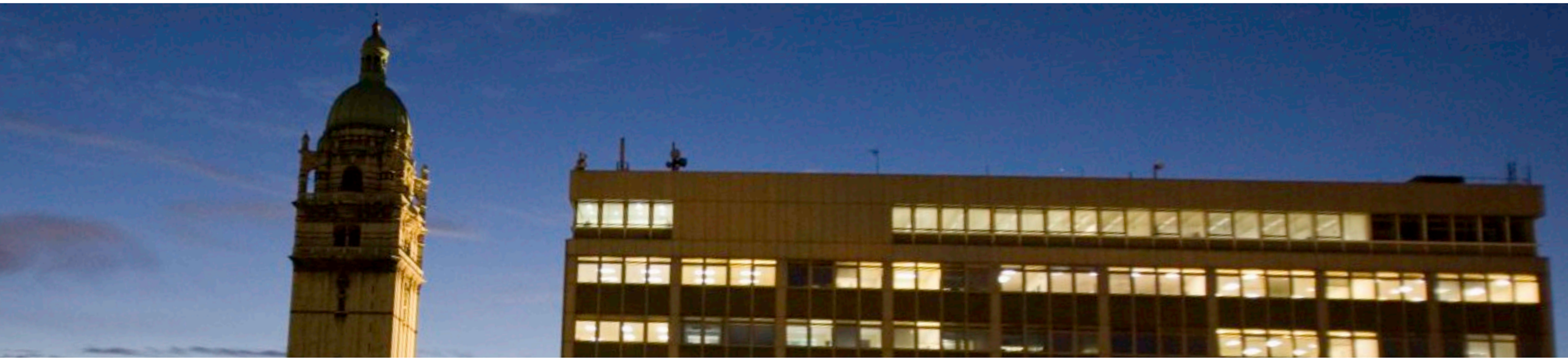
Post-quantum cryptography in the pre-quantum era



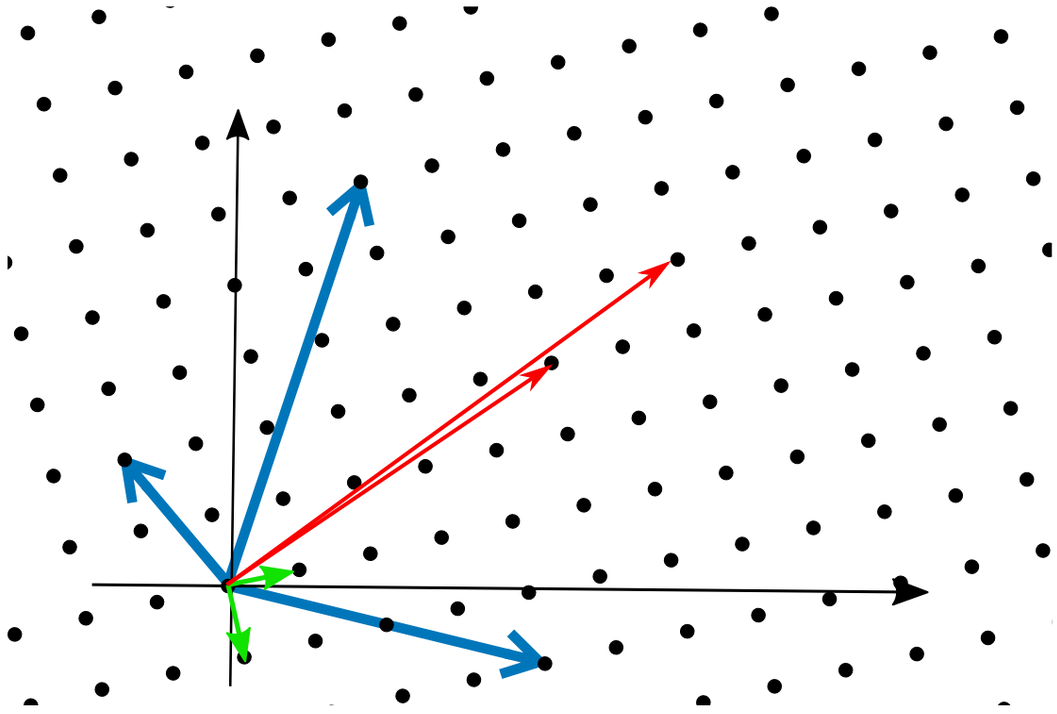
Florian Mintert
Imperial College

Cryptography

prime factor decomposition

$$\xrightarrow{\text{easy}}$$
$$3 \times 5 = 15$$
$$\xleftarrow{\text{hard}}$$

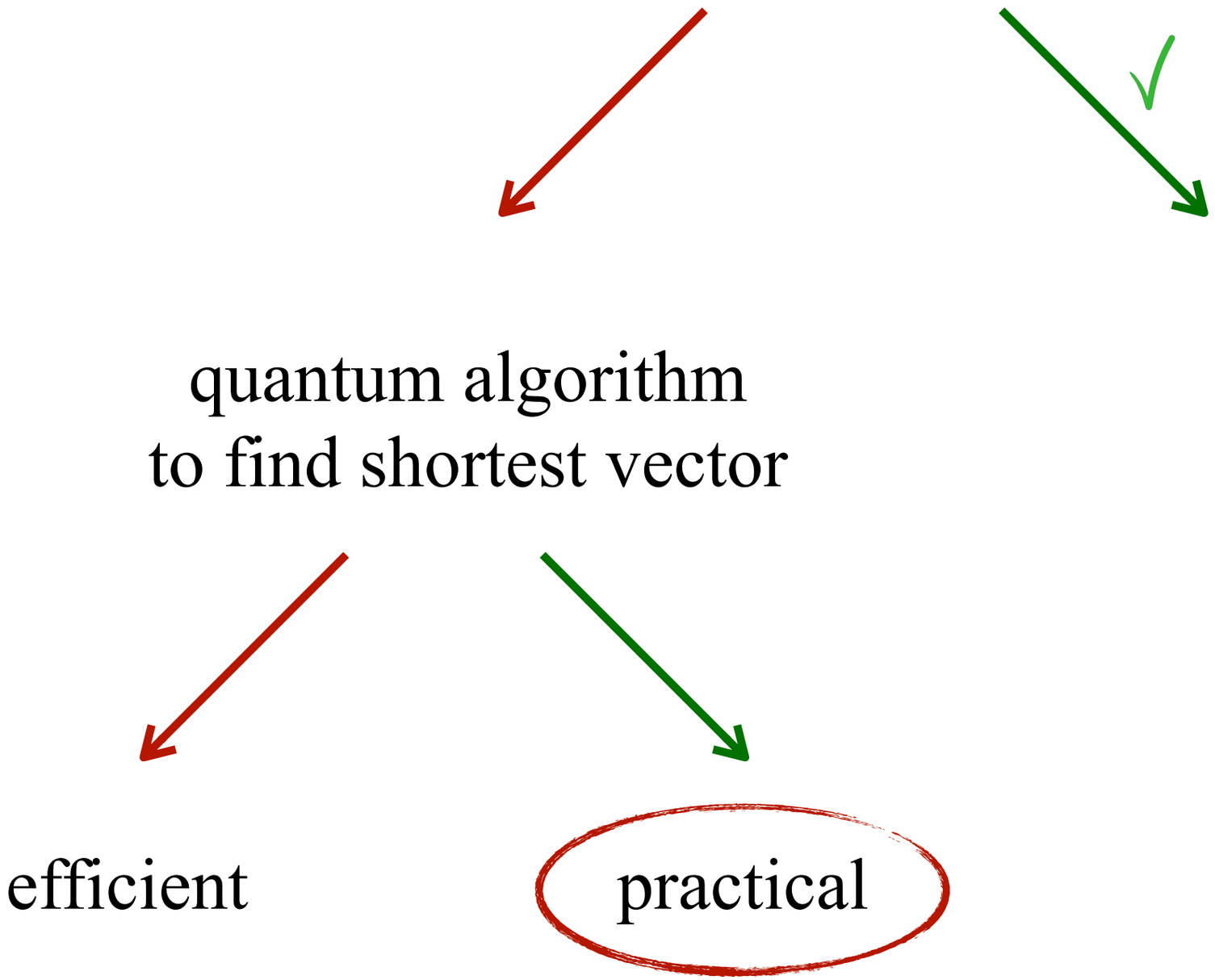
lattices



shortest vector problem SVP

Is it really save?

Is lattice-based cryptography save against quantum attacks?



Quantum mechanics

$$i|\dot{\Psi}\rangle = H|\Psi\rangle \qquad\qquad |\Psi(t)\rangle = U(t,t_0)|\Psi(t_0)\rangle$$

$$|\Psi\rangle = \sum_j \Psi_j |\phi_j\rangle$$

measurement in basis $\{|\phi_j\rangle\}$

probability to obtain $|\phi_j\rangle$

$$p_j = \left|\langle\phi_j|\Psi\rangle\right|^2 = |\Psi_j|^2$$

measurement in basis $\{|\chi_j\rangle\}$

probability to obtain $|\chi_j\rangle$

$$q_j = |\langle\chi_j|\Psi\rangle|^2$$

Quantum mechanics

$$|\Psi\rangle = \sum_{jk\ldots} \Psi_{jk\ldots} |\Phi_j\rangle \otimes |\Phi_k\rangle \otimes \ldots$$

exponential scaling

independent measurements

Quantum mechanics

$$H|\Psi_j\rangle = \lambda_j|\Psi_j\rangle$$

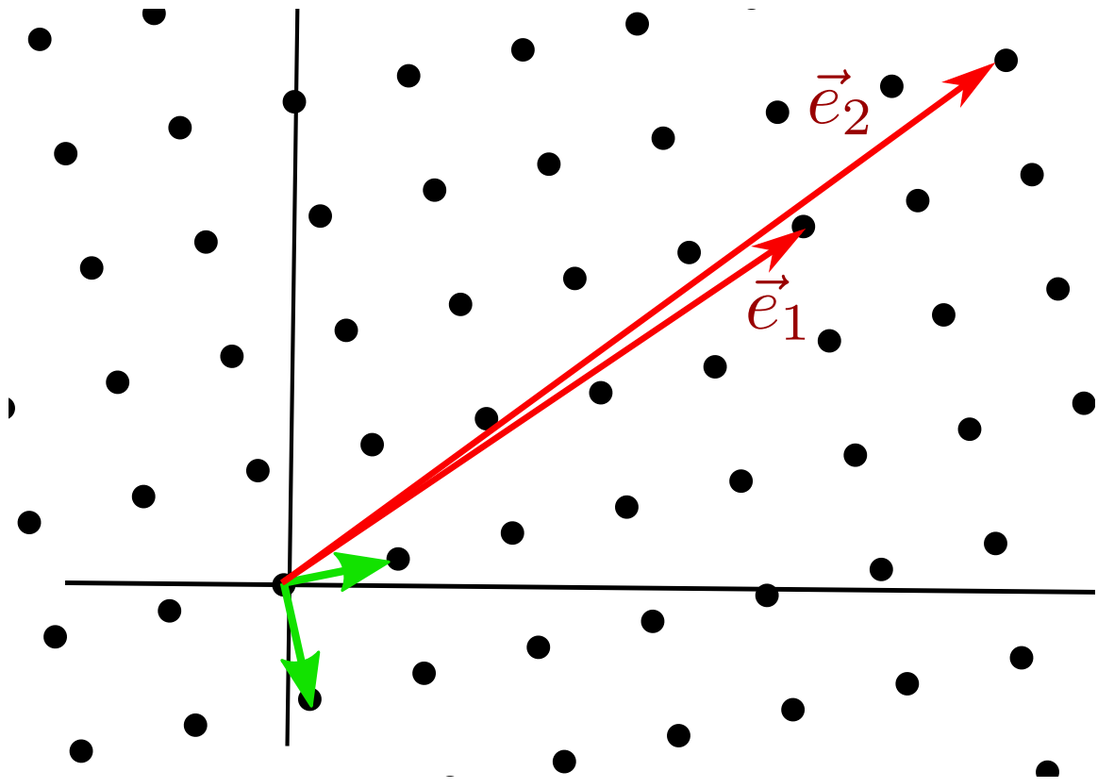
eigenstates

problem Hamiltonian :

an eigenstate contains the full information
on the solution of the problem

problem Hamiltonian

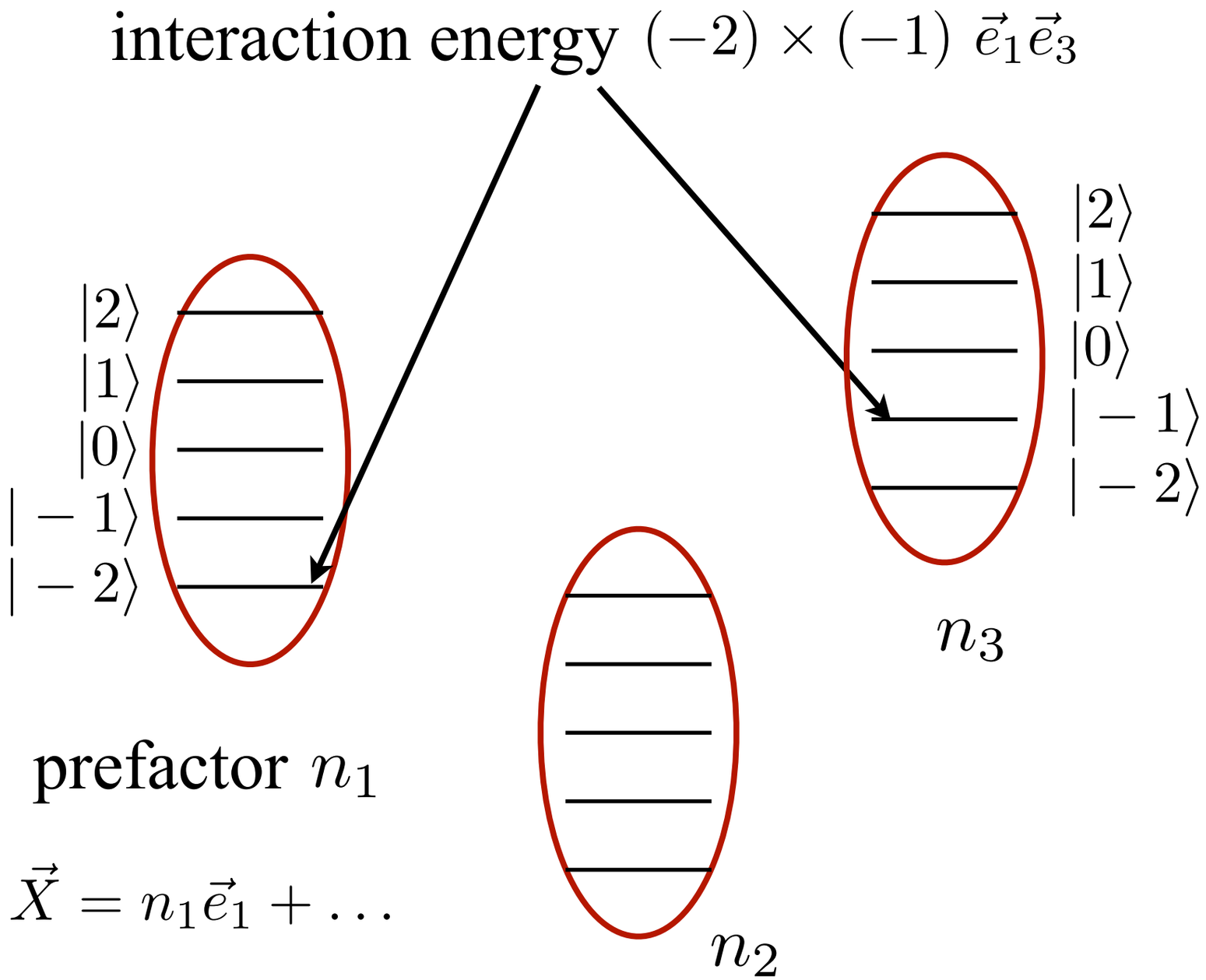
lattice basis vectors $\vec{e}_i$



general lattice vector $\vec{X} = \sum_i n_i \vec{e}_i$

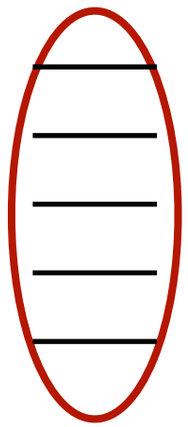
length of lattice vector $|\vec{X}|^2 = \sum_{ij} n_i n_j \ \vec{e}_i \vec{e}_j$

problem Hamiltonian



problem Hamiltonian

linear dispersion $$Q = \sum_j j|j\rangle\langle j|$$



properties of the lattice

problem Hamiltonian $$H_p = \sum_{ij} Q_i Q_j \boxed{\vec{e}_i \vec{e}_j}$$

with eigen-energies $$\omega_{\vec{n}} = \sum_{ij} n_i n_j \ \vec{e}_i \vec{e}_j$$

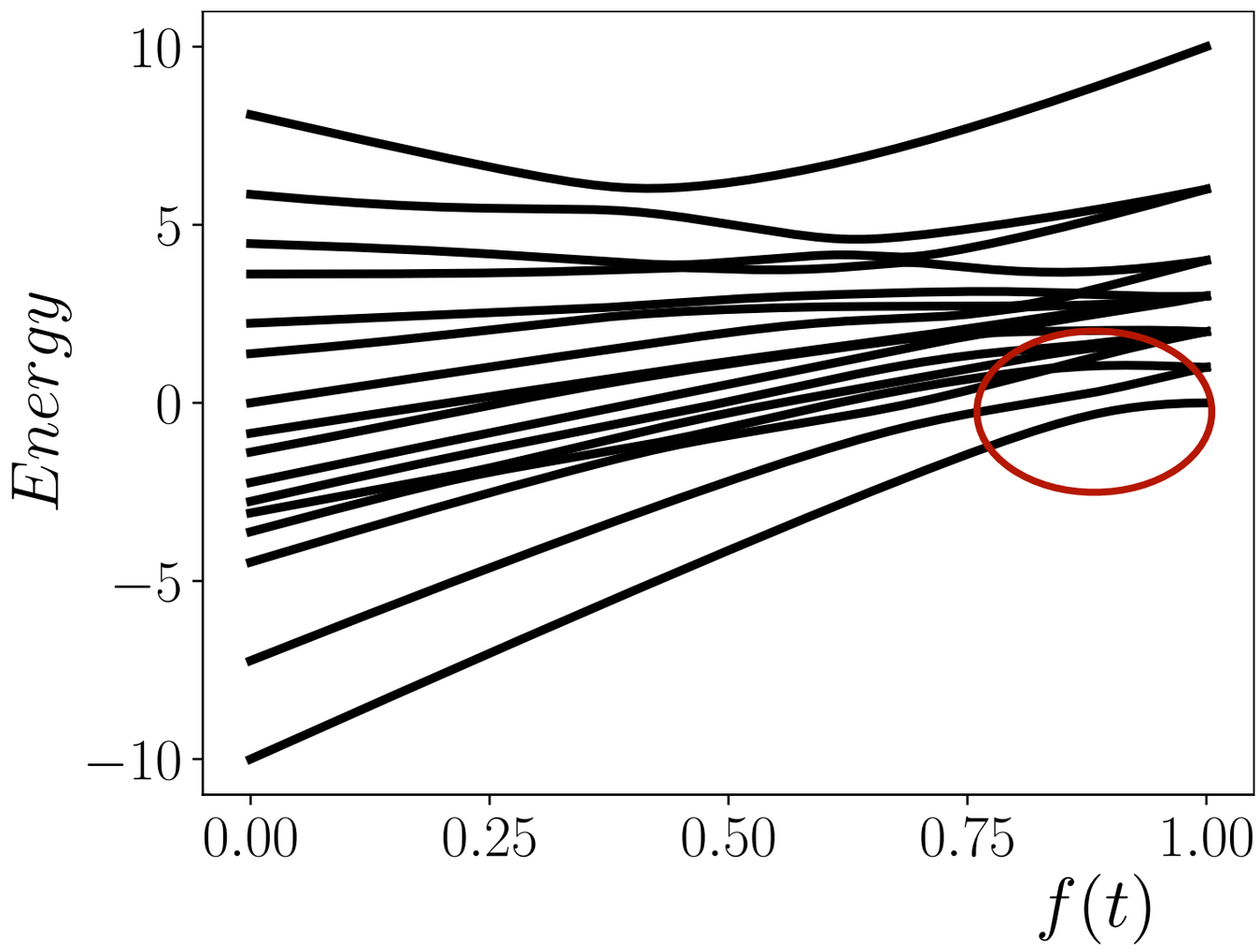
find first excited state, or some low-energy state

Adiabatic Quantum Computation

complicated problem Hamiltonian H_p

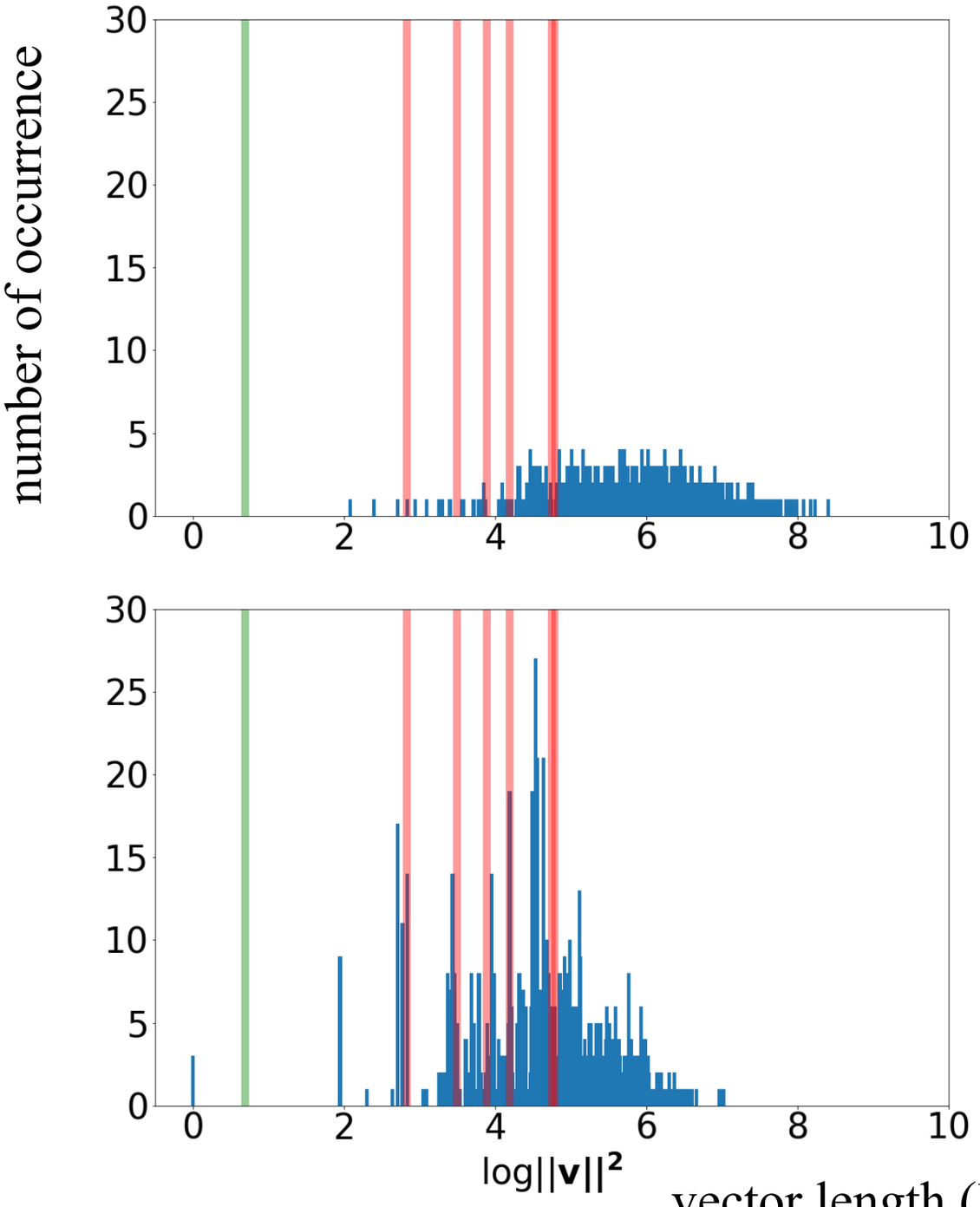
simple driver Hamiltonian H_d

adiabatic dynamics $H(t) = (1 - f(t))H_d + f(t)H_p$



Adiabatic Quantum Computation

occurrences in 900 runs



David Joseph, Adam Callison, Cong Ling & FM, PRA **103**, 032433 (2021)

AQC and QAOA

adiabatic dynamics $\quad H(t) = (1 - f(t))H_d + f(t)H_p$

discretise $\quad f(t)$

$$|\Psi_1\rangle = \exp\left(-i\left((1 - f_1)H_d + f_1 H_p\right)T\right)|\Psi_0\rangle$$

$$|\Psi_2\rangle = \exp\left(-i\left((1 - f_2)H_d + f_2 H_p\right)T\right)|\Psi_1\rangle$$

$$|\Psi_3\rangle = \ldots$$

ignore non-commutativity (short times)

$$\exp\left(-i\left((1 - f_j)H_d + f_j H_p\right)T\right) \simeq \exp\left(-i(1 - f_j)H_d T\right)\ \exp\left(-i f_j H_p T\right)$$

AQC and QAOA

$$\ldots \exp\left(-i(1-f_2)H_d T\right)\ \exp\left(-if_2 H_p T\right) \exp\left(-i(1-f_1)H_d T\right)\ \exp\left(-if_1 H_p T\right)$$

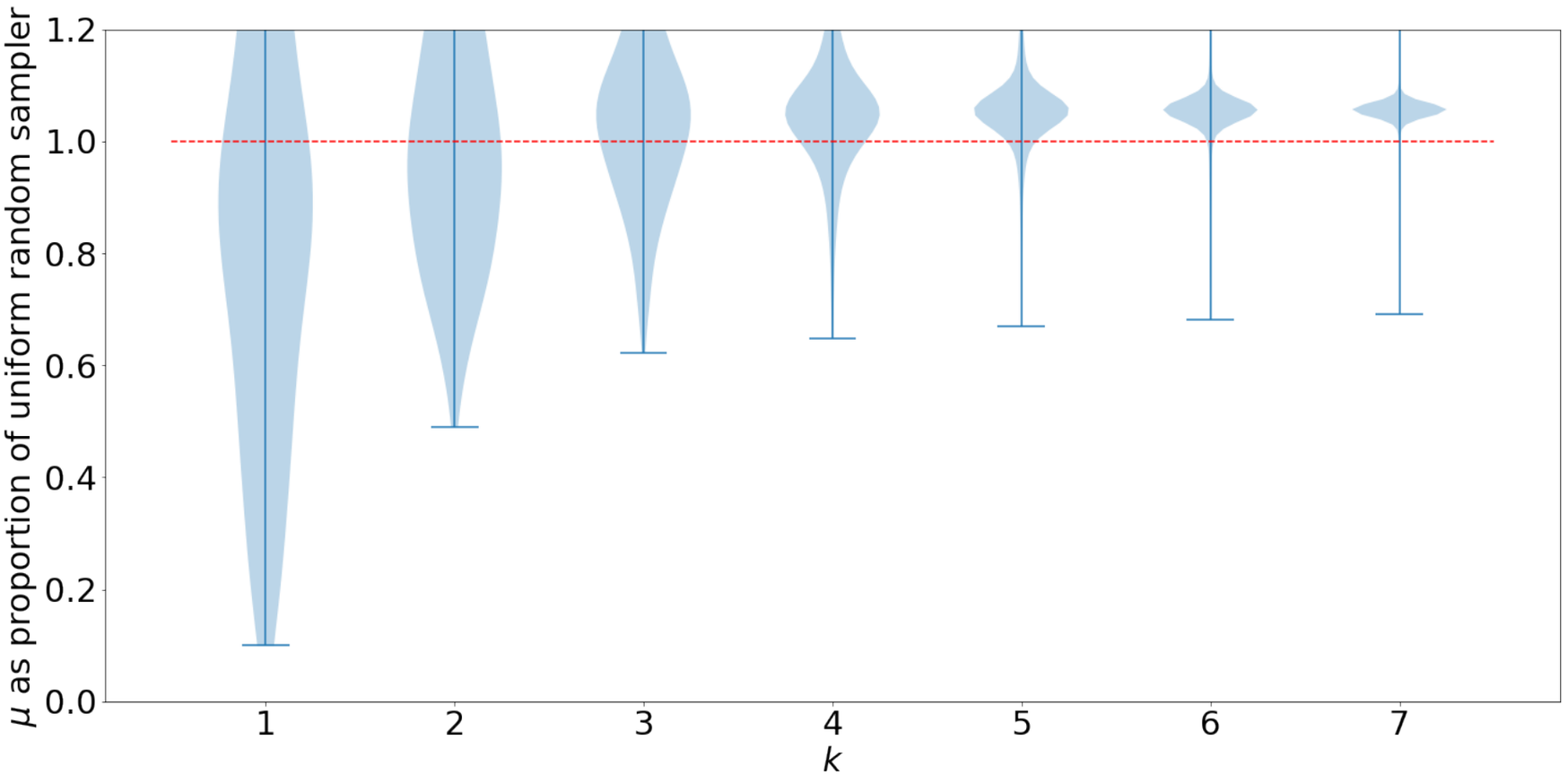
replace by $\quad \exp\left(-i\beta H_d\right) \quad \exp\left(-i\gamma H_p\right)$

potentially really bad approximation

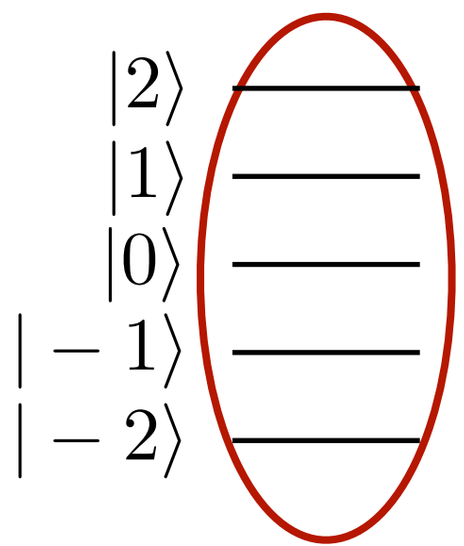
very few gates

sampling

$$|\Psi_\gamma\rangle = \exp\left(-i\frac{\pi}{4}H_d T\right)\ \exp\left(-i\gamma H_p T\right)|\Psi_0\rangle$$



size of each subsystem (log-scale)



energy expectation

expectation value of problem Hamiltonian $\mu_\gamma = \langle \Psi_\gamma | H_p | \Psi_\gamma \rangle$

$$\langle \Psi_0 | \underbrace{\exp\left(i\gamma H_p\right) \exp\left(i\frac{\pi}{4} H_d\right) H_p \exp\left(-i\frac{\pi}{4} H_d\right) \exp\left(-i\gamma H_p\right)}_{\text{feasible}} | \Psi_0 \rangle$$

difficult to construct

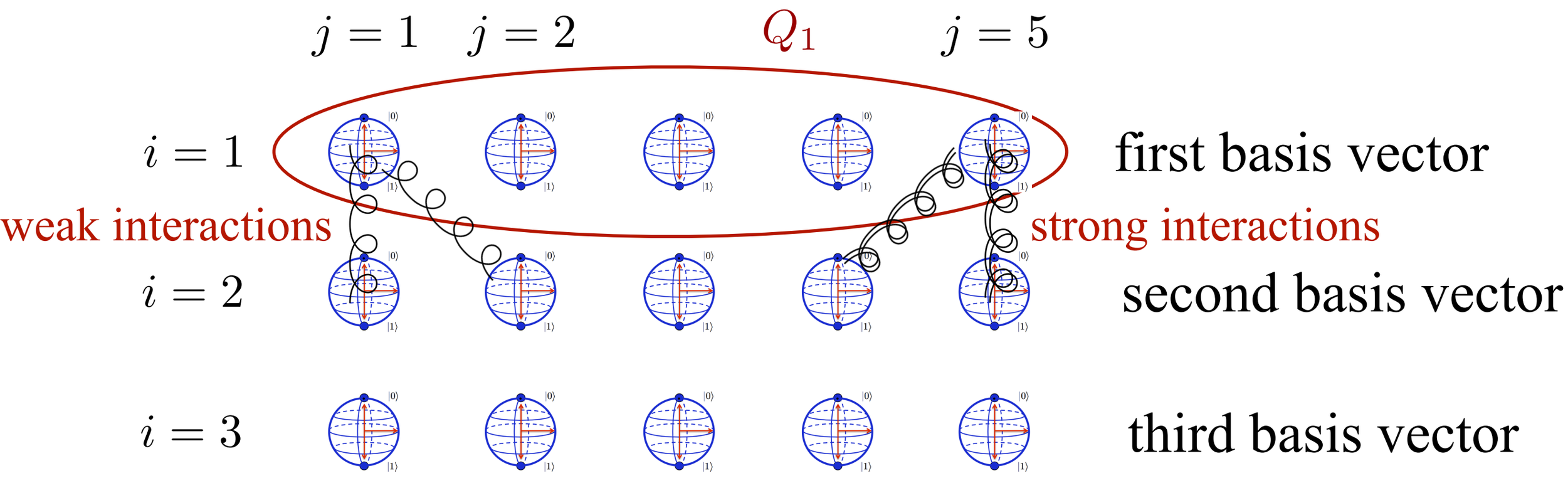
SVP Hamiltonian

problem Hamiltonian

$$H_p = \sum_{ij} Q_i Q_j \ \vec{e}_i \vec{e}_j$$

coupling operator

$$Q_i = \sum_j 2^{j-1} Z_{ij} + \frac{\mathbf{1}}{2}$$



energy expectation

$$\langle \Psi_0 | \exp(i\gamma H_p) \exp\left(i\frac{\pi}{4} H_d\right) H_p \exp\left(-i\frac{\pi}{4} H_d\right) \exp(-i\gamma H_p) | \Psi_0 \rangle$$

$$= \sum_{ij} F_{ij}$$

all qubits

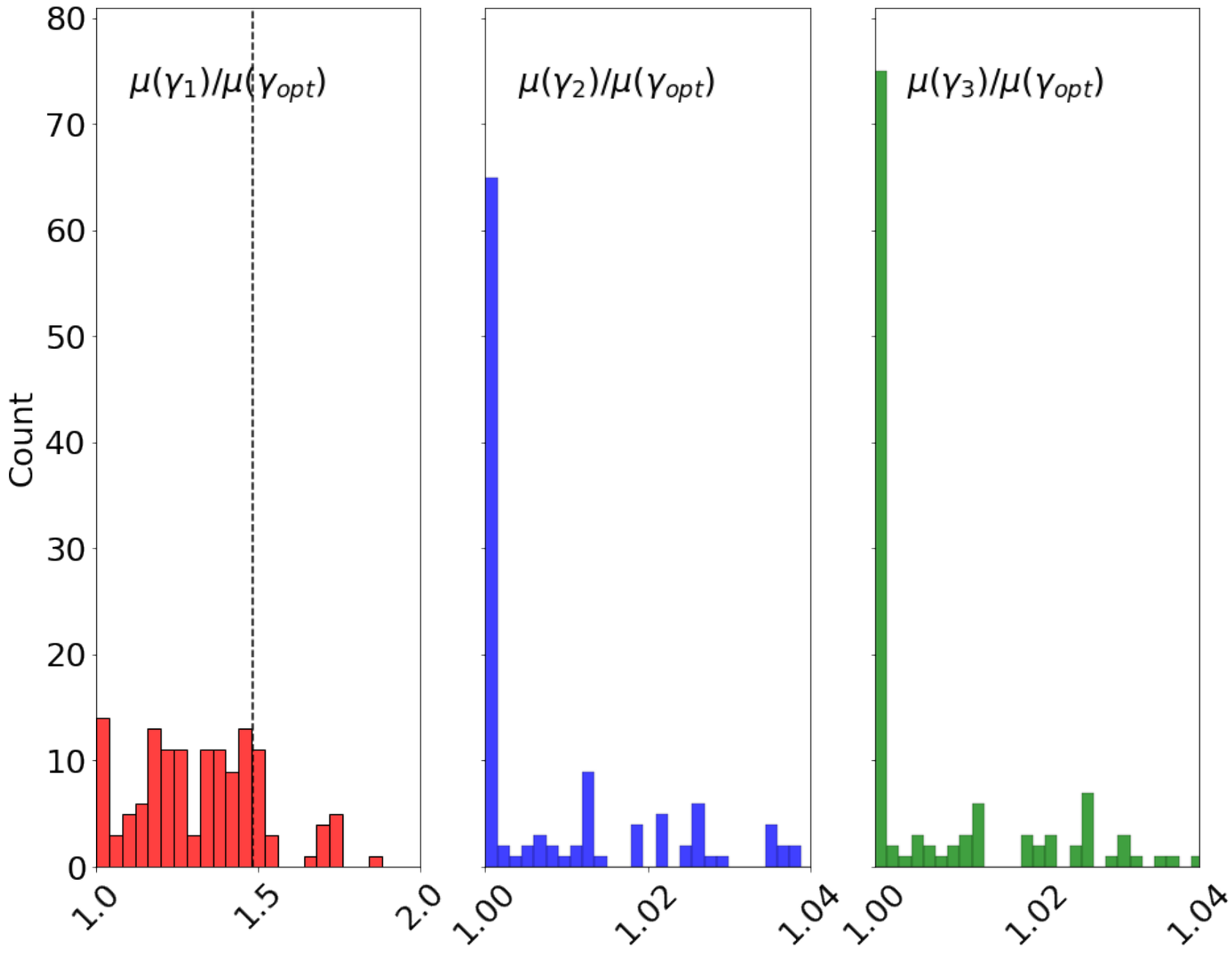
all pairs of qubits → only significant qubits

energy expectation (simulated)

two most significant qubits

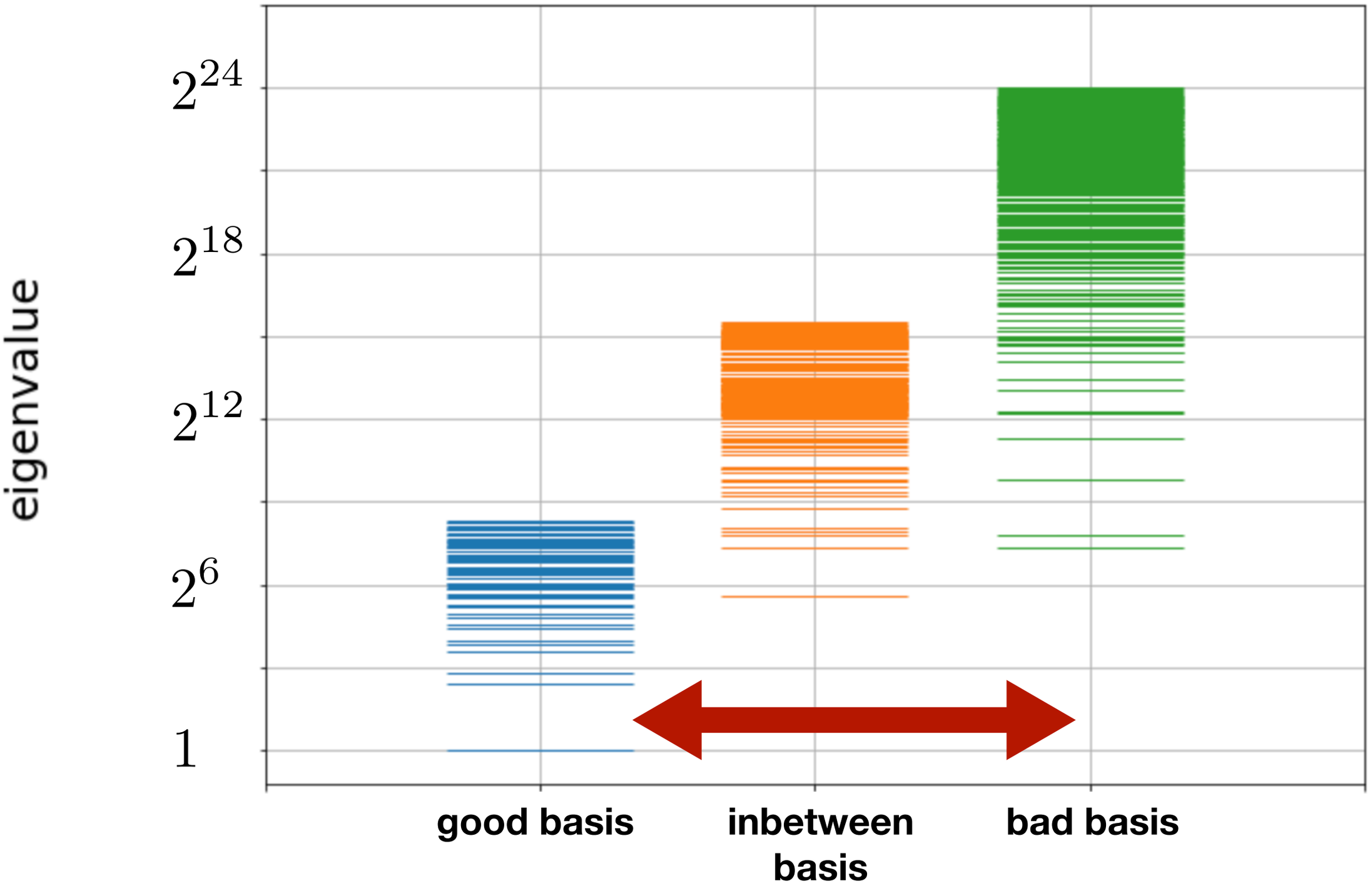
most significant qubits

three most significant qubits

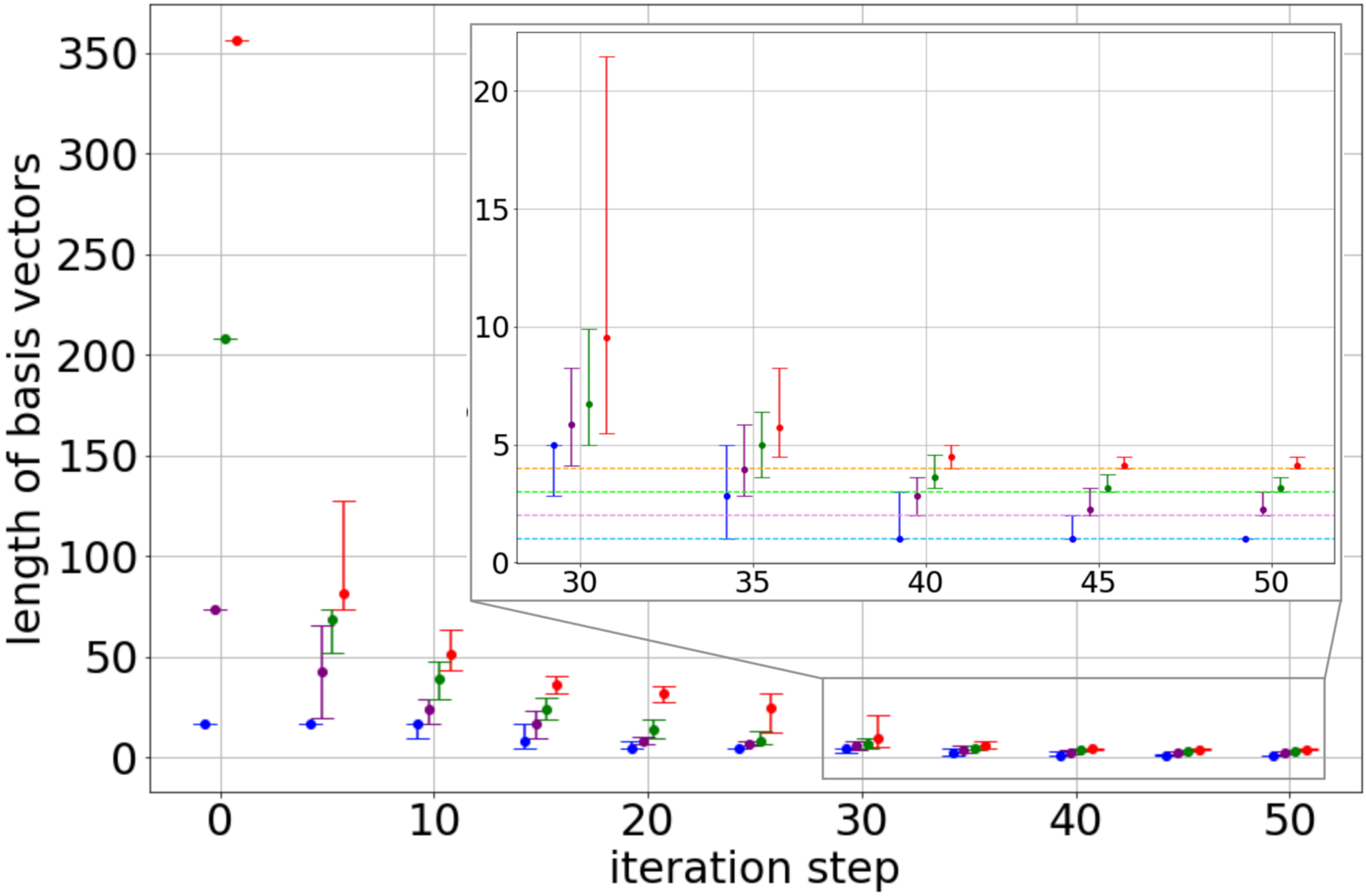


David Joseph, Antonio Martinez, Cong Ling & FM, Phys. Rev. A (accepted) arXiv:2105.13106

truncation errors



hybrid algorithm



Yifeng Rocky Zhu, David Joseph, Cong Ling & FM, arXiv:2204.13432

perspective for quantum SVP

combination of classical and quantum elements

optimisation
sampling

problem Hamiltonian

the team

David Joseph

Adam Callison

Yifeng Zhu

Cong Ling

EPSRC
Pioneering research and skills

YQSE
Quantum Systems Engineering

Controlled Quantum Dynamics

QUANTUM FLAGSHIP

QUANTERA
ERA-NET Cofund in Quantum Technologies