Universal construction of decoders from encoding black boxes

Satoshi Yoshida, Akihito Soeda, Mio Murao

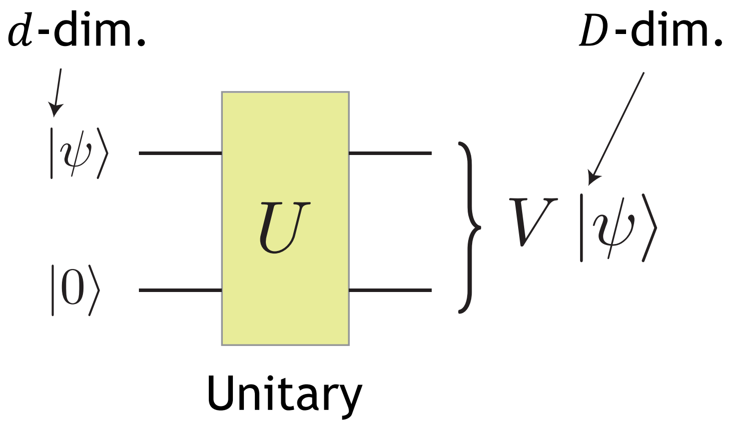
Department of Physics, The University of Tokyo

東京大学
THE UNIVERSITY OF TOKYO

arXiv: 2110.00258

Motivation

- Isometry operation
- Encoding of quantum state on a higher-dimensional Hilbert space

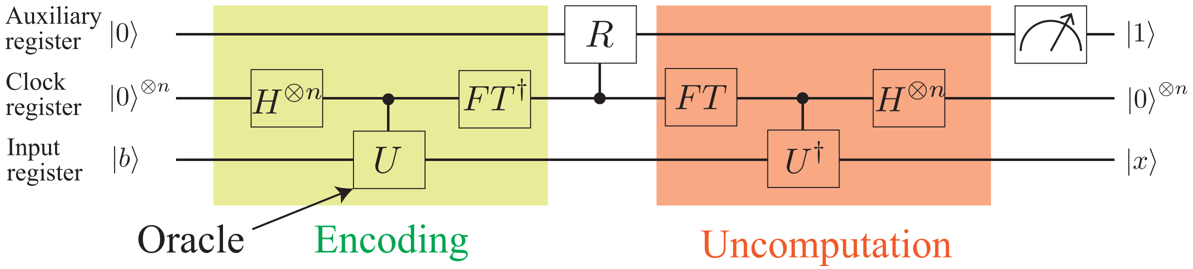


- Decoding: inverse operation of encoding

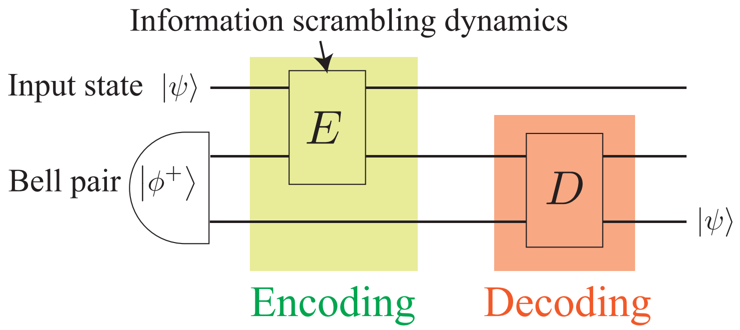
Motivation

- Examples of black box isometry

- Encoding oracle in quantum algorithms (eg. HHL algorithm) [Harrow et al. 2009]



- Information scrambling dynamics as error correcting code [Hayden, Preskill 2007]



Motivation

- Question

How to decode an encoding operation given as a black box?

- Straightforward strategy: Process tomography

- Tomography of a black box isometry $\tilde{\mathcal{V}}$

→ Implement its inverse $\tilde{\mathcal{V}}_{\mathrm{inv}}$ based on the classical description of $\tilde{\mathcal{V}}$

× The cost of tomography is very heavy.

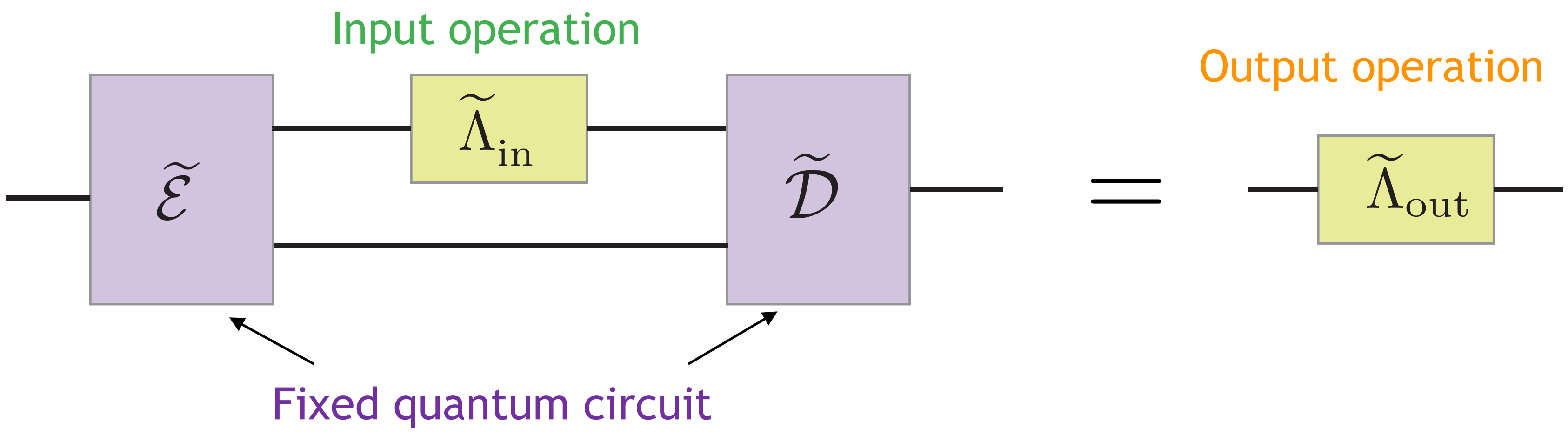
- Another strategy: Higher-order quantum transformation

- Transform a black box isometry $\tilde{\mathcal{V}}$ to its inverse $\tilde{\mathcal{V}}_{\mathrm{inv}}$ without knowing its classical description

✓ Less query complexity of $\tilde{\mathcal{V}}$ than tomography.

Higher-order quantum transformation

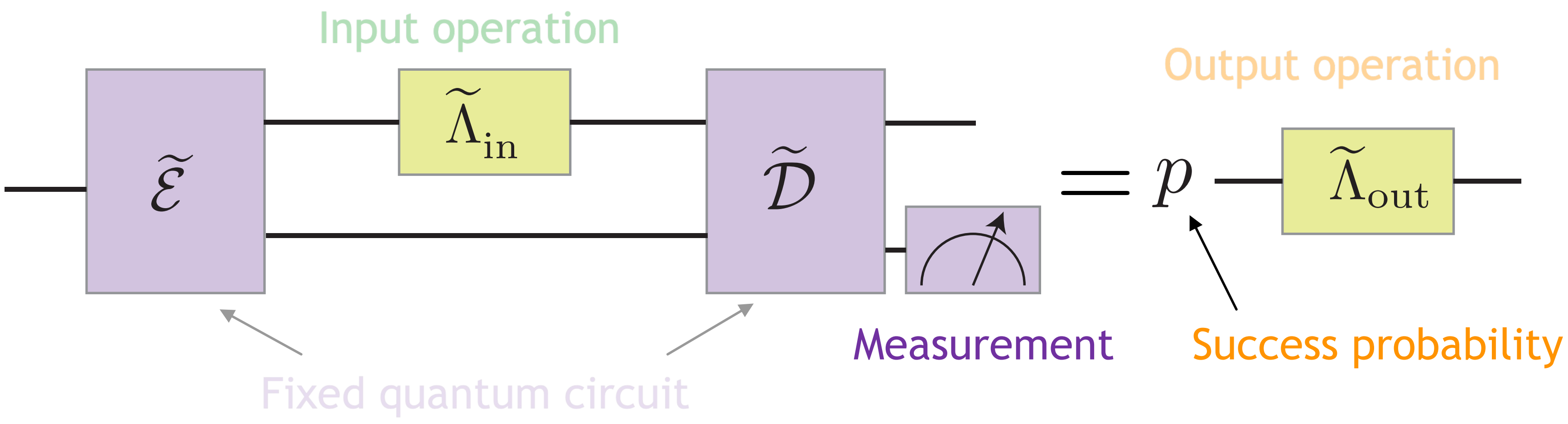
- Input black box operation + Fixed quantum circuit = Output operation



Higher-order quantum transformation

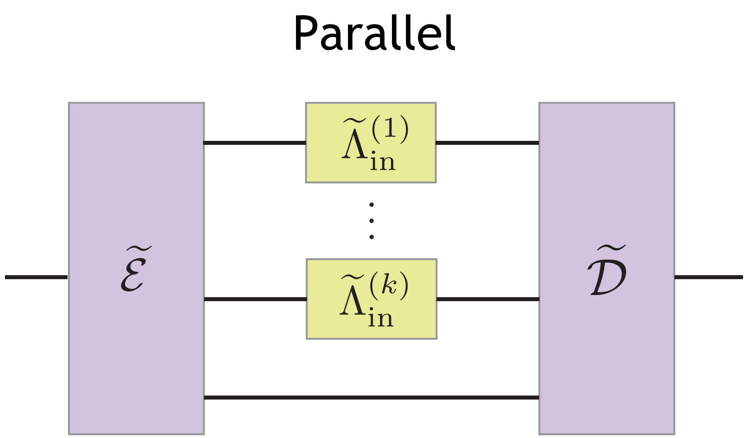
- Probabilistic protocol

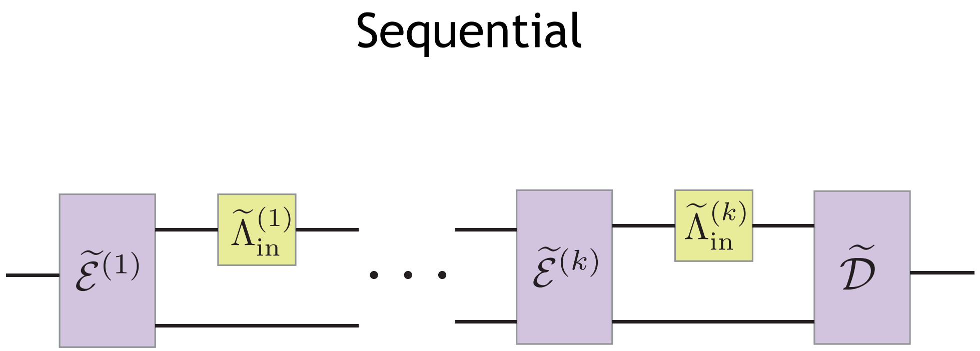
Determine accept/reject based on the measurement outcome



Higher-order quantum transformation

- Multiple input case

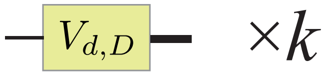




Cf. We can also consider higher-order quantum transform that cannot be implemented by quantum circuit.

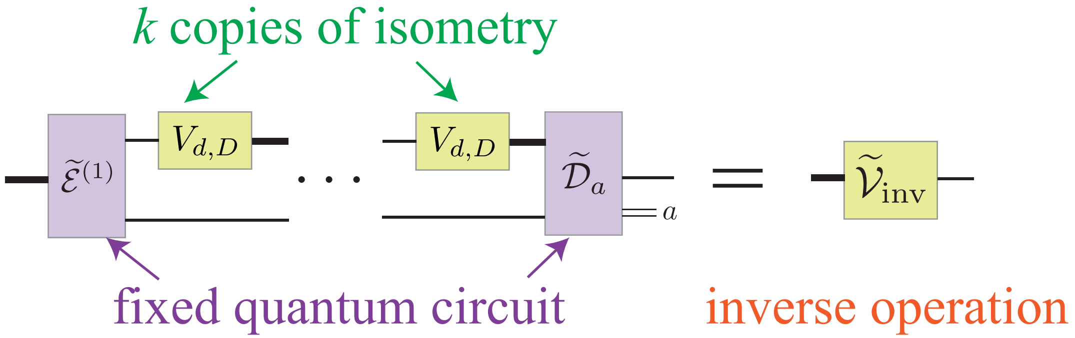
Task: Isometry inversion

- Given: ***k* copies of a black box isometry** $\widetilde{\mathcal{V}}: \mathcal{L}(\mathbb{C}^d) \to \mathcal{L}(\mathbb{C}^D)$



***Thick wire**: D-dimensional space

- Task: Implement the **inverse operation** $\widetilde{\mathcal{V}}_{\text{inv}}$ s.t. $\widetilde{\mathcal{V}}_{\text{inv}} \circ \widetilde{\mathcal{V}} = \widetilde{\text{id}}$.



Previous work: Unitary inversion

- The special case $(D = d)$ of isometry inversion = Unitary inversion
- Given: ***k* copies of a black box unitary** $\tilde{\mathcal{U}}: \mathcal{L}(\mathbb{C}^d) \to \mathcal{L}(\mathbb{C}^d)$
- Task: Implement the **inverse operation** $\tilde{\mathcal{U}}^\dagger$

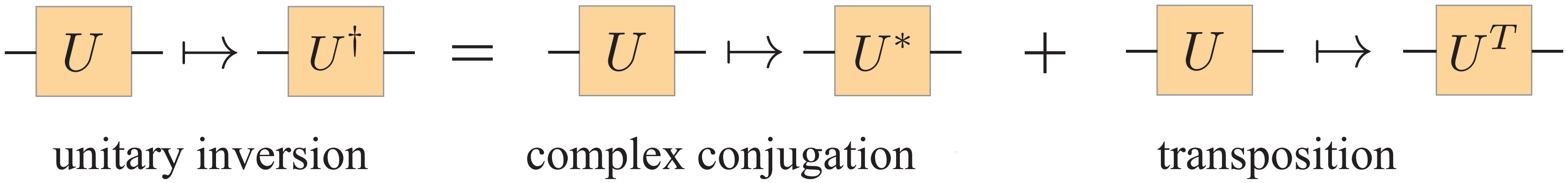
Theorem [Quintino et al. 2019].

There exists a unitary inversion protocol with the success probability

$$p = 1 - \mathcal{O}(d^3/k)\,.$$

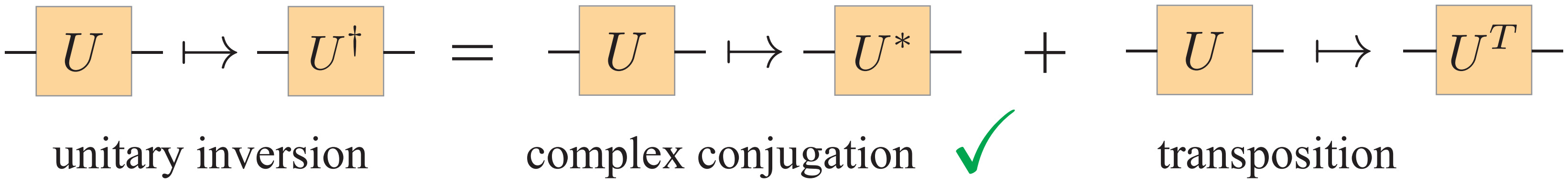
Previous work: Unitary inversion

- Main idea

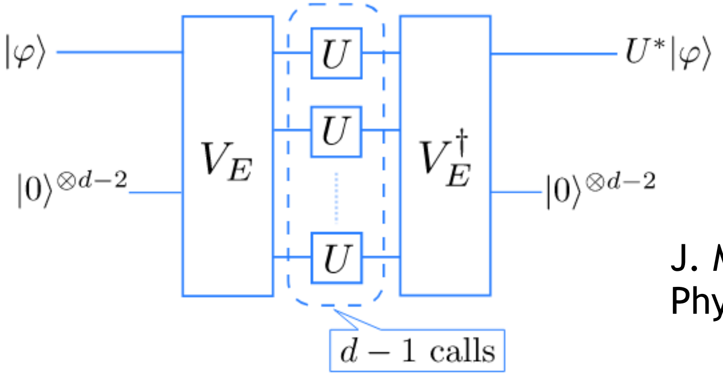


Previous work: Unitary inversion

- Main idea



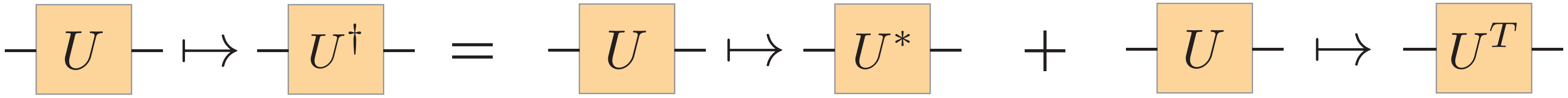
- Unitary complex conjugation [Miyazaki et al. 2019]



J. Miyazaki, A. Soeda, and M. Murao,
Phys. Rev. Research **1**, 013007 (2019).

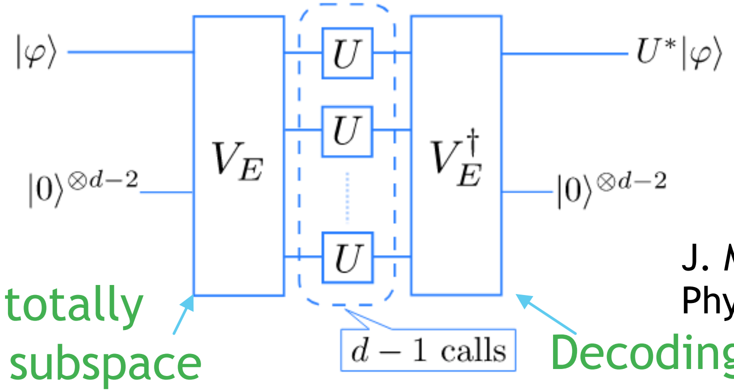
Previous work: Unitary inversion

- Main idea



unitary inversion = complex conjugation ✓ + transposition

- Unitary complex conjugation [Miyazaki et al. 2019]



Encoding onto totally antisymmetric subspace

Decoding

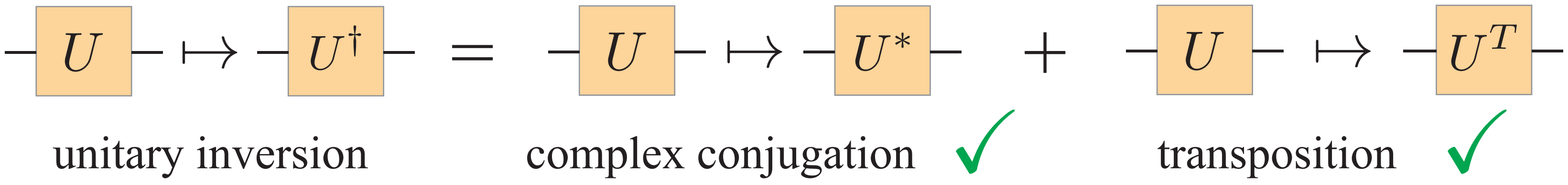
J. Miyazaki, A. Soeda, and M. Murao, Phys. Rev. Research 1, 013007 (2019).

Irreducible decomposition of $U^{\otimes d-1}$: $U^{\otimes d-1} \simeq U^* \oplus \cdots$

Totally antisymmetric subspace

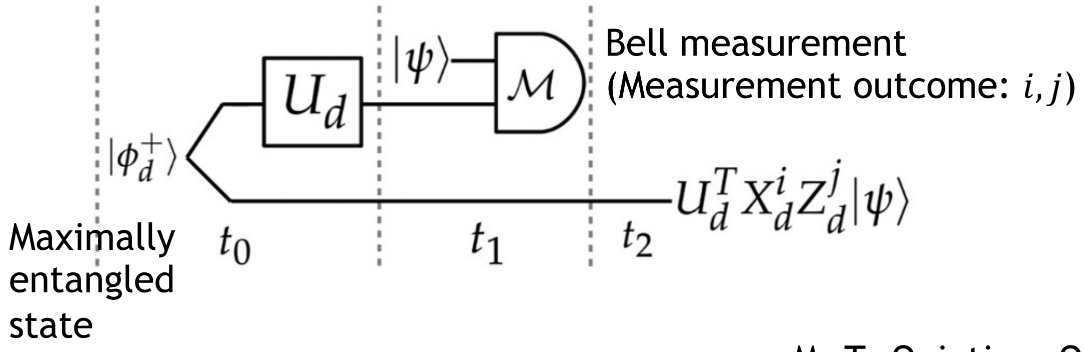
Previous work: Unitary inversion

- Main idea



- Unitary transposition [Quintino et al. 2019]

Gate teleportation



M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda and M. Murao, Phys. Rev. A 100, 062339 (2019).

Previous work: Unitary inversion

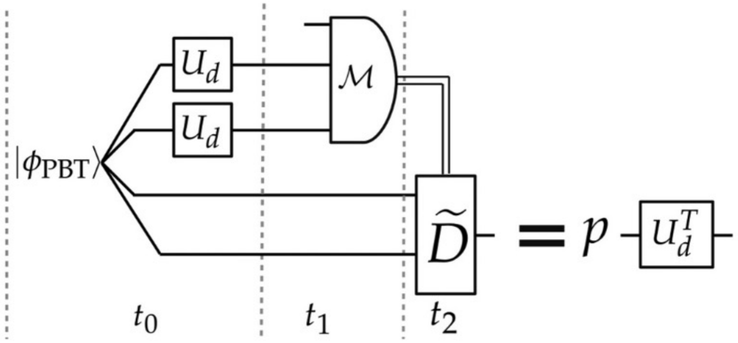
- Main idea

$$-\boxed{U}- \mapsto -\boxed{U^\dagger}- \;=\; -\boxed{U}- \mapsto -\boxed{U^*}- \;+\; -\boxed{U}- \mapsto -\boxed{U^T}-$$

unitary inversion — complex conjugation ✓ — transposition ✓

- Unitary transposition [Quintino et al. 2019]

Port-based teleportation [Ishizaka and Hiroshima, 2008]

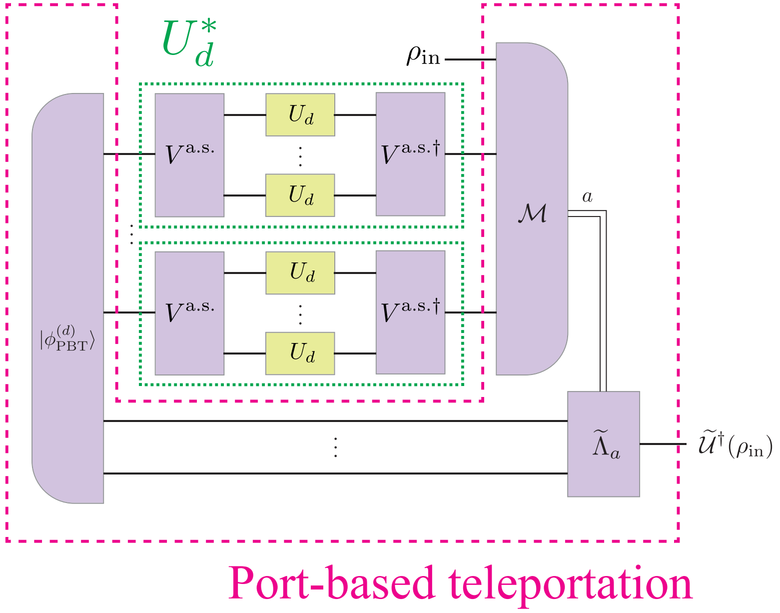


M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda and M. Murao, Phys. Rev. A 100, 062339 (2019).

Previous work: Unitary inversion

- Unitary inversion [Quintino et al. 2019]

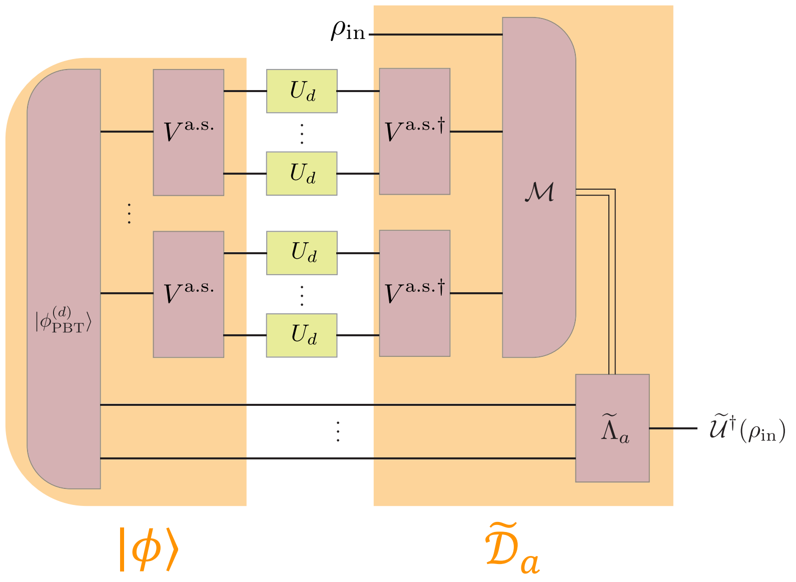
Unitary complex conjugation + Port-based teleportation



Previous work: Unitary inversion

- Unitary inversion [Quintino et al. 2019]

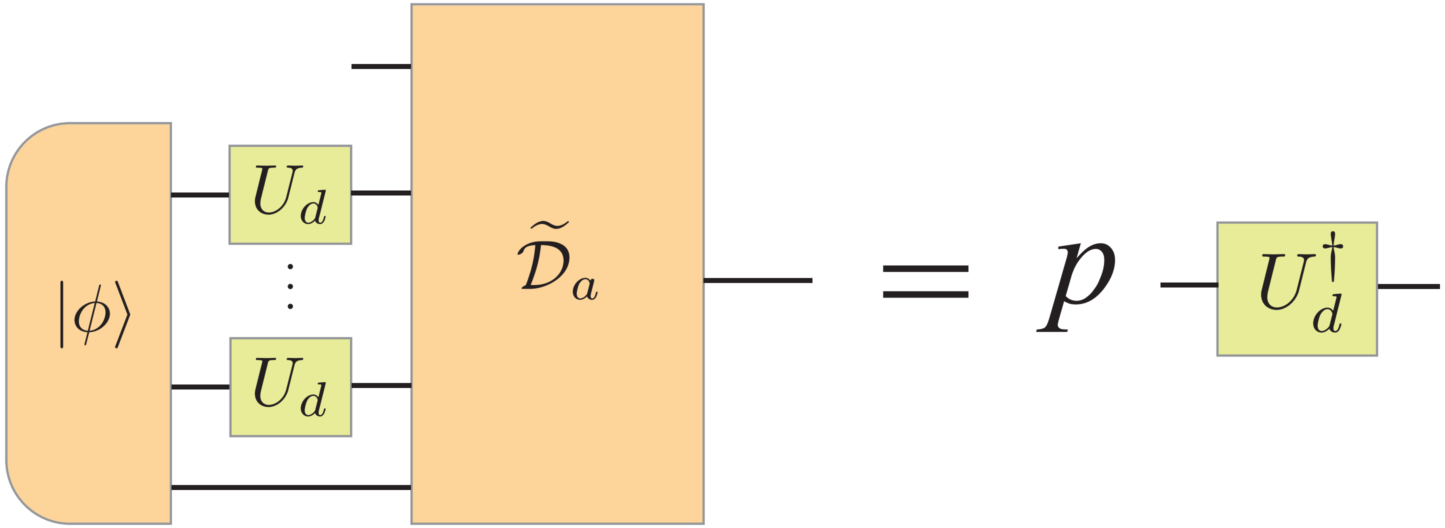
Unitary complex conjugation + Port-based teleportation



Previous work: Unitary inversion

- Unitary inversion [Quintino et al. 2019]

Unitary complex conjugation + Port-based teleportation



Extension of unitary inversion?

- Decomposition of unitary inversion

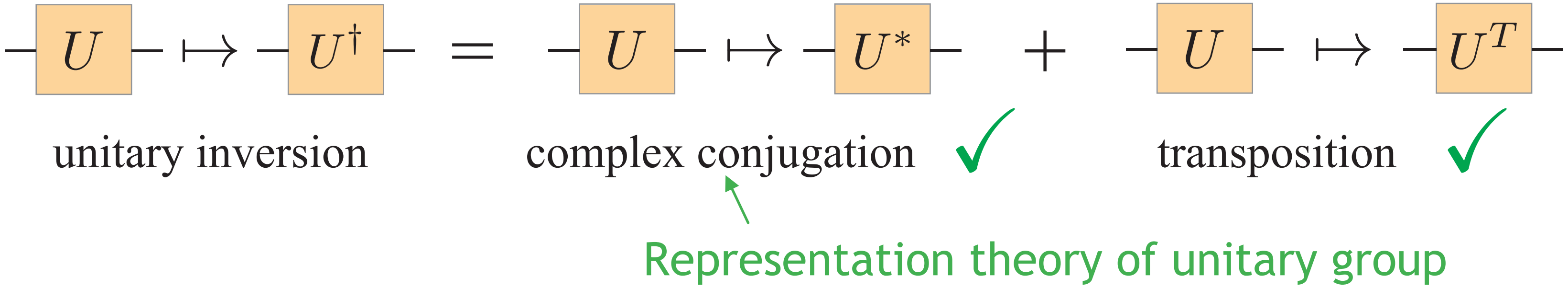
$$\boxed{U} \mapsto \boxed{U^\dagger} = \boxed{U} \mapsto \boxed{U^*} + \boxed{U} \mapsto \boxed{U^T}$$

unitary inversion — complex conjugation ✓ — transposition ✓

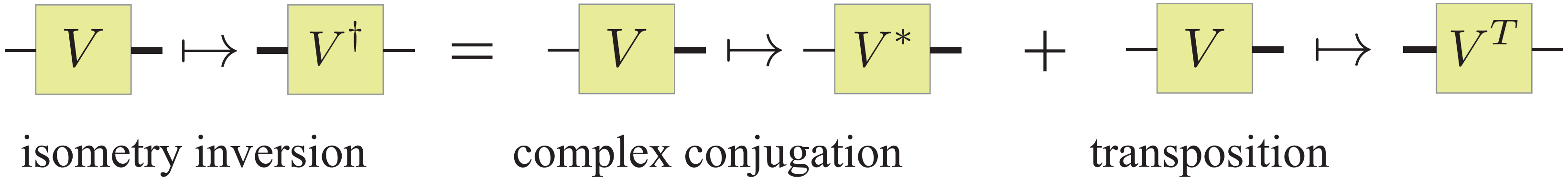
Representation theory of unitary group

Extension of unitary inversion?

- Decomposition of unitary inversion

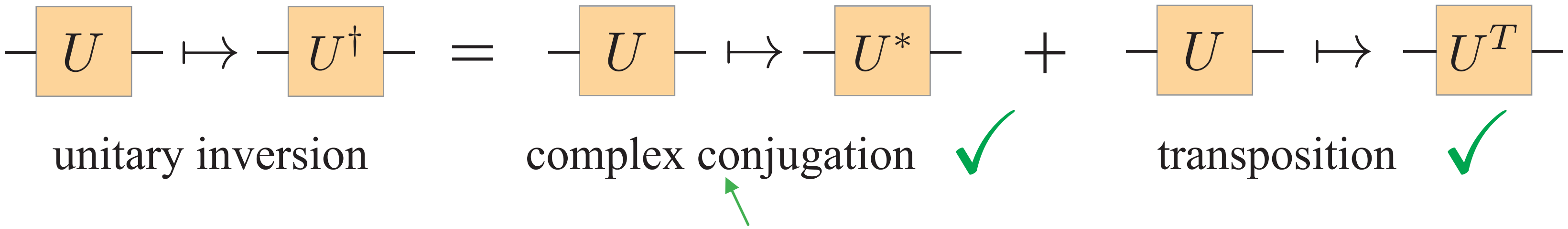


- Direct extension?



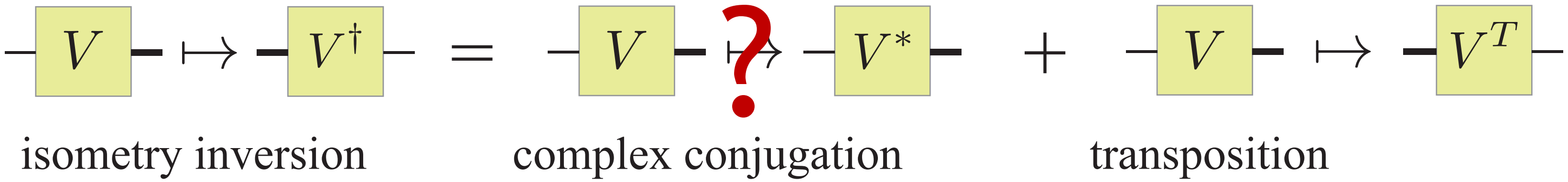
Extension of unitary inversion?

- Decomposition of unitary inversion



Representation theory of unitary group

- Direct extension? → Isometry does not form a group

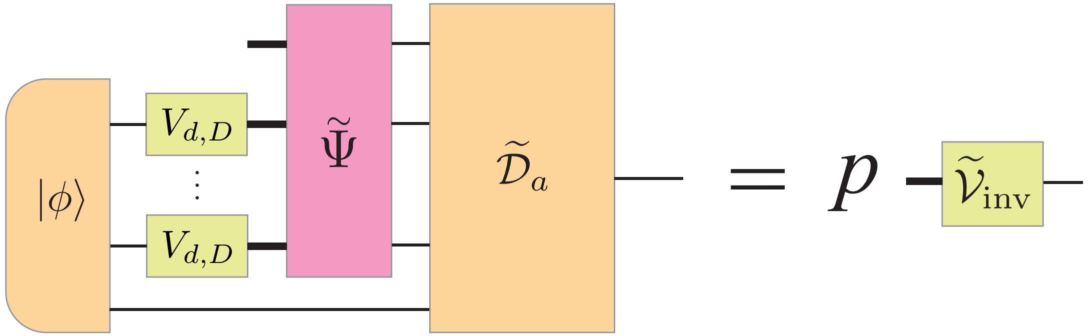


Research question

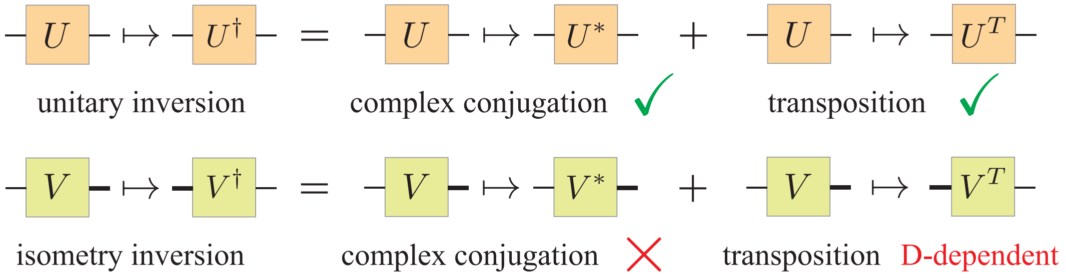
- How to implement isometry inversion?
- Difference with unitary inversion?

Result

- Construction of efficient probabilistic protocol for isometry inversion

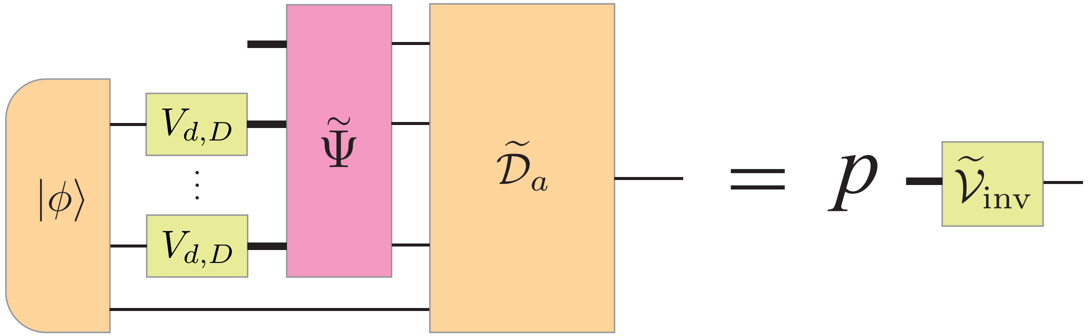


- Difference between unitary inversion and isometry inversion



Result

- Construction of efficient probabilistic protocol for isometry inversion

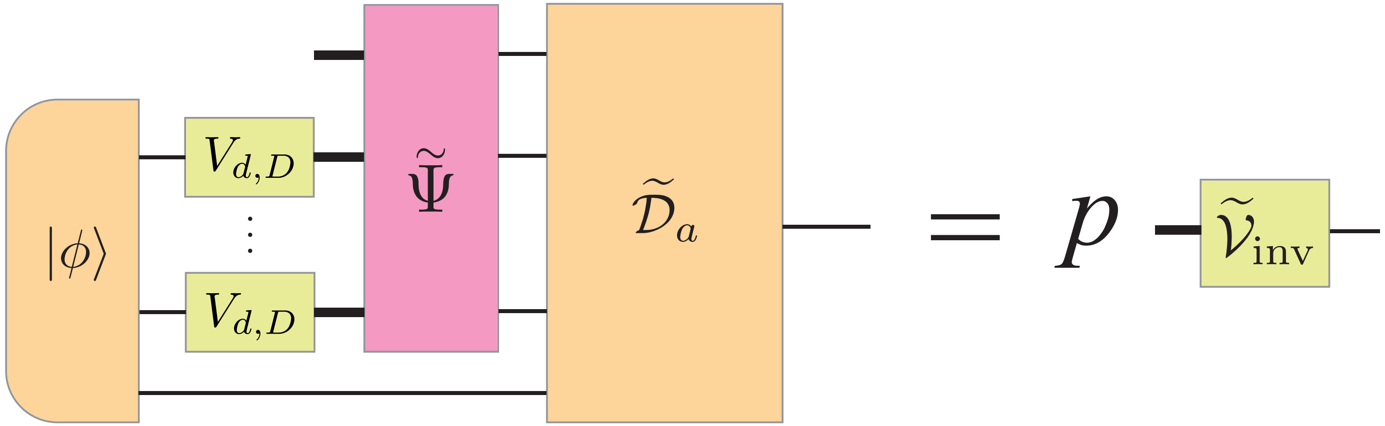


- Difference between unitary inversion and isometry inversion

Result 1:
Probabilistic isometry inversion protocol

Theorem 1. The following quantum circuit implements isometry inversion with the success probability

$$p = 1 - \mathcal{O}(d^3/k)$$ ← Independent of D

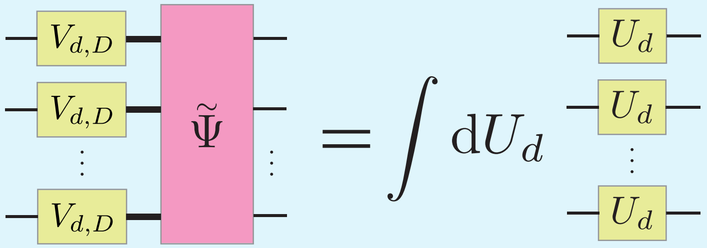


Result 1:
Probabilistic isometry inversion protocol

- Main idea

Construct a CPTP map $\tilde{\Psi}$ satisfying the following lemma.

Lemma 2. For any isometry $V_{d,D}: \mathbb{C}^d \to \mathbb{C}^D$, the following relation holds, where $\mathrm{d}U_d$ is the Haar measure on the unitary group $U(d)$.



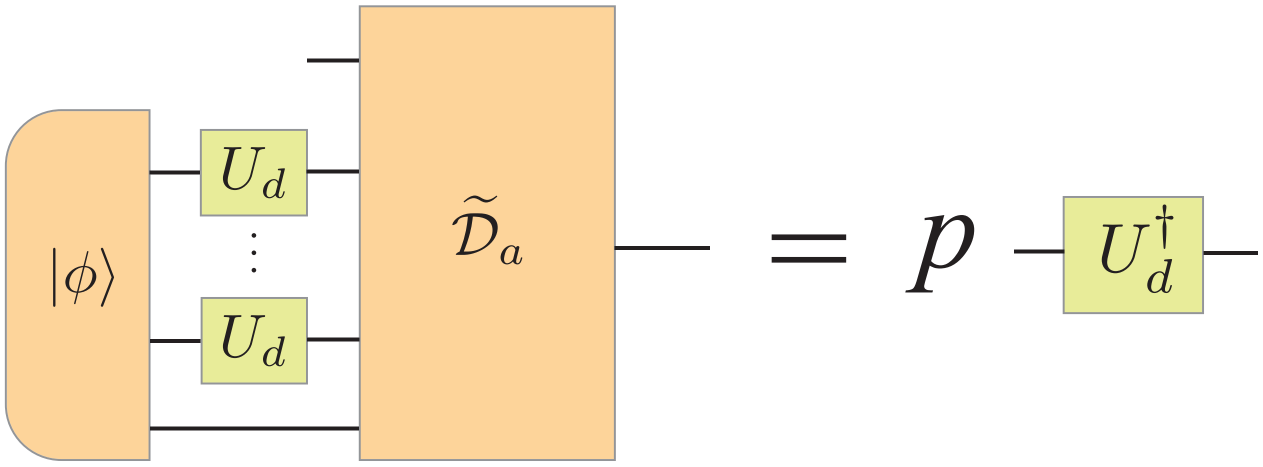
CPTP map $\tilde{\Psi}$ = Quantum Schur transform [Harrow, 2005]+“trace-and-replace”

A. W. Harrow, PhD Thesis, arXiv: quant-ph/0512255

Result 1:
Probabilistic isometry inversion protocol

- Main idea

Insert the CPTP map $\widetilde{\Psi}$ into a unitary inversion protocol

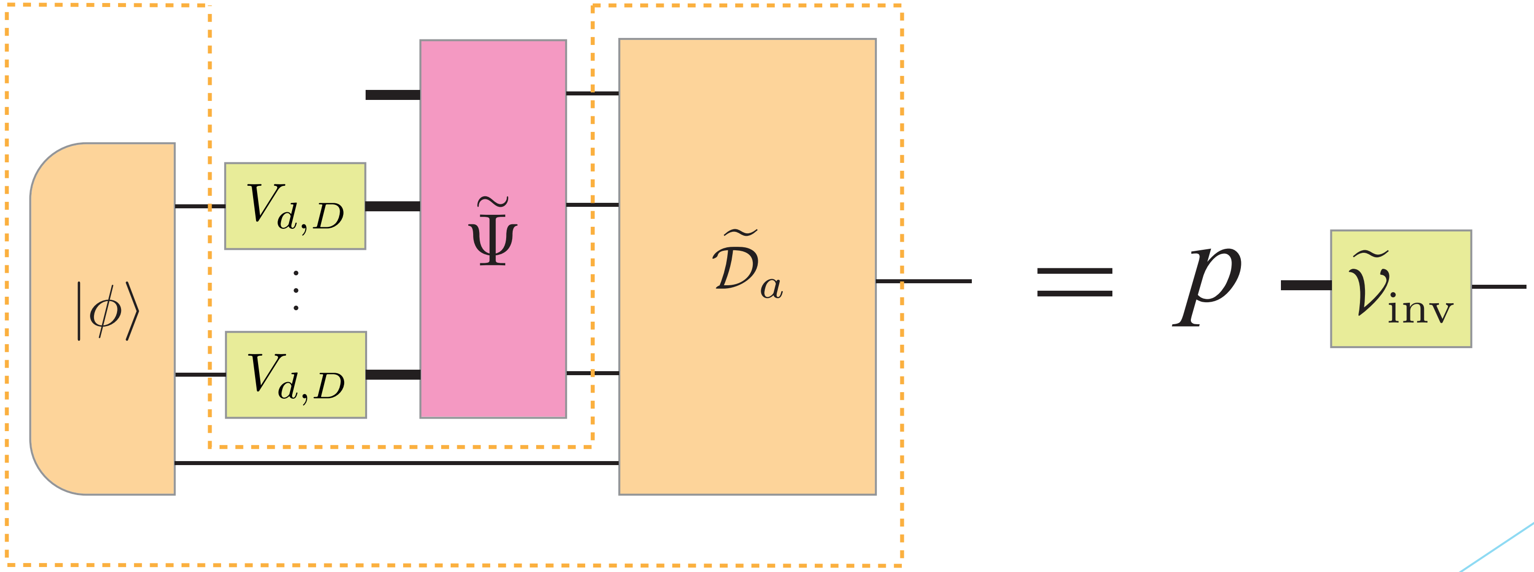


Unitary inversion

Result 1:
Probabilistic isometry inversion protocol

- Main idea

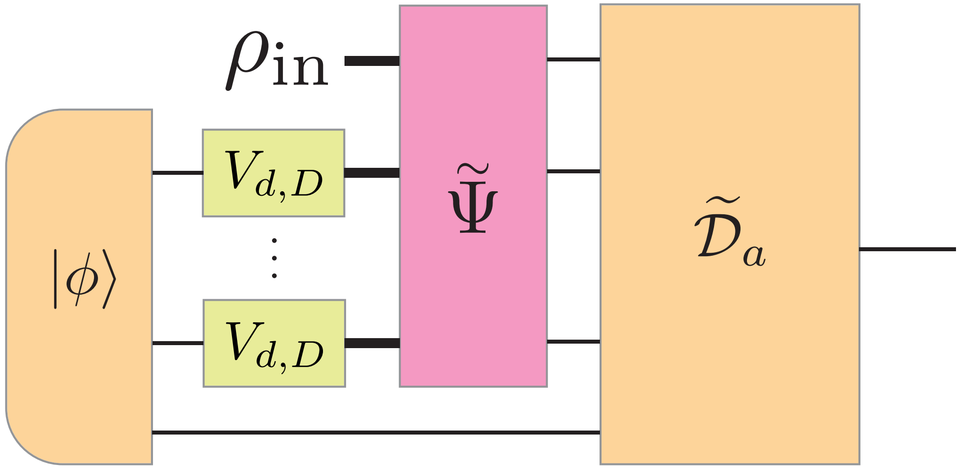
Insert the CPTP map $\widetilde{\Psi}$ into a unitary inversion protocol



Result 1:
Probabilistic isometry inversion protocol

- Proof

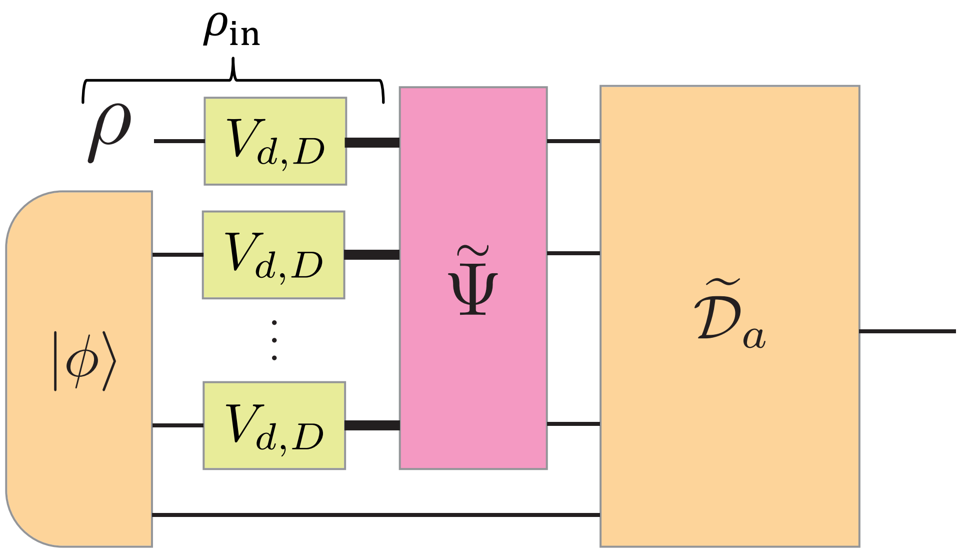
If the input state is $\rho_{\text{in}} = V\rho V^\dagger$,



Result 1:
Probabilistic isometry inversion protocol

- Proof

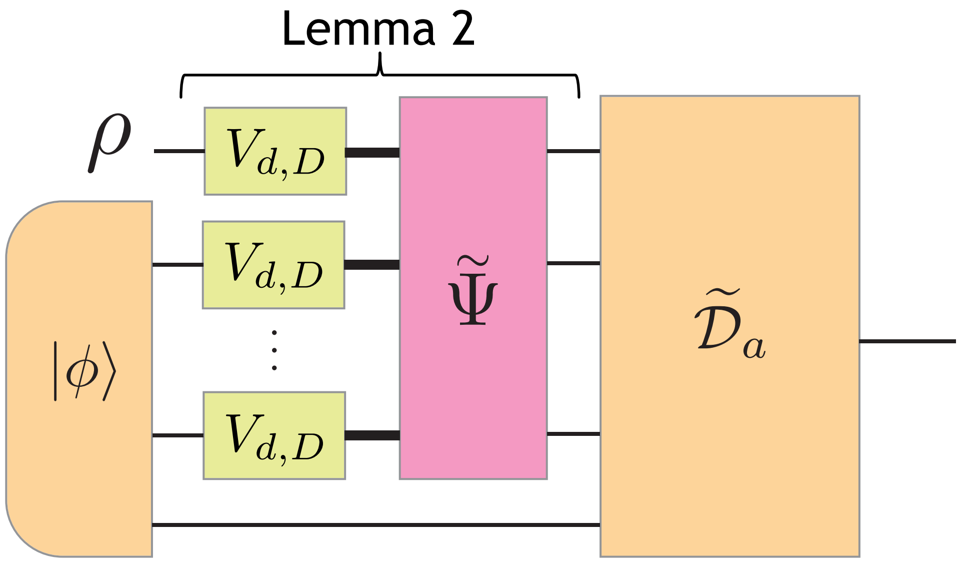
If the input state is $\rho_{\text{in}} = V\rho V^\dagger$,



Result 1:
Probabilistic isometry inversion protocol

- Proof

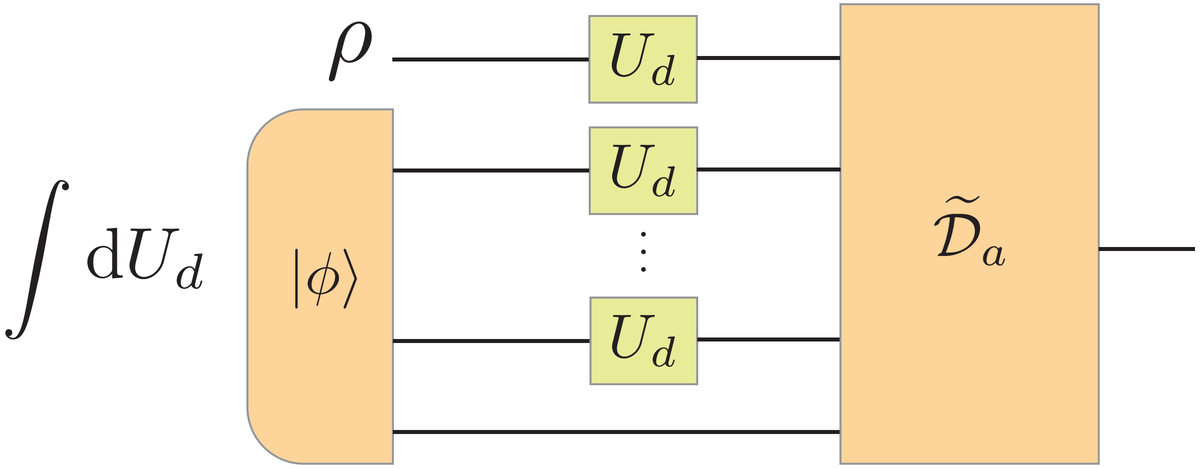
If the input state is $\rho_{\text{in}} = V\rho V^\dagger$,



Result 1:
Probabilistic isometry inversion protocol

- Proof

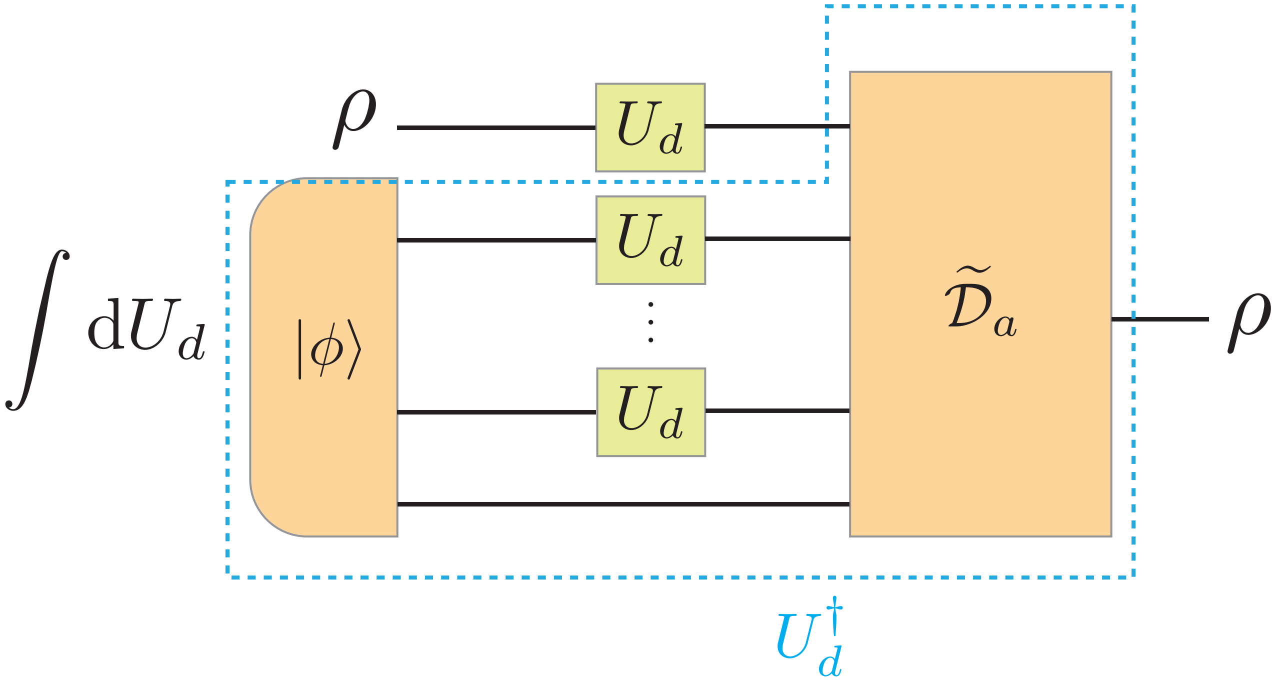
If the input state is $\rho_{\text{in}} = V\rho V^\dagger$,



Result 1:
Probabilistic isometry inversion protocol

- Proof

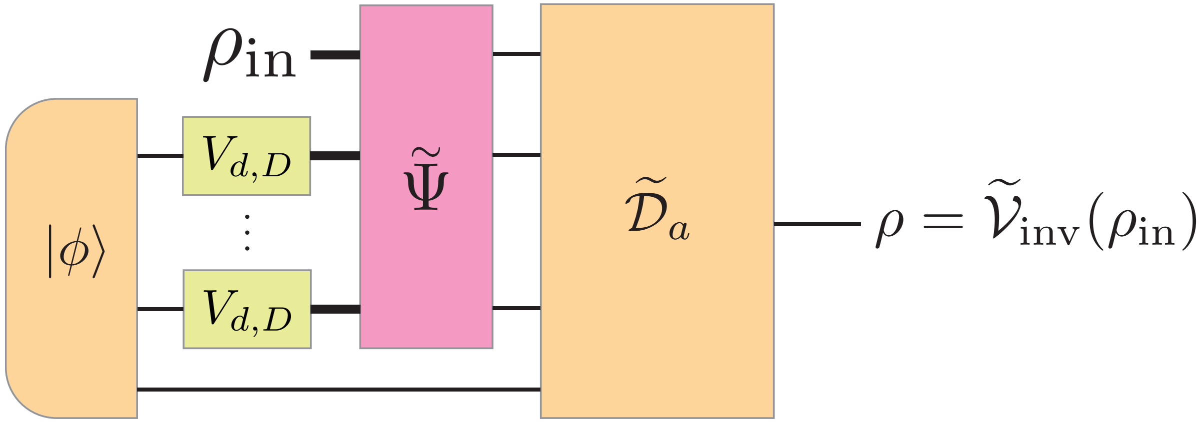
If the input state is $\rho_{\text{in}} = V\rho V^\dagger$, the output state is ρ



Result 1:
Probabilistic isometry inversion protocol

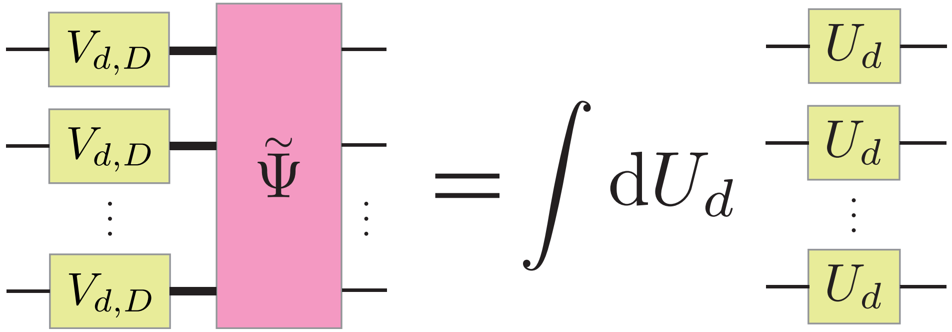
- Proof

If the input state is $\rho_{\text{in}} = V\rho V^\dagger$, the output state is ρ



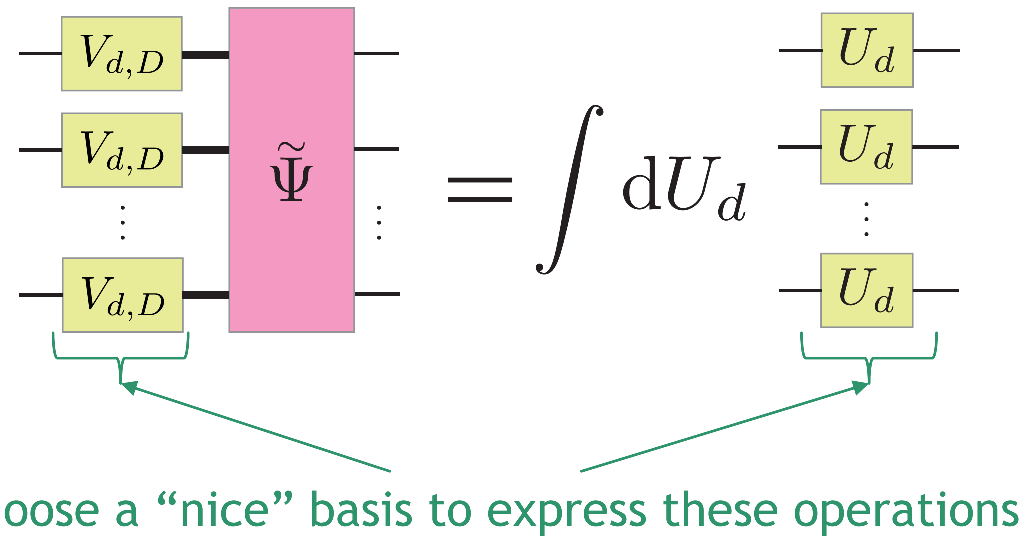
Result 1:
Construction of the CPTP map $\tilde{\Psi}$

- The CPTP map $\tilde{\Psi}$ should satisfy



Result 1:
Construction of the CPTP map $\tilde{\Psi}$

- The CPTP map $\tilde{\Psi}$ should satisfy



Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Result 1: Construction of the CPTP map $\widetilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Unitary group $U(d) \ni U \mapsto U^{\otimes k} \in \mathcal{L}(\mathcal{H})$

Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Unitary group $U(d) \ni U \mapsto U^{\otimes k} \in \mathcal{L}(\mathcal{H})$

Symmetric group $\mathfrak{S}_k \ni \sigma \mapsto S_\sigma \in \mathcal{L}(\mathcal{H})$ s.t. $S_\sigma|i_1, \cdots, i_k\rangle = |i_{\sigma^{-1}(1)}, \cdots, i_{\sigma^{-1}(k)}\rangle$

Permutation operator

Result 1: Construction of the CPTP map $\widetilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Unitary group $U(d) \ni U \mapsto U^{\otimes k} \in \mathcal{L}(\mathcal{H})$

Symmetric group $\mathfrak{S}_k \ni \sigma \mapsto S_\sigma \in \mathcal{L}(\mathcal{H})$ s.t. $S_\sigma |i_1, \cdots, i_k\rangle = |i_{\sigma^{-1}(1)}, \cdots, i_{\sigma^{-1}(k)}\rangle$

Permutation operator

Schur-Weyl duality:

$$\mathcal{H} = \bigoplus_\mu \mathcal{U}_\mu^{(d)} \otimes \mathcal{S}_\mu^{(k)}$$

μ: Young tableau with k boxes

Result 1:
Construction of the CPTP map $\tilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Unitary group $U(d) \ni U \mapsto U^{\otimes k} \in \mathcal{L}(\mathcal{H})$

Symmetric group $\mathfrak{S}_k \ni \sigma \mapsto S_\sigma \in \mathcal{L}(\mathcal{H})$ s.t. $S_\sigma|i_1, \cdots, i_k\rangle = |i_{\sigma^{-1}(1)}, \cdots, i_{\sigma^{-1}(k)}\rangle$

Permutation operator

Schur-Weyl duality:

$$\mathcal{H} = \bigoplus_\mu \mathcal{U}_\mu^{(d)} \otimes \mathcal{S}_\mu^{(k)}$$
$$U^{\otimes k} = \bigoplus_\mu U_\mu \otimes I_{\mathcal{S}_\mu}$$
$$S_\sigma = \bigoplus_\mu I_{\mathcal{U}_\mu} \otimes \sigma_\mu$$

μ: Young tableau with k boxes

Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Schur-Weyl duality

Consider the following representations on $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes k}$:

Unitary group $U(d) \ni U \mapsto U^{\otimes k} \in \mathcal{L}(\mathcal{H})$

Symmetric group $\mathfrak{S}_k \ni \sigma \mapsto S_\sigma \in \mathcal{L}(\mathcal{H})$ s.t. $S_\sigma|i_1, \cdots, i_k\rangle = |i_{\sigma^{-1}(1)}, \cdots, i_{\sigma^{-1}(k)}\rangle$

Permutation operator

Schur-Weyl duality:

$$\mathcal{H} = \bigoplus_\mu \mathcal{U}_\mu^{(d)} \otimes \mathcal{S}_\mu^{(k)}$$
$$U^{\otimes k} = \bigoplus_\mu U_\mu \otimes I_{\mathcal{S}_\mu}$$
$$S_\sigma = \bigoplus_\mu I_{\mathcal{U}_\mu} \otimes \sigma_\mu$$

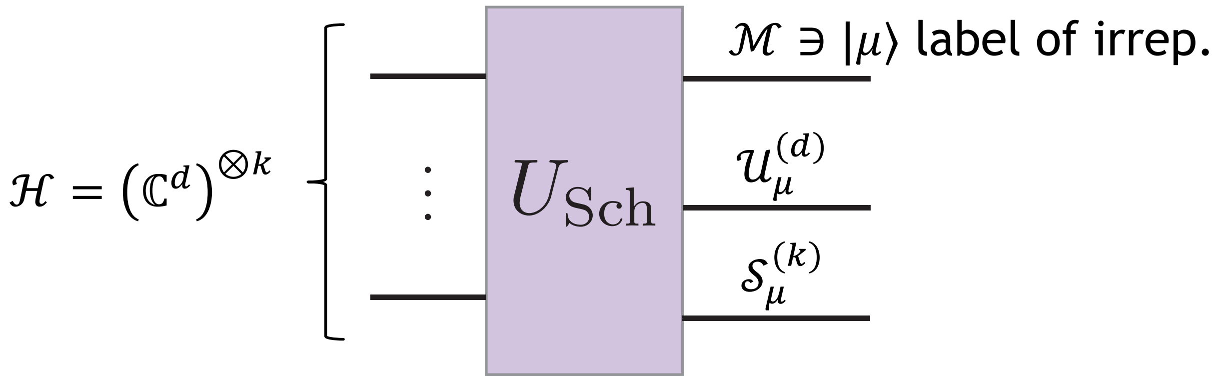
μ: Young tableau with k boxes

Irreducible representation

Result 1: Construction of the CPTP map $\widetilde{\Psi}$

- Quantum Schur transform

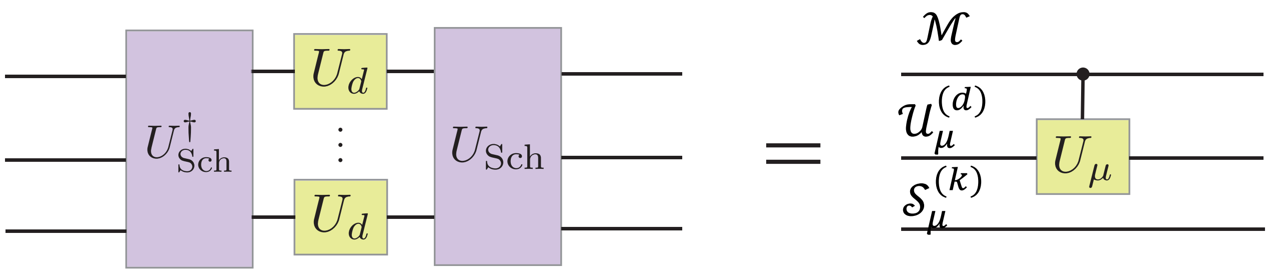
Transformation from computational basis to Schur-Weyl basis



Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Decomposition of $U^{\otimes k}$

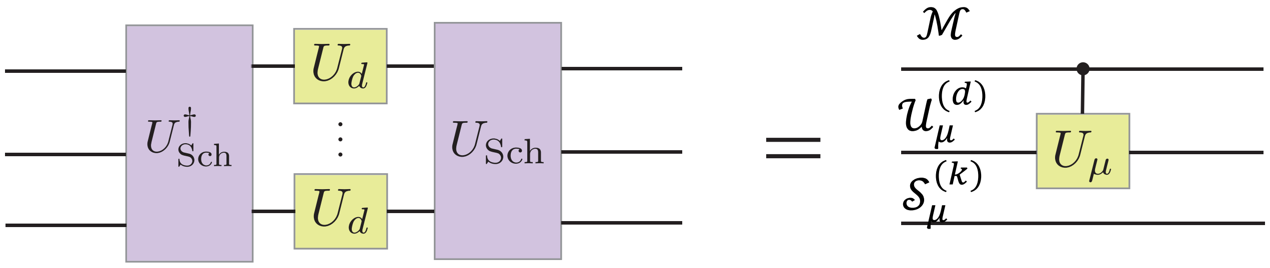
$$U^{\otimes k} = \bigoplus_{\mu} U_{\mu} \otimes I_{\mathcal{S}_{\mu}}$$



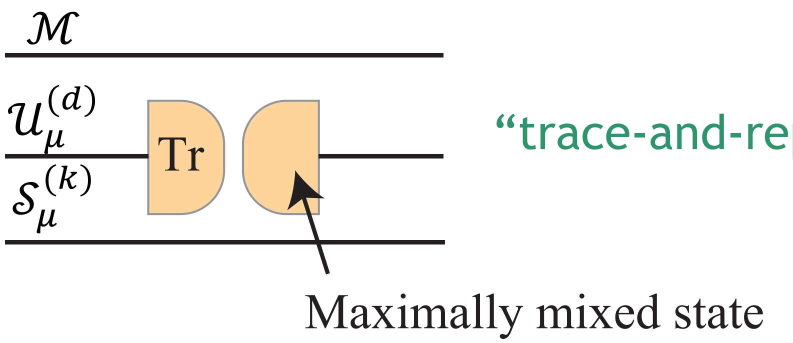
Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Decomposition of $U^{\otimes k}$

$$U^{\otimes k} = \bigoplus_{\mu} U_{\mu} \otimes I_{\mathcal{S}_{\mu}}$$



Random sampling of U_d



“trace-and-replace” of $\mathcal{U}_{\mu}^{(d)}$

Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Extend to decomposition of $V^{\otimes k}$ for isometry $V\colon \mathbb{C}^d \to \mathbb{C}^D$

$$V^{\otimes k} = \bigoplus_\mu V_\mu \otimes I_{\mathcal{S}_\mu}$$

Result 1:
Construction of the CPTP map $\widetilde{\Psi}$

- Extend to decomposition of $V^{\otimes k}$ for isometry $V: \mathbb{C}^d \to \mathbb{C}^D$

$$V^{\otimes k} = \bigoplus_\mu V_\mu \otimes I_{\mathcal{S}_\mu}$$

Isometry

$$V_\mu : \mathcal{U}_\mu^{(d)} \to \mathcal{U}_\mu^{(D)}$$

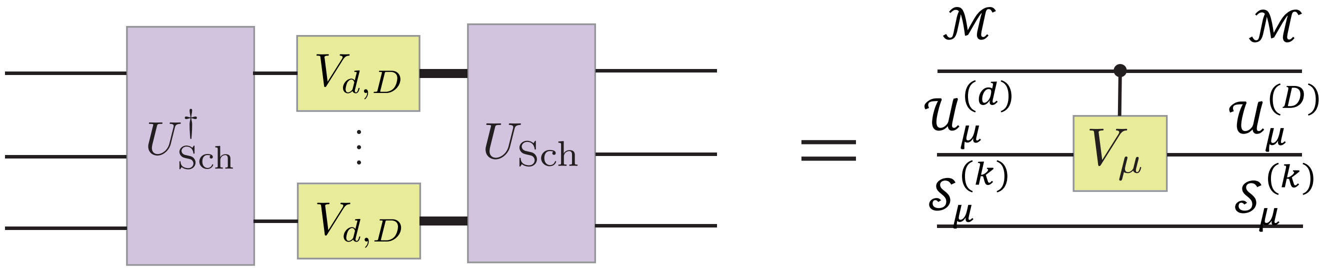
Identity

$$I_{\mathcal{S}_\mu} : \mathcal{S}_\mu^{(k)} \to \mathcal{S}_\mu^{(k)}$$

Result 1: Construction of the CPTP map $\widetilde{\Psi}$

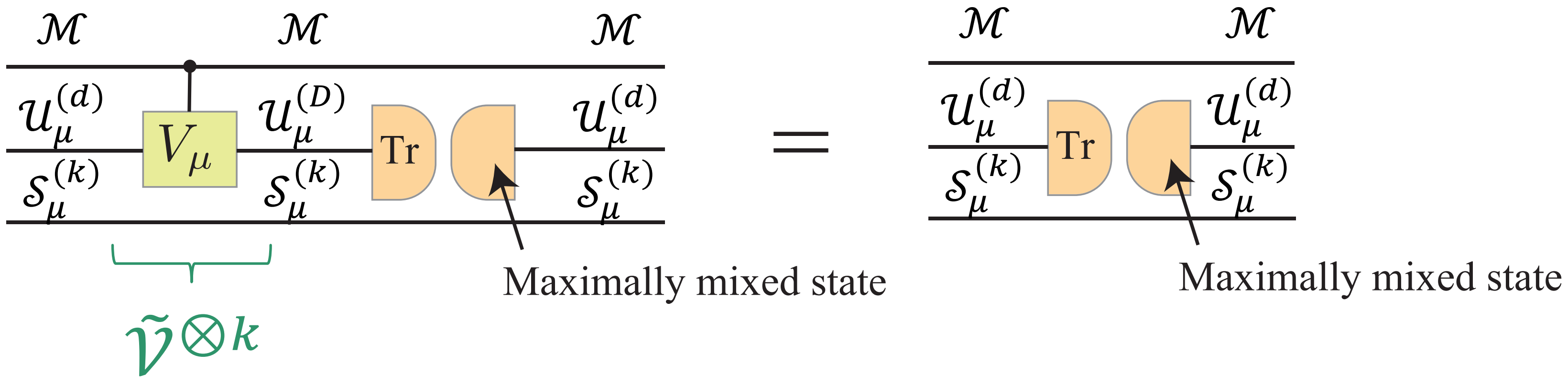
- Extend to decomposition of $V^{\otimes k}$ for isometry $V: \mathbb{C}^d \to \mathbb{C}^D$

$$V^{\otimes k} = \bigoplus_\mu V_\mu \otimes I_{\mathcal{S}_\mu}$$



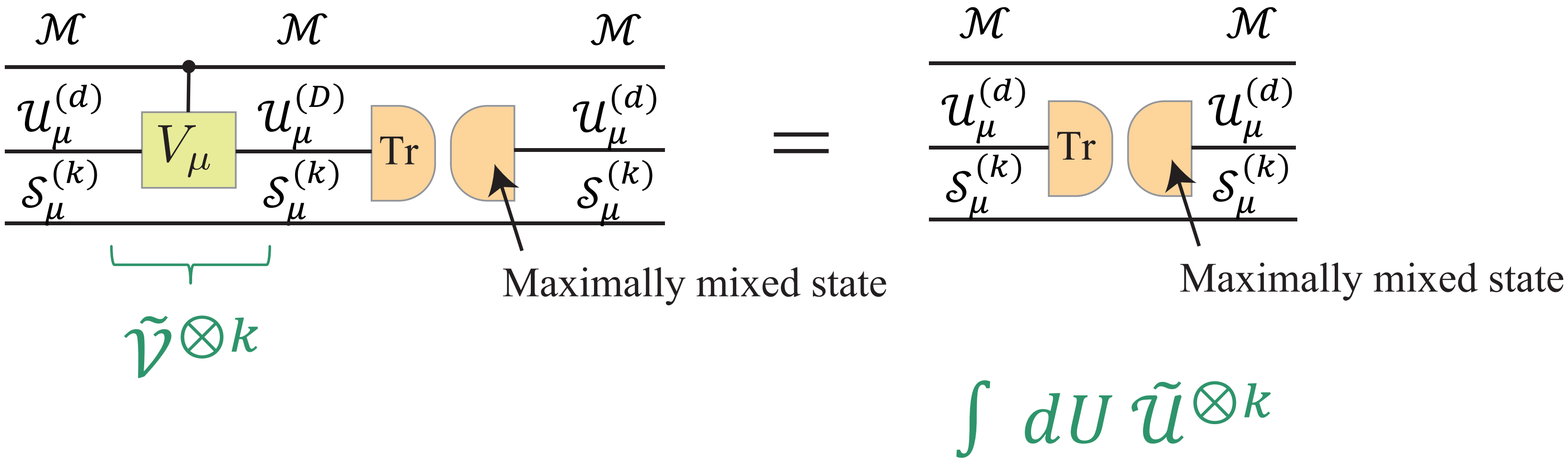
Result 1:
Construction of the CPTP map $\tilde{\Psi}$

- "Trace-and-replace" of $\mathcal{U}_\mu^{(D)}$ after $V^{\otimes k}$



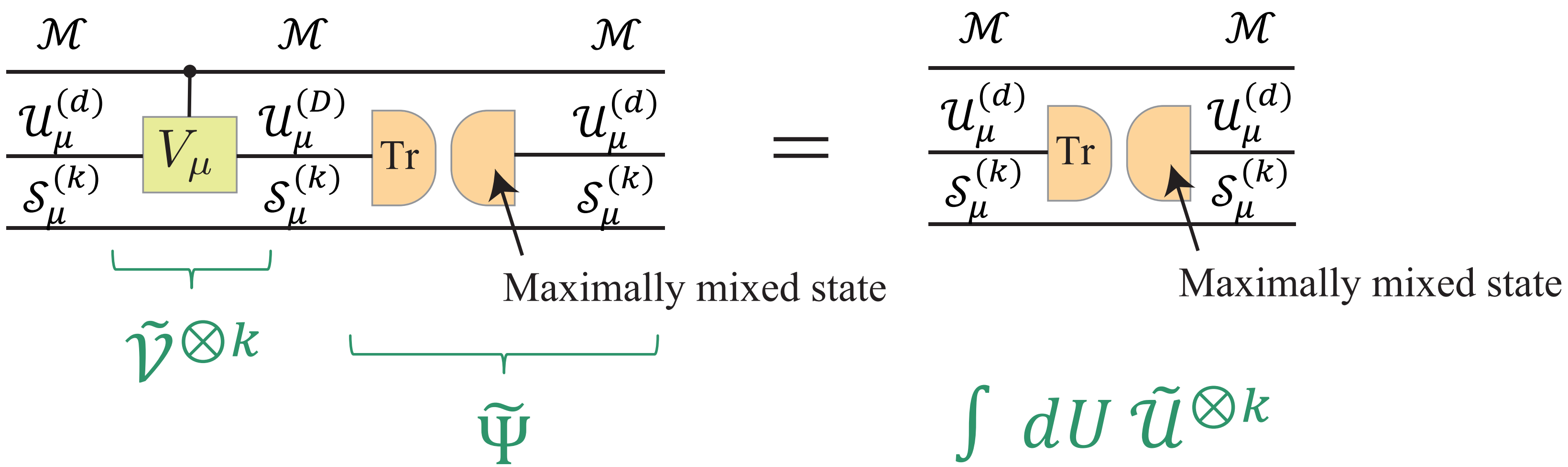
Result 1: Construction of the CPTP map $\tilde{\Psi}$

- "Trace-and-replace" of $\mathcal{U}_\mu^{(D)}$ after $V^{\otimes k}$



Result 1:
Construction of the CPTP map $\tilde{\Psi}$

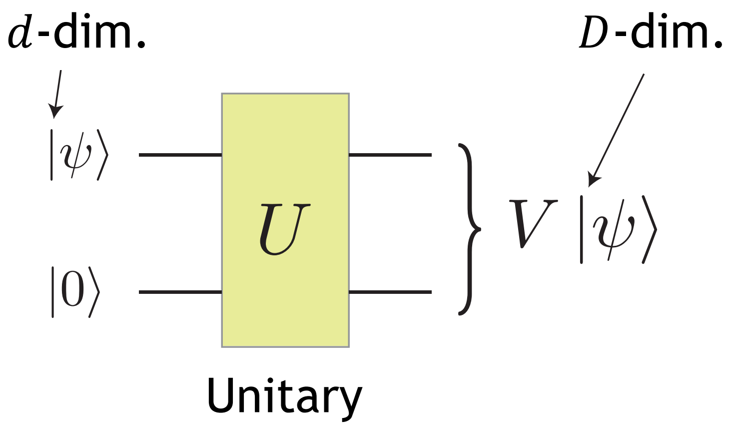
- "Trace-and-replace" of $\mathcal{U}_\mu^{(D)}$ after $V^{\otimes k}$



Result 1: Performance of isometry inversion

- Performance comparison with unitary embedding strategy

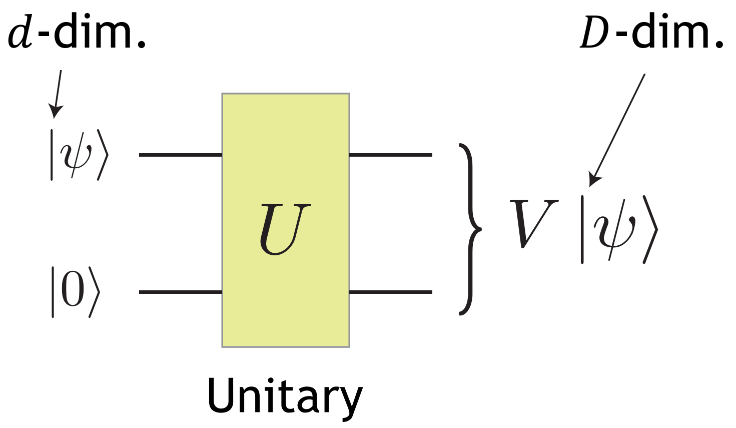
If an isometry V is given as the following form, the inverse operation $\tilde{\mathcal{V}}_{\mathrm{inv}}$ can be implemented by inverting the unitary U.



Result 1:
Performance of isometry inversion

- Performance comparison with unitary embedding strategy

If an isometry V is given as the following form, the inverse operation $\tilde{\mathcal{V}}_{\mathrm{inv}}$ can be implemented by inverting the unitary U.

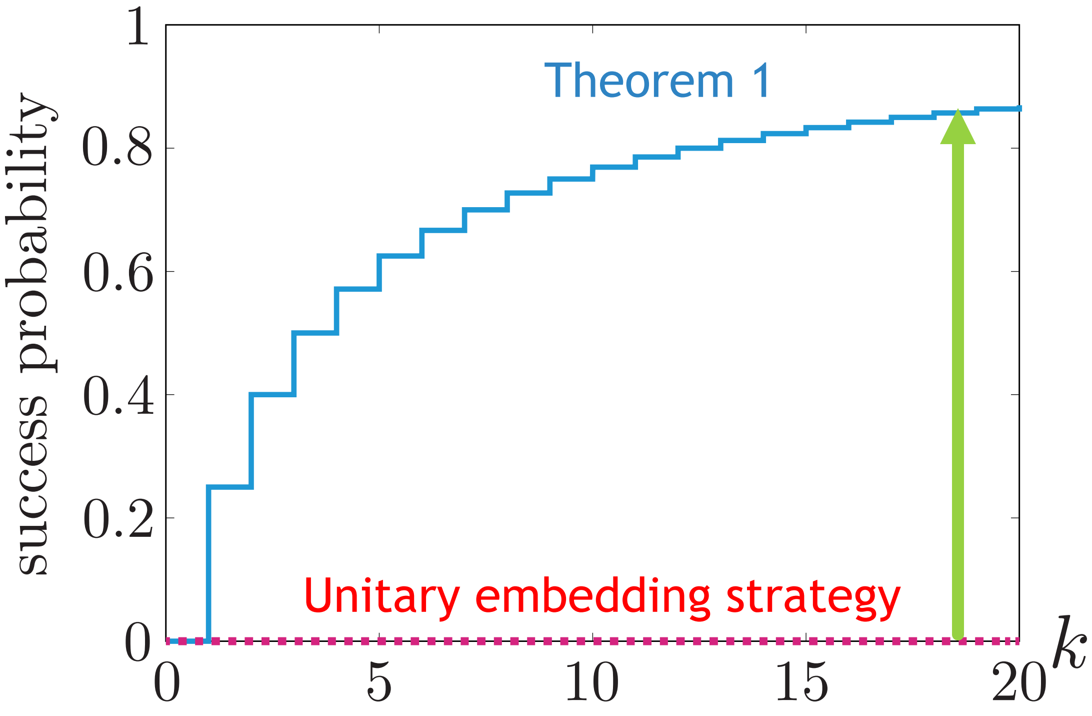


However, the success probability depends on D.

Result 1:
Performance of isometry inversion

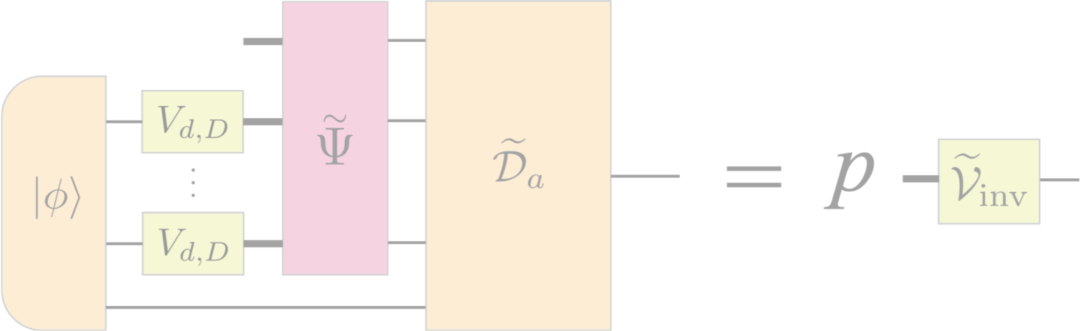
- Performance comparison with unitary embedding strategy

Eg. 5 qubit code ($d = 2, D = 2^5$)

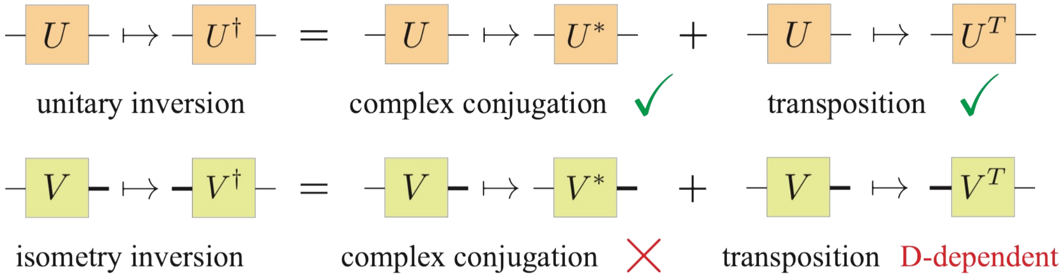


Result

- Construction of efficient probabilistic protocol for isometry inversion



- Difference between unitary inversion and isometry inversion



Result 2:
Direct extension of unitary inversion?

- Main idea for unitary inversion protocol in [Quintino et al. 2019]

$$-\boxed{U}- \mapsto -\boxed{U^\dagger}- \;=\; -\boxed{U}- \mapsto -\boxed{U^*}- \;+\; -\boxed{U}- \mapsto -\boxed{U^T}-$$

unitary inversion — complex conjugation ✓ — transposition ✓

Result 2:
Direct extension of unitary inversion?

- Main idea for unitary inversion protocol in [Quintino et al. 2019]

$$U \mapsto U^\dagger \quad = \quad U \mapsto U^* \quad + \quad U \mapsto U^T$$

unitary inversion — complex conjugation ✓ — transposition ✓

- Similar strategy for isometry inversion?

$$V \mapsto V^\dagger \quad = \quad V \mapsto V^* \quad + \quad V \mapsto V^T$$

isometry inversion — complex conjugation — transposition

Result 2:
Direct extension of unitary inversion?

- Main idea for unitary inversion protocol in [Quintino et al. 2019]

$$U \mapsto U^\dagger \quad = \quad U \mapsto U^* \quad + \quad U \mapsto U^T$$

unitary inversion | complex conjugation ✓ | transposition ✓

- Similar strategy for isometry inversion? → No!

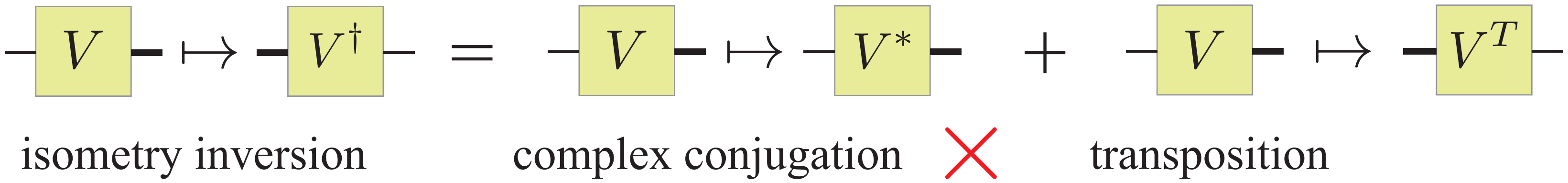
$$V \mapsto V^\dagger \quad = \quad V \mapsto V^* \quad + \quad V \mapsto V^T$$

isometry inversion | complex conjugation | transposition

Result 2:
Direct extension of unitary inversion?

- Isometry complex conjugation is impossible.

> **Theorem 3.** Probabilistic isometry complex conjugation is impossible when $D \geq 2d$.

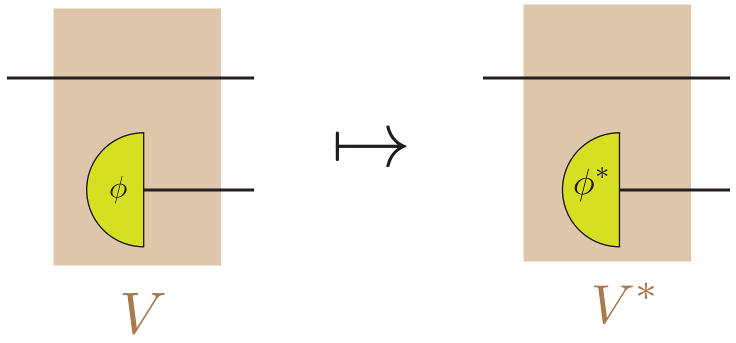


Result 2:
Direct extension of unitary inversion?

- Isometry complex conjugation is impossible.

Theorem 3. Probabilistic isometry complex conjugation is impossible when $D \geq 2d$.

Proof idea: Impossibility of state complex conjugation $|\phi\rangle \mapsto |\phi^*\rangle$ [Yang et al. 2014]

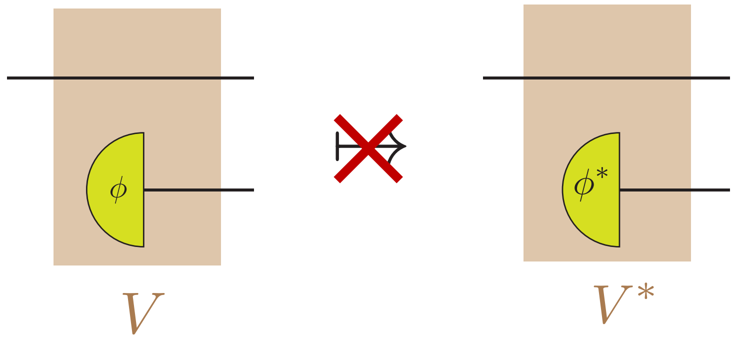


Result 2:
Direct extension of unitary inversion?

- Isometry complex conjugation is impossible.

Theorem 3. Probabilistic isometry complex conjugation is impossible when $D \geq 2d$.

Proof idea: Impossibility of state complex conjugation $|\phi\rangle \mapsto |\phi^*\rangle$ [Yang et al. 2014]



Result 2:
Direct extension of unitary inversion?

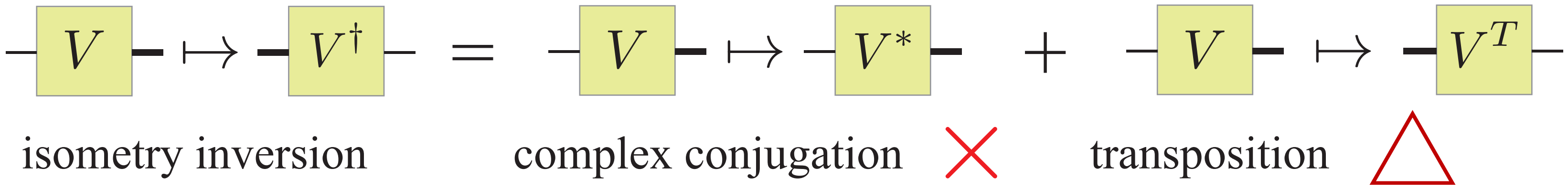
- Isometry transposition is possible but inefficient.

Modified port-based teleportation → Isometry transposition

Theorem 4. There exists a probabilistic isometry transposition protocol with the success probability

$$p = \frac{k}{Dd + k - 1}.$$

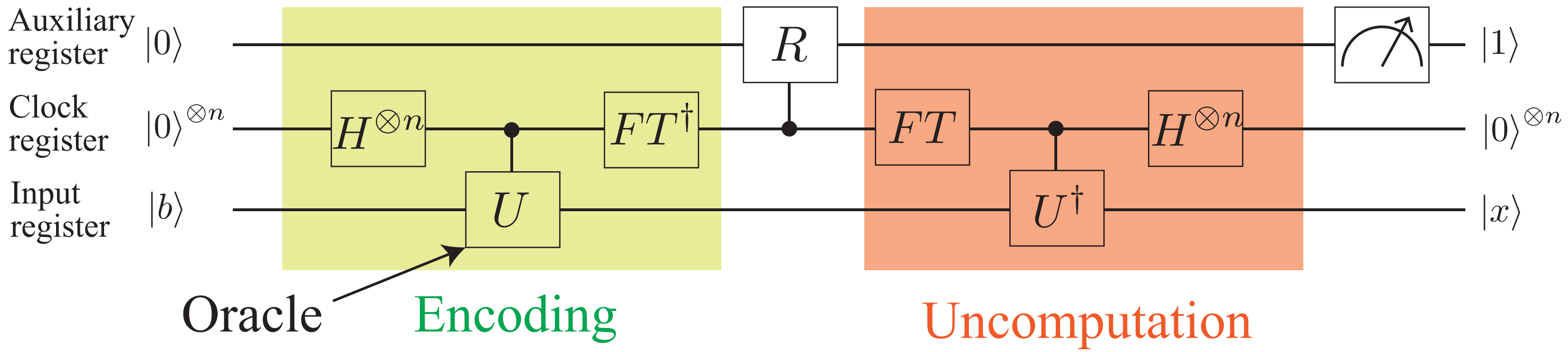
But this protocol is inefficient since the success probability depends on D.



Application

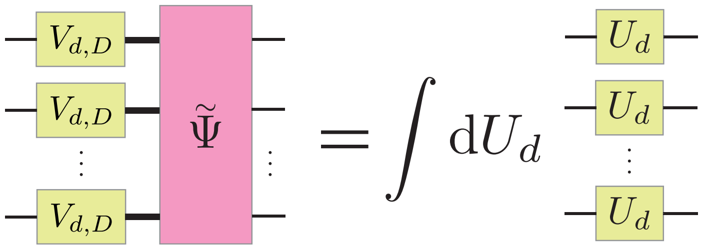
- Quantum algorithms with encoding oracle and its inverse (uncomputation)

Eg. HHL algorithm



Summary

- Isometry inversion: Decoding a black box encoding V using k copies of the black box
- Success probability $p = 1 - \mathcal{O}(d^3/k)$ ⟵ Independent of D
- Main idea: CPTP map $\widetilde{\Psi}$ transforms parallel copies of any isometry into parallelized random unitary



- Difference with unitary inversion