

# Suprématie quantique : où en sommes-nous aujourd'hui?

André Chailloux, Inria de Paris

2 juin 2021, Collège de France

## Suprématie quantique [Preskill 2012]

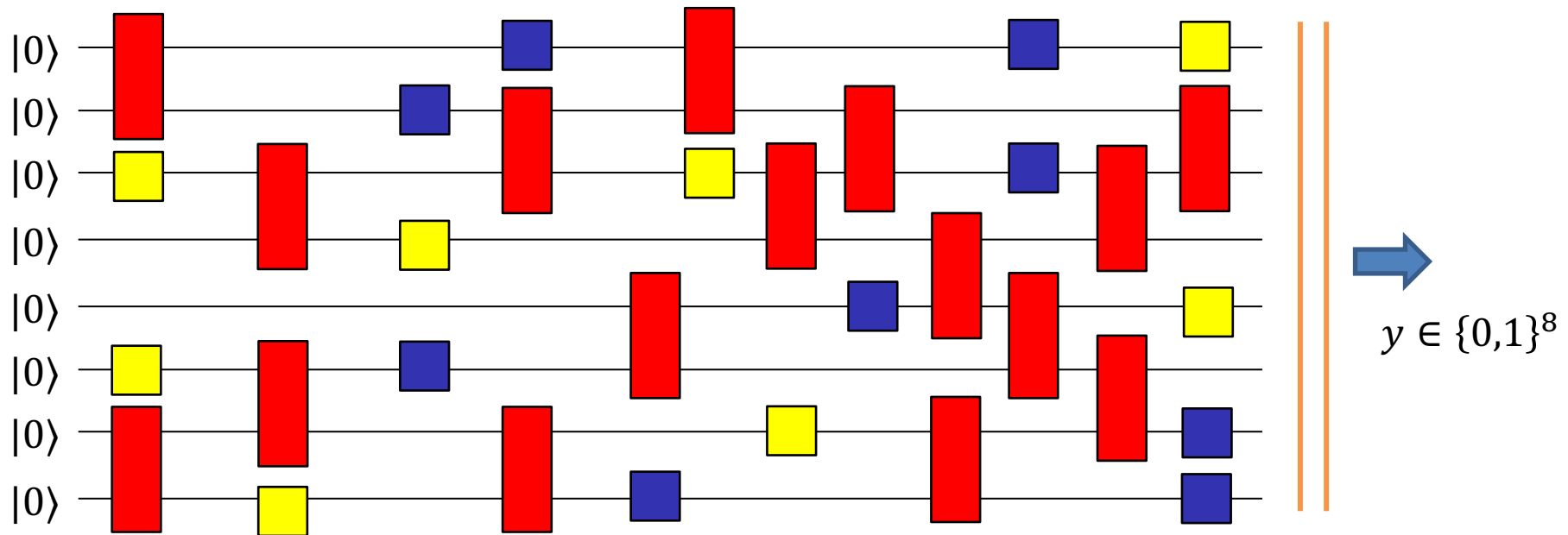
Résoudre un problème calculatoire grâce à un ordinateur quantique qu'on n'est pas capable de résoudre avec un ordinateur classique.

1. Le problème d'Echantillonnage de Circuit Quantique Aléatoire
2. La puce SYCAMORE et le calcul effectué
3. Difficulté du problème classique
4. Suprématie quantique, où en sommes nous aujourd'hui

# Le problème ECQA

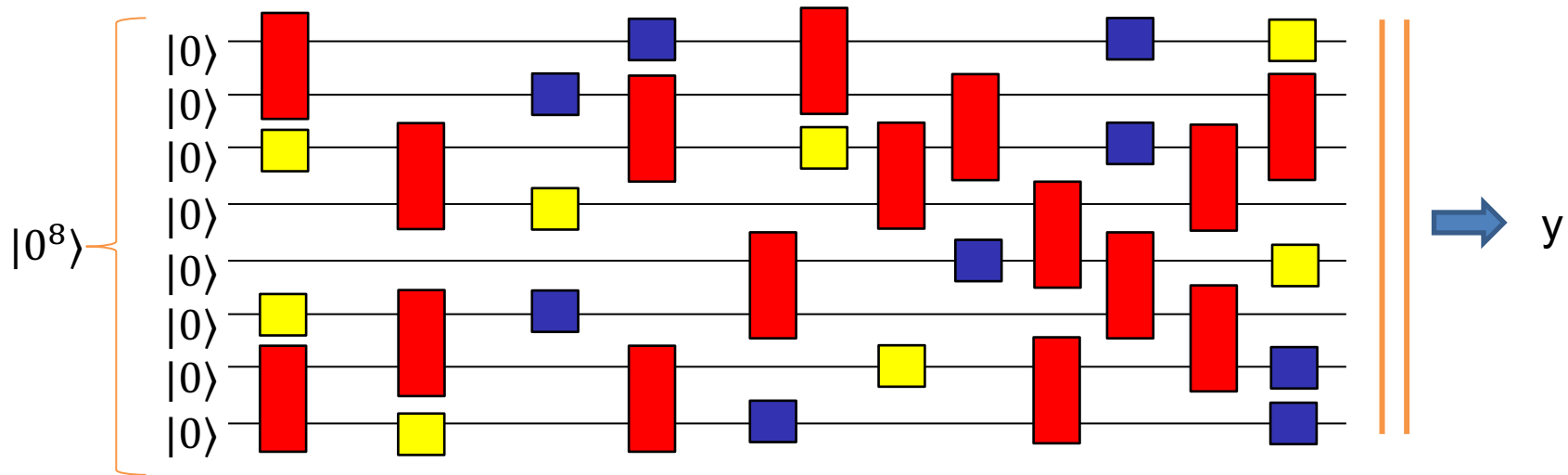
# Circuits quantiques

- Circuit quantique: manière de modéliser un calcul quantique.



Exemple de circuit sur 8 qubits avec 33 portes logiques quantiques (sur 1 ou 2 qubits) et une mesure finale

# Circuits quantiques



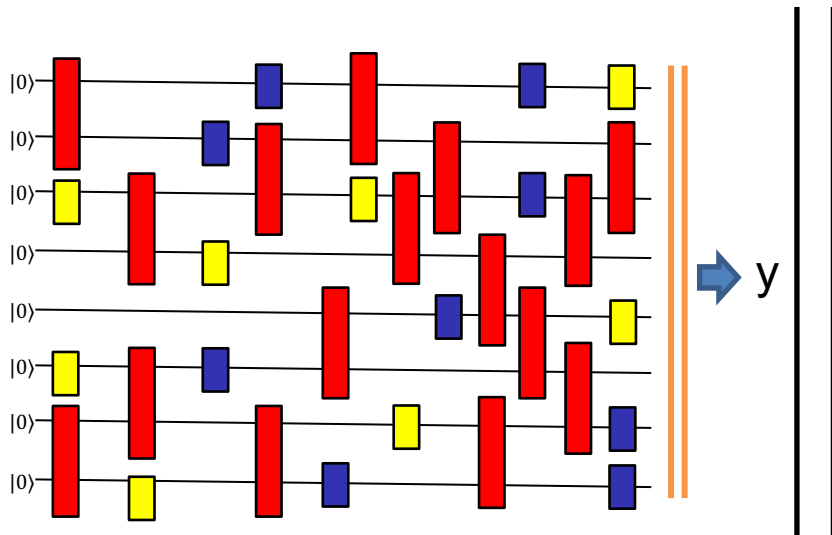
Exemple de circuit sur 8 qubits avec 33 portes logiques quantiques et une mesure finale

- Pour un circuit  $C$  qui agit sur  $n$  qubits, soit  $p_y^C$  la probabilité de mesurer  $y$  sur l'entrée  $|0^n\rangle$ . C'est-à-dire :  $p_y^C = |\langle y|C|0^n\rangle|^2$ .
- Un circuit quantique sur  $n$  qubit agit sur  $2^n$  amplitudes simultanément.

- Problème d'Echantillonnage de Circuit Quantique Aléatoire

- Entrée: la description d'un circuit C choisi aléatoirement qui agit sur n qubits.
- Sortie: trouver un programme qui va être capable de sortir y avec probabilité  $p_y^C$ .

Entrée: description de C



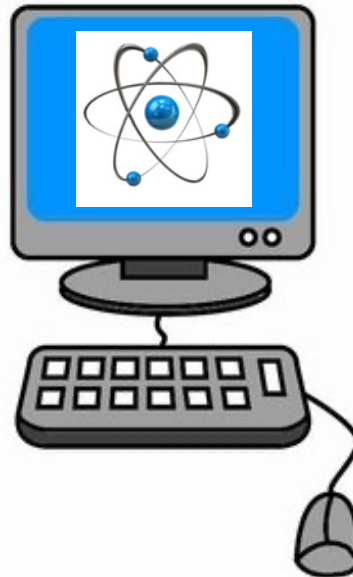
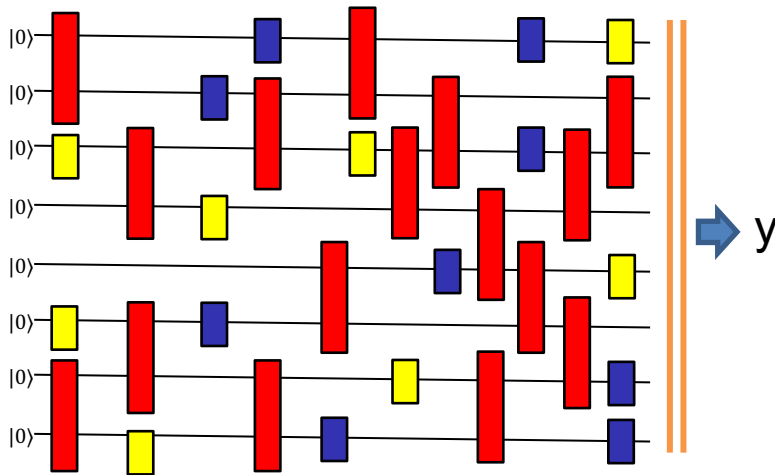
Sortie: un programme qui sort y avec proba  $p_y^C$



# Résoudre le problème Problème ECQA

- Résoudre le problème ECQA avec un ordinateur quantique programmable:

Description de C



Programme:

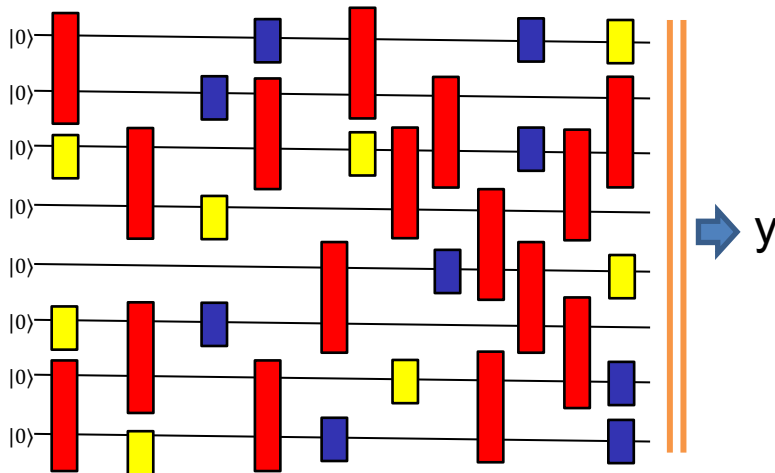
- Lance le circuit C sur l'entrée  $|0^n\rangle$
- Mesure la sortie y
- Renvoie y



# Résoudre le problème Problème ECQA

- Résoudre le problème ECQA avec nos ordinateurs actuels

Description de C



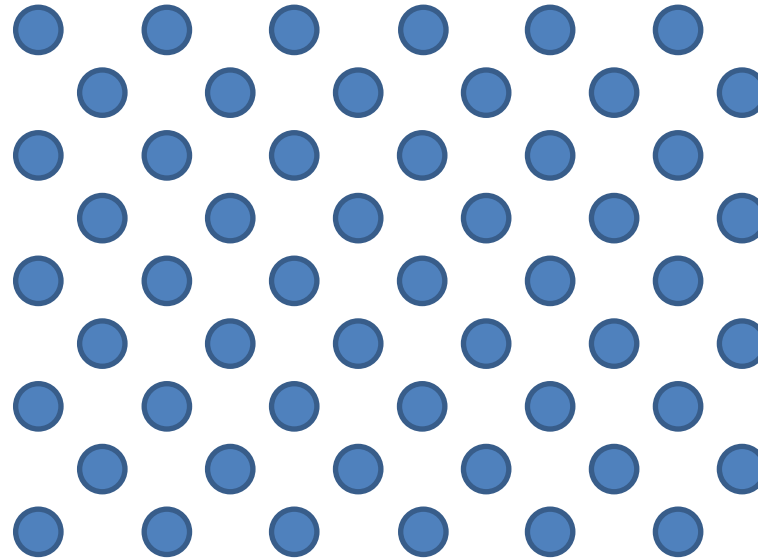
Programme:

- Simule le circuit quantique C et essaie de sortir  $y$  avec proba  $p_y^C$ .
- Cette simulation semble trop complexe.

# La puce SYCAMORE et la démonstration de suprématie

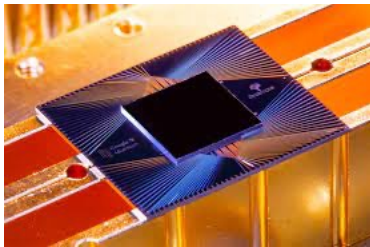
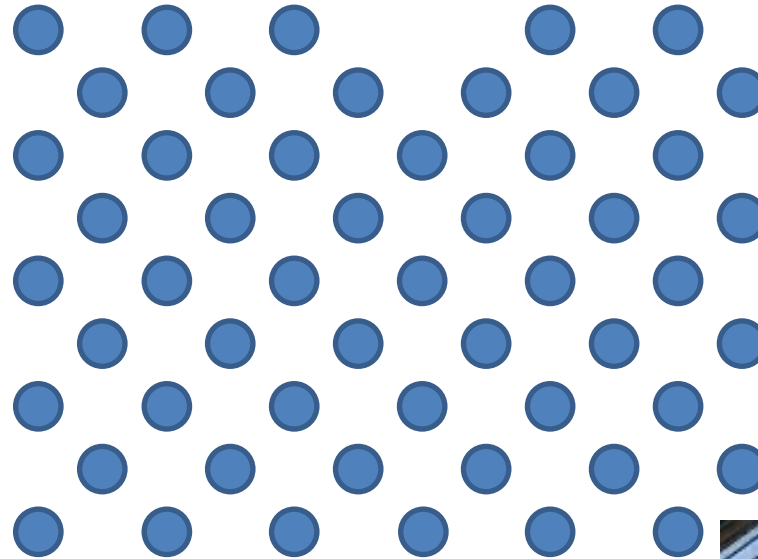
Résultat annoncé (2019): création d'une puce quantique avec des qubits suffisamment stables pour faire tourner des calculs complexes, impossibles à réaliser avec un ordinateur usuel (Suprématie quantique)

- 54 qubits agencés dans un carré de  $9 \times 6$



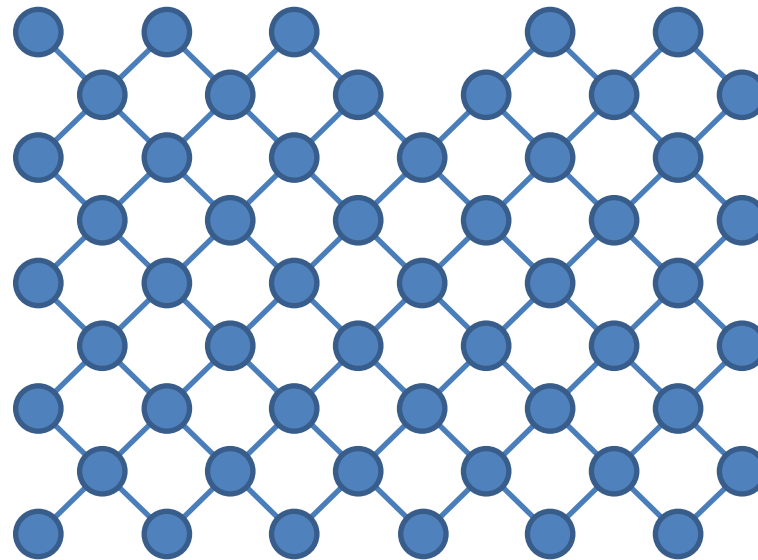
# Circuit SYCAMORE

- 54 53 qubits agencés dans un carré de  $9 \times 6$



# Circuit SYCAMORE

- ~~54~~ 53 qubits agencés dans un carré de  $9 \times 6$
- Liaisons selon certains voisins



- On peut appliquer des portes logiques quantiques sur 1 qubit ou sur des paires de qubits reliés.

- Portes sur 1 qubit

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}; S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}; T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \sqrt{-i} \\ \sqrt{-i} & 1 \end{pmatrix}$$

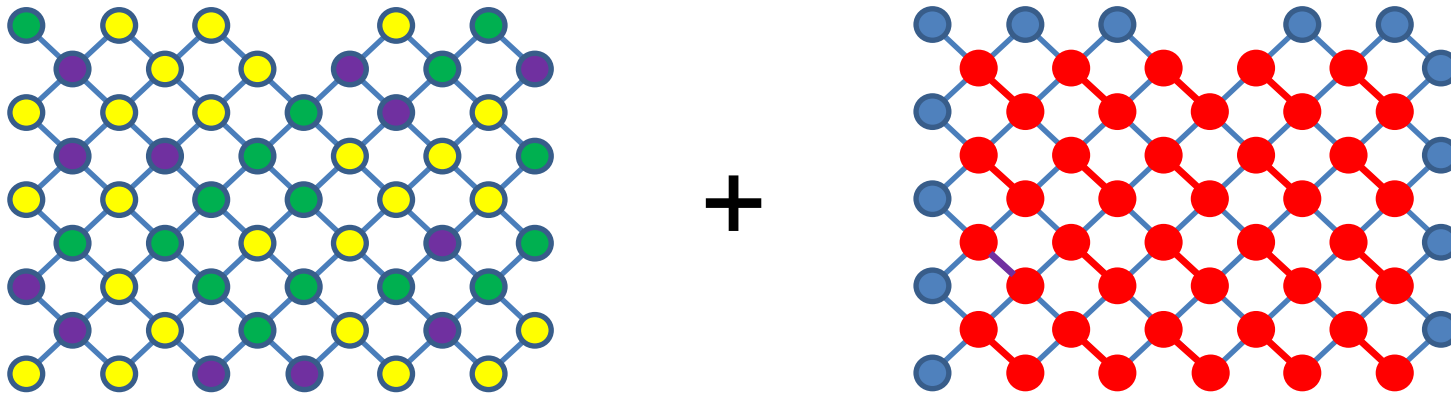
- Porte sur 2 qubits

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\theta) & -i\sin(\theta) & 0 \\ 0 & -i\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \text{ avec } \theta \approx \frac{\pi}{2} \text{ et } \phi \approx \frac{\pi}{6}.$$

- Ce jeu de portes est universel.

# Calcul fait dans l'expérience

- Calcul fait sur la puce SYCAMORE: 20 couches de



- Description du circuit: Pour chaque couche
  - Pour chaque qubit, quelle porte parmi R,S,T est utilisée (vert,jaune,violet)
  - Quelle est la disposition des portes U à 2 qubits (disposition en rouge)
- Au total:  $(53 + [19; 24]) * 20 = [1440;1540]$  portes quantiques



- SYCAMORE est capable de faire tourner un tel circuit C sur 53 qubits avec 20 couches.
- 40 microsecondes par calcul : capable de sortir beaucoup d'échantillons.
- Mais: la puce SYCAMORE est imparfaite donc ne renvoie pas exactement  $y$  avec probabilité  $p_y^C$ .

- La probabilité que le circuit fonctionne correctement est  $\approx 0.2\%$ 
  - Quand le circuit ne fonctionne pas, on fait l'hypothèse que le résultat sorti est aléatoire.

- La probabilité  $q_y^C$  que le circuit SYCAMORE sorte  $y$  est donc

$$q_y^C = \frac{998}{1000} * \frac{1}{2^{53}} + \frac{2}{1000} * p_y^C$$

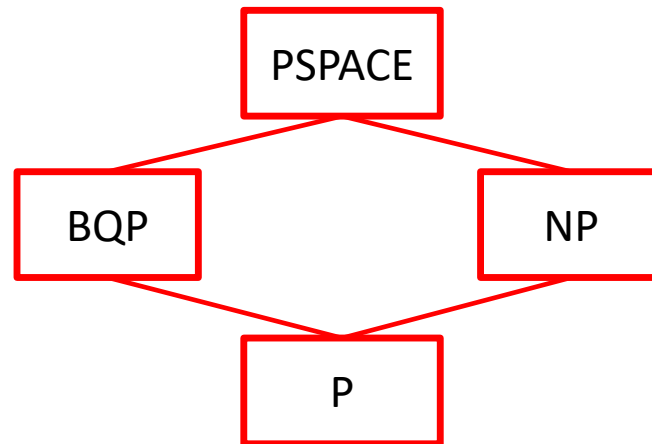
- C'est un faible biais par rapport à l'uniforme mais ça semble quand même dur pour un ordinateur classique.
- Comment vérifier le calcul?
  - Principalement de l'extrapolation, et critère *XEB*.
  - Confiance raisonnable que le calcul sort  $y$  avec proba  $q_y^C$ .

Difficulté classique de ce problème calculatoire

- Deux arguments principaux:
  1. Un argument issu de la théorie de la complexité
  2. Un argument empirique

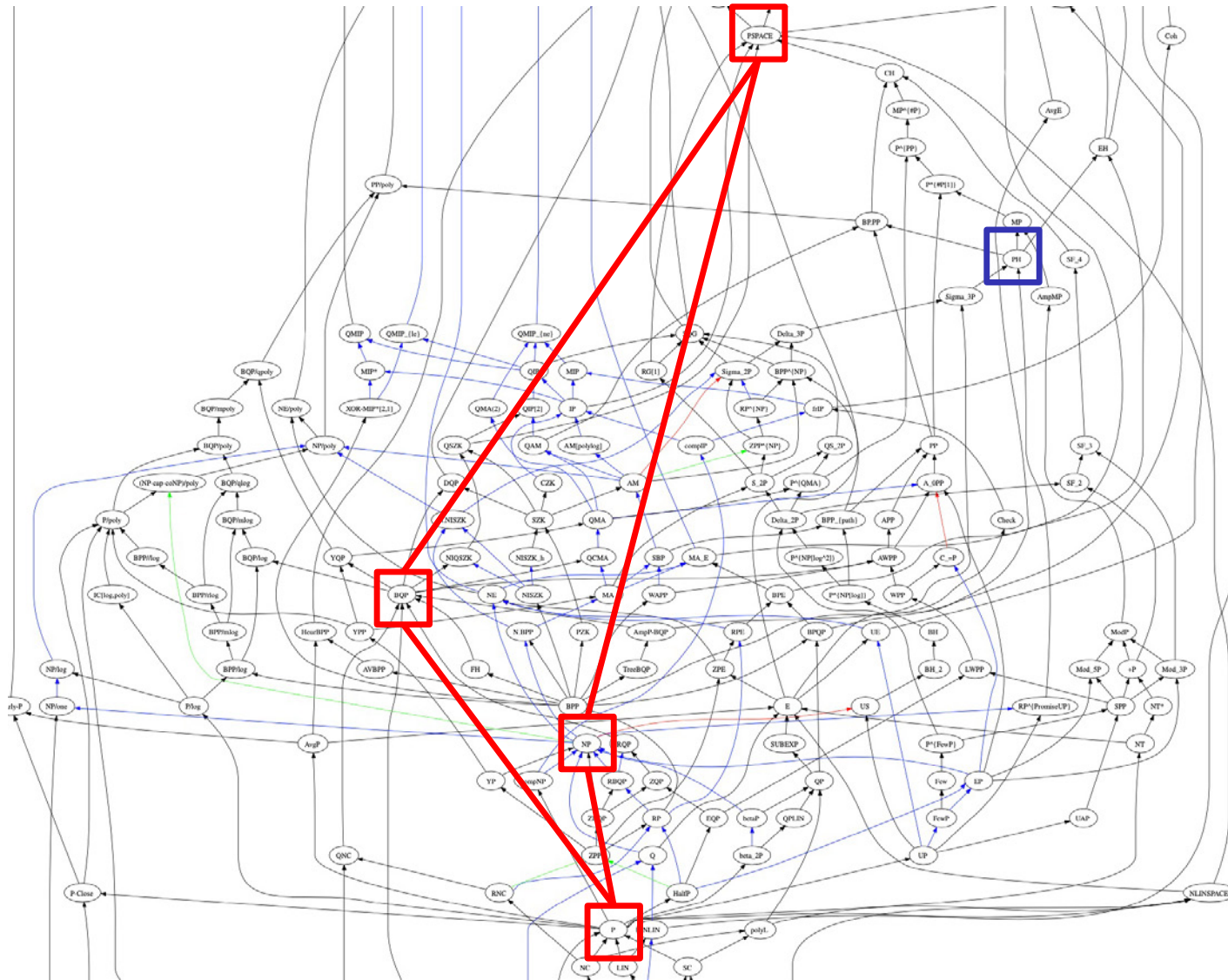
S'il existe un algorithme classique qui résout le problème ECQA en temps polynomial alors la Hierarchie Polynomiale s'effondre au 3<sup>ème</sup> niveau

- La théorie de la complexité essaie entre-autres de classier la difficulté des problèmes calculatoires.
- Exemple de classes de complexité: P, NP, BQP, PSPACE



- Très difficile de montrer des inclusions strictes (question P vs. NP)

# Complexity zoo



# L'argument de complexité

- La classe de complexité PH: La hiérarchie polynomiale.
- [Simplifié] Au  $i$ -ème niveau, la classe correspond au problème suivant: pour un circuit C efficace donné, déterminer si

$$\forall y_1 \exists y_2 \dots \forall y_{i-1} \exists y_i, C(y_1, \dots, y_i) = 1.$$

- PH est l'union sur  $i$  de tous les niveaux.
- Si on sait échantillonner un circuit quantique aléatoire C efficacement, PH se ramène aux problèmes de la forme

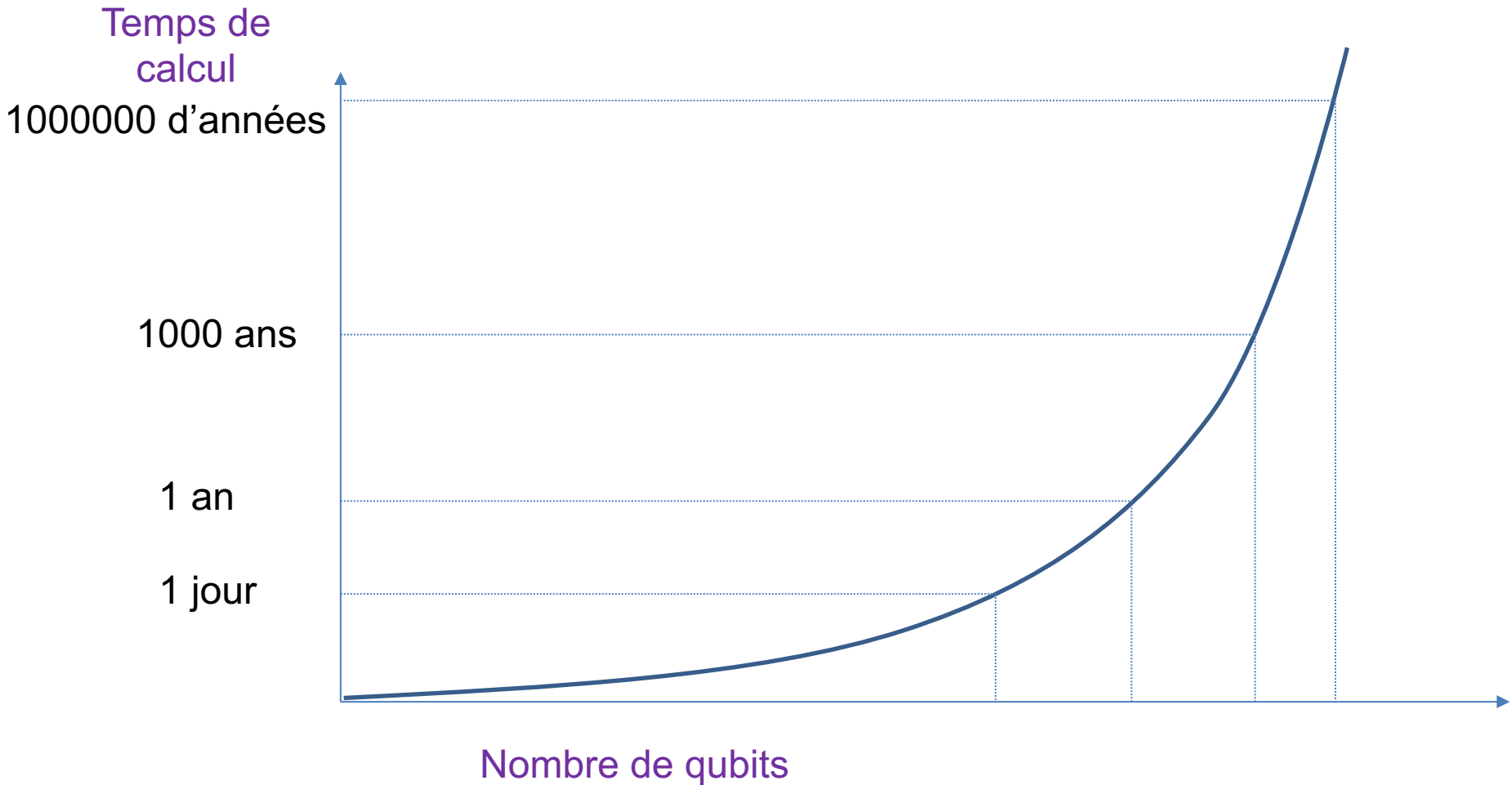
$$\forall y_1 \exists y_2 \forall y_3, C(y_1, y_2, y_3) = 1.$$

- On conjecture que chaque niveau permet de résoudre des problèmes plus complexes. questions plus complexes.
  - Contradiction.



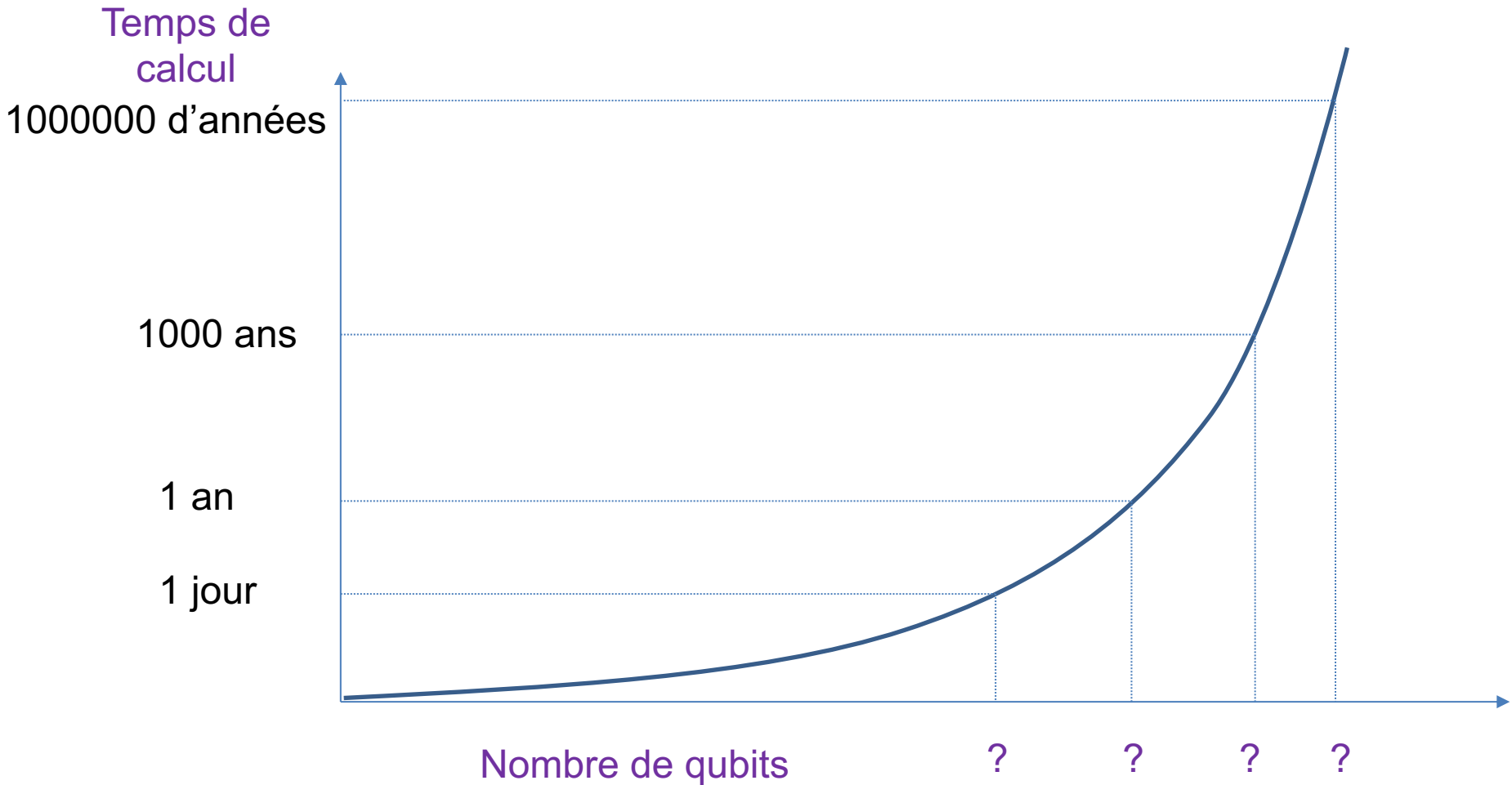
# Comment interpréter le résultat de complexité

- Sauf événement improbable, le problème ECQA est **difficile**.



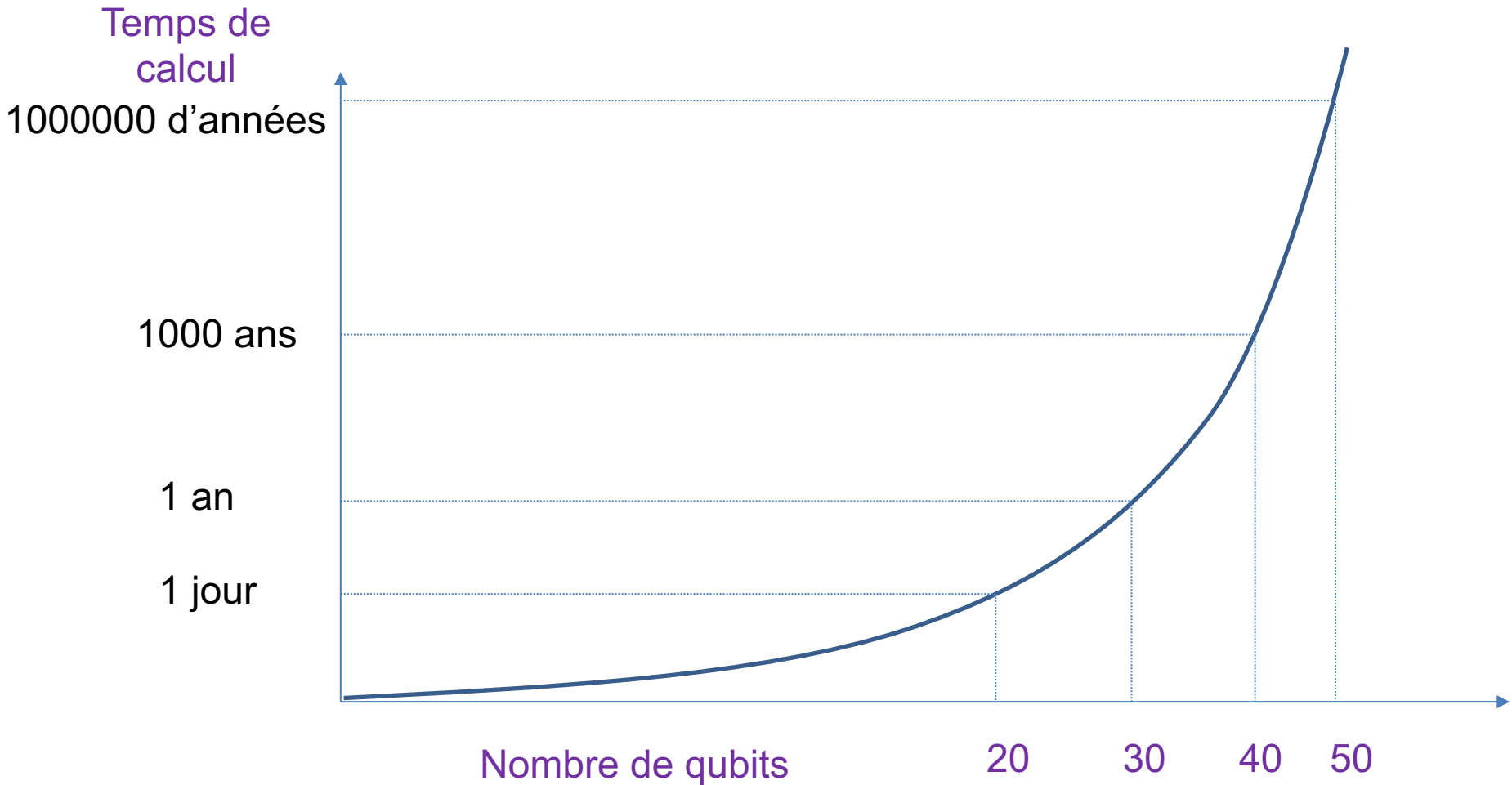
# Comment interpréter le résultat de complexité

- Sauf événement improbable, le problème ECQA est **difficile**.



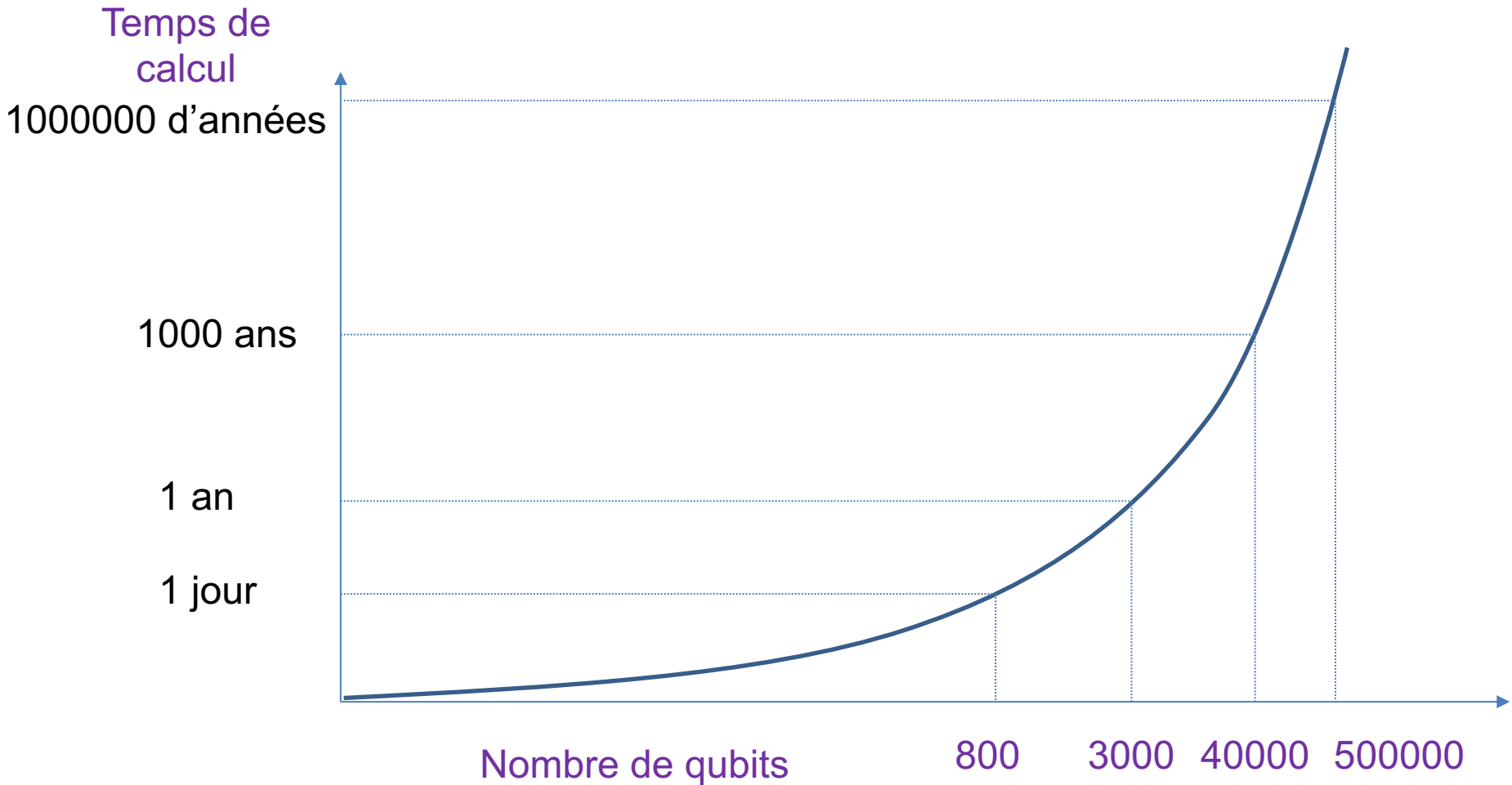
# Comment interpréter le résultat de complexité

- Sauf événement improbable, le problème ECQA est **difficile**.



# Comment interpréter le résultat de complexité

- Sauf événement improbable, le problème ECQA est **difficile**.



- La puce SYCAMORE arrive à produire des échantillons corrects avec probabilité 0.2%, pour  $n = 53$  et 20 couches de portes (de profondeur 2)
  - Beaucoup de bruit: mais on a aussi des arguments de complexité (plus faibles) pour ce cas là.
  - Est-ce-que  $n = 53$  et 20 couches sont suffisants pour rendre le problème difficile?
- Argument empirique: on regarde les meilleurs algorithmes existants

- 2 méthodes principales:

1. La méthode de Schrödinger: plutôt efficace mais demande de la mémoire exponentielle en  $n$ .
2. La méthode de Feynman: moins efficace mais demande beaucoup moins de mémoire.

# Résolution classique de problème ECQA: l'analyse de Google

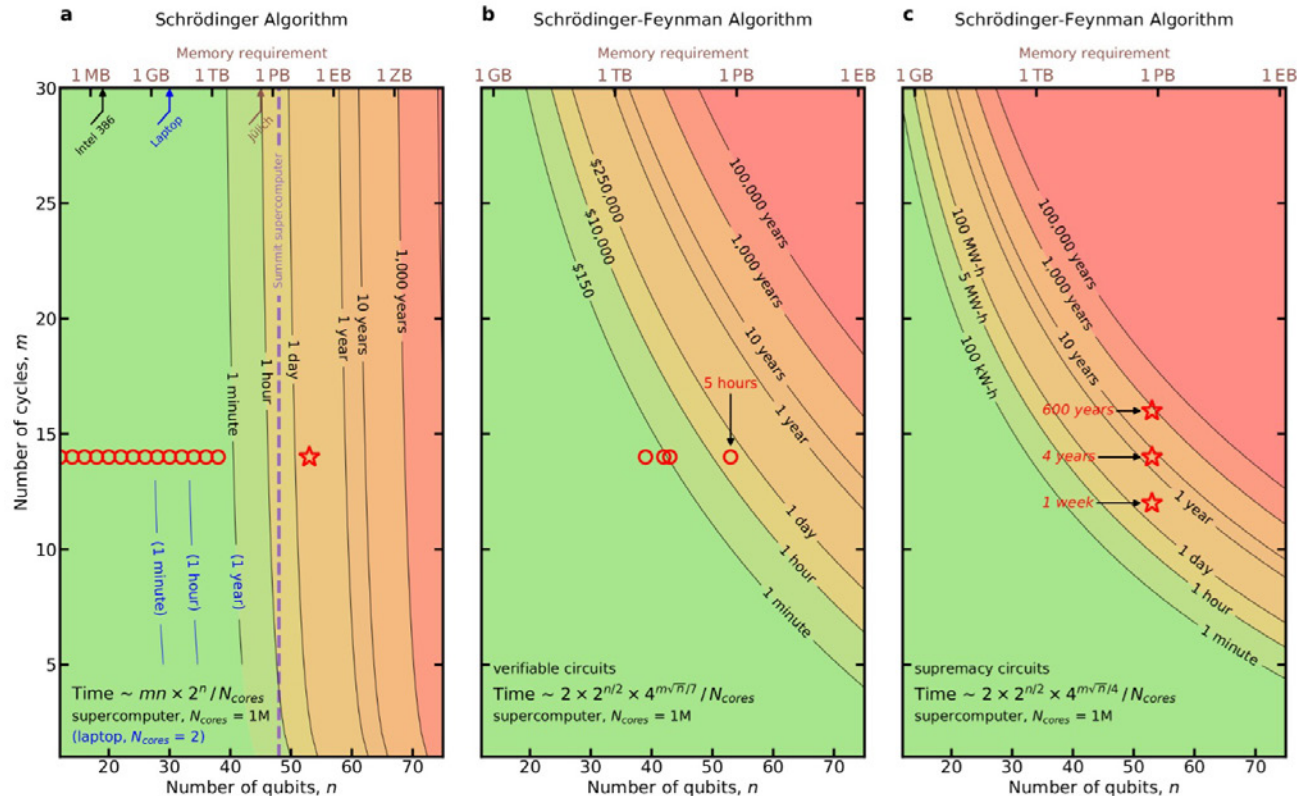


FIG. S50. Scaling of the computational cost of XEB using SA and SFA. **a**, For a Schrödinger algorithm, the limitation is RAM size, shown as vertical dashed line for the Summit supercomputer. Circles indicate full circuits with  $n = 12$  to 43 qubits that are benchmarked in Fig. 4a of the main paper. 53 qubits would exceed the RAM of any current supercomputer, and is shown as a star. **b**, For the hybrid Schrödinger-Feynman algorithm, which is more memory efficient, the computation time scales exponentially in depth. XEB on full verifiable circuits was done at depth  $m = 14$  (circle). **c**, XEB on full supremacy circuits is out of reach within reasonable time resources for  $m = 12, 14, 16$  (stars), and beyond. XEB on patch and elided supremacy circuits was done at  $m = 14, 16, 18$ , and 20.

# Avancées sur le problème de simulation de la puce SYCAMORE

- Réfutation d'IBM: théorique.
- Récemment [Pan,Zhang 21]:

	# bitstrings	Time complexity	Space complexity	Computational time	Computational hardware
Google [1]	$10^6$	—	—	10,000 years	Summit supercomputer
Cotengra [12]	1	$3.10 \times 10^{22}$	$2^{27}$	3,088 years	One NVIDIA Quadro P2000
Alibaba [18]	64	$6.66 \times 10^{18}$	$2^{29}$	267 days	One V100 GPU
Ours	<b>2097152</b>	$4.51 \times 10^{18}$	$2^{30}$	149 Days	One A100 GPU

TABLE II. Comparison of computational cost among different methods on Sycamore circuit with 53 qubits and 20 cycles.

- On sait maintenant reproduire en quelques jours les résultats obtenus par SYCAMORE.
  - On sait même faire de meilleures simulations (avec précision = 74%)
  - Mais ça prend quand même plus de temps.



- La revendication de suprématie quantique est fausse.
- Néanmoins, est-ce le plus important?

Some skeptics have warned that a quantum computer may not be possible [64? ], for example due to the fragility of quantum information at large qubit number and exponentially large Hilbert space. The demonstration here of quantum behavior at  $10^{16}$  Hilbert space is strong confirmation that nothing unusual or unexpected happens to our current understanding of quantum mechanics at this scale.

- Quelle sera la technologie utilisée pour la prochaine étape?

Merci de votre attention