Recursive linear optical networks for realizing quantum algorithms

Gelo Noel Tabia

APS March Meeting 2016 | 14-18 March 2016

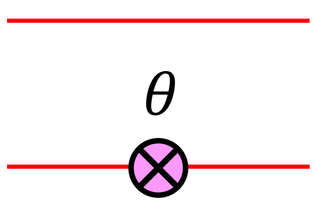
Motivation

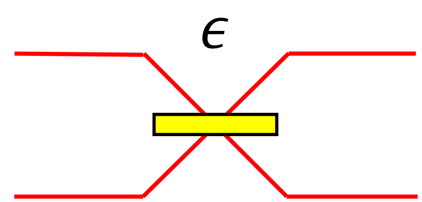
- Many practical quantum technolgies have been achieved with linear optics (LO).
- Progress in LO quantum computation with photonic integrated circuits (PIC)
- Goal: recipes for translating quantum algorithms into practical LO schemes

Linear optics (LO)

- Photons manipulated by a network of phase shifters and beam splitters

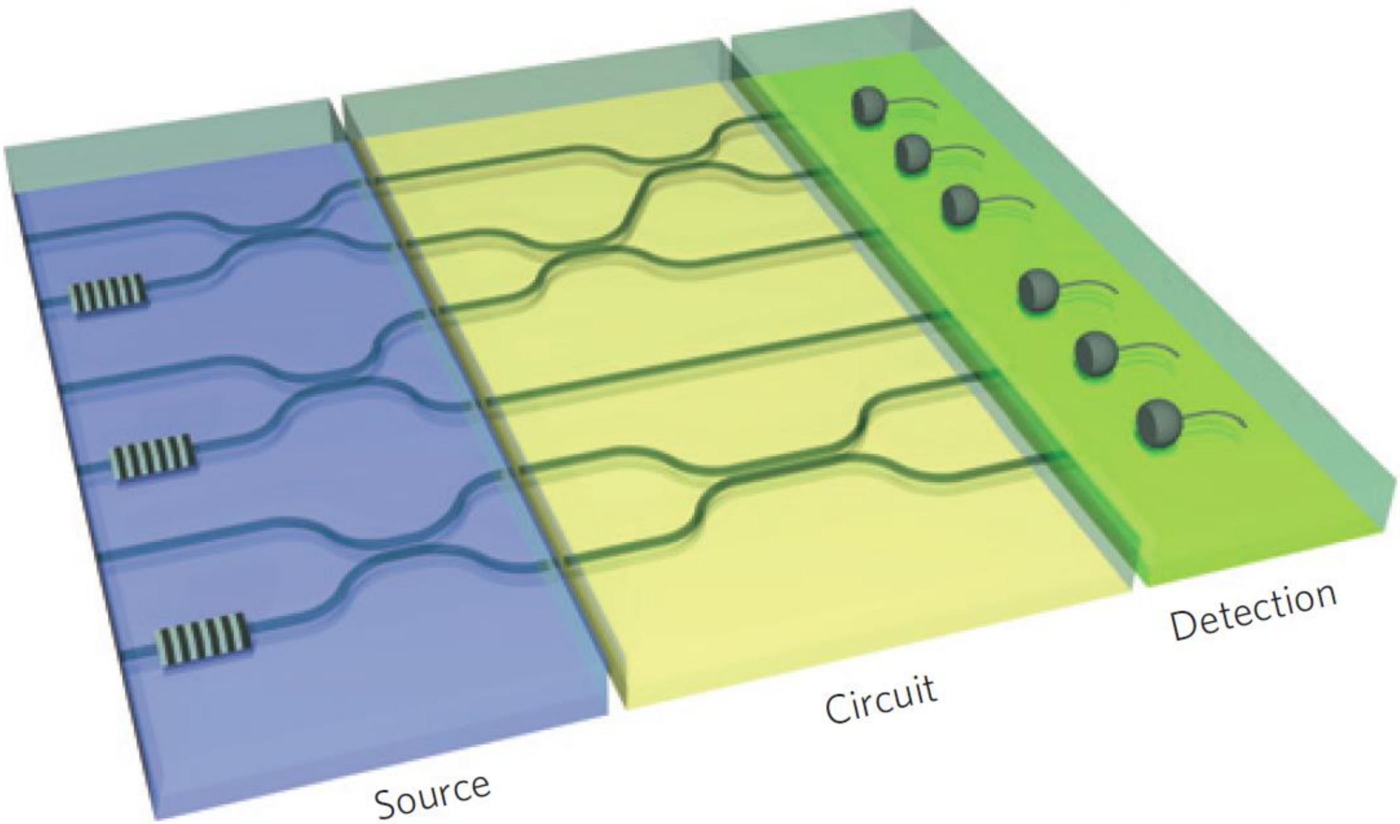
$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \qquad B_\epsilon = \begin{pmatrix} \sqrt{\epsilon} & \sqrt{1-\epsilon} \\ \sqrt{1-\epsilon} & -\sqrt{\epsilon} \end{pmatrix}$$





Photonic integrated circuit

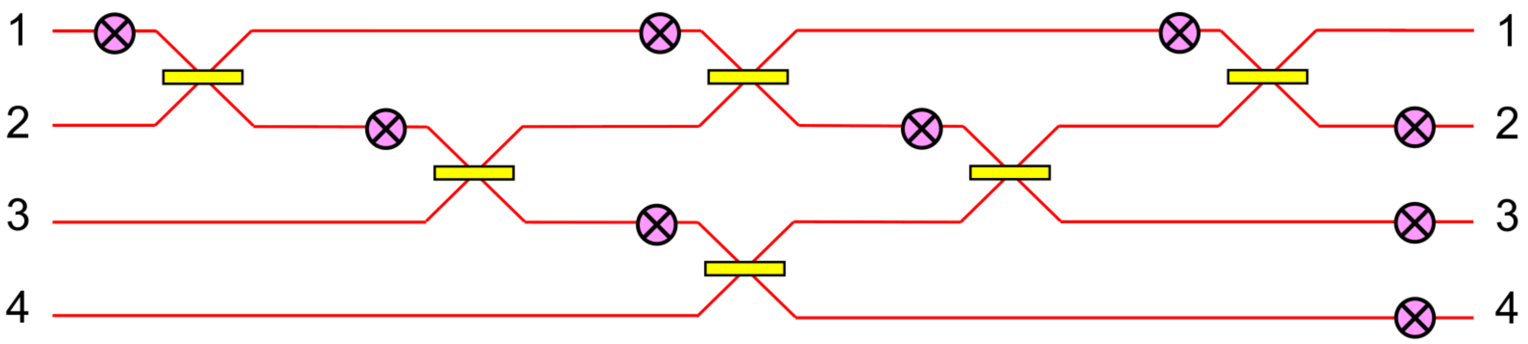
- Waveguide-based linear optics



Path-encoded qudits

Unitary gates

- Reck, et al. (1994)
- Any unitary $U \in SU(d)$ can be realized by a LO network on d modes using $d^2 - 1$ elements



Main results

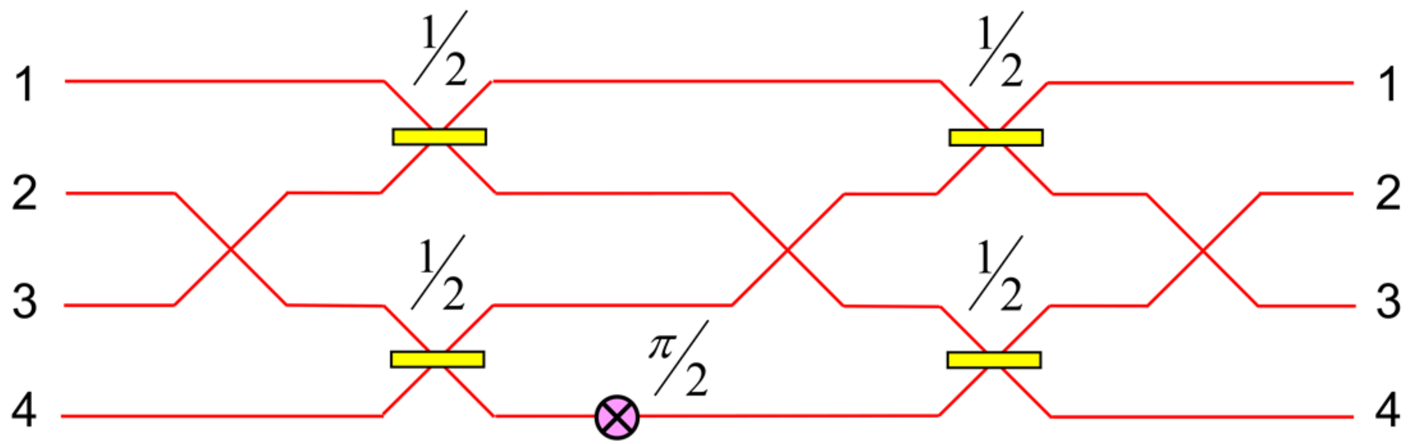
- Recursive LO networks for quantum Fourier transform (QFT) and Grover inversion
- Circuit for U_{2d} built using a pair of circuits for U_d
- Unitary matrix decomposition into (2×2)-block-diagonal matrices

[arXiv:1509.04246]

Quantum Fourier transform

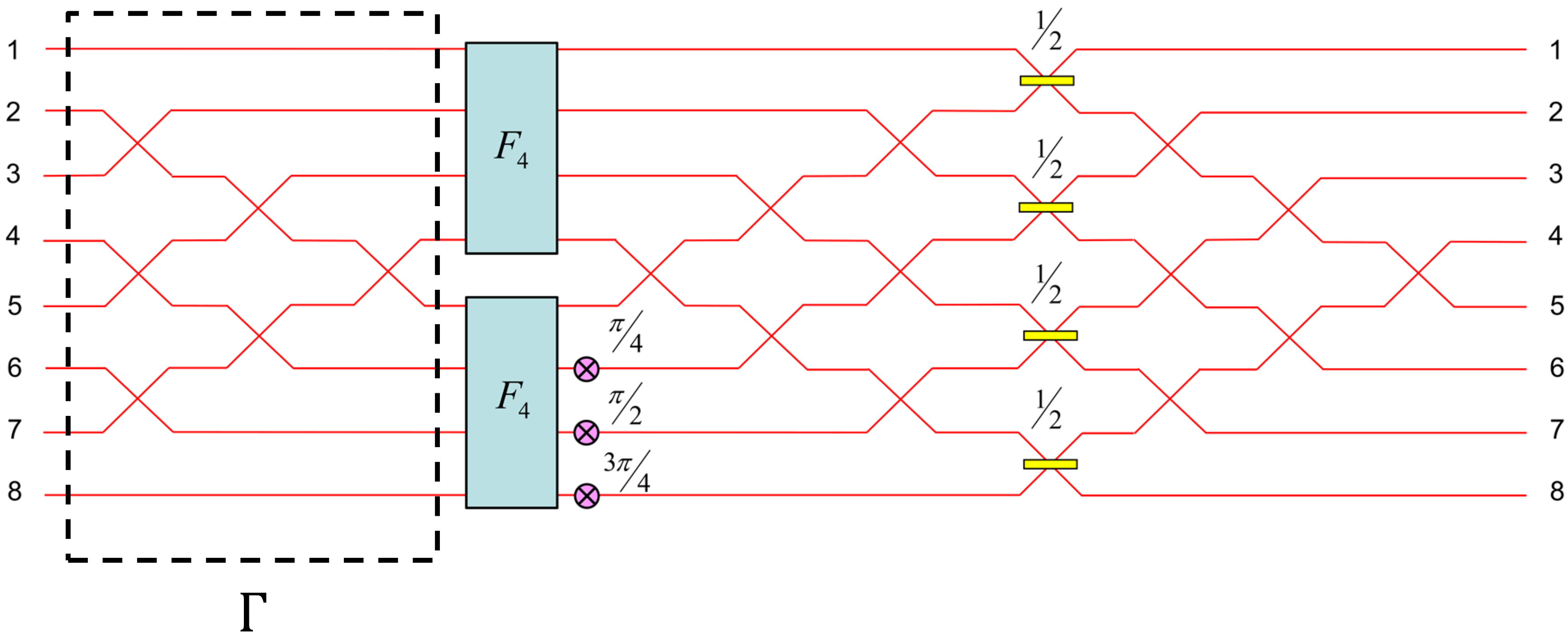
- Fourier transform on quantum states

$$F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$



Recursive QFT circuit

- e.g. QFT circuit F_8 given circuit for F_4



$$\Gamma: (1,2,3,4,5,6,7,8) \mapsto (1,3,5,7,2,4,6,8)$$

Fourier matrix factorization

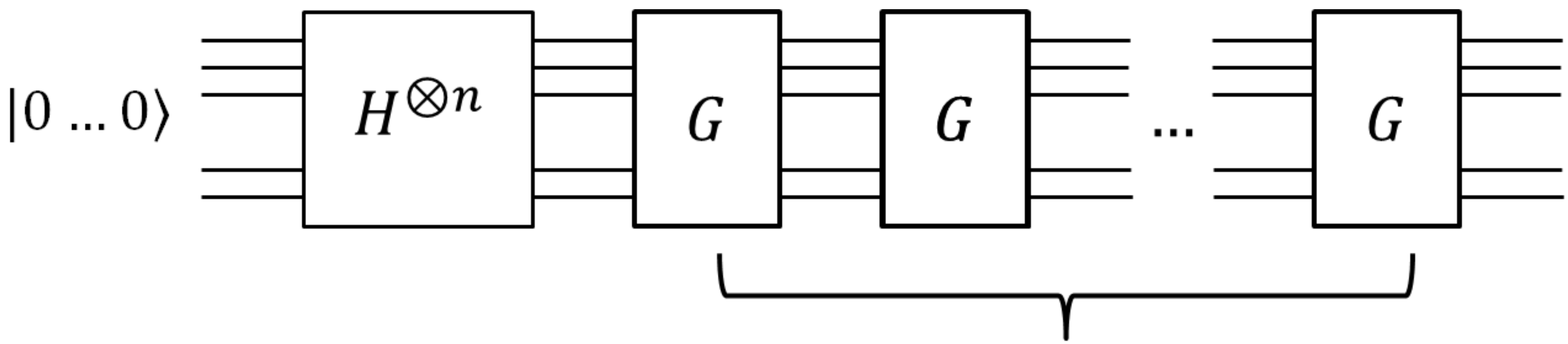
- First discovered by Gauss, this is the basis for fast Fourier transform (Cooley-Tukey algorithm):

$$F_{2d} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & D \\ D & I \end{pmatrix} \begin{pmatrix} F_d & 0 \\ 0 & F_d \end{pmatrix} \Gamma$$

$$D = \mathrm{diag}(1, \omega, \dots, \omega^{d-1})$$

$$\omega = e^{2\pi i/d}$$

Grover's algorithm



$\lfloor \pi\sqrt{n}/4 \rfloor$ times

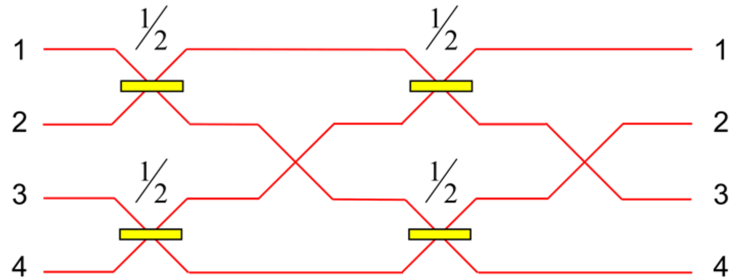
$$G = WU_f$$

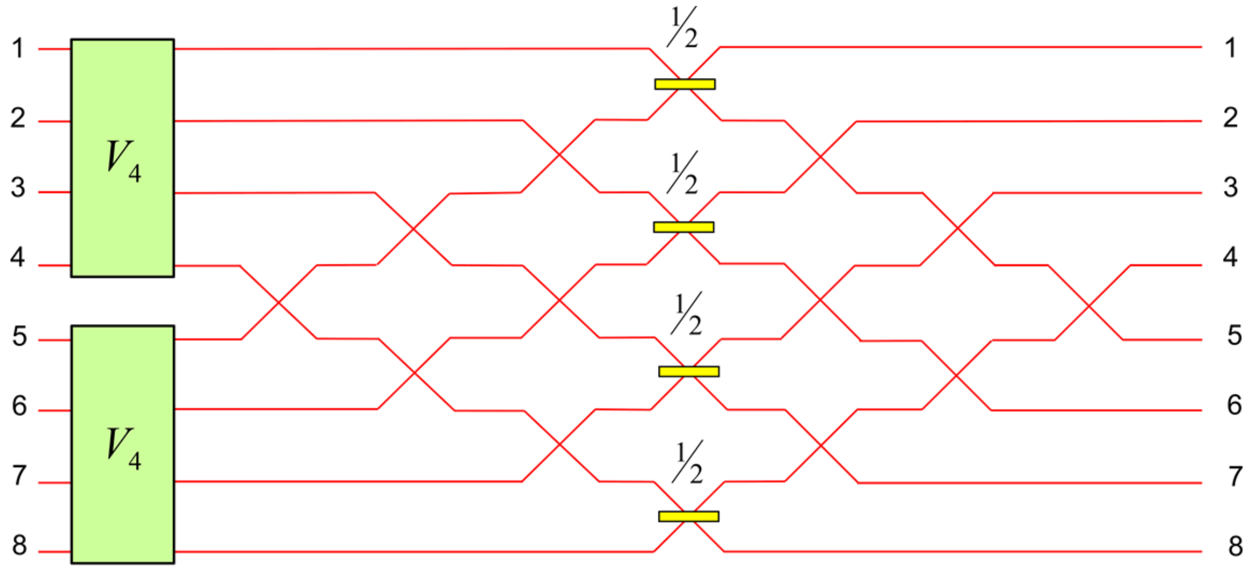
$$U_f\colon |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

- We construct a recursive LO circuit for Grover inversion W_d

Recursive V_d circuit

- Constructing V_8 from V_4

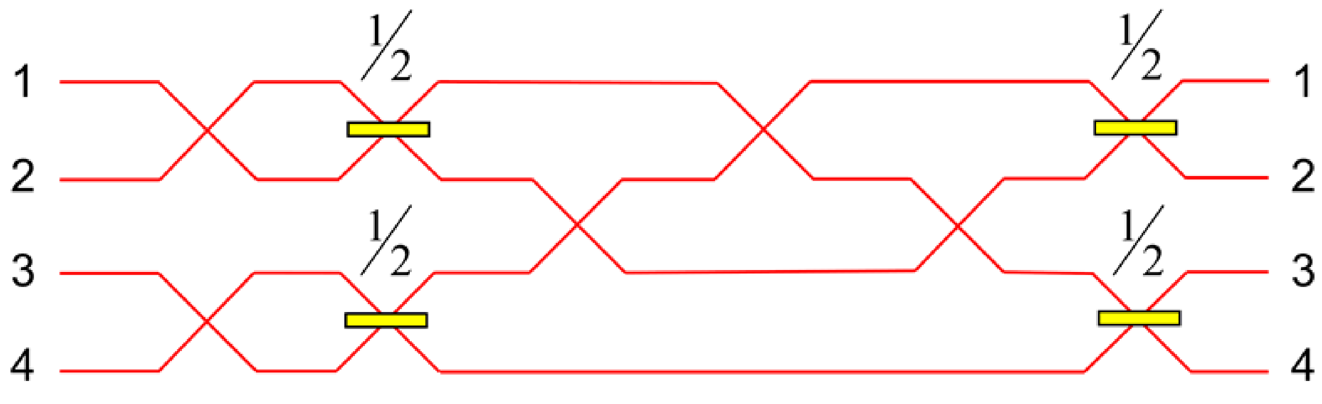




Recursive W_d circuit

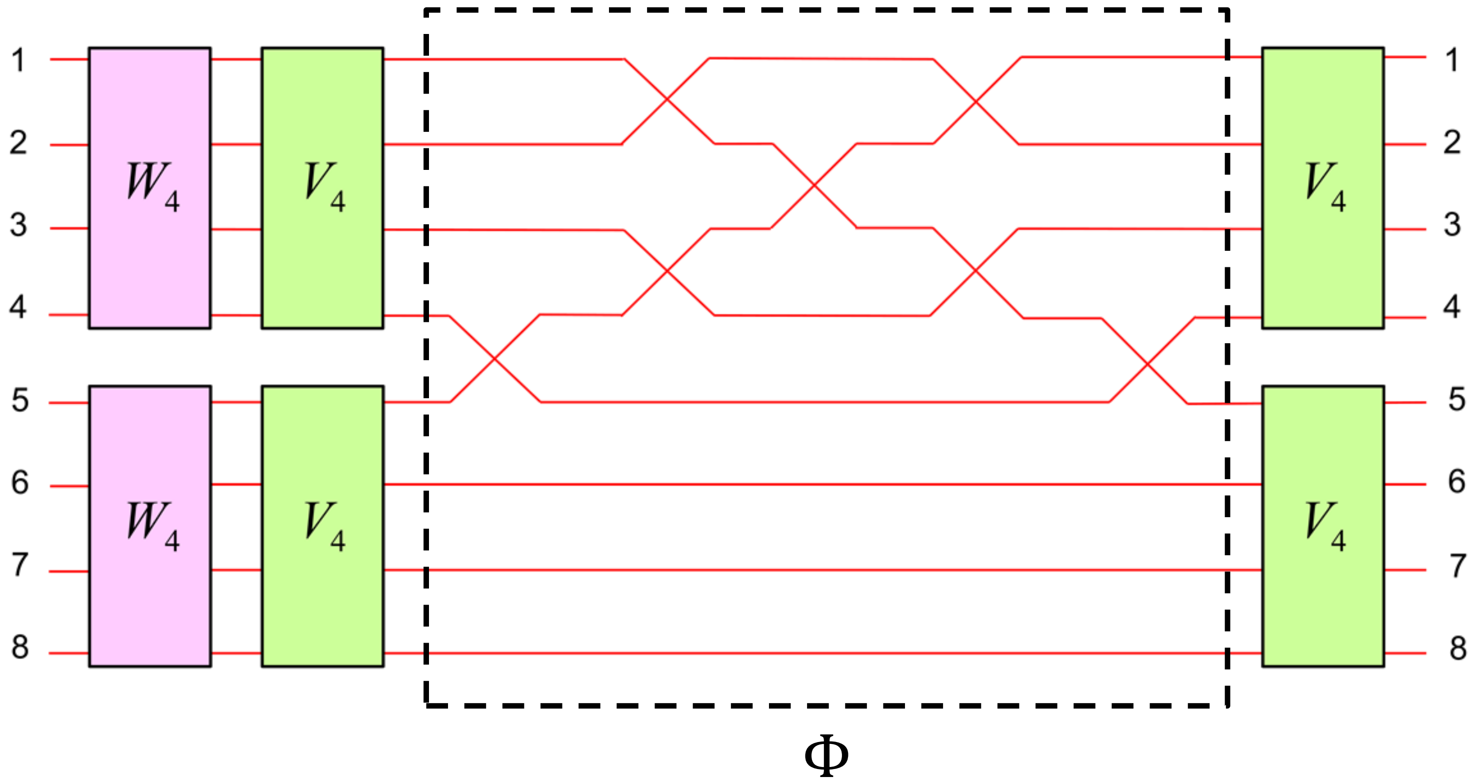
- Grover inversion W_4

$$W_4 = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$



Recursive W_d circuit

- W_8 given the circuit for W_4 and V_4



$\Phi: (1,2,3,4,5,6,7,8) \mapsto (5,2,3,4,1,6,7,8)$

W_d matrix decomposition

- Formally this corresponds to

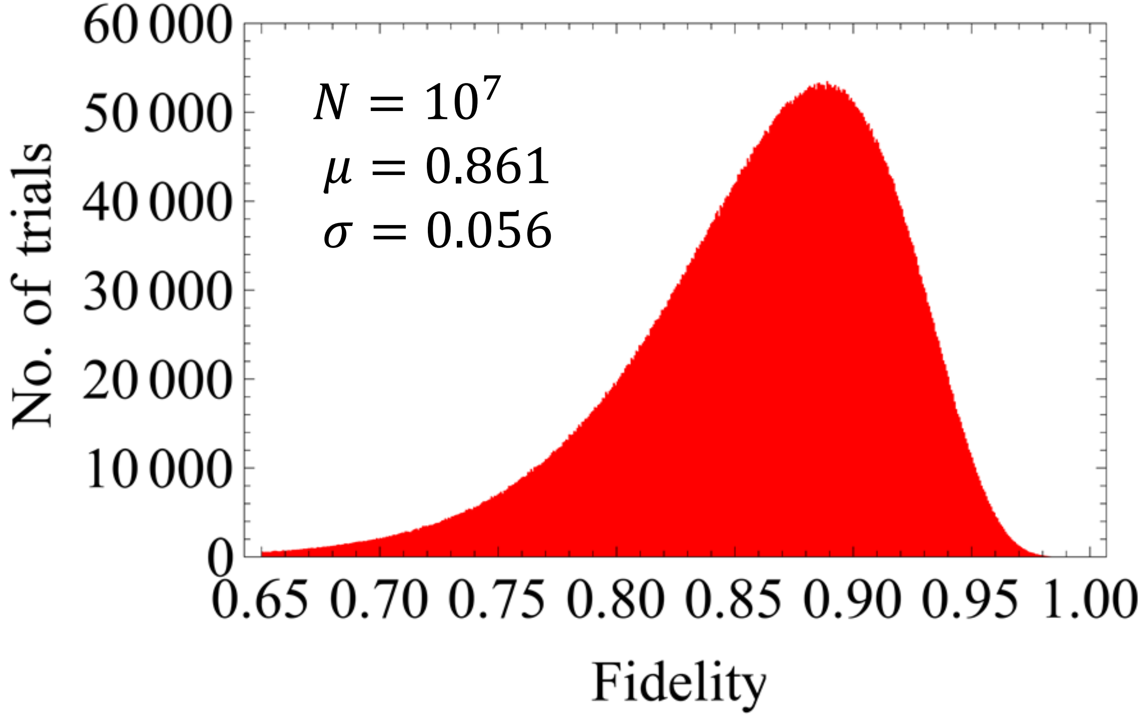
$$W_{2d} = \begin{pmatrix} V_d & 0 \\ 0 & V_d \end{pmatrix} \Phi \begin{pmatrix} V_d & 0 \\ 0 & V_d \end{pmatrix} \begin{pmatrix} W_d & 0 \\ 0 & W_d \end{pmatrix}$$

$$V_{2d} = H \otimes I_d \begin{pmatrix} V_d & 0 \\ 0 & V_d \end{pmatrix}$$

$$W_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad V_2 = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Simulation results

- Haar-uniform input states for QFT



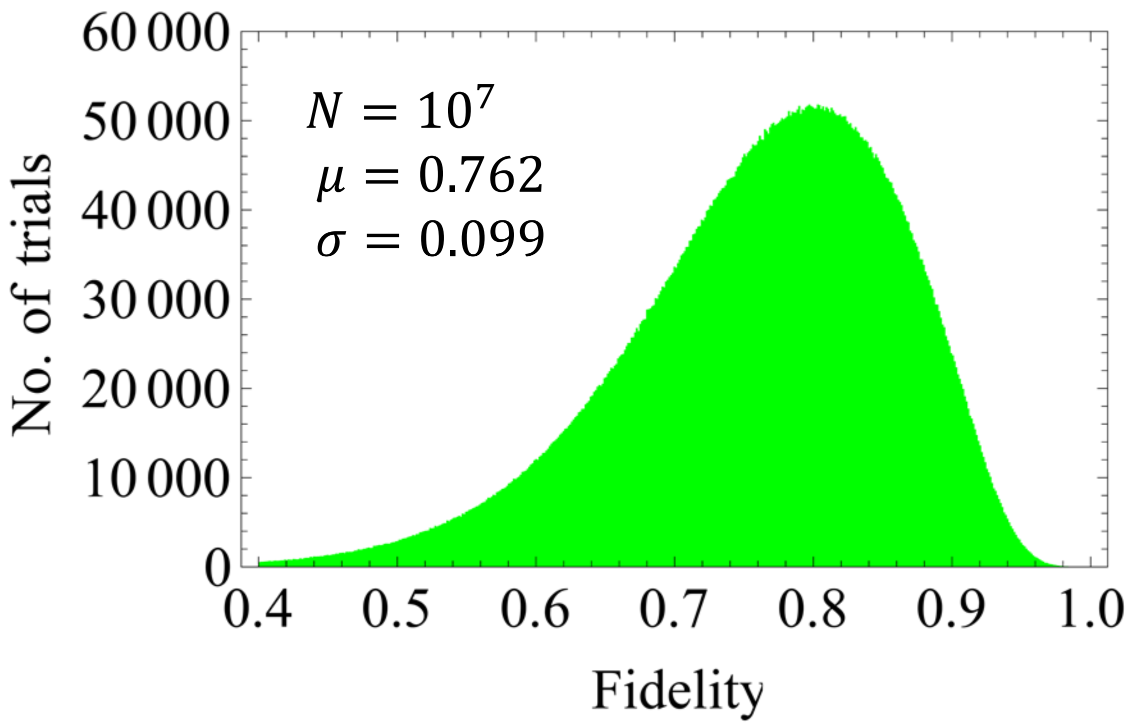
Error model

- BS: $\epsilon \sim N(0.5, 0.04\ )$
- PS: $\alpha \sim N^{+}(0.05, 0.025)$

$$f = |\langle\phi|\psi\rangle|^2$$

Simulation results

- 8-item Grover search



Error model

- BS: $\epsilon \sim N(0.5, 0.04\ )$
- PS: $\alpha \sim N^{+}(0.05, 0.025)$

$$f = |\langle\phi|\psi\rangle|^2$$

Conclusion

- Recursive formula for LO circuits of QFT and Grover inversion
- Size complexity: $d\log d\,;d^2\ [d^2]$
- Depth complexity: $5d\ [2d]$
- Applications: tool for boson sampling (QFT), Grover-like algorithms (GI)

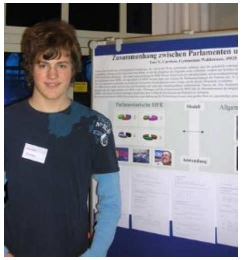
Acknowledgement

- Quantum cryptography group in Tartu

Dominique Unruh

Ehsan Ehbrami

Mayuresh Anand



Tore Vincent Carstens

  - Post-quantum security of encryption schemes
  - Verification of quantum cryptographic proofs
  - Quantum collision finding problem
  - Quantum proofs of knowledge