quantum Information

Subject: Quantum Information

Date: November 27, 2024 - 11:00 AM

URL: https://pirsa.org/24110085

Abstract:

Abstract: Randomness is a powerful resource for information-processing applications. For example, classical randomness is essential for modern information security and underpins many cryptographic schemes. Similarly, quantum randomness can protect quantum information against noise or eavesdroppers who wish to access or manipulate that information. These observations raise a set of related questions: How quickly and efficiently can we generate quantum randomness? How much quantum randomness is necessary for a given task? What can we use quantum randomness for? In this talk, I address these questions using all-to-all Brownian circuits, a family of random quantum circuits for which exact results can often be obtained via mean-field theory. I will first demonstrate that all-to-all Brownian circuits form k-designs in a time that scales linearly with k. I will then discuss how these circuits can be applied to study Heisenberg-limited metrology and quantum advantage. In particular, I will discuss a time-reversal protocol that can achieve Heisenberg-limited precision in cavity QED and trapped ion setups; I will also discuss the application of these circuits to studying classical spoofing algorithms for the linear cross-entropy benchmark, a popular measure of quantum advantage.

Brownian Circuits & Quantum Randomness

Gregory Bentsen
Minerva University
The College of William & Mary

Quantum Information Seminar

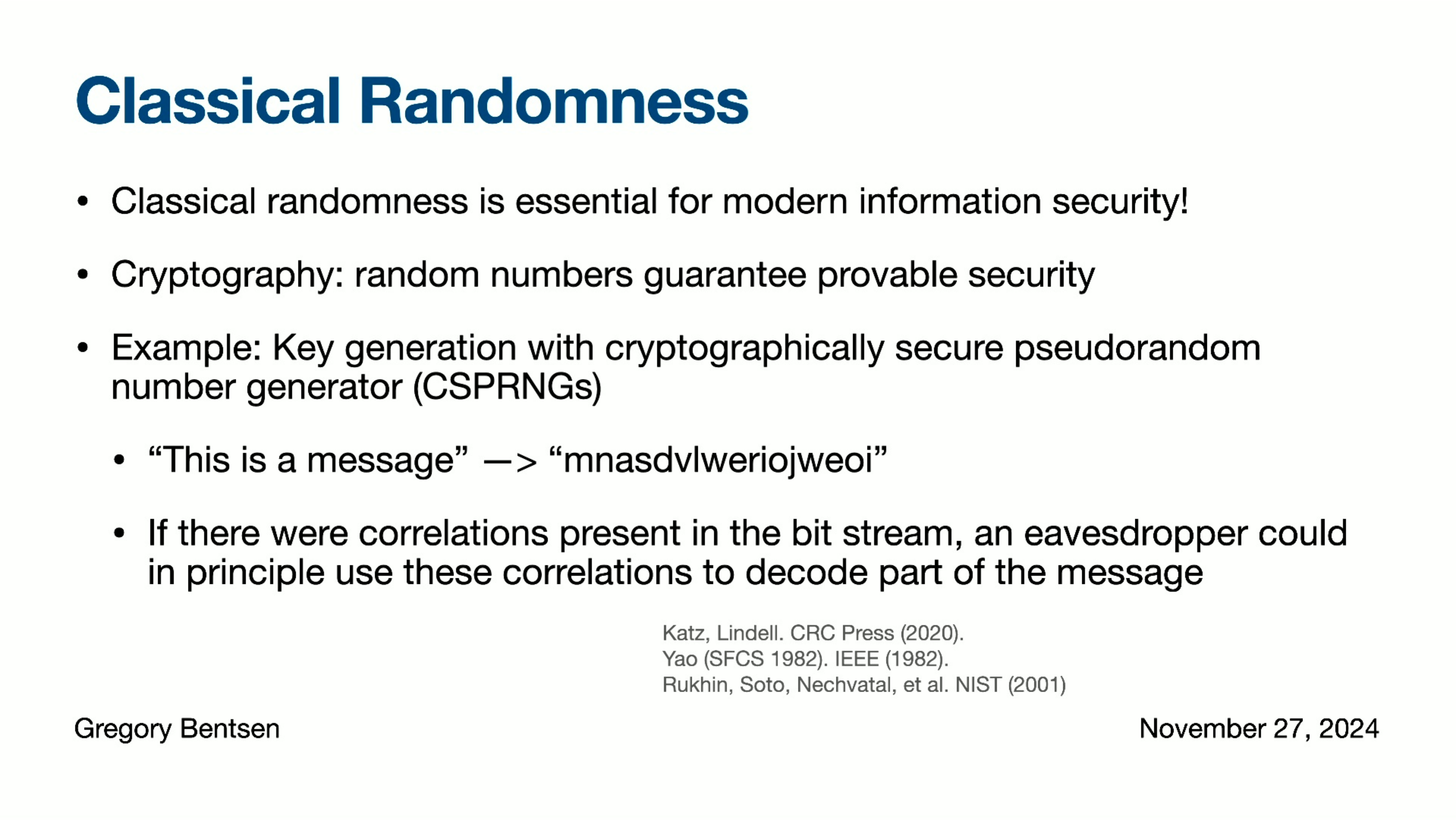
November 27, 2024

This Talk: Randomness

- Randomness is a valuable resource
- How quickly / efficiently can we generate randomness?
- How much randomness is necessary for a given task?
- What can we use randomness for?

Brownian Circuits & Quantum Randomness

- Introduction & motivations
- k-designs
- Metrology
- Quantum Advantage



Classical Randomness

- Classical randomness is essential for modern information security!
- Cryptography: random numbers guarantee provable security
- Example: Key generation with cryptographically secure pseudorandom number generator (CSPRNGs)
  - “This is a message” —> “mnasdvlweriojweoi”
  - If there were correlations present in the bit stream, an eavesdropper could in principle use these correlations to decode part of the message

Katz, Lindell. CRC Press (2020).
Yao (SFCS 1982). IEEE (1982).
Rukhin, Soto, Nechvatal, et al. NIST (2001)

Quantum Randomness

- Random state $|\psi\rangle$ or random unitary U
- Example: Non-Malleable Quantum Encryption
  - Encode some quantum information via encoding unitary: $\overset{\text{Encoded info}}{|\psi'\rangle} = U\,\overset{\text{Quantum info}}{|\psi\rangle}$
  - Randomness (and entanglement) in $|\psi\rangle$ guarantees that an attacker can neither **learn** nor **modify** the encoded info

Ambainis, Bouda, Winter *J. Math. Phys.* 50, 042106 (2009)

- "Gold standard" = Haar-random unitary U
- Can we efficiently generate Haar-random unitaries?

(No, but we can get close! —> k-designs)

Gregory Bentsen

November 27, 2024

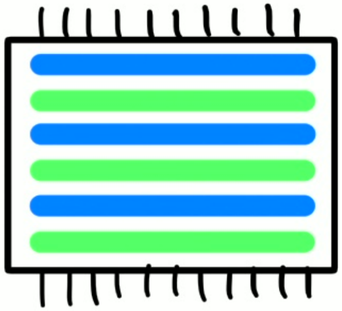
Applications of Quantum Randomness

- Cryptography
- Models of thermalization in many-body physics
- Classical shadows
- Quantum gravity and black holes
- Quantum advantage
- Metrology

Brownian Circuits

- What kinds of systems do we expect to rapidly generate randomness?
  - Fast Scramblers!
- Ingredients:
  - Highly chaotic
  - No spatial structure (avoid Lieb-Robinson bounds!)
  - Bonus: continuous time —> effective Hamiltonian
- Conceptual advantage: randomness <—> many-body physics

$U =$

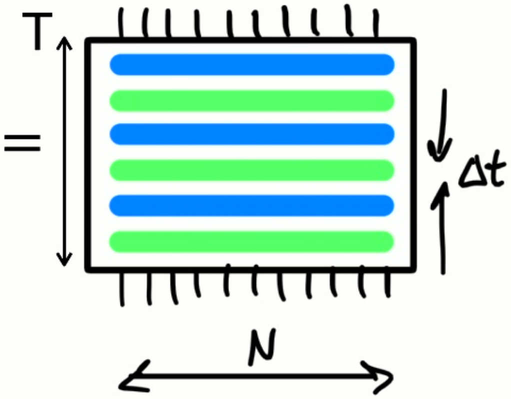


Gregory Bentsen

November 27, 2024

Brownian Circuits

- N spins $\vec{S}_i = S_i^\alpha$ $\quad i = 1, \ldots, N$, $\quad \alpha = x, y, z$

$U =$  $= \prod_t U_t$

- **2-body** Brownian interactions (all-to-all)
  - Spin squeezing in a random direction
  - Known fast scrambler, large-N control

$$U_t = \exp(-iH_t \Delta t)$$

$$H_t = \sum_{ij,\alpha\beta} J_{ij}^{\alpha\beta}(t)\ S_i^\alpha S_j^\beta$$

$J_{ij}^{\alpha\beta}(t) =$ Gaussian white noise

$$\mathbb{E}\left(J_{ij}^{\alpha\beta}(t)\right) = 0$$

$$\mathbb{E}\left(J_{ij}^{\alpha\beta}(t) J_{kl}^{\mu\nu}(t')\right) = \frac{J}{\Delta t N} \delta_{tt'} \delta_{ik} \delta_{jl} \delta^{\alpha\mu} \delta^{\beta\nu}$$

Lashkari, Stanford, et al. JHEP 22 (2013)
GSB, Sahu, Swingle, PRB 104, 094304 (2021)

Brownian Circuits

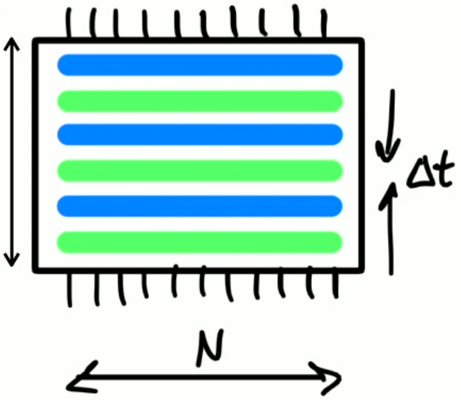
- Efficient generation of quantum randomness
- Analytical results (mean field theory)
- Access to higher moments of distribution
- Effective Hamiltonian H_{eff}

$$\mathbb{E}\left[\underbrace{U \otimes U^* \otimes U \otimes U^* \otimes \cdots}\right] = e^{-TH_{\text{eff}}}$$

k `Forward' copies

k `Backward' copies

$U =$



Gregory Bentsen

November 27, 2024

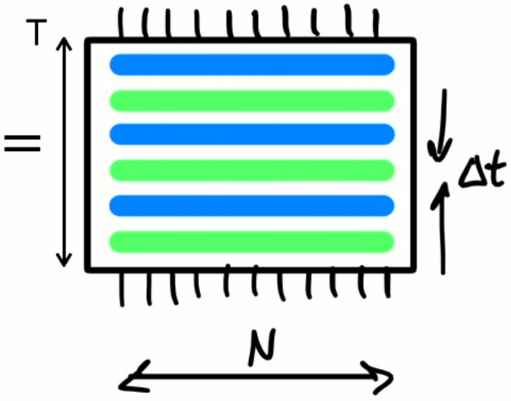
Brownian Circuits

- For fixed N, T, (with J scaled to 1), these circuits define an **ensemble** $U \in \mathscr{E}$, where we disorder average over the Brownian coefficients $J_{ij}^{\alpha\beta}(t)$

- We're interested in this ensemble as a function of time T and at large $N \to \infty$

- Other comments
  - All-to-all, but can also add spatial structure
  - No temporal structure: system is at infinite temperature
  - Focus on spins here, but can also do fermions

$U =$



(a selection of) Prior Work

- k-designs

Dankert (2005) quant-ph/0512217
Gross, Audenaert, Eisert (2007) J. Math. Phys. *48*(5)
Ambainis, Emerson (2007) *(CCC'07)* (pp. 129-140). IEEE.
Dankert, Cleve, Emerson, Livine (2009) PRA *80*(1), 012304
Roy, Scott (2009) Designs, codes and cryptography, 53, 13-31.
...

- Random unitary circuits

Emerson, Livine, Lloyd (2005) PRA *72*(6), 060302
Harrow, Low (2009) Comm. Math. Phys., 291, 257-302
Harrow, Low (2009) Int'l Workshop Approx. Algor. (pp. 548-561)
Brown, Viola (2010) PRL *104*(25), 250501
Brandão, Harrow, Horodecki (2016) Comm. Math. Phys., 346, 397-434
Nakata, Hirche, Koashi, Winter (2017) PRX *7*(2), 021006
Hunter-Jones (2019) arXiv:1905.12053
Haferkamp, Hunter-Jones (2021) PRA, 104(2), 022417
Haferkamp (2022) Quantum, 6, 795
Harrow, Mehraban (2023) Comm. Math. Phys., 401(2), 1531-1626.
...

- Clifford circuits

Kueng, Gross (2015) arXiv:1510.02767
Webb (2016) Quantum Info. and Comp. 16, 1379-1400
Haferkamp, et al (2023) Comm. Math. Phys., 397(3), 995-1041
...

- Connections to chaos & complexity

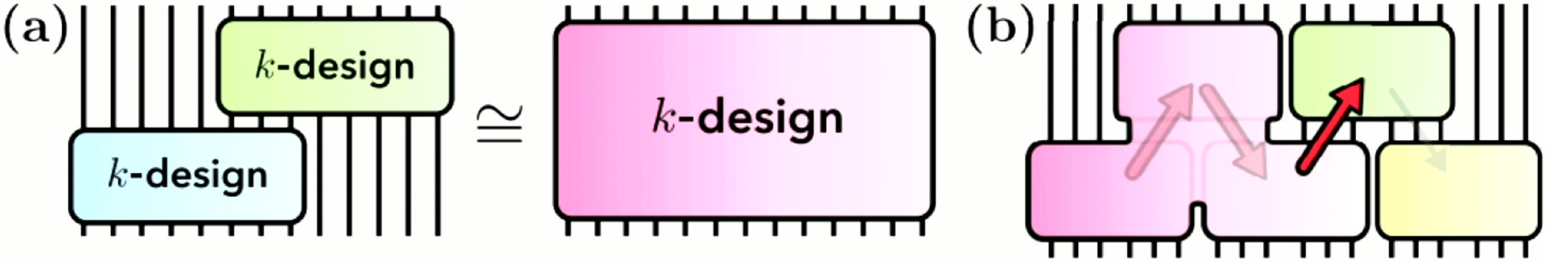
Roberts, Yoshida (2017) JHEP, 2017(4), 1-64.
Brandão, Chemissany, et al, (2021) PRX Quantum 2, 030316
...

- Pseudorandomness (poly-depth circuits)

Ji, Liu, Song (2018) Adv. Cryptology–CRYPTO 2018 Part III 38 (pp. 126-152)
...

(a selection of) Recent Work

- Chen, Bouland, Brandão et al (2024): k-designs in $O(k\ \mathrm{poly}(N))$ depth
- Chen, Haah, Haferkamp et al (2024): k-designs in $O(k\ N^2)$ depth
- Schuster, Haferkamp, Huang (2024): k-designs in $O(k\ \log N)$ depth (!)



Gregory Bentsen

November 27, 2024

Brownian Circuits & Quantum Randomness

- Introduction & motivations
- k-designs
- Metrology
- Quantum Advantage

Quantifying Randomness

- “Is $U \in \mathscr{E}$ distinguishable from a Haar-random?”
- Imagine a “spoof” challenge:
  - Alice tries to “spoof” Bob into thinking her Brownian circuit $U \in \mathscr{E}$ is actually a Haar-random unitary.
  - Bob’s task is to devise a test that can distinguish U from a Haar-random, using only k uses of the channel (plus ancillae)

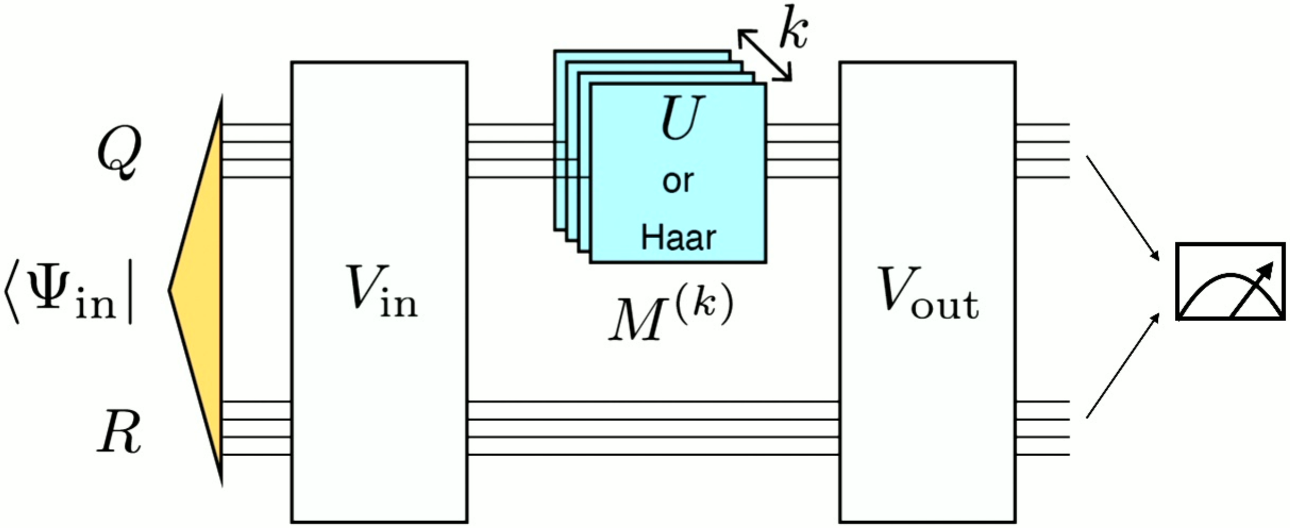
Gregory Bentsen

November 27, 2024

Quantifying Randomness

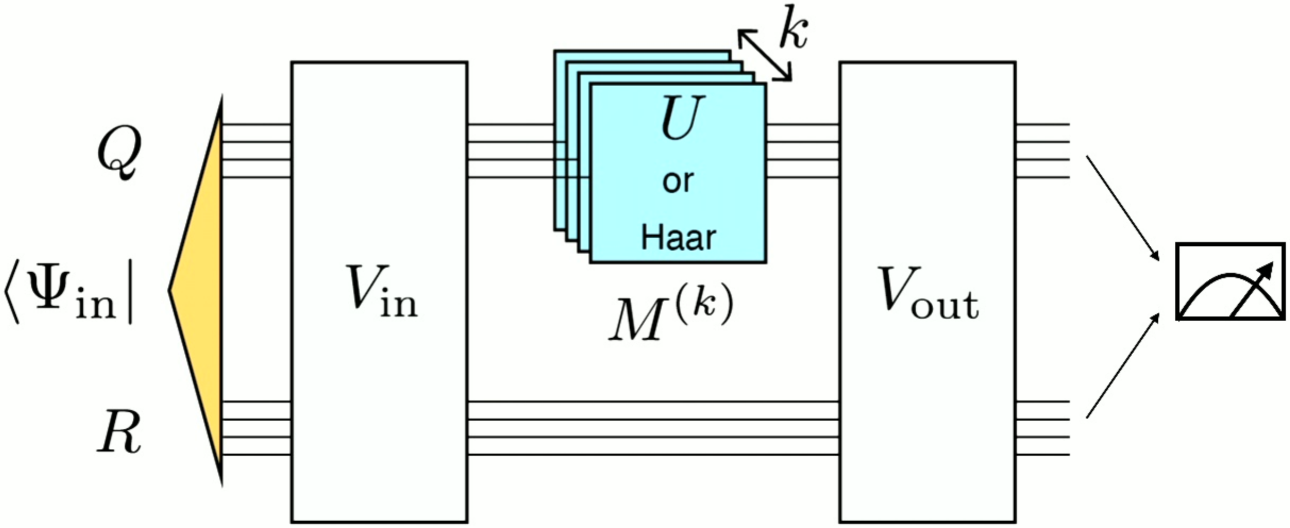
Roberts, Yoshida, JHEP 2017, 121 (2017)
Hunter-Jones, 1905.12053
Brandão, et al, PRX Quantum 2, 030316 (2021)

- Bob's ability to distinguish is captured by the Diamond Norm
  - kth moment map: $M^{(k)}_{\mathscr{E}}(X) \equiv \mathbb{E}\left[U^{\otimes k}\, X\, (U^{\dagger})^{\otimes k}\right]$
  - Diamond Norm: $\|M^{(k)}_{\mathscr{E}} - M^{(k)}_{\text{Haar}}\|_{\diamond}$ ← Bounds single-shot distinguishability



Quantifying Randomness

- Intuition: optimal “bias signal” to detect variations from Haar-random
- Any channel that passes the “spoof” test up to some k is called a **k-design**
- k-designs suffice for many realistic tasks! (e.g. 2-design for non-malleable encryption)



Frame Potential (FP) $F^{(k)}$

- Diamond Norm is the right information-theoretic quantity, but is unwieldy
- Instead, use simpler tool for calculations: Frame Potential
  - $F^{(k)} \equiv \mathbb{E}_{U,V} \left| \mathrm{Tr}\left[V^\dagger U\right] \right|^{2k}$ ⟵ Overlap of two different unitaries from the ensemble $\mathscr{E}$
- Key property: FP bounds the Diamond Norm
  - $\| M^{(k)}_{\mathscr{E}} - M^{(k)}_{\mathrm{Haar}} \|^2_\diamond \leq D^{2k} \left(F^{(k)} - F^{(k)}_{\mathrm{Haar}} \right)$ $\qquad D = 2^N$

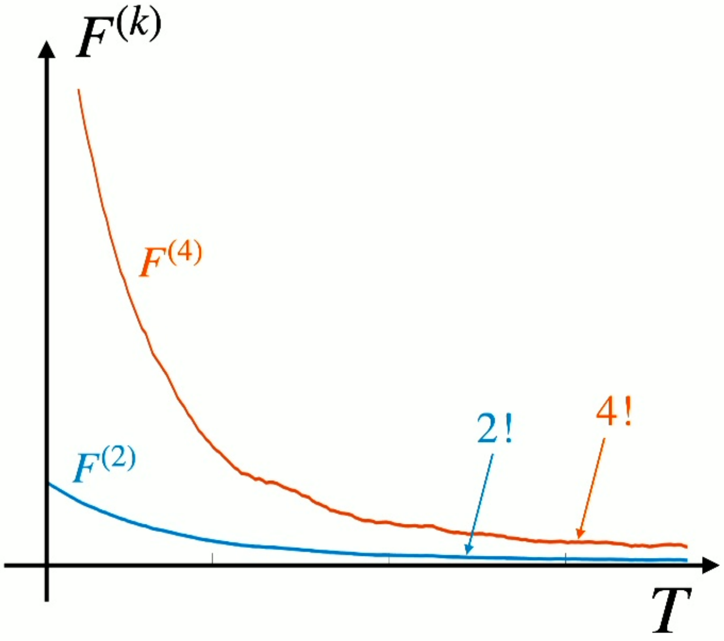
$$F^{(k)} \geq F^{(k)}_{\mathrm{Haar}} = k!$$

Gregory Bentsen

November 27, 2024

Frame Potential (FP) $F^{(k)}$

- **Main point: smallness of FP directly measures a channel's randomness**
  - FP measures closeness to Haar-random
  - $F^{(k)} \geq F^{(k)}_{\text{Haar}} = k!$
- In the following, I will show that Brownian circuits achieve $F^{(k)} \to k!$ in linear time $T \sim kN$



Gregory Bentsen

Jian, GSB, Swingle, *J. High Energ. Phys.* 2023, 190 (2023)

November 27, 2024

Calculation of FP for Brownian Circuits

$$F^{(k)} \sim \operatorname{Tr} \mathbb{E}\left[U^{\otimes k} \otimes (U^*)^{\otimes k}\right]$$

$2kN$ spins $\vec{S}_{ri} = S^{\alpha}_{ri}$

replica index

site index

$i = 1,\ldots,N$

$r = 1,\ldots,2k$

$\alpha = x, y, z$

r = 1 2 3 4

$$k = 2 \qquad \mathbb{E}\left[U \otimes U^* \otimes U \otimes U^*\right]$$

$$\mathbb{E}\left(1 - iJ^{\alpha\beta}_{ij} S^{\alpha}_{1i} S^{\beta}_{1j} \Delta t\right)\left(1 + iJ^{\mu\nu}_{kl} S^{\mu}_{2k} S^{\nu}_{2l} \Delta t\right)(\cdots)_3(\cdots)_4$$

$$1 + \frac{J}{N}\left(S_{1i} \cdot S_{2i}\right)^2 \Delta t - \frac{J}{N}\left(S_{1i} \cdot S_{3i}\right)^2 \Delta t + \cdots$$

$$e^{-H_{\text{eff}}\Delta t}$$

$$H_{\text{eff}} \equiv \frac{J}{2N} \sum_{r<s} (-1)^{r+s} \left(\sum_i \vec{S}_{ri} \cdot \vec{S}_{si} \right)^2$$

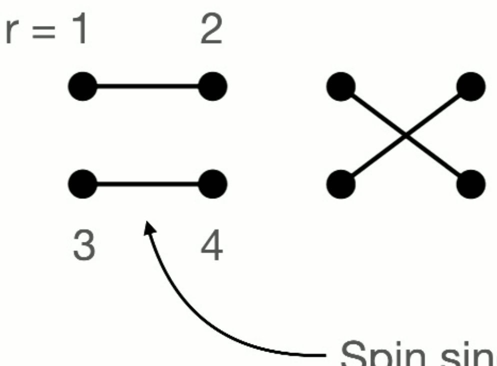
Gibbs weight in partition function

$$\mathbb{E}\left(J^{\alpha\beta}_{ij}(t)\right) = 0$$

$$\mathbb{E}\left(J^{\alpha\beta}_{ij}(t) J^{\mu\nu}_{kl}(t')\right) = \frac{J}{\Delta t N} \delta_{tt'} \delta_{ik} \delta_{jl} \delta^{\alpha\mu} \delta^{\beta\nu}$$

Calculation of FP for Brownian Circuits

- Large-N limit: mean-field theory $H_{\text{eff}} \equiv \frac{J}{2N} \sum_{r<s} (-1)^{r+s} \left(\sum_i \vec{S}_{ri} \cdot \vec{S}_{si} \right)^2$
  - Minimize mean-field energy $E = \frac{JN}{2} \sum_{r<s} (-1)^{r+s} G_{rs}^2$ $\quad G_{rs} = \frac{1}{N} \sum_i \langle \vec{S}_{ri} \cdot \vec{S}_{si} \rangle$
- $k = 2$
  - 2 ground states



Spin singlets $G_{rs} = -3/4$

Calculation of FP for Brownian Circuits

$$F^{(k)} \sim \mathrm{Tr}\,\mathbb{E}\left[U^{\otimes k} \otimes (U^{*})^{\otimes k}\right]$$

$2kN$ spins $\vec{S}_{ri} = S^{\alpha}_{ri}$

replica index

site index

$$i = 1,\ldots,N$$
$$r = 1,\ldots,2k$$
$$\alpha = x, y, z$$

r = 1 2 3 4

$$k = 2 \qquad \mathbb{E}\left[U \otimes U^{*} \otimes U \otimes U^{*}\right]$$

$$\mathbb{E}\left(1 - iJ^{\alpha\beta}_{ij} S^{\alpha}_{1i} S^{\beta}_{1j} \Delta t\right)\left(1 + iJ^{\mu\nu}_{kl} S^{\mu}_{2k} S^{\nu}_{2l} \Delta t\right)(\cdots)_3(\cdots)_4$$

$$1 + \frac{J}{N}\left(S_{1i} \cdot S_{2i}\right)^2 \Delta t - \frac{J}{N}\left(S_{1i} \cdot S_{3i}\right)^2 \Delta t + \cdots$$

$$e^{-H_{\mathrm{eff}}\Delta t}$$

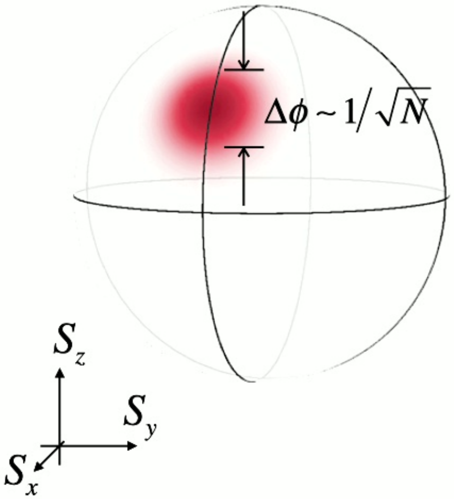
Gibbs weight in partition function

$$\mathbb{E}\left(J^{\alpha\beta}_{ij}(t)\right) = 0$$

$$\mathbb{E}\left(J^{\alpha\beta}_{ij}(t) J^{\mu\nu}_{kl}(t')\right) = \frac{J}{\Delta t N}\delta_{tt'}\delta_{ik}\delta_{jl}\delta^{\alpha\mu}\delta^{\beta\nu}$$

Limits on Precision Measurement

Coherent Spin State (CSS)



Phase sensitivity:

$$\Delta\phi \sim 1/\sqrt{N}$$

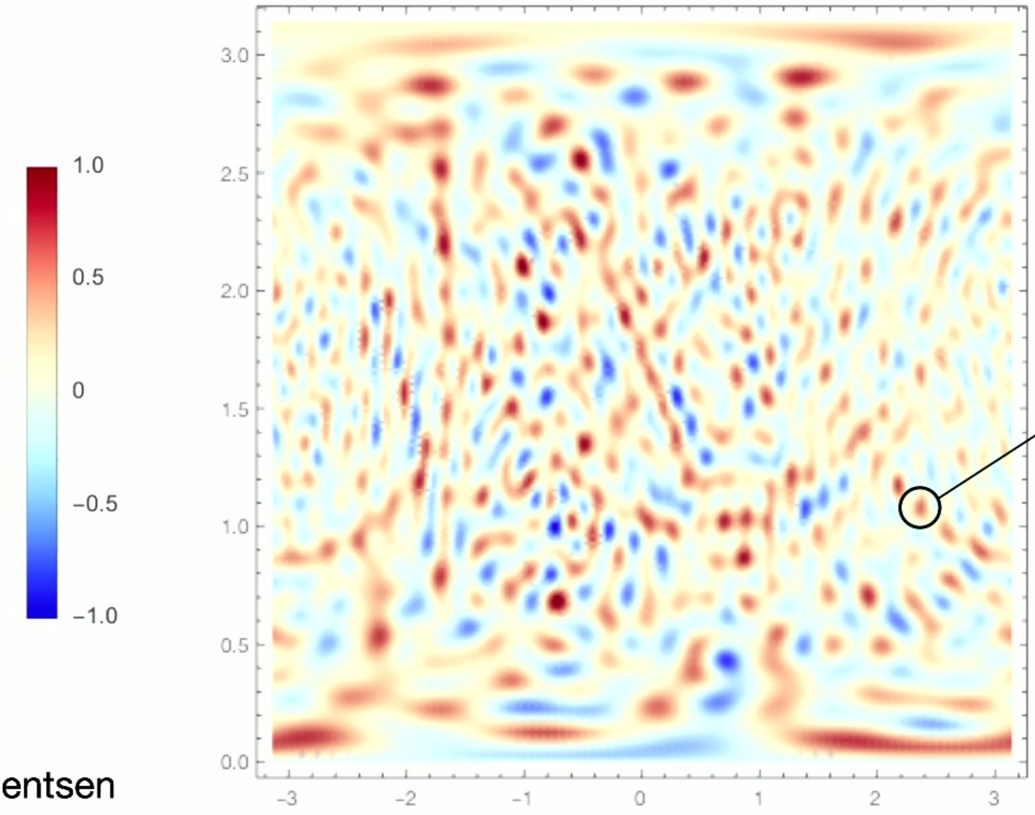
Standard Quantum Limit (SQL)

“The best you can do with N *uncorrelated* particles”

Gregory Bentsen

November 27, 2024

Random Quantum States for Metrology



Features scale like 1/N

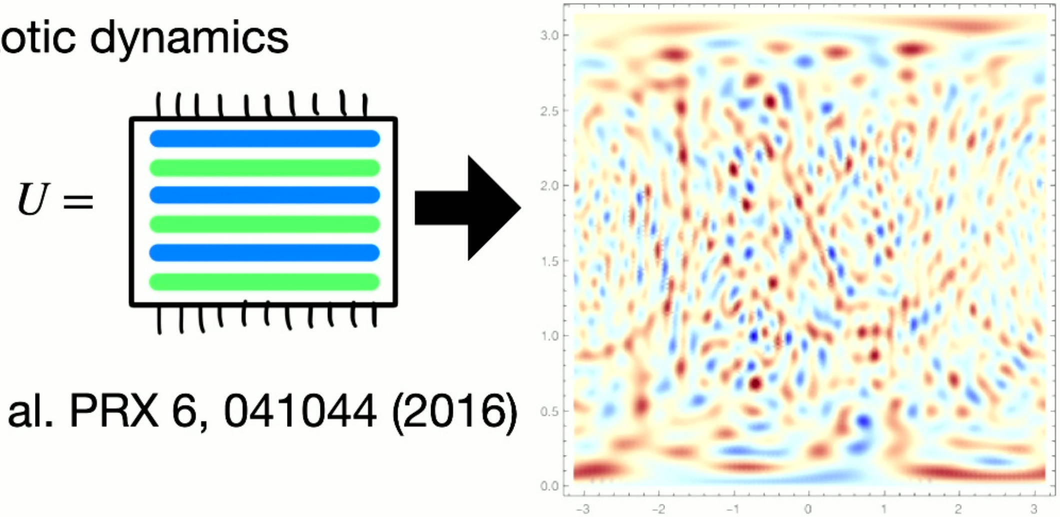
Can we use these states for Heisenberg-limited metrology?

Gregory Bentsen

November 27, 2024

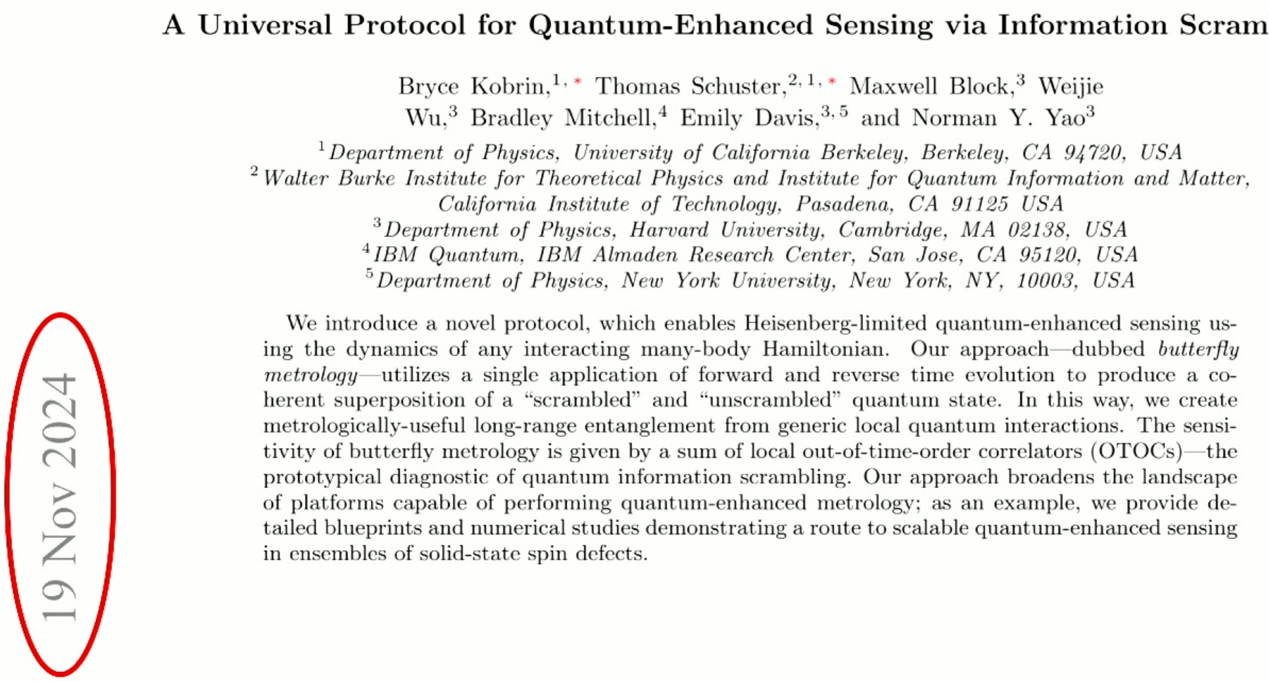
Random Quantum States for Metrology

- Can generate these states using chaotic dynamics
  - Kicked top
  - Brownian circuits



- Prior work:
  - Oszmaniec, Augusiak, Gogolin, et al. PRX 6, 041044 (2016)
  - Shi, Smerzi, Pezzè 2407.11822
  - Showed that QFI ~ N^2 (Heisenberg scaling)
  - But only for random states in the *symmetric* (Dicke) subspace

(Very!) Recent Work



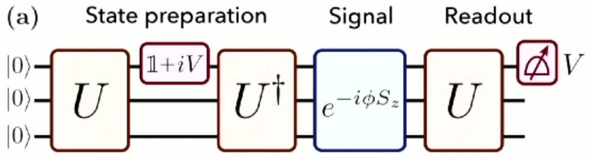
19 Nov 2024

A Universal Protocol for Quantum-Enhanced Sensing via Information Scrambling

Bryce Kobrin,[1,*] Thomas Schuster,[2,1,*] Maxwell Block,[3] Weijie Wu,[3] Bradley Mitchell,[4] Emily Davis,[3,5] and Norman Y. Yao[3]

[1] *Department of Physics, University of California Berkeley, Berkeley, CA 94720, USA*
[2] *Walter Burke Institute for Theoretical Physics and Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125 USA*
[3] *Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[4] *IBM Quantum, IBM Almaden Research Center, San Jose, CA 95120, USA*
[5] *Department of Physics, New York University, New York, NY, 10003, USA*

We introduce a novel protocol, which enables Heisenberg-limited quantum-enhanced sensing using the dynamics of any interacting many-body Hamiltonian. Our approach—dubbed *butterfly metrology*—utilizes a single application of forward and reverse time evolution to produce a coherent superposition of a "scrambled" and "unscrambled" quantum state. In this way, we create metrologically-useful long-range entanglement from generic local quantum interactions. The sensitivity of butterfly metrology is given by a sum of local out-of-time-order correlators (OTOCs)—the prototypical diagnostic of quantum information scrambling. Our approach broadens the landscape of platforms capable of performing quantum-enhanced metrology; as an example, we provide detailed blueprints and numerical studies demonstrating a route to scalable quantum-enhanced sensing in ensembles of solid-state spin defects.



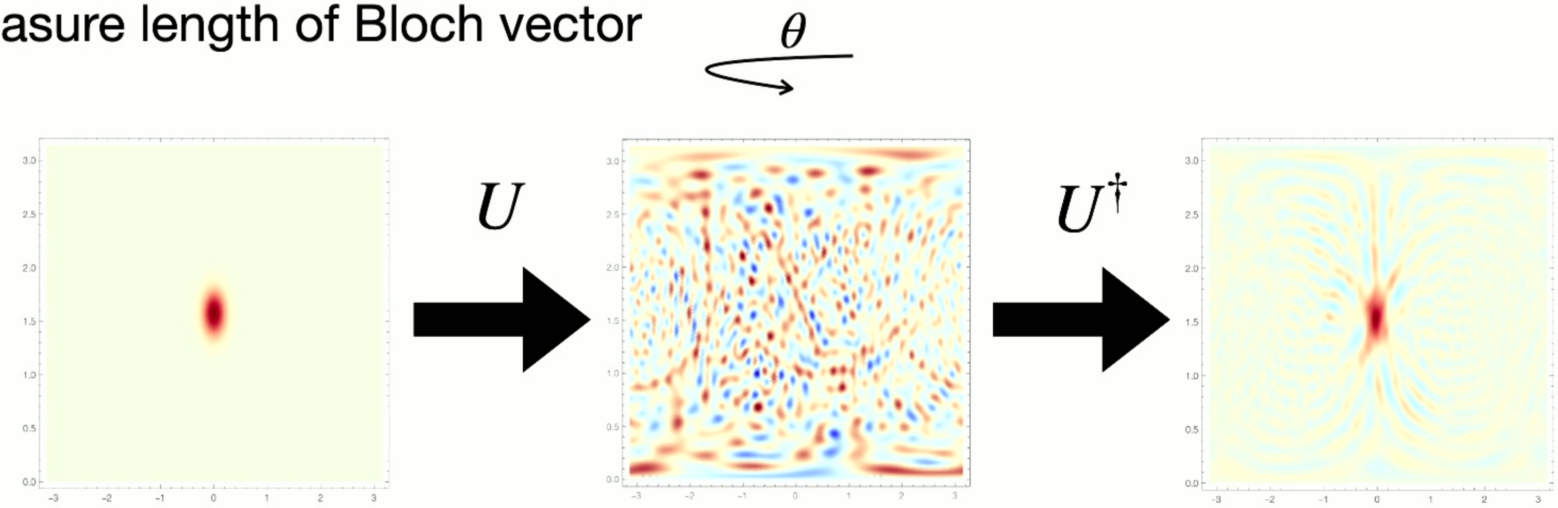
Gregory Bentsen

November 27, 2024

Time-Reversal Protocol

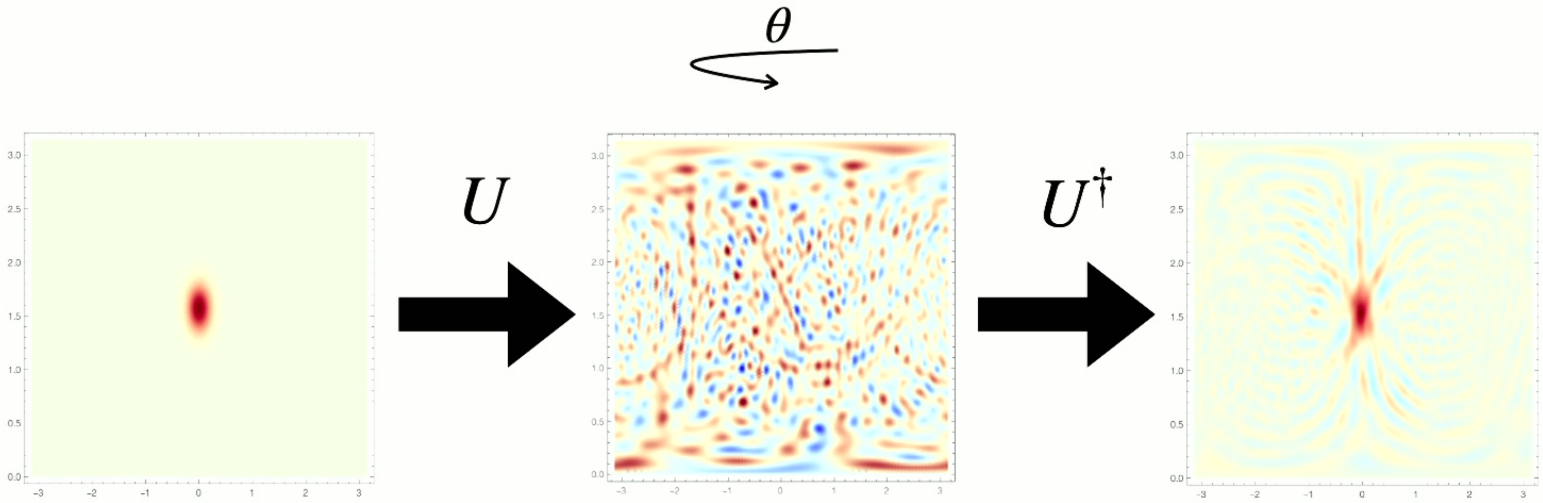
w.i.p. with Vuletic, Gorshkov, Swingle, Zaporski, et al.

- Prepare metrological state via random U
- Rotate by unknown angle θ
- Time-reverse $U^\dagger$
- Measure length of Bloch vector

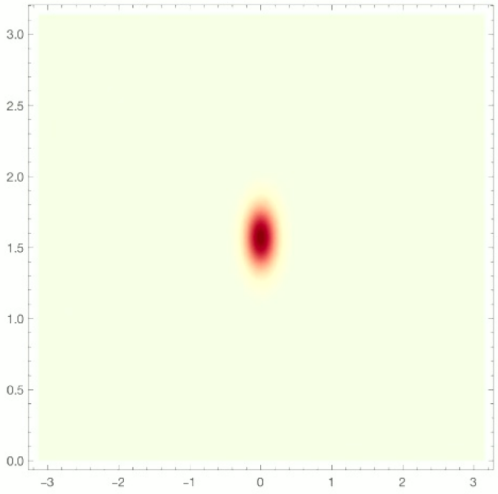


Time-Reversal Protocol

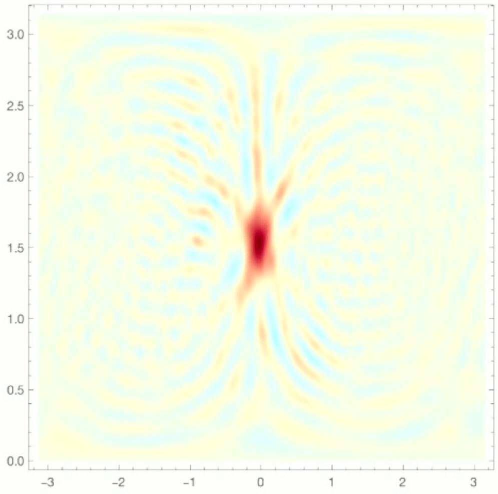
- For $\theta = 0$, get back CSS with maximal Bloch vector
- For $\theta \neq 0$, get back another random state, with minimal Bloch vector
- So Bloch vector length is a proxy for the rotation angle θ



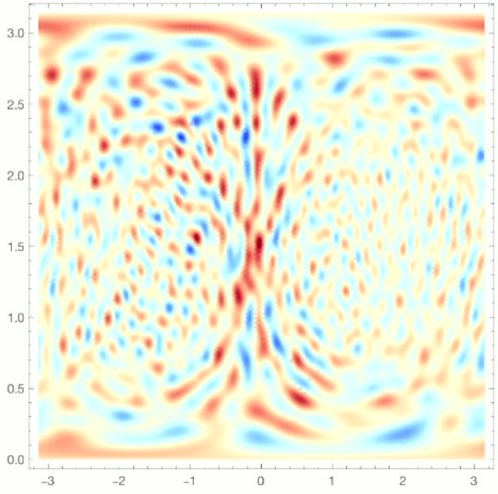
Time-Reversal Protocol



$\theta = 0$



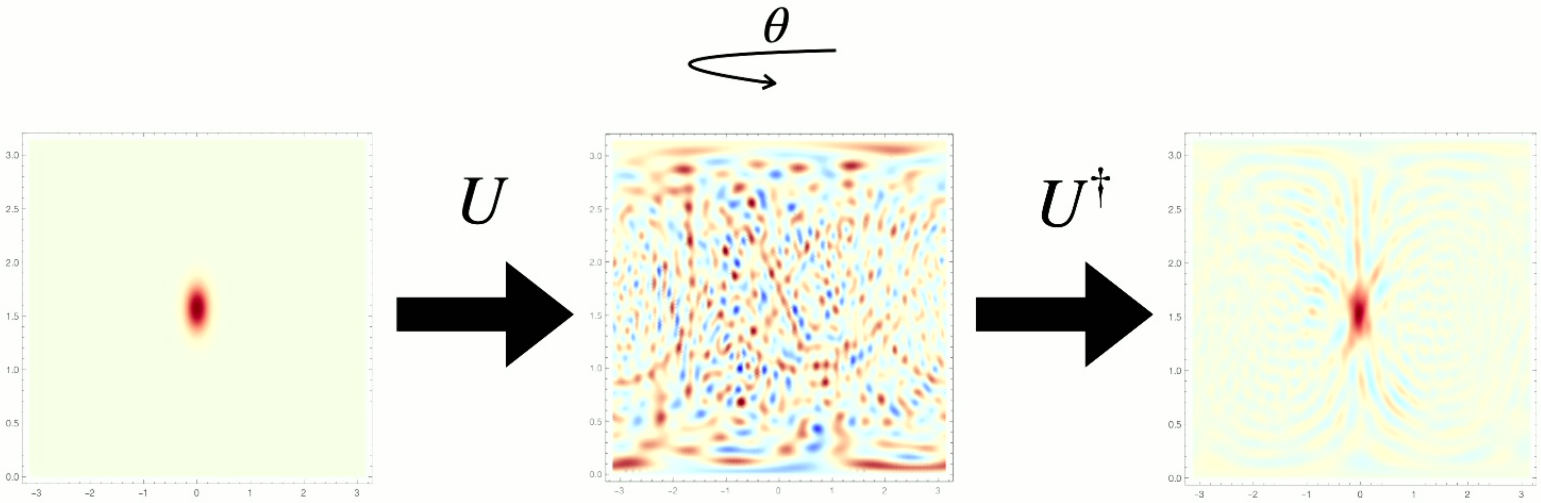
$\theta = 0.05$



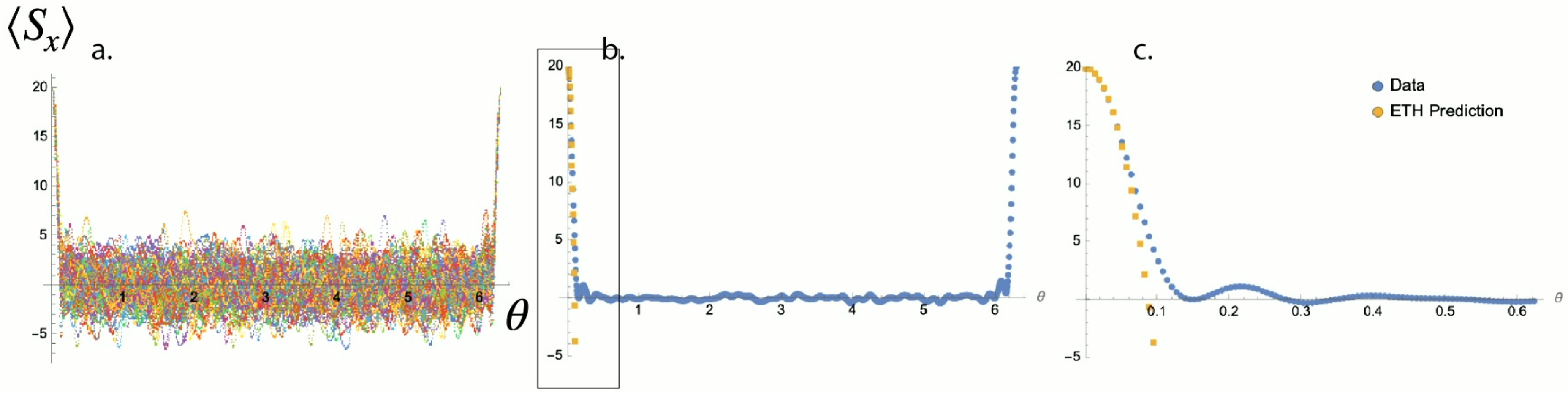
$\theta = 0.1$

Time-Reversal Protocol

- For $\theta = 0$, get back CSS with maximal Bloch vector
- For $\theta \neq 0$, get back another random state, with minimal Bloch vector
- So Bloch vector length is a proxy for the rotation angle θ



Time-Reversal Protocol



$S = 20$

Gregory Bentsen

November 27, 2024

Time-Reversal Protocol

- Heisenberg-limited precision
- Signal-to-noise: $\dfrac{\langle S_x \rangle - S}{\Delta S_x} \sim -N\theta$
- Rotation can be around an *arbitrary* axis $\hat{n}$
- Analytical arguments using eigenstate thermalization hypothesis (ETH)

$$\langle \overline{m} \,|\, A \,|\, \overline{n} \rangle = \overline{A}\delta_{mn} + \sqrt{\frac{\overline{A^2}}{D}} R_{mn}$$

$$\overline{A} = \frac{1}{D}\sum_i A_i$$

Time-Reversal Protocol

- Outlook & open questions
  - How does dissipation affect the time-reversal protocol?
    - Collective decay
    - Single-atom decay / dephasing
  - Can we realistically implement this in a cavity QED system?
    - How much time-evolution is needed?
    - Preliminary: Kicked top OAT with k = 6, T = 4 kicks
    - Need Wigner function to wrap around Bloch sphere

w.i.p. with Vuletic, Gorshkov, Swingle, Zaporski, et al.

$$e^{-ik/(2S+1)S_z^2}$$

Gregory Bentsen

November 27, 2024

Time-Reversal Protocol

- Outlook & open questions
    - How does dissipation affect the time-reversal protocol?
        - Collective decay
        - Single-atom decay / dephasing
    - Can we realistically implement this in a cavity QED system?
        - How much time-evolution is needed?
        - Preliminary: Kicked top OAT with k = 6, T = 4 kicks
        - Need Wigner function to wrap around Bloch sphere

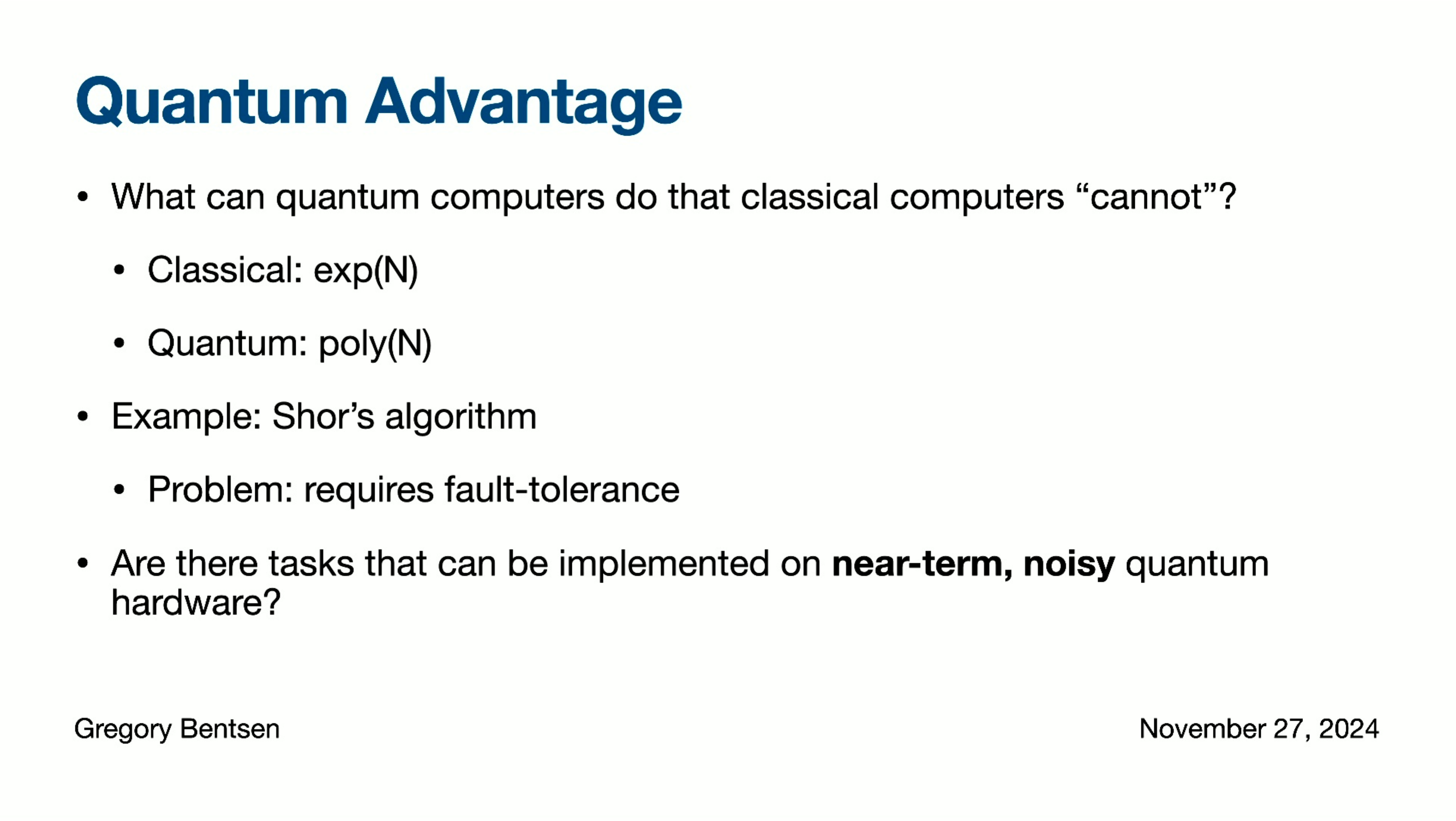
w.i.p. with Vuletic, Gorshkov, Swingle, Zaporski, et al.

$$e^{-ik/(2S+1)S_z^2}$$

Quantum Advantage

- What can quantum computers do that classical computers “cannot”?
  - Classical: exp(N)
  - Quantum: poly(N)
- Example: Shor’s algorithm
  - Problem: requires fault-tolerance
- Are there tasks that can be implemented on **near-term, noisy** quantum hardware?

Gregory Bentsen November 27, 2024

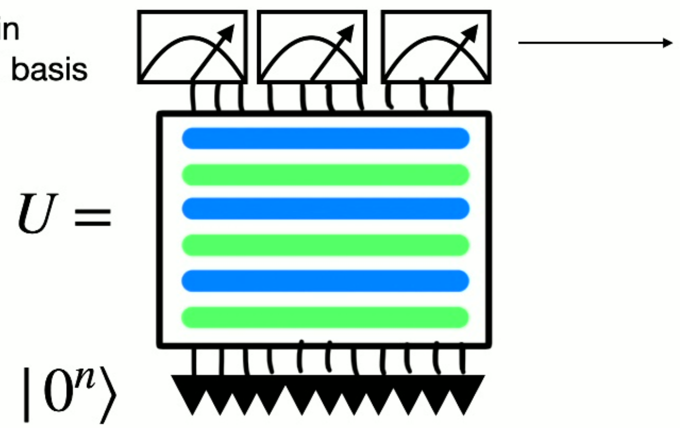


Quantum Advantage

- What can quantum computers do that classical computers “cannot”?
  - Classical: exp(N)
  - Quantum: poly(N)
- Example: Shor’s algorithm
  - Problem: requires fault-tolerance
- Are there tasks that can be implemented on **near-term, noisy** quantum hardware?

Random Circuit Sampling

- Sample from output distribution of random circuits
- Bit-string distribution $p_U(x) = |\langle x | U | 0 \rangle|^2$
- Sampling from this distribution is believed to be classically #P hard
  - (Polynomial hierarchy collapses if there exist efficient classical samplers)



Measure in
computational basis

$U =$

$|0^n\rangle$

Bit-string x,
prob $p_U(x)$

Boixo, et al. Nature Physics, 14(6), 595-600. (2018)
Arute, et al. Nature 574, 505–510 (2019)

Gregory Bentsen

November 27, 2024

Spoofing the XEB

- Does XEB actually certify quantum advantage?
- Put another way: does every efficient classical spoofing algorithm necessarily achieve a low XEB score?
- The answer appears to be “no”
  - Gao et al: disjoint circuits (“Harvard algorithm”)
  - Aharonov et al: Pauli paths

Gao, Kalinowski, Chou, et al. PRX Quantum **5**, 010334 (2024)

Aharonov, Gao, Landau, et al. ACM STOC (2023)

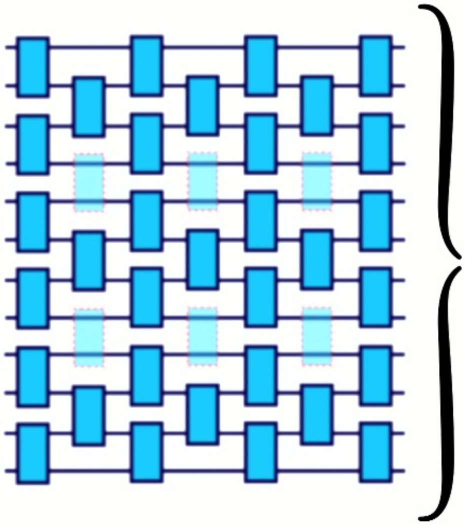
Gregory Bentsen

November 27, 2024

Spoofing the XEB

Gao, Kalinowski, Chou, et al. PRX Quantum **5**, 010334 (2024)

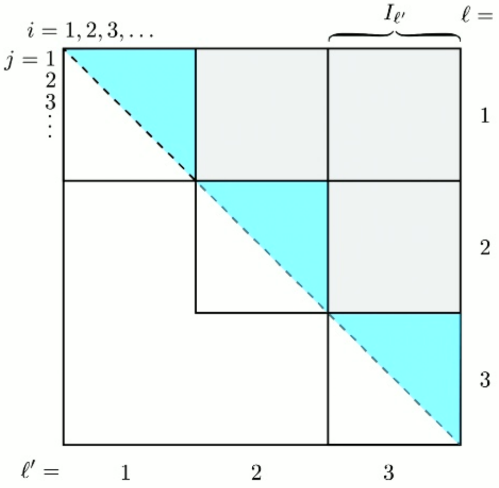
- Does XEB actually certify quantum advantage?
- Gao et al: disjoint circuits ("Harvard algorithm")
- Achieves "high" XEB scores ("5–12% of those obtained in the state-of-the-art experiments, within just a few seconds using a single GPU machine")



M disjoint subsystems

Spoofing the XEB

- What about all-to-all circuits?
- Our results: for all-to-all circuits, Gao et al achieves high XEB on **average**, but **fluctuations** are large, scaling exponentially with number of subsystems M
- So the “Harvard algorithm” is **not a reliable method for spoofing XEB in the all-to-all case**



$$M = N/\log N$$

Disjoint subsystems

GSB, Fefferman, Gullans, Ghosh, Liu
arXiv:2411.04169

Gregory Bentsen

November 27, 2024

XEB for Brownian All-to-All Circuits

Ideal all-to-all circuit

XEB Fluctuations $$\sum_x \mathbb{E}[p^2(x)q^2(x)] = \frac{2^{1+M}}{2^{4N}}\left[\left(1-e^{-12JT}\right)^4 + \left(1+e^{-12JT}\right)^4\right]^N$$

Disjoint circuit

$$\Big\Downarrow$$

Exponential growth of fluctuations

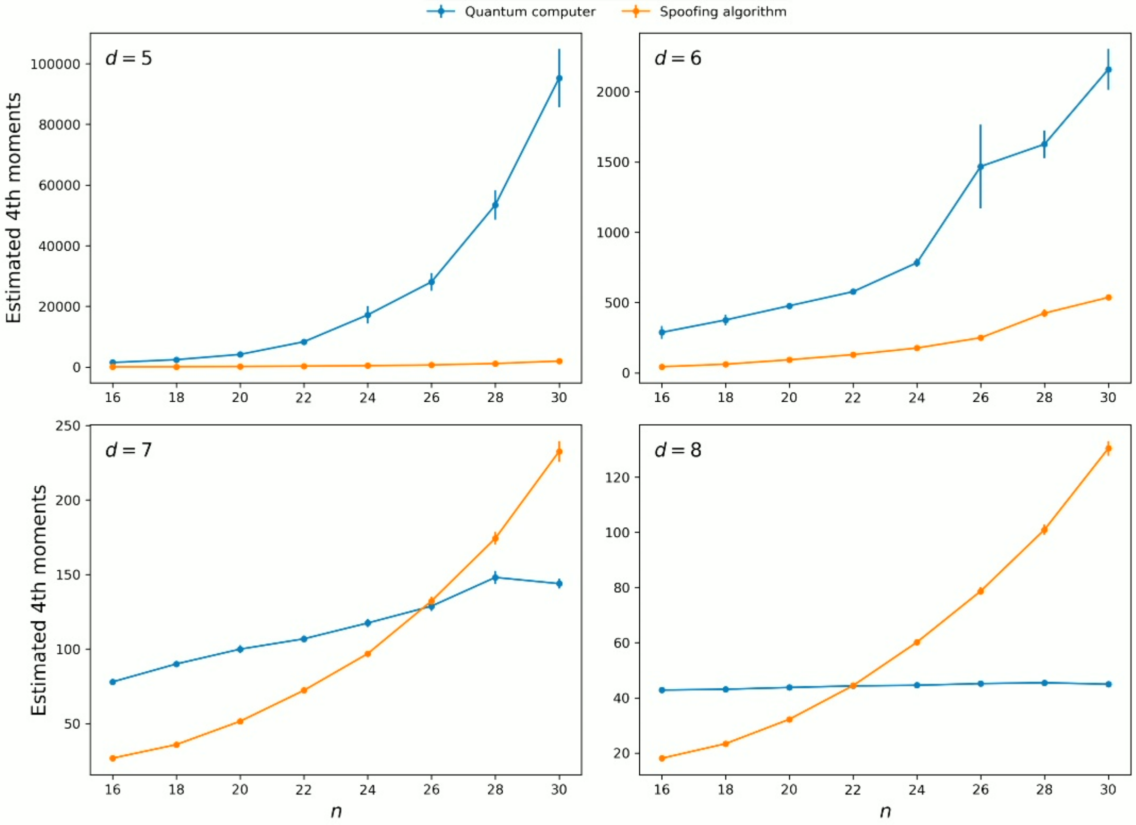
$$\mathrm{VarXEB}(p,q) \sim \frac{2^{1+M}}{2^{4N}}$$

GSB, Fefferman, Gullans, Ghosh, Liu arXiv:2411.04169

Gregory Bentsen

November 27, 2024

Numerical Results



$$M = N/\log N$$

Disjoint subsystems

Gregory Bentsen

November 27, 2024

Outlook

- Can we draw precise connections between Brownian circuits and discrete random circuits?
- Is XEB robust against other types of spoofing algorithms, especially for all-to-all circuits?
- Connections to complexity theory: can we prove hardness of sampling from Brownian circuits?

Gregory Bentsen

November 27, 2024

Acknowledgments

Brian Swingle
Shao-Kai Jian
Subhayan Sahu

Michael Gullans
Bill Fefferman
Soumik Ghosh
Calvin Liu

Vladan Vuletic
Alexey Gorshkov
Leon Zaporski
Ron Belyansky
Jacob Bringewatt

MINERVA® UNIVERSITY

WILLIAM & MARY
CHARTERED 1693

Brandeis
TRUTH · EVEN UNTO ITS INNERMOST PARTS
אמת

U.S. DEPARTMENT OF ENERGY
Office of Science

GeoFlow Collaboration