Making Quantum Verification Middle-term Ready

JFQI2023 Workshop

Bo Yang, 2023.12.14

Project members

Bo Yang

Dominik Leichtle

Elham Kashefi

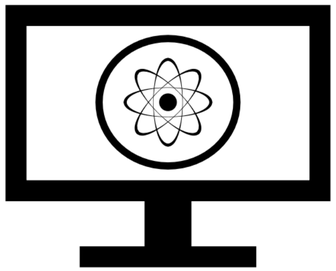
Harold Ollivier

LIP6 SORBONNE UNIVERSITÉ cnrs ‹QSL› Quantum Software Lab Inria

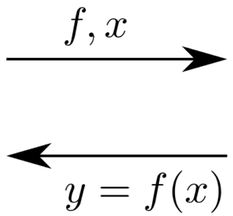
Future Quantum Ecosystems

Delegation of quantum computation

Limited computational ability



Client



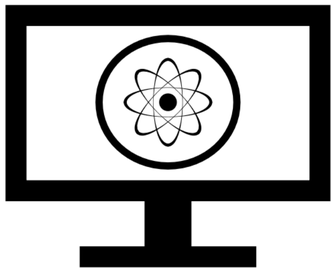
Universal computational ability

Server

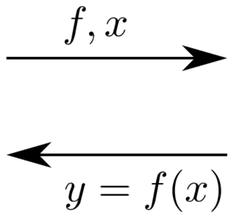
Future Quantum Ecosystems

Two-party Prepare-and-send Model

Limited computational ability
(single-qubit preparation only)



Client



single-qubit quantum
communication

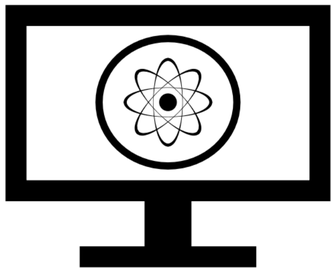
Universal computational ability

Server

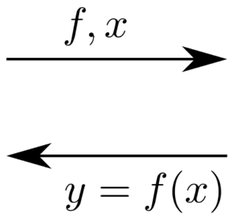
Future Quantum Ecosystems

Two-party Prepare-and-send Model

Limited computational ability
(single-qubit preparation only)



Client



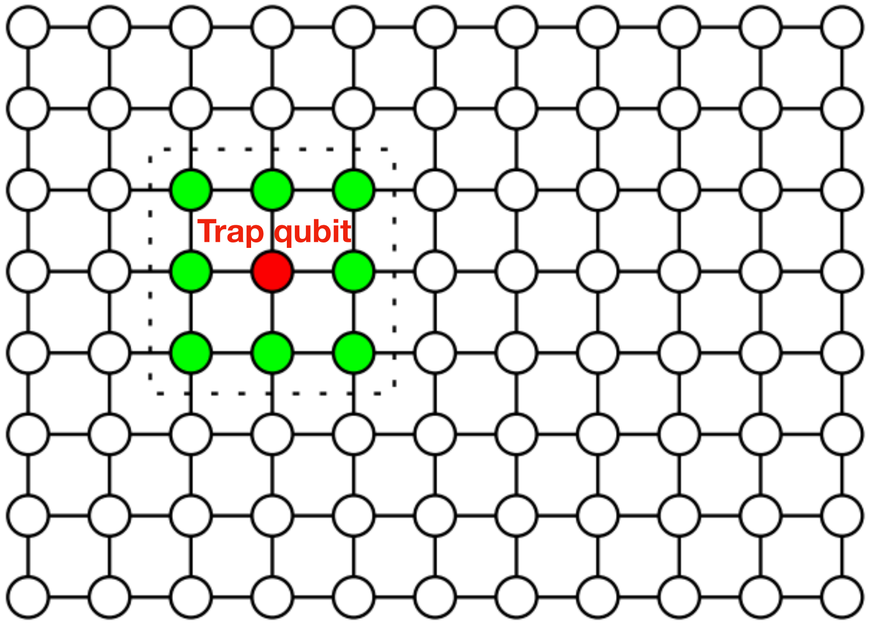
single-qubit quantum
communication

Universal computational ability

Server

- **Blindness -> Randomisation**
- **Verifiability -> Trappification (trap qubits)**

Verification of Prepare-and-send Model

	Classical output	Quantum output
Classical input	1. [initialisation] Client initialises each qubit $\|+_\alpha\rangle = \|0\rangle + e^{i\alpha}\|1\rangle$ and sends them to the server	**Measurement-based quantum computation (MBQC)**  Fig. in [Kapourniotis, Kashefi, Leichtle, Music, Ollivier, 2022]
Quantum input	2. [interactive loop] Client sends measurement angle $\tilde{\theta}_v = \theta_v + x_v\pi$ and gets the results from the server	

VBQC [Fitzsimons, Kashefi, 2012]

Verification of Prepare-and-send Model

Classical output

Quantum output

Classical input

Quantum input

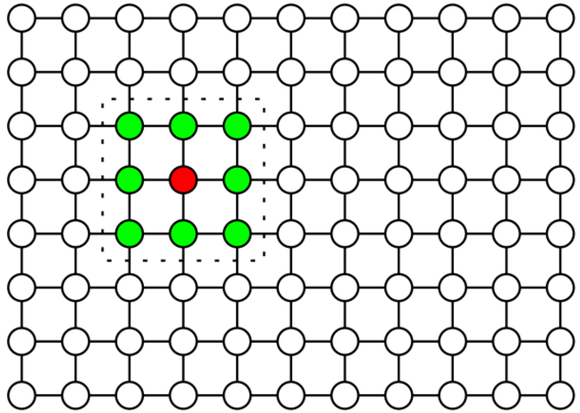


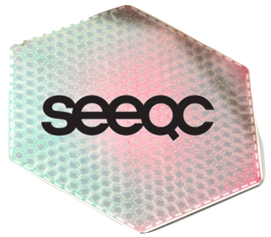
Fig. in [Kapourniotis, Kashefi, Leichtle, Music, Ollivier, 2022]

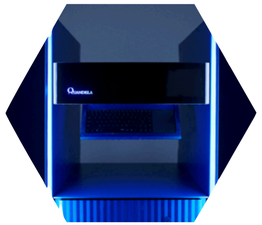
- Require fault-tolerance for the exponential verifiability
- Too sensitive to tolerated noise

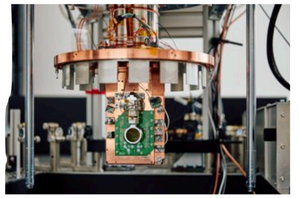
VBQC [Fitzsimons, Kashefi, 2012]

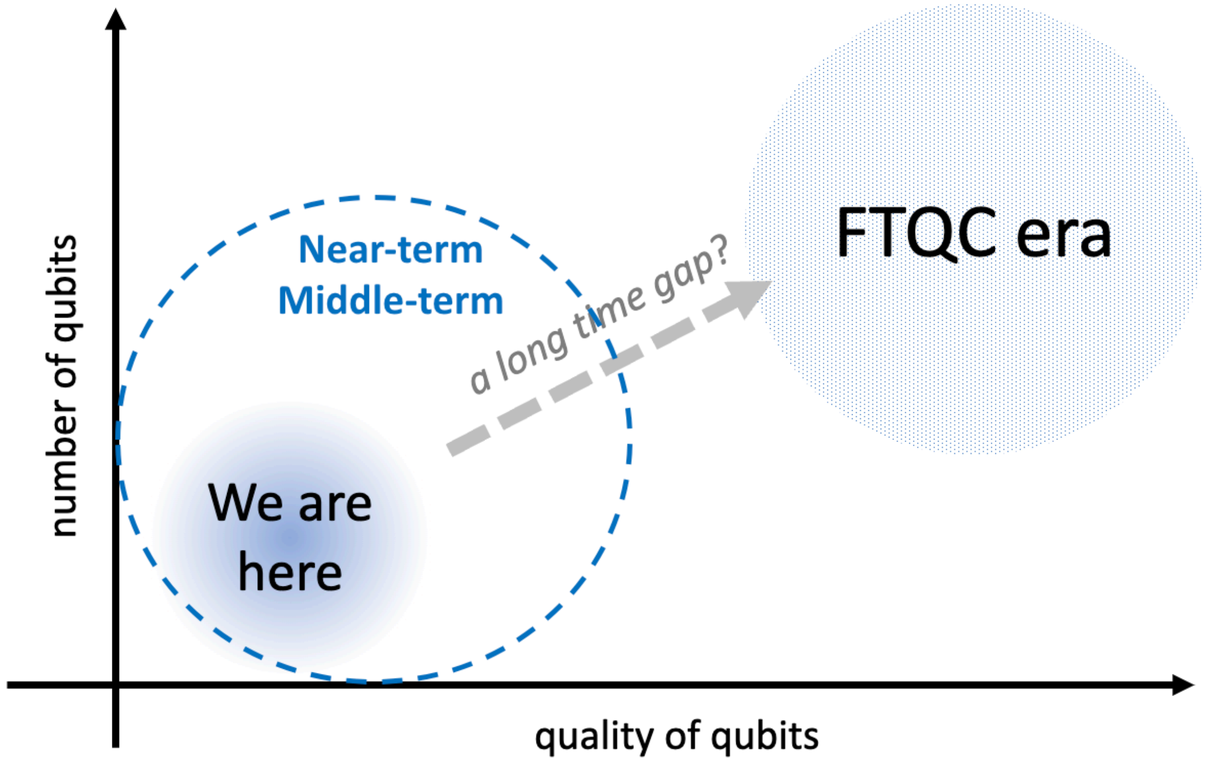
Near-future Devices

Very Limited Fault-tolerance







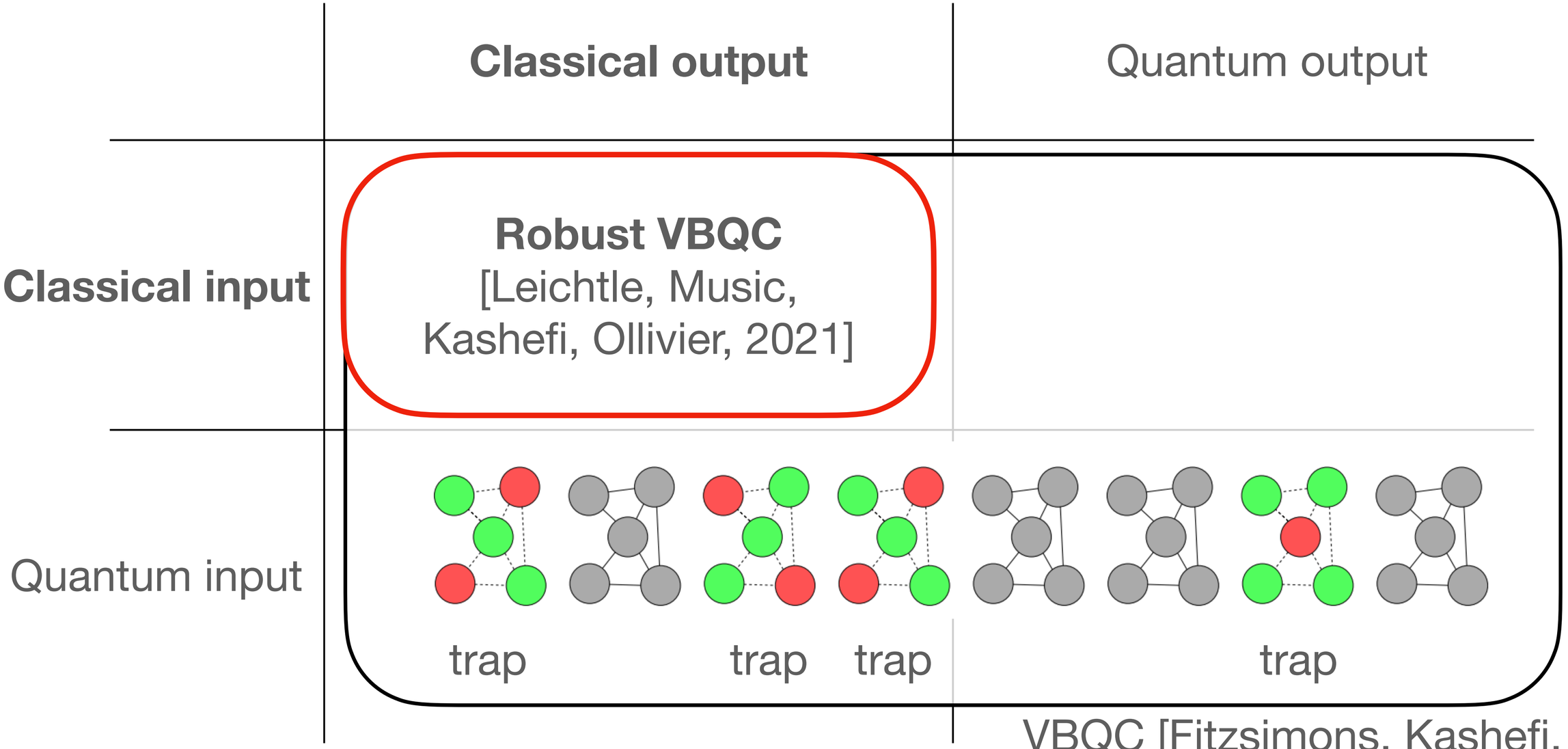


Limited size/connection of qubits
→ Hardware-efficient quantum circuits

Short coherent time
→ Shallow quantum circuits
without intermediate measurement

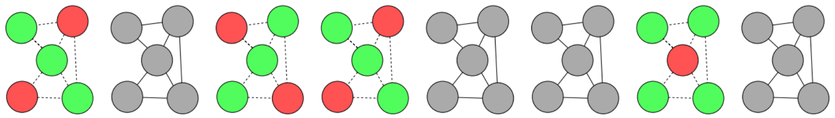
Non-negligible noises
→ Noise-resilient algorithm/circuit design

Robust Verification of Prepare-and-send Model



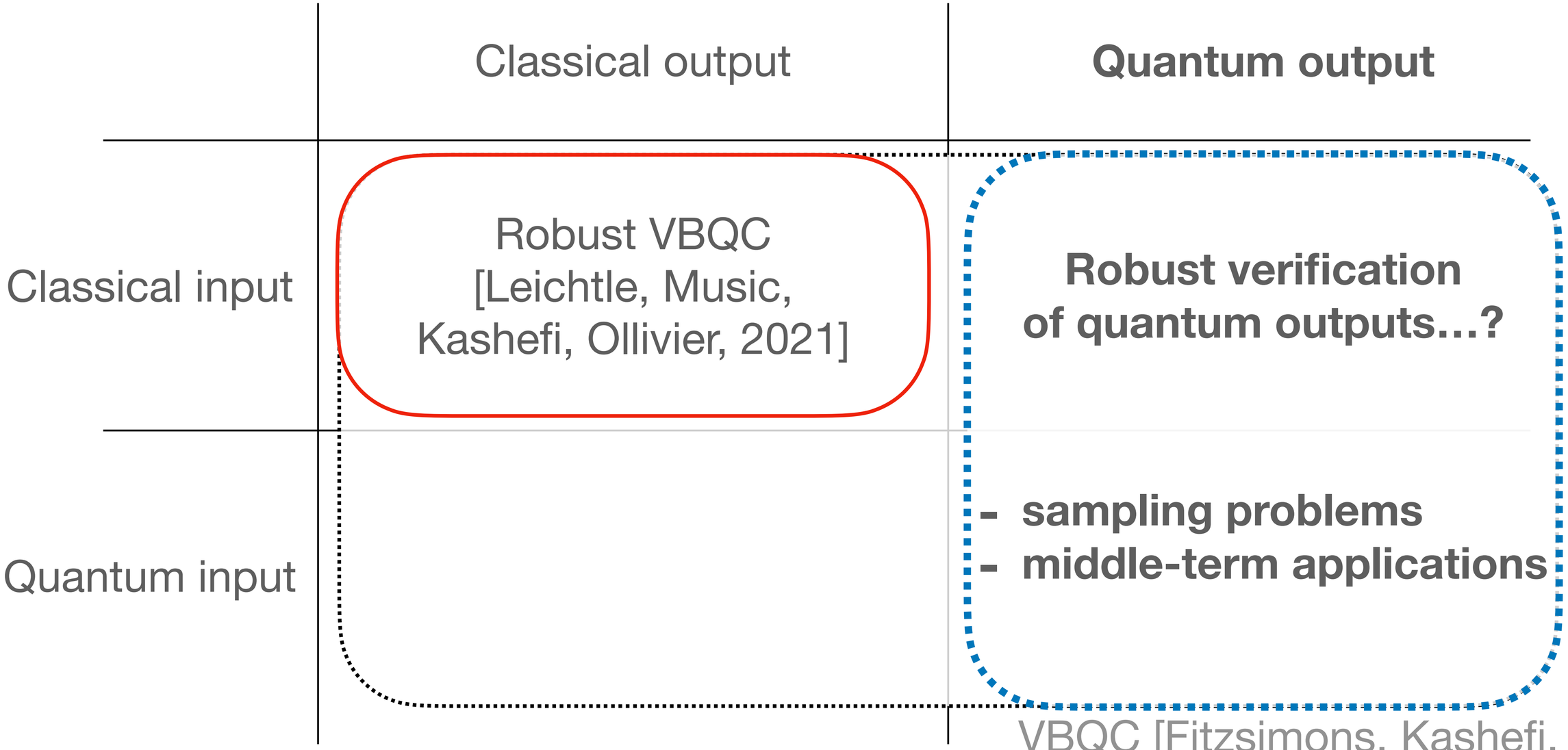
VBQC [Fitzsimons, Kashefi, 2012]

Robust Verification of Prepare-and-send Model

	Classical output	Quantum output
Classical input	**Robust VBQC** [Leichtle, Music, Kashefi, Ollivier, 2021]	
Quantum input	- Robust verification (to harmless errors) - Efficient exponential verifiability by classical majority vote (= without additional qubits)	

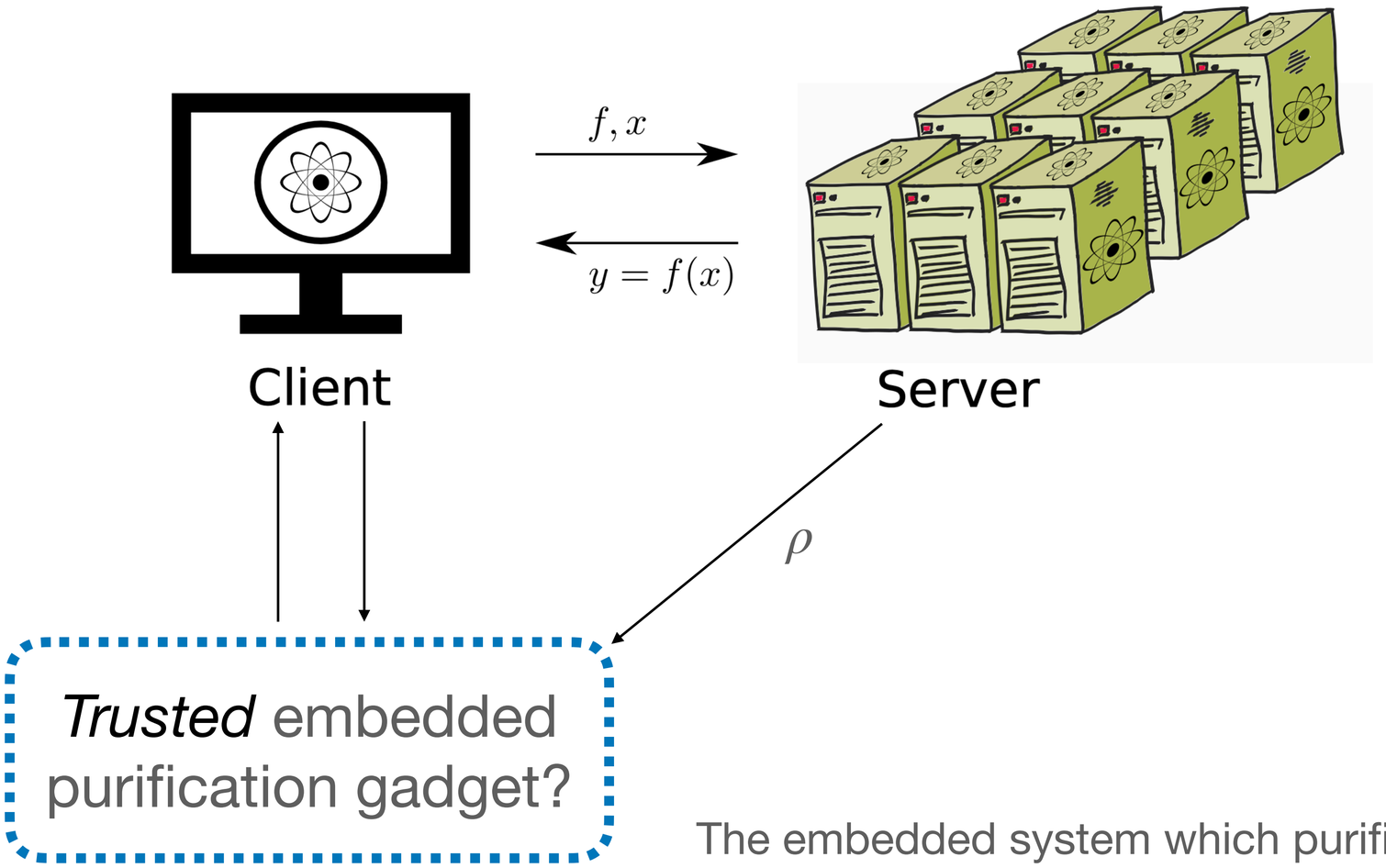
VBQC [Fitzsimons, Kashefi, 2012]

Robust Verification of Quantum Outputs?



Potentially Possible Architecture?

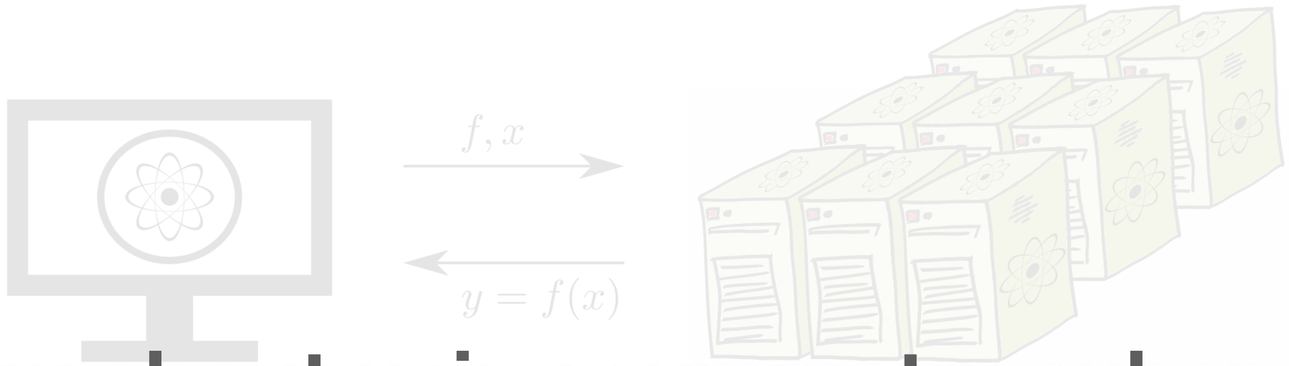
State Purification WITHOUT Fault-tolerance



The embedded system which purifies the quantum states in the same way

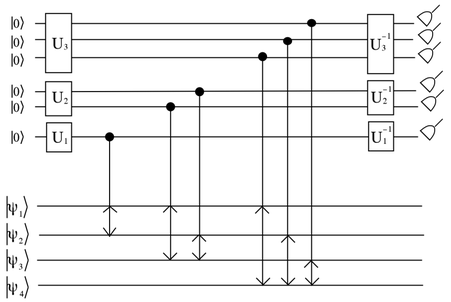
Potentially Possible Architecture?

Drawing on past wisdom for inspiration



How about using symmetry subspace of multiple state copies?

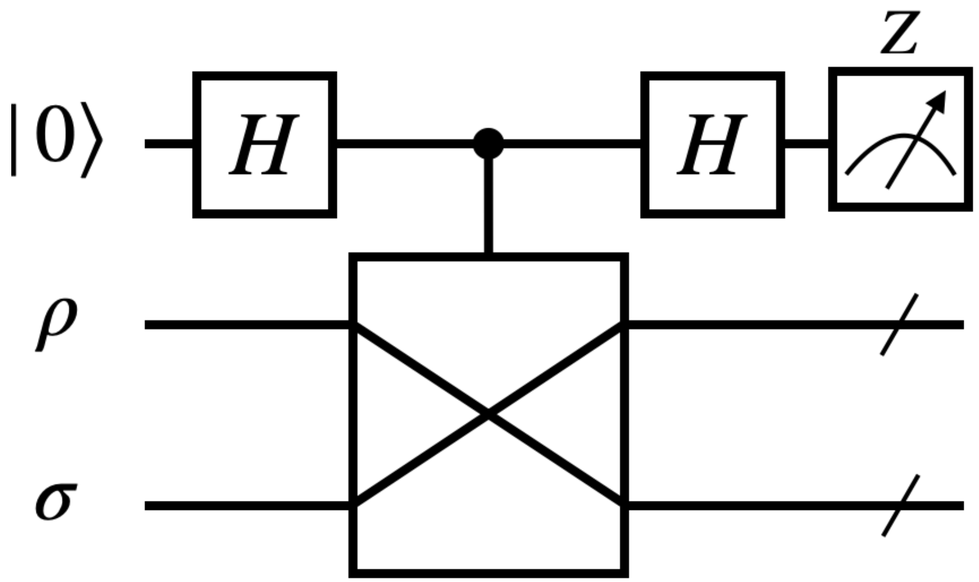
Trusted **embedded purification gadget?**



→ The same idea is also used in Quantum Error Mitigation (QEM)

[Barenco, Berthiaume, Deutsch, Ekert, Jozsa, Macchiavello, 1996]

A Simple Example: SWAP Test



→ **Projector:** $\frac{1}{2}\left(P_{12} \pm P_{21}\right) = \frac{1}{2}(I \pm \mathrm{SWAP})$

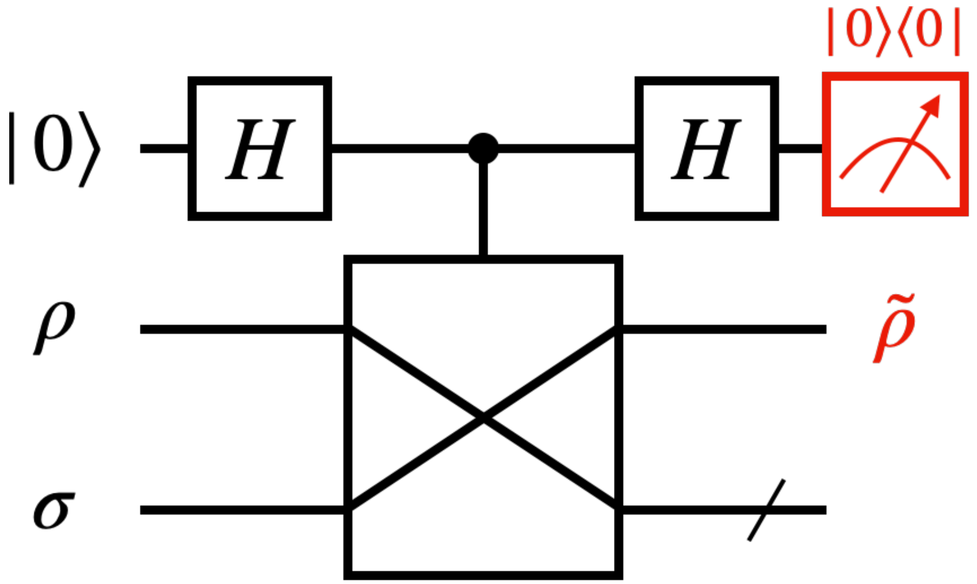
$$\mathrm{P}_0 = \mathrm{Tr}\left[\frac{1}{4}(\rho + \rho\sigma + \sigma\rho + \sigma)\right]$$

$$= \frac{1}{2}\left(1 + \frac{\mathrm{Tr}[\rho\sigma] + \mathrm{Tr}[\sigma\rho]}{2}\right)$$

$$\mathrm{P}_1 = \mathrm{Tr}\left[\frac{1}{4}(\rho - \rho\sigma - \sigma\rho + \sigma)\right]$$

$$= \frac{1}{2}\left(1 - \frac{\mathrm{Tr}[\rho\sigma] + \mathrm{Tr}[\sigma\rho]}{2}\right)$$

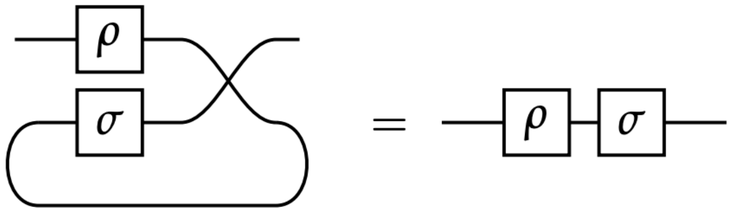
A Simple Example: SWAP Gadget



→ **Projector:** $\frac{1}{2}\left(P_{12}+P_{21}\right)=\frac{1}{2}(I+\mathrm{SWAP})$

$$\mathrm{P}_0=\mathrm{Tr}\left[\frac{1}{4}(\rho+\rho\sigma+\sigma\rho+\sigma)\right]$$

$$=\frac{1}{2}\left(1+\frac{\mathrm{Tr}[\rho\sigma]+\mathrm{Tr}[\sigma\rho]}{2}\right)$$



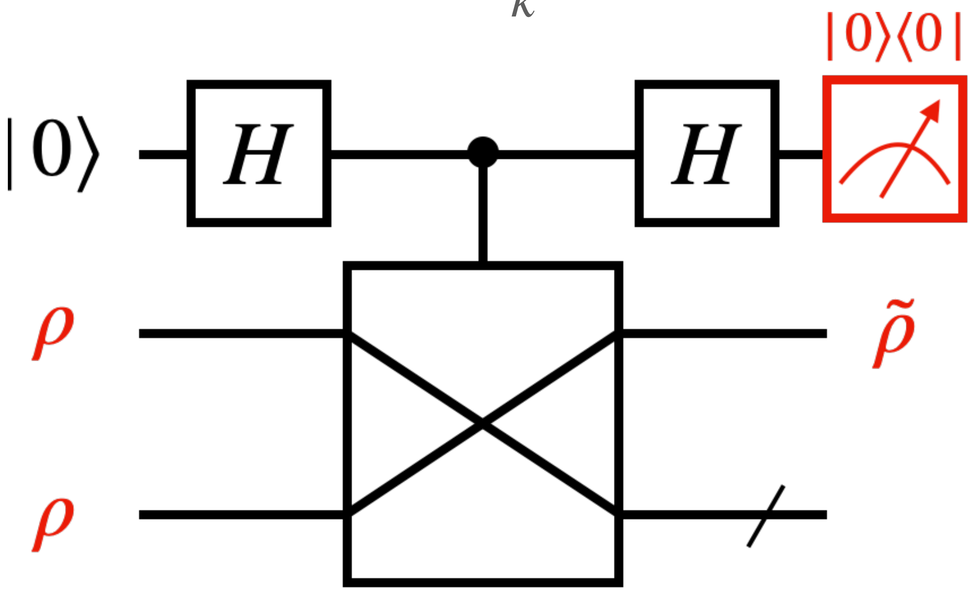
Eq. (5) in [Childs, Fu, Leung, Li, Ozols, Vyas, 2023]

$$\tilde{\rho}=\frac{1}{4\,\mathrm{P}_{\vec{0}}}\mathrm{Tr}_2\left[\left(P_{12}+P_{21}\right)(\rho\otimes\sigma)\left(P_{12}+P_{21}\right)\right]$$

$$=\frac{1}{4\,\mathrm{P}_{\vec{0}}}(\rho+\rho\sigma+\sigma\rho+\sigma)$$

SWAP Gadget for State Purification

When $\rho = \sigma = \sum_k \lambda_k |\lambda_k\rangle\langle\lambda_k|$, with $\lambda_0 > \lambda_1 > \lambda_2 > \cdots$

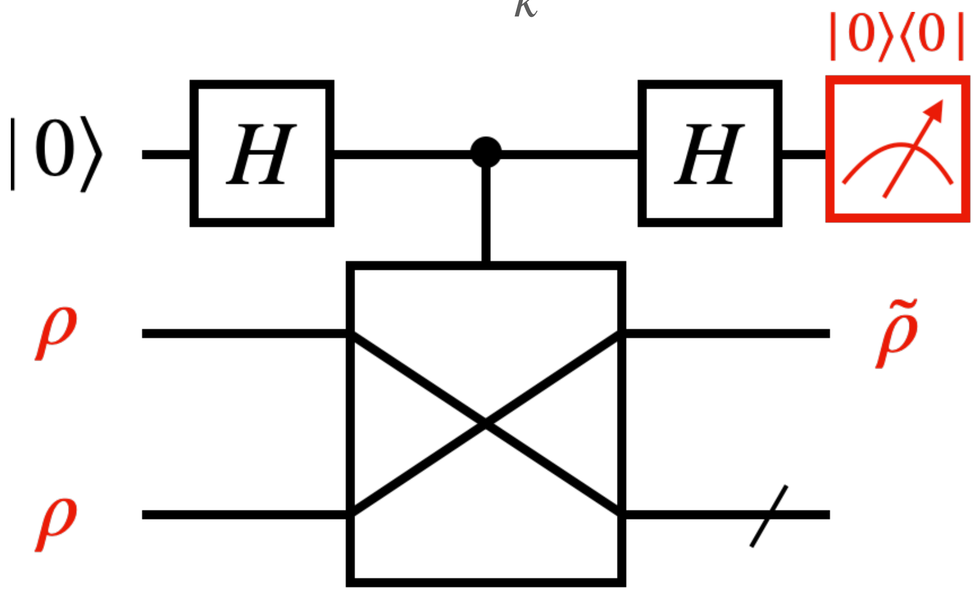


$$P_0 = \frac{1}{2}\left(1 + \mathrm{Tr}\left[\rho^2\right]\right)$$

$$\tilde{\rho} = \frac{1}{P_{\vec{0}}}\frac{\rho + \rho^2}{2} = \frac{\rho + \rho^2}{1 + \mathrm{Tr}\left[\rho^2\right]}$$

SWAP Gadget for State Purification

When $\rho = \sigma = \sum_k \lambda_k |\lambda_k\rangle\langle\lambda_k|$, with $\lambda_0 > \lambda_1 > \lambda_2 > \cdots$



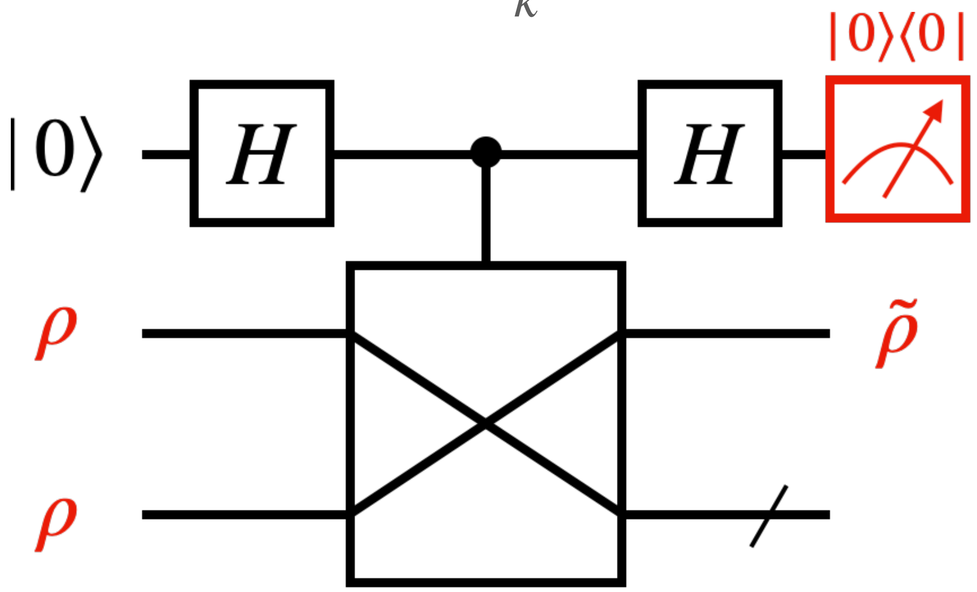
$$P_0 = \frac{1}{2}\left(1 + \mathrm{Tr}\left[\rho^2\right]\right)$$

$$\tilde{\rho} = \frac{1}{P_{\vec{0}}}\frac{\rho + \rho^2}{2} = \frac{\rho + \rho^2}{1 + \mathrm{Tr}\left[\rho^2\right]}$$

$$\rho^2 = \sum_k \lambda_k^2 |\lambda_k\rangle\langle\lambda_k| = \lambda_0^2 \left(|\lambda_0\rangle\langle\lambda_0| + \sum_{k>0} \left(\frac{\lambda_k}{\lambda_0}\right)^2 |\lambda_k\rangle\langle\lambda_k| \right)$$

SWAP Gadget for State Purification

When $\rho = \sigma = \sum_k \lambda_k |\lambda_k\rangle\langle\lambda_k|$, with $\lambda_0 > \lambda_1 > \lambda_2 > \cdots$



$$P_0 = \frac{1}{2}\left(1 + \mathrm{Tr}\left[\rho^2\right]\right)$$

$$\tilde{\rho} = \frac{1}{P_{\vec{0}}}\frac{\rho + \rho^2}{2} = \frac{\rho + \rho^2}{1 + \mathrm{Tr}\left[\rho^2\right]}$$

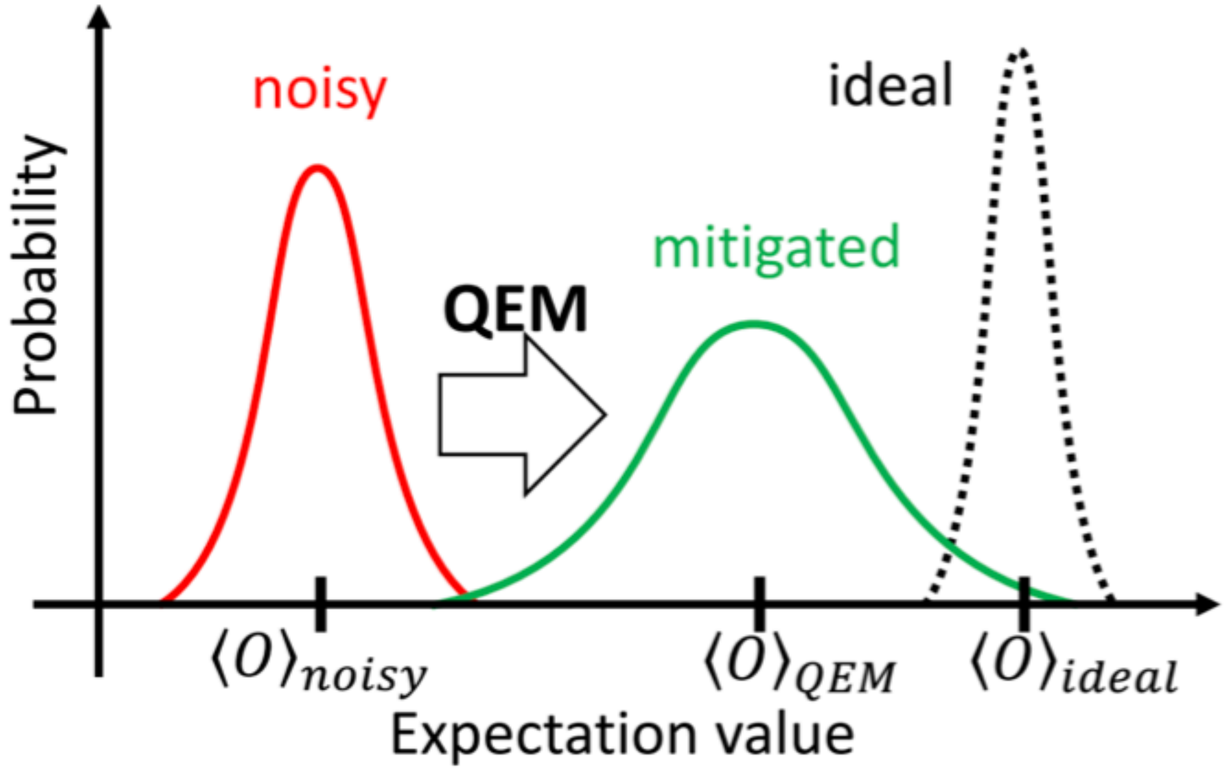
$$\rho^M = \sum_k \lambda_k^M |\lambda_k\rangle\langle\lambda_k| = \lambda_0^M \left(|\lambda_0\rangle\langle\lambda_0| + \sum_{k>0} \left(\frac{\lambda_k}{\lambda_0}\right)^M |\lambda_k\rangle\langle\lambda_k| \right)$$

Suppression of submissive eigenvectors

Application in Quantum Error Mitigation

QEM: Classical postprocessing
to improve expectation values

$$\langle O \rangle_{\mathrm{ESD}} = \frac{\mathrm{Tr}\left[\rho^M O\right]}{\mathrm{Tr}\left[\rho^M\right]}$$ [Koczor, 2021], [Huggins et al., 2021]



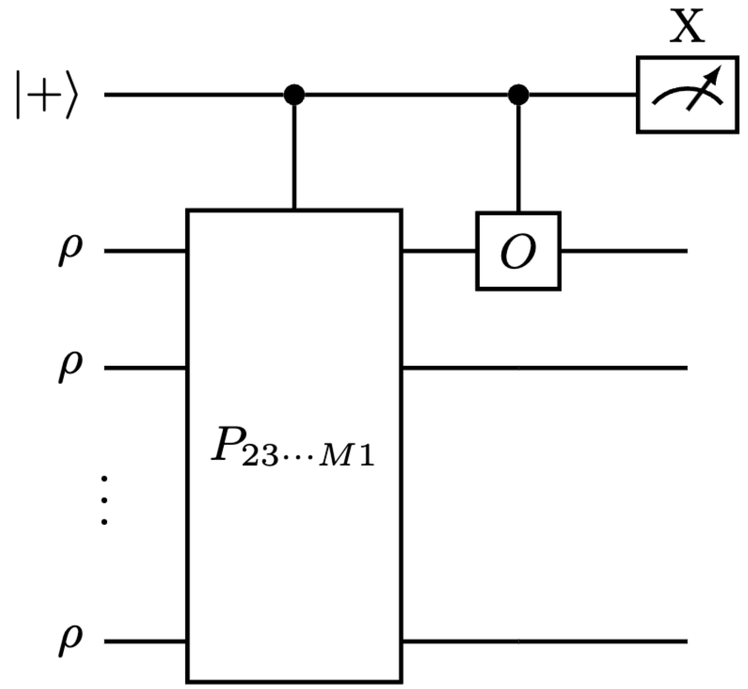


Fig. 2(a) from [Yang et al., 2023]

Application in Quantum Error Mitigation

$$\langle O \rangle_{\mathrm{ESD}} = \frac{\mathrm{Tr}\left[\rho^M O\right]}{\mathrm{Tr}\left[\rho^M\right]}$$

[Koczor, 2021],
[Huggins et al., 2021]

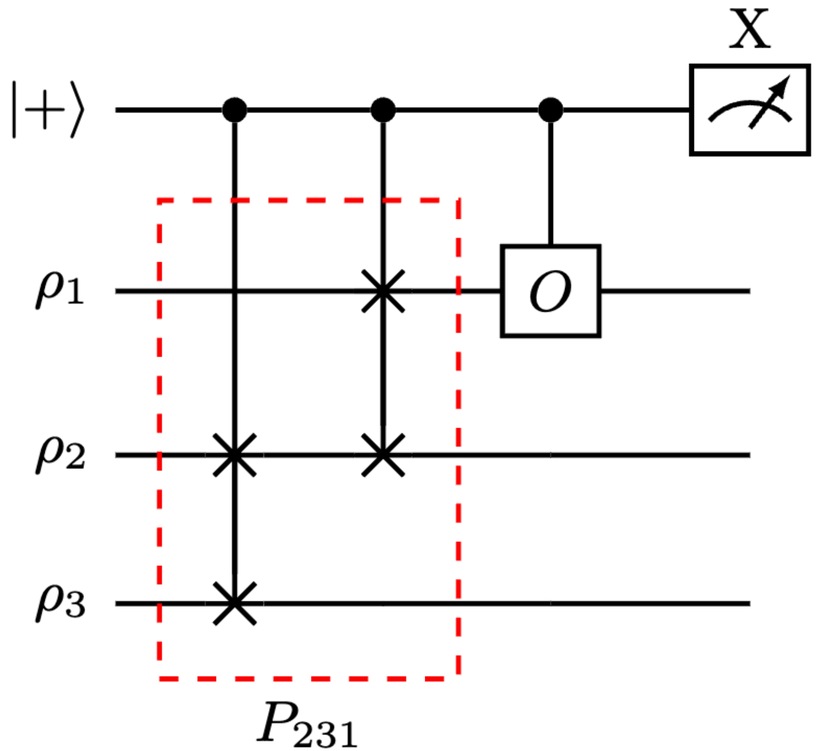


Fig. 2(b) from [Yang et al., 2023]

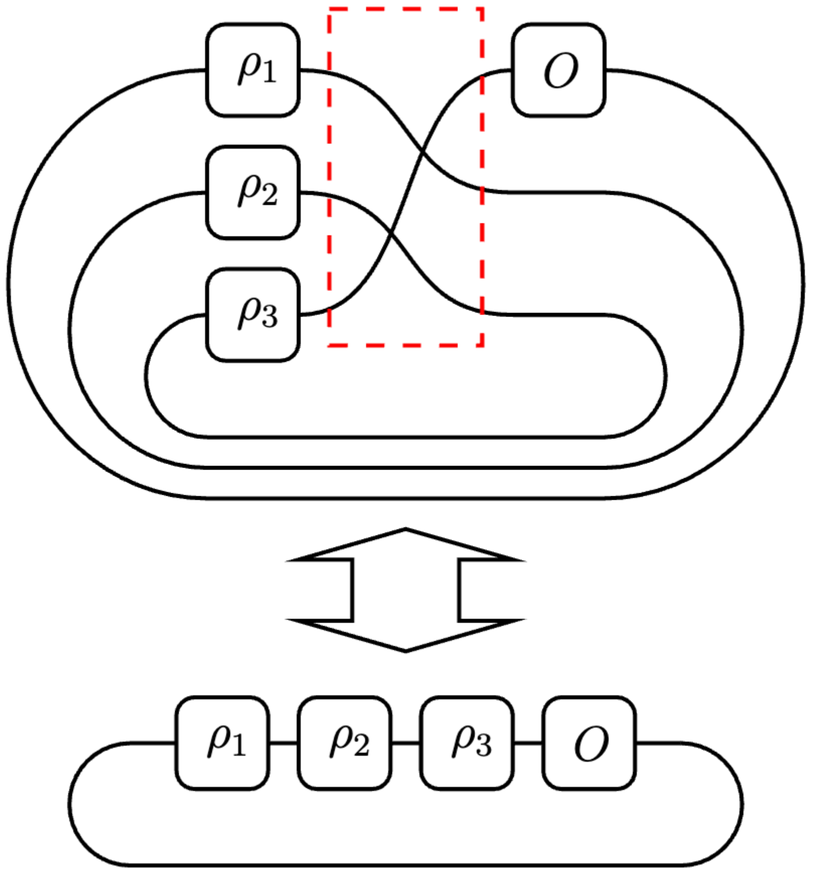
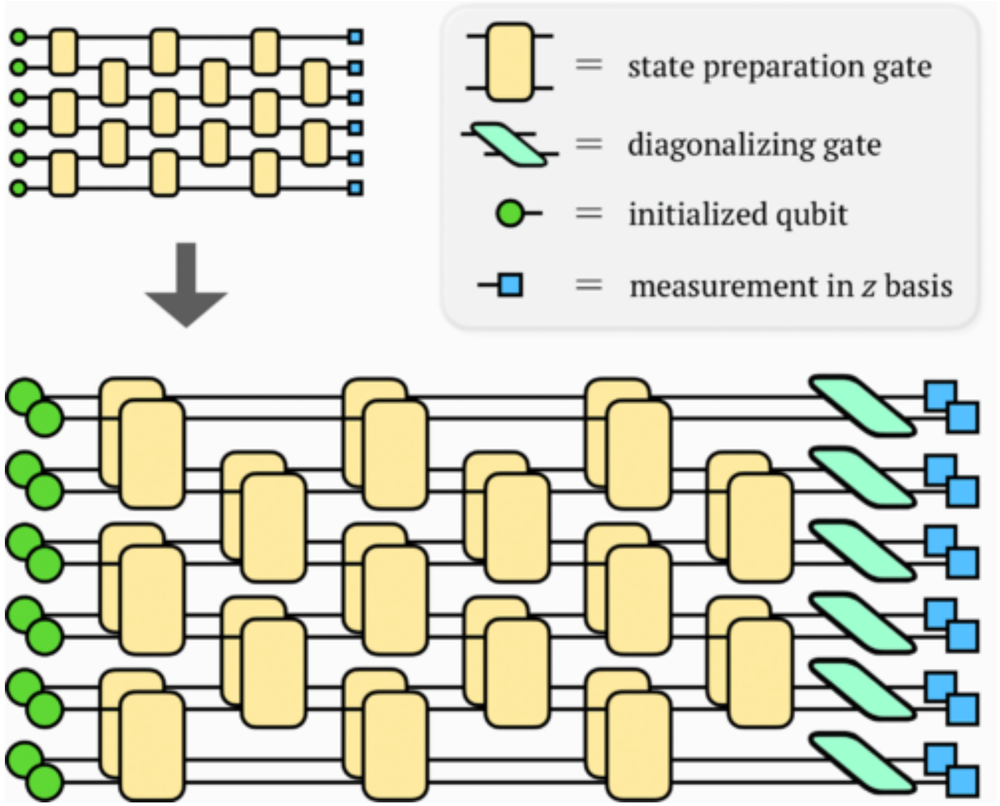
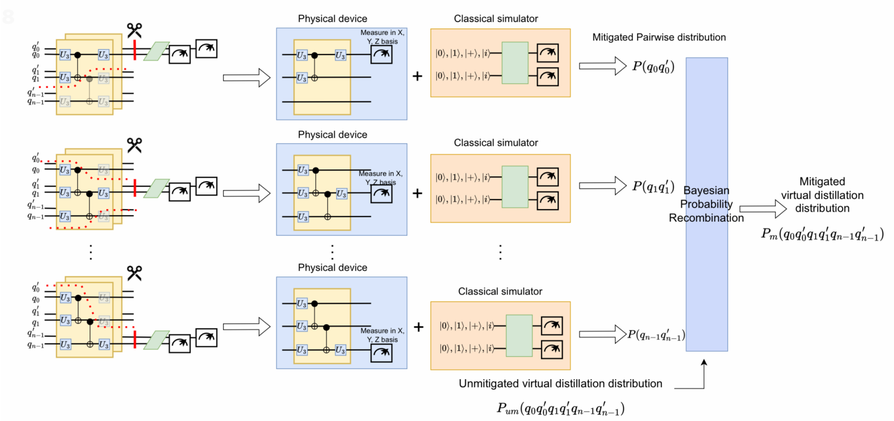


Fig. 2(c) from [Yang et al., 2023]

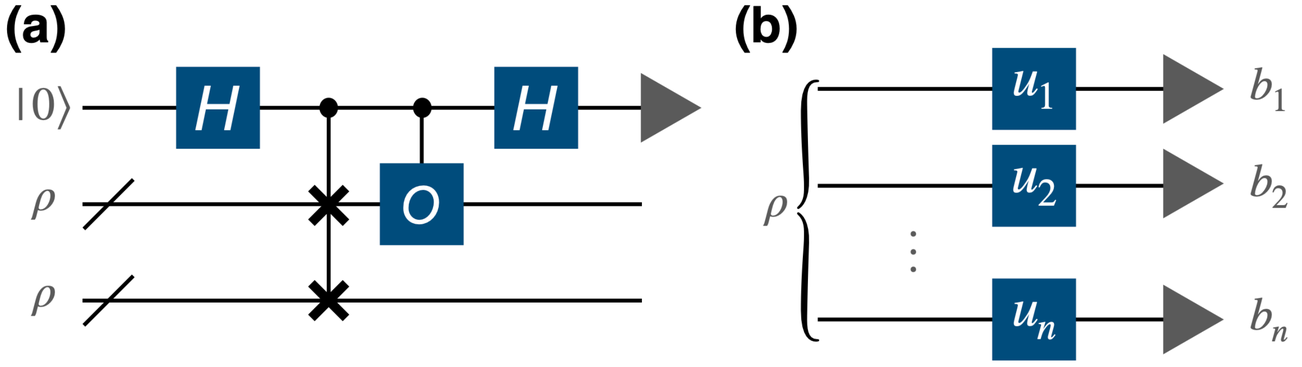
Resource-efficient Implementation of $\mathrm{Tr}\left[\rho^M\right]$



Virtual Distillation (VD)
[Huggins et al., 2021]

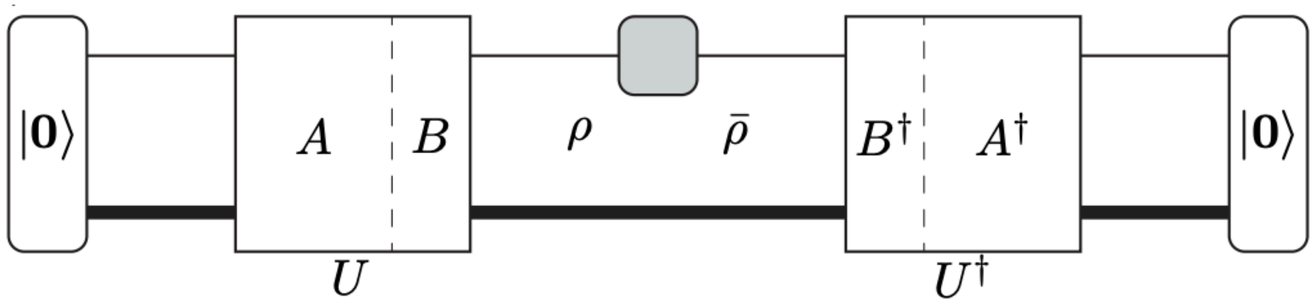


Circuit-cut for VD [Li et al., 2023]



Shadow Distillation
[Seif et al., 2023]

Resource-efficient Implementation of $\mathrm{Tr}\left[\rho^M\right]$

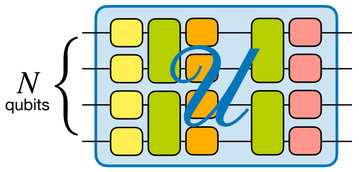


Dual-state Purification
[Huo and Li, 2021]

Implementation of $\mathrm{Tr}\left[\rho^2\right]$
without state copies.

Input
(Noisy state)

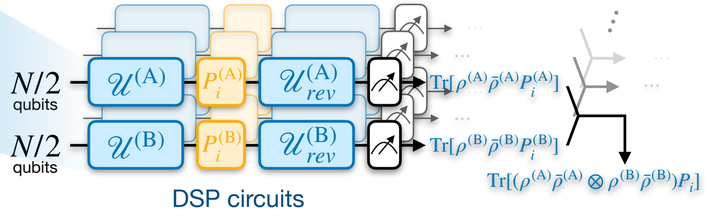
$\rho = \mathcal{U}(\rho_{\vec{0}})$



Dual-GSE (with Divide-and-conquer Subspace)

Quantum process (Mitigation circuits)

$$\rho_{\mathrm{DGSE}} = \cdots + \sum_{i,j\geq 2} \alpha_i^* \alpha_j H^{i-2}(\rho^{(\mathrm{A})}\bar{\rho}^{(\mathrm{A})} \otimes \rho^{(\mathrm{B})}\bar{\rho}^{(\mathrm{B})})H^{j-2}$$



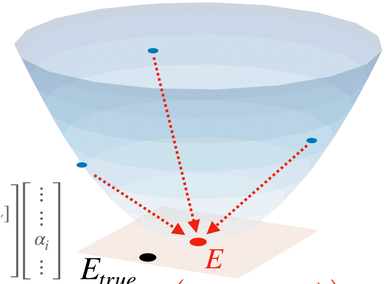
DSP circuits

Classical postprocessing

$$E = \min_{\vec{\alpha}} \mathrm{Tr}[H\rho_{\mathrm{QSE}}(\vec{\alpha})]$$
subject to $\mathrm{Tr}[\rho_{\mathrm{QSE}}(\vec{\alpha})] = 1$

$$\begin{bmatrix} \cdots & \cdots \\ \mathrm{Tr}[\rho P_i H P_j] & \cdots \\ \vdots & \end{bmatrix} \begin{bmatrix} \vdots \\ \alpha_i \\ \vdots \end{bmatrix} = E \begin{bmatrix} \cdots & \cdots \\ \mathrm{Tr}[\rho P_i P_{j'}] & \cdots \\ \vdots & \end{bmatrix} \begin{bmatrix} \vdots \\ \alpha_i \\ \vdots \end{bmatrix}$$

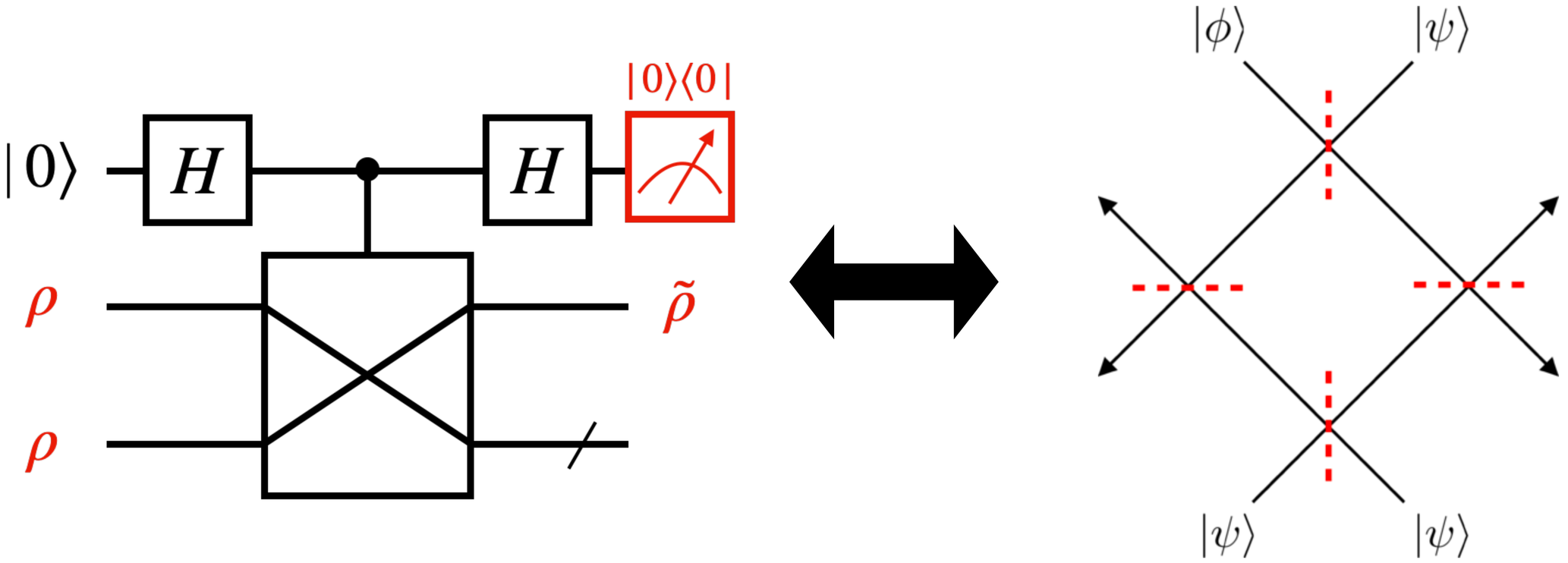
$$\mathcal{H}\vec{\alpha} = E\mathcal{S}\vec{\alpha}$$



Further resource-efficient implementation [Yang et al., 2023]

Implementation of SWAP Gadget

Compatibility with Photonic Platforms



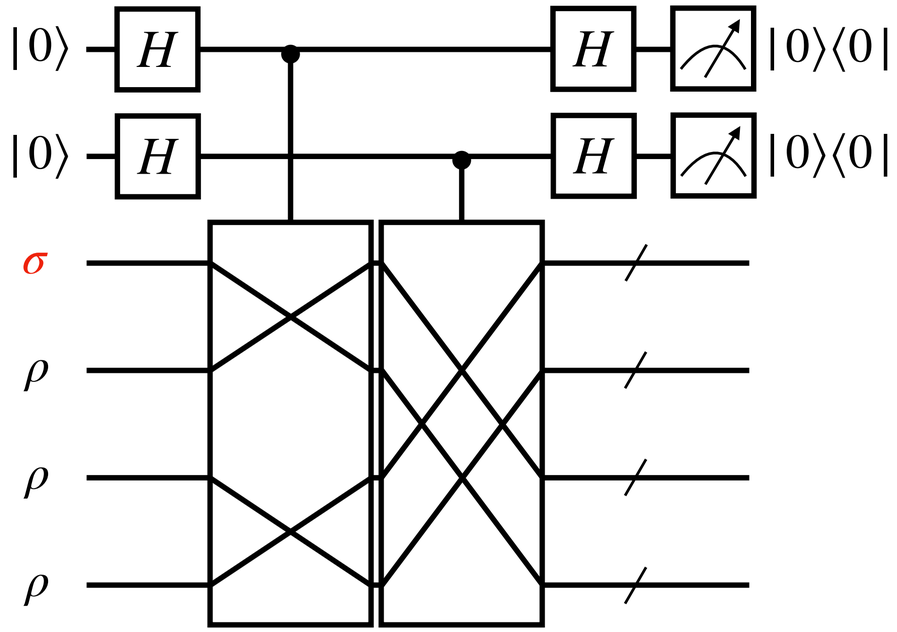
- Use of ancillary qubits
- Heavy controlled operations

passive linear optics: a simple interferometer composed only of balanced beam splitters

Fig. 6 in [Chabaud, Diamanti, Markham, Kashefi, Joux, 2018]

Generalised SWAP Gadget

[Chabaud, Diamanti, Markham, Kashefi, Joux, 2018]



→ Projector: $P_{\mathrm{GSG}} = \dfrac{1}{|\mathscr{F}|} \sum_{\sigma \in \mathscr{F}} P_\sigma$

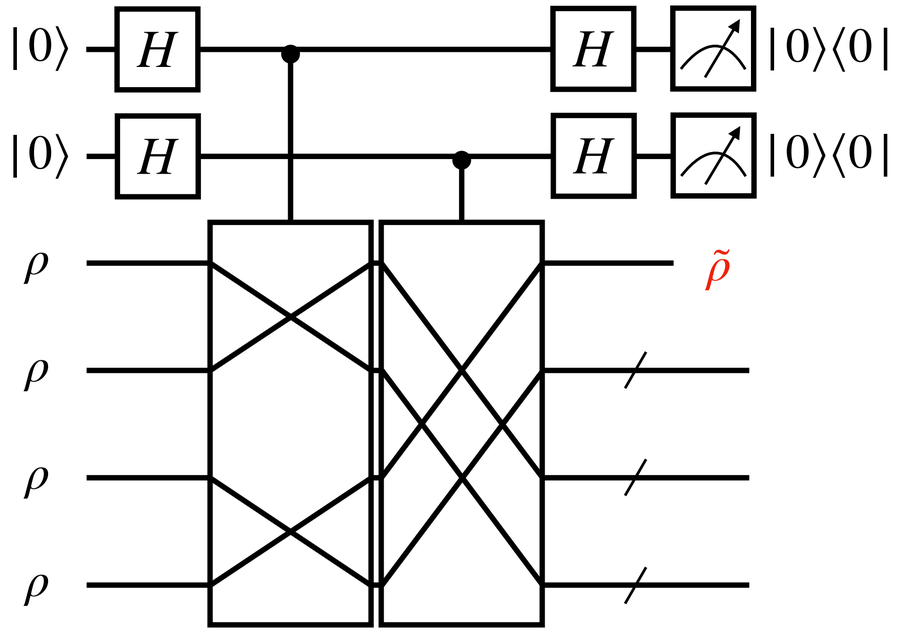
$\mathscr{F} = \{\text{Pairwise swap operations in FFT}\}$

$$\mathrm{P}_{\vec{0}} = \frac{1}{M} + \frac{M-1}{M} \mathrm{Tr}\left[\rho^2\right]^{\frac{M}{2}-1} \mathrm{Tr}\left[\sigma\rho\right]$$

$$= \frac{1}{M} + \frac{M-1}{M} |\langle\psi|\phi\rangle|^2$$

Generalised SWAP Gadget

[Chabaud, Diamanti, Markham, Kashefi, Joux, 2018]



→ Projector: $P_{\mathrm{GSG}} = \dfrac{1}{|\mathscr{F}|} \sum_{\sigma \in \mathscr{F}} P_\sigma$

$\mathscr{F} = \{\text{Pairwise swap operations in FFT}\}$

$$\mathrm{P}_{\vec{0}} = \frac{1}{M} + \frac{M-1}{M} \mathrm{Tr}\left[\rho^2\right]^{\frac{M}{2}}$$

$$\mathrm{P}_{\vec{0}}\tilde{\rho} = \frac{1}{M}\rho + \frac{M-1}{M} \mathrm{Tr}\left[\rho^2\right]^{\frac{M}{2}-1} \rho^2$$

Why Not Projecting into the Full Symmetry Subspace?

[Barenco et al., 1996]

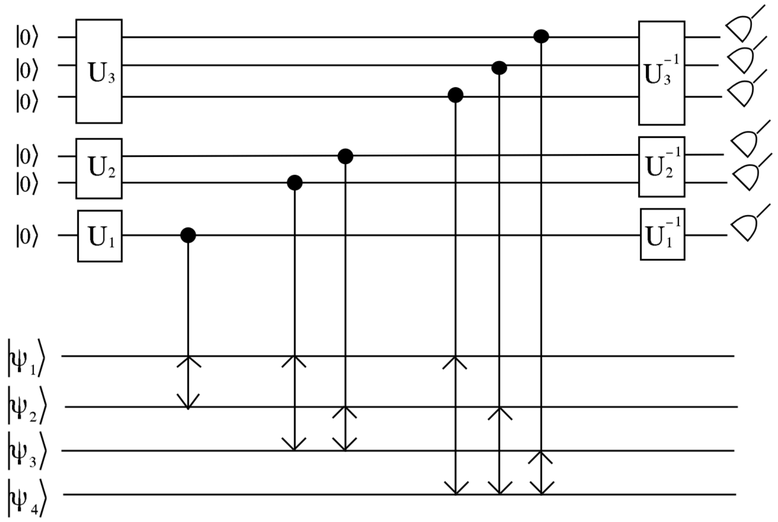
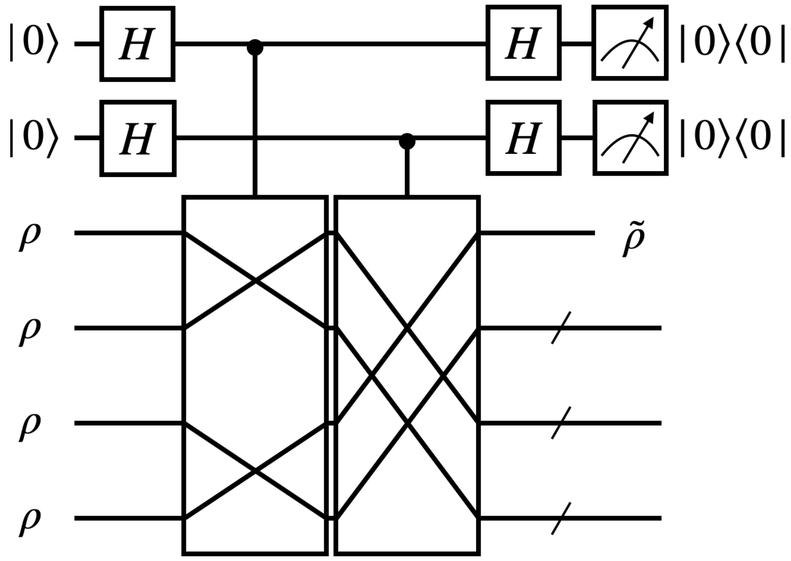


Fig. 2 in [Barenco et al., 1996]

$$P_{\mathrm{SYM}} = \frac{1}{M!} \sum_{\sigma \in \mathcal{S}} P_\sigma$$

TOO COMPLICATED

[Chabaud et al., 2018]



$$P_{\mathrm{GSG}} = \frac{1}{\log(M)} \sum_{\sigma \in \mathcal{F}} P_\sigma$$

$$\frac{1}{M}\rho + \frac{M-1}{M} \mathrm{Tr}\left[\rho^2\right]^{\frac{M}{2}-1} \rho^2$$

[Koczor, 2021]

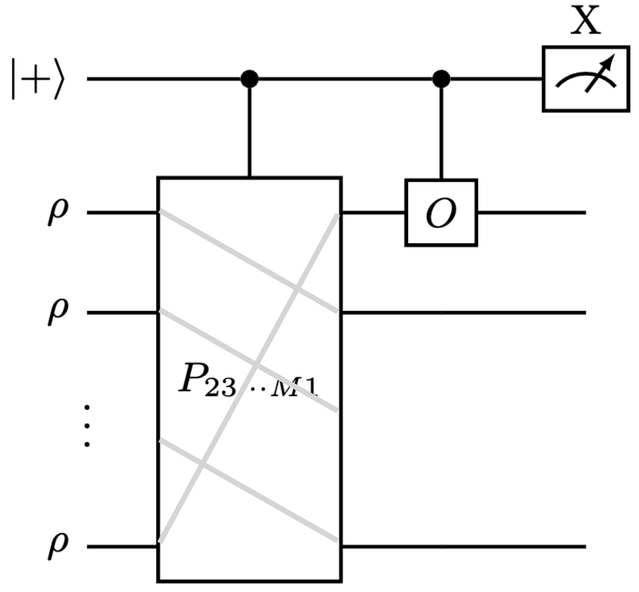


Fig. 2(a) from [Yang et al., 2023]

$$P_{\mathrm{ESD}} = \frac{1}{2}\left(I + P_{23\cdots M1}\right)$$

$$\frac{1}{2}\left(\rho + \rho^M\right)$$

Why Not Projecting into the Full Symmetry Subspace?

[Barenco et al., 1996]

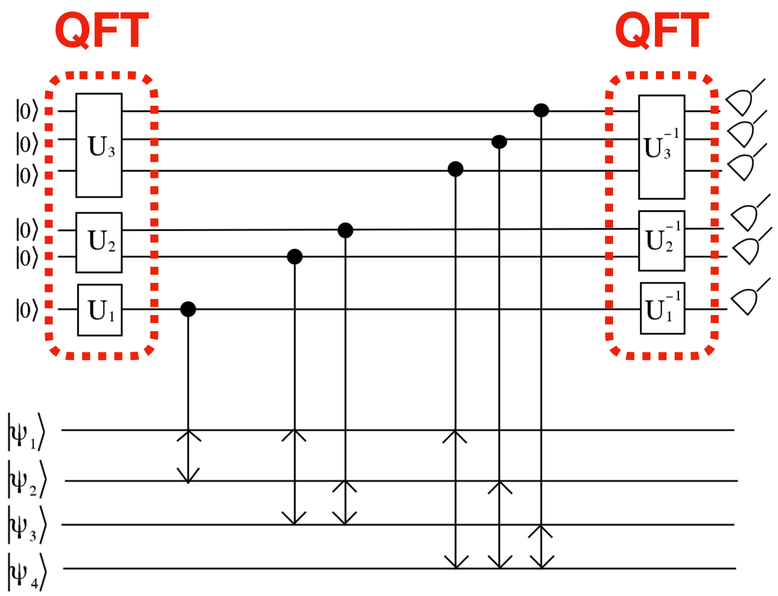
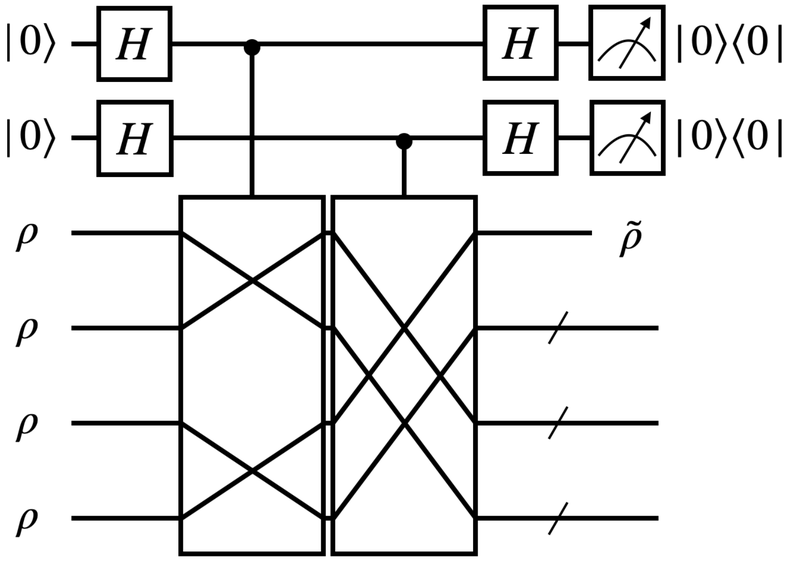


Fig. 2 in [Barenco et al., 1996]

$$P_{\mathrm{SYM}} = \frac{1}{M!} \sum_{\sigma \in \mathcal{S}} P_\sigma$$

TOO COMPLICATED

[Chabaud et al., 2018]



$$P_{\mathrm{GSG}} = \frac{1}{\log(M)} \sum_{\sigma \in \mathcal{F}} P_\sigma$$

$$\frac{1}{M}\rho + \frac{M-1}{M} \mathrm{Tr}\left[\rho^2\right]^{\frac{M}{2}-1} \rho^2$$

[Koczor, 2021]

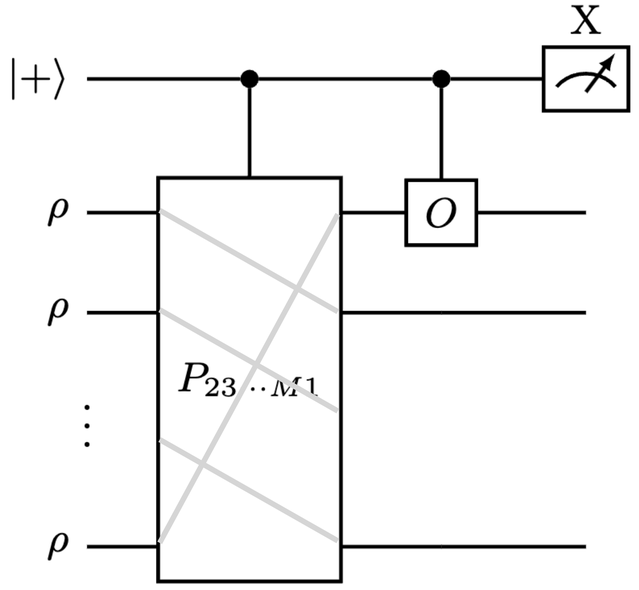


Fig. 2(a) from [Yang et al., 2023]

$$P_{\mathrm{ESD}} = \frac{1}{2}\left(I + P_{23\cdots M1}\right)$$

$$\frac{1}{2}\left(\rho + \rho^M\right)$$

What Decides the Purification Quality?

[Barenco et al., 1996]

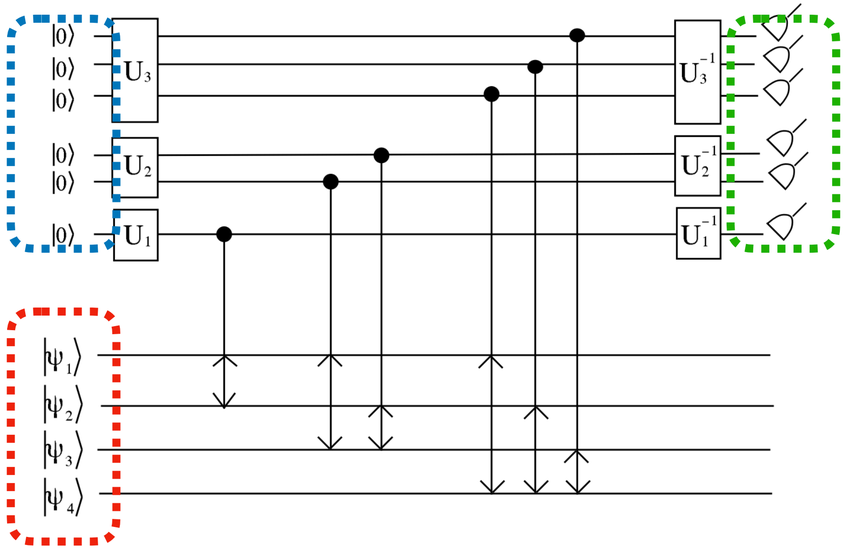
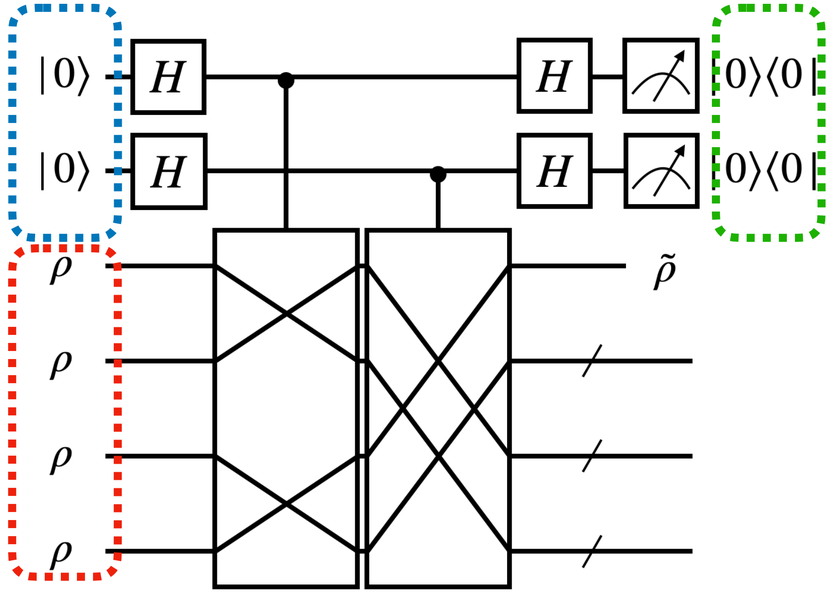


Fig. 2 in [Barenco et al., 1996]

[Chabaud et al., 2018]



[Koczor, 2021]

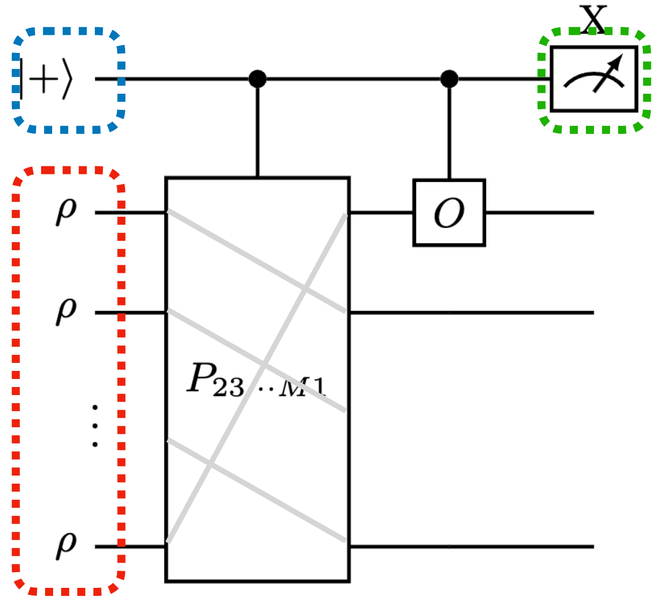


Fig. 2(a) from [Yang et al., 2023]

1. **The number of ancillary qubits**
   (= the number of superpositions for different projectors)
2. **The number of copies (which upper bounds the power degree of ρ)**
3. **The range of states to be post-selected**

Any Sweet Spot?

Better and practical projectors???

[Barenco et al., 1996]

[Chabaud et al., 2018]

[Koczor, 2021]

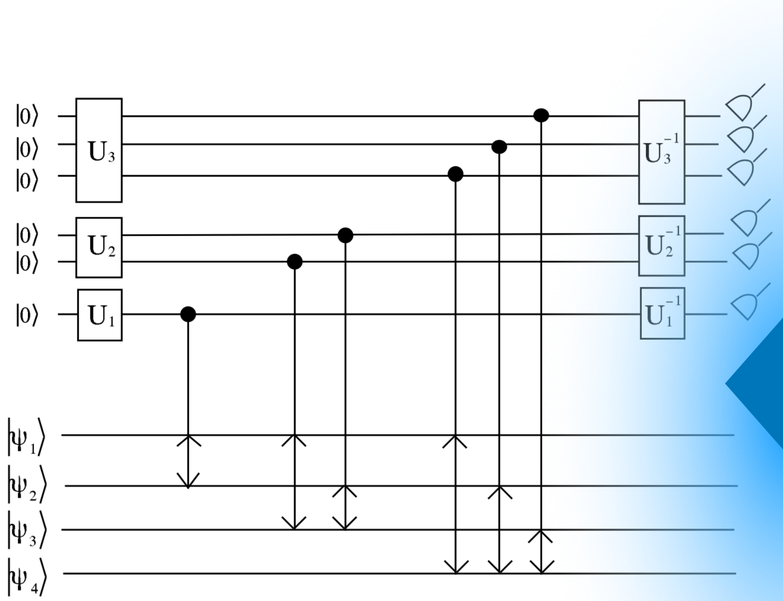
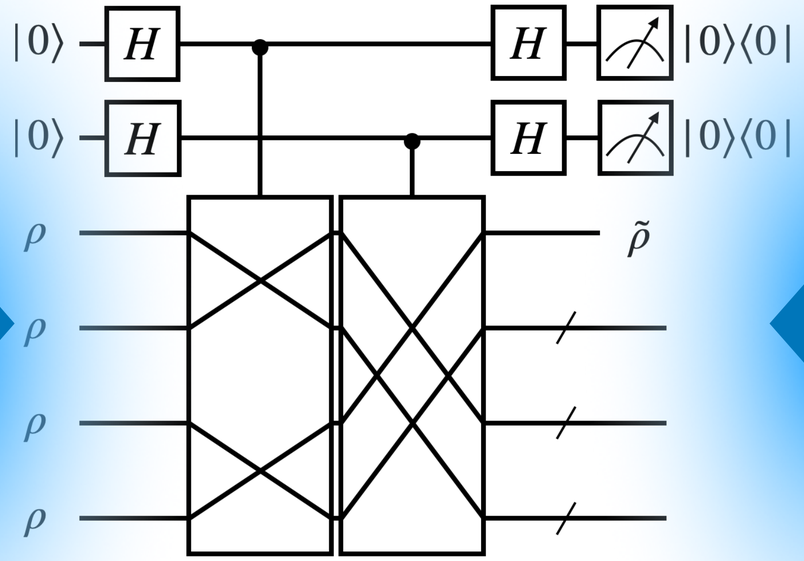


Fig. 2 in [Barenco et al., 1996]



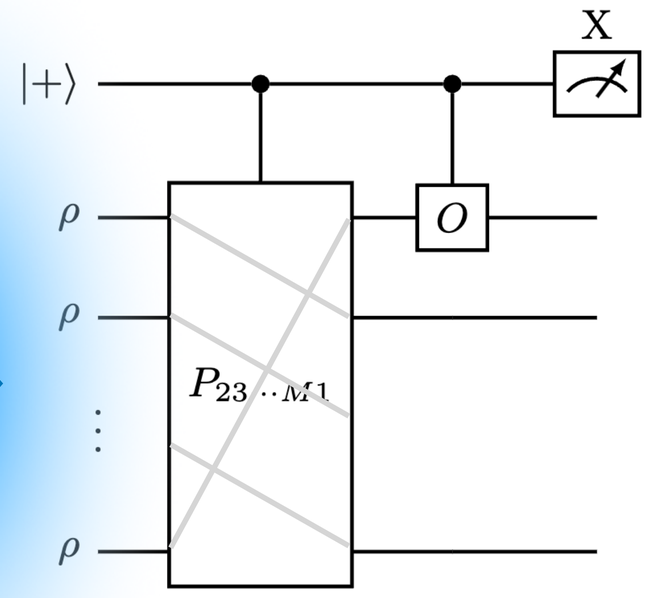


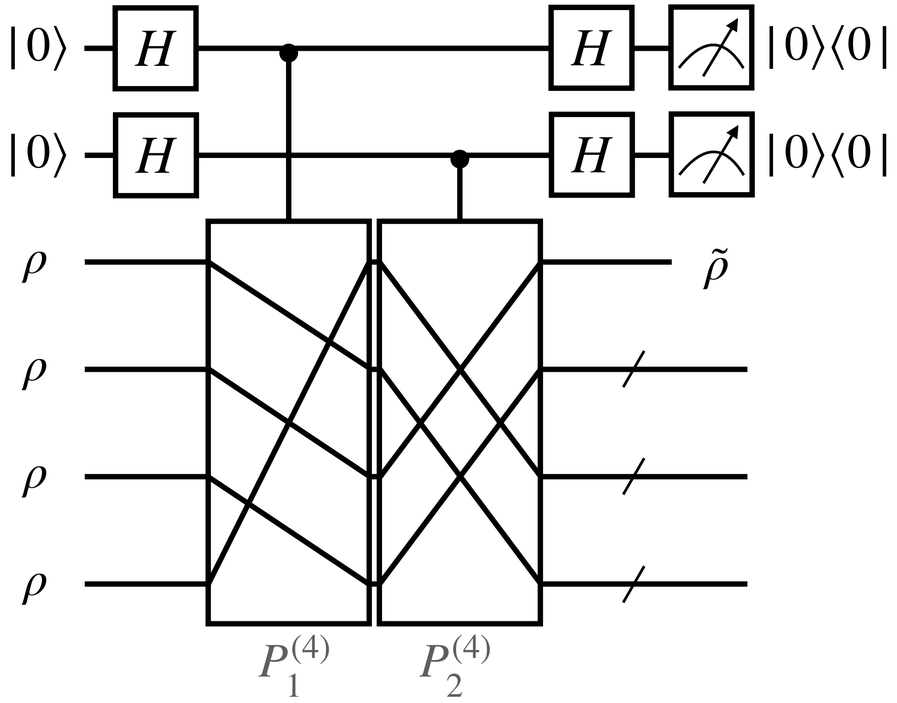
Fig. 2(a) from [Yang et al., 2023]

1. **The number of ancillary qubits**
   (= the number of superpositions for different projectors)
2. **The number of copies (which upper bounds the power degree of ρ)**
3. **The range of states to be post-selected**

[Our Proposal] (Members: Bo, Dominik, Elham, and Harold)

Cyclic Group Gadget

C_M : cyclic group with order M



→ Projector: $P_{\mathrm{CGG}} = \dfrac{1}{|C_M|} \sum_{\sigma \in C_M} P_\sigma^{(M)}$

$$\mathrm{P}_{\vec{0}} = \frac{1}{M} \sum_{k|M} \varphi(k) \mathrm{Tr}\left[\rho^k\right]^{\frac{M}{k}}$$

$$\mathrm{P}_{\vec{0}} \tilde{\rho} = \mathrm{Tr}_{2\ldots M}\left[\left(\frac{1}{M} \sum_{P_i \in C_M} P_i\right)\left(\rho^{\otimes M}\right)\left(\frac{1}{M} \sum_{P_i \in C_M} P_i^\dagger\right)\right]$$

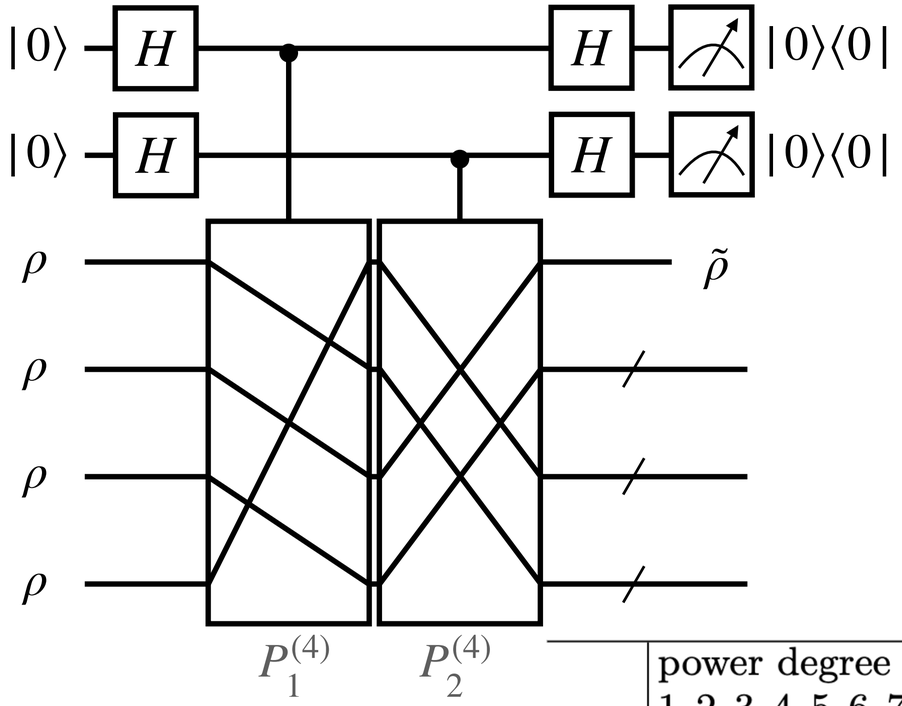
$$= \frac{1}{M} \sum_{k|M} \varphi(k) \mathrm{Tr}\left[\rho^k\right]^{\frac{M}{k}-1} \rho^k$$

$\varphi(k)$: Euler's totient function

[Our Proposal]

Cyclic Group Gadget

C_M : cyclic group with order M



→ Projector: $P_{\mathrm{CGG}} = \dfrac{1}{|C_M|} \sum_{\sigma \in C_M} P_\sigma^{(M)}$

$$\mathrm{P}_{\vec{0}} = \frac{1}{M} \sum_{k|M} \varphi(k) \mathrm{Tr}\left[\rho^k\right]^{\frac{M}{k}}$$

$$\mathrm{P}_{\vec{0}} \tilde{\rho} = \mathrm{Tr}_{2\ldots M}\left[\left(\frac{1}{M} \sum_{P_i \in C_M} P_i\right)\left(\rho^{\otimes M}\right)\left(\frac{1}{M} \sum_{P_i \in C_M} P_i^\dagger\right)\right]$$

$$= \frac{1}{M} \sum_{k|M} \varphi(k) \mathrm{Tr}\left[\rho^k\right]^{\frac{M}{k}-1} \rho^k$$

$\varphi(k)$: Euler's totient function

M \ power degree of ρ	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1		2					
4	1	1		2				
5	1				4			
6	1	1	2			2		
7	1						6	
8	1	1		2				4

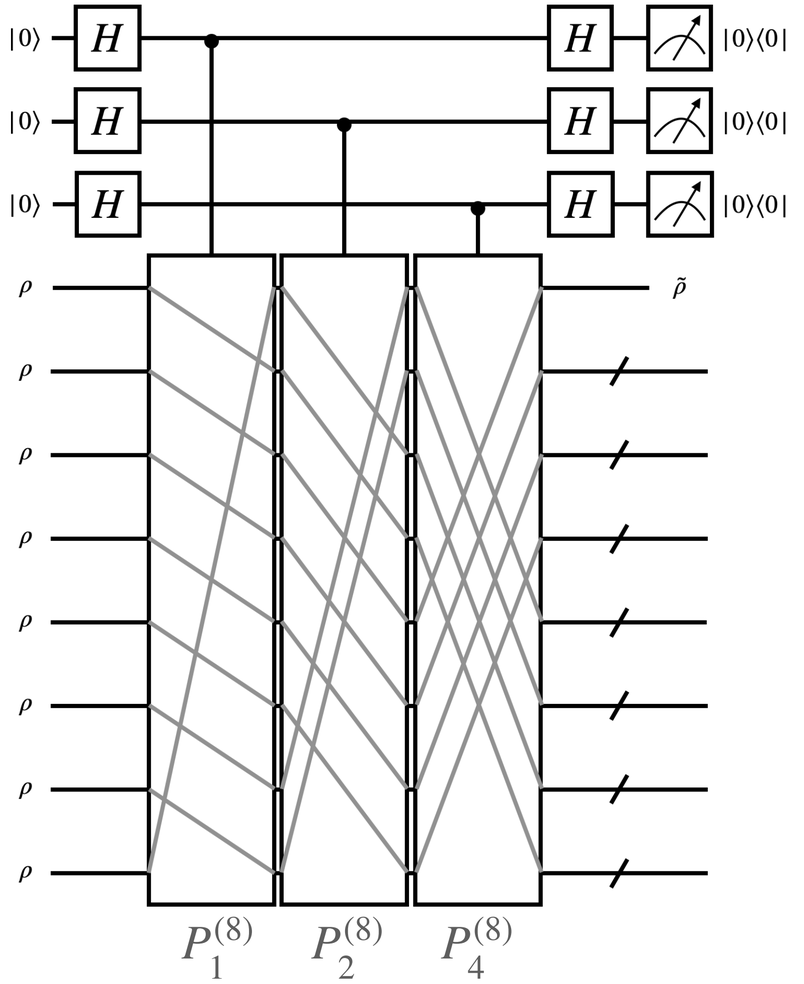
[Our proposal]

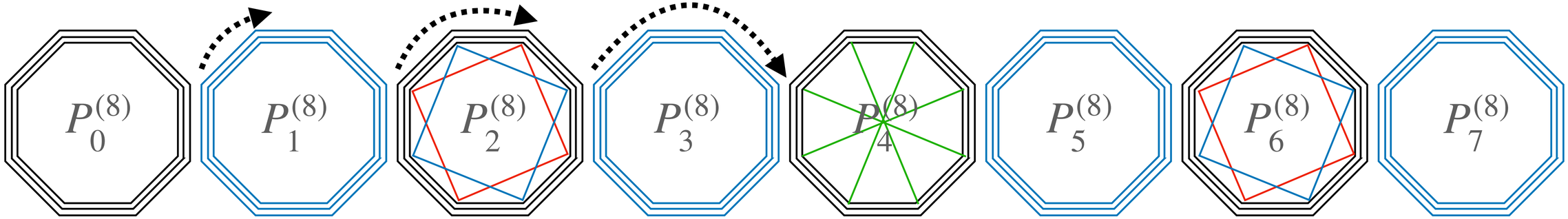
Example: $M = 8$

$$\text{Projector: } P_{\mathrm{CGG}} = \frac{1}{8} \sum_{\sigma \in C_8} P_{\sigma}^{(M)}$$

$$\mathrm{P}_{\vec{0}}\tilde{\rho} = \frac{1}{8}\rho + \frac{1}{8} \sum_{i=1}^{3} 2^{i-1} \operatorname{Tr}\left[\rho^{2^i}\right]^{2^{3-i}-1} \rho^{2^i}$$

$$= \frac{1}{8}\left(\rho + \operatorname{Tr}\left[\rho^2\right]^3 \rho^2 + 2\operatorname{Tr}\left[\rho^4\right]\rho^4 + 4\rho^8\right)$$





[Our proposal]

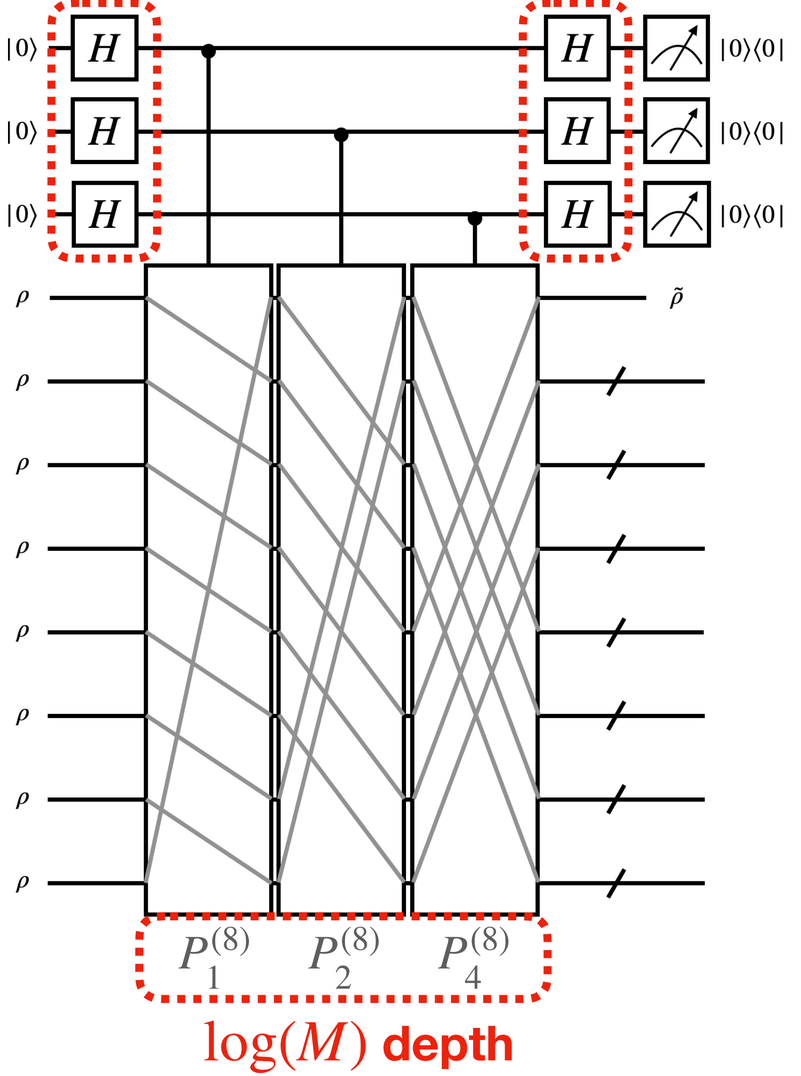
Example: $M = 8$

Only local Hadamard gates for en/decoding

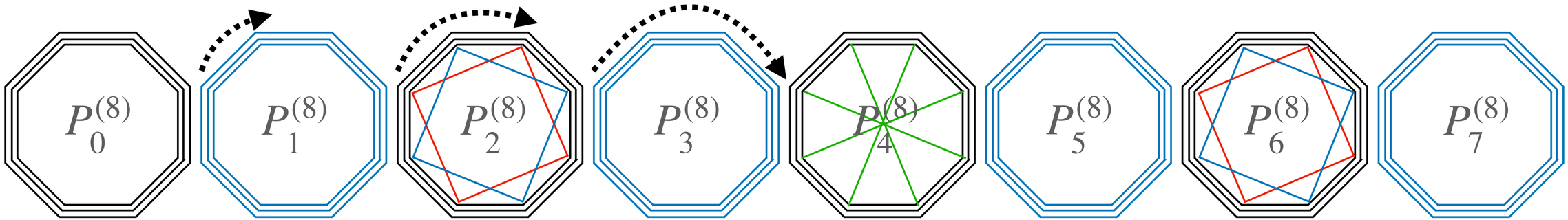
Projector: $P_{\mathrm{CGG}} = \frac{1}{8} \sum_{\sigma \in C_8} P_\sigma^{(M)}$

$$\mathrm{P}_{\vec{0}}\tilde{\rho} = \frac{1}{8}\rho + \frac{1}{8}\sum_{i=1}^{3} 2^{i-1}\,\mathrm{Tr}\left[\rho^{2^i}\right]^{2^{3-i}-1}\rho^{2^i}$$

$$= \frac{1}{8}\left(\rho + \mathrm{Tr}\left[\rho^2\right]^3\rho^2 + 2\,\mathrm{Tr}\left[\rho^4\right]\rho^4 + 4\rho^8\right)$$

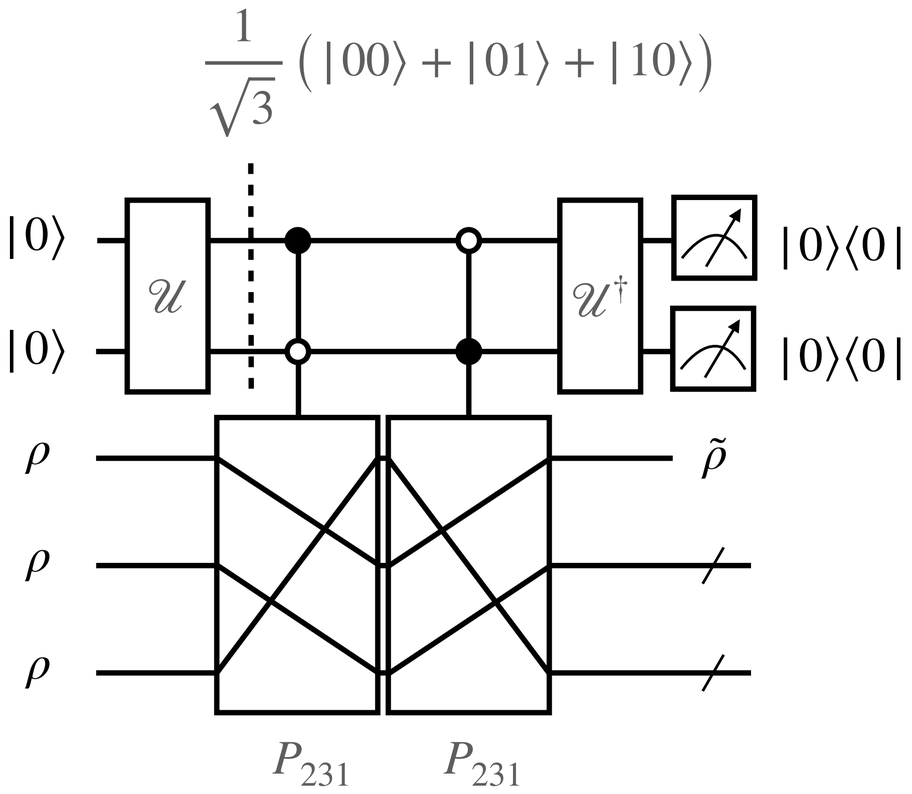


$\log(M)$ **depth**



[Our Proposal]

Cyclic Group Gadget



M	power degree of ρ 1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1		2					
4	1	1		2				
5	1				4			
6	1	1	2			2		
7	1						6	
8	1	1		2				4

For prime M,

Post-selection probability: $\mathrm{P}_{\vec{0}} = \frac{1}{M} + \frac{M-1}{M}\mathrm{Tr}\left[\rho^M\right]$

Purified state: $\tilde{\rho} = \frac{1}{\mathrm{P}_{\vec{0}}}\left(\frac{1}{M}\rho + \frac{M-1}{M}\rho^M\right)$

[Our Proposal]

Monotonicity of $\tilde{p}$ to M in CGG

Post-selection probability: $$\mathrm{P}_{\vec{0}} = \frac{1}{M} + \frac{M-1}{M}\mathrm{Tr}\left[\rho^M\right]$$

Purified state: $$\tilde{\rho} = \frac{1}{\mathrm{P}_{\vec{0}}}\left(\frac{1}{M}\rho + \frac{M-1}{M}\rho^M\right)$$

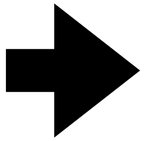
$$\rho^M = \lambda_0^M\left(|\lambda_0\rangle\langle\lambda_0| + \sum_{k>0}\left(\frac{\lambda_k}{\lambda_0}\right)^M |\lambda_k\rangle\langle\lambda_k|\right)$$

There seems to be an optimal M for p
that maximises the purification performance

[Our Proposal]

CGG with Depolarised Inputs (for prime M)

The input quantum state with depolarising rate p: $\rho = (1-p)\rho_0 + p\frac{I}{d}$



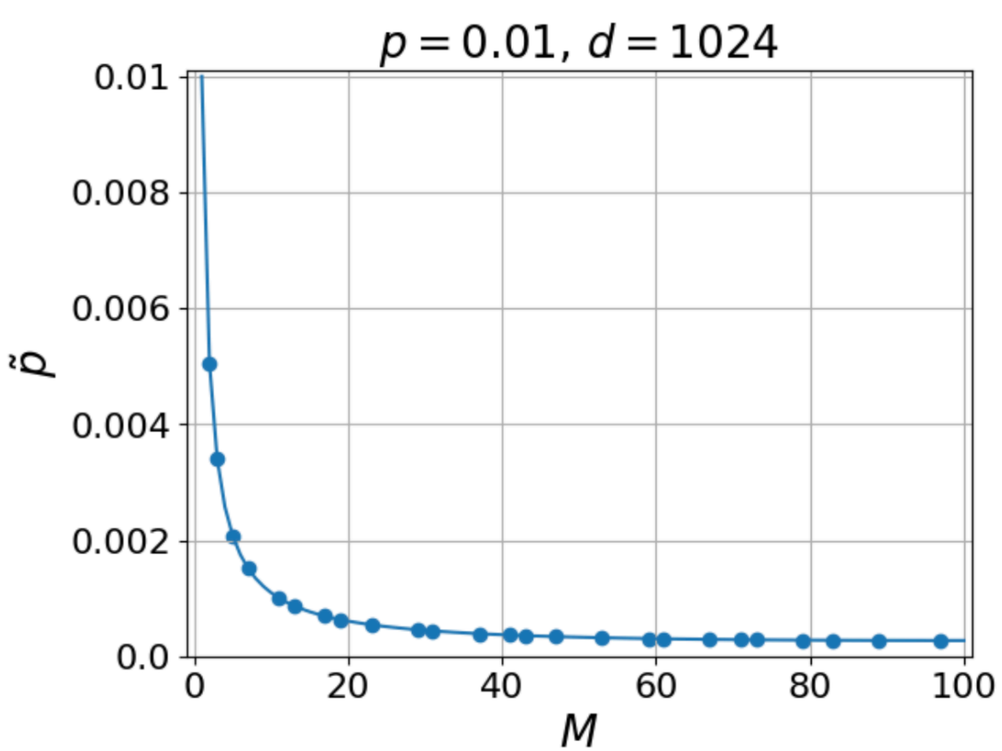
Output quantum state from CGG: $\tilde{\rho} = (1-\tilde{p})\rho_0 + \tilde{p}\frac{I}{d}$

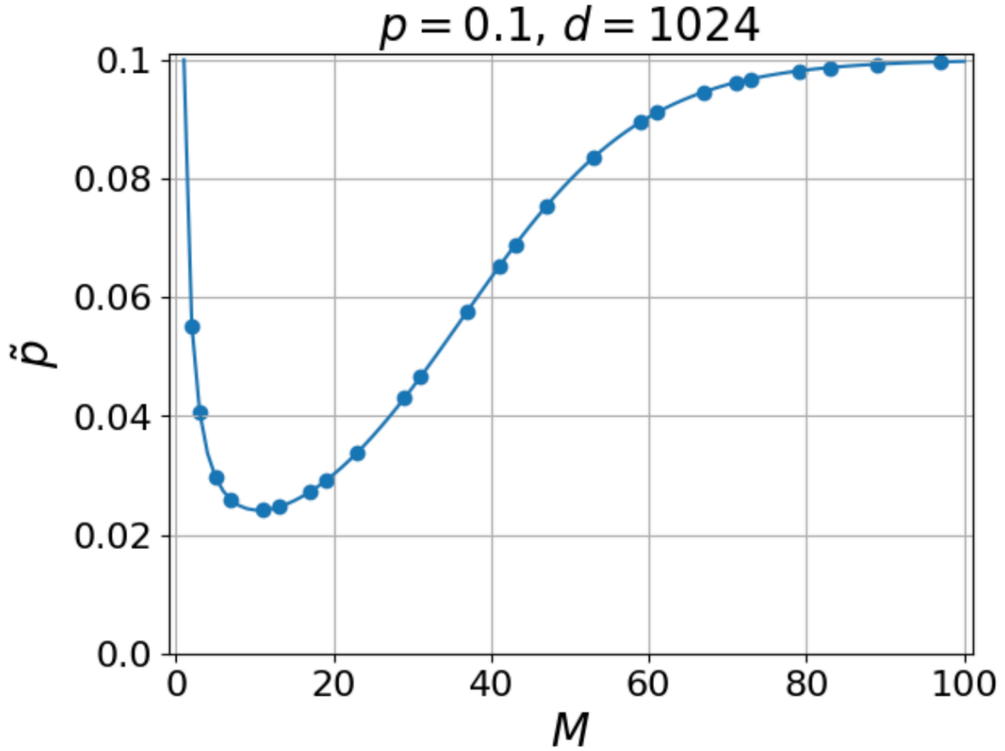
with a new depolarising rate $\tilde{p} = \dfrac{1+(M-1)\left(\frac{p}{d}\right)^{M-1}}{1+(M-1)\left(\left(1-p+\frac{p}{d}\right)^{M}+\left(\frac{p}{d}\right)^{M}(d-1)\right)}p$

[Our Proposal]

Monotonicity of $\tilde{p}$ to (prime) M

$$\tilde{p} = \frac{1 + (M-1)\left(\frac{p}{d}\right)^{M-1}}{1 + (M-1)\left(\left(1 - p + \frac{p}{d}\right)^{M} + \left(\frac{p}{d}\right)^{M}(d-1)\right)} p$$

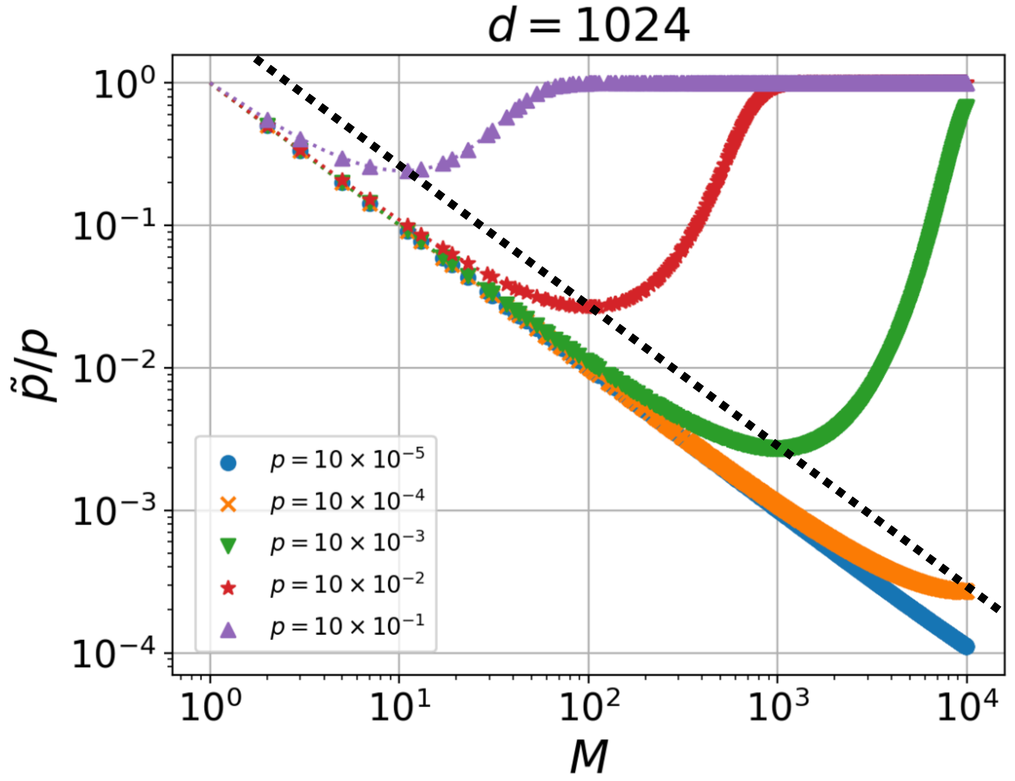




[Our Proposal]

Monotonicity of $\tilde{p}$ to M

$$\tilde{p} = \frac{1 + (M-1)\left(\frac{p}{d}\right)^{M-1}}{1 + (M-1)\left(\left(1 - p + \frac{p}{d}\right)^{M} + \left(\frac{p}{d}\right)^{M}(d-1)\right)} p$$



Almost linear

Sufficient condition: $p < \frac{d}{d-1}\left(1 - e^{\frac{1}{1-M}}\right)$

or, equivalently,

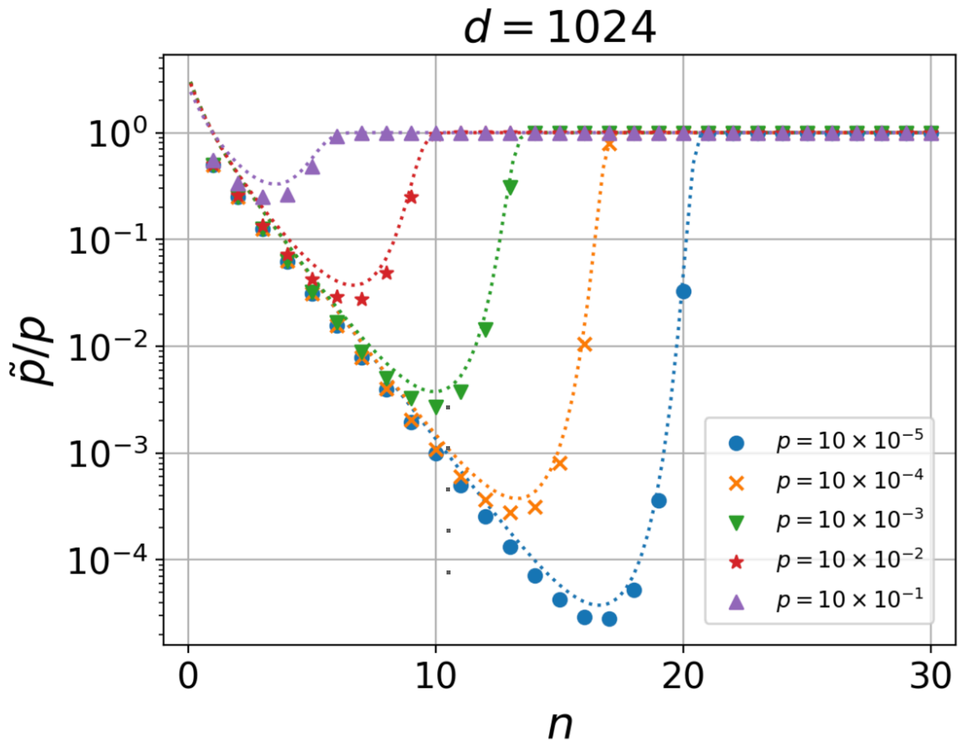
$$M < 1 - \frac{1}{\log\left(1 - \left(1 - \frac{1}{d}\right)p\right)}$$

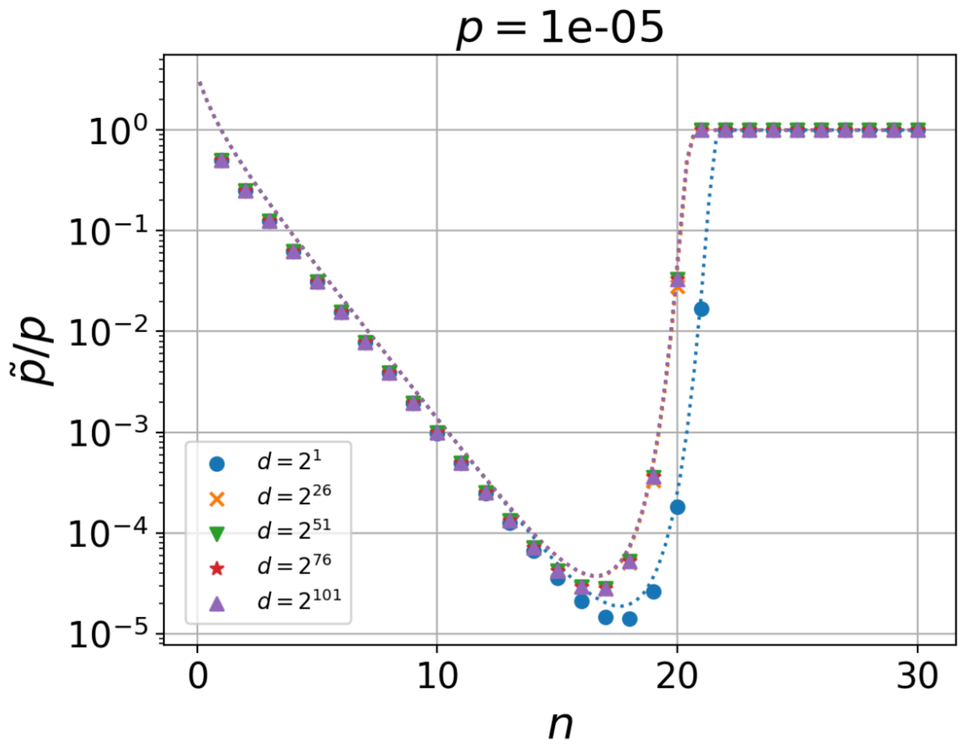
[Our Proposal]

when $M = \alpha^n$, under depolarising noise

$$\tilde{p} = \frac{1 + \sum_{i=1}^{n} \alpha^{i-1} \left(\beta^{\alpha^i} + \gamma^{\alpha^i}(d-1)\right)^{\alpha^{n-1}-1} \gamma^{\alpha^i - 1}}{1 + \sum_{i=1}^{n} \alpha^{i-1} \left(\beta^{\alpha^i} + \gamma^{\alpha^i}(d-1)\right)^{\alpha^{n-i}}} p \qquad \text{where } \beta = 1 - \left(1 - \frac{1}{d}\right) p, \quad \gamma = \frac{p}{d}$$

When $\alpha = 2$

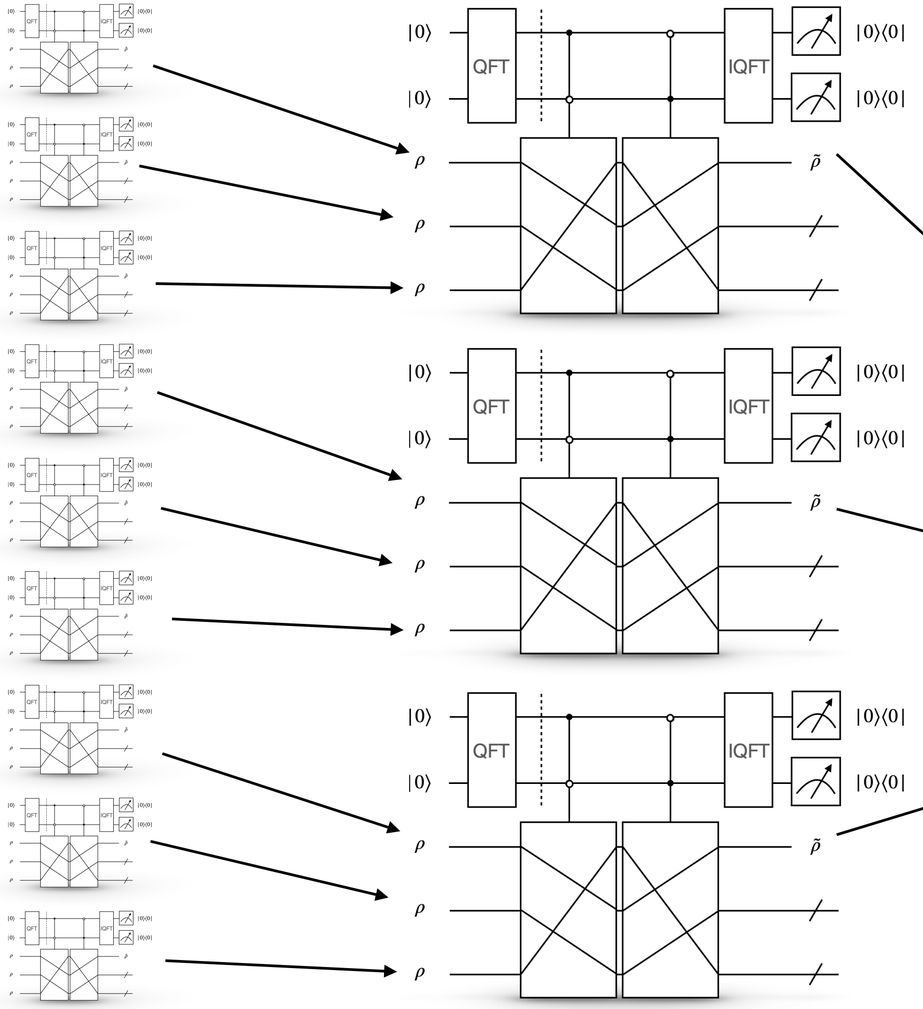




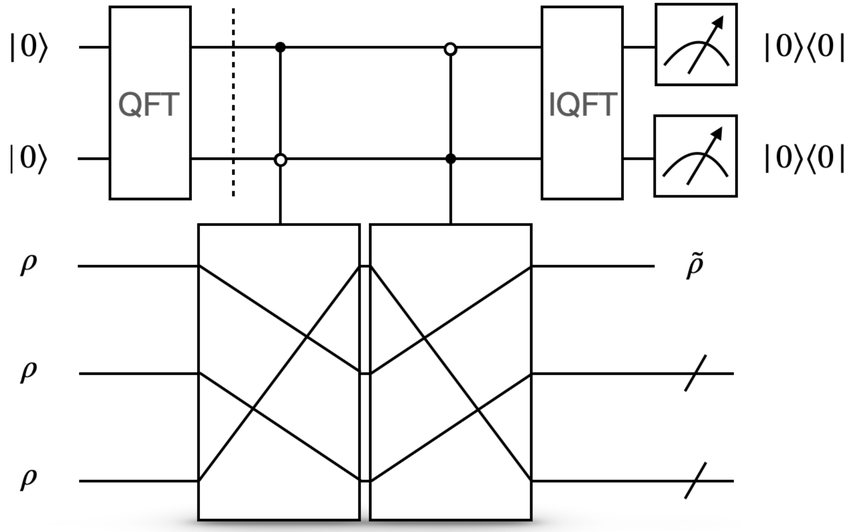
Work in Progress, Future Work

- Analysis
  - of different inputs (non i.i.d. settings of noise)
  - of other noise models: general stochastic noise
  - with different performance metrics: entropy, fidelity
  - of recursive application of this gadget
- Application to specific problem: Simon's problem with faulty oracle
- Optimality of conditions

Work in Progress, Future Work



- Analysis of recursive application of this gadget



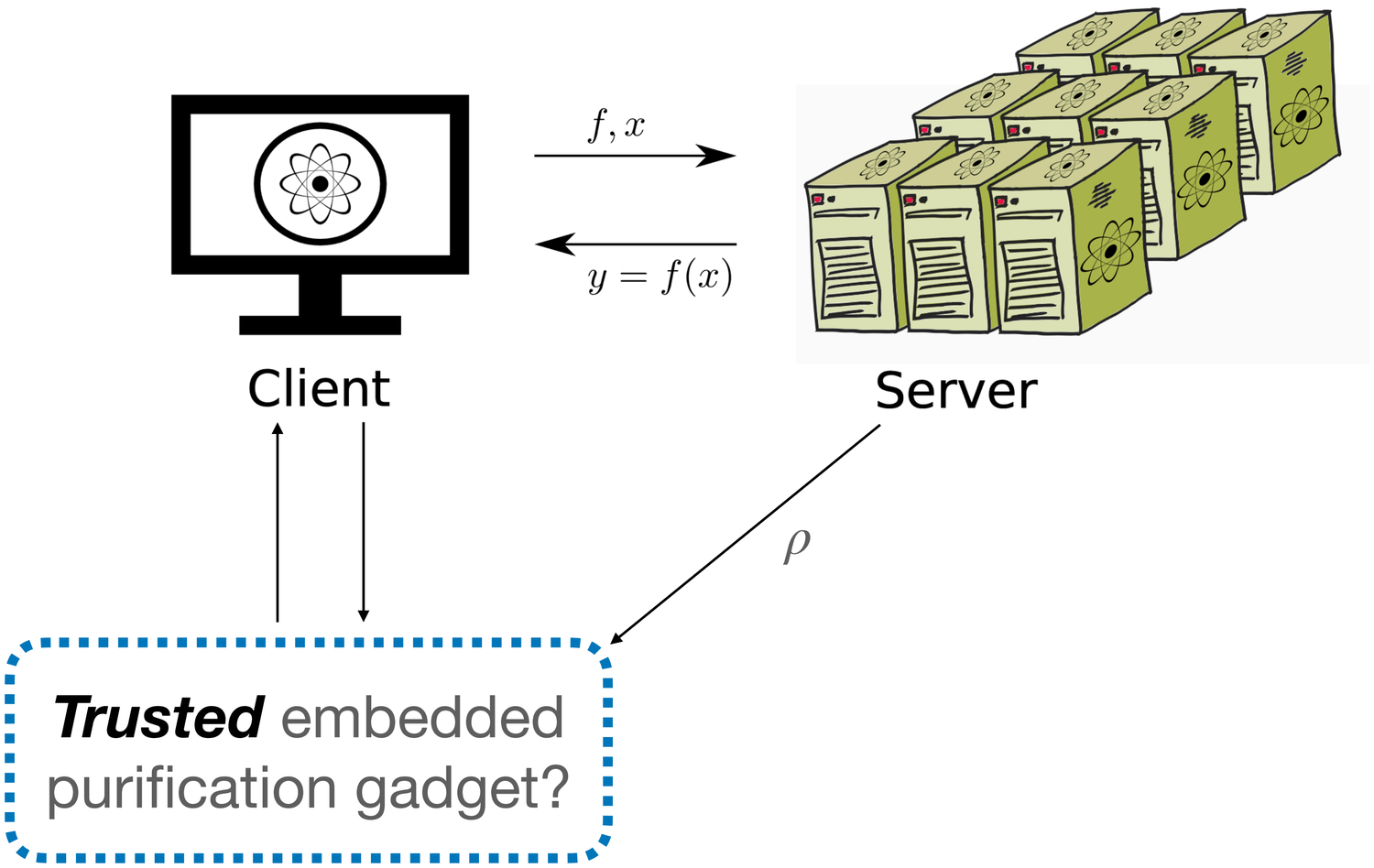
Comparison with [Childs, Fu, Leung, Li, Ozols, Vyas, 2023] where they used the recursive application of the SWAP gadget

Application of CGG

Targeted to the middle-term era

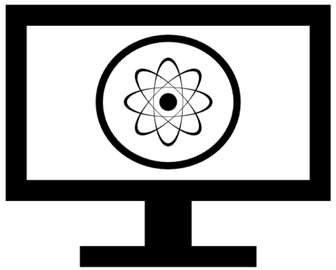
- **A variation of quantum majority vote**
- **Keeping quantum advantage of sampling problems under noise**
  e.g.) Simon's problem with faulty oracles
- **Link with Information theoretic limitation of this type of gadget**
- **Computation of some properties in photonics**

Various Potential Architectures for Ecosystems



Various Potential Architectures for Ecosystems

Untrusted embedded purification gadget?



f, x

$y = f(x)$

Client

with enough quantum memory?

Server

Blind embedded SWAP gadget???

Let’s exploit the symmetry together!

We will publish our results soon!