$\langle\psi_f|U|\psi_i\rangle \overset{CPT}{\longleftrightarrow} \langle\psi_i|U^\dagger|\psi_f\rangle$ like S-matrix — to solve NP (postBQP), improve error correction and stability

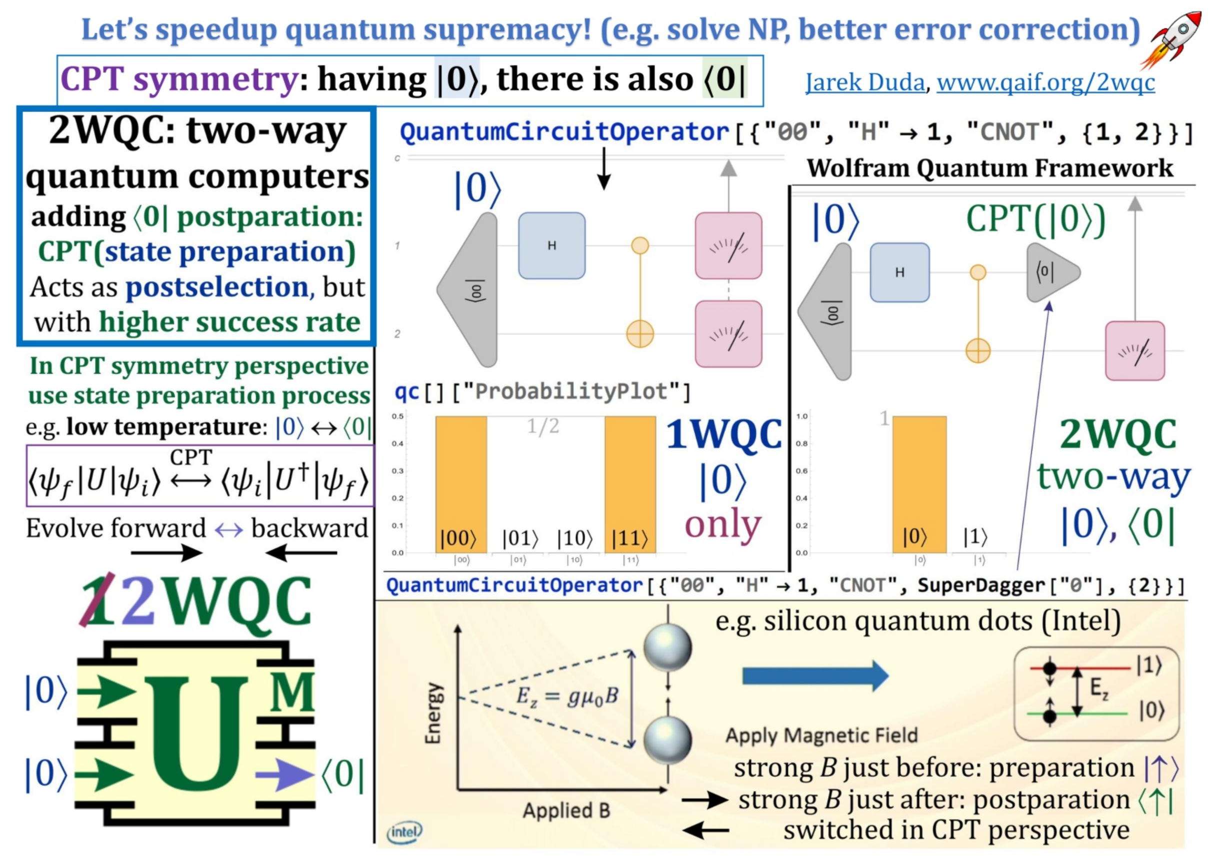
# 1̸2WQC: two-way quantum computers

Jarosław Duda, JU
www.qaif.org/2wqc
slides from th.if.uj.edu.pl/~dudaj/

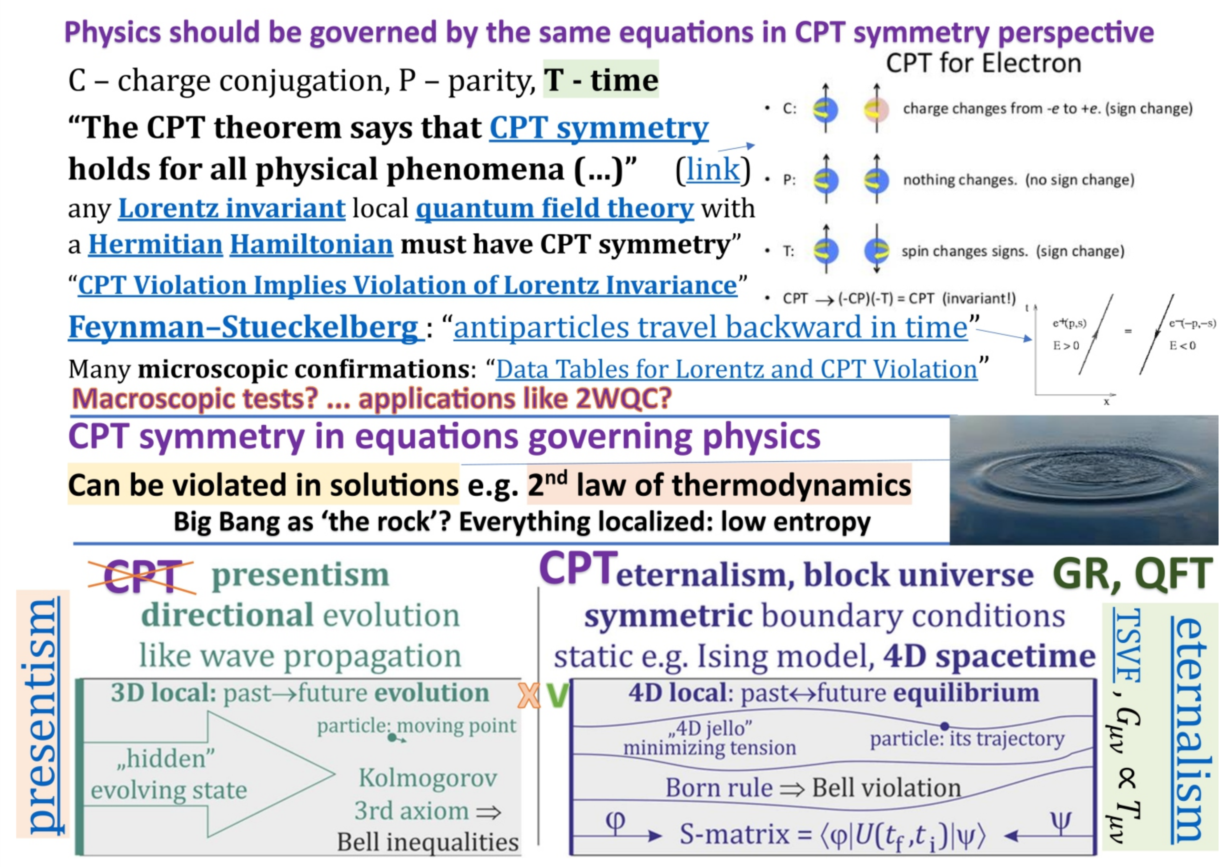
~postselection of higher success rate — evolving backward in time (CPT), conditions as for state preparation e.g. $V(t) \overset{CPT}{\longleftrightarrow} -V(-t)$

## adding postparation as state preparation in CPT perspective

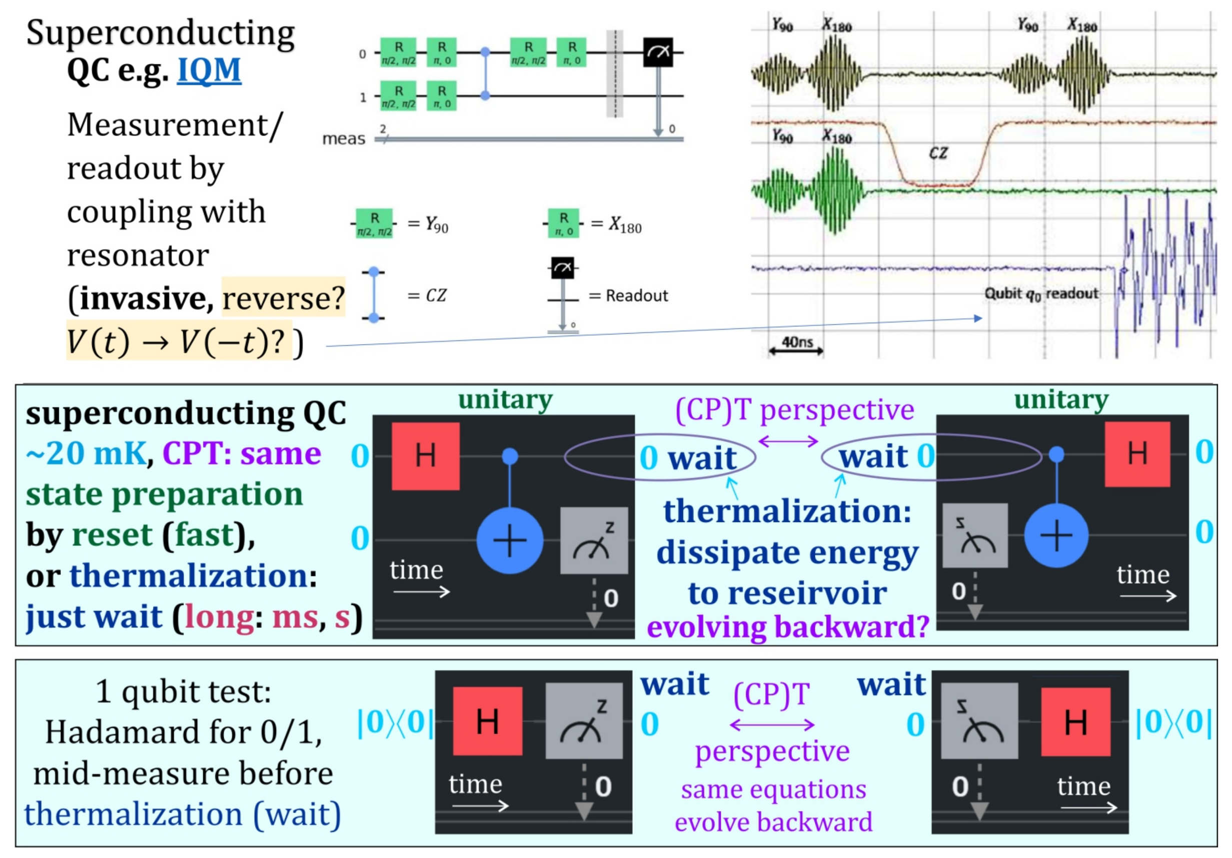
1) Standard **1WQC** assumes **state preparation** $|0\rangle$, then **unitary evolution** $U$, then **measurements**. However, physics is believed to be **CPT symmetric** - governed by nearly the same equations when **evolving backward in time**. Therefore, applying conditions which for backward evolution are original state preparation conditions, e.g. $V(t) \leftrightarrow -V(-t)$ **reversed shape of prepare impulse**, we should get **postparation** $\langle 0|$ - analogously enforcing the final state, mathematically acting as **postselection** $\langle 0|$, but with **higher success rates**.



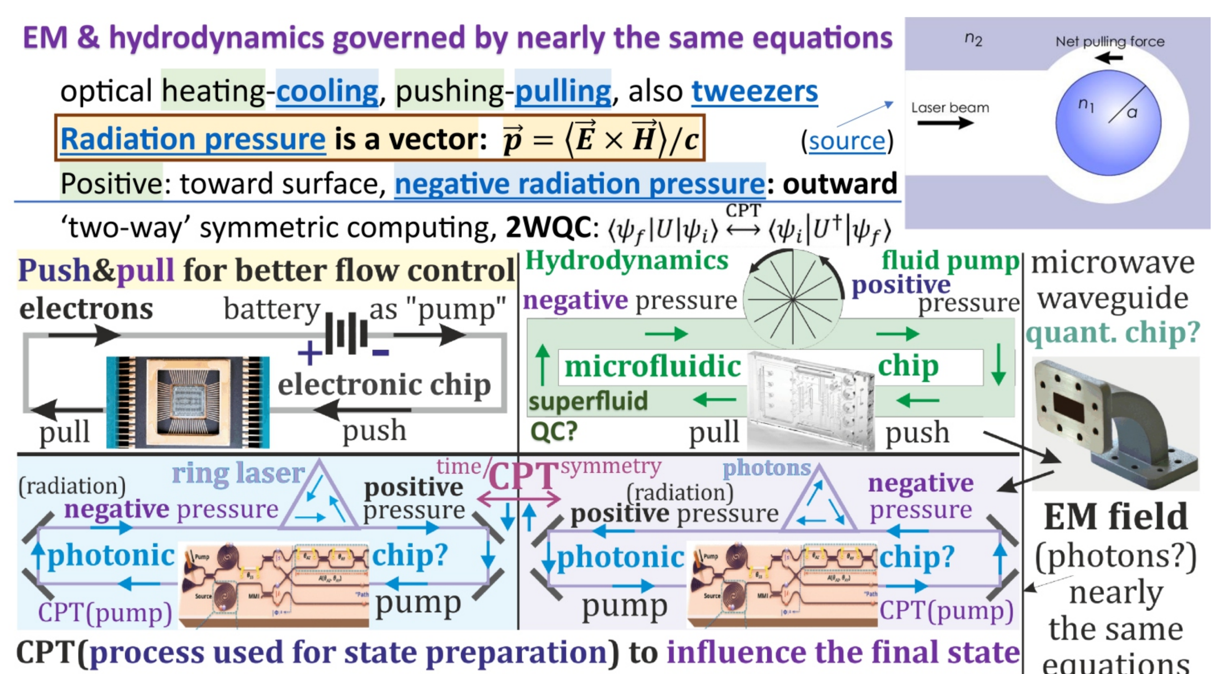

2) **CPT symmetry** is crucial for modern physics, experimentally **widely tested**, however, seems **only in microscale**. **Macroscopic applications** are proposed here, which **if unsuccessful** would present **experimental macroscopic CPT violation**, requiring to modify modern physics. For **CPT symmetric**: **general relativity** and **quantum field theories**, it is crucial to use **eternalism/block universe philosophy of time**: traveling through already found **4D solution**, working on **4D scenarios** like spacetime shape or **Feynman paths/diagrams**.




3) Evolving in **low temperature reservoir**, like in superconducting quantum computers, eventual **energy is dissipating** to reservoir, allowing to prepare nearly certain (Boltzmann) **ground state 0 by just waiting: thermalization**. **Evolving backward** in time (e.g. **Lindbladian** from $+\infty \to 0$ instead of $-\infty \to 0$): temperature is the same, CPT says equations should be practically the same, so shouldn't **energy also dissipate to 0**? It suggests to **just wait thermalization time** (~1s) after unitary evolution to **enforce given qubit to 0 (postparation)**.

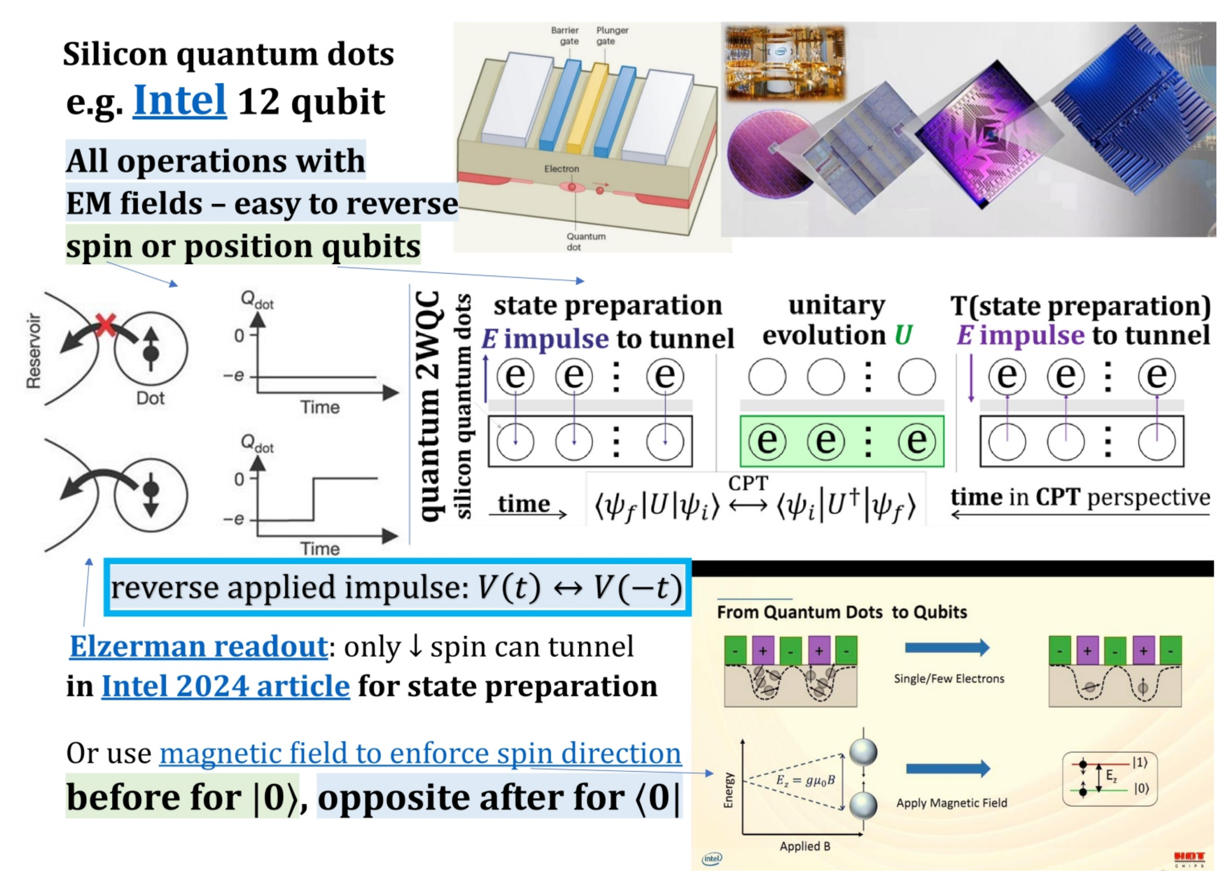



4) Standard **electronics has two-way control**: we both push and pull electrons by electric potential. Also for **hydrodynamics** we have **two-way control** using **pump**, for **superfluid QC** getting **2WQC**. EM and (superfluid) hydrodynamics are governed by nearly the same equations, suggesting to take two-way control to microwaves and photons. For "**pump for photons**" we need e.g. **ring laser** or **synchrotron source**, in CPT perspective emitting photon in reversed direction - injecting them to the back of photonic chip, analogously as in hydrodynamics.




| setting | Gauge fields | Circulation | Gauge condition | Matter field |
|---|---|---|---|---|
| Electro-dynamics | $\varphi$, $\vec{A}$ four-potential | $\vec{B} = \nabla \times \vec{A}$ magnetic f. | $\nabla \cdot \vec{A} + \frac{1}{c^2}\frac{\partial\varphi}{\partial t} = 0$ | $\vec{E}_e = -\frac{\partial \vec{A}}{\partial t} - \nabla\varphi$ |
| Hydro-dynamics | $\chi = v^2/2$, $\vec{v}$ flow velocity | $\vec{\omega} = \nabla \times \vec{v}$ vorticity | $\nabla \cdot \vec{v} + \frac{1}{c_s^2}\frac{\partial \chi}{\partial t} = 0$ | $\vec{E}_h = -\frac{\partial \vec{v}}{\partial t} - \nabla\chi$ |

5) For example in silicon quantum dots, all **operations have to be realized with electromagnetic impulses**, for which e.g. $V(t) \leftrightarrow -V(-t)$ impulses of reversed shape would become the original one in **perspective of CPT symmetry**. For example impulse of electric field can be used to tunnel electrons to dots for state preparation, reversed impulse would do it in CPT perspective. Or strong magnetic field can enforce spin direction: applied before unitary evolution for **preparation** of initial state, after for **postparation** of final state.




6) Mathematically, we can treat the **final density matrix** (including noise) in various ways: in **1WQC** we just measure $n$ qubits. We can use additional $m$ qubits and postselect them (**p1WQC**): measure and **discard** if getting unwanted values, however, its **success probability usually drops exponentially** with $m$. In **2WQC** we would like to go through unitary evolution in reversed direction, or equivalently apply projection to this final density matrix - getting the same probability distribution as with postselection, but **without exponential drop of success probability** - allowing to attack **postBQP** containing **NP problems**.

**2WQC – "higher success rate postselected 1WQC"**

Quantum computing → $\rho$ density matrix (including noise), then:

**1WQC: measurement (e.g. $n$ qubits):** $P(s) = \mathrm{Tr}(\Pi_s \rho)$

**p1WQC: earlier postselect to condition $c$** ($m$ qubits)

**Measure $n+m$ qubits discarding all but $c$:** $P(s) = \frac{\mathrm{Tr}((\Pi_s \otimes \Pi_c)\rho)}{P(c)}$

$P(c) = \sum_s \mathrm{Tr}((\Pi_s \otimes \Pi_c)\rho) = \mathrm{Tr}((I_s \otimes \Pi_c)\rho) \sim 2^{-m}$ **success rate**

**2WQC:** $\rho \to (I_s \otimes \Pi_c)\rho(I_s \otimes \Pi_c)$ **postpare/project to $c$,**

**then measure $n$ qubits:** $P(s) = \frac{\mathrm{Tr}((\Pi_s \otimes \Pi_c)\rho)}{P(c)}$ **as in p1WQC**

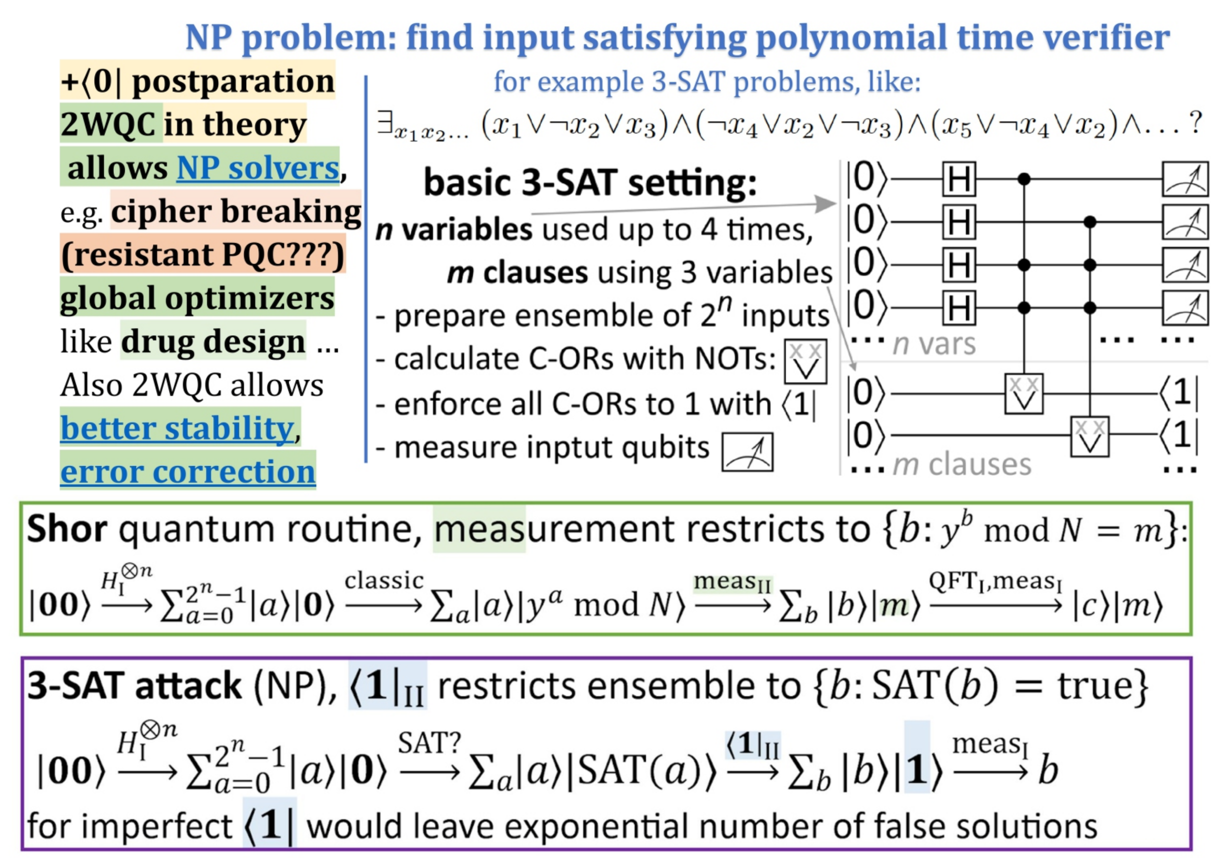
**but with ≈ 1 success rate** (instead of $\sim 2^{-m}$ for p1WQC)

**Potentially exponential speedup, e.g. to solve NP problems**

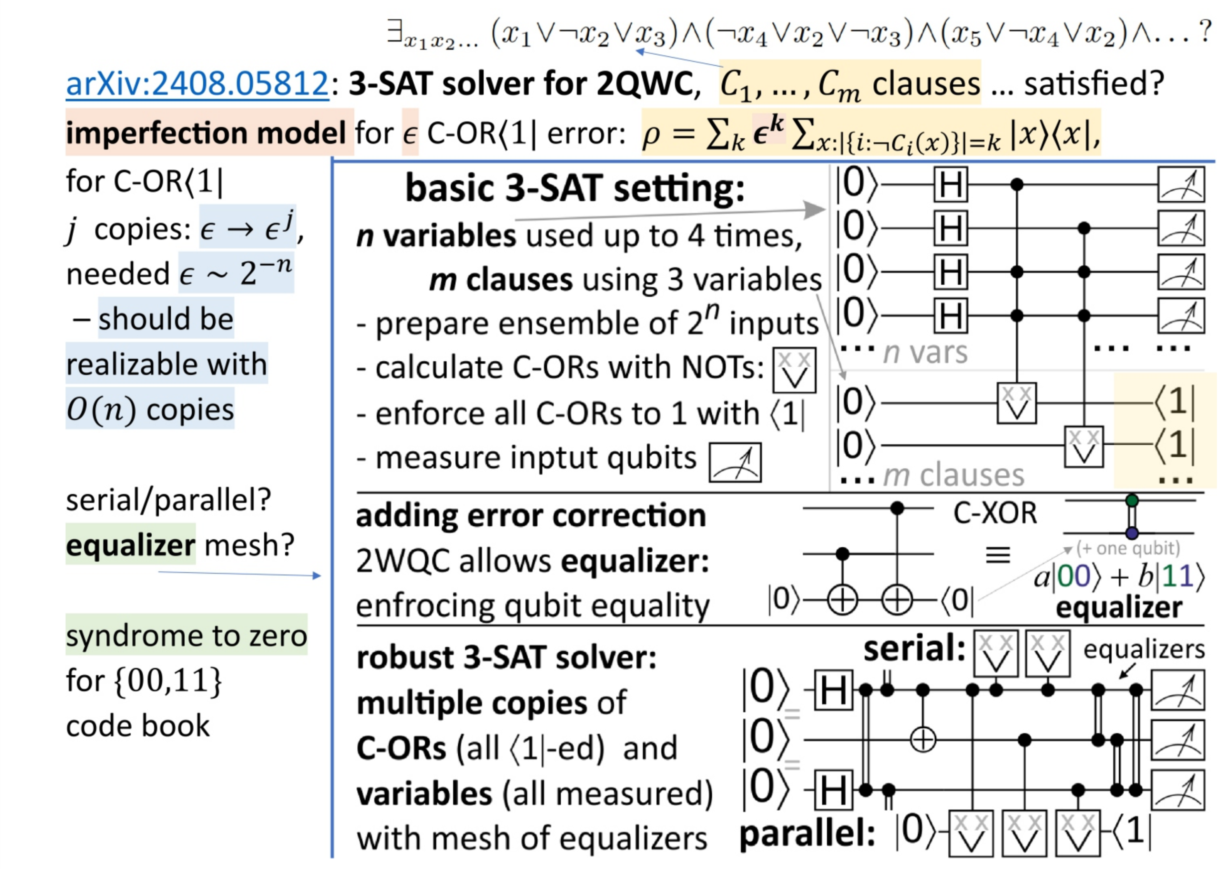
**Aaronson's postBQP adding postselection: containing NP**

conflicts need imperfections e.g. $\langle 0|1\rangle$ ferromagnet: ↑↑↑↑↑↑↑↑↓↓↓

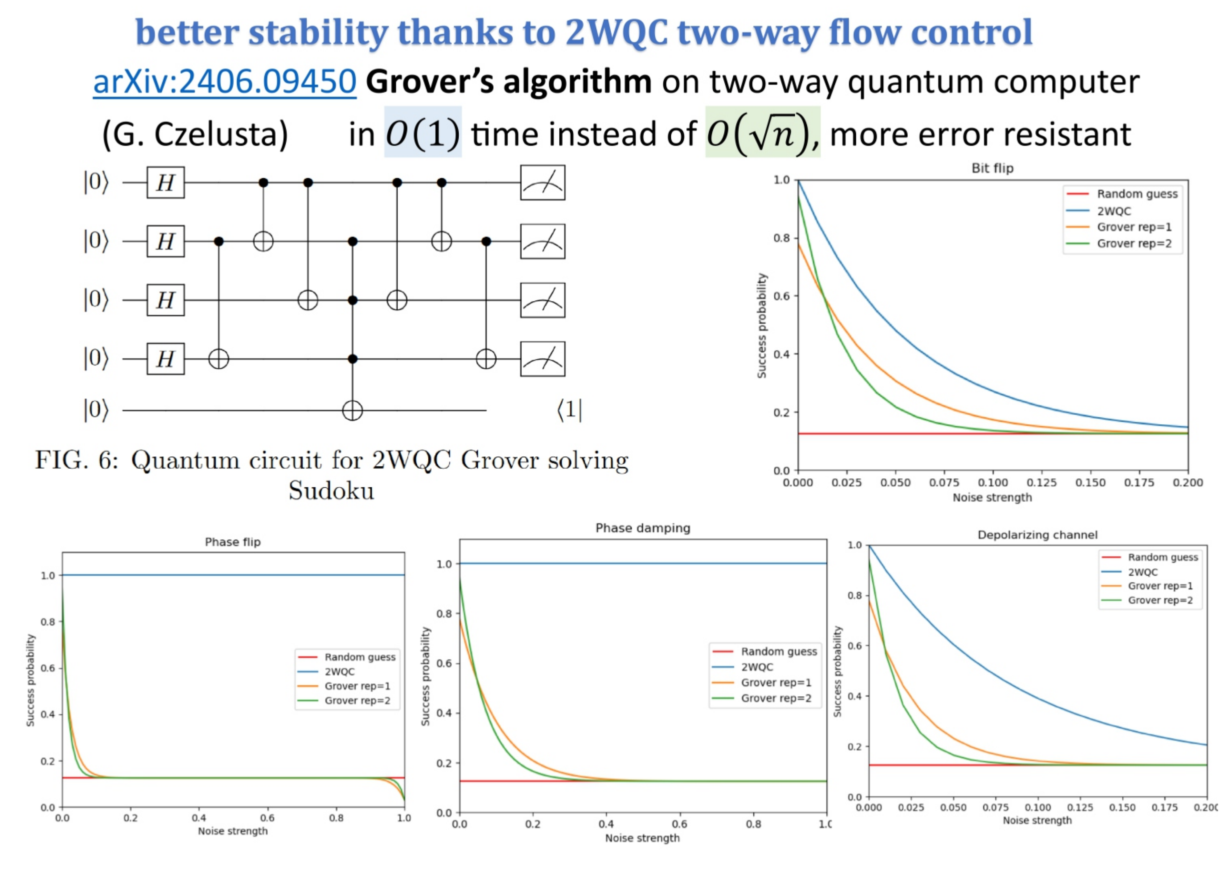
7) One of potential approaches to **quantum NP solvers** is based on **Shor algorithm**: start with state preparation, then Hadamard gates to get ensemble of exponential number of inputs, then some classical function, and finally its measurements restricting ensemble to fixed output of this function, which is periodic - by Fourier transform getting hint for factorization. For **quantum NP solver** we could use **verifier as classical function**, and **replace measurement with postparation** to restrict ensemble to only satisfying our instance of NP.




8) To overcome **imperfections**, such potential quantum NP solver would rather **require exponential reduction of error rate**. Fortunately, **postparation also provides new error correction** ways, like **equalizer** below allowing to work on multiple identical copies, hopefully to arbitrarily reduce error rate, or generally on **superpositions of codewords** of some error correction codes, having large Hamming distance. **Working on copies** is different than **cloning**, which is still forbidden for postselection and postparation (arXiv:2407.15623).




9) **Grover's algorithm** offers alternative approach for **NP solvers**, and with **postparations** seems to allow for exponential speedup. For below simple setting it allowed to reduce time to constant O(1), and its **two-way control** of information flow also allowed to **improve stability: resistance to various types of noise**, like bit flip, phase flip, phase damping, depolarization channel.




10) **Current post-quantum cryptography is focused** on **Shor** and **Grover**. Possibility of e.g. **quantum NP solver** seems completely **neglected**(?) - what seems highly **irresponsible**. For **resistance** in some **nextgen PQC**, we could **increase required resources** by orders of magnitudes above reachable in near future, e.g. requiring costly initialization to build large decoding tables based on the key. Another way is going to higher complexity classes, like still practical **PSPACE**, e.g. requiring **multiple interaction game** to establish connection.

**Post-quantum cryptography** (PQC): now focused on Shor, Grover

What if better algorithms, upgrades like 2WQC are there/coming?

**NP solver** verifier: does decryption with given key lower entropy?

Are some of current PQC already resistant? (NP-hard is not enough)

**Building nextgen PQC**: immune/resistant to quantum NP solver?

E.g. **require initialization**: large calculations based on cryptographic key before proper decoding (tough for key superposition)

Maybe based on **higher class like PSPACE** (private/public key?)

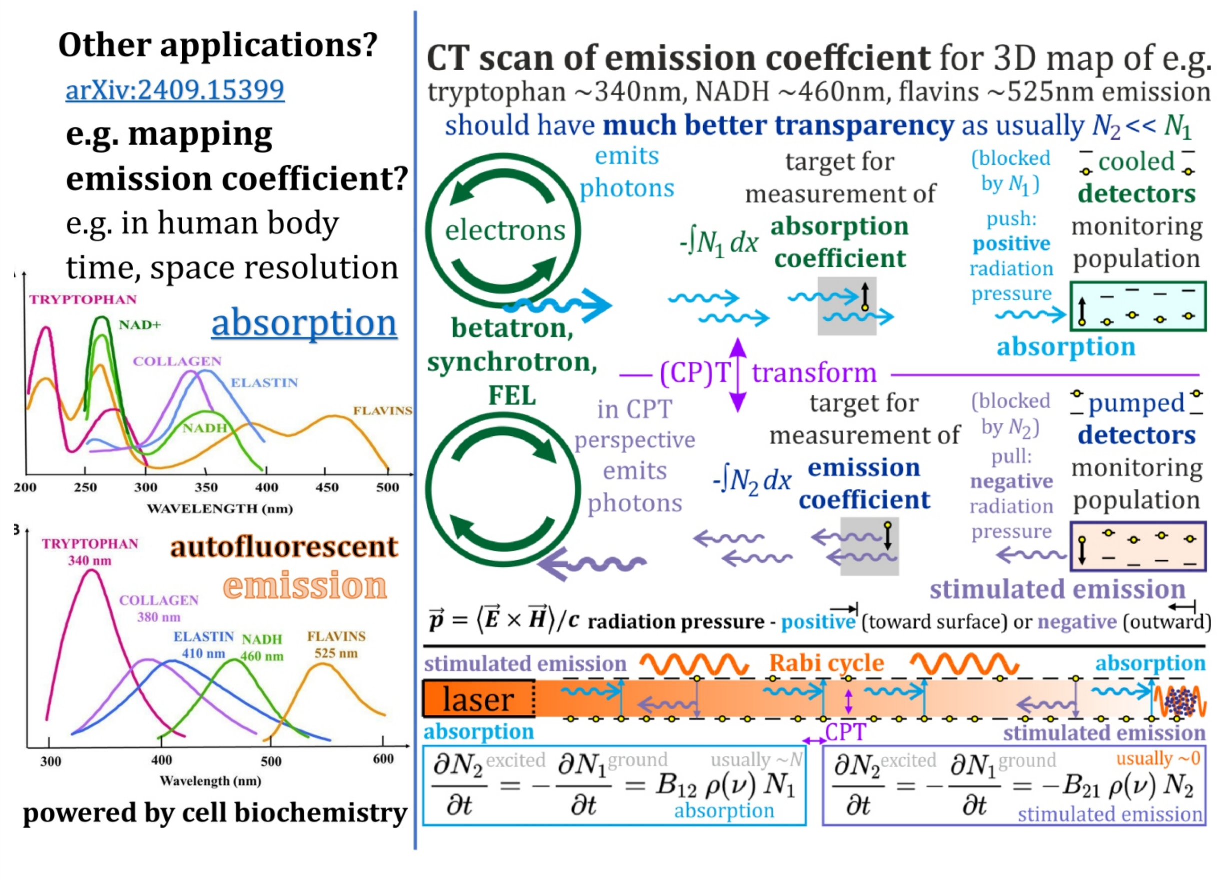
https://en.wikipedia.org/wiki/PSPACE-complete

e.g. formal languages, **3-SAT + ∀** quantifier $(\forall_{x,\ldots}\exists_{y,\ldots}(\vee\vee)\wedge\ldots)$,

**reconfiguration**: find path satisfying constraints (~arXiv:1204.5317),

**puzzles/games**: multiple-interaction cryptography (before low entropy)

11) This research has also lead to proposed **further potential applications of CPT symmetry**, or, **if unsuccessful**, tests to show **CPT violation**. For scenarios **emitting photons in CPT perspective**, like **synchrotron** with charge travelling on circle in both perspectives, for us should cause deexcitation with **stimulated emission** e.g. for novel **radiotherapy** to starve cancer tissue. Or CPT analog of **CT scanner** below, **mapping emission coefficient** instead of **absorption**, what should have much **better transparency** as blocked only by excited atoms $N$.




12) The **general relativity** in theory allows for additional realizations, rather impractical but valuable as **stimulating thought experiment**. While **below black hole horizon it rotates time into space** light cones, e.g. **non-orientable wormhole** could allow to rotate twice further - e.g. reversing time direction inside a rocket travelling through it. For **external observer**, entropy would decrease **there**, 1WQC would use **pre-measurement** and **postparation**, its laser would **cause stimulated emission**, CT scanner would map **emission coefficients**.