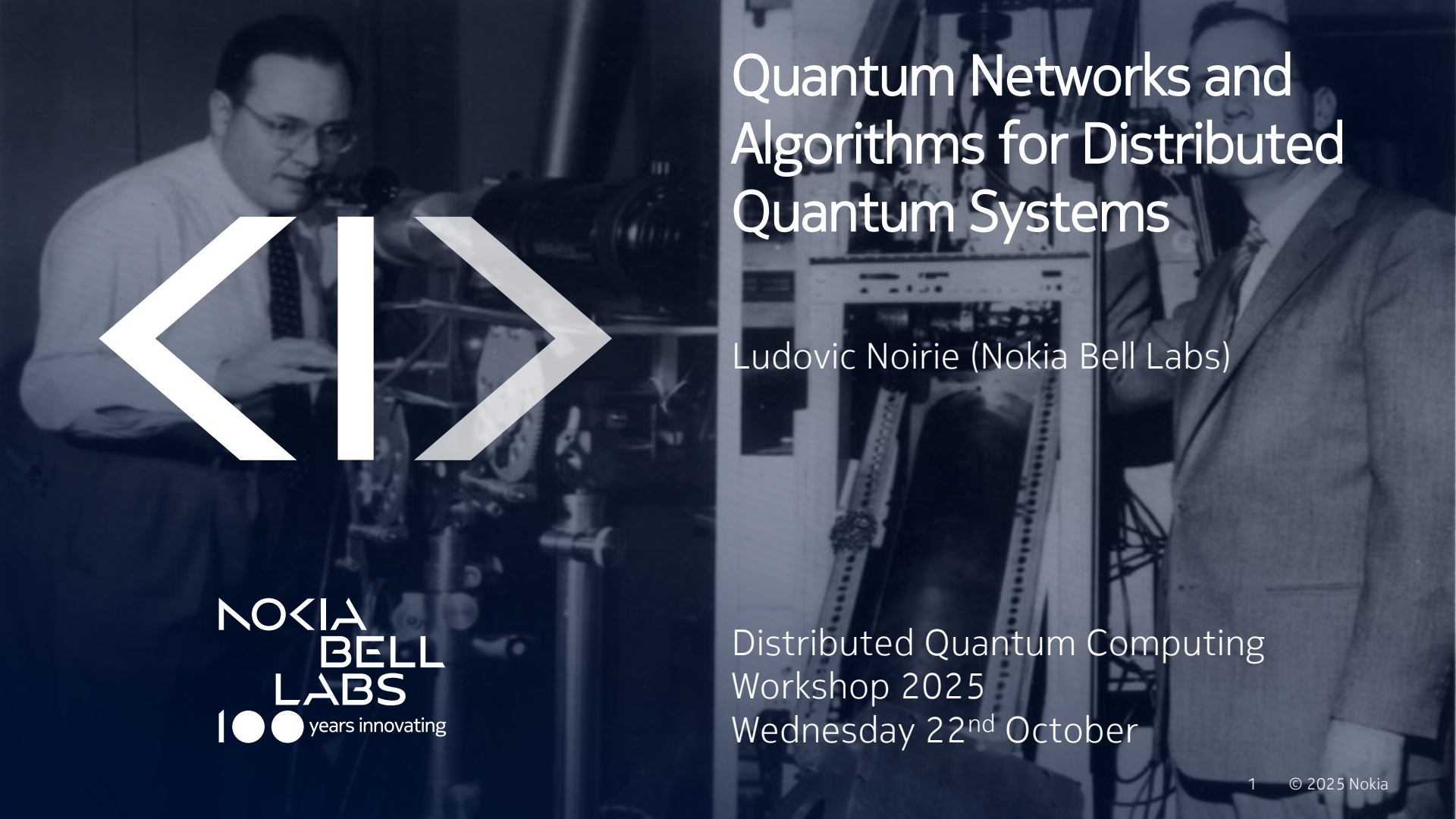


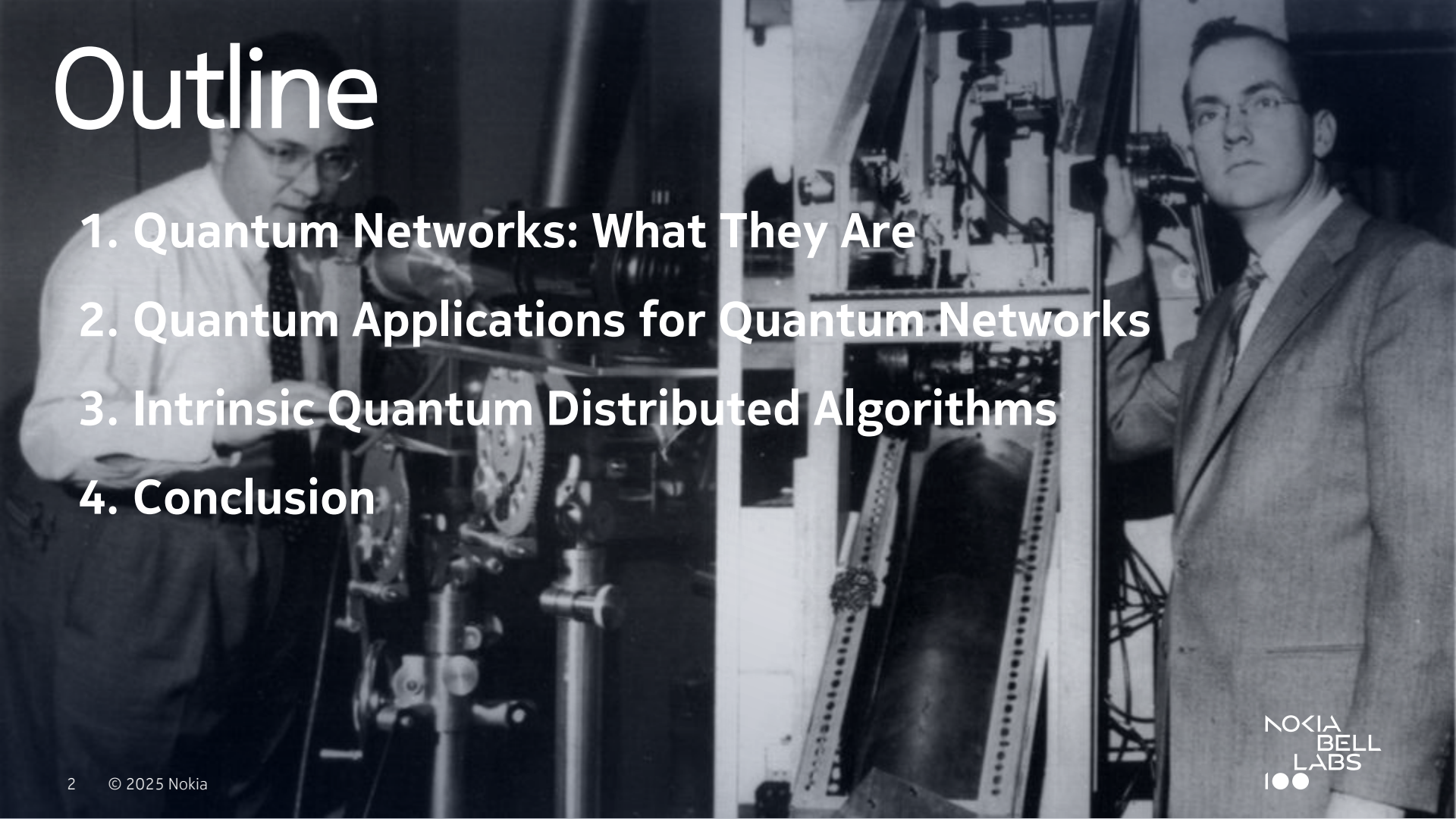
Quantum Networks and Algorithms for Distributed Quantum Systems

Ludovic Noirie (Nokia Bell Labs)

Distributed Quantum Computing Workshop 2025
Wednesday 22nd October

Outline

1. Quantum Networks: What They Are
2. Quantum Applications for Quantum Networks
3. Intrinsic Quantum Distributed Algorithms
4. Conclusion



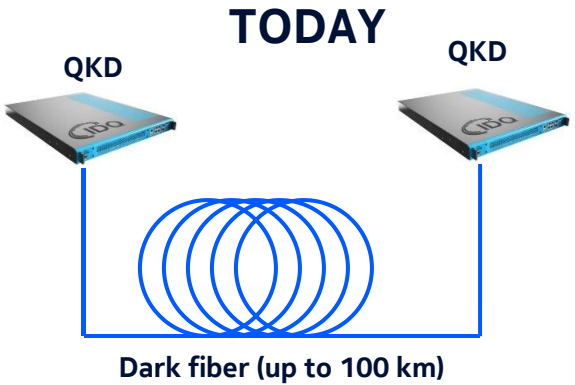
NOKIA BELL LABS 100

Outline

1. Quantum Networks: What They Are
2. Quantum Applications for Quantum Networks
3. Intrinsic Quantum Distributed Algorithms
4. Conclusion

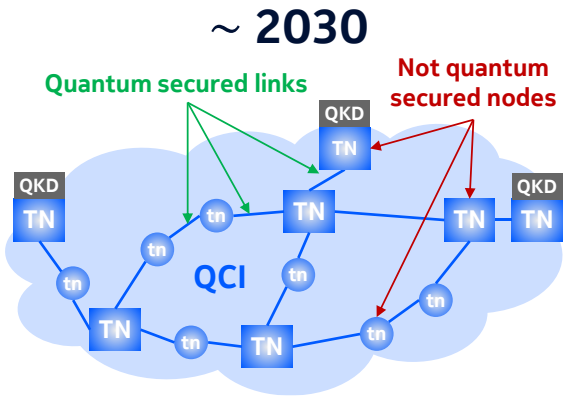
1. Quantum Networks: What They Are

Motivation: From Commercially-Available QKD Towards the Future Quantum Networks



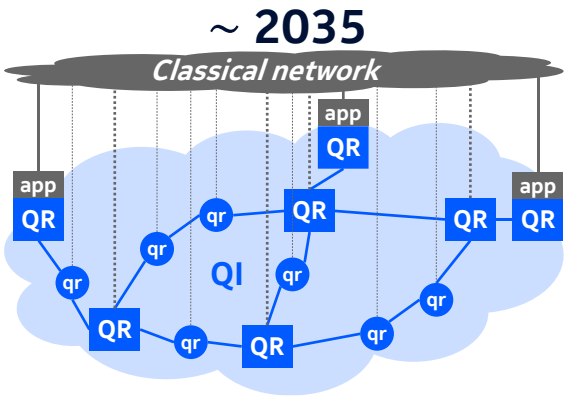
Quantum Key Distribution (QKD) systems on dark fibers

- Creation of shared secrete keys which are proven to be secured thanks to quantum physics laws
- Commercially available, e.g., IDQ
- Limitation in distance (typ. ~100 km for fiber and ~1000 km by satellites) and rate (typ. few kbit/s key rate)



Quantum Comm. Infrastructure (QCI) with trusted nodes (TN)

- 1st step to increase QKD distance
- Tested in field trials, see EuroQCI
- No limit in distance, but it requires to trust the intermediate nodes (security weak points)
- Only for QKD application



Quantum Internet (QI) with quantum repeaters/routers (QR)

- Best solution to increase QKD distance
- No limit in distance, no need to trust the nodes nor the entire network
- Any quantum application: QKD, distributed quantum computing, etc.
- Technology not yet mature, but first proofs of concepts

See L. Noirie, "From Existing Quantum Key Distribution Systems towards Future Quantum Networks," ICCAS 2024

1. Quantum Networks: What They Are

Quantum Networks = Distributed Systems That Distributes Entanglement

Source: Quantum Internet Research Group (QIRG@IRTF)

- RFC9340: *Architectural Principles for a Quantum Internet*, by Wojciech Kozlowski, Stephanie Wehner, Rodney Van Meter, Bruno Rijsman, Angela Sara Cacciapuoti, Marcello Caleffi and Shota Nagayama.
- "Quantum networks are distributed systems of quantum devices that utilize fundamental quantum mechanical phenomena such as superposition, entanglement, and quantum measurement to achieve capabilities beyond what is possible with non-quantum (classical) networks [Kimble08]."

  ⇒ Qubit transmission between nodes of a network.
- "The observation that we only need to be able to distribute Bell pairs relies on the fact that this enables the distribution of any other arbitrary entangled state. This can be achieved via quantum state teleportation."

  ⇒ **Quantum networks = Distributed systems that create entangled pairs of qubits (Bell pairs) between any pair of nodes in a network.**
- Quantum applications consume Bell pairs: quantum key distribution (QKD), distributed quantum computing, quantum sensing networks, etc.
- Quantum networks will not replace classical networks! They will need classical networks!

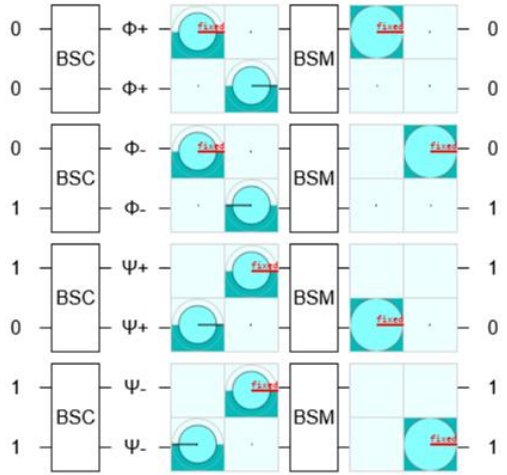
[Kimble08] Kimble, H.J., "The quantum internet," Nature Vol. 453, Iss. 7198, pp. 1023-1030, DOI 10.1038/nature07127, June 2008

NOKIA BELL LABS

1. Quantum Networks: What They Are

Entanglement = Bell States

BSC: Bell State Creation
BSM: Bell State Measurement

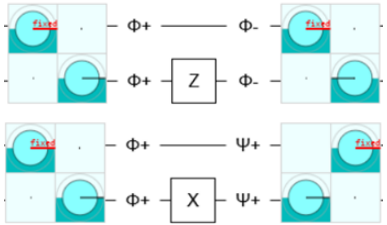


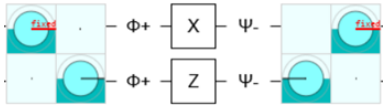
The 4 Bell states vs. computational basis: Quirk circuit

- Unitary operators: $BSC = (CNOT) \times (H \otimes Id) \Rightarrow BSM = (H \otimes Id) \times (CNOT) = BSC^{-1}$.
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = BSC|00\rangle \Rightarrow BSM|\Phi^+\rangle = |00\rangle$.
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = BSC|01\rangle \Rightarrow BSM|\Phi^-\rangle = |01\rangle$.
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = BSC|10\rangle \Rightarrow BSM|\Psi^+\rangle = |10\rangle$.
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = BSC|11\rangle \Rightarrow BSM|\Psi^-\rangle = |11\rangle$.

Pauli corrections for Bell state conversion: Quirk circuit

- Use of Pauli gates $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i \cdot Z \times X$.
- $(Z \otimes Id) \times BSC|b_1 b_0\rangle = (Id \otimes Z) \times BSC|b_1 b_0\rangle = |b_1 \overline{b_0}\rangle$.
- $(X \otimes Id) \times BSC|b_1 b_0\rangle = (Id \otimes X) \times BSC|b_1 b_0\rangle = |\overline{b_1} b_0\rangle$.





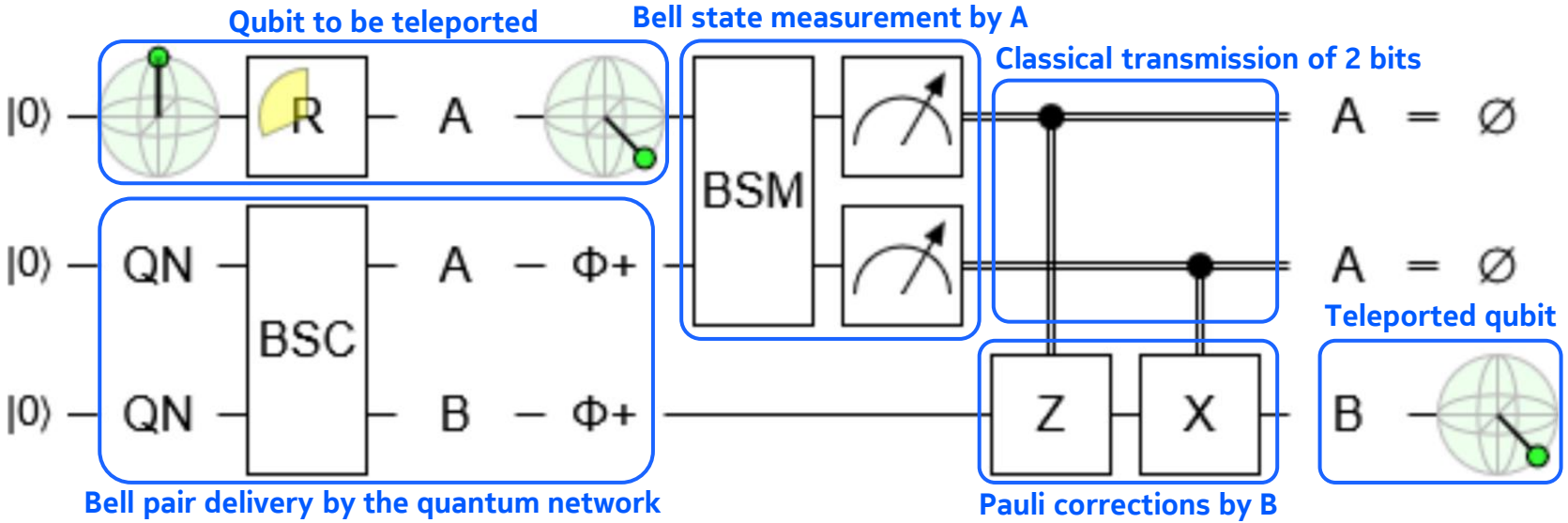
1. Quantum Networks: What They Are

Quantum Teleportation

Quantum teleportation mechanism [Bennet93]: Quirk circuit

- Use of a Bell pair to teleport a qubit state.

$$BSC = (CNOT) \times (H \otimes Id)$$
$$\Rightarrow BSM = (H \otimes Id) \times (CNOT) = BSC^{-1}$$



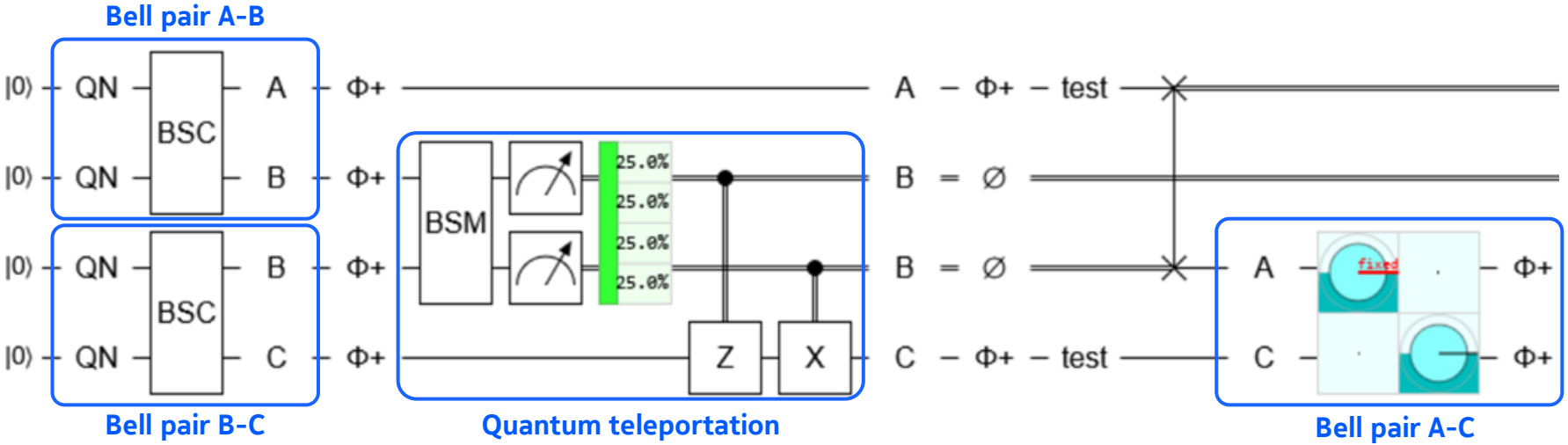
[Bennett93] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W.K., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical Review Letters Vol. 70, Iss. 13, pp. 1895-1899, DOI 10.1103/PhysRevLett.70.1895, March 1993

1. Quantum Networks: What They Are

Quantum Repeaters: Entanglement Swapping = Entanglement Teleportation 1/3

Entanglement swapping: Quirk circuit

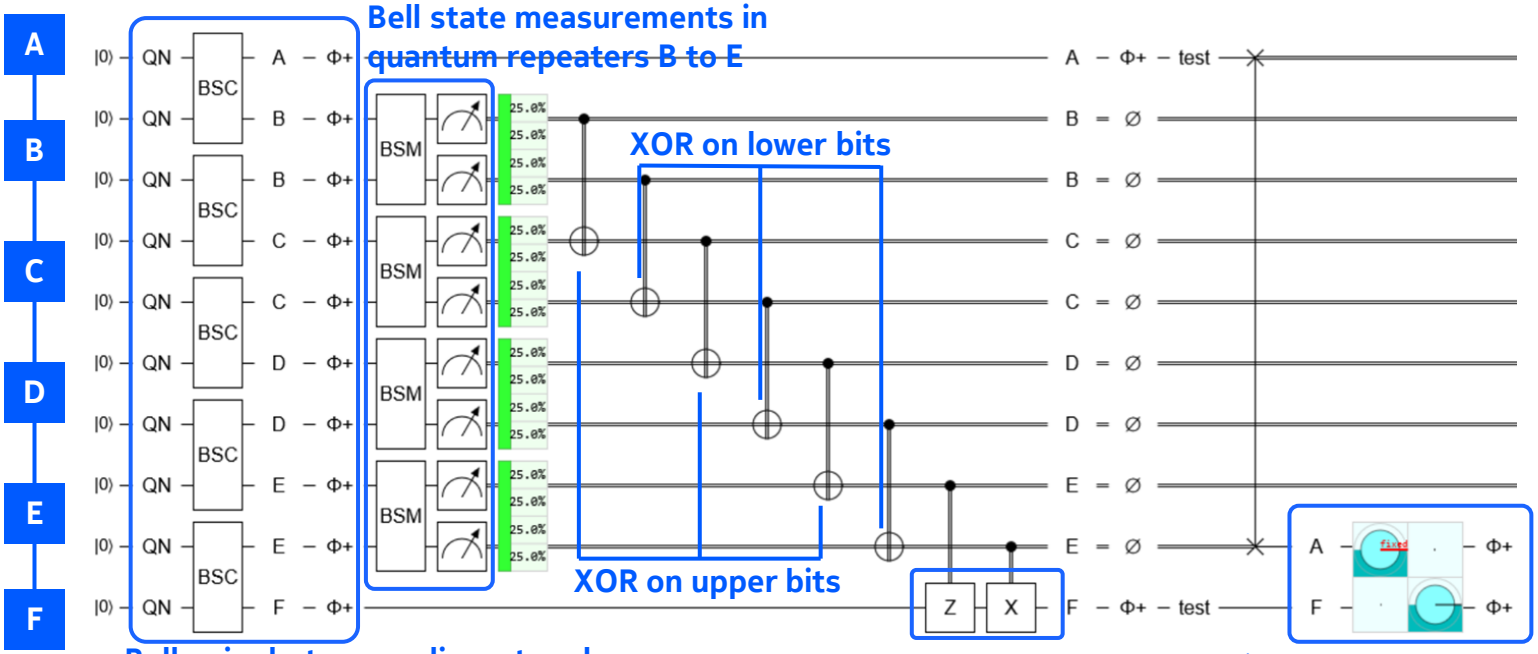
- Quantum teleportation of a qubit belonging to another Bell pair.



1. Quantum Networks: What They Are

Quantum Repeaters: Entanglement Swapping = Entanglement Teleportation

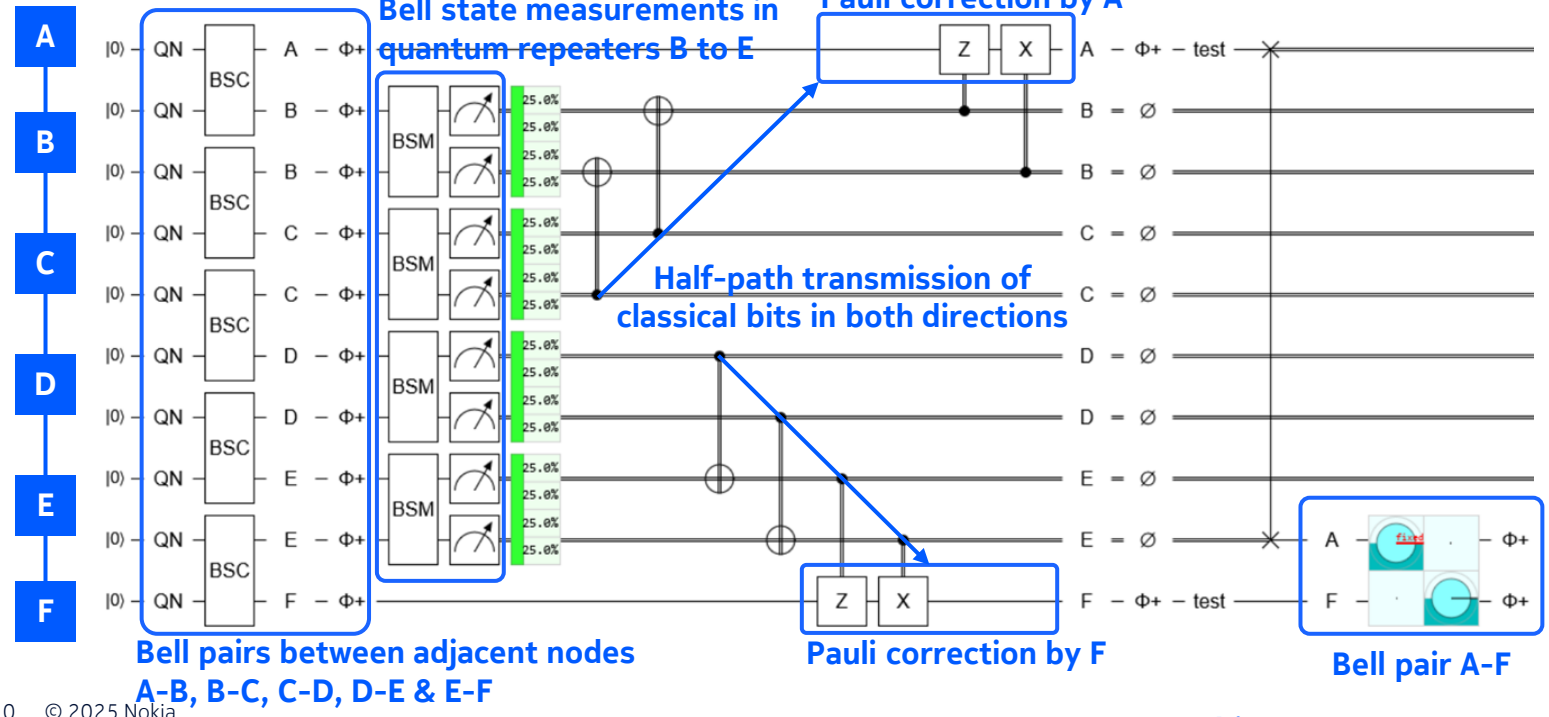
End-to-end Bell pair delivery: [quantum-gate-optimized Quirk circuit]



1. Quantum Networks: What They Are

Quantum Repeaters: Entanglement Swapping = Entanglement Teleportation

End-to-end Bell pair delivery: [time-optimized Quirk circuit]

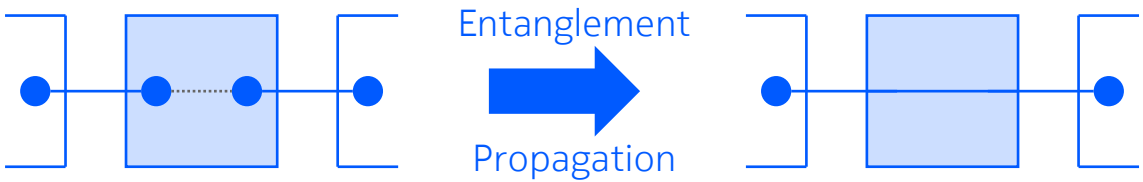


1. Quantum Networks: What They Are

Quantum Routers: Entanglement Routing

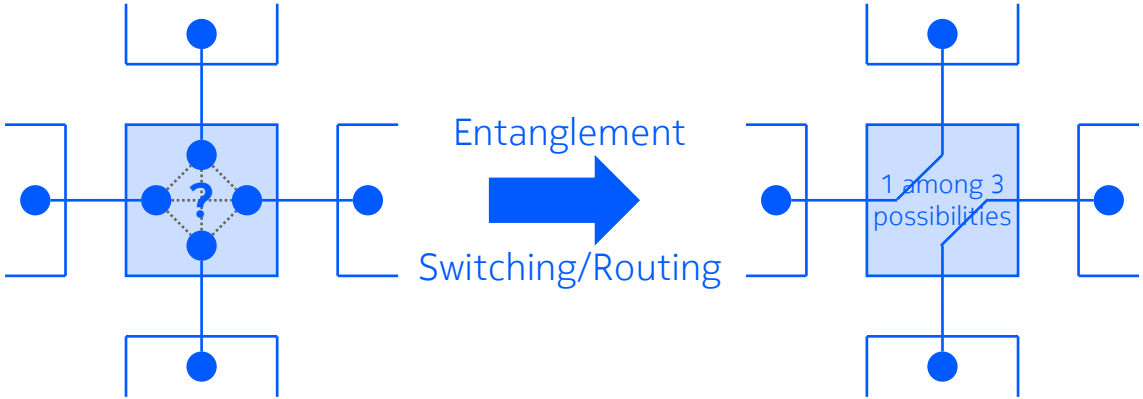
Quantum repeater: $degree = 2$

- No choice on the links to entangle.



Quantum router: $degree \geq 3$

- Choice on the links to entangle.



1. Quantum Networks: What They Are

Technological Challenges ⇒ Very Long-Term Research

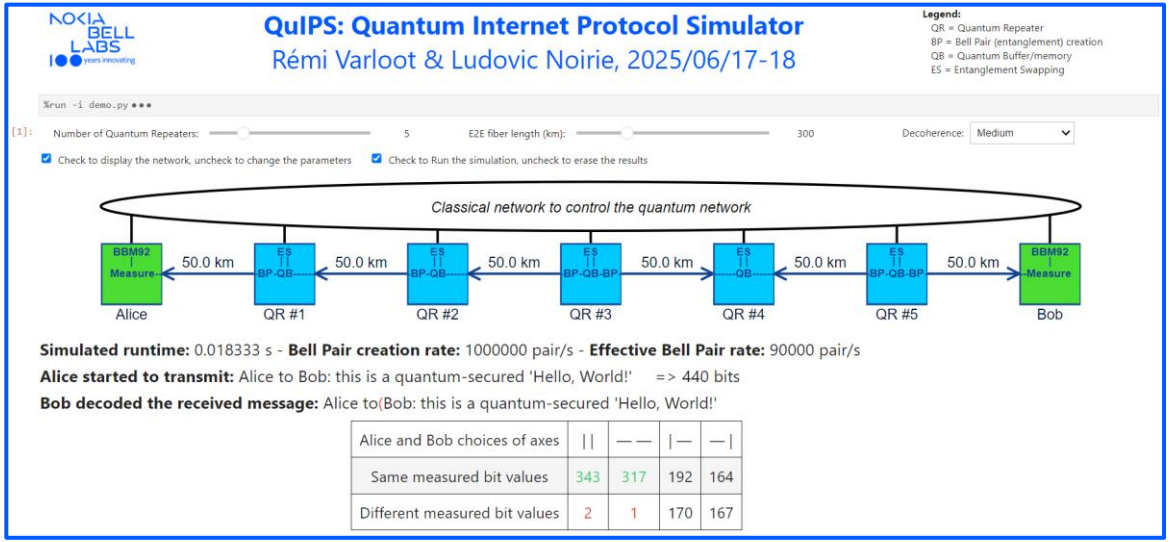
Hardware challenges: the technology is not yet mature

- Quantum memories, photon-to matter and matter-to-photon qubit transduction, entanglement swapping.

Software challenges: control & management of quantum networks

Our research in Nokia Bell Labs (in NSSR lab): control & management

- Quantum network protocol stack.
- Quantum network simulations: QuIPS.
- Bell pair fidelity: Bell state purification & quantum error correction.
- Quantum applications.
  About QKD: Globecom 2023, Noirie & Varloot, “Authentication Through Error Estimation in QKD”.
- Distributed quantum systems.
  2 CIFRE theses with Marc-Olivier Renou (Inria).
- Hardware: technology watch only.



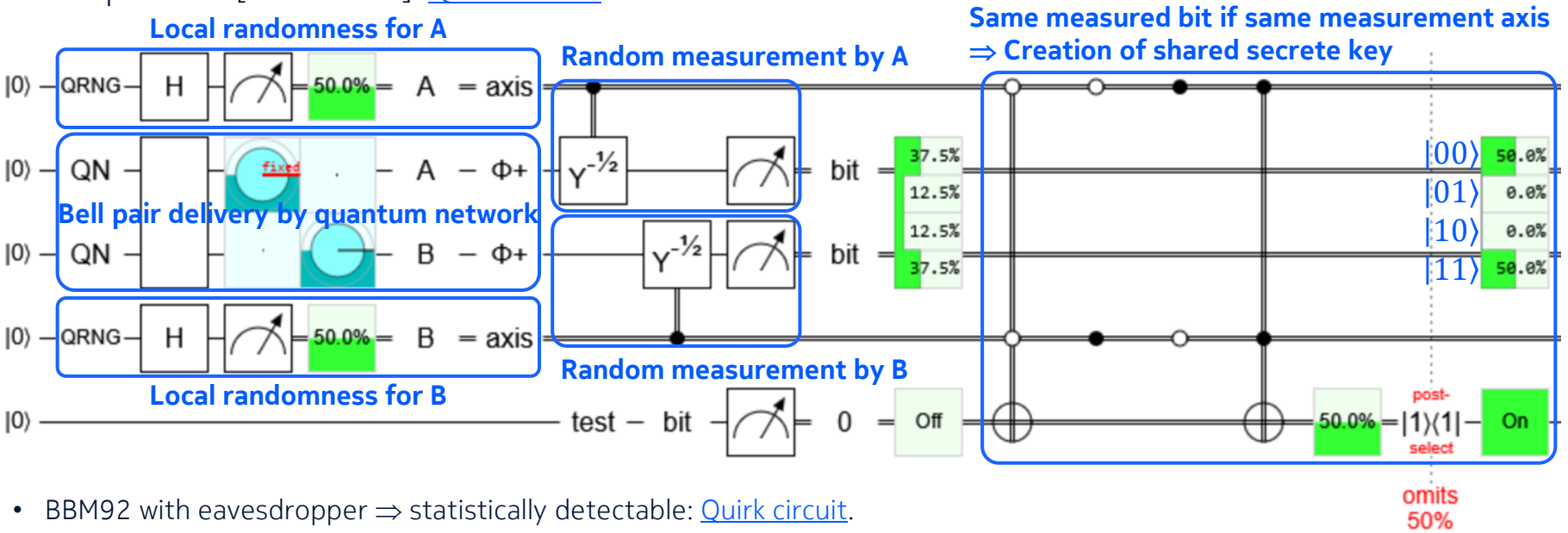
Outline

1. Quantum Networks: What They Are
2. Quantum Applications for Quantum Networks
3. Intrinsic Quantum Distributed Algorithms
4. Conclusion

2. Quantum Applications for Quantum Networks

Quantum Key Distribution (QKD)

BBM92 protocol [Bennett92]: Quirk circuit



- BBM92 with eavesdropper ⇒ statistically detectable: Quirk circuit.
- Other QKD protocols: Notebook §7.2.

[Bennett92] Bennett, C.H., Brassard, G, and Mermin N.D., "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. 68:557-559 (1992), DOI 10.1103/PhysRevLett.68.557.

NOKIA BELL LABS

2. Quantum Applications for Quantum Networks

Distributed Quantum Computing

Different use cases for distributed quantum computing

- Split quantum algorithms in small pieces to run them in different quantum computers.
  - In same datacenter, to increase the capacity of current quantum computing units interconnecting many of them.
  - Between datacenters?
- Delegated quantum computing = Quantum input sent to a remote quantum computers (~ quantum cloud).
- Blind (quantum) computing = Secured delegated quantum computing.

Distributed quantum computing primitives

- Quantum state transmission using quantum teleportation of many qubits.
- Distributed (non-local) quantum gates to run them with qubits on different locations.

2. Quantum Applications for Quantum Networks

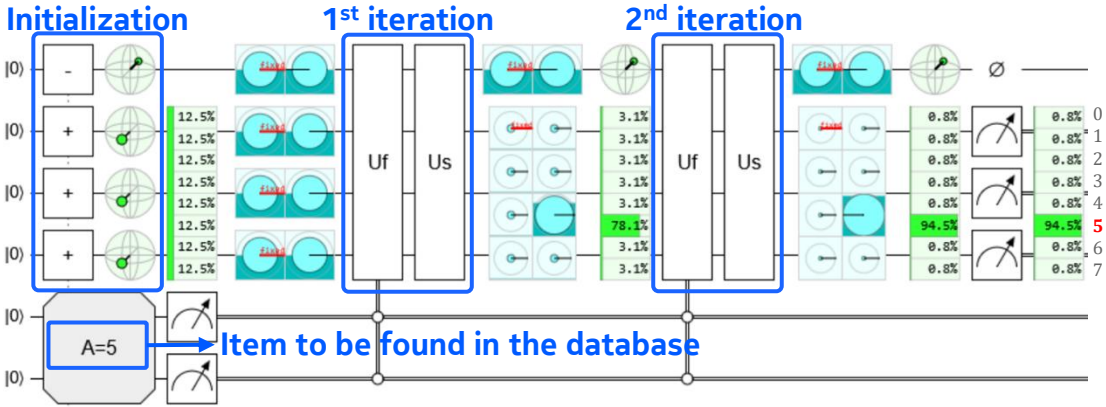
Distributed Quantum Computing – Toy Example: Grover's Search Algorithm 1/2

Grover's quantum search algorithm [Grover96]: Quirk circuit

- Find unknown item m among 2^N.
  - Here: $m = 5$, $2^N = 2^3 = 8$.
- Oracle gate U_f: $f(n) = \delta_{m,n}$.
  - $n \neq m \Rightarrow U_f|n, b\rangle = |n, b\rangle$.
  - $n = m \Rightarrow U_f|m, b\rangle = |m, \bar{b}\rangle$.

auxiliary qubit b

- Grover diffusion operator $U_G = 2|s\rangle\langle s| - I$. with $|s\rangle = \frac{1}{\sqrt{2^N}} \sum_{n=0}^{2^N-1} |n\rangle = |+\rangle^{\otimes N}$.
- Initialization with $|+\rangle^{\otimes N} \otimes |-\rangle$.



- Iterate r times with product of operators $U_s \times U_f$ with realizing U_G with auxiliary qubit.
- Classical search: on average $r = 2^N/2$ tries (iterations).
- Quantum search: $r \approx \frac{\pi}{4}\sqrt{2^N}$ iterations with probability $p_n \to 1$ when $N \to +\infty \Rightarrow$ **Quadratic speedup**.
- For details, see notebook §7.3.

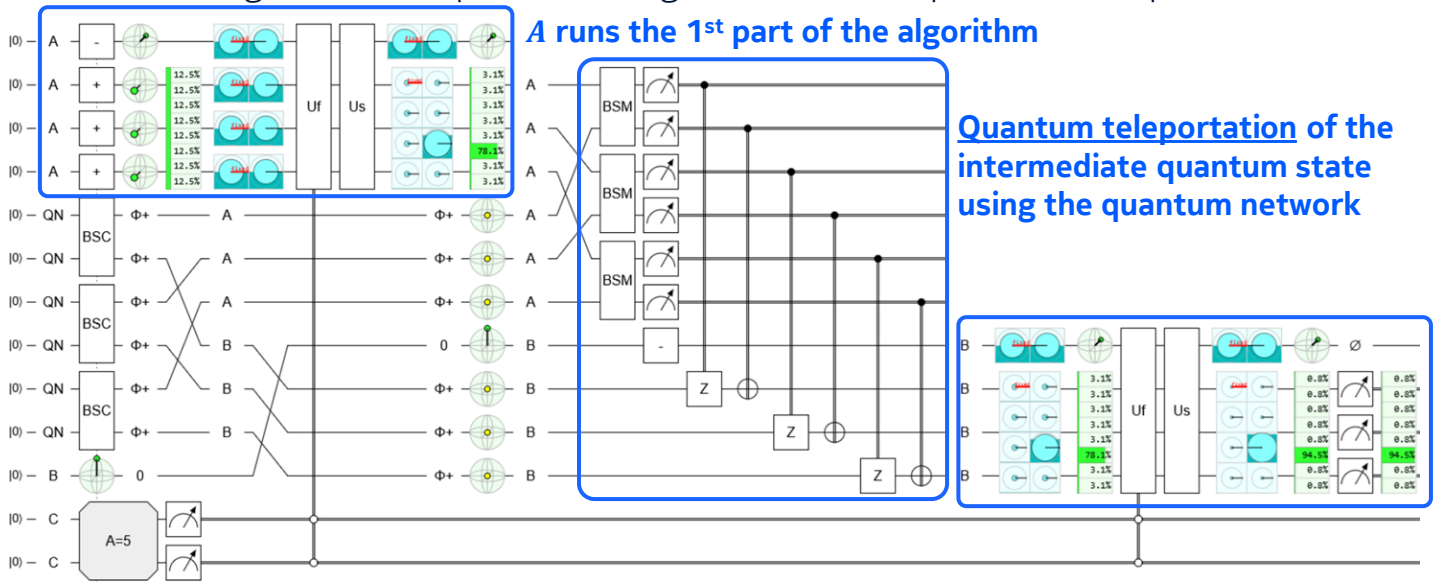
[Grover96] Grover, L. K., "A fast quantum mechanical algorithm for database search," STOC '96, pp. 212–219, arXiv, July 1996

NOKIA BELL LABS

2. Quantum Applications for Quantum Networks

Distributed Quantum Computing – Toy Example: Grover's Search Algorithm 2/2

Split of Grover's algorithm in 2 parts running in 2 different quantum computers A and B: Quirk circuit



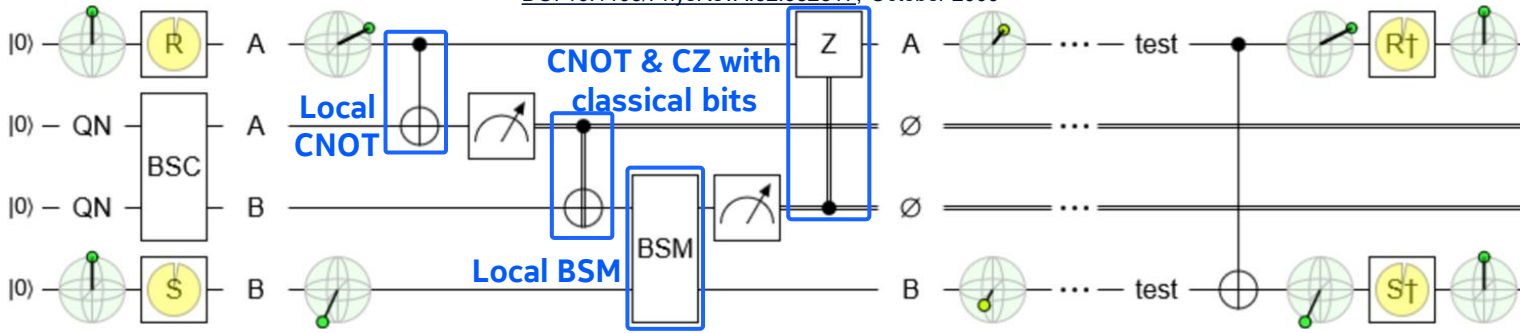
- Intermediate output quantum state cannot be measured before quantum teleportation: Quirk circuit.
- Classical networks cannot be used instead of quantum networks: Quirk circuit.

2. Quantum Applications for Quantum Networks

Distributed Quantum Gates

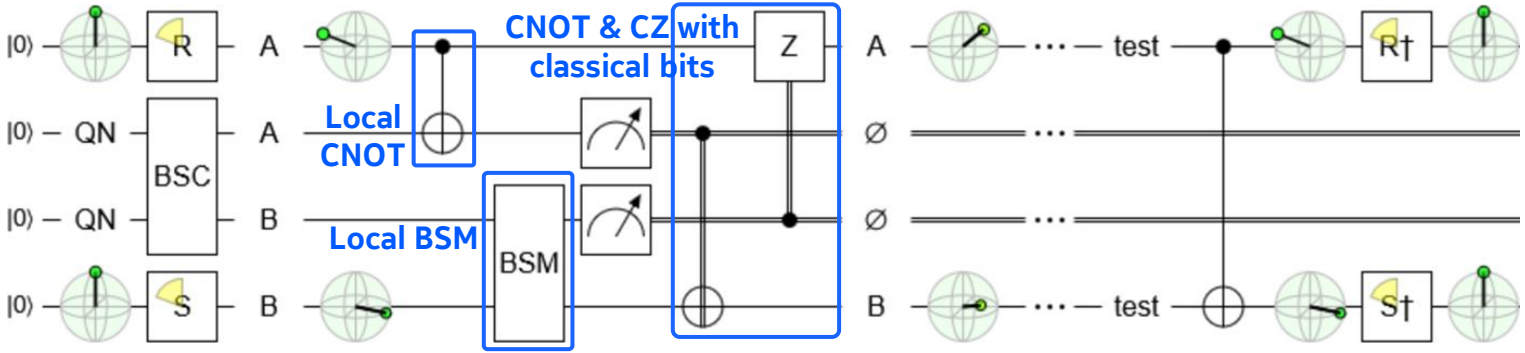
Distributed CNOT: Quirk circuit 1

J. Eisert et al., "Optimal local implementation of nonlocal quantum gates," Physical Review A, vol. 62, 052317, DOI 10.1103/PhysRevA.62.052317, October 2000



Alternative circuit for distributed CNOT: Quirk circuit 2

D. Cuomo et al., "Towards a distributed quantum computing ecosystem," IET Quantum Communication, vol. 1, no. 1, pp. 3-8, 2020, DOI 10.1049/iet-qtc.2020.0002



2. Quantum Applications for Quantum Networks

Some Other Quantum Applications

Shared randomness

- Use of GHZ_N states to create a shared coin (see next section).

Quantum Byzantine agreement (quantum consensus)

- Objective: agreement between N agents when K of them are malicious.
- Quantum vs. classical Byzantine agreement:
  - Same limitations in acceptable ratio of malicious nodes: $\mathrm{K/N} < 1/3$.
  - Less rounds: $O(N)$ (Classical deterministic) vs. $O\left(\sqrt{N/\log N}\right)$ (Classical probabilistic) vs. $O(1)$ (Quantum).

See Luis Muñecas Tomás presentation during this workshop on Byzantine agreement variants and open problems

Network of distributed quantum sensors

- Quantum sensors: accelerometer, gravimeter, magnetometer, etc.
- Example: quantum interconnection of several telescopes for higher accuracy.

D. Gottesman et al., "Longer-Baseline Telescopes Using Quantum Repeaters," Physical Review Letters, vol. 109, 070503, DOI 10.1103/PhysRevLett.109.070503, August 2012

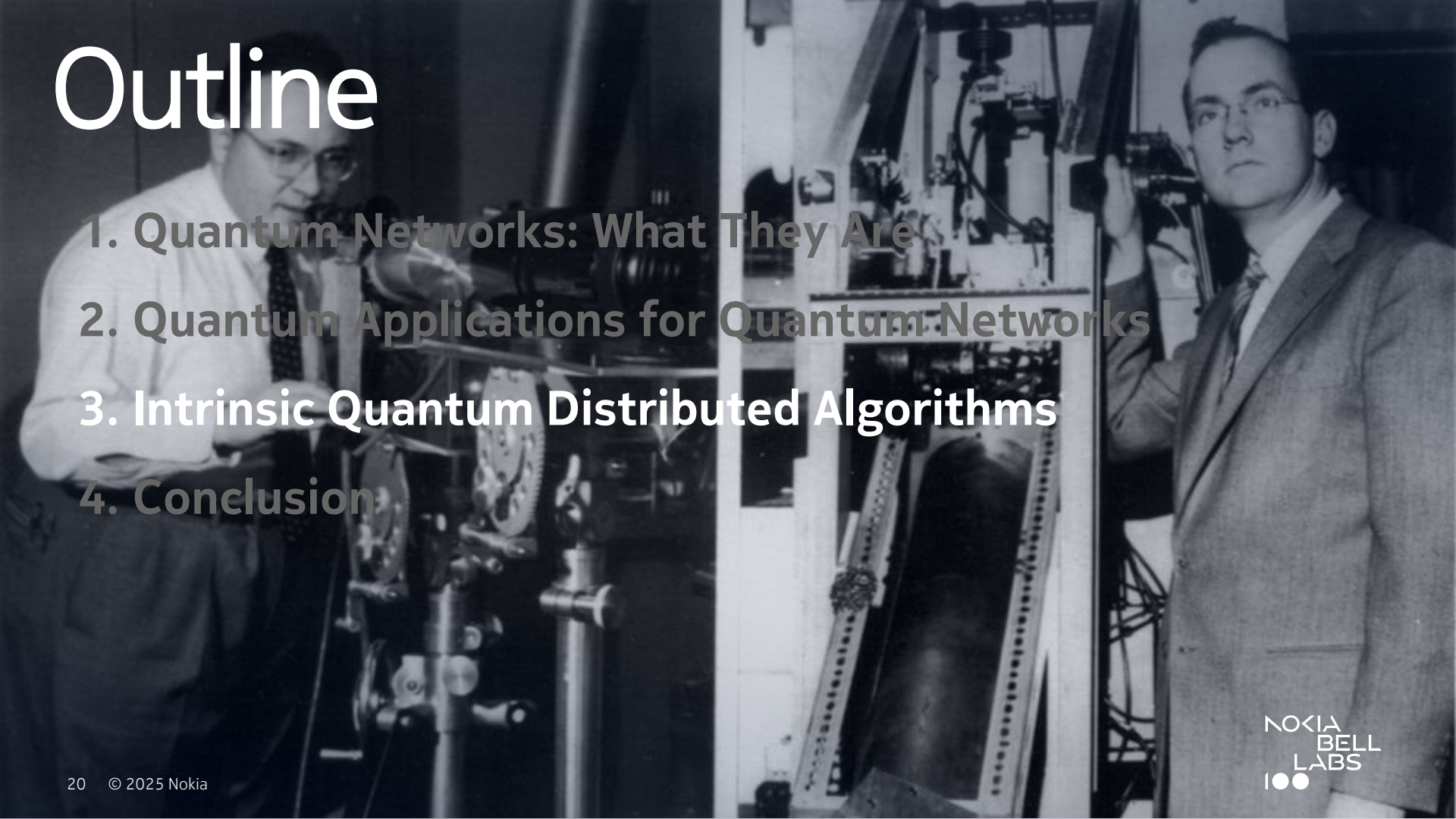
Quantum physics experiments

- Example: Proving that complex numbers are required in quantum physics…

M.-O. Renou et al., "Quantum theory based on real numbers can be experimentally falsified," Nature, vol. 600, pp. 625–629, DOI 10.1038/s41586-021-04160-4, December 2021
Z.-D. Li et al., "Testing Real Quantum Theory in an Optical Quantum Network," Phys. Rev. Lett., vol. 128, 040402 , DOI 10.1103/PhysRevLett.128.040402, January 2022

Outline

1. Quantum Networks: What They Are
2. Quantum Applications for Quantum Networks
3. **Intrinsic Quantum Distributed Algorithms**
4. Conclusion



3. Intrinsic Quantum Distributed Algorithms

Generic Quantum Distributed Algorithm

Universal set of quantum gates [Barenco95]

- "A set of gates that consists of all one-bit quantum gates ($U(2)$) and the two-bit exclusive-or gate (that maps Boolean values (x, y) to $(x, x \oplus y)$) is universal in the sense that all unitary operations on arbitrarily many bits n ($U(2^n)$) can be expressed as compositions of these gates."
- Any unitary operator on n qubits can be decomposed into 1-qubit gates and CNOT gates.

⇒ Any quantum algorithm can be distributed on multiple quantum computers

- On each quantum computer: 1-qubit gates and local CNOT gates (and any other local unitary operator).
- Between quantum computers, thanks to entanglement distribution by a quantum network:
  - Quantum teleportation of qubit states using Bell pairs and transmission of classical bits.
  - Distributed CNOT gates using Bell pairs and transmission of classical bits.

⇒ Optimal split of quantum algorithms, minimizing the number of distributed CNOT gates?

- Intra-datacenter: Interesting problem when quantum computers are limited in size.
- Inter-datacenters: When is it useful to split quantum algorithms in different datacenters?

[Barenco95] A. Barenco et al., "Elementary gates for quantum computation," Phys. Rev. A 52, 3457, DOI 10.1103/PhysRevA.52.3457, November 1995

NOKIA BELL LABS

3. Intrinsic Quantum Distributed Algorithms

Genuine Quantum Distributed Algorithms

Distributed quantum algorithms that intrinsically requires to run on different locations.

Some applications require to process qubits locally:

- Quantum key distribution…
- Quantum Byzantine agreement.
- Etc.

Use of entangled quantum states split over N nodes:

- GHZ_N states.
- Graph states framework, see Wikipedia page.
  - Equivalence concept with local unitary operations…
  - Luis Muñecas Tomás internship “Entanglement Routing for Quantum Networking” within Nokia Bell Labs in 2024.
- Other multi-qubit states with various entanglement types.

3. Intrinsic Quantum Distributed Algorithms

Bipartite and Multipartite Quantum States

Bipartite states

- 2 entangled qubits.
- Only 1 class: Bell state like.

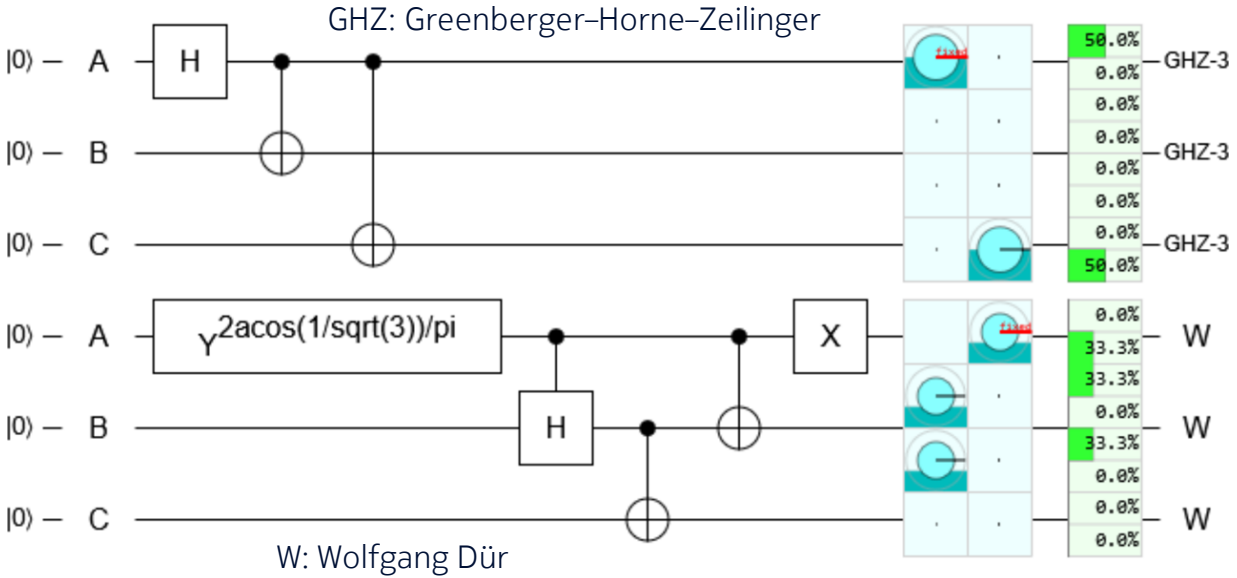
Tripartite states

- 3 entangled qubits.
- 2 classes:
  - $|GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$,
  - $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.
- Quirk circuit.

Multipartite states

- Generalization to N qubits.
- More classes for larger N…

2 non-biseparable classes of three-qubit states

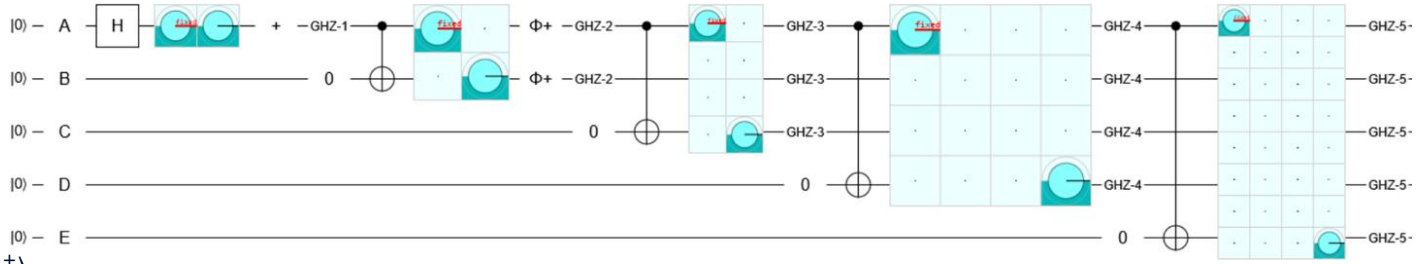


3. Intrinsic Quantum Distributed Algorithms

GHZ-N States as an Example of Multipartite Quantum States

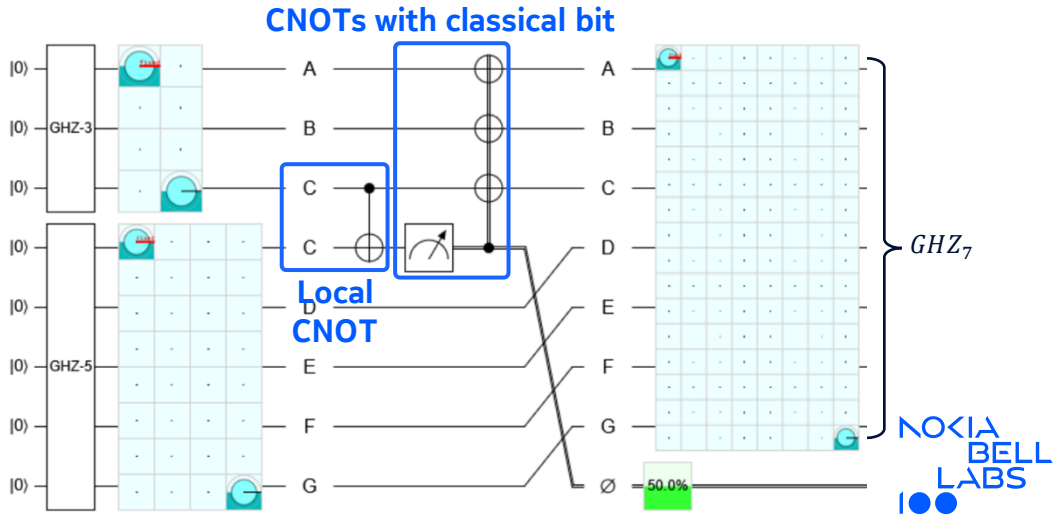
GHZ_N states :

- Quirk circuit.
- $|GHZ_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.
- $|GHZ_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$.
- $|GHZ_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$.
- $|GHZ_{N+1}\rangle = \text{CNOT}_{k,N}|0\rangle \otimes |GHZ_N\rangle, 0 \le k \le N-1$.



Quantum networks and GHZ_N states

- Merge circuit: Quirk circuit.
  - $GHZ_N + GHZ_M \to GHZ_{N+M-1}$.
  - Example: $GHZ_3 + GHZ_5 \to GHZ_7$.
- Tree circuit: Quirk circuit.
  - From Bell states to GHZ_N in $\log N$ steps.
  - $GHZ_2 \to GHZ_3 \to GHZ_5 \to GHZ_9 \to \cdots$



3. Intrinsic Quantum Distributed Algorithms

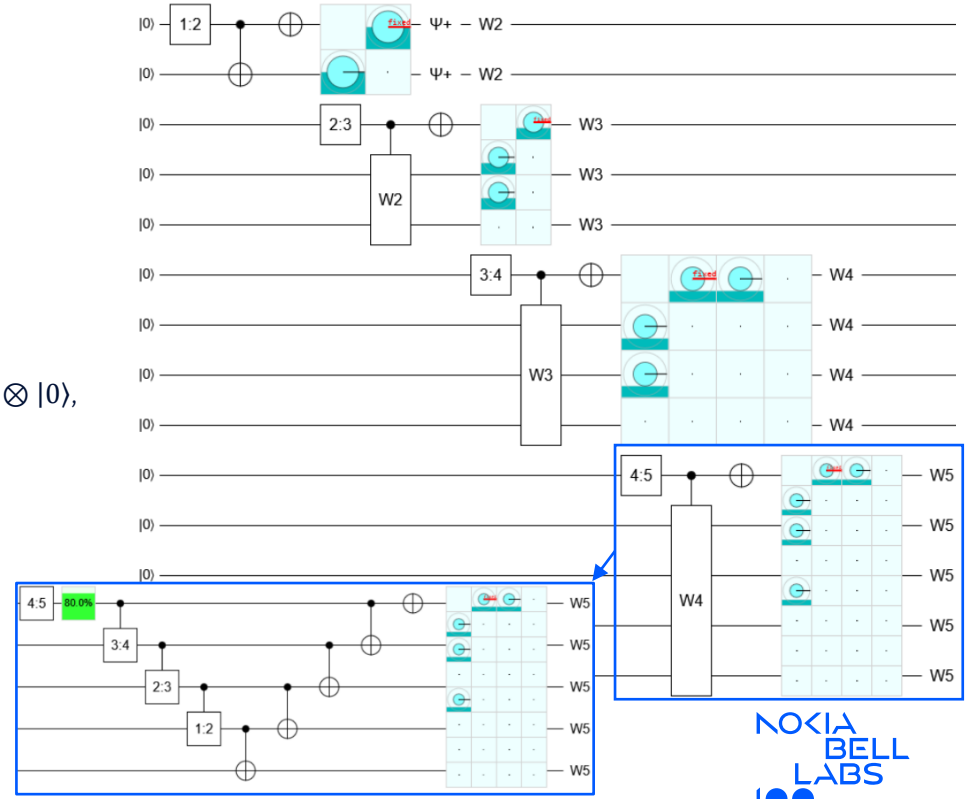
W-N States as an Example of Multipartite Quantum States

W_N states :

- Quirk circuit.
- $|W_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$.
- $|W_3\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.
- $|W_N\rangle = \frac{1}{\sqrt{N}}(|00\cdots01\rangle + |00\cdots10\rangle + \cdots + |01\cdots00\rangle + |10\cdots00\rangle)$
- More compact circuit:
  $|W_{N+1}\rangle = W_{0-N}|0\rangle^{\otimes(N+1)} = \mathrm{NOT}_0 \times \mathrm{C}{-}W_{0,1-N} \times (\mathrm{N}{-}1{:}\,\mathrm{N})_0 |W_N\rangle \otimes |0\rangle$,
  with $(\mathrm{N}{-}1{:}\,\mathrm{N})_0|0\rangle = \sqrt{\frac{N-1}{N}}\,|0\rangle + \sqrt{\frac{1}{N}}\,|1\rangle$

Quantum networks and W_N states

- CNOT gates can be teleported,
- C-U gates with $U \in U(2)$ can be made with 1 CNOT and other 1-qubit unitary operators before and after



Outline

1. Quantum Networks: What They Are
2. Quantum Applications for Quantum Networks
3. Intrinsic Quantum Distributed Algorithms
4. **Conclusion**

NOKIA BELL LABS 100

4. Conclusion

Summary

Quantum networks = Distributed system to create entangled pairs of qubits (Bell pairs) between any pair of nodes in a network

- Long term research (~10 years) ⇒ Future quantum networks.
- Challenges on hardware technologies and software (control & management) for these future quantum network.

Many quantum applications can run on the future quantum networks

- Quantum Key Distribution (QKD) systems (commercially available for point-to-point quantum communication).
- Distributed quantum computing (essentially for intra-datacenter interconnexion).
- Blind computing / Secured Delegated computing.
- Genuine quantum distributed algorithms: shared coin, Byzantine agreement and variants.
- Distributed quantum sensors.
- **Other?**

4. Conclusion

Nokia Bell Labs Interests in Distributed Quantum Algorithms

Quantum advantages for quantum networks?

- Extension of QKD distance without trusted nodes.
- Quantum Byzantine agreement: faster communication $O(1)$.
- Higher measurement accuracy for distributed sensors using entanglement.

Certification mechanisms for quantum networks?

- Use of self-testing techniques to ensure that nothing wrong happen between end users.
- Example: testing Bell pairs between two end users (e.g., useful for QKD).
- Certification of other entangled quantum states (e.g., GHZ_N)?

New quantum applications (distributed quantum algorithms) with new quantum advantages?

- Investigation of variants of Byzantine agreement with new quantum advantages?
- Shared coin with GHZ_N states?
- Other?

4. Conclusion

Quirk Tool

Quirk: a drag-and-drop quantum circuit simulator

- Web site for the on-line version: https://algassert.com/quirk.
- Free, open-source software: https://github.com/Strilanc/Quirk/.
- By Craig Gidney, "software engineer turned research scientist on the quantum computing team at Google".
  - Note: this is not an official Google product.

My usage of Quirk

- Quantum Circuits used in this presentation: https://www.ludovic-noirie.fr/QC/DQS.
- More information about how to use Quirk: see notebook.