A framework for private distributed quantum sensing

Luís Bugalho

Instituto Superior Técnico, Universidade de Lisboa, Portugal
Physics of Information and Quantum Technologies Group, PQI – Portuguese Quantum Institute & CeFEMA, Portugal
Sorbonne Université, LIP6, CNRS, Paris, France

SNQS Workshop - 29-Jan-2025

Motivation

- Some states hold an important property for a quantum sensor network:

Privacy!

GHZ state is capable of estimating the average of a set of parameters

$$\theta_1 + \theta_2 + \ldots + \theta_n$$

Goal

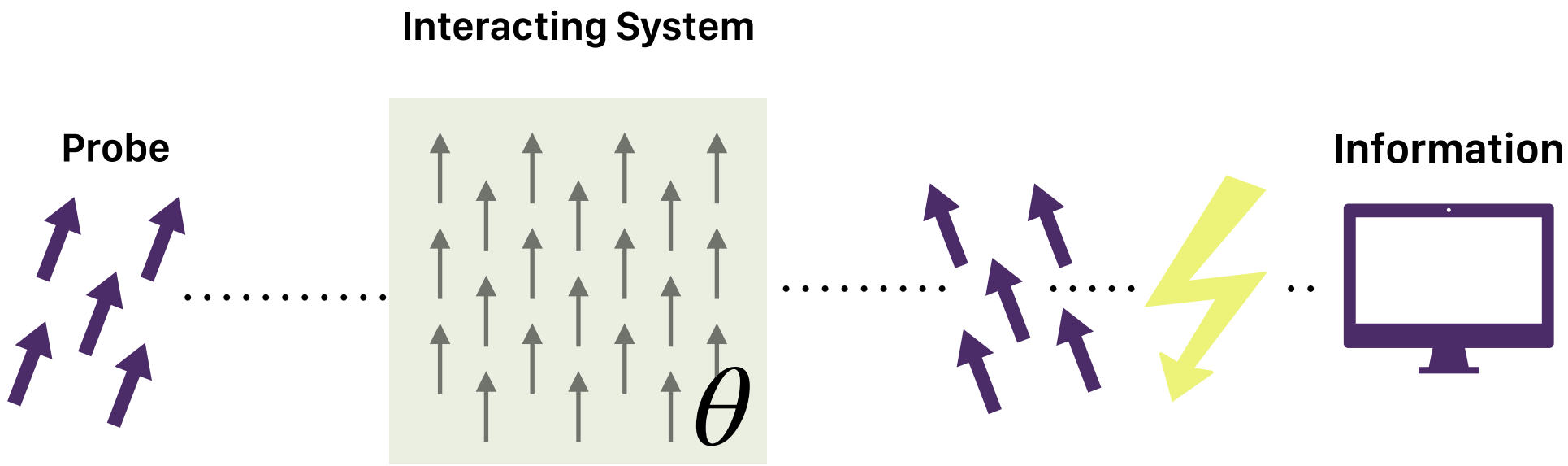
- **How do we find private states?**
- **Are there more than the canonical private state (GHZ state)?**
- **What should we take into account to find them?**
- **How do we make them resilient?**

State of the art

- **Quantum Sensor Networks**
  - Formulation and results regarding entanglement advantage or not
  - Rubio, J., Knott, P. A., Proctor, T. J. & Dunningham, J. A. *Quantum sensing networks for the estimation of linear functions*. Journal of Physics A: Mathematical and Theoretical **53**, 344001 (2020)
  - Qian, T., Bringewatt, J., Boettcher, I., Bienias, P. & Gorshkov, A. V. *Optimal measurement of field properties with quantum sensor networks*. Physical Review A 103, L030601 (2021).
- **Private quantum sensor networks**
  - Introduction of the notion of privacy in networks of quantum sensors
  - Shettell, N., Hassani, M. & Markham, D. *Private network parameter estimation with quantum sensors*. arXiv.2207.14450 (2022).
  - Shettell, N., Kashefi, E. & Markham, D. *Cryptographic approach to quantum metrology*. Phys. Rev. A 105, L010401 (2022).

Quantum Sensing

Quantum sensing for a local parameter:



$$\rho_0 \longmapsto \Lambda_\theta(\,\cdot\,) \longmapsto \rho_\theta \longmapsto \Pi_x \longmapsto p(x\,|\,\theta)$$

$\rho_0 \in \mathscr{H}_n$

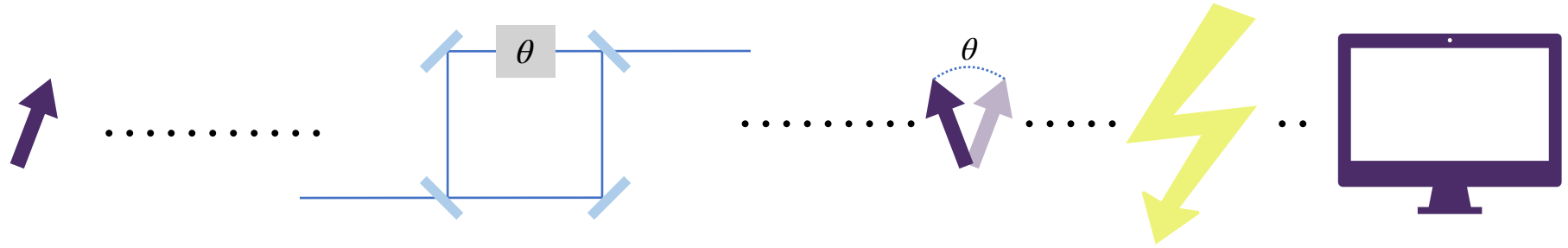
Quantum Sensing

Example:

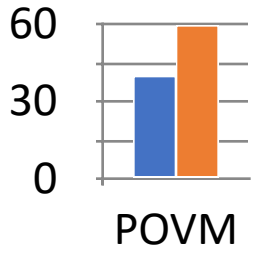
Probe
Photon

Interacting System
Interferometer

Information



$$|0\rangle + |1\rangle \longmapsto e^{i\theta\hat{Z}} \longmapsto |0\rangle + e^{i\theta}|1\rangle \longmapsto \begin{matrix} |+\rangle\langle +| \\ |-\rangle\langle -| \end{matrix} \longmapsto \begin{matrix} p(+|\theta) = \cos(2\theta)^2 \\ p(-|\theta) = \sin(2\theta)^2 \end{matrix}$$



MLE $\longrightarrow$ $\hat{\theta} = f^{-1}(p)$

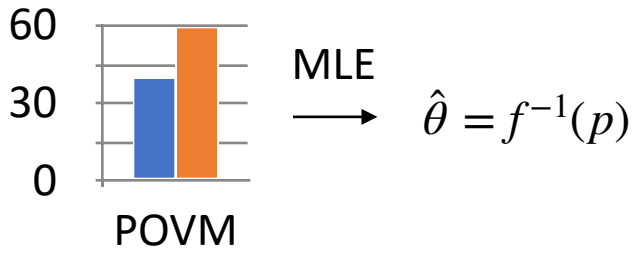
Maximum Likelihood Estimator

$$\text{mle}(\boldsymbol{\theta}) = \prod_x p(x|\boldsymbol{\theta})^{f(x)}$$

$$\log \text{mle}(\boldsymbol{\theta}) = \sum_x f(x) \ \log p(x|\boldsymbol{\theta})$$

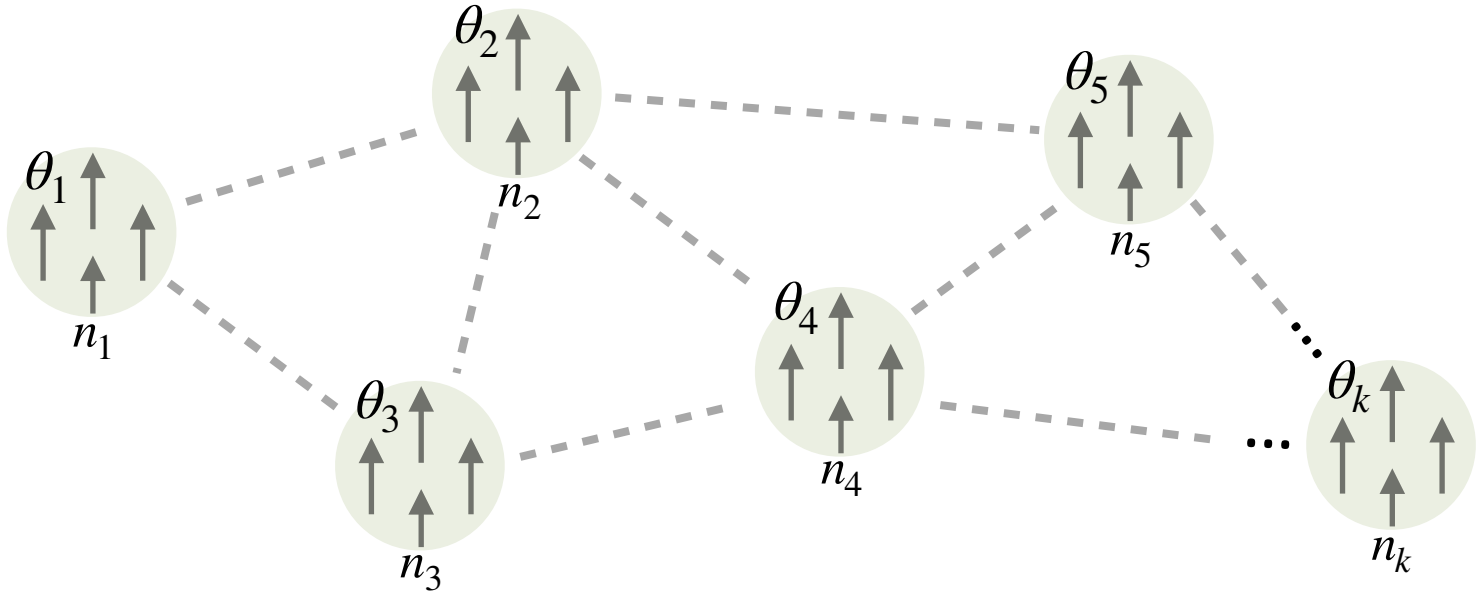
$$\hat{\boldsymbol{\theta}} \rightarrow \arg\max_{\boldsymbol{\theta}} \text{mle}(\boldsymbol{\theta})$$

$$F(\boldsymbol{\theta}) \rightarrow -\nabla^2 \log \text{mle}(\hat{\boldsymbol{\theta}})$$



Quantum Sensor Networks

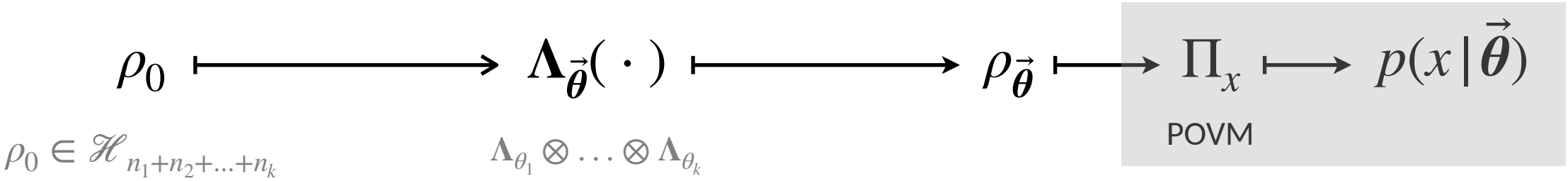
Now, consider we have a network, where a collection of parameters is encoded in each qubit via a process similar as before:



$$\rho_0 \longmapsto \Lambda_{\vec{\theta}}(\,\cdot\,) \longmapsto \rho_{\vec{\theta}} \longmapsto \Pi_x \longmapsto p(x\,|\,\vec{\theta})$$

$\rho_0 \in \mathscr{H}_{n_1+n_2+\ldots+n_k}$ $\quad$ $\Lambda_{\theta_1} \otimes \ldots \otimes \Lambda_{\theta_k}$

Quantum Sensor Networks



Important metrics in this scenario:

- **Precision** one can achieve for estimating θ (scaling with the #resources)
  - $\text{cov}(\vec{\theta}) \geq \frac{\boldsymbol{F}_{\mathcal{Q}}^{-1}}{m}$
- **Robustness** to errors in the system
- **Privacy** against dishonest parties:
  - Access to a shared function of the parameters $f(\vec{\theta})$

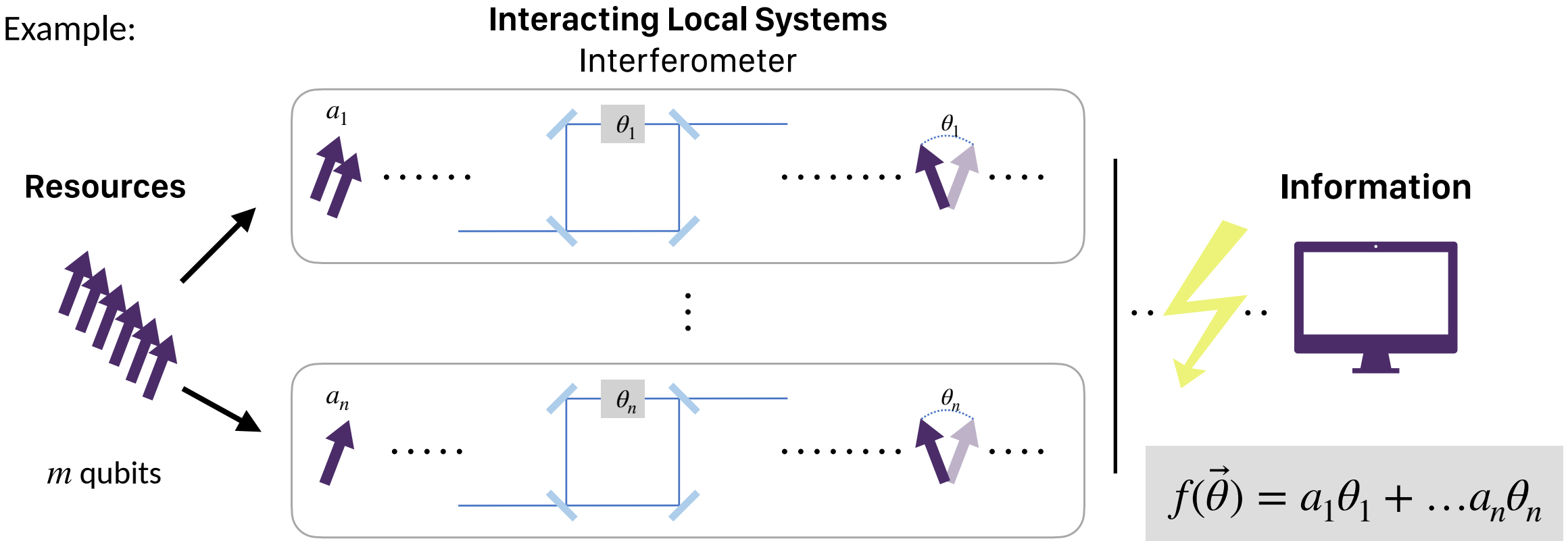
Shettell, N., Hassani, M. & Markham, D. Private network parameter estimation with quantum sensors. arXiv.2207.14450 (2022).

Distributed Quantum Sensing

Example:

Interacting Local Systems

Interferometer



$$f(\vec{\theta}) = a_1\theta_1 + \ldots a_n\theta_n$$

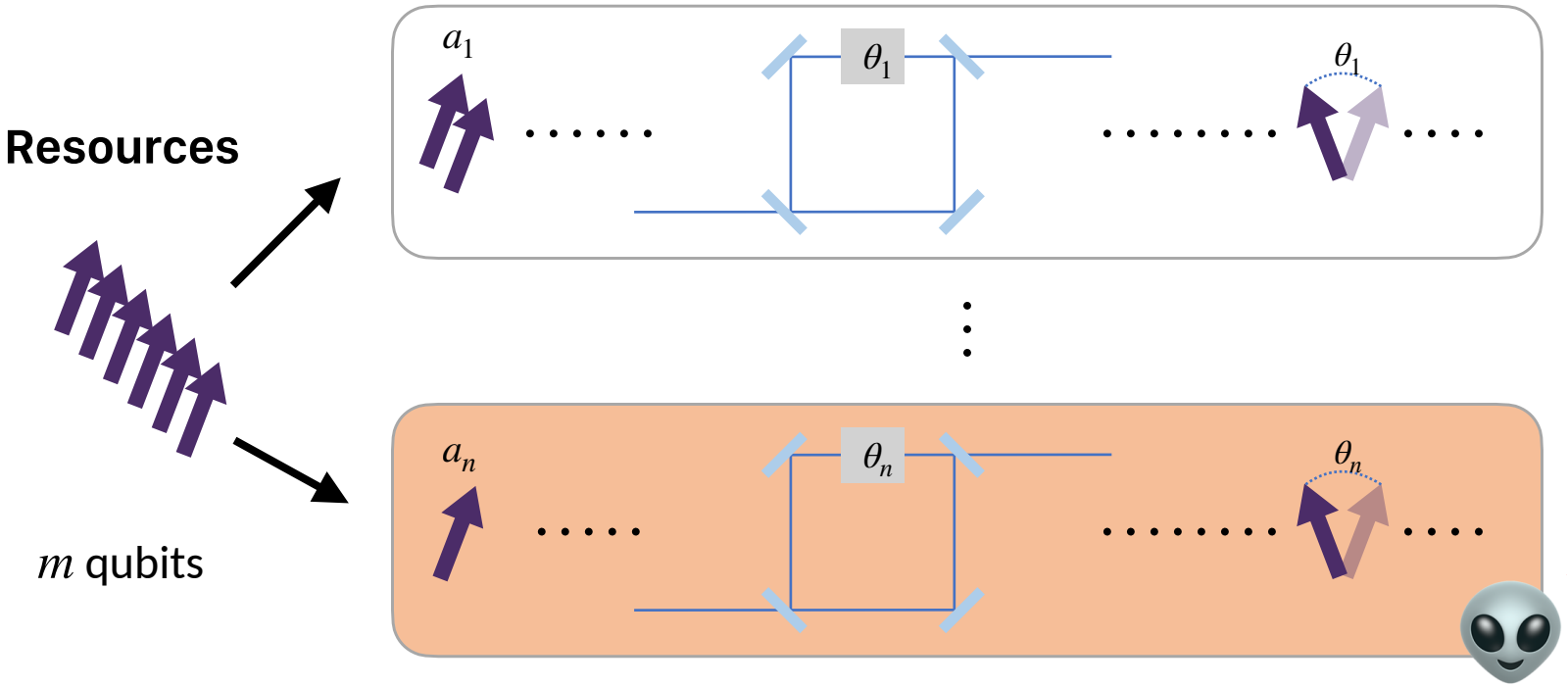
$$|0\rangle^{\otimes m} + |1\rangle^{\otimes m} \longmapsto |0\rangle^{\otimes m} + e^{if(\vec{\theta})}|1\rangle^{\otimes m} \longmapsto \begin{matrix} |E\rangle\langle E| \\ |O\rangle\langle O| \end{matrix} \longmapsto \begin{matrix} p(E|\theta) = \cos(2f(\vec{\theta}))^2 \\ p(O|\theta) = \sin(2f(\vec{\theta}))^2 \end{matrix}$$

Distributed Quantum Sensing

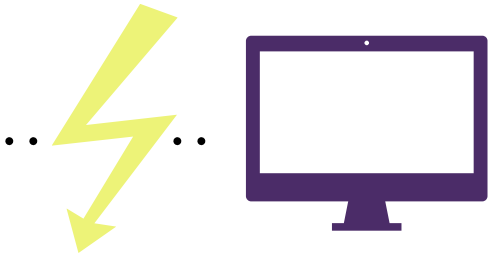
Example:

Interacting Local Systems

Interferometer



Information



$$f(\vec{\theta}) = a_1\theta_1 + \ldots a_n\theta_n$$

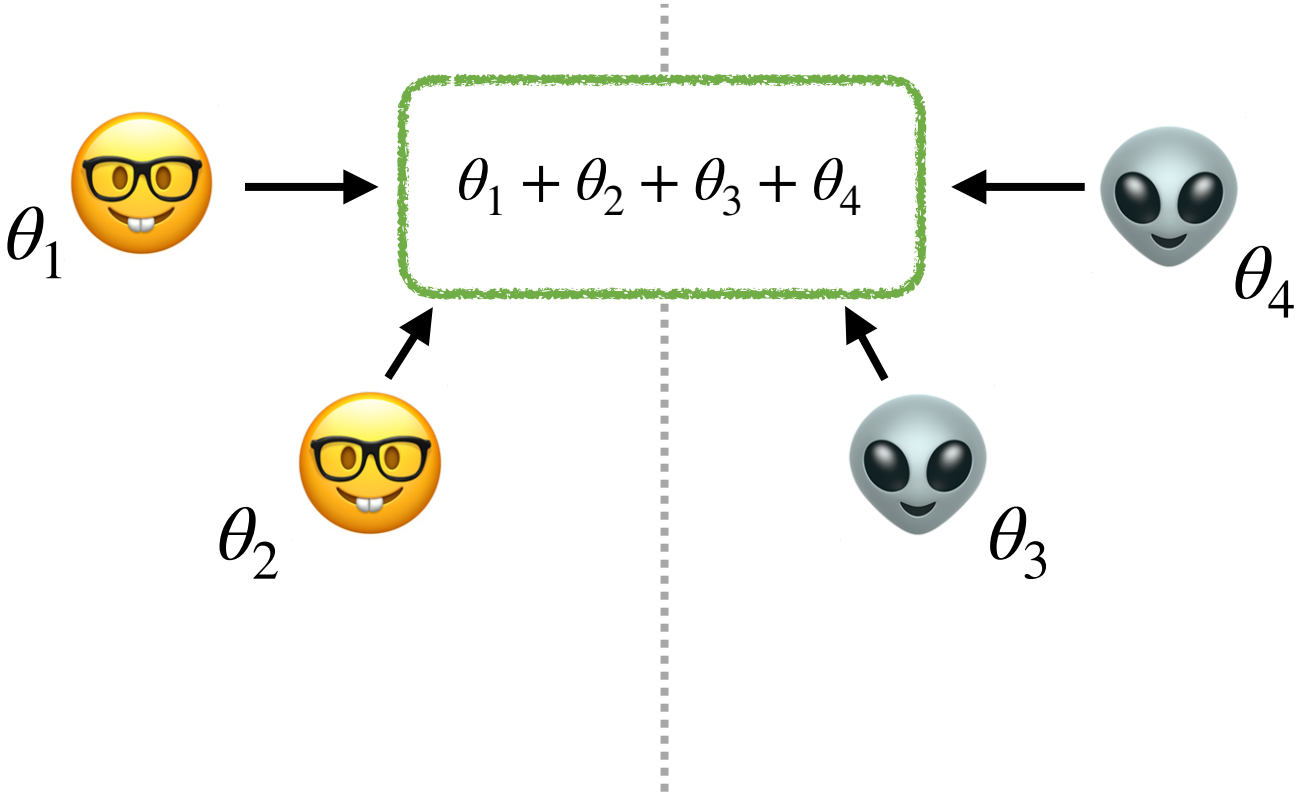
$$g(\vec{\theta}) = ?$$

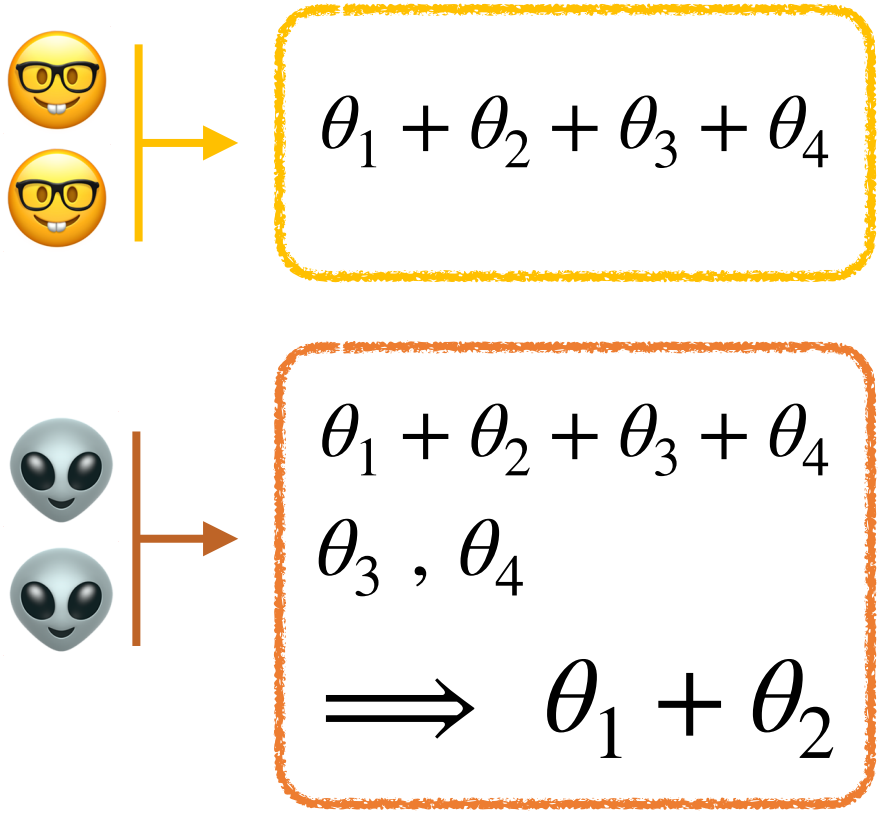
Privacy - Basics

- The privacy definition can be stated by the following:
  i. Let H and D be the subsets of honest and dishonest parties, respectively;
  ii. If all parties are honest, they can estimate $f(\vec{\theta})$
  iii. For any set of dishonest parties D, the set D can only know the function $f(\vec{\theta})$ and all θ_μ for $\mu \in D$ (and functions thereof).

Privacy - Example

- Considering we have 4 parties: 2 honest and 2 dishonest





Privacy - Defining a Measure

- **Privacy Measure**:
  - $\mathscr{P} = \mathscr{P}(\mathcal{Q}, \vec{a})$, the privacy is a function of the QFI matrix with respect to parameters $\vec{\theta}$, and the target function characterized by $f(\vec{\theta}) = \vec{a} \cdot \vec{\theta}$
  - $\mathscr{P}(\mathcal{Q}, \vec{a}) \in [0,1]$
  - $\mathscr{P}(\mathcal{Q}, \vec{a}) = 1$ iff. $\mathcal{Q} = \alpha \vec{a}\vec{a}^T$
  - $\mathscr{P}(B\mathcal{Q}B^T, B\vec{a}) = \mathscr{P}(\mathcal{Q}, \vec{a})$
  - Continuity of the QFI should imply continuity of the privacy measure

DEF: $$\mathscr{P}(\mathcal{Q}, \vec{a}) = \frac{\vec{a}^T \mathcal{Q} \vec{a}}{\mathrm{Tr}\,\mathcal{Q}} \equiv \frac{\mathrm{Tr}\left[\mathcal{Q}\vec{a}\vec{a}^T\right]}{\mathrm{Tr}\,\mathcal{Q}} = \frac{\mathrm{Tr}\left[\mathcal{Q}W_{\vec{a}}\right]}{\mathrm{Tr}\,\mathcal{Q}}$$

Privacy - Defining a Measure

- **Privacy Example**:
  - Suppose I have a QFI matrix given by:

$$\mathcal{Q} = \lambda_1 \vec{a}\vec{a}^T + \lambda_2 \vec{b}\vec{b}^T$$

$$||\vec{a}|| = ||\vec{b}|| = 1$$

$$\mathcal{P}(\mathcal{Q}, \vec{a}) = \frac{\lambda_1}{\lambda_1 + \lambda_2} < 1$$

This means that one could build an estimator with finite variance for any linear function $h(\vec{\theta}) = \vec{c} \cdot \vec{\theta}$, where $\vec{c} \in \mathcal{L}(\vec{a}, \vec{b})$. Suppose $\vec{c} = \alpha\vec{a} + \beta\vec{b}$, then the variance of an estimator for $\hat{h}$ would be:

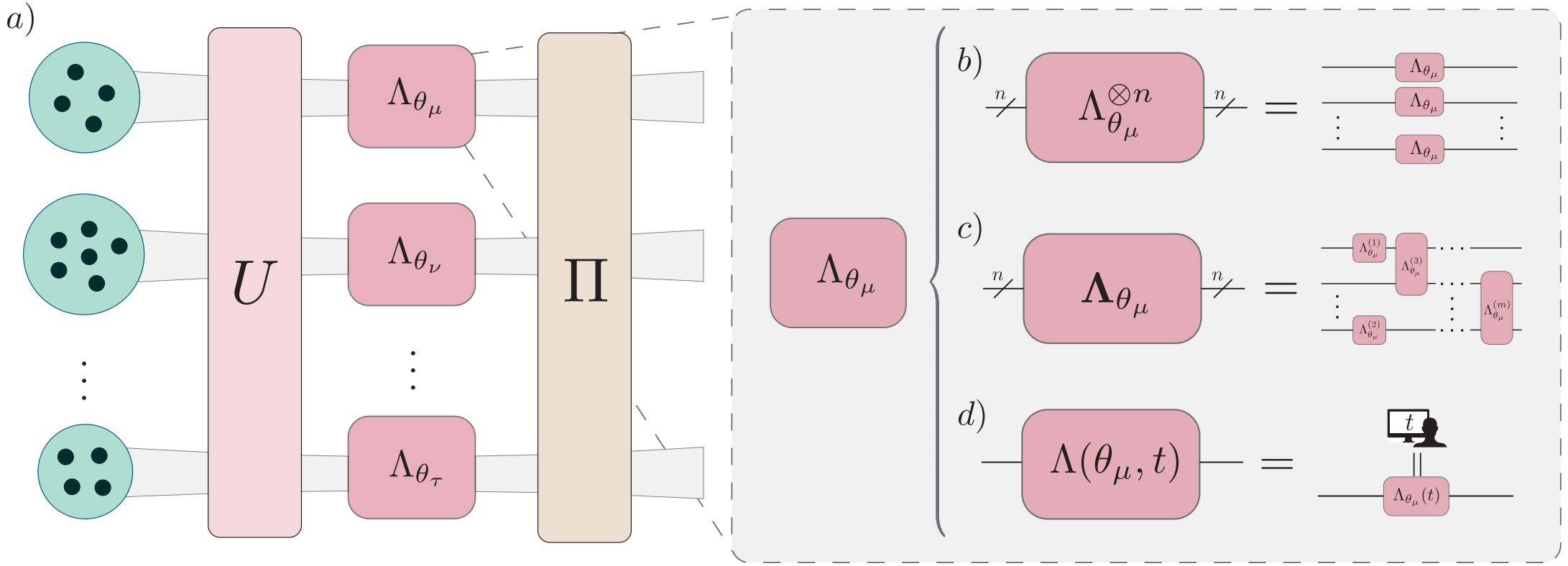
$$\Delta\hat{h}^2 = \frac{|\alpha|^2}{\lambda_1} + \frac{|\beta|^2}{\lambda_2} = \vec{c}^T \mathcal{Q}^+ \vec{c}$$

Privacy - Assumptions

- **Privacy** will depend on three main things:
  - Encoding dynamics
  - Linear Functions
  - Resources

THEY ARE ALL CONNECTED!

Privacy - Encoding Dynamics



Local Dynamics!

$$\rho_0 \quad \rightarrow \quad \rho_{\boldsymbol{\theta}}$$

Privacy - Linear Functions

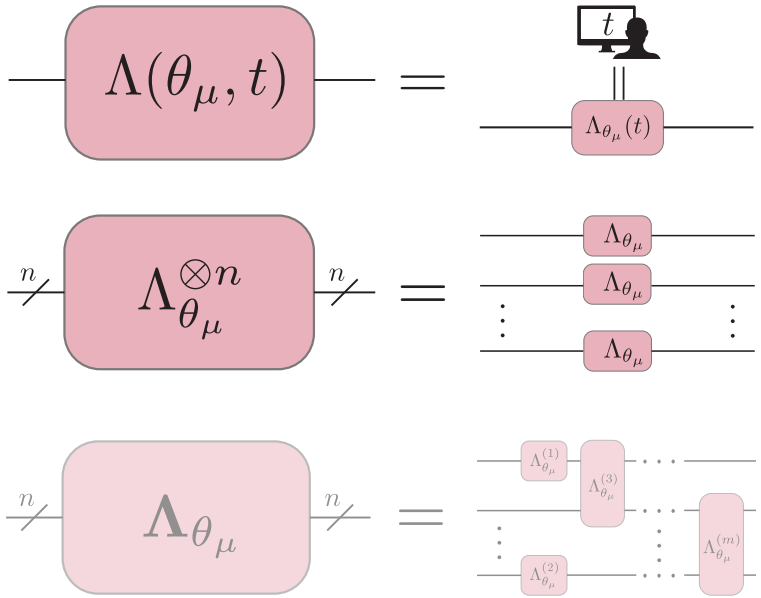
$$f(\vec{\theta}) = \vec{a} \cdot \vec{\theta}$$

(or any $g(\vec{\theta}) = \alpha f(\vec{\theta}), \alpha \in \mathbb{R}$)

(a) $\vec{a} \in \mathbb{R}^k$ - requires controllable encoding dynamics

(b) $\vec{a} \in \mathbb{Z}^k$ - related with the number of qubits available locally ($\vec{a} \in \mathbb{Q}^k$ can be reduced to this case)

(c) $\vec{a} \in \mathcal{O}_-^2$ - requires knowledge of the local hamiltonians' eigenvalues



$$t \to \vec{t} = \vec{a}, \quad \vec{n} = \vec{1}$$

$$gcd(\vec{a}) = gcd(a_1, a_2, \ldots, a_k) = 1\,!$$

$$\simeq$$

$$\vec{a} \in \Lambda_1 \times \ldots \times \Lambda_k, \; \Lambda_\mu = \{\lambda_j^\mu\}_{j \in \mu}$$

Privacy - Resources in Separable Dynamics

- A resource for sensing relates with the amount of sampling done. For separable local Hamiltonians the sampling is the number of qubits.
- **Resources** vectors $\vec{n}$: number of qubits in each node

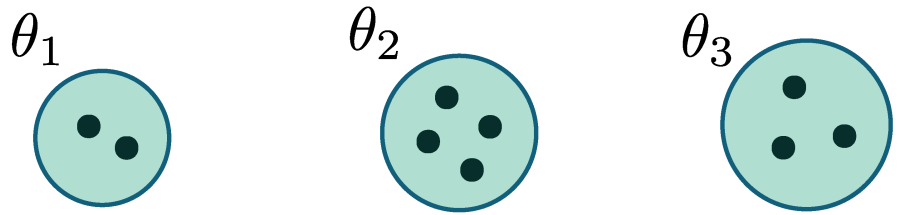
  (I) $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$ - No privacy Zone

  (II) $\vec{n} = \vec{a}$ - Minimal Privacy Zone

  (III) $\vec{a} \prec \vec{n}$ and ($\vec{n} \prec 2\vec{a}$ or $\vec{n} \not\preceq 2\vec{a}$) - Minimal plus Ancilla Privacy Zone

  (IV) $2\vec{a} \preceq \vec{n}$ - Multiple Privacy Zone
- Examples:
  - $\vec{n} = (1,2,3) \prec (1,3,4) = \vec{a}$ (I)
  - $\vec{n} = (2,4,3) \not\prec (1,3,4) = \vec{a}$ (I)
  - $\vec{a} = (1,3,4) \prec \vec{n} = (2,5,4) \prec (2,6,8) = 2\vec{a}$ (III)
  - $2\vec{a} = (2,6,8) \prec (3,10,12) = \vec{n}$ (IV)

Step 1: *Verify if we have sufficient qubits for the target function*



$$gcd(\vec{a}) = gcd(a_1, a_2, \cdots, a_k) = 1$$

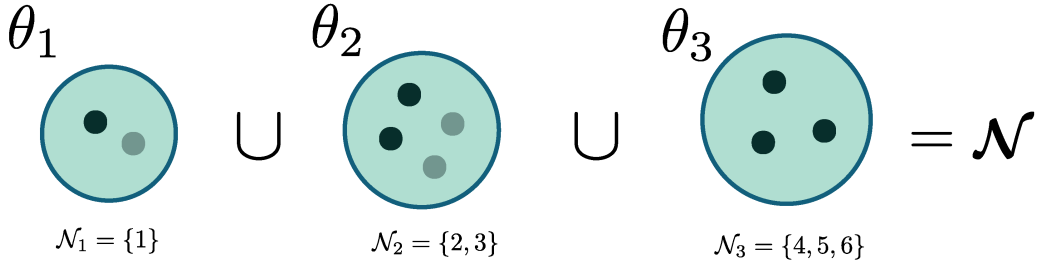
$$\vec{n} = (2, 4, 3) \succeq \vec{a} = (1, 2, 3)$$

Thms. 3.1 and 3.3: ∃ minimum amount of qubit resources required!

Need at least $\vec{n} = \vec{a}$ distributed resources.

Bugalho, L., Hassani, M., Omar, Y. & Markham, D. Private and Robust States for Distributed Quantum Sensing. Quantum **9**, 1596 (2025)

Step 2: *Build first private state family with minimal resources*



$n = 1+2+3, s \in \{0,1\}^n$

$s_0 = (0\ 00\ 000) \quad s_1 = (1\ 11\ 111)$

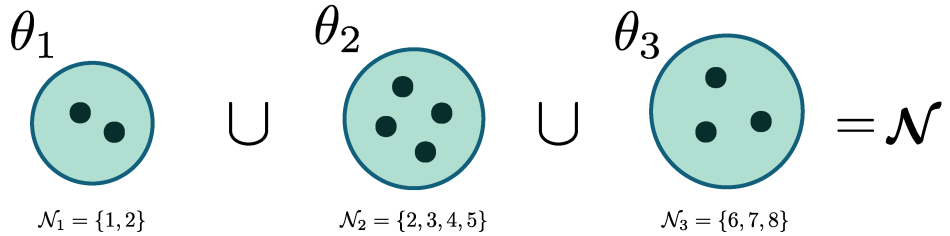
Such that: $\vec{h}_{\mathcal{N}}(s_1) - \vec{h}_{\mathcal{N}}(s_0) = \vec{a}$

$$\mathcal{F} = \{\alpha |s_0\rangle + \beta |s_1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

Thms. 3.2 and 3.4: ∃ only one family of private states for $\vec{n} = \vec{a}$ distributed resources.

Bugalho, L., Hassani, M., Omar, Y. & Markham, D. Private and Robust States for Distributed Quantum Sensing. Quantum **9**, 1596 (2025)

Step 3: *Build robust and private families by adding extra qubits*



$$n = 2+4+3, s \in \{0,1\}^n$$

$$
\begin{aligned}
s_0^0 &= (\overset{b_2}{0}0\ \overset{b_1b_0}{0}000\ 000), s_1^0 = (\overset{b_2}{1}0\ \overset{b_1b_0}{1}100\ 111)\\
s_0^1 &= (00\ 0001\ 000), s_1^1 = (10\ 1101\ 111)\\
s_0^2 &= (00\ 0011\ 000), s_1^2 = (10\ 1111\ 111)\\
s_0^3 &= (01\ 0000\ 000), s_1^3 = (11\ 1100\ 111)\\
s_0^4 &= (01\ 0001\ 000), s_1^4 = (11\ 1101\ 111)\\
s_0^5 &= (01\ 0011\ 000), s_1^5 = (11\ 1111\ 111)
\end{aligned}
$$

Such that: $\vec{h}_{\mathcal{N}}(s_1^j) - \vec{h}_{\mathcal{N}}(s_0^j) = \vec{a},\ \forall\ j$

$$\mathcal{F}_j = \left\{ \sum_{\sigma \in S_{\mathcal{N}}} \alpha_\sigma \left|\sigma(s_0^j)\right\rangle + \sum_{\sigma \in S_{\mathcal{N}}} \beta_\sigma \left|\sigma(s_1^j)\right\rangle, \alpha_\sigma, \beta_\sigma \in \mathbb{C}, \text{normalized} \right\}$$

Thm. 3.5: ∃ a countable number of families of private states for $2\vec{a} \succeq \vec{n} \succeq \vec{a}$ distributed resources.

$$\mathcal{F}_j = \left\{ \sum_{\sigma \in S_{\mathcal{N}}} \alpha_\sigma \left| \sigma(s_0^j) \right\rangle + \sum_{\sigma \in S_{\mathcal{N}}} \beta_\sigma \left| \sigma(s_1^j) \right\rangle, \alpha_\sigma, \beta_\sigma \in \mathbb{C}, \text{normalized} \right\}$$

$$\begin{matrix} |0\rangle_L \\ |1\rangle_L \end{matrix} \longmapsto |\psi\rangle = \sum_j \alpha_j |j_1\rangle_L |j_2\rangle_L \dots |j_l\rangle$$

Thm. 3.6: All states built like this are private states.

Bugalho, L., Hassani, M., Omar, Y. & Markham, D. Private and Robust States for Distributed Quantum Sensing. Quantum **9**, 1596 (2025)

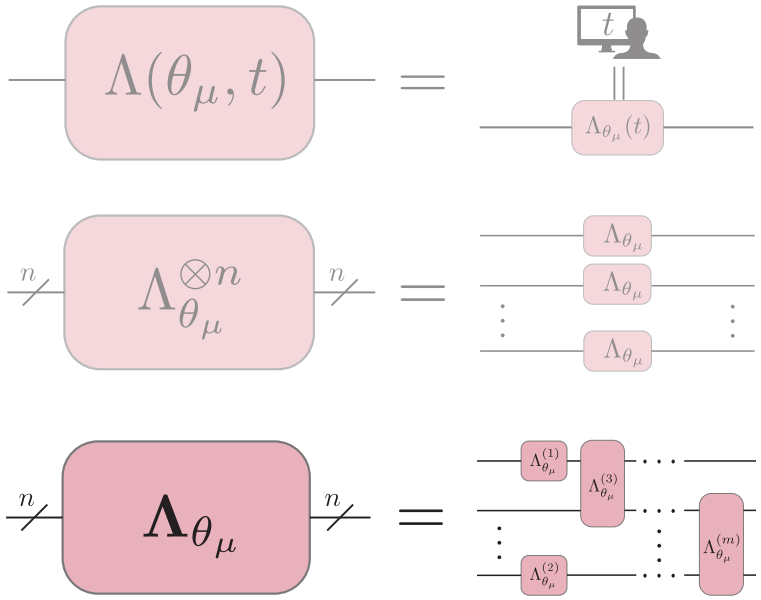
Privacy - Linear Functions

$$f(\vec{\theta}) = \vec{a} \cdot \vec{\theta}$$

(a) $\vec{a} \in \mathbb{R}^k$ - requires controllable encoding dynamics

(b) $\vec{a} \in \mathbb{Z}^k$ - related with the number of qubits available locally ($\vec{a} \in \mathbb{Q}^k$ can be reduced to this case)

(c) $\vec{a} \in \mathcal{O}_{-}^{2}$ - requires knowledge of the local hamiltonians' eigenvalues



$$t \to \vec{t} = \vec{a}, \quad \vec{n} = \vec{1}$$

$$gcd(\vec{a}) = gcd(a_1, a_2, \ldots, a_k) = 1!$$

$$\vec{a} \in \Lambda_1 \times \ldots \times \Lambda_k, \; \Lambda_\mu = \{\lambda_j^\mu\}_{j \in \mu}$$

$\simeq$

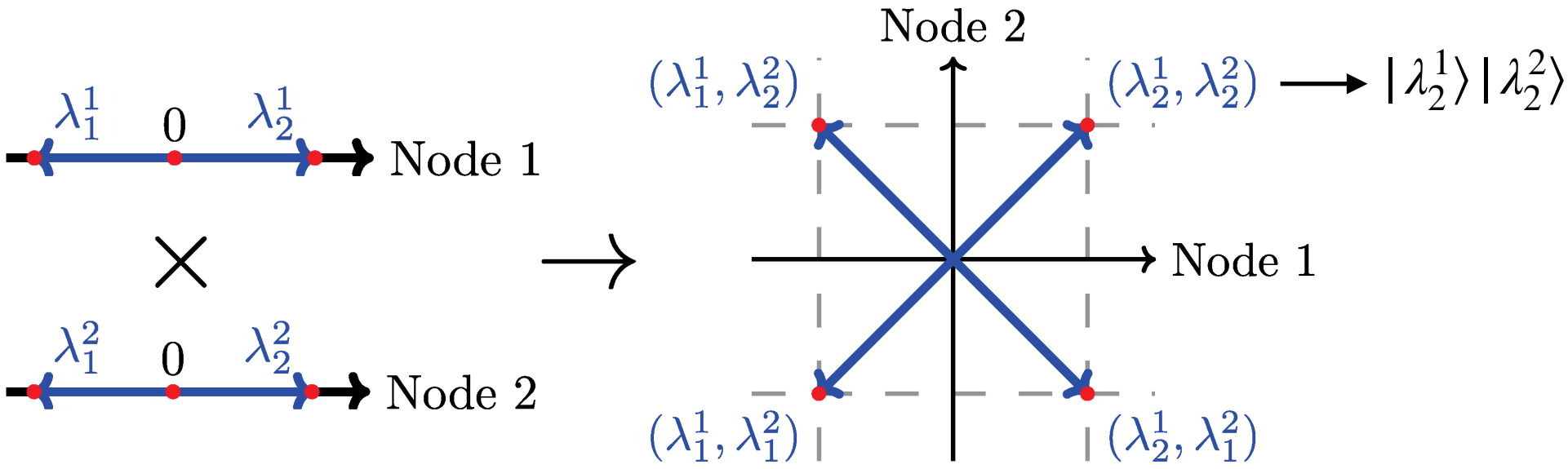
Privacy - Private Orthotope

For general local Hamiltonian dynamics, one can find the following structure:

$$\boldsymbol{H}_\mu |\lambda_j^\mu\rangle = \lambda_j^\mu |\lambda_j^\mu\rangle, \quad \mathscr{B}^\mu = \{|\lambda_j^\mu\rangle\}_{i\in\mu}, \quad \mathscr{O}_\mu = \{\lambda_j^\mu\}_{j\in\mu},$$

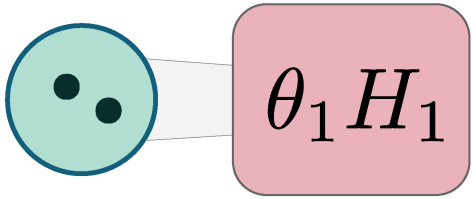
Using this, we can define an orthotope by doing the cartesian product of the eigenvalues in $\mathscr{O}_\mu$.

E.g.

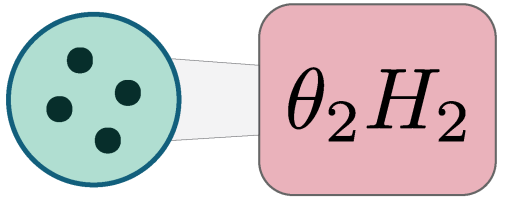


Sekatski, P., Wölk, S. & Dür, W. Optimal distributed sensing in noisy environments. Physical Review Research **2**, 1–8 (2019).

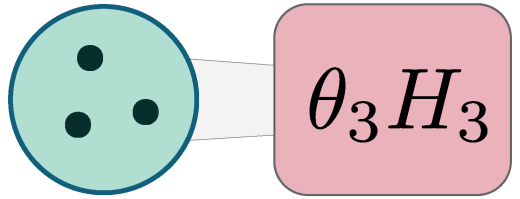
Step 1: *Identify the local eigenstates and eigenvalues*



$$\mathcal{B}^1 = \{|\lambda_1^1\rangle, \ldots, |\lambda_4^1\rangle\}$$
$$\mathcal{O}^1 = \{\lambda_1^1, \ldots, \lambda_4^1\}$$



$$\mathcal{B}^2 = \{|\lambda_1^2\rangle, \ldots, |\lambda_{16}^2\rangle\}$$
$$\mathcal{O}^2 = \{\lambda_1^2, \ldots, \lambda_{16}^2\}$$

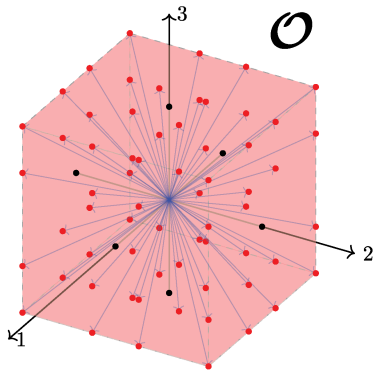


$$\mathcal{B}^3 = \{|\lambda_1^3\rangle, \ldots, |\lambda_8^3\rangle\}$$
$$\mathcal{O}^3 = \{\lambda_1^3, \ldots, \lambda_8^3\}$$

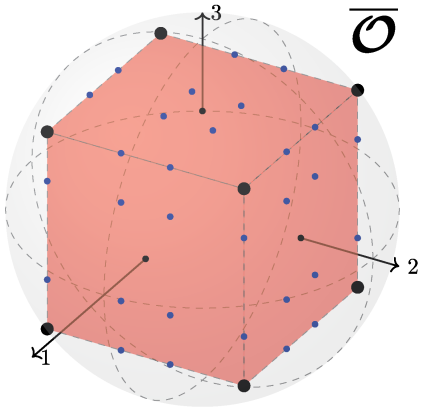
Step 2: *Construct the distributed orthotope*

$\mathcal{O}^1 = \{\lambda_1^1, \ldots, \lambda_4^1\}$ $\times$ $\mathcal{O}^2 = \{\lambda_1^2, \ldots, \lambda_{16}^2\}$ $\times$ $\mathcal{O}^3 = \{\lambda_1^3, \ldots, \lambda_8^3\}$ $=$

$=$



$\mathcal{O}$



$\overline{\mathcal{O}}$

Step 3: *Construct the private orthotope and states*

$$\mathcal{O}_{-}^{2} = \{\vec{v} - \vec{w} : \forall \vec{v}, \vec{w} \in \mathcal{O}\}$$

$$\vec{v} = (\lambda_{j_1}^1, \lambda_{j_2}^2, \lambda_{j_3}^3) \leftrightarrow |\lambda_{j_1}^1\rangle |\lambda_{j_2}^2\rangle |\lambda_{j_3}^3\rangle$$
$$\vec{w} = (\lambda_{k_1}^1, \lambda_{k_2}^2, \lambda_{k_3}^3) \leftrightarrow |\lambda_{k_1}^1\rangle |\lambda_{k_2}^2\rangle |\lambda_{k_3}^3\rangle$$

$$\longmapsto |\psi\rangle = \alpha |\lambda_{j_1}^1\rangle |\lambda_{j_2}^2\rangle |\lambda_{j_3}^3\rangle + \beta |\lambda_{k_1}^1\rangle |\lambda_{k_2}^2\rangle |\lambda_{k_3}^3\rangle$$

Is private for $\vec{v} - \vec{w}$!

Thms. 3.6: ∀ vectors in $\mathcal{O}_{-}^{2}$ there exists at least one family of private states

More than this, only for vectors in $\mathcal{O}_{-}^{2}$ there exists private states

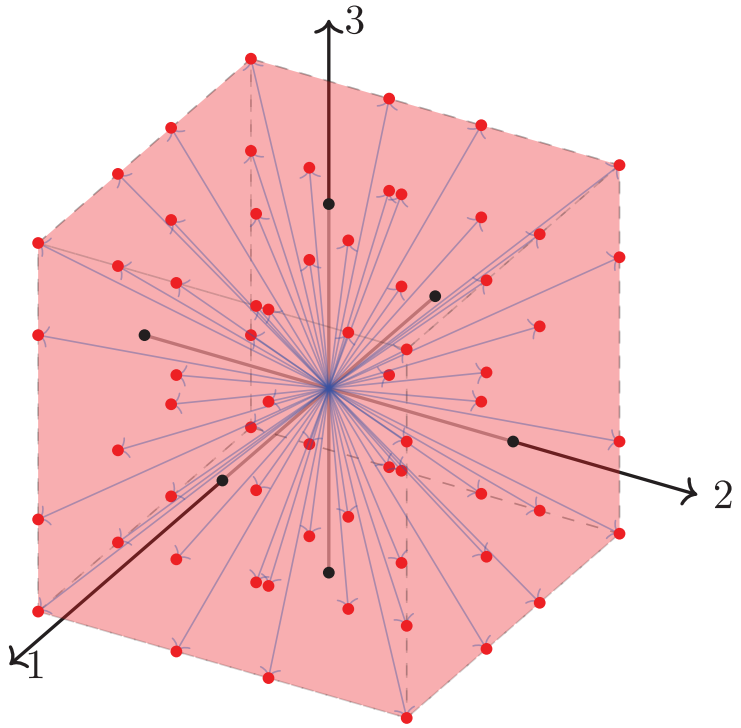
Bugalho, L., Hassani, M., Omar, Y. & Markham, D. Private and Robust States for Distributed Quantum Sensing. Quantum **9**, 1596 (2025)

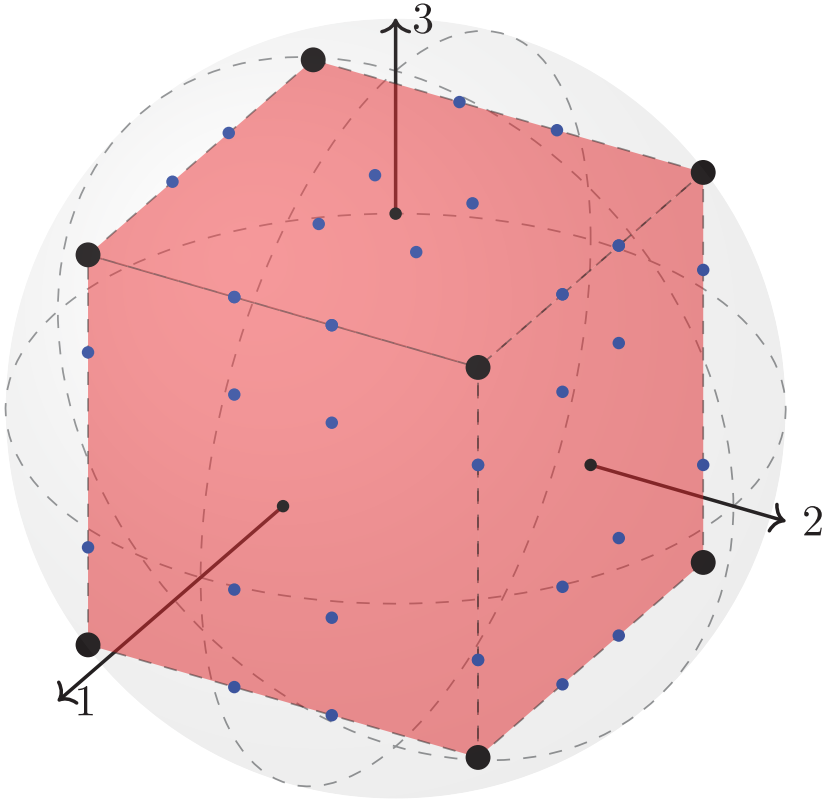
Privacy — Results

Target	Hamiltonian	Resources	Private Family	Theorem
$\vec{a} \in \mathbb{R}^k$	Controlable (Fig. 2 d))	$\vec{n} = \vec{1}$	GHZ State	Thm. 3.4
$\vec{a} \in \mathbb{N}^k$	Separable (Fig. 2 a))	Zone (I)	None	Thms. 3.1, 3.3
		Zone (II)	GHZ State	Thms. 3.2, 3.4
		Zone (III)	Ancilla-Private States	Thm. 3.5
		Zone (IV)	Private Logical States	Thm. 3.6
$\vec{a} \in \mathcal{O}_-^2$	General (Fig. 2 b))	Depends on H	$\exists$ Private State	Thm. 3.7

Table 1: Main results regarding the existence of private states under the assumptions on the encoding dynamics, the target functions and the resources utilized.

Privacy — Bonus!





If we take separable dynamics, then the only state at the vertice of the private orthotope is the GHZ state (up to LU)! This means, the vector with largest norm and equal to $\mathrm{Tr}(\mathcal{Q})$.

Privacy — Robustness

- **QFI for mixed states under separable dynamics**
  - Here we fixed the dynamics to $\hat{Z}$ (without loss of generality)
  - Working with a private state (up to LU)

Noise Models	Results
Dephasing	GHZ state **maintains** privacy, decoheres **exponentially**
Bit-Flip	GHZ state **looses** privacy, decoheres **exponentially**
Depolarizing	GHZ state **maintains** privacy, decoheres **exponentially**
Amplitude-Damping	GHZ state **maintains** privacy, decoheres **exponentially**
Particle-loss	∃ Private states that **maintain** privacy

$$s_0^4 = (01\ 0001\ 000), s_1^4 = (11\ 1101\ 111)$$

$\downarrow\ \sigma \in S_{\mathcal{N}}$ $\qquad$ $\downarrow\ \sigma \in S_{\mathcal{N}}$

$$s_1 = (01\ 0001\ 000) \qquad \bar{s}_1 = (10\ 1110\ 111)$$
$$s_2 = (01\ 0010\ 000) \qquad \bar{s}_2 = (10\ 1101\ 111)$$
$$s_3 = (01\ 0100\ 000) \qquad \bar{s}_3 = (10\ 1011\ 111)$$
$$s_4 = (01\ 1000\ 000) \qquad \bar{s}_4 = (10\ 0111\ 111)$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \left(\sum_i |s_i\rangle + |\bar{s}_i\rangle \right)$$

$\langle 0|(\cdot)|0\rangle$ $\qquad$ $\langle 1|(\cdot)|1\rangle$

Trace out whichever qubit i in node 2

$$\rho = \mathrm{Tr}_i[\,|\psi\rangle\langle\psi|\,] = \alpha\,|\psi_0\rangle\langle\psi_0| + (1-\alpha)\,|\psi_1\rangle\langle\psi_1|$$

$|\psi_0\rangle, |\psi_1\rangle$ **are private!**
(and orthogonal)

Quantum
the open journal for quantum science

PAPERS PERSPECTIVES

Private and Robust States for Distributed Quantum Sensing

Luís Bugalho[1,2,3,4], Majid Hassani[4], Yasser Omar[1,2,3], and Damian Markham[4]

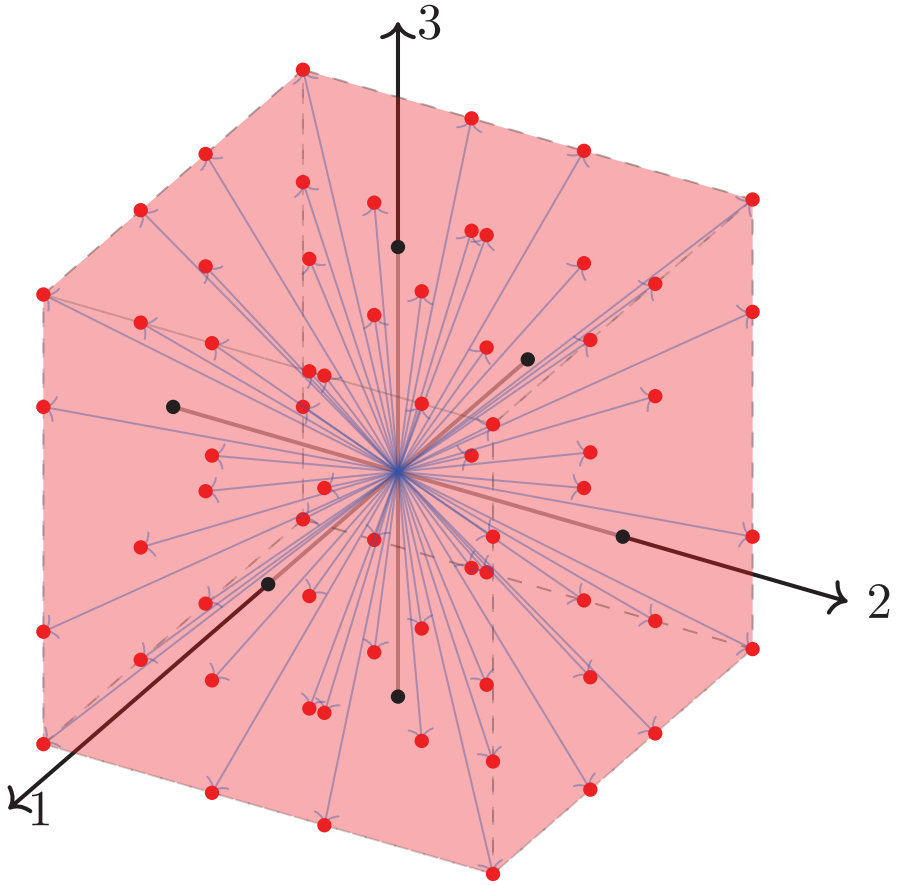
[1]Instituto Superior Técnico, Universidade de Lisboa, Portugal
[2]Physics of Information and Quantum Technologies Group, Centro de Física e Engenharia de Materiais Avançados (CeFEMA), Portugal
[3]PQI – Portuguese Quantum Institute, Portugal
[4]Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France

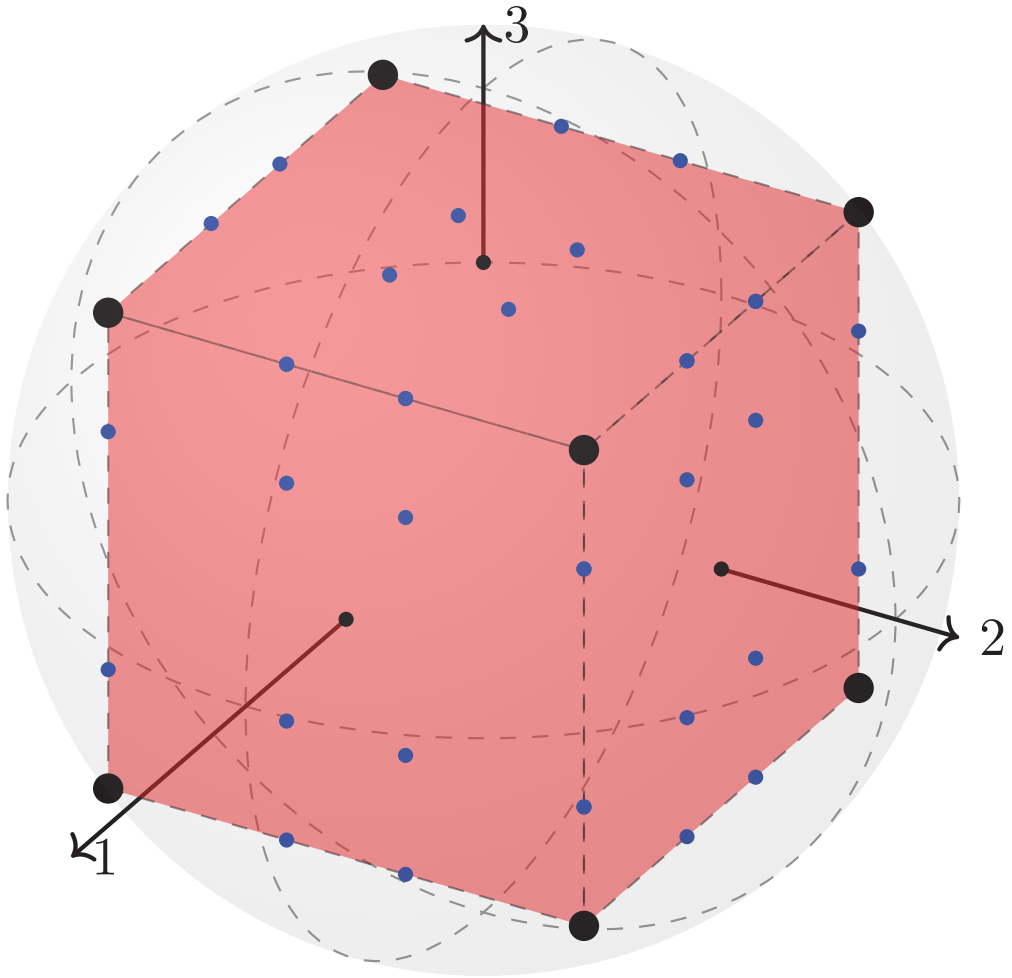
Published: 2025-01-15, volume 9, page 1596
Editor: Christos Gagatsos
Eprint: arXiv:2407.21701v2
Doi: https://doi.org/10.22331/q-2025-01-15-1596
Citation: Quantum 9, 1596 (2025).

Take Home Messages

- **Privacy**
  - Minimum amount to create the first private state ~ **GHZ state**
  - Build the rest by adding ancillas and doing local operations ~ **countable number of families** of private states (each containing a continuous set of states)
  - Build logical qubits in the private subspaces ~ one can use robustness results from non-distributed sensing
- **Robustness**
  - States that are robust against particle-loss, while preserving privacy
  - Relation between noise types and preserving the privacy
- **Connection between information and the internal structure of an Hamiltonian**

Privacy — Private Orthotope





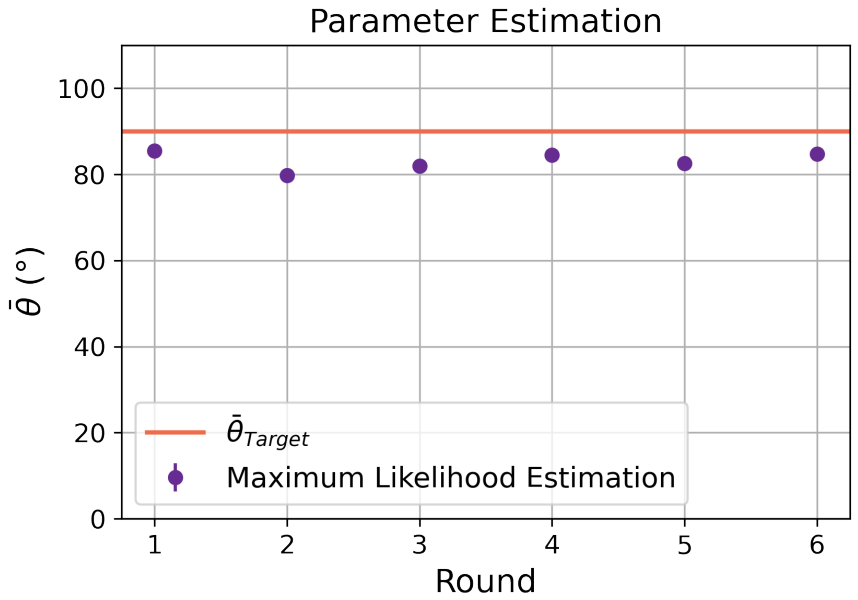
Current Work - *Next Steps*

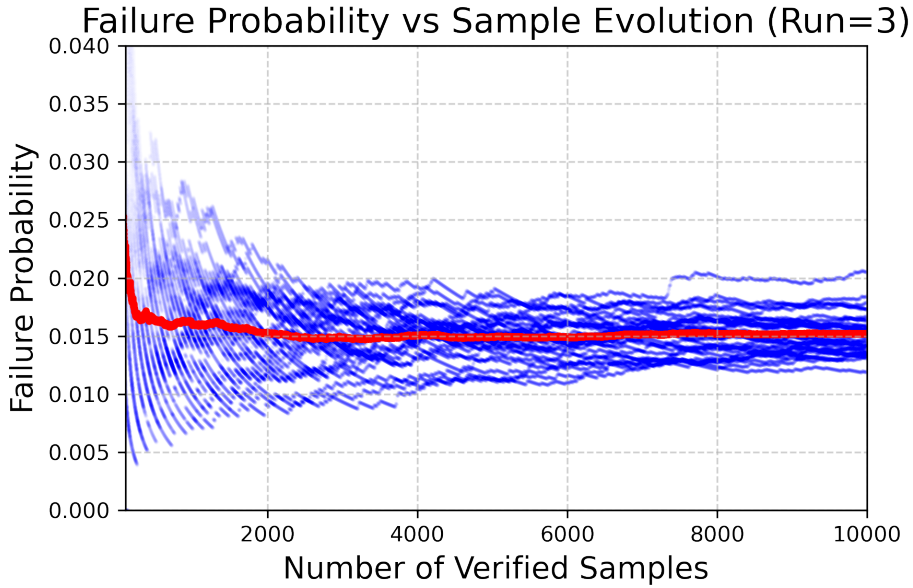
- **Experimental work on implementing a secure and private sensor network**
  - Undergoing work with experimental team
  - Martins, L. dos S., Laurent-Puig, N., Lefebvre, P., Neves, S. & Diamanti, E. *Realizing a Compact, High-Fidelity, Telecom-Wavelength Source of Multipartite Entangled Photons*. arXiv.2407.00802 (2024).
- **Finding out what problems fit in this - linear functions with private estimation**
  - Creating a framework for a general class of problems that are efficiently and privately dealt with these states
- **Network Deployment with Optimization over quantum strategies**
  - Creating a framework to deal with deploying over quantum networks
- **Application and real-life protocols for quantum sensors - atom interferometry**

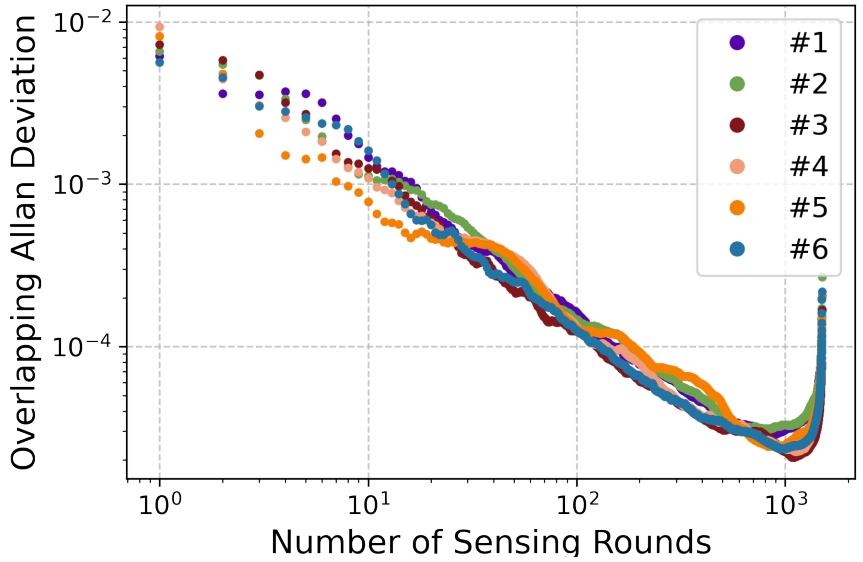
- (Generalizing results of Privacy?)
- (Exploring connections with other areas? Multi-party quantum computation?)

Experimental Work

- **Experimental work on implementing a secure and private sensor network -** using a certification protocol to ensure the distributed states is private (a GHZ state)







Obrigado

Acknowledgements:

The authors acknowledge the support from the EU Quantum Flagship project QIA (101102140) and France 2030 under the French National Research Agency projects HQI ANR-22-PNCQ- 0002 and the PEPR integrated project EPiQ ANR-22-PETQ-0007. L.B. and Y.O. thank the support from Fundação para a Ciência e a Tecnologia (FCT, Portugal), namely through project UIDB/04540/2020. L.B. acknowledges the support of FCT through scholarship BD/05268/2021.

Appendix

Privacy — QFI Matrix

$$\mathcal{Q}_{\mu\nu}(\rho_{\vec{\theta}}) = 4 \sum_{\vec{m}} |\alpha_{\vec{m}}|^2 \lambda^{\mu}_{m_\mu} \lambda^{\nu}_{m_\nu} - \sum_{\vec{m}} |\alpha_{\vec{m}}|^2 \lambda^{\mu}_{m_\mu} \sum_{\vec{q}} |\alpha_{\vec{q}}|^2 \lambda^{\nu}_{q_\nu}$$

$$\mathbf{\mathcal{Q}}(\rho_{\vec{\theta}}) = C \mathfrak{Q} C^T$$

$$C = \begin{pmatrix} \vec{a}_1 - \\ \vec{a}_2 - \\ \vdots \\ \vec{a}_{2^n} - \end{pmatrix}$$

Contains information about the hamiltonian orthotope

$$\overrightarrow{\alpha} = (|\alpha_{\vec{m}}|^2, \dots)$$

$$\mathfrak{Q} = \mathsf{diag}(\overrightarrow{\alpha}) - \overrightarrow{\alpha}\,\overrightarrow{\alpha}^T$$

Contains information about the superposition of the eigenstates

Privacy — Results

(II) One Copy Privacy Zone

- Only one stabilizer state and a corresponding family of pure states, up to LU
- $\mathcal{F}_{\text{GHZ}} = \{\alpha|0\rangle^{\otimes n} + \beta|1\rangle^{\otimes n}, |\alpha|^2 + |\beta|^2 = 1\}$
- Example:

$$f(\vec{\theta}) = 1\theta_1 + 3\theta_2 + 4\theta_3 \implies \vec{a} = (1,3,4) \implies \vec{n} = (1,3,4)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|\underbrace{0}_{n_1}\ \underbrace{000}_{n_2}\ \underbrace{0000}_{n_3}\rangle + |\underbrace{1}_{n_1}\ \underbrace{111}_{n_2}\ \underbrace{1111}_{n_3}\rangle\right]$$

Privacy - Results

(III) One Copy plus Ancilla Privacy Zone

- All families of arbitrary pure states which are private
- Building “symmetric” states — states that are superpositions of states with equal Hamming weights:
- Example:

$$f(\vec{\theta}) = 1\theta_1 + 3\theta_2 + 4\theta_3 \implies \vec{a} = (1,3,4) \qquad \vec{n} = (2,4,4) = \vec{a} + (1,1,0)$$

Ancilla on first node Ancilla on second node

$$|\psi\rangle = \frac{1}{\sqrt{N}} \left[\sum_{\sigma \in S_{\mathcal{N}}} |\underbrace{00}_{n_1} \underbrace{0001}_{n_2} \underbrace{0000}_{n_3}\rangle + \sum_{\sigma \in S_{\mathcal{N}}} |\underbrace{10}_{n_1} \underbrace{1111}_{n_2} \underbrace{1111}_{n_3}\rangle \right]$$

Private!

$$h(s) = (0,1,0) \qquad h(s') = (1,4,4) \longrightarrow h(s') - h(s) = \vec{a}$$

Privacy - Results

(IV) Multiple Copies Privacy Zone

- Logical states, built from the families of private states in regions (II),(III)
- All states built from these logical states are private (no completeness proof)
- Example:

$$f(\vec{\theta}) = 1\theta_1 + 3\theta_2 + 4\theta_3 \implies \vec{a} = (1,3,4) \qquad \vec{n} = (4,8,8) = 2[\vec{a} + (1,1,0)]$$

$$|0_L\rangle = \frac{1}{\sqrt{N}} \sum_{\sigma \in S_{\mathcal{N}}} |\underbrace{00}_{n_1}\ \underbrace{0001}_{n_2}\ \underbrace{0000}_{n_3}\rangle$$

$$|1_L\rangle = \frac{1}{\sqrt{N}} \sum_{\sigma \in S_{\mathcal{N}}} |\underbrace{10}_{n_1}\ \underbrace{1111}_{n_2}\ \underbrace{1111}_{n_3}\rangle$$

$$\longrightarrow \quad |\psi\rangle = \frac{1}{\sqrt{2}} \left[|0_L 0_L\rangle + |1_L 1_L\rangle \right]$$

Privacy — Robustness

- **Expressions** for dephasing:

  - $\mathscr{D}_i(\rho, p) = (1-p)\rho + pZ_i\rho Z_i, \qquad Z\,|\,\mathscr{G}_0^{\pm}\rangle = |\,\mathscr{G}_0^{\mp}\rangle$

  - $\mathscr{Q}_{\mu\nu}(\rho_\theta) = 4\dfrac{(\lambda_+ - \lambda_-)^2}{\lambda_+ + \lambda_-}\langle\mathscr{G}_0^+|\,\boldsymbol{Z}_\mu\,|\,\mathscr{G}_0^-\rangle\langle\mathscr{G}_0^-|\,\boldsymbol{Z}_\nu\,|\,\mathscr{G}_0^+\rangle$

  - $= 4(\lambda_+ - \lambda_-)^2 a_\mu a_\nu$

$$\lambda_+ - \lambda_- \sim (1-2p)^n$$

Maintains privacy
QFI decreases exponentially

Privacy — Robustness

- **Expressions** for bit-flip:
  - $\mathscr{D}_i(\rho, p) = (1-p)\rho + p\boldsymbol{X}_i\rho\boldsymbol{X}_i, \qquad \boldsymbol{X}_i\,|\,\mathscr{G}_0^{\pm}\rangle = |\,\mathscr{G}_i^{\pm}\rangle$
  - $\rho = \lambda_0\,|\,\mathscr{G}_0^{+}\rangle\langle\mathscr{G}_0^{+}\,| + \sum_{i=1}^{2^{n-1}-1} \lambda_i\,|\,\mathscr{G}_i^{+}\rangle\langle\mathscr{G}_i^{+}\,|$
  - $\mathscr{Q}_{\mu\nu}(\rho_\theta) = \lambda_0 a_\mu a_\nu +$ non-private component

$$\lambda_0 \sim (1-p)^n + p^n$$

Breaks privacy
QFI decreases exponentially

Privacy — Robustness

- **Expressions** for depolarizing:

$$\mathscr{D}_i^p(\rho) = p\rho + \frac{1-p}{3}\left(X_i\rho X_i^\dagger + Y_i\rho Y_i^\dagger + Z_i\rho Z_i^\dagger\right)$$

$$\rho = \lambda_0^+ |\mathscr{G}_0^+\rangle\langle\mathscr{G}_0^+| + \lambda_0^- |\mathscr{G}_0^-\rangle\langle\mathscr{G}_0^-| + \sum_{i=1}^{2^{n-1}-1} \lambda_i |i\rangle\langle i|$$

$$\mathscr{Q}_{\mu\nu}(\rho_\theta) = 4\frac{(\lambda_0^+ - \lambda_0^-)^2}{\lambda_0^+ + \lambda_0^-} a_\mu a_\nu$$

$$\lambda_0 \sim (1-\alpha\epsilon)^n$$

Maintains privacy
QFI decreases exponentially

Privacy — Robustness

- **Expressions** for particle-loss:
  - $|0_L\rangle, |1_L\rangle$ belong to private states
    - One-copy privacy zone -> zero information after particle loss
    - One-copy-plus-ancilla -> still some information after particle loss
  - Depends on the state chosen for the logical kets
  - Best option -> local permutations invariant logical states

Maintains privacy