Blind Oracle Quantum Computation

David DiVincenzo

KCIK on-line symposium,

May 15, 2020

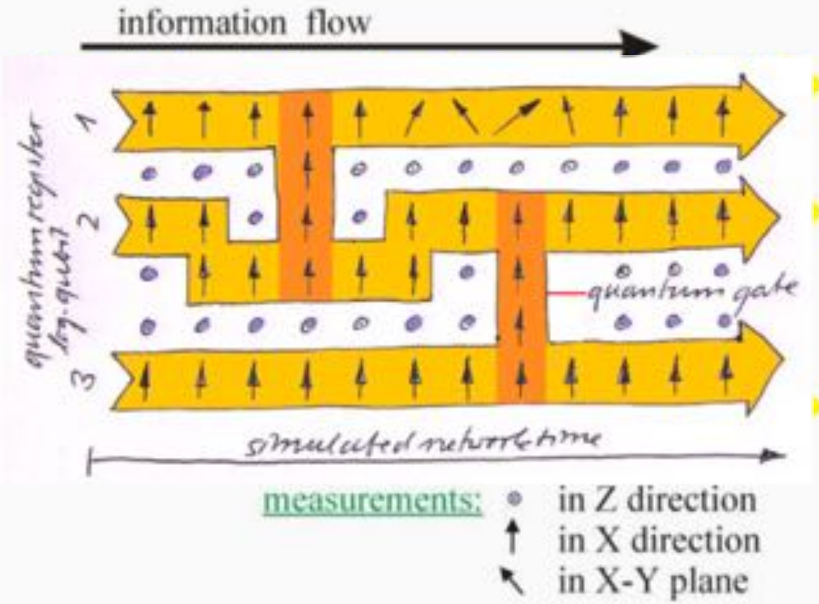
Outline

With PhD student Cica Gustiani

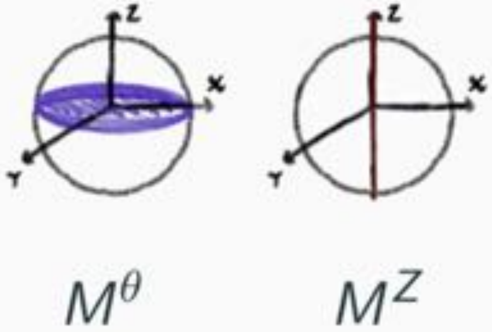
- Motivations:
  - Give meaning to quantum oracles, and oracle algorithms, in a distributed-computing setting
  - Extend the setting of „blind quantum computation“
  - Optimise small, interesting distributed q. algorithms
- New setting: Blind Oracle (Distributed) Q. Comp.
- Review: Blind Q. Comp.,
- Review: Measurement-based Q. Comp.
- Interesting oracle: exact Grover search
- Implementation ideas: networked NV centers

One-way quantum computer (1WQC)[2]

QC: cluster states $|\Phi_{\mathcal{C}}\rangle$



algorithm: adaptive measurements



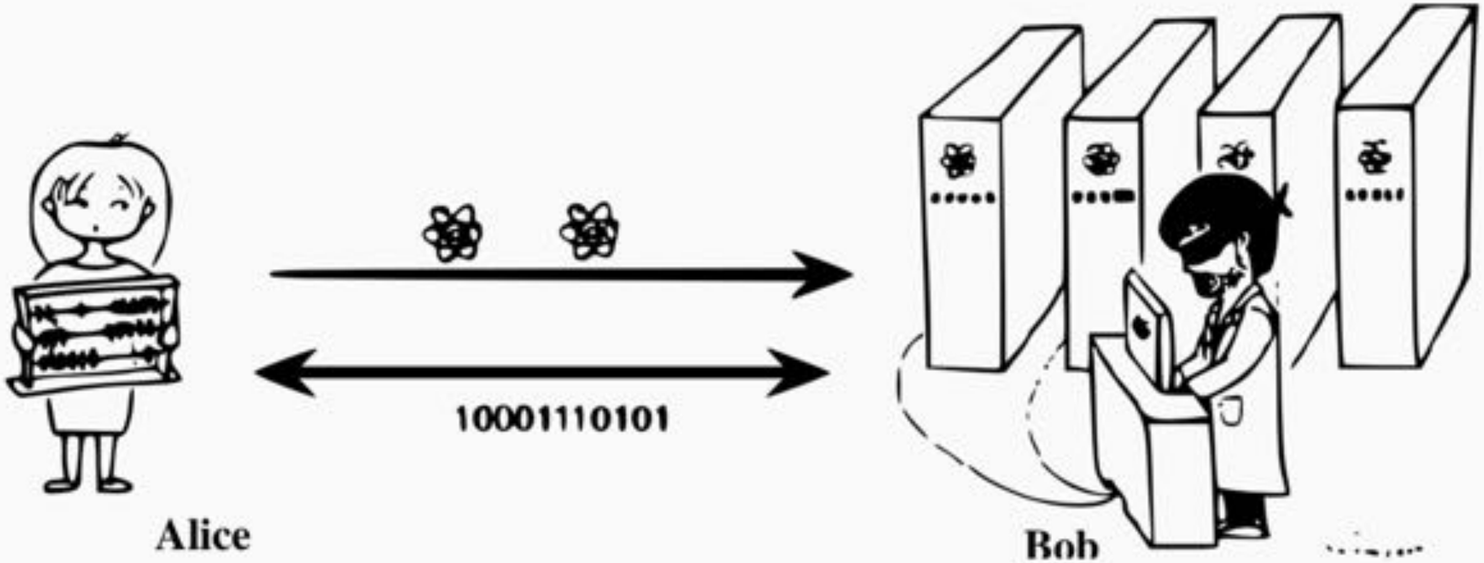
$$M^\theta = \{|+_\theta\rangle\langle+_\theta|, |-_\theta\rangle\langle-_\theta|\},$$
$$M^Z = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$$

2

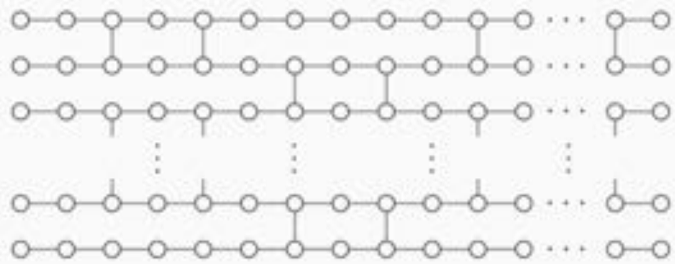
$$|\pm_\theta\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\theta}|1\rangle\right)$$

[2] R. Raussendorf and H. J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. 86, 5188 (2001).

Universal blind quantum computation (UBQC)

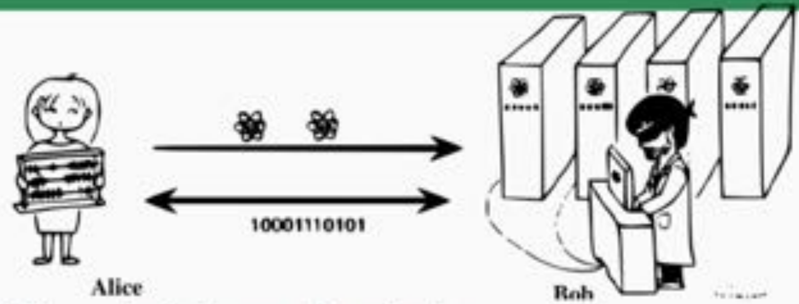


©J. F. Fitzsimons



(brickwork state)

UBQC: protocol[4]



Graph state preparation

- Alice: has in mind $\{(G_b, I, O), \vec{\phi}\}$, G_b =brickwork state
  prepares $Q = \{|\psi\rangle, |+_{\theta_i}\rangle_{i \in I^c}\}$ and send them to Bob
- Bob: entangles Q according to G_b

Classical interaction and measurement

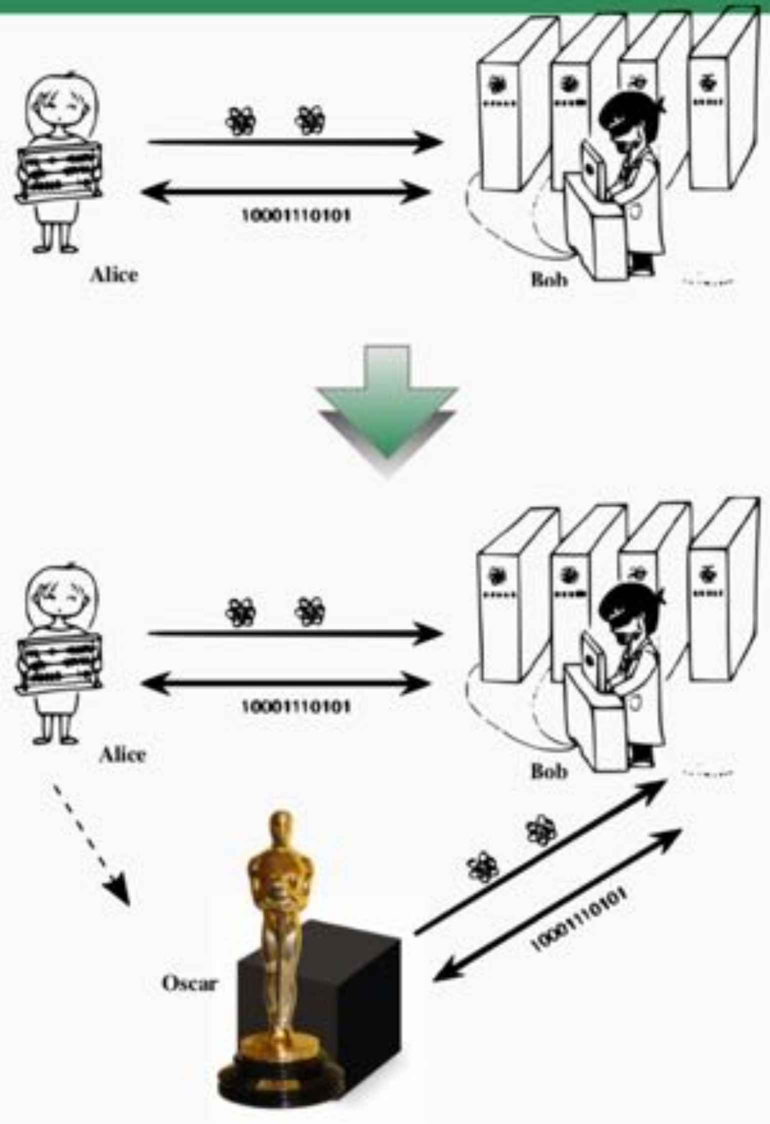
For each $i \in O^c$:

- Alice: computes ϕ'_i (function of $\boldsymbol{\phi}$ and previous measurement outcomes)
  computes $\delta_i = \phi'_i + \theta_i + \pi r_i$, $r_i \in \{0, 1\}$, and broadcast δ_i
- Bob: measures i with angle δ_i
  broadcast measurement outcome s_i
- Alice: real outcome $s_i \oplus r_i$

$$\theta_i, \delta_i, \phi'_i \in \left\{0, \frac{\pi}{4}, \ldots \frac{7\pi}{4}\right\}$$

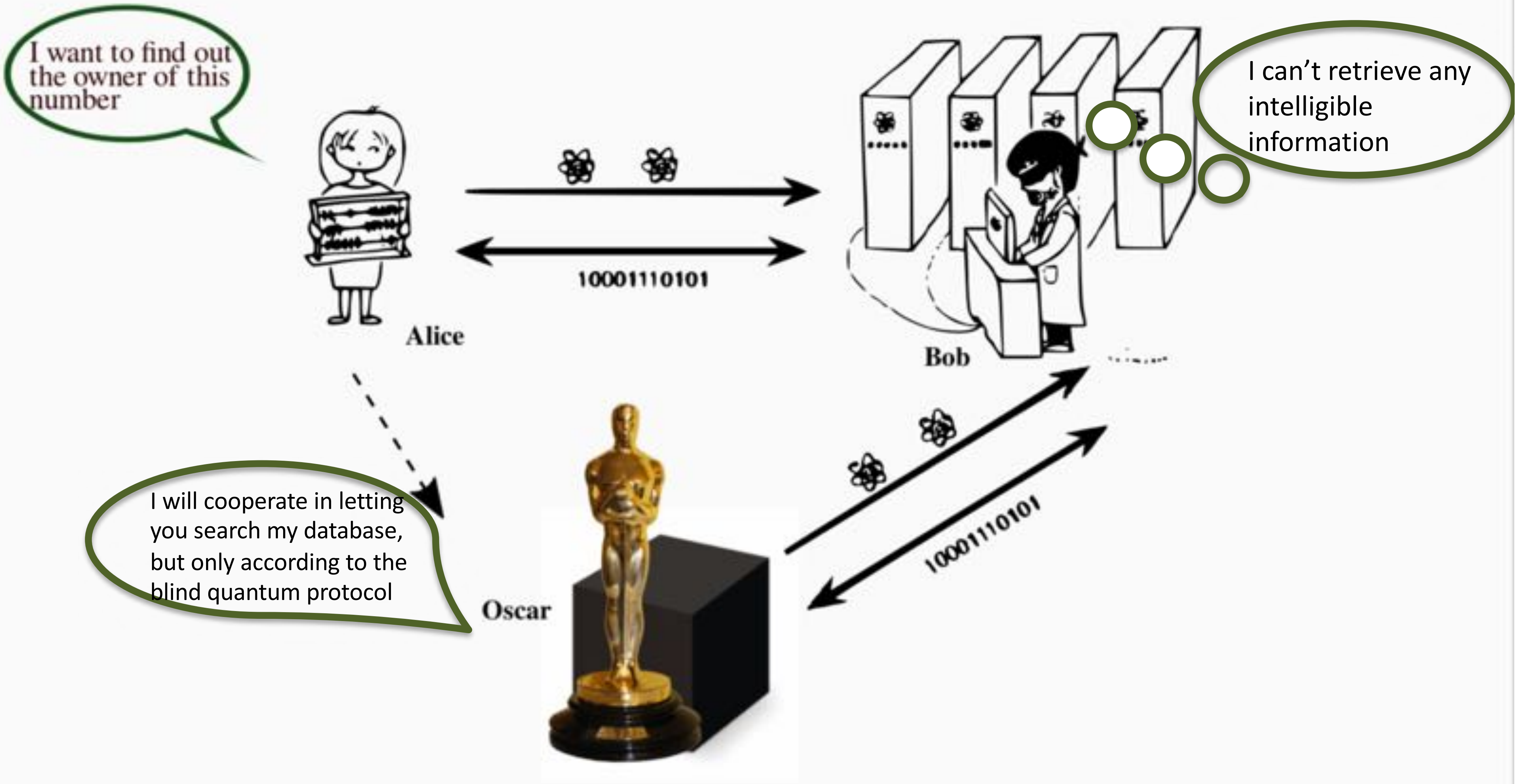
[3] Broadbent, *et al.*, Universal blind quantum computation, arXiv:0807.4154

Our work: blind oracular quantum computation (BOQC)[5]



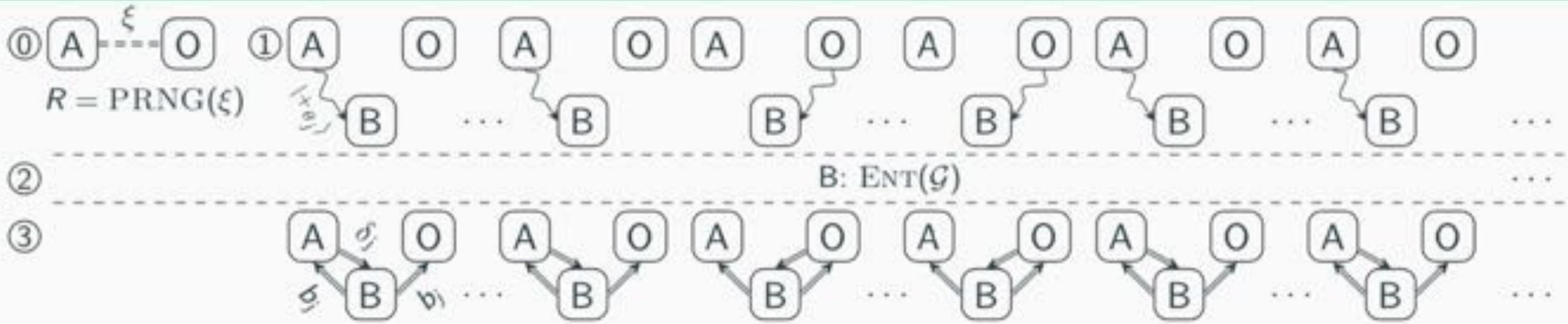
[4] Cica Gustiani, David P. DiVincenzo, Three-qubit exact Grover within the blind oracular quantum computation scheme, 2019, arXiv:1902.05534

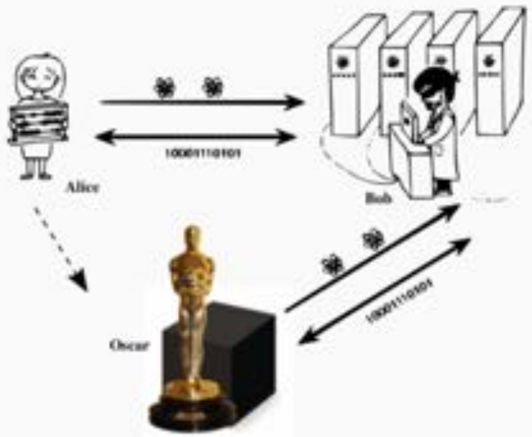
Our work: blind oracular quantum computation (BOQC)



Example for Grover oracle: telephone-number database search

BOQC: protocol





Graph states preparation

Alice: has in mind $\{(G, I, O), \vec{\phi}\}$, $G \equiv \{G_j\}$, without oracles, input $|\psi\rangle$

Oscar: has in mind $\{\{F_j\}, \vec{\varphi}\}$ (total graph $\mathcal{G}$)

Alice, Oscar: share ξ via secure channel; $\vec{r} = PRNG(\xi)$

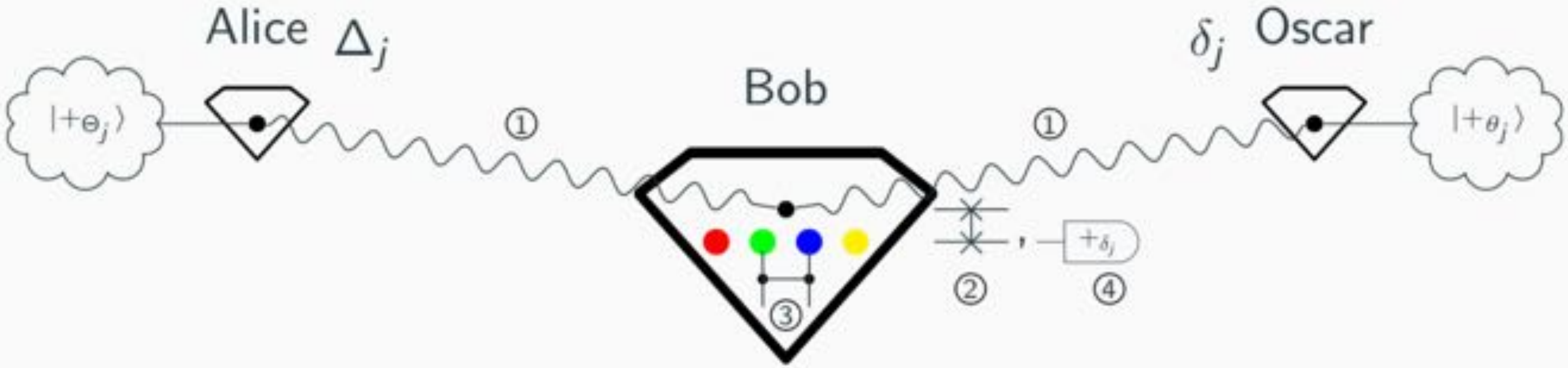
Alice and Oscar send their qubits to Bob

Bob: entangle qubits according to $\mathcal{G}$

Classical interaction and measurement

Like UBQC; everyone knows which nodes belong to Alice/Oscar.

BOQC in NV-centers



① Remote state preparation:
$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+_\theta -_\theta\rangle - |-_\theta +_\theta\rangle)$, Alice/Oscar measures in θ; Bob receives $\frac{1}{\sqrt{2}}(|0\rangle + e^{i(\theta + a\pi)}|1\rangle)$

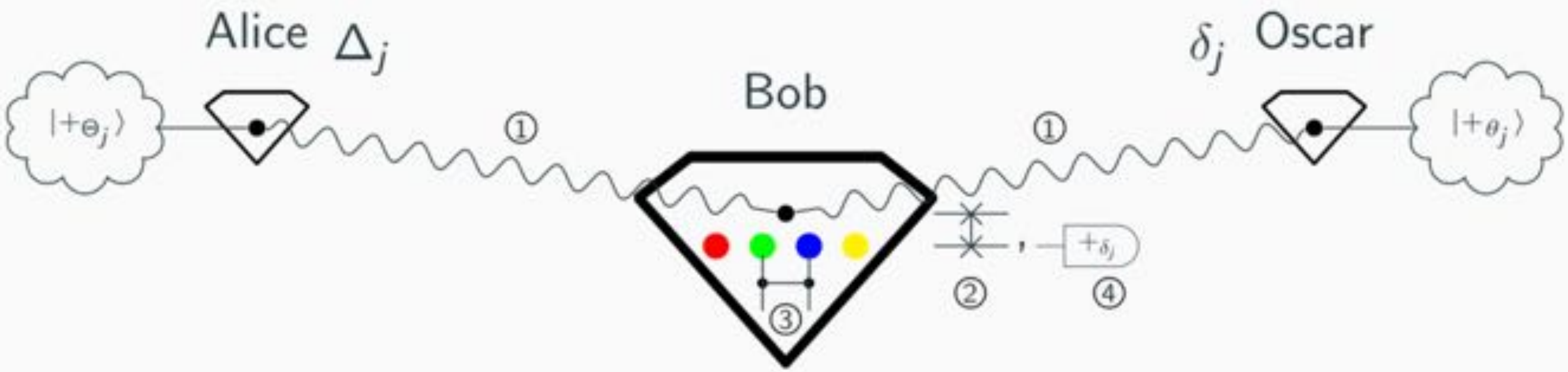
② Swap electron-nuclear spin

③ Entangling (CPHASE) operations

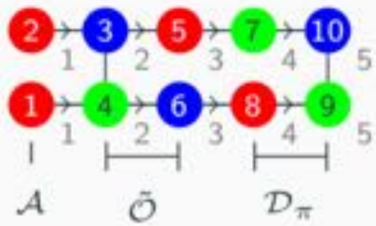
④ Measure in δ

No timing coordination; Alice and Bob do ① after the corresponding qubit is free

BOQC in NV-centers: 3- and 2-qubit BEQS



2-qubit BEQS: 3 physical qubits ≈ 305ms



BEQS: Blind Exact Quantum Search (i.e., Grover problem)

Going to 3-qubit Grover

- 2 interactions with oracle needed
- We will go beyond textbook Grover
  - modify so that it is zero-error (Peter Høyer)
- 3-qubit isn‘t the same as N=8
- Try subset strategy to reduce circuit count

Grover, Høyer

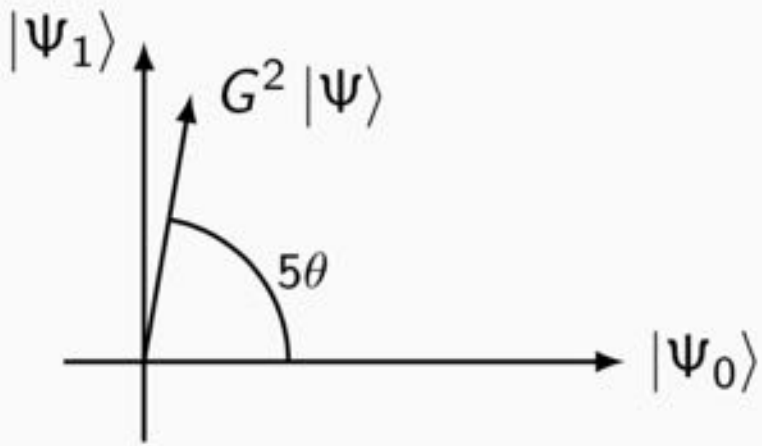
Indices $x = \{0, \ldots, N-1\}; N := 2^n$

Oracle: sol. $y = \{j \in x : f(j) = 1\}$; nsol. $x/y\{j \in x : f(j) = 0\}$

$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{j \in x} |j\rangle = \sqrt{a}\,|\Psi_1\rangle + \sqrt{1-a}\,|\Psi_0\rangle\,; a := M/N$

Grover

$G^k, \quad k \approx \sqrt{N/M}$



Høyer

$Q(\phi, \psi)$ rotates $|\alpha| \leq 2\theta$

$Q(\pi, \pi) \equiv G$ rotates 2θ

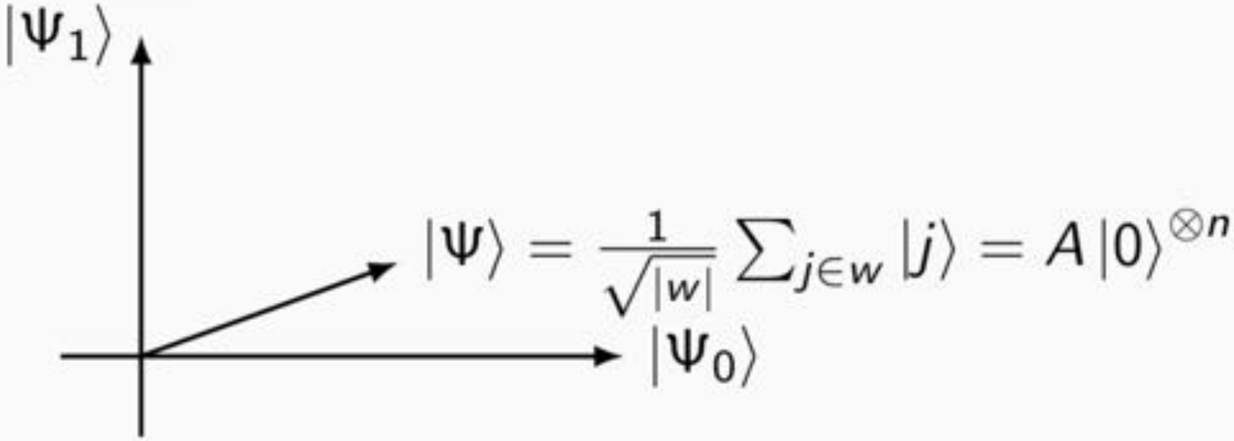
$Q(\phi, \psi) = D(\psi)O(\phi)$

$D(\psi) = I - (1 - e^{i\psi})\,|\Psi\rangle\langle\Psi|$

$O(\phi) = I - (1 - e^{i\phi})\,|\Psi_1\rangle\langle\Psi_1|$

Grover + Høyer

$w \subset x$, database choice



k or $k+1$ iterations

All possible 3-qubit exact Grover circuits

3 qubits, N=8, states are 01234567
(i.e, 000,001,010,011,100,101,110,111)

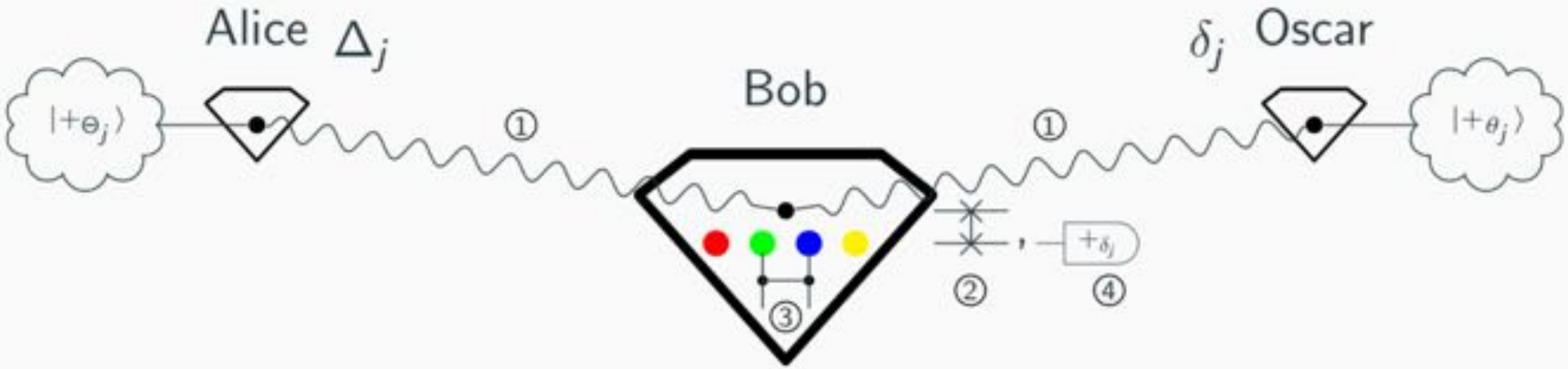
But smaller instances can also be created inside 3 qubits:

N=5: 01234, 01247, 01256 (all others equivalent to these 3)
N=6: 012345, 012347, 012567 (all others equivalent to these 3)
N=7: 0123456 (all others equivalent)

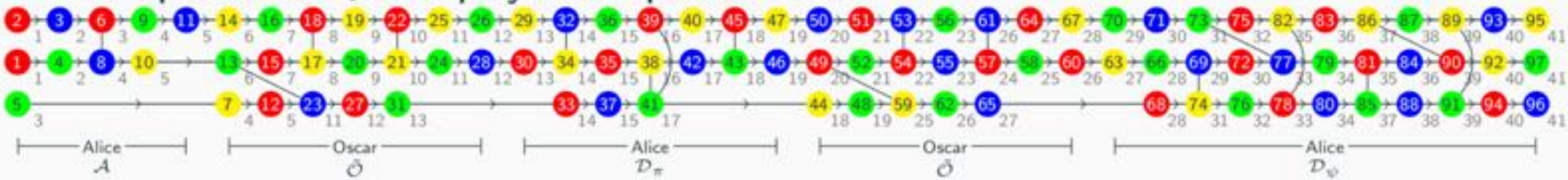
Circuit count is different for all these.

The most efficient that we have found is N=5, 01256, but where item 0 gives output as superposition of 0 and 4.

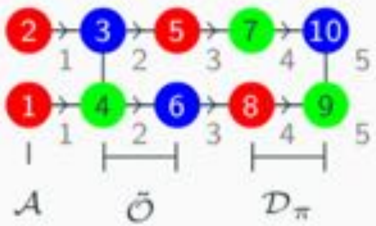
BOQC in NV-centers: 3- and 2-qubit BEQS

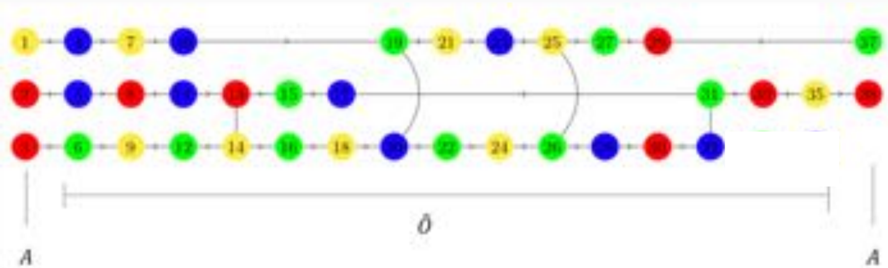


3-qubit BEQS: 4 physical qubits $\approx 3s$



2-qubit BEQS: 3 physical qubits $\approx 305ms$





2-qubit Blind Simon – 4 physical qubits (R. Sachdeva)

Current work – formalize security with the tools of Abstract Cryptography

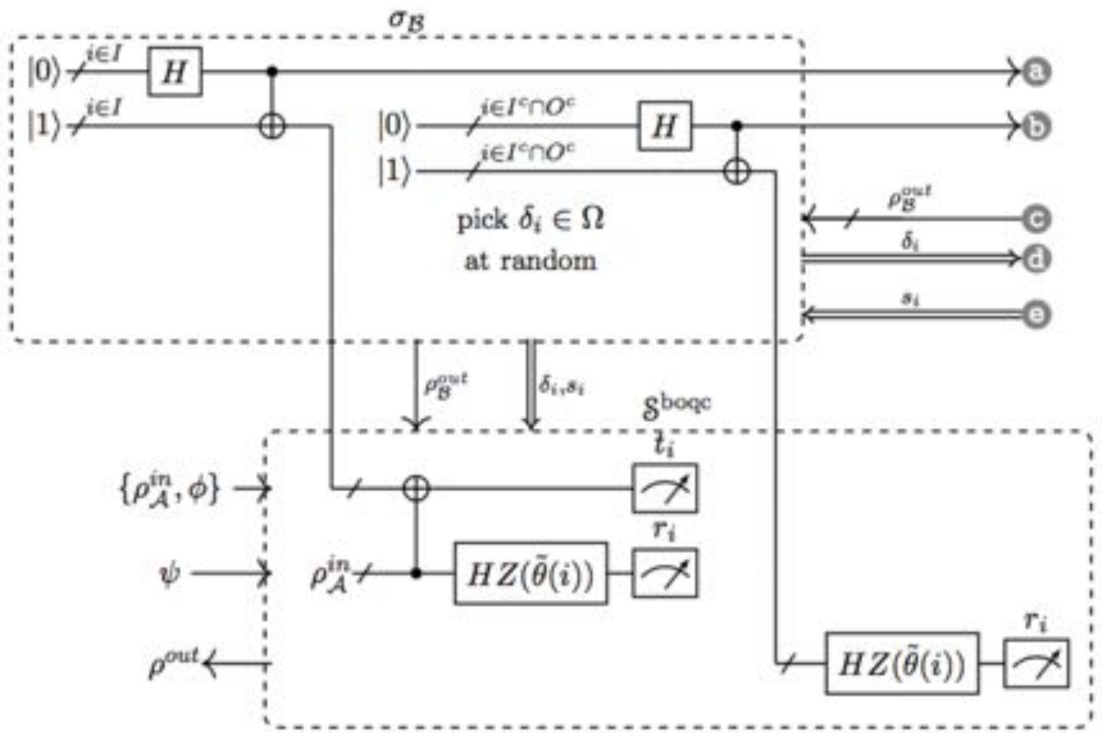


Figure 7: Pictorial representation of $\sigma_B \mathcal{S}^{\text{boqc}}$ defined in Protocol 3. Each variable

Outline

With PhD student Cica Gustiani

- Motivations:
  - Give meaning to quantum oracles, and oracle algorithms, in a distributed-computing setting
  - Extend the setting of „blind quantum computation“
  - Optimise small, interesting distributed q. algorithms
- New setting: Blind Oracle (Distributed) Q. Comp.
- Review: Blind Q. C., Measurement-based Q. C.
- Interesting oracle: exact Grover search
- Implementation ideas: networked NV centers