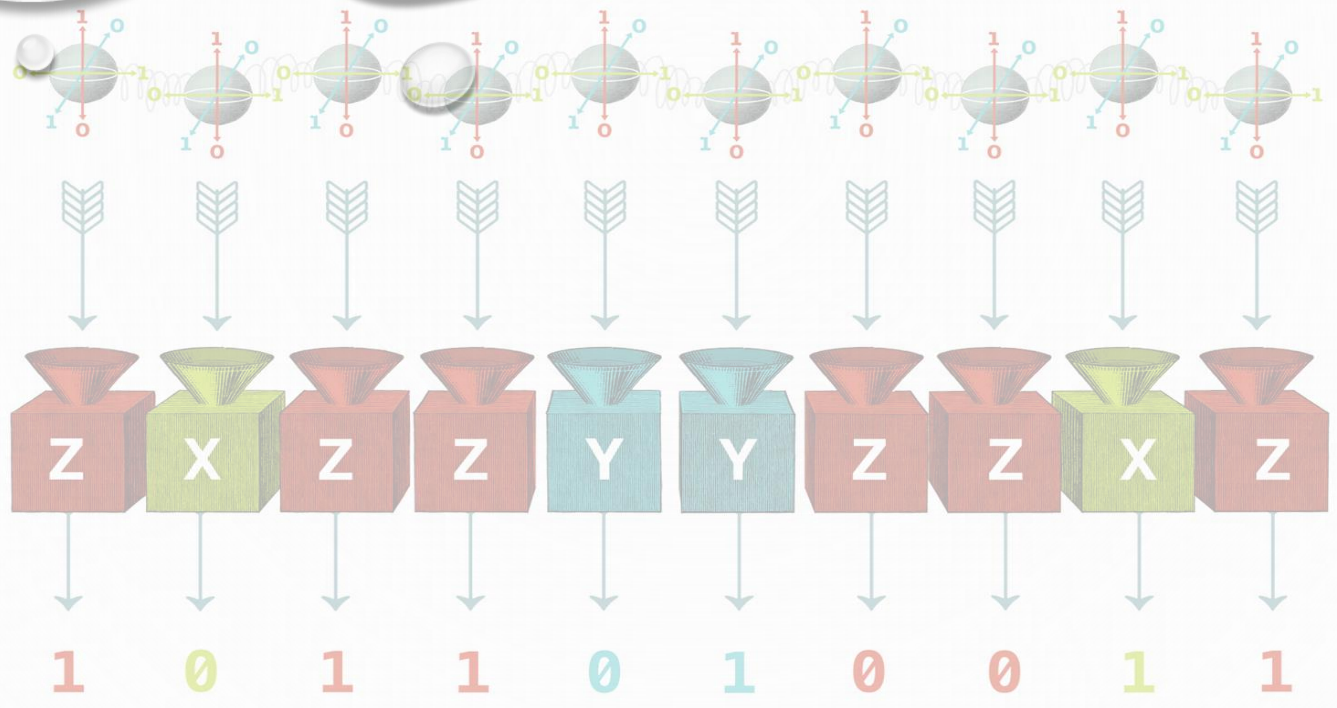


VERIFICATION OF QUANTUM TECHNOLOGIES

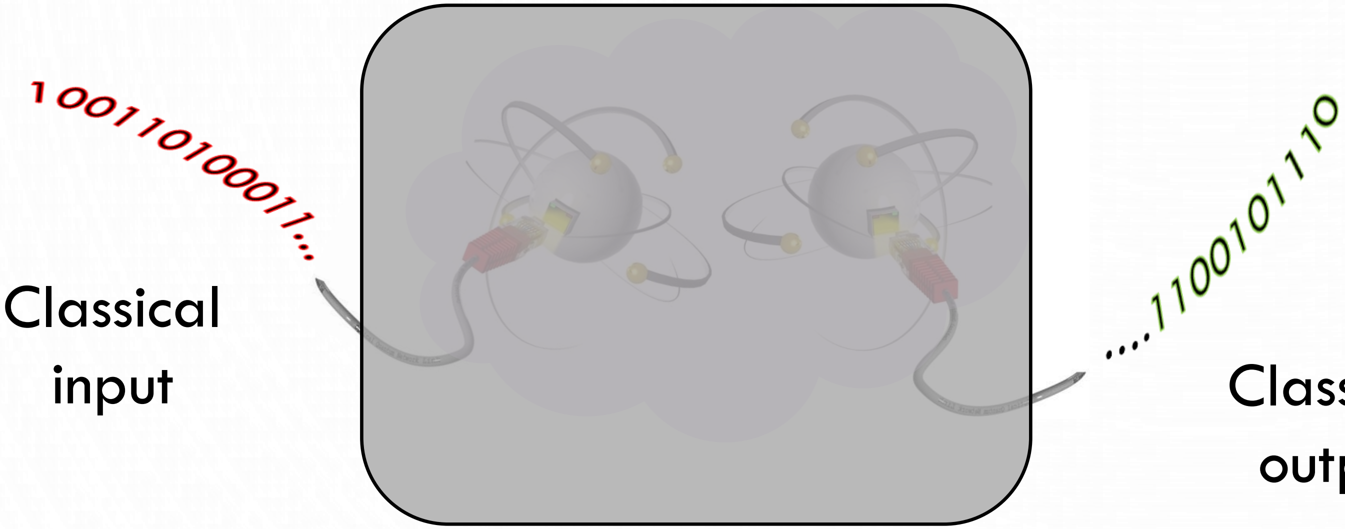
BORIVOJE DAKIĆ

UNIVERSITY OF VIENNA

BPU11 Congress, Belgrade, 28 August - 1 September, 2022, Serbia

QUANTUM TECHNOLOGY

QUANTUM INFORMATION PROCESSING



Classical input

Classical output

Coherent (quantum) processing

APPLICATIONS

- ❑ QUANTUM COMMUNICATION
- ❑ QUANTUM COMPUTING
- ❑ QUANTUM SENSING & METROLOGY
- ❑ QUANTUM SIMULATIONS

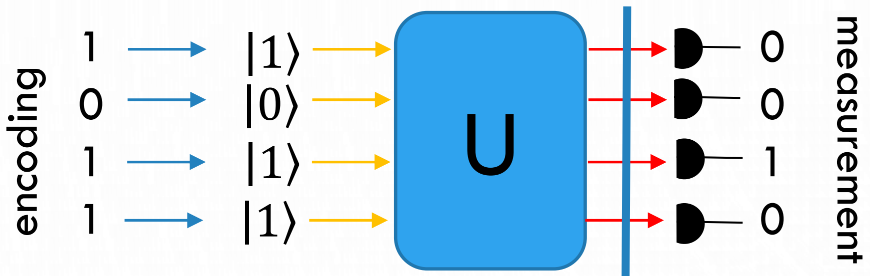
OUTPERFORM (BY ORDERS OF MAGNITUDE) STANDARD/CLASSICAL METHODS

Example of an exponential speed-up:

$$2^{59}\ s\ (\text{Age of Universe}) \rightarrow 59\ s$$

QUANTUM INFORMATION PROCESSING

Quantum circuit



Maths

$$P_{0010\ldots} = |\langle 0010\ldots|U|1011\ldots\rangle|^2$$

Appear Randomly (Born rule)

(potential) output

$2^n \times 2^n$ unitary matrix

input

Where does the speed-up come from?

Standard narrative:

Output state

$$|\psi\rangle_{out} = U\,\big|1011\ldots\rangle = \sum_{i_1 i_2\ldots} c_{i_1 i_2\ldots}\,|i_1 i_2\ldots\rangle$$

$$c'_{i_1 i_2\ldots} = U^{j_1 j_2\ldots}_{i_1 i_2\ldots}\, c_{j_1 j_2\ldots}$$

$2^n \times 2^n$ unitary matrix

coherent processing in complex vector space of exp. dimension 2^n

Classical processing in space of exp. dimension:

$$p'_{i_1 i_2\ldots} = S^{j_1 j_2\ldots}_{i_1 i_2\ldots}\, p_{j_1 j_2\ldots}$$

QUANTUM MAGIC

- **<u>HISTORICAL NOTE:</u>**

- „OLD“ QUANTUM THEORY → ENSEMBLE OF SYSTEM (**<u>MEAN VALUES,</u>** COLLECTIVE OBSERVABLES)

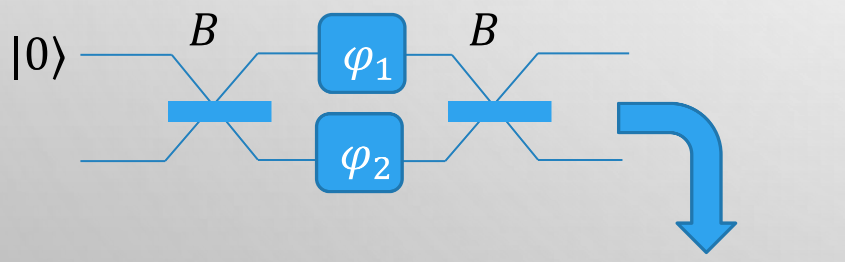
- „NEW“ QUANTUM THEORY → SINGLE SYSTEM (TRUE RANDOM **<u>INDIVIDUAL CLICKS</u>**)

- QI HAS DEEP ROOTS IN FOUNDATIONAL THINKING

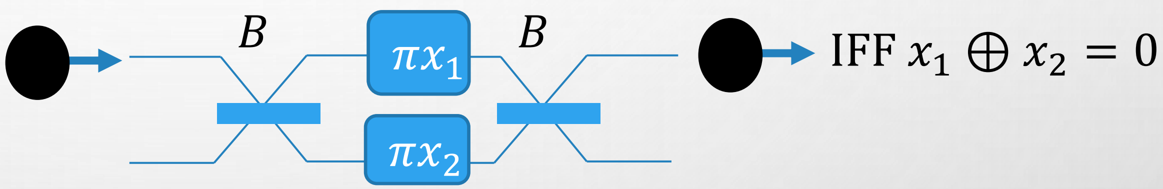
A) <u>Quantum superpositions</u>

Qubit: $\alpha|0\rangle + \beta|1\rangle$

Physical implementation:



$$\cos(\varphi_1 - \varphi_2)\,|0\rangle + \sin(\varphi_1 - \varphi_2)|1\rangle$$



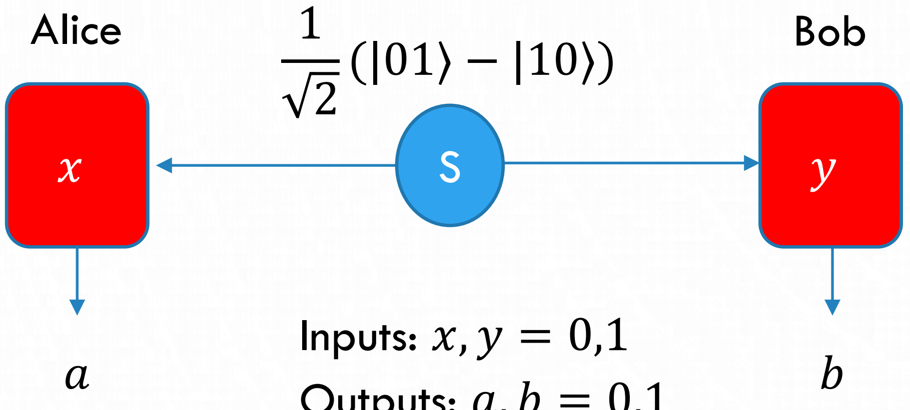
$x_1, x_2 = 0{,}1$

D. Deutsch, 1980s

<u>Many-worlds interpretation</u>:
There are 2 worlds needed in order perform this „non-local“ computation

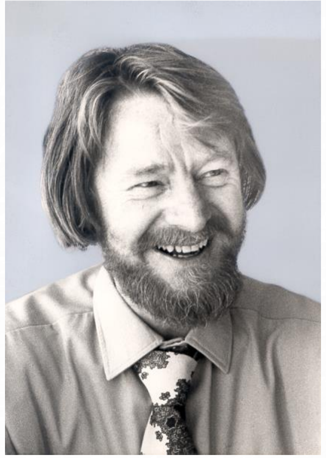
QUANTUM MAGIC

B) <u>**QUANTUM ENTANGLEMENT**</u> (CORRELATIONS)



Inputs: $x, y = 0,1$

Outputs: $a, b = 0,1$



J. Bell, 1960s

<u>**Quantum nonlocality**</u>:

$a \oplus b = xy$

<u>**Classical**</u>: $P_{win} = 75\%$

<u>**Quantum**</u>: $P_{win} \approx 85\%$

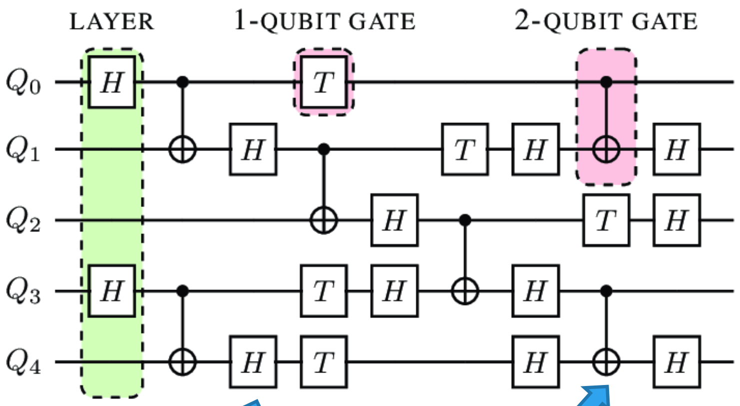
IFF entanglement is present

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

<u>Combination of</u>

A) Quantum superpositions

B) Quantum entanglement



superposition

entanglement

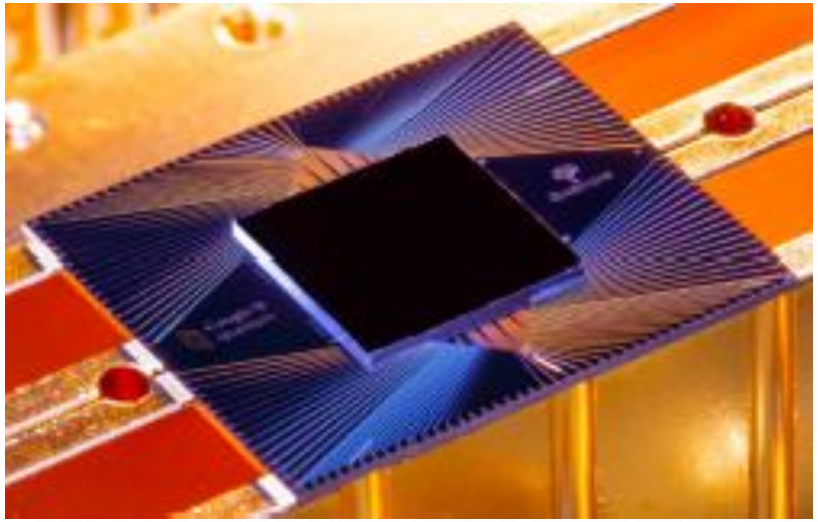
Exponential speed-ups!

QUANTUM ROADMAP

…	1980	1990	2000	2010	2020	…. ? …
Quantum Foundations →	First theoretical concepts/control of ind. systems	Complete theory	Proof-of-concept demonstrtions	Serious investments (Google, IBM, National flagships)	Quantum computational supremacy	Fully fledged quantum computer

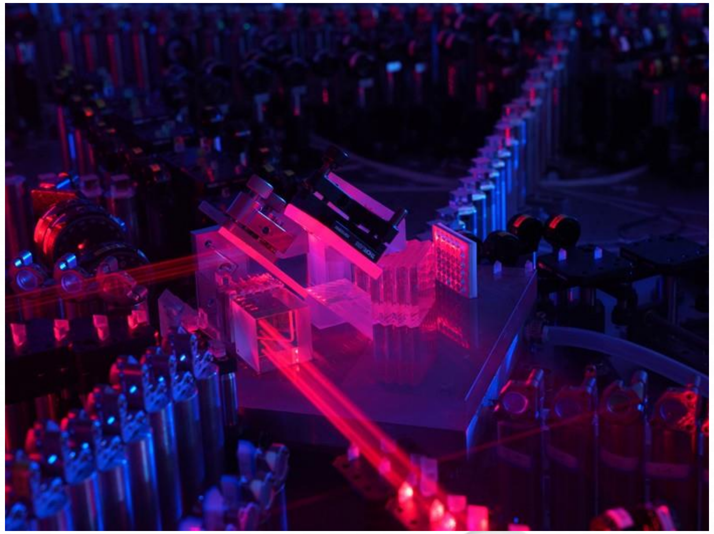
Most important milestone!

Google AI



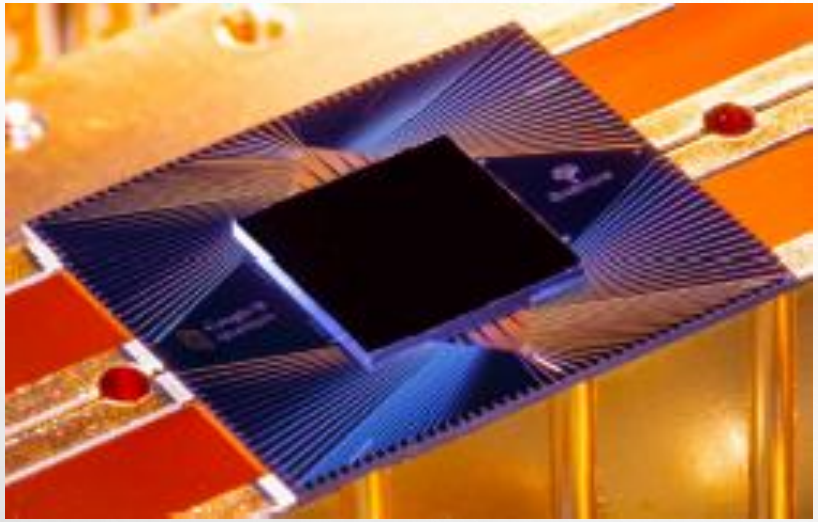
54 qubits, the Sycamore processor, Nature 2019.

China NL

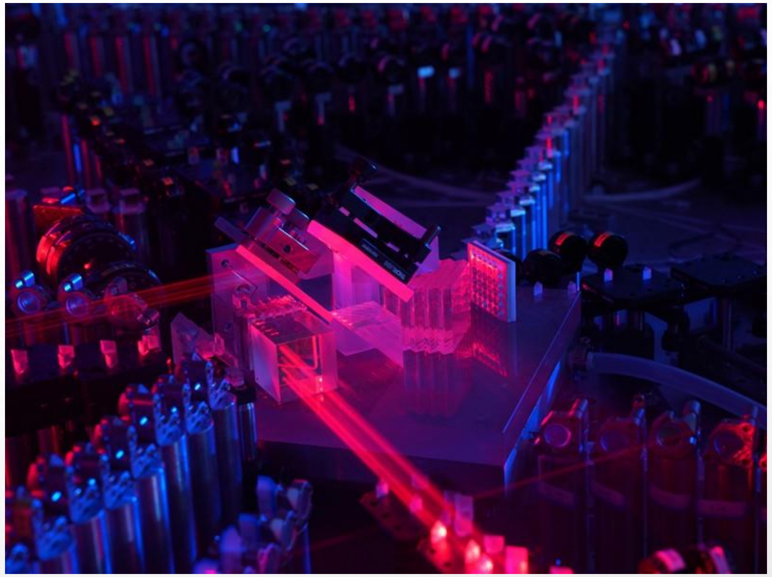


100+ photons, Science 2020, arXiv:2106.15534, July 2021.

NEAR-TERM QUANTUM DEVICES & VERIFICATION PROBLEM



54 qubits, the Sycamore processor, Nature 2019.

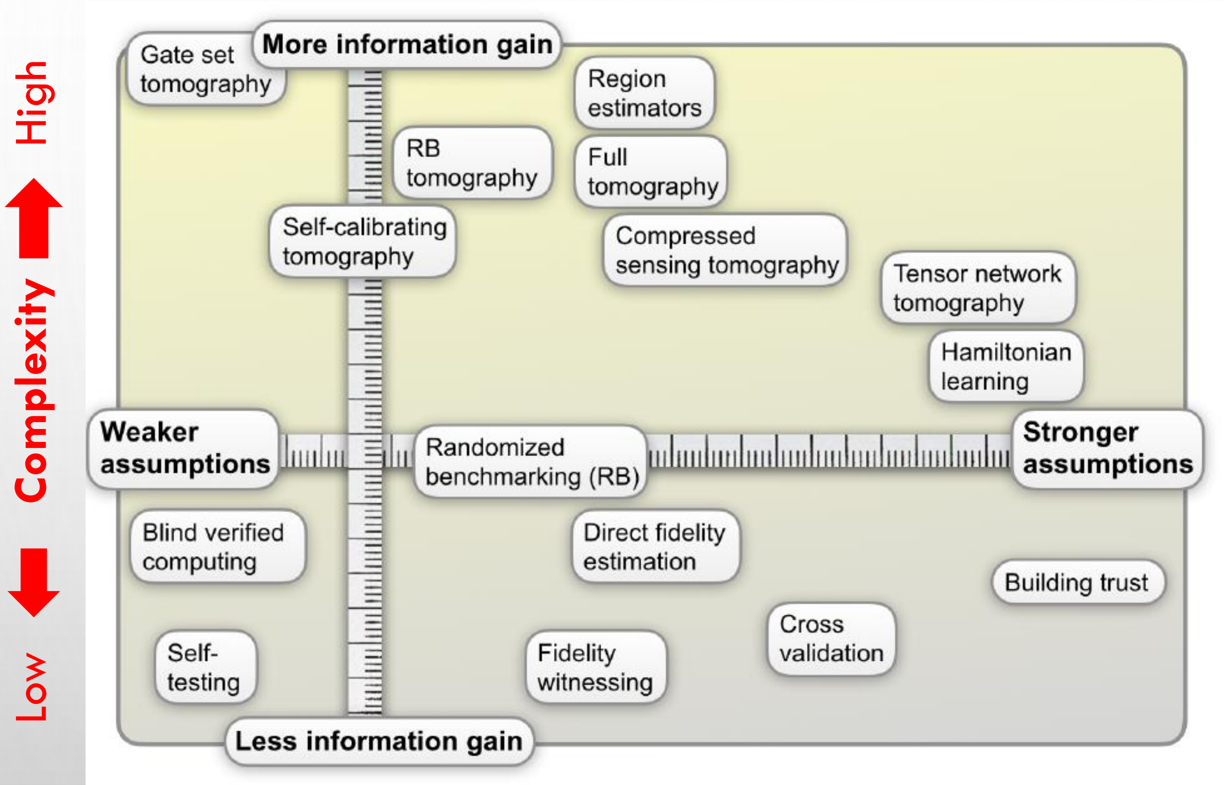


100+ photons, Science 2020, arXiv:2106.15534, July 2021.

- ❑ Era of the noisy intermediate-scale quantum devices (NISQD, Preskill18), 50+ qubits,
- ❑ NISQD are not universal, not-protected by error-correction, etc.
- ❑ Verification & benchmarking is of the central importance.

Is the device functioning in the anticipated fashion?

VERIFICATION PROBLEMS



Eisert et al, Nature Reviews Physics 2, 382-390 (2020).

Verification (certification/characterization) tasks: Entanglement, non-locality, fidelity estimation, state/process tomography, computing, simulations, property testing, etc.

Complexity (effort) of the problem:

- ❑ **Sample complexity** (# of exp. repetitions/copies)
- ❑ **Quantum computational complexity** (# of quantum gates)
- ❑ **Post-processing complexity** (classical memory & computational cost)

Scale in general unfavourably with the system size (exp. growth)

Goal: Find tractable examples

Info. processing —system size→ advantage

Diagnostics → hendicap

VERIFICATION PROGRAM

Exp. in size!

Golden standard

Quantum state tomography

exp. complexity

data samples → State ρ → Any property A

Aaronson's program

(S. Aaronson, 2018)

Shadow tomography

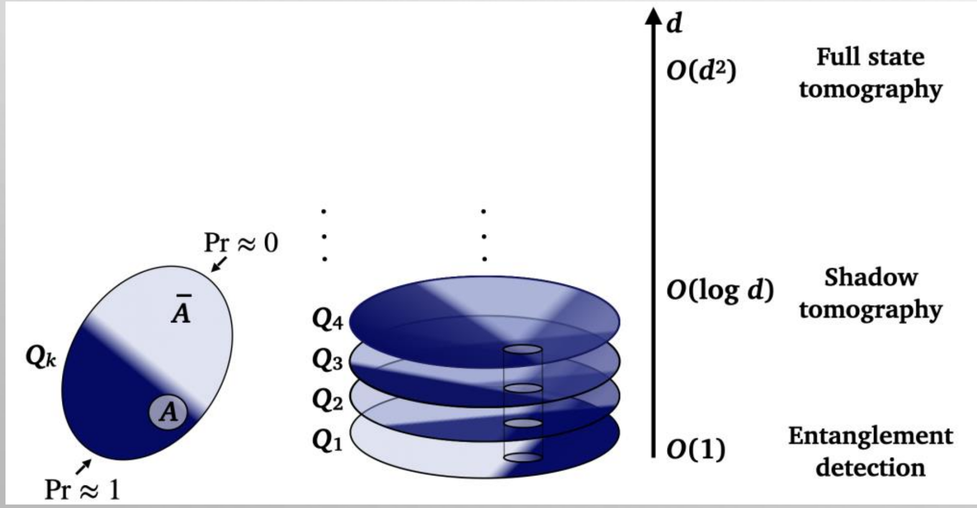
moderate complexity

Small size!

Universal data record → ~~State ρ~~ → Any (reasonable/physical) property A

direct inference!

Central question: *Given a limited number of interactions with a large system, how much classical information can we learn with a high degree of certainty?*



QI Perspective: Quering the system with certain questions $Q_1, Q_2, \ldots, Q_K$ to verify some property A

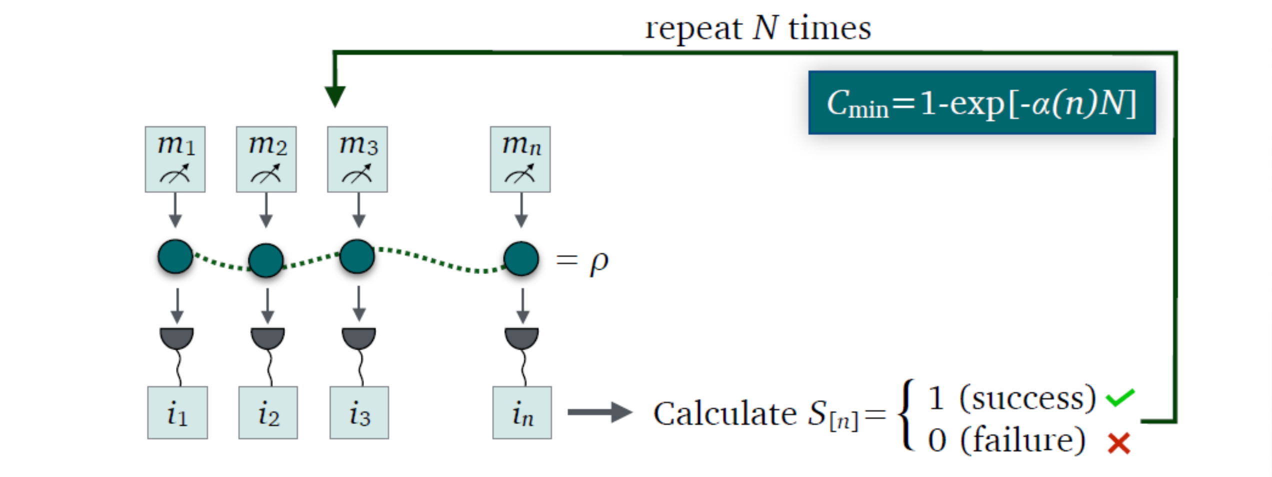
$$\Pr[pass\ all | \rho \in \bar{A}] = \exp[-\alpha\, N\, r(d)]$$

N is number of repetitions

$d = 2^n$ is dimension of system

- J. Morris, V. Saggio, A. Gočanin and B. Dakić, Advanced Quantum Technologies, 2021, review article.

VERIFICATION PROGRAM



$$\Pr[pass\ all|\rho \in \bar{A}] = \exp[-\alpha\ N\ r(d)]$$

$$d = 2^n$$

- **<u>WHAT DO WE WANT:</u>**

a) **<u>Dimension demarcation</u>** ($r(d)$ is typically constant in d),

b) <u>Fast convergence</u> in the number of queries N,

c) <u>Low computational complexity</u> (e.g. Qs are implemented locally or low depth circuits),

d) <u>Simple post-processing</u>, e.g. simple evaluation of the decision function.

<u>Review in this talk</u>: Single- and few- copy **<u>entaglement detection</u>**, application to quantum **<u>state verification & certification</u>**, and quantum state **<u>tomography</u>** (selective tomography and classical shadows)

- J. Morris, V. Saggio, A. Gočanin and B. Dakić, Advanced Quantum Technologies, 2021, review article.

FEW-COPY ENTANGLEMENT DETECTION

Standardly: witness method (Gühne09): STATE IS ENTANGLED IF $\langle W \rangle < 0$

In practice: $W = \sum_s w_s P_{local}^{(s)}$ ➡ measure local components to get $\langle W \rangle$ to accuracy ϵ

Re-formulation into queries: is $\langle W \rangle < 0$ true? (i.e. state is entangled or not?)

Queries (sample randomly)

Sampling weights ➡ **Exp. fast convergence!**

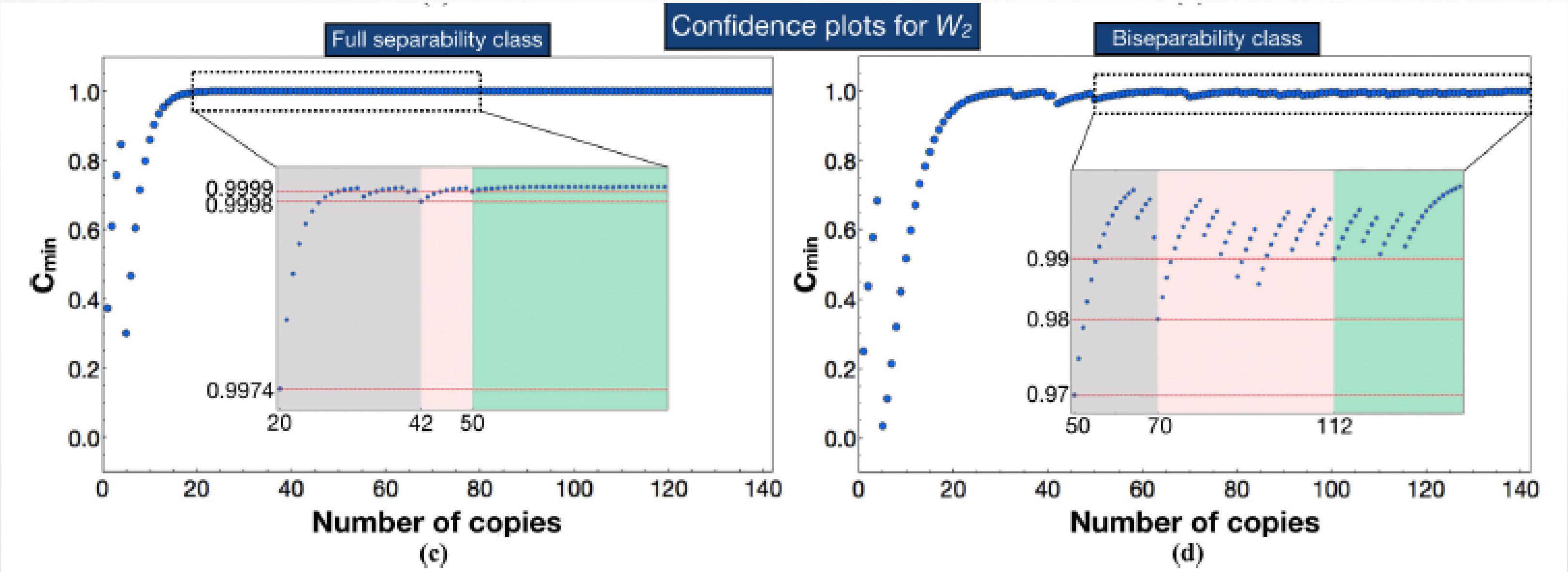
Results: $N \sim log\delta^{-1}$ (removes ϵ-dependence from $N \sim \frac{log\delta^{-1}}{\epsilon^2}$)

- Verification as a decision procedure (YES/NO),
- Translation works for a generic witness,
- No size dependence, e.g. verifies entaglement in graphs states wit 99% with 16 copies only (regardless of the size),
- Efficient for a large class of quantum states (e.g. many-body ground states).

- V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, Nature Physics 15, 935, 2019.

EXPERIMENT

- Experimental 6-qubit photonic graph state (Saggio et al, Nature Physics, 2019):

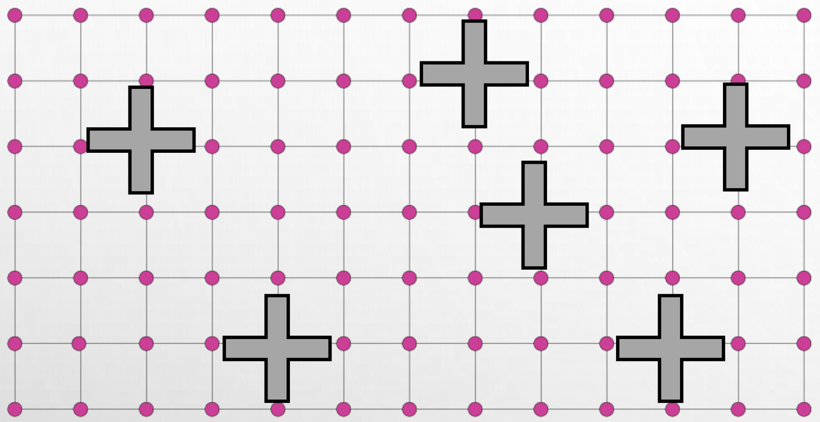


SOME ENTAGLEMENT	GENUINE 6-QUBIT ENTANGLEMENT
≈ 20 copies	≈ 100 copies

- V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, Nature Physics 15, 935, 2019.

SINGLE-COPY ENTANGLEMENT DETECTION

- Furher reduction to the logical limit (one click)
- Robust states (e.g. cluster states or GS of local Hamiltonians)



Random sampling of:

$$\begin{matrix} & X & \\ X & Z & X \\ & X & \end{matrix}$$

$$\begin{matrix} & X & \\ X & Z & X \\ & X & \end{matrix} = 1 \text{ for CS state only}$$

$$C = 1 - \exp(-\alpha N)$$

For sufficiently large N, almost certain entaglement verification from <u>ONE COPY</u>

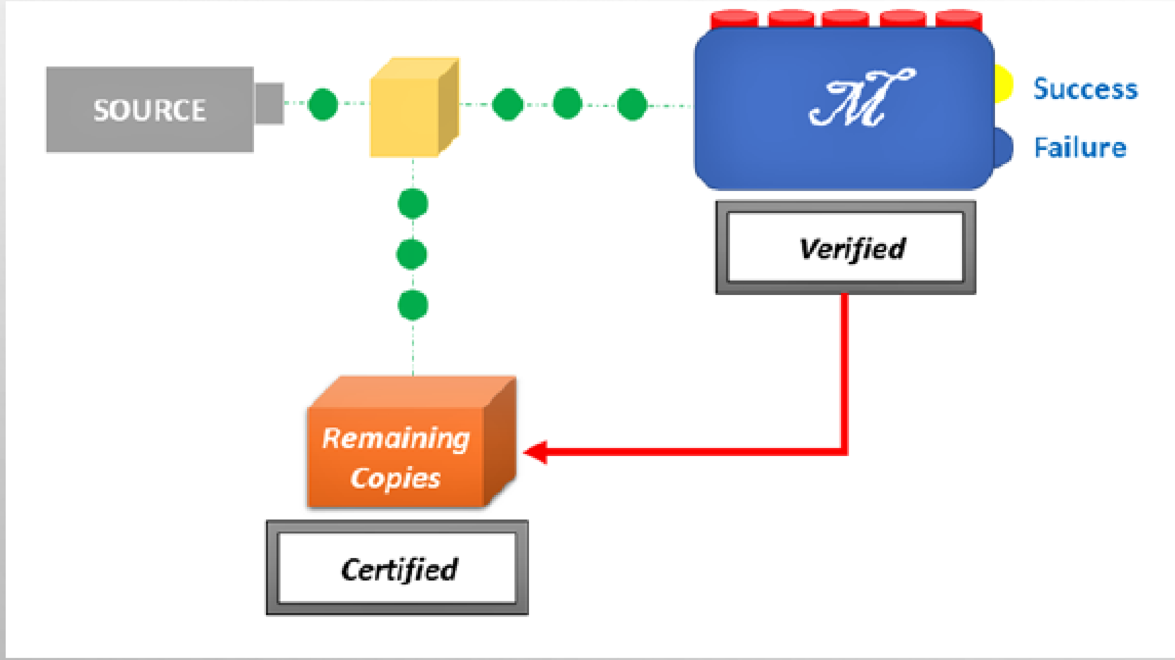
<u>Example</u>: One copy of 24-qubit LCS suffcies to verify entanglement with >95%!

<u>Summary</u>: Single-shot entanglement verification for a large class of states (cluster states, TNS states, GS of local Hamiltoninans).

- A. Dimić and B. Dakić, npj Quantum Information 4, 11, 2018.

DEVICE-INDEPENDENT QUANTUM STATE VERIFICATION&CERITIFICATION (QSV&C)

- **QSV TASK (Palister18):** Are $\sigma_1, \sigma_2, \dots, \sigma_N$ produced by an unknown source ϵ-close to the target state? ➡ $N = O(\epsilon^{-1})$ ➡ Optimal scaling (very cheap)
- **PROBLEMS**: Artificial constrants (e.g. all σs are ϵ-close to the target or not), trusted devices, certification problem.



Self-testing methods + our methods:

- Device-indpendent setting,
- Non-adversarial scenario (non IID),
- Certification is resolved.

$N = O(\epsilon^{-1})$ ➡ Optimal scaling

- A. Dimić, I. Šupić and B. Dakić, Phys. Rev. X Quantum 3, 010317 (2022).

QUANTUM STATE TOMOGRAPHY

- **Task:** Determine unknown quantum state of a d-dim. quantum system
- **Figure of merit:** $\left\|\rho^{exp} - \rho^{th}\right\|_1 \leq \varepsilon$ (trace-distance norm)
- **Resources** (# of required copies N for a fixed error ε):

	N
Best strategy*	$O(d^2/\varepsilon^2)$
Independent strategy**	$O(d^3/\varepsilon^2)$
Low rank (r) matrix***	$\Omega\left(\frac{rd}{\varepsilon^2}\right)/\ln(dr/\varepsilon)$

* Harrow17, O'Donnell15; ** Kueng14; *** Flammia11, Harrow17

- **Sampling complexity:** For composite systems, e.g. qubits ($d = 2^n$), explicit dim. dependence makes the task completely intractable: $N \sim \exp(n)$!
- **Post-processing:** Memory & computational cost is huge for storing and manipulating exp. large matrices!

→ Full tomography is intractable

AN ALTERNATIVE: SHADOW TOMOGRAPHY

- **Full tomo**: $\left\|\rho^{exp} - \rho^{th}\right\|_1 \leq \varepsilon$ (trace-distance norm)
- Estimated density matrix allows for the prediction of any measurement to accuracy ε
- Most of this information is irellevant/not of practical use

- **Different task:** Shadow tomogrpahy, i.e. tomography **for all practical purposes.**

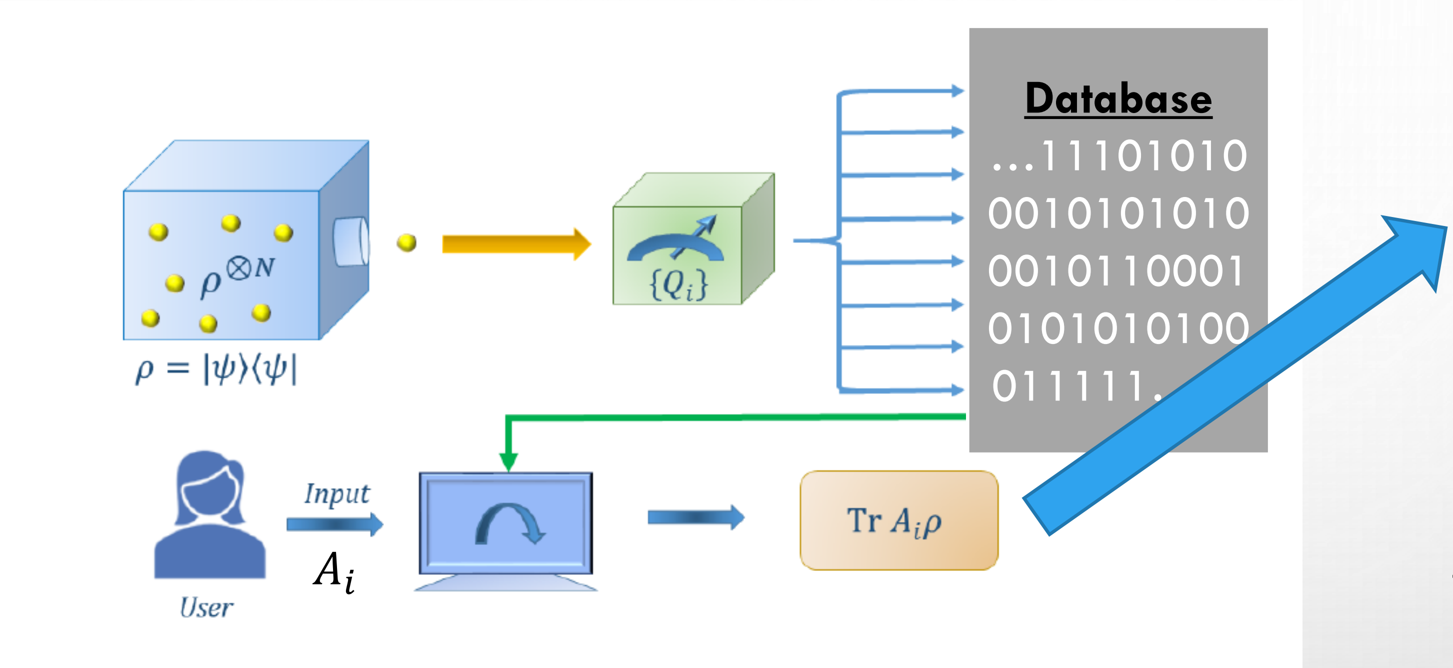
- Given a set of observables $E_1, E_2, \dots, E_M$ the set of mean values $\langle E_1\rangle, \langle E_2\rangle, \dots, \langle E_M\rangle$ to be estimated by using a moderate number of resources (copies)?

$N = \tilde{O}(\log \delta^{-1} \log d \log^4 M/\varepsilon^4)$ → Requires universal quantum computer

- **OUR GOAL**: Put constraints on desired observables $E_1, E_2, \dots, E_M$ to reduce (quantum) computational effort while still maintaining extraction of the exp. # of E_ks, e.g. $M \sim \exp(\alpha\, n)$

- S. Aaronson, SIAM Journal on Computing 2019, 49, 5 STOC18

SELECTIVE QUANTUM STATE TOMOGRAPHY (SQST)



Allows for multiple estimations (of various A_is) from the same data

Universal data samples

Complete for selective (partial) tomography!

Benefits:

- Data samples of constant size (no dimension scaling),
- Can be repeated M times at a very low cost, i.e. $N \sim logM$
- Measurements are computationaly cheap, e.g. linear depth $\sim n$
- Post-processing is very simple, no need to store and manipulate exp. large matrices

- J. Morris and B. Dakić, arXiv:1909.05880 (2019), H. Huang and R. Kueng, arXiv:1908.08909 (2019).

MEASURING OFF-DIAGONAL ELEMENTS

Classical task: Given unkown distribution $(p_1, \dots, p_d)$ what is the minimal number of runs nedeed to estimate all p_k's to a given accuracy ϵ?

$$max_k|p_k - p_k^{est}| < \epsilon$$

➡ Tomography in MAX norm

$$N = O\left(log\frac{d}{\delta}/\varepsilon^2\right)$$

(Kamath15, Aaronson18)

Quantum task (Selective Quantum State Tomography): Given unkown state ρ what is the min number of runs nedeed to estimate all ρ_{ij}'s to a given accuracy ϵ?

$$max_{ij}|\rho_{ij} - \rho_{ij}^{est}| < \epsilon$$

➡ Tomography in MAX norm

Our result:

- Random sampling from mutually unbiases bases (MUBs via linear depth $\sim n$ circuits)
- To extract M elements to accuracy ϵ

$$N = O(\log M / \varepsilon^2)$$

- Full tomo in MAX norm (i.e. all elements) reuqires $O(\log d / \varepsilon^2)$ copies,
- Applied to to the full (trace-norm) tomo results in $\tilde{O}(d^3/\varepsilon^2)$ copies, which is optimal scaling.

- J. Morris and B. Dakić, arXiv:1909.05880 (2019).

CLASSICAL SHADOWS

- **SQST**: POVM elements are MUBs known as quantum 2-designs (Morris&Dakić, arXiv:1909.05880, 2019).
- Efficient estimation in 1-norm: $||A||_1 = \sum_{ij} |a_{ij}| \leq K$ ⇒ $N = O(K^2 \epsilon^{-2} log M)$
- **CLASSICAL SHADOWS**: POVM elements are random Clifford circuits, i.e. 3-designs (Huang&Kueng, arxiv:1908.08909, 2019).
- Efficient estimation in Frobenius norm: $||A||_2 = \sum_{ij} |a_{ij}|^2 \leq K$ ⇒ $N = O(K^2 \epsilon^{-2} log M)$

APPLICATIONS: fidelity estimation, off-diagonal elements (coherence), short-range observables (Hamiltonian, energy), entaglement detection, state verification etc.

- H. Huang and R. Kueng, arXiv:1908.08909 (2019), H. Huang, R. Kueng and J. Preskill, Nature Physics 16, 1050 2020.

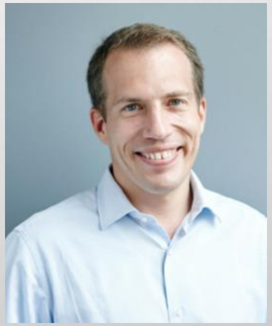
SUMMARY

- **Partial tomography**: Avoid full tomography and directly extract/verify desired quantites
- Very powerful for large-scale systems:

a) **Dimension demarcation**
b) Fast convergence
c) Low computational complexity
d) Simple post-processing




Strong bonds to experimental quantum photonics

P. Walther

References:
1. S. Aaronson, SIAM Journal on Computing 2019, 49, 5 STOC18,
2. J. Morris, V. Saggio, A. Gočanin and B. Dakić, Advanced Quantum Technologies, 2021, review article,
3. A. Dimić and B. Dakić, npj Quantum Information 4, 11, 2018,
4. V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, Nature physics 15, 935, 2019,
5. A. Dimić, I. Šupić and B. Dakić, Phys. Rev. X Quantum 3, 010317 (2022),
6. H. Huang and R. Kueng, arXiv:1908.08909 (2019),
7. H. Huang, R. Kueng and J. Preskill, Nature Physics 16, 1050, 2020.

THANK YOU!

beyondC   ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN   Vienna Center for Quantum Science and Technology   universität wien