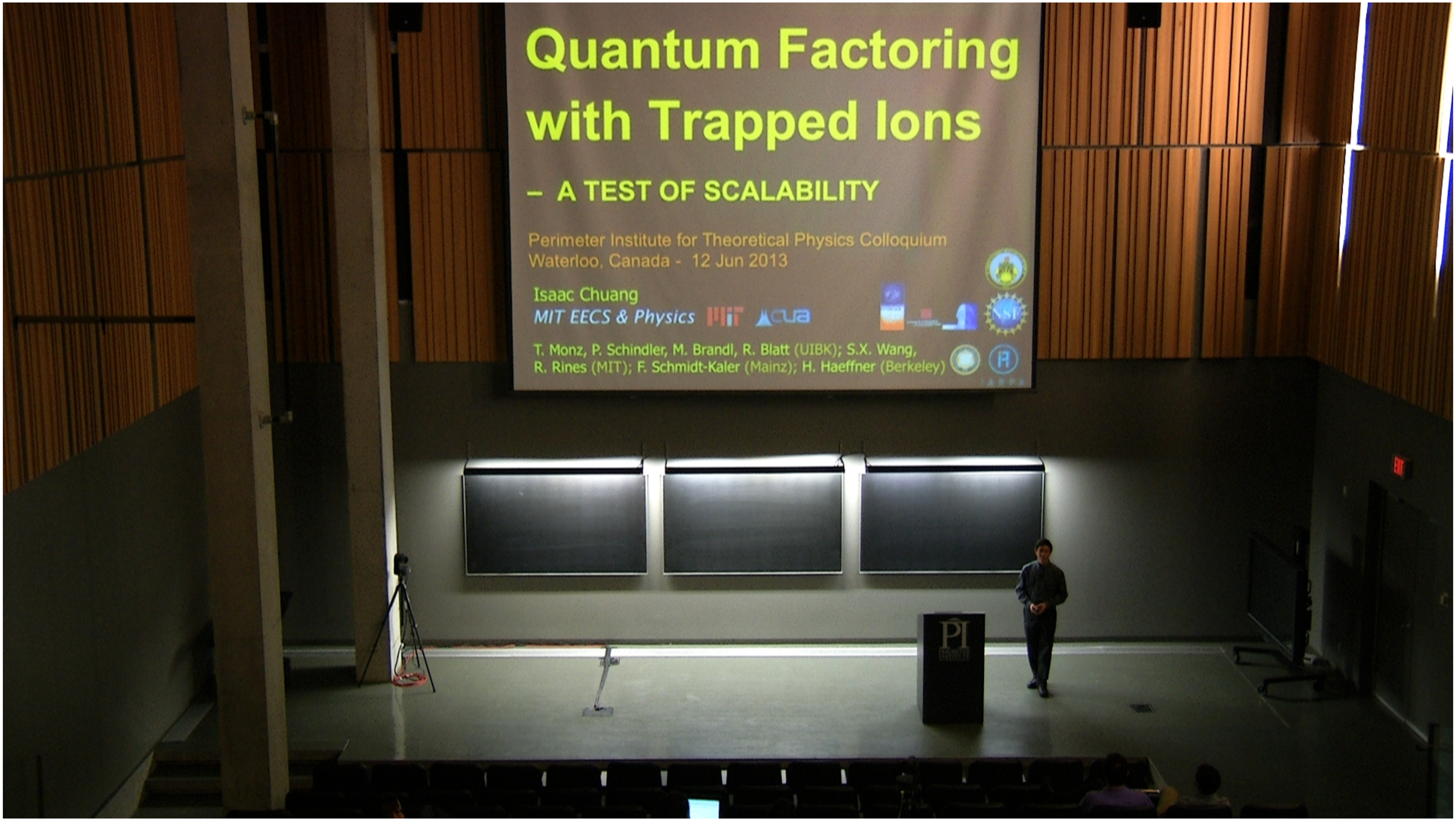
Title: Quantum Factoring with Trapped Ions - A test of scalability

Date: Jun 12, 2013 02:00 PM

URL: http://pirsa.org/13060002

Abstract: Shor's algorithm can be a meaningful test for experimental quantum processing systems, when suitably realized. I present results from a recent implemenation of quantum factoring using trapped ion qubits, demonstrating feed-forward control, use of quantum memory during computation, and cascaded three-qubit gates. Such capabilities are necessary ingredients for a future large-scale,
fault-tolerant quantum computing system.


EXIT
PERIMETER
INSTITUTE


Quantum Factoring
with Trapped Ions
– A TEST OF SCALABILITY
Perimeter Institute for Theoretical Physics Colloquium
Waterloo, Canada - 12 Jun 2013
Isaac Chuang
MIT EECS & Physics
T. Monz, P. Schindler, M. Brandl, R. Blatt (UIBK); S.X. Wang,
R. Rines (MIT); F. Schmidt-Kaler (Mainz); H. Haeffner (Berkeley)

Shor's Q. Factoring Algorithm

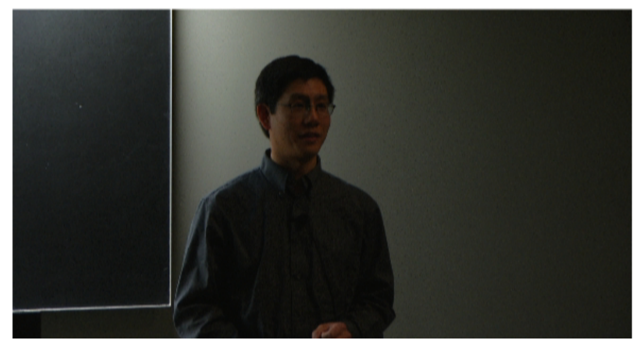
$$f(x) = a^{x} \bmod N$$

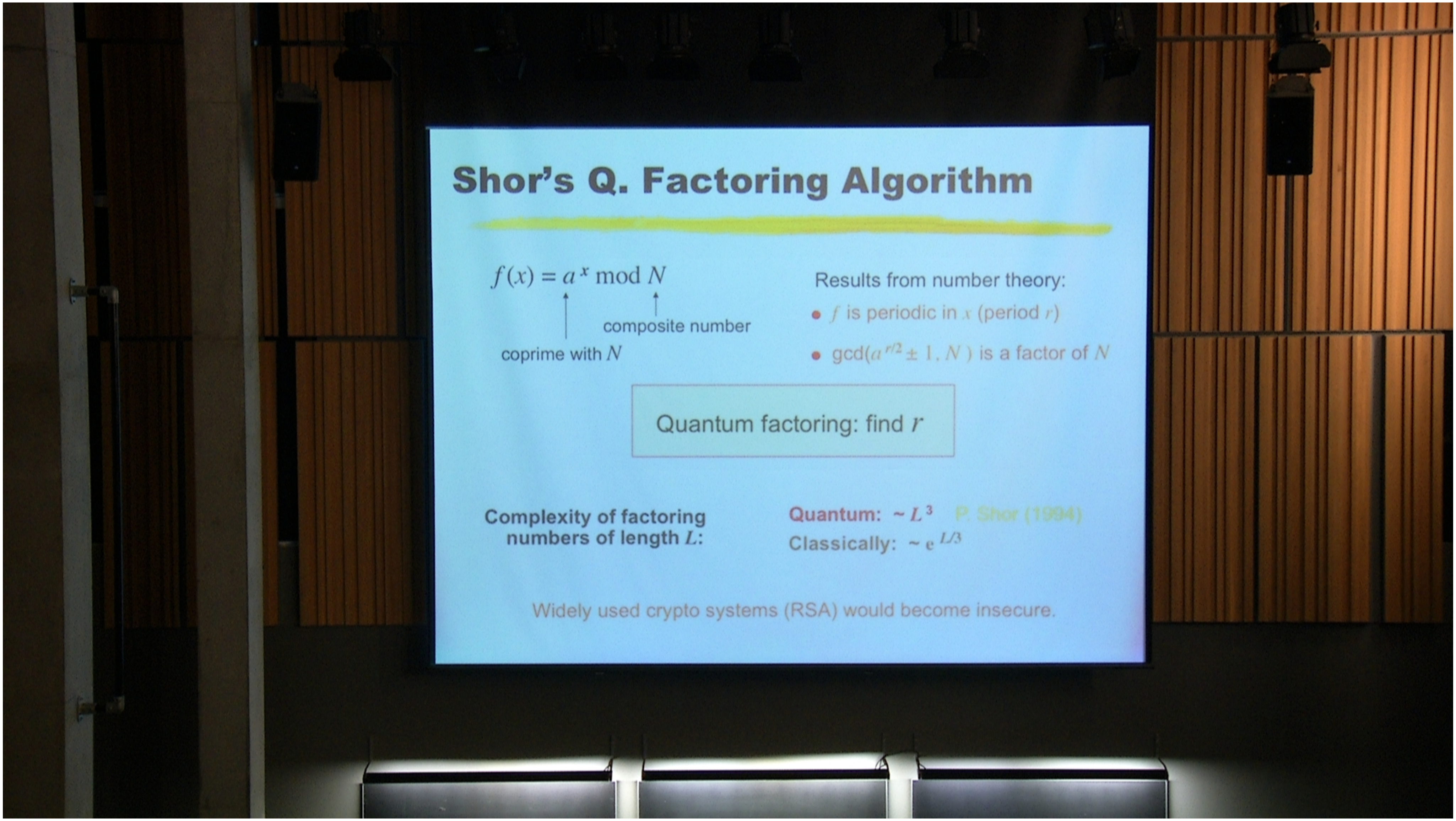
composite number

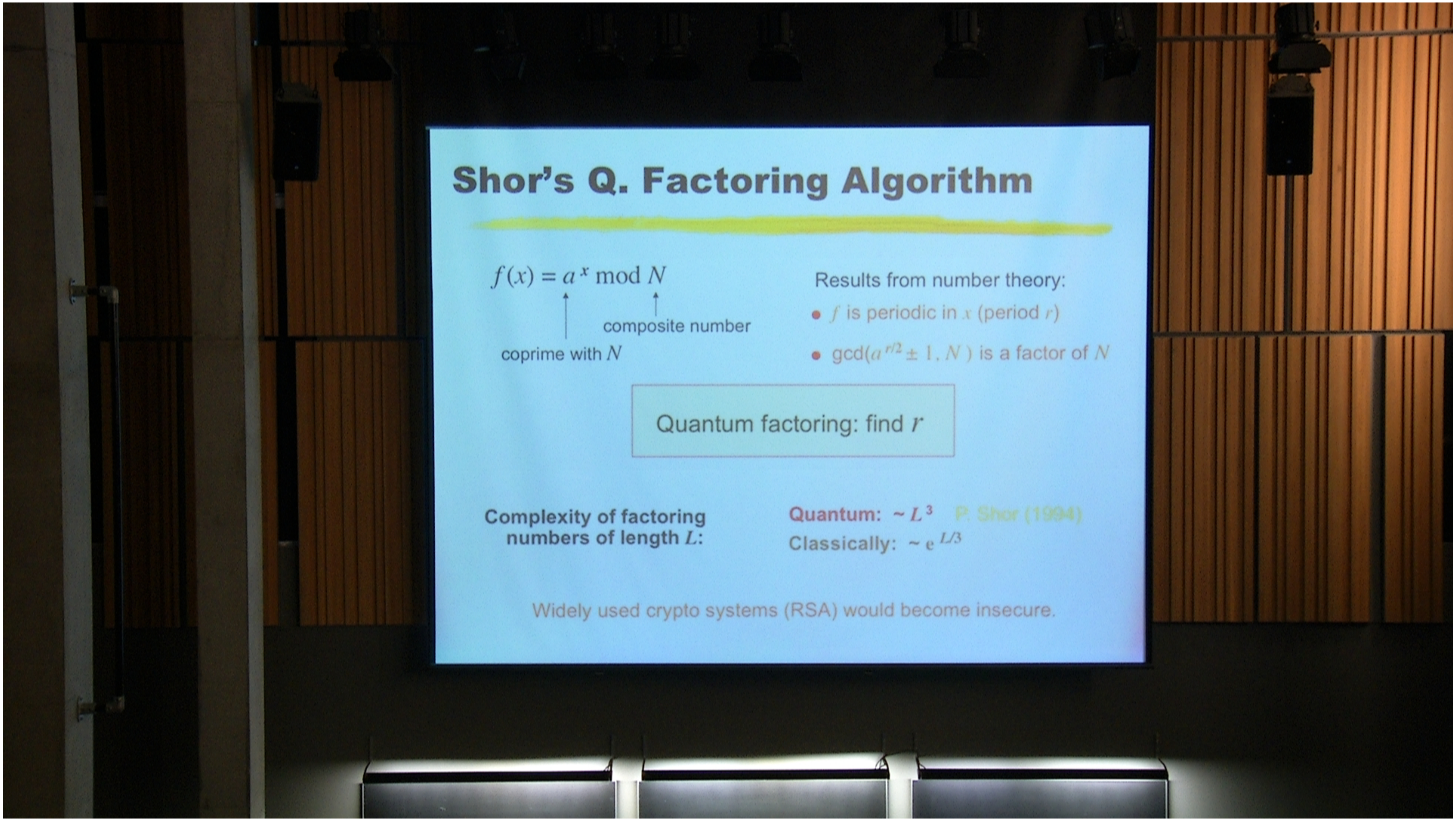
coprime with N

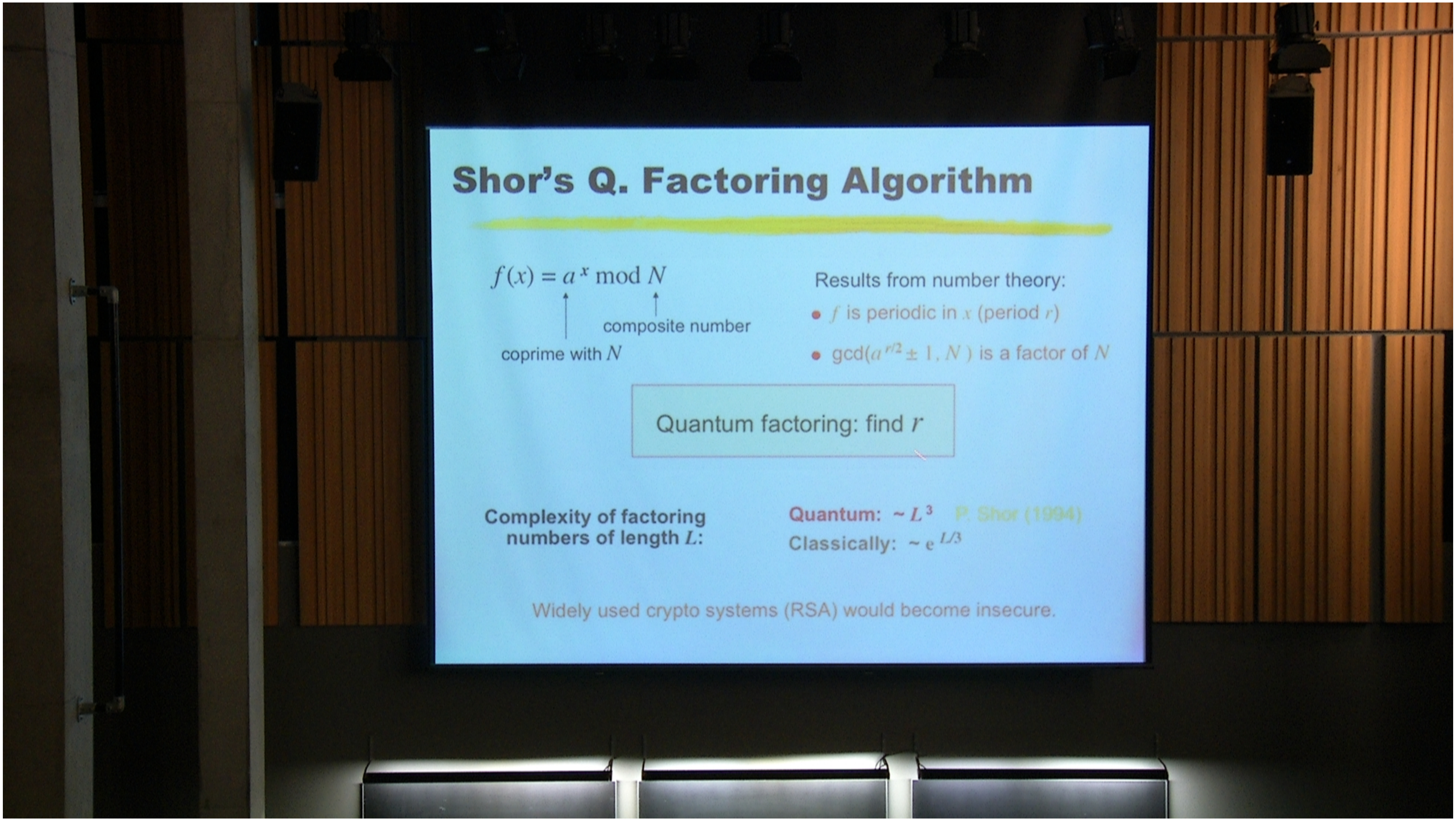
Results from number theory:

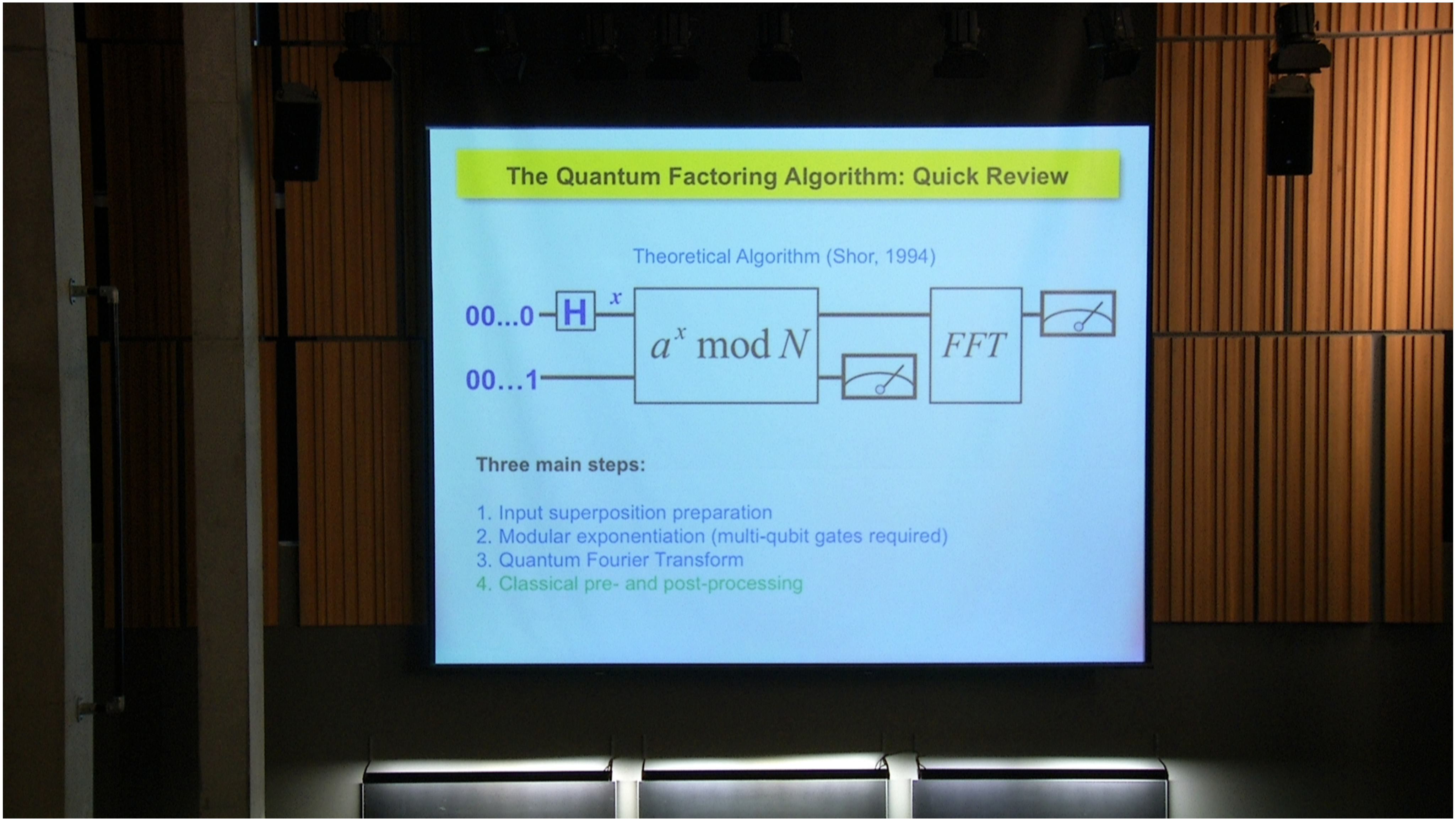
- f is periodic in x (period r)
- $\gcd(a^{r/2} \pm 1, N)$ is a factor of N

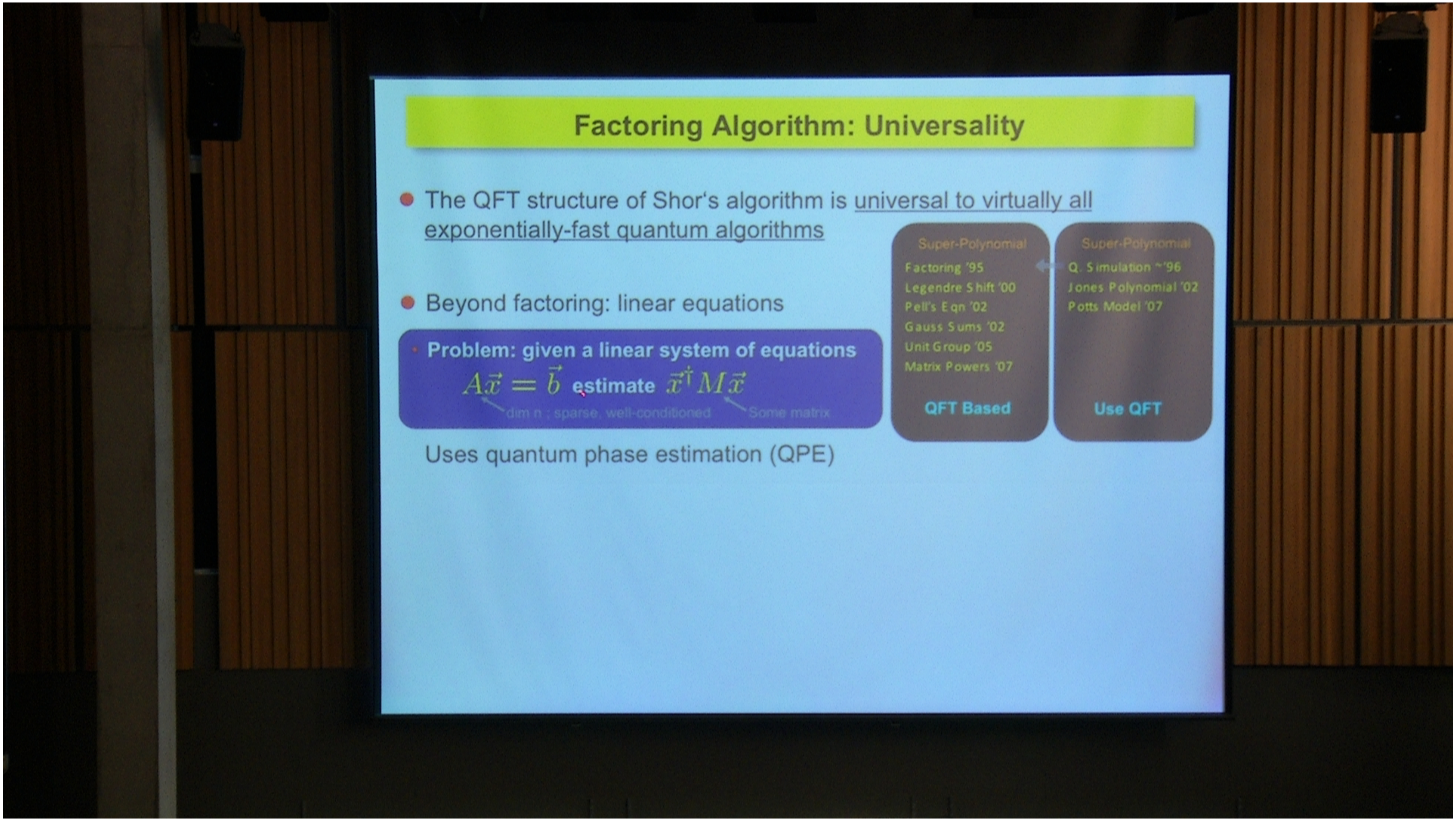


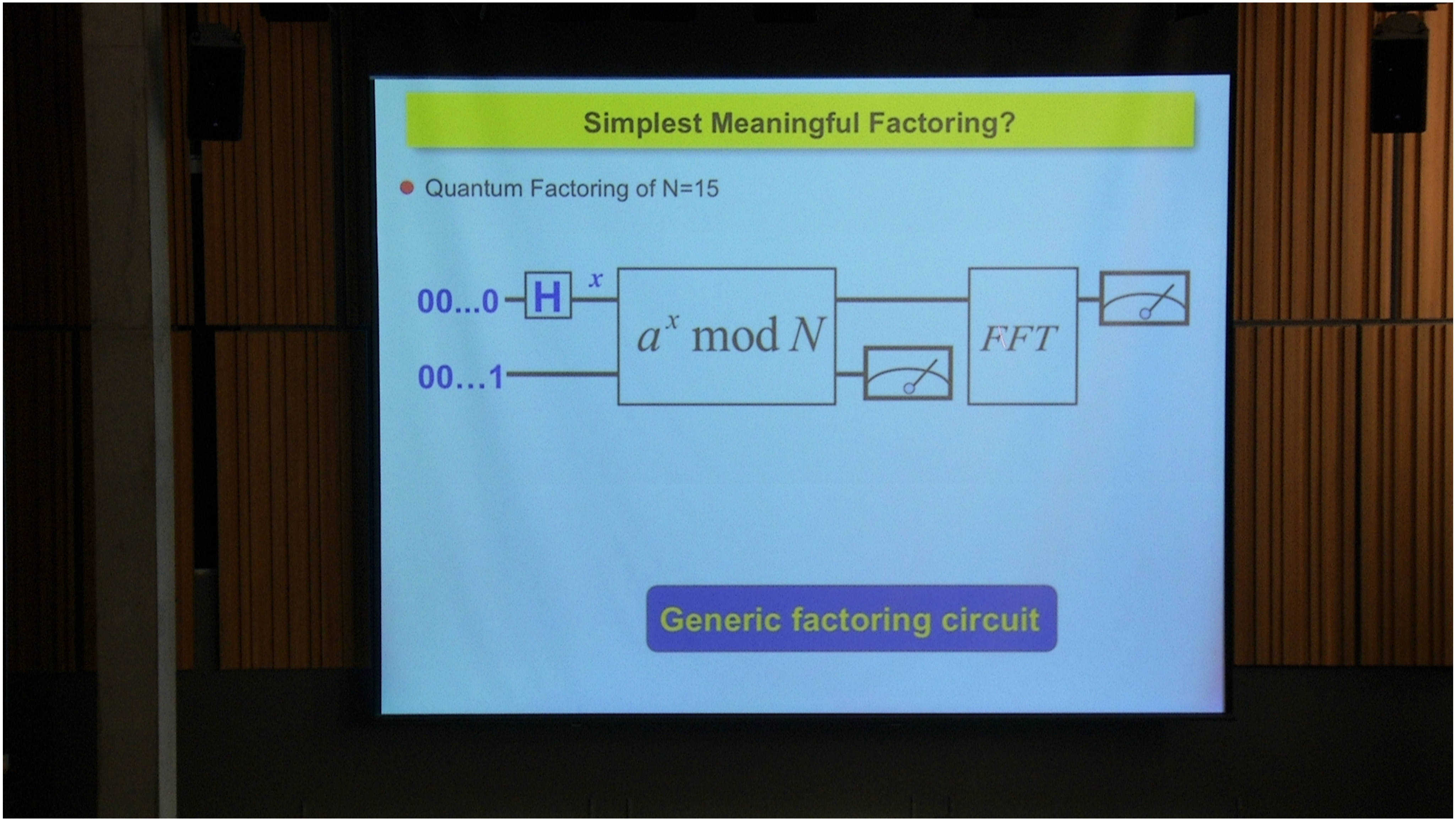

Shor's Q. Factoring Algorithm
$f(x) = a^x \bmod N$
composite number
coprime with N
Results from number theory:
• f is periodic in x (period r)
• $\gcd(a^{r/2} \pm 1, N)$ is a factor of N
Quantum factoring: find r
Complexity of factoring numbers of length L:
Quantum: $\sim L^3$ P. Shor (1994)
Classically: $\sim e^{L/3}$
Widely used crypto systems (RSA) would become insecure.

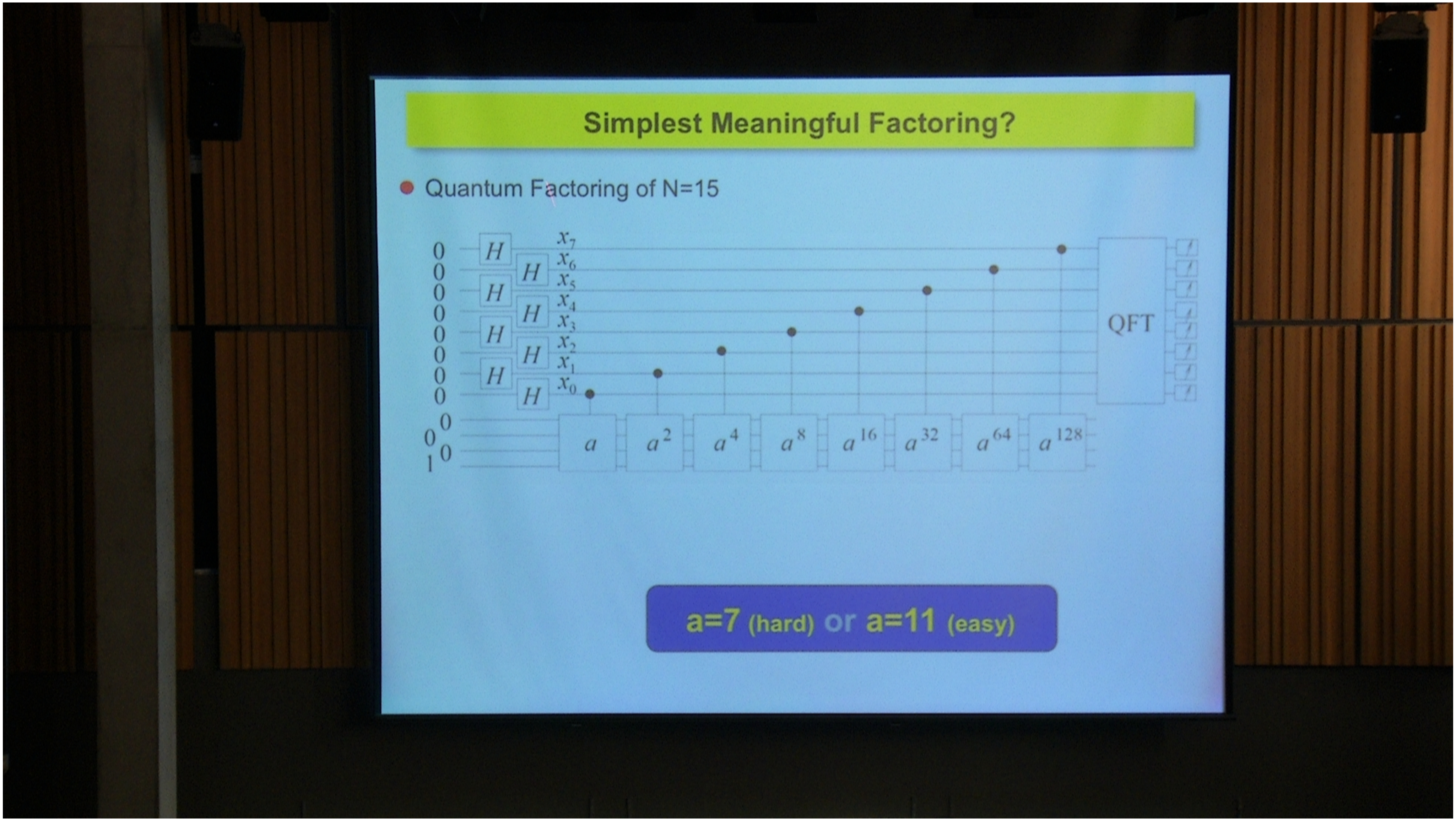

Shor's Q. Factoring Algorithm
$f(x) = a^x \bmod N$
composite number
coprime with N
Results from number theory:
• f is periodic in x (period r)
• gcd($a^{r/2} \pm 1, N$) is a factor of N
Quantum factoring: find r
Complexity of factoring numbers of length L:
Quantum: ~ L^3 P. Shor (1994)
Classically: ~ $e^{L/3}$
Widely used crypto systems (RSA) would become insecure.


Shor's Q. Factoring Algorithm
$f(x) = a^x \bmod N$
composite number
coprime with N
Results from number theory:
f is periodic in x (period r)
$\gcd(a^{r/2} \pm 1, N)$ is a factor of N
Quantum factoring: find r
Complexity of factoring numbers of length L:
Quantum: $\sim L^3$
P. Shor (1994)
Classically: $\sim e^{L/3}$
Widely used crypto systems (RSA) would become insecure.

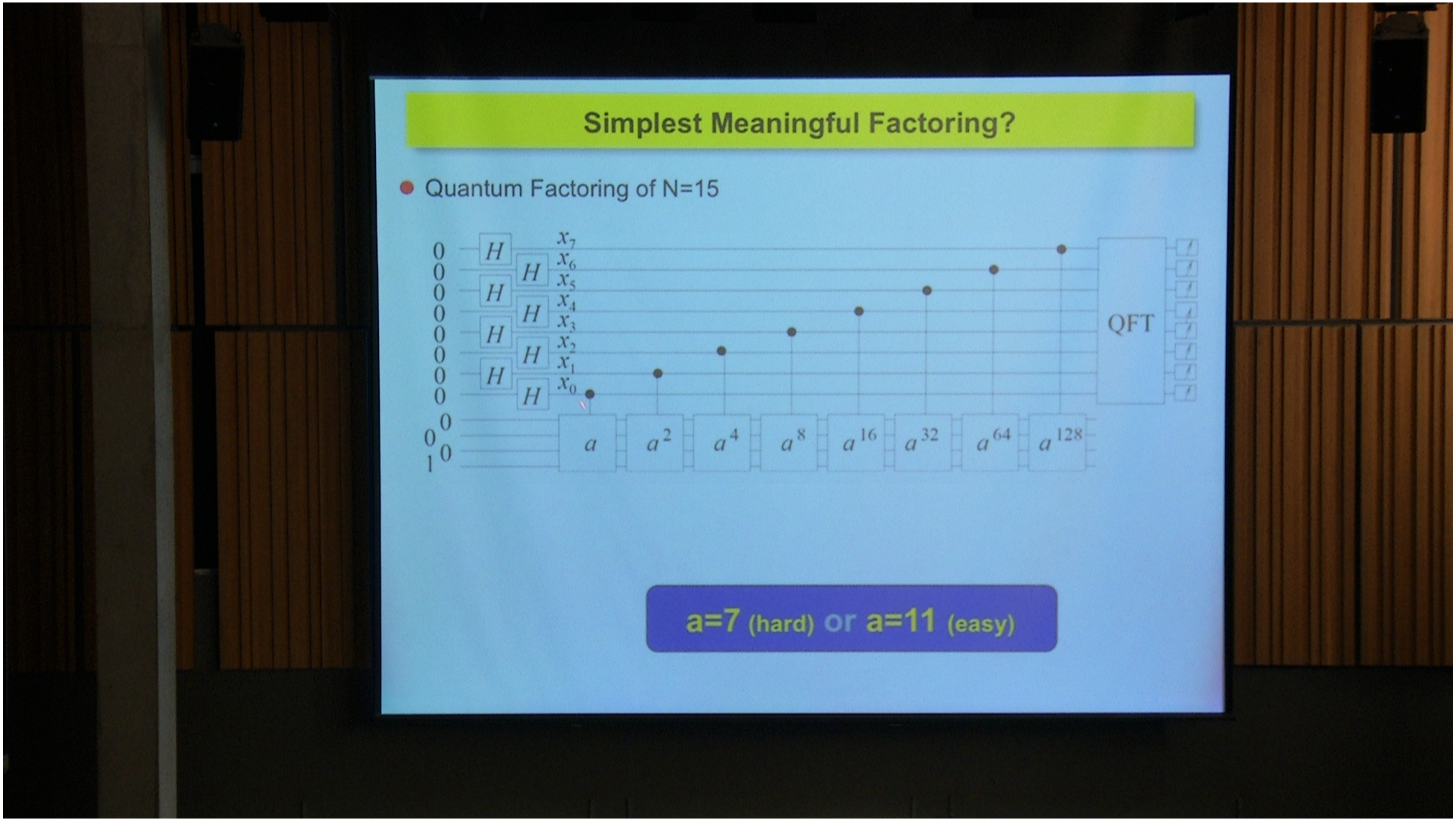

The Quantum Factoring Algorithm: Quick Review
Theoretical Algorithm (Shor, 1994)
00...0
H
x
a^x mod N
00...1
FFT
Three main steps:
1. Input superposition preparation
2. Modular exponentiation (multi-qubit gates required)
3. Quantum Fourier Transform
4. Classical pre- and post-processing

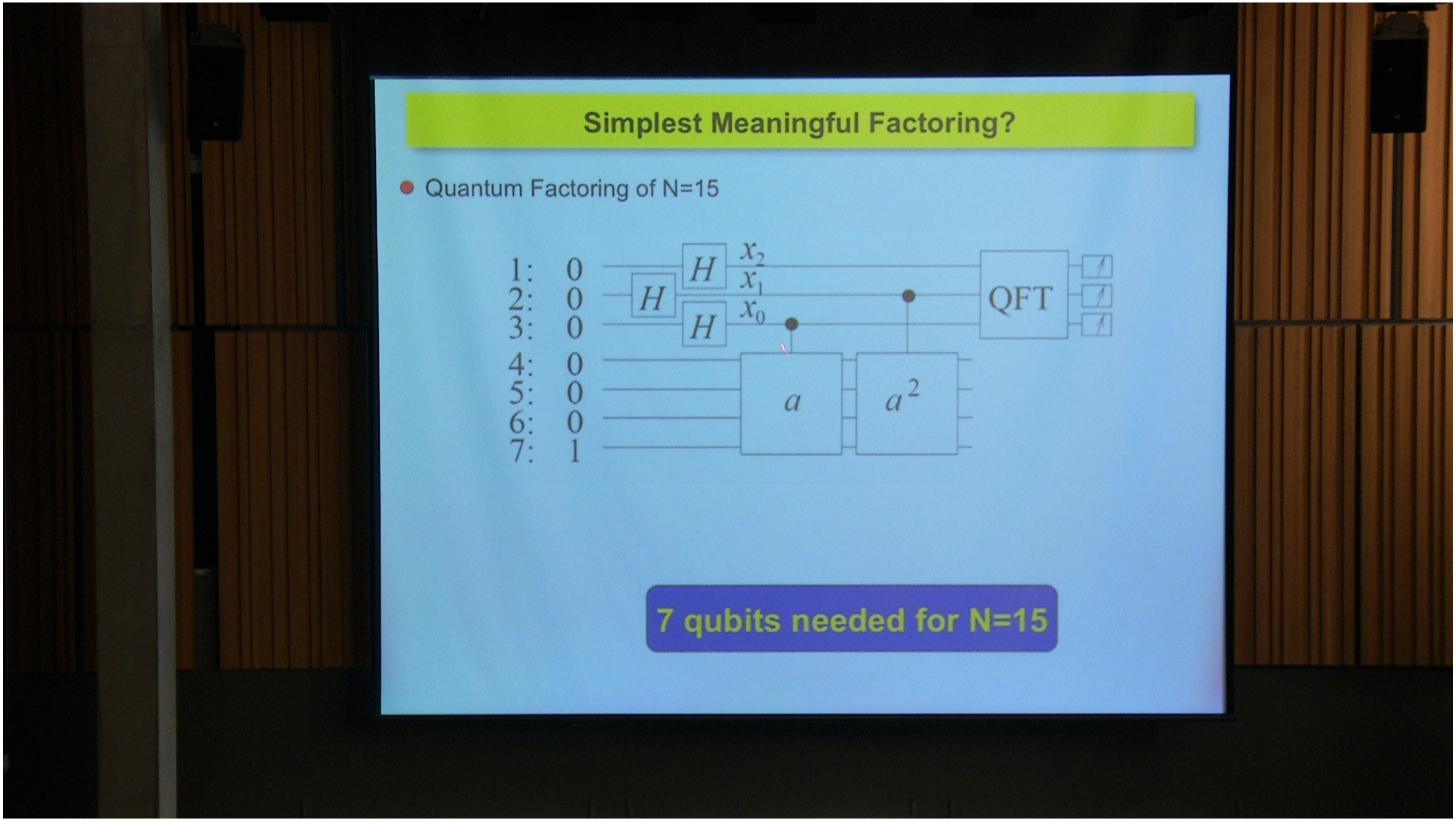

Factoring Algorithm: Universality
The QFT structure of Shor's algorithm is universal to virtually all exponentially-fast quantum algorithms
Beyond factoring: linear equations
Problem: given a linear system of equations
$A\vec{x} = \vec{b}$ estimate $\vec{x}^\dagger M \vec{x}$
dim n ; sparse, well-conditioned
Some matrix
Uses quantum phase estimation (QPE)
Super-Polynomial
Factoring '95
Legendre Shift '00
Pell's Eqn '02
Gauss Sums '02
Unit Group '05
Matrix Powers '07
QFT Based
Super-Polynomial
Q. Simulation ~'96
Jones Polynomial '02
Potts Model '07
Use QFT

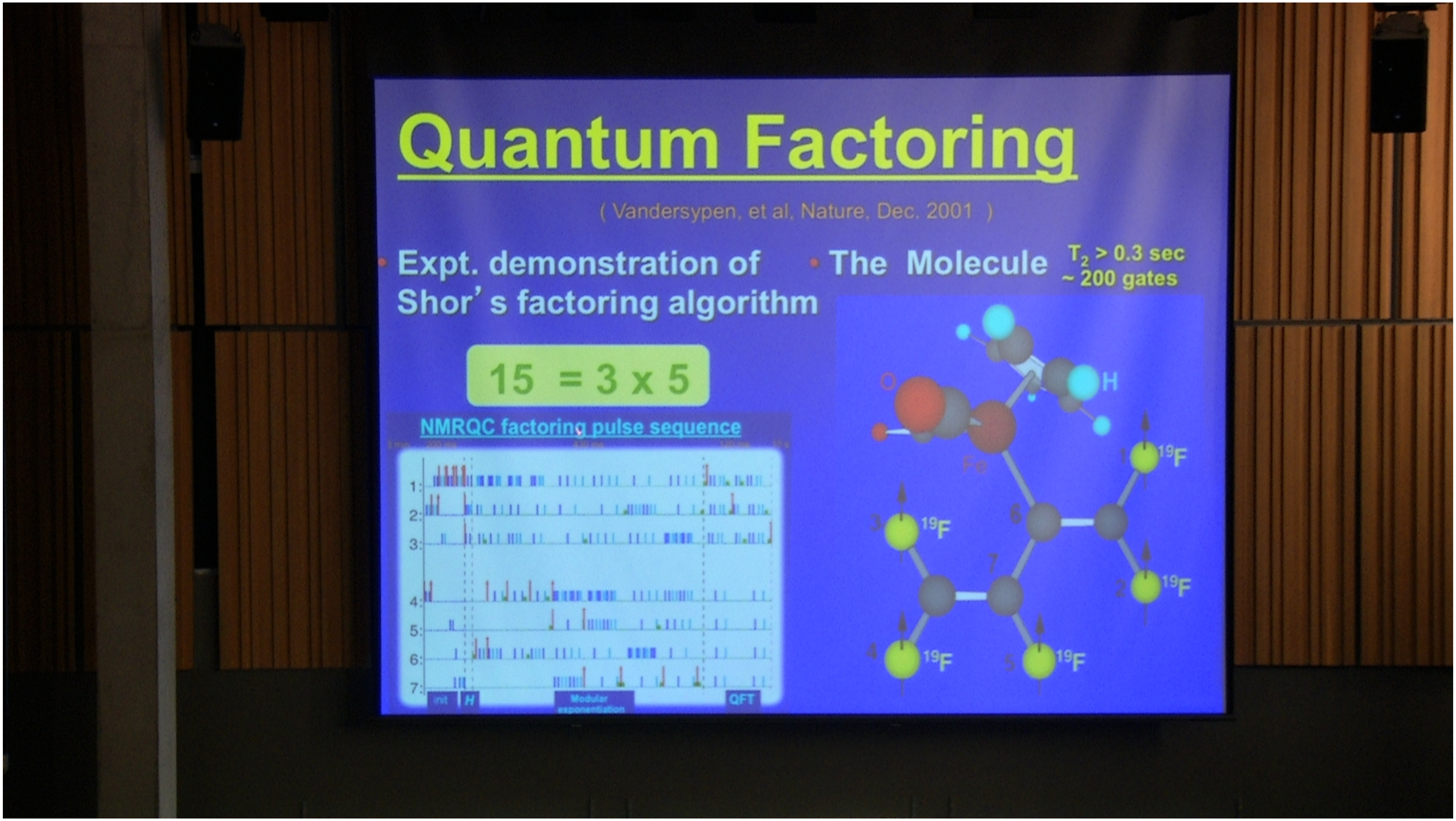

Simplest Meaningful Factoring?
Quantum Factoring of N=15
00...0
H
x
00…1
a^x mod N
FFT
Generic factoring circuit



Simplest Meaningful Factoring?
Quantum Factoring of N=15
H
QFT
a=7 (hard) or a=11 (easy)


Simplest Meaningful Factoring?
Quantum Factoring of N=15
H
x7
x6
x5
x4
x3
x2
x1
x0
a
a2
a4
a8
a16
a32
a64
a128
QFT
a=7 (hard) or a=11 (easy)


Simplest Meaningful Factoring?
Quantum Factoring of N=15
1: 0
2: 0
3: 0
4: 0
5: 0
6: 0
7: 1
H
H
H
x_2
x_1
x_0
a
a^2
QFT
7 qubits needed for N=15


Quantum Factoring
(Vandersypen, et al, Nature, Dec. 2001)
Expt. demonstration of Shor's factoring algorithm
The Molecule
T2 > 0.3 sec
~ 200 gates
15 = 3 x 5
NMRQC factoring pulse sequence
1:
2:
3:
4:
5:
6:
7:
init
H
Modular exponentiation
QFT
O
H
Fe
19F
19F
19F
19F
19F

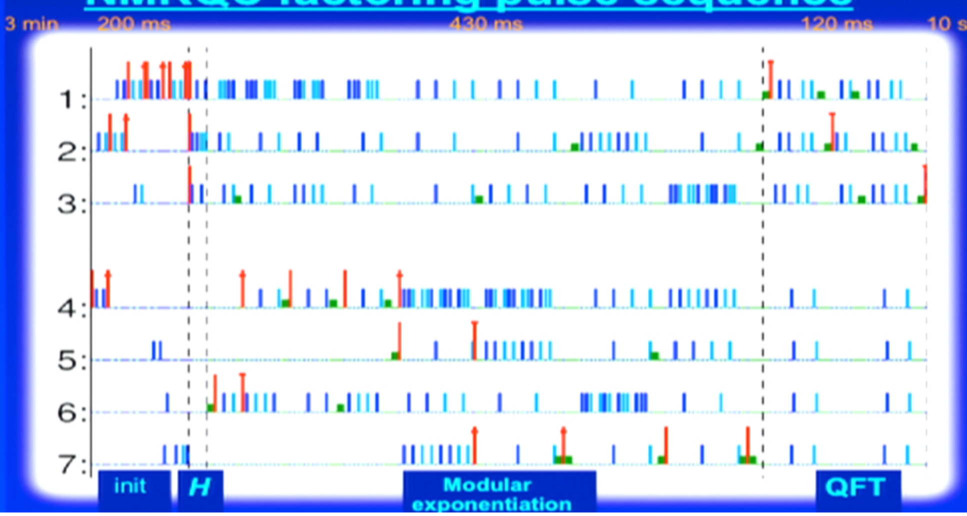
Quantum Factoring

(Vandersypen, et al, Nature, Dec. 2001)

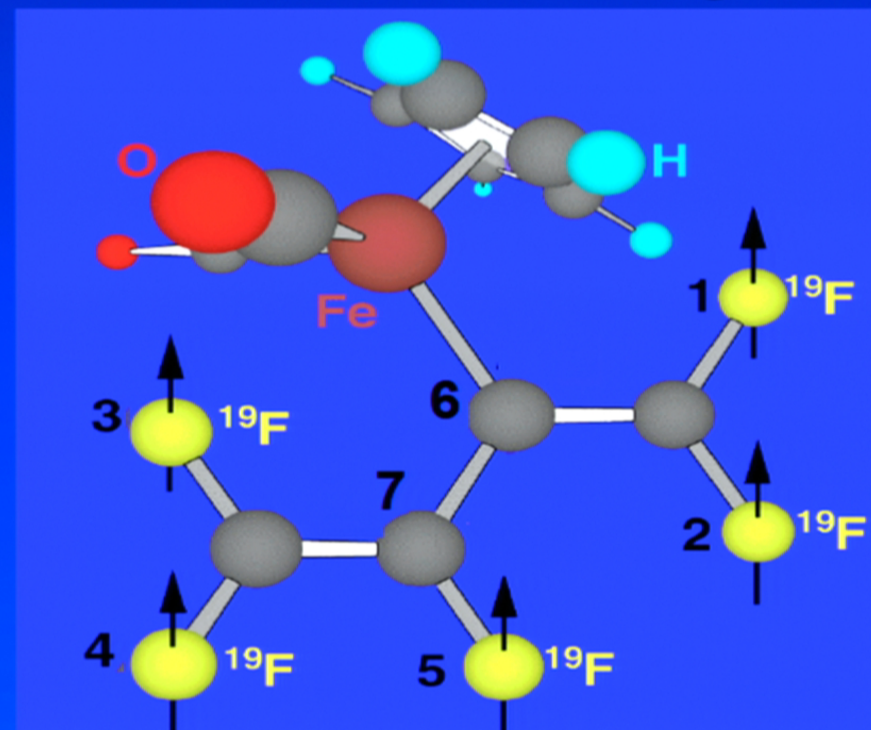
- **Expt. demonstration of Shor's factoring algorithm**

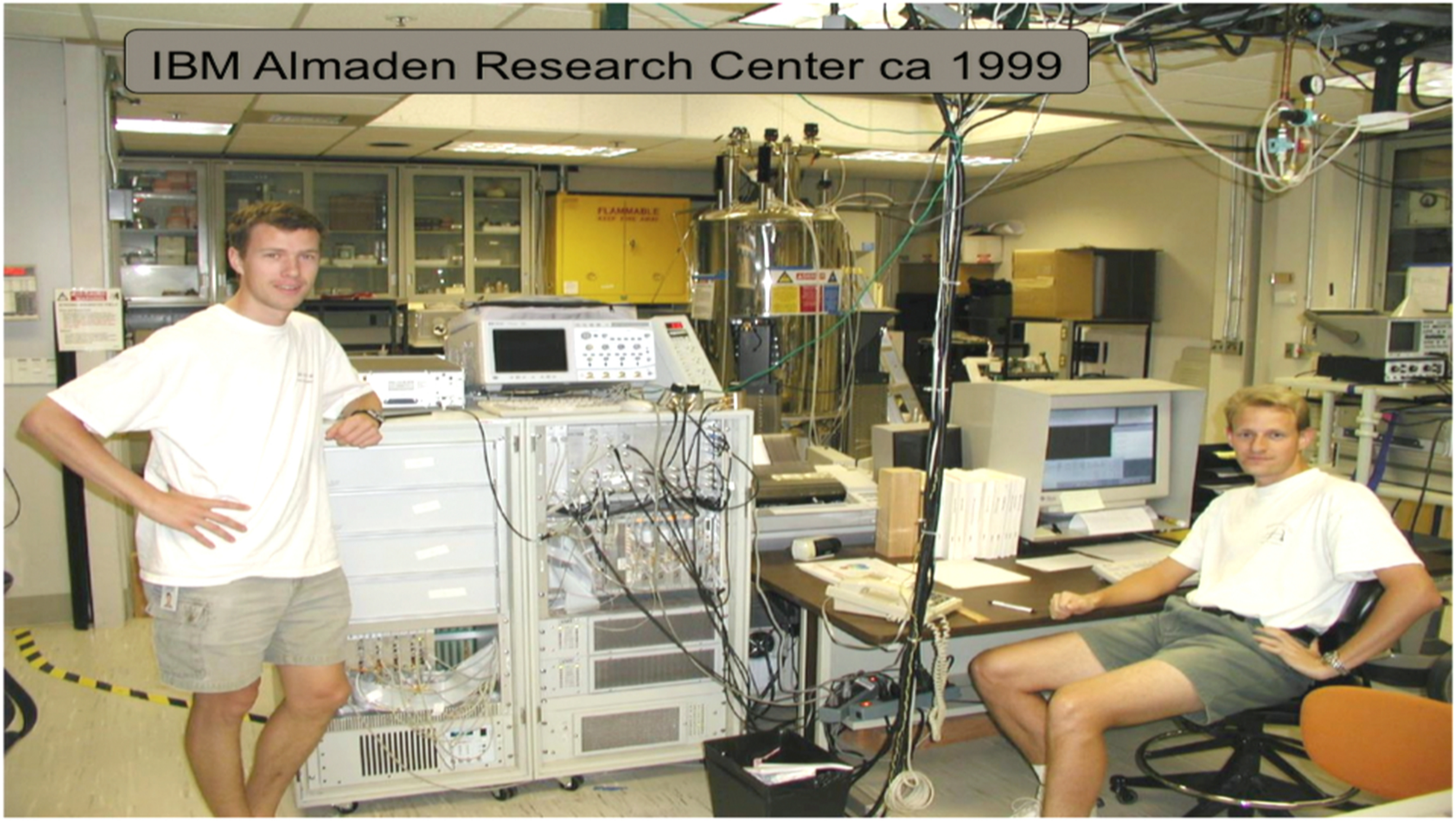
15 = 3 x 5

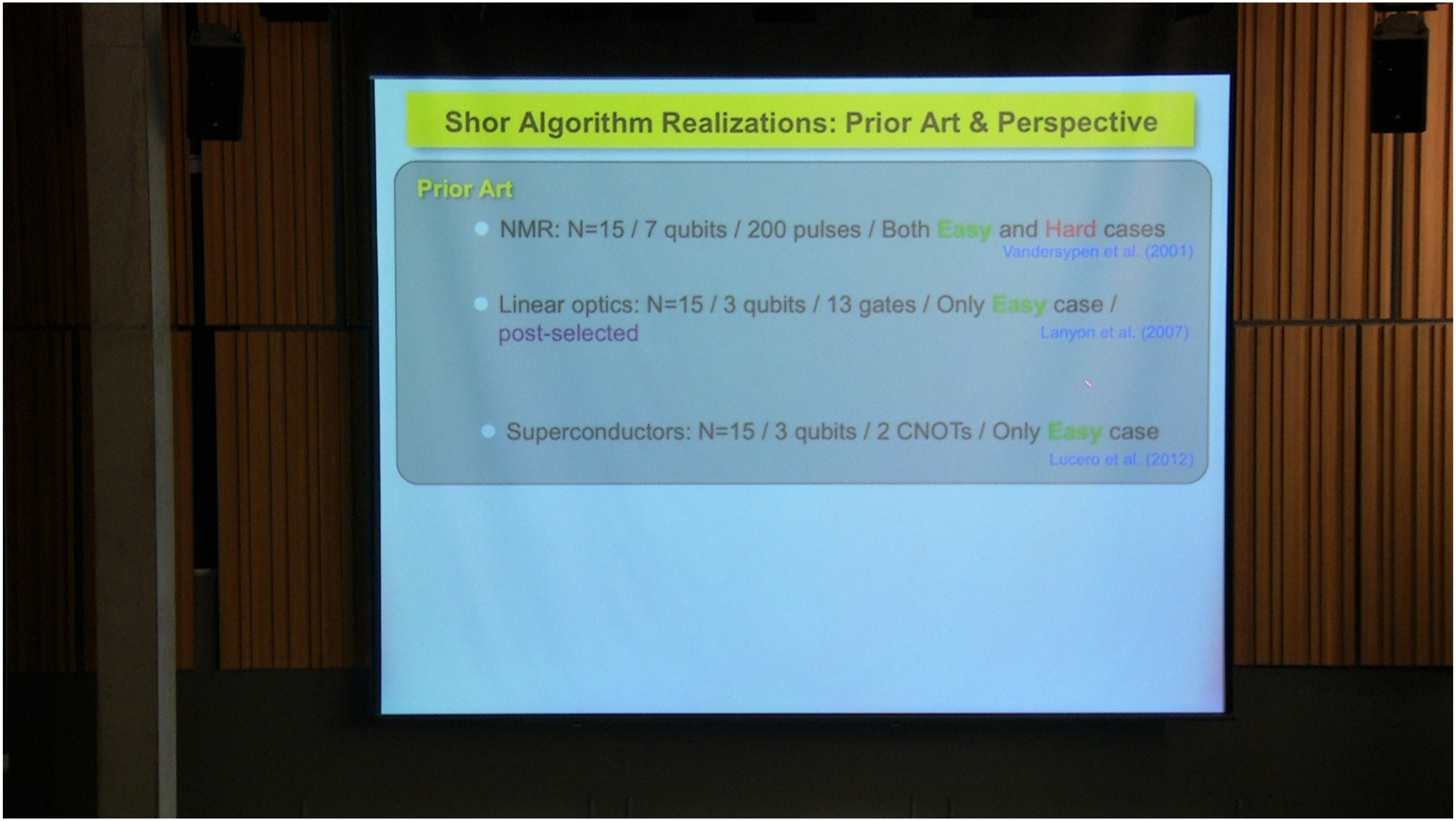
NMRQC factoring pulse sequence



- **The Molecule** $T_2 > 0.3$ sec ~ 200 gates



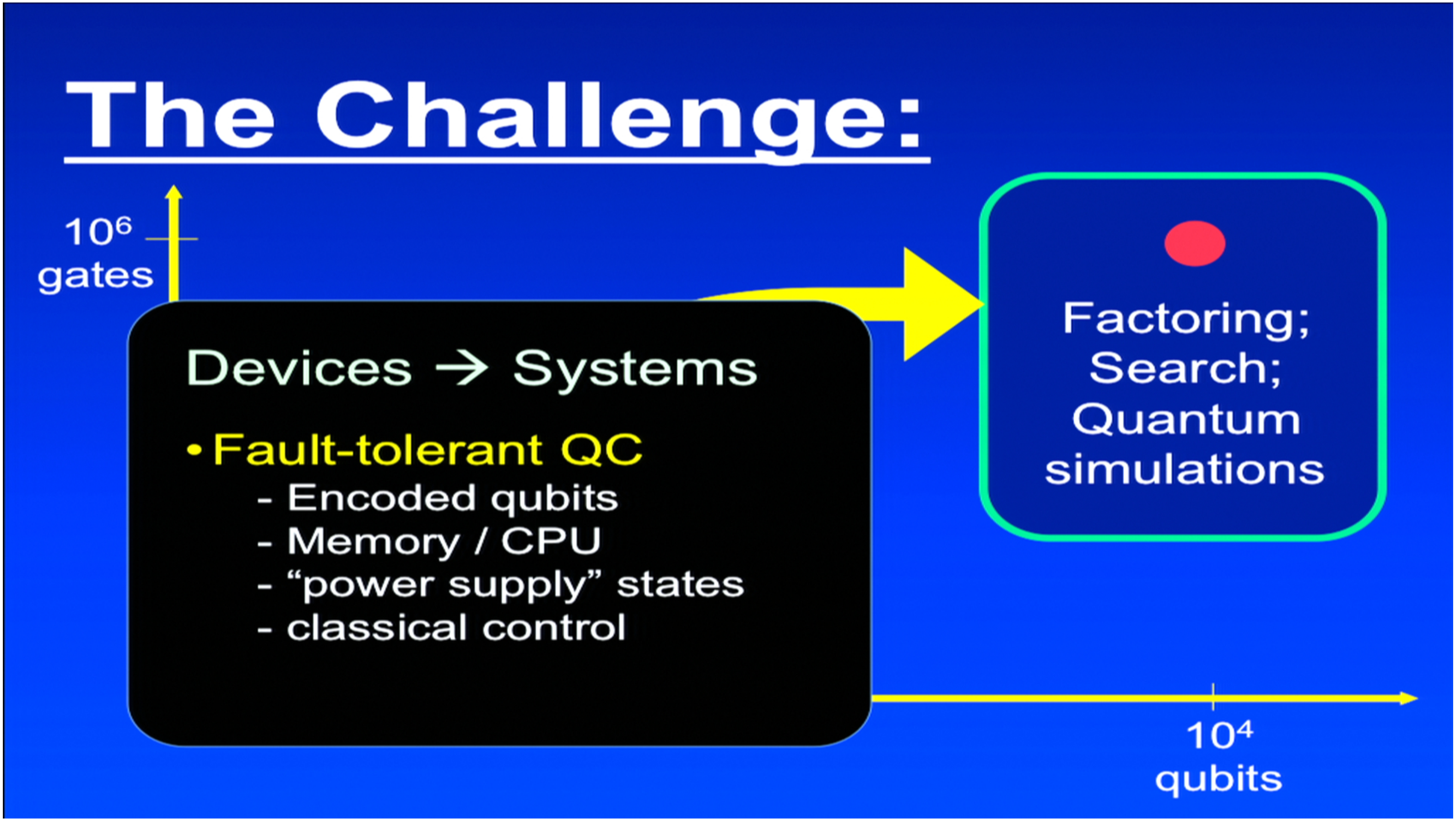

IBM Almaden Research Center ca 1999
FLAMMABLE

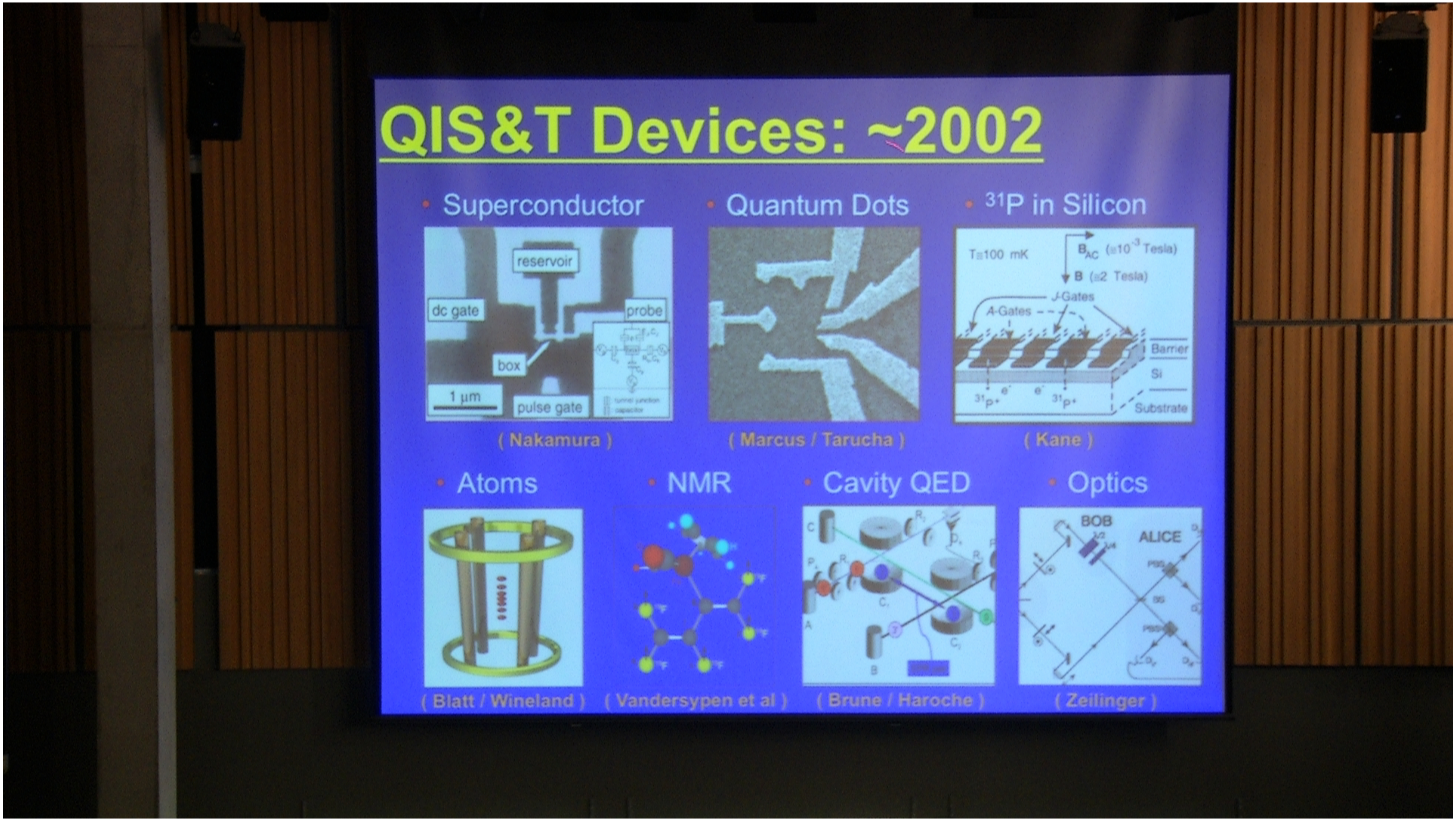

Shor Algorithm Realizations: Prior Art & Perspective
Prior Art
NMR: N=15 / 7 qubits / 200 pulses / Both Easy and Hard cases
Vandersypen et al. (2001)
Linear optics: N=15 / 3 qubits / 13 gates / Only Easy case / post-selected
Lanyon et al. (2007)
Superconductors: N=15 / 3 qubits / 2 CNOTs / Only Easy case
Lucero et al. (2012)

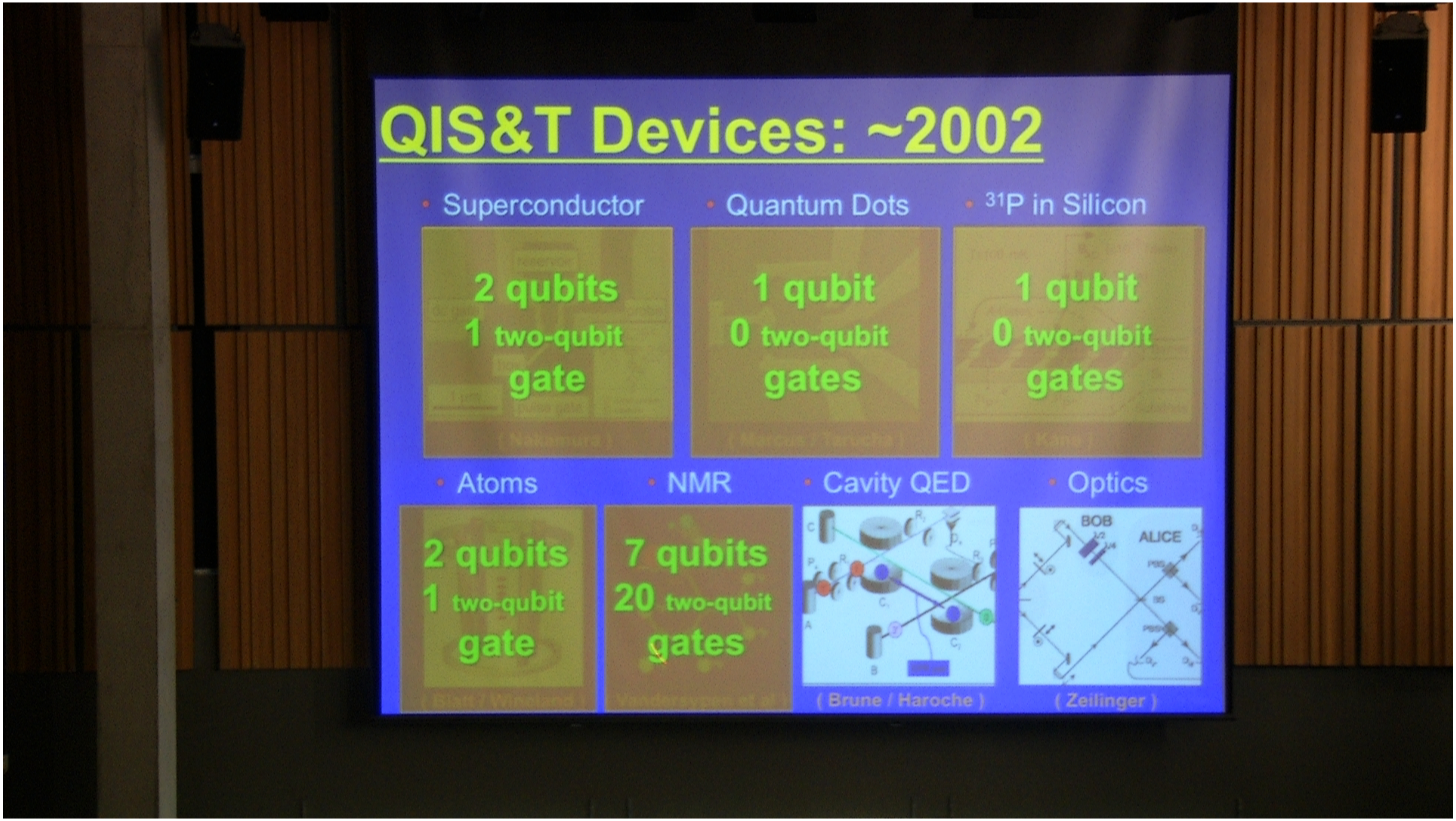
Shor Algorithm Realizations: Prior Art & Perspective

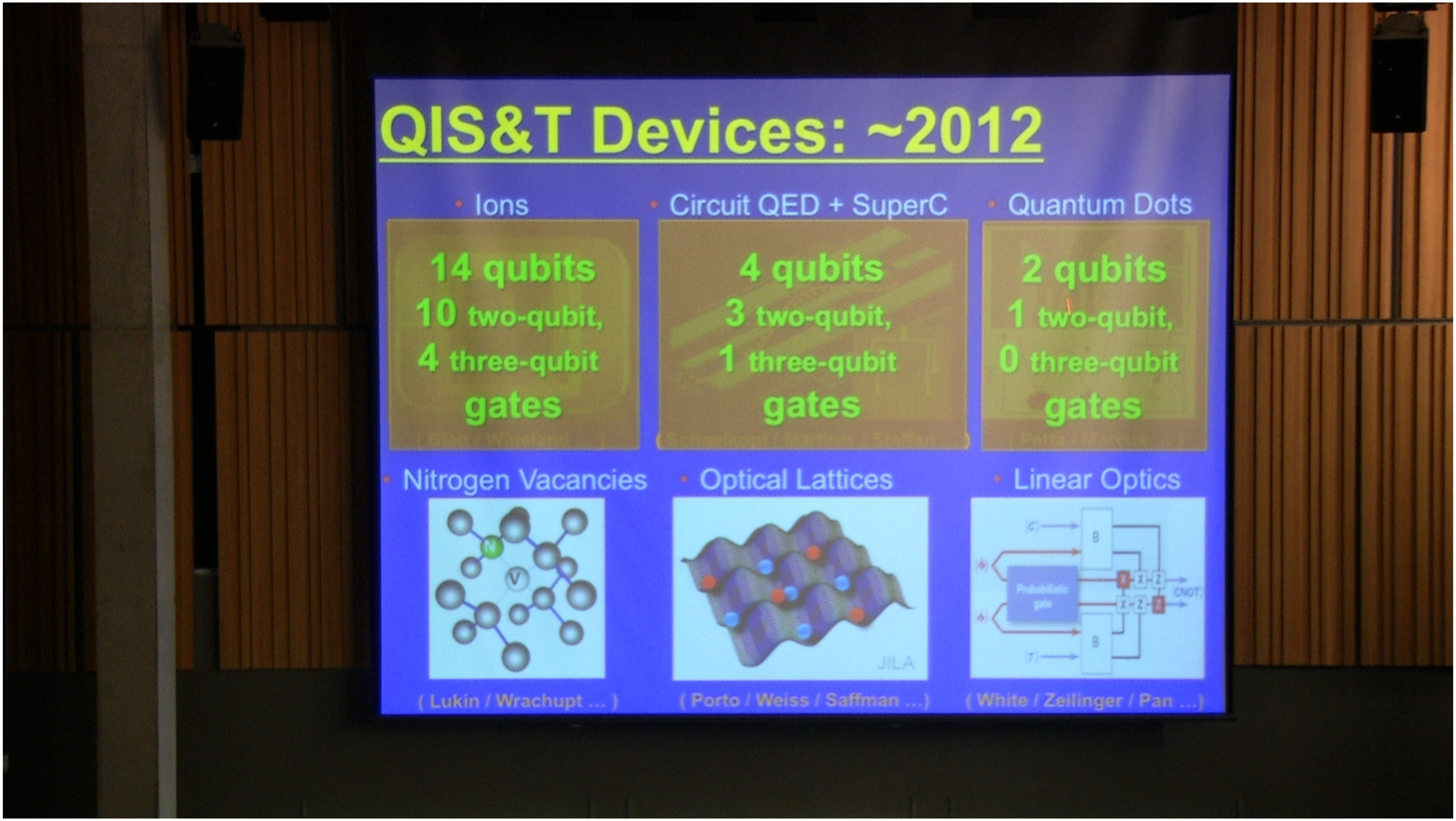
Prior Art

- NMR: N=15 / 7 qubits / 200 pulses / Both **Easy** and Hard cases
  Vandersypen et al. (2001)
- Linear optics: N=15 / 3 qubits / 13 gates / Only **Easy** case / post-selected
  Lanyon et al. (2007)
  N=21 / 4 qubits / 26 gates / Only **Easy** case
  Lopez et al. (2011)
- Superconductors: N=15 / 3 qubits / 2 CNOTs / Only **Easy** case
  Lucero et al. (2012)

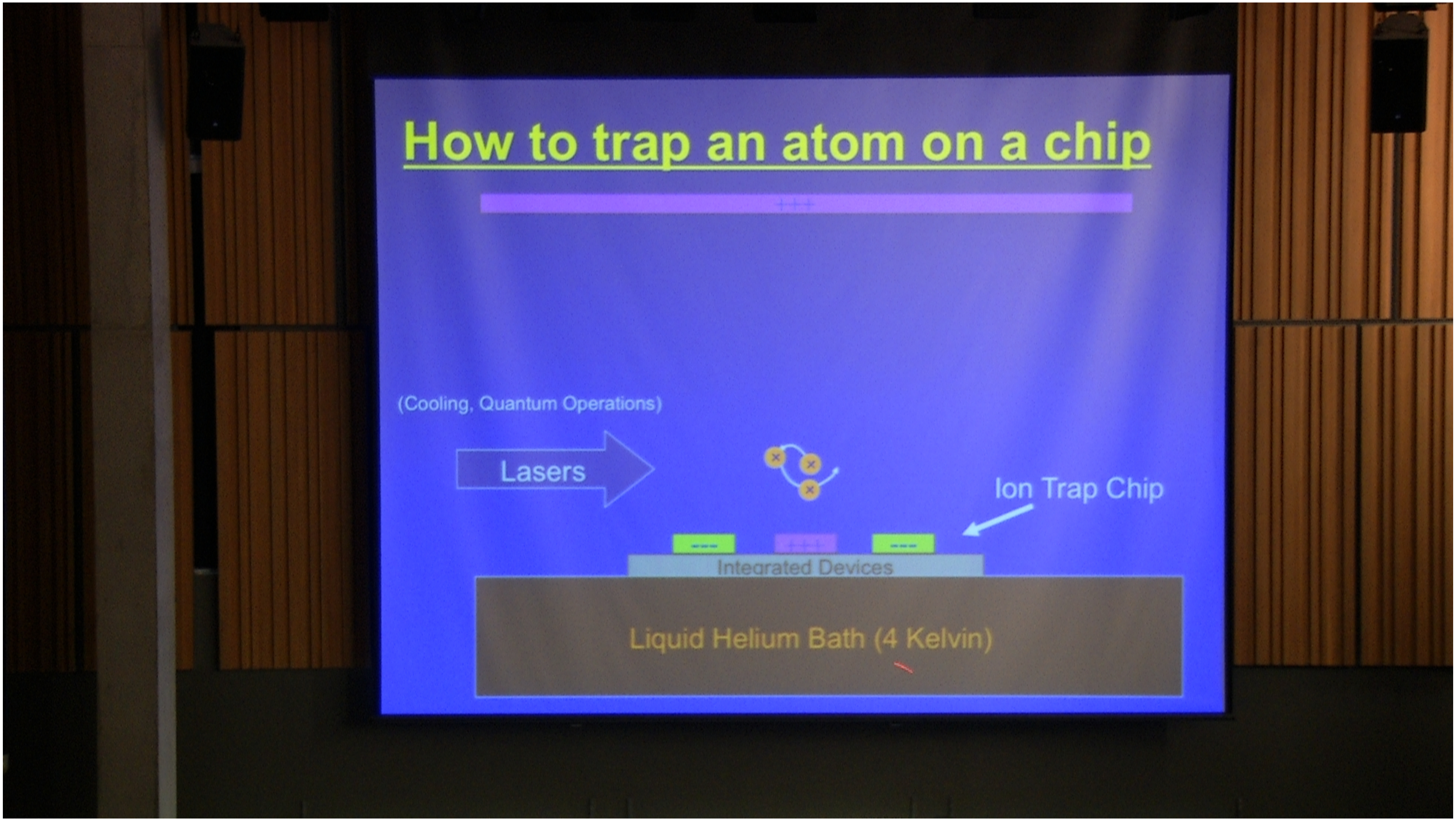

The Challenge:
10^6 gates
Devices → Systems
• Fault-tolerant QC
- Encoded qubits
- Memory / CPU
- “power supply” states
- classical control
Factoring; Search; Quantum simulations
10^4 qubits


QIS&T Devices: ~2002
Superconductor
reservoir
dc gate
probe
box
1 µm
pulse gate
(Nakamura)
Quantum Dots
(Marcus / Tarucha)
31P in Silicon
T≅100 mK
B (≅2 Tesla)
J-Gates
A-Gates
Barrier
Si
Substrate
(Kane)
Atoms
(Blatt / Wineland)
NMR
(Vandersypen et al)
Cavity QED
(Brune / Haroche)
Optics
BOB
ALICE
(Zeilinger)


QIS&T Devices: ~2002
Superconductor
2 qubits
1 two-qubit gate
Quantum Dots
1 qubit
0 two-qubit gates
31P in Silicon
1 qubit
0 two-qubit gates
Atoms
2 qubits
1 two-qubit gate
NMR
7 qubits
20 two-qubit gates
Cavity QED
(Brune / Haroche)
Optics
BOB
ALICE
(Zeilinger)

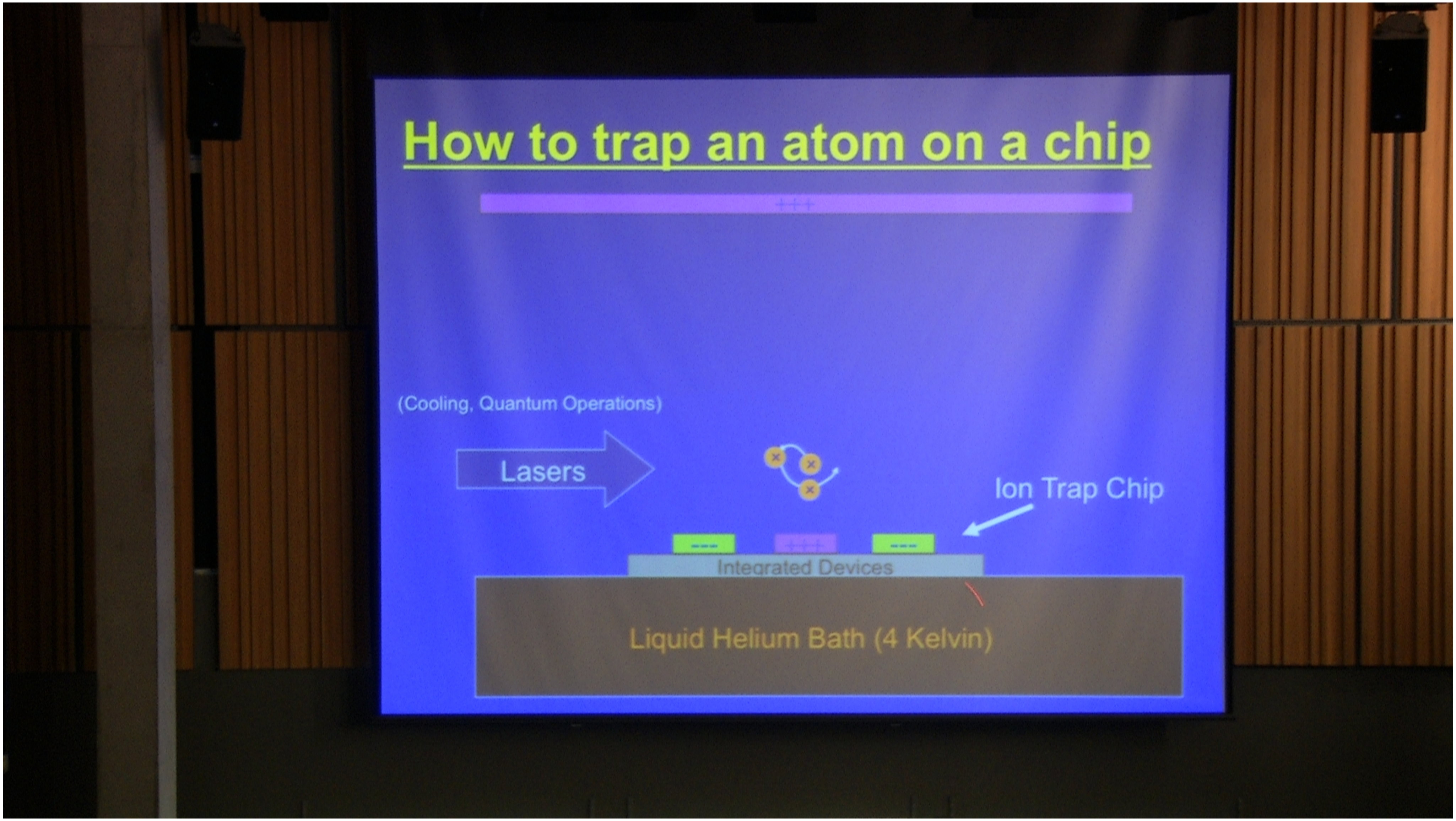


QIS&T Devices: ~2012
Ions
14 qubits
10 two-qubit,
4 three-qubit
gates
Circuit QED + SuperC
4 qubits
3 two-qubit,
1 three-qubit
gates
Quantum Dots
2 qubits
1 two-qubit,
0 three-qubit
gates
Nitrogen Vacancies
N
V
(Lukin / Wrachupt ...)
Optical Lattices
JILA
(Porto / Weiss / Saffman ...)
Linear Optics
B
CNOT
(White / Zeilinger / Pan ...)


How to trap an atom on a chip
+++
(Cooling, Quantum Operations)
Lasers
Ion Trap Chip

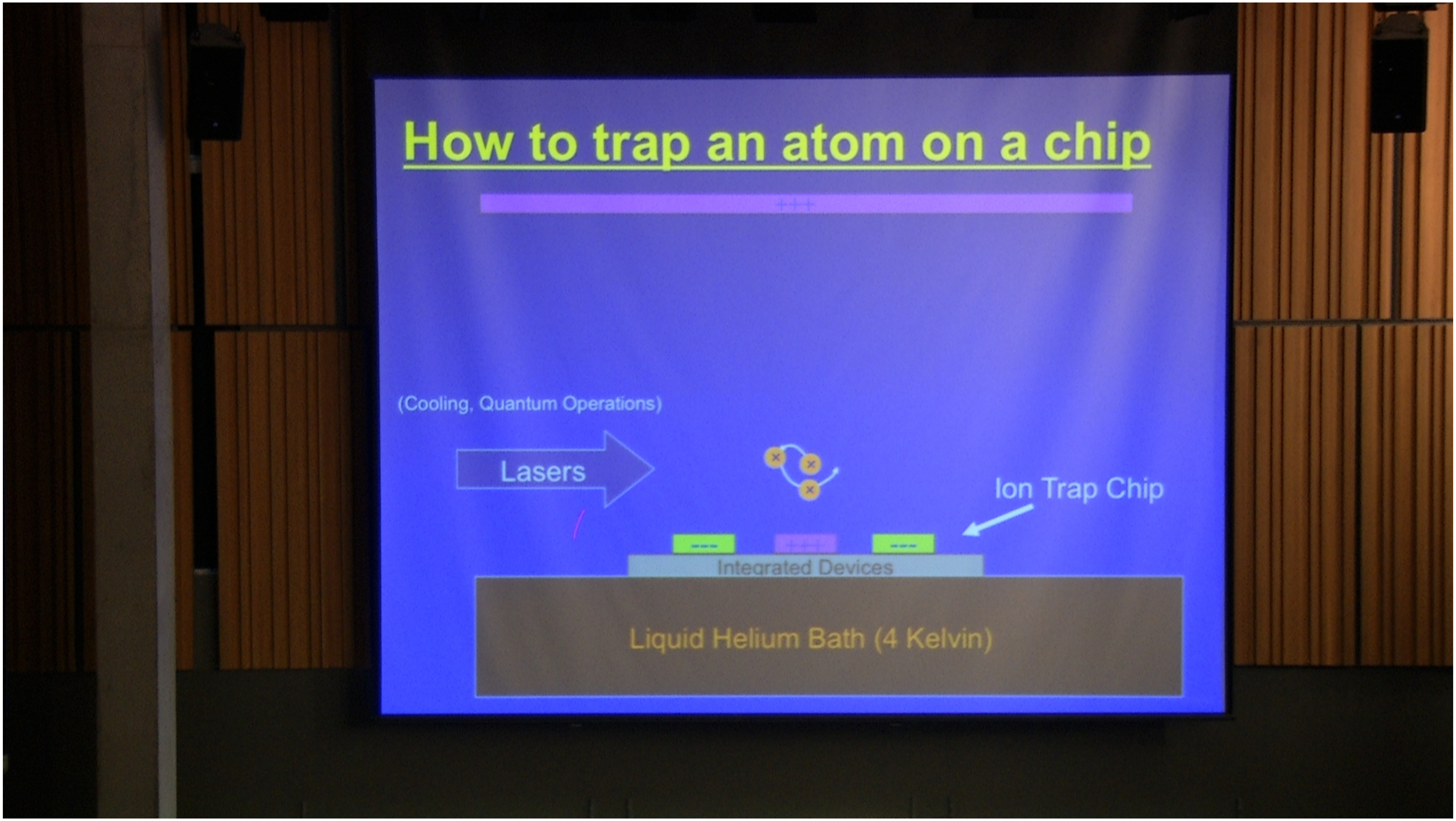
++++

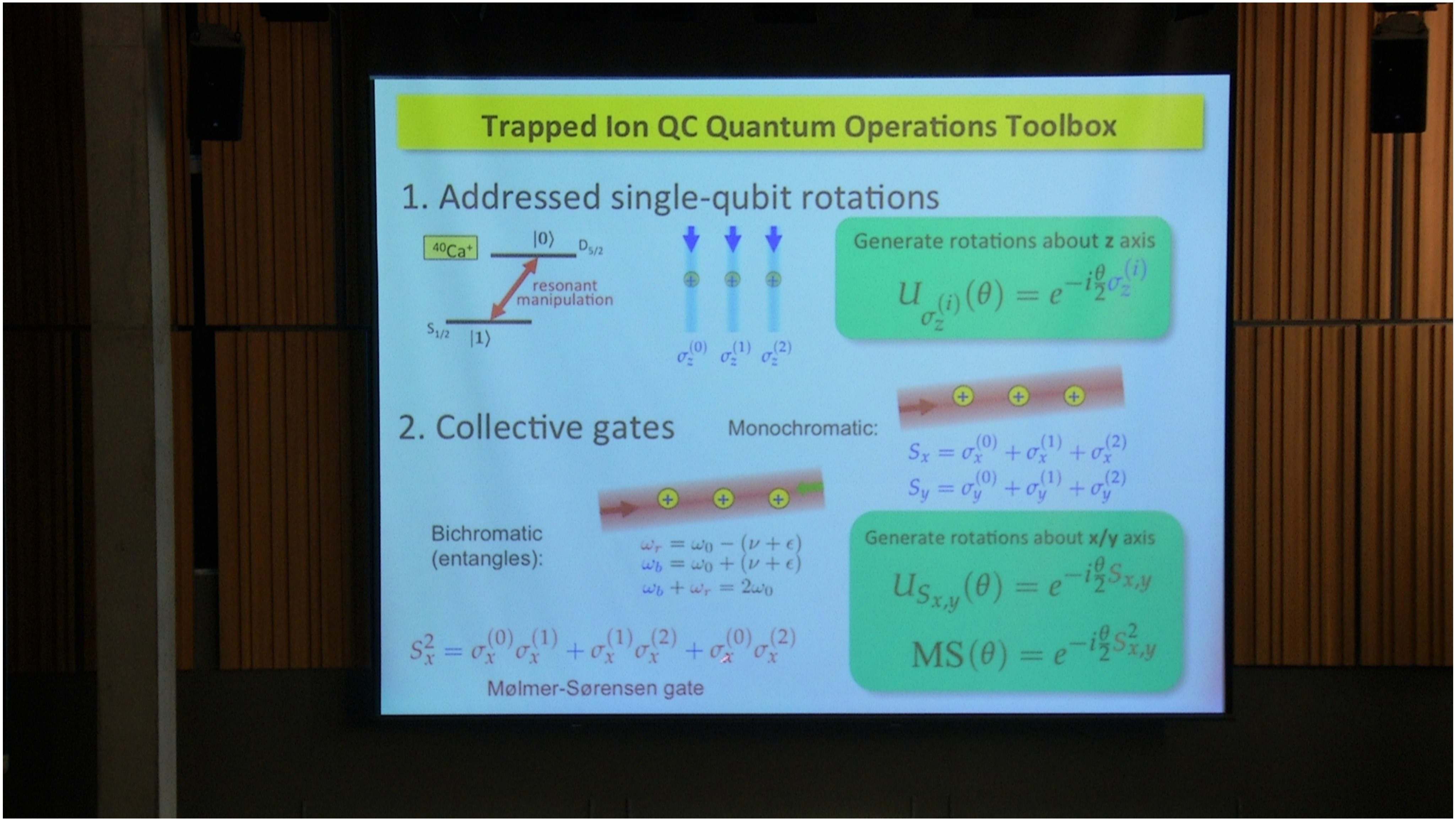
Integrated Devices
Liquid Helium Bath (4 Kelvin)


How to trap an atom on a chip
+++
(Cooling, Quantum Operations)
Lasers
Ion Trap Chip

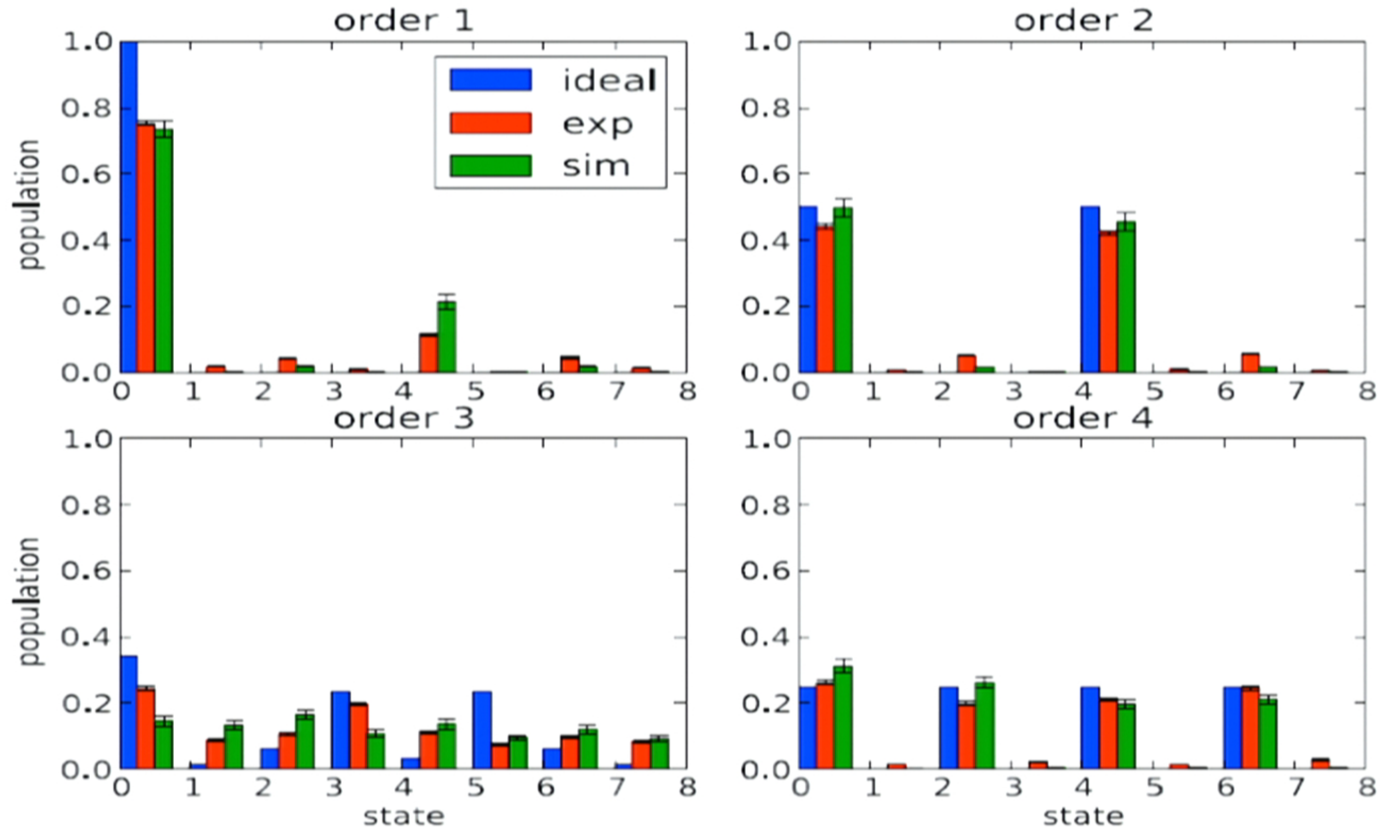
+++

Integrated Devices
Liquid Helium Bath (4 Kelvin)


How to trap an atom on a chip
(Cooling, Quantum Operations)
Lasers
Ion Trap Chip
Integrated Devices
Liquid Helium Bath (4 Kelvin)

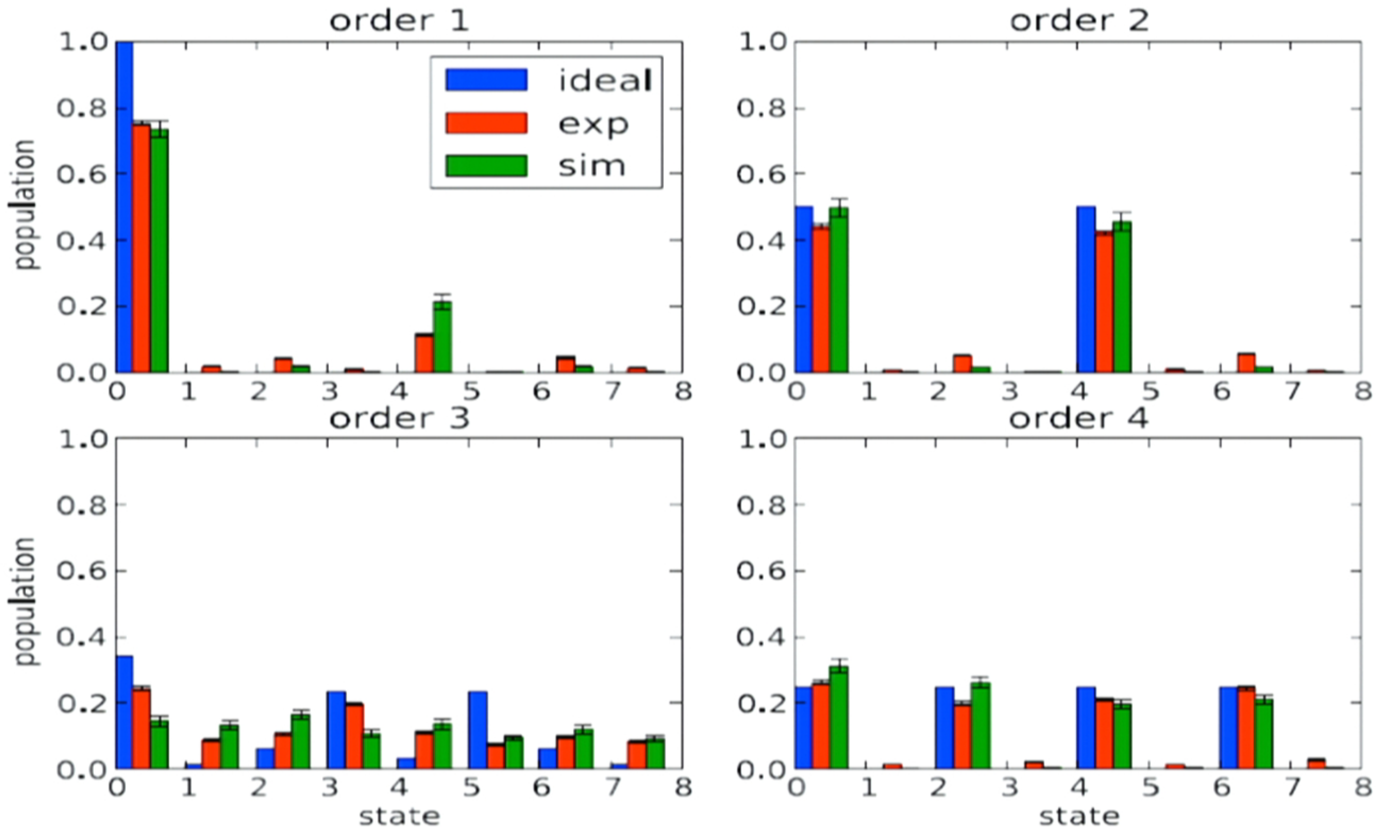

Trapped Ion QC Quantum Operations Toolbox
1. Addressed single-qubit rotations
40Ca+
|0⟩
D5/2
resonant
manipulation
S1/2
|1⟩
Generate rotations about z axis
2. Collective gates
Monochromatic:
Bichromatic
(entangles):
Generate rotations about x/y axis
Mølmer-Sørensen gate

Challenge 4: Predicting Scaling → TIQC-SPICE

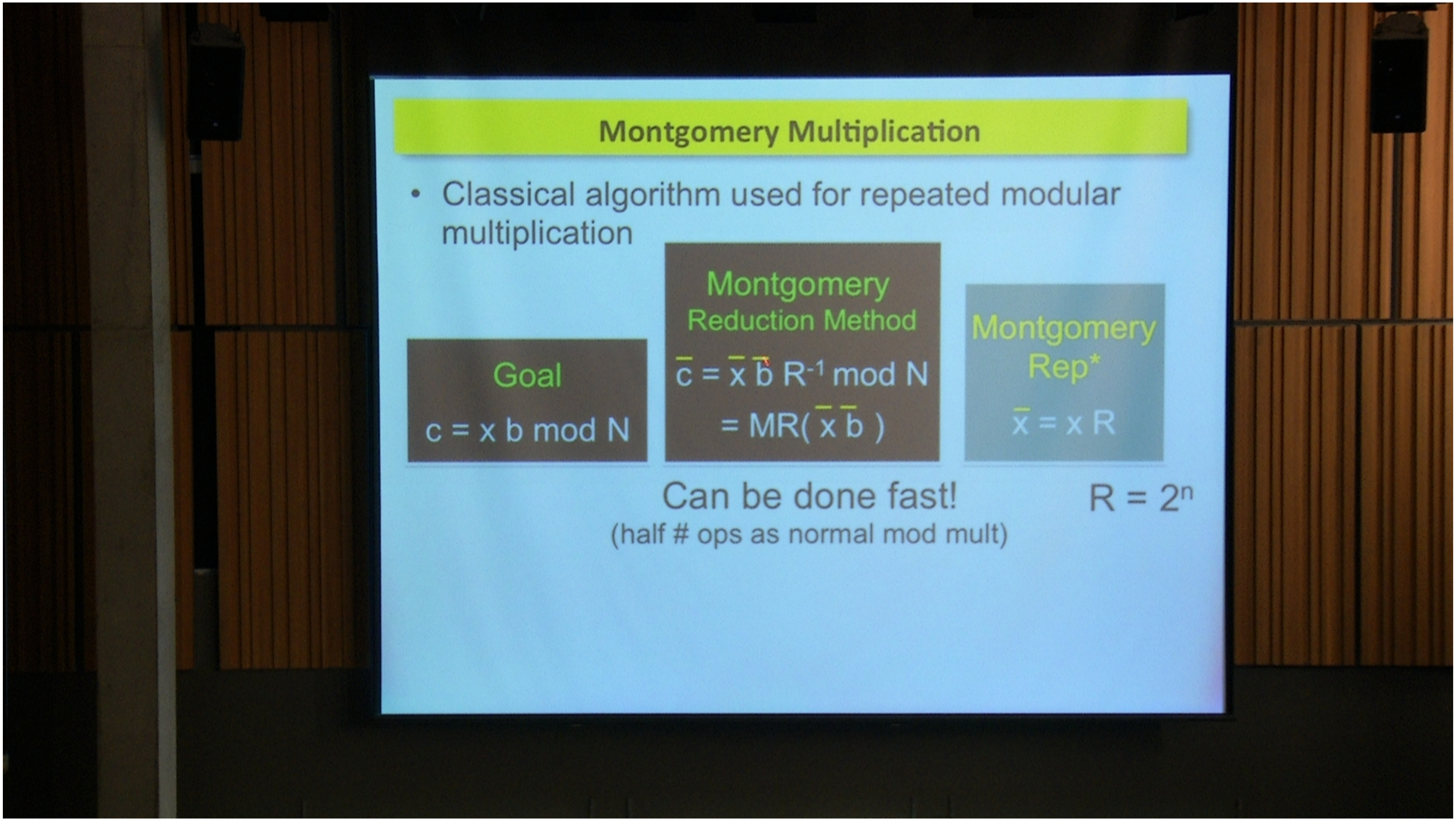


No fit parameters!! Entirely based on system calibration

Challenge 4: Predicting Scaling → TIQC-SPICE



No fit parameters!! Entirely based on system calibration


Montgomery Multiplication
• Classical algorithm used for repeated modular multiplication
Goal
$c = x\, b \bmod N$
Montgomery
Reduction Method
$\bar{c} = \bar{x}\, \bar{b}\, R^{-1} \bmod N$
$= MR(\bar{x}\, \bar{b})$
Montgomery
Rep*
$\bar{x} = x\, R$
Can be done fast!
(half # ops as normal mod mult)
$R = 2^n$

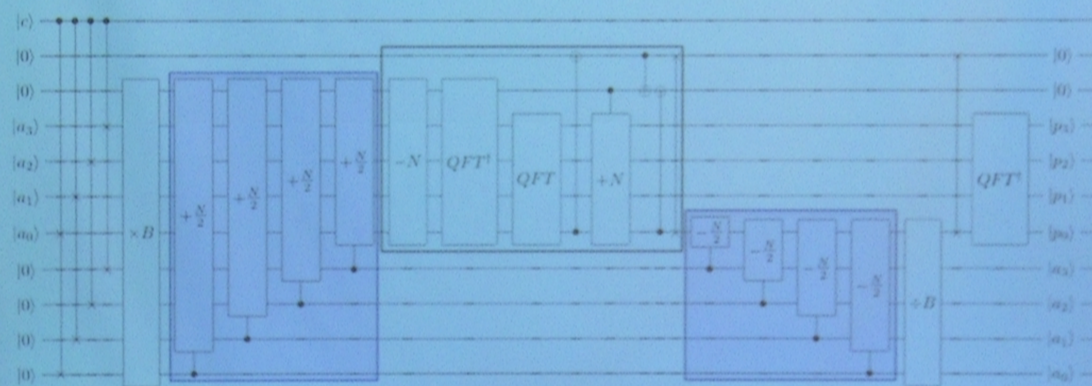
Quantum Fourier Montgomery Multiplication (QFMM)

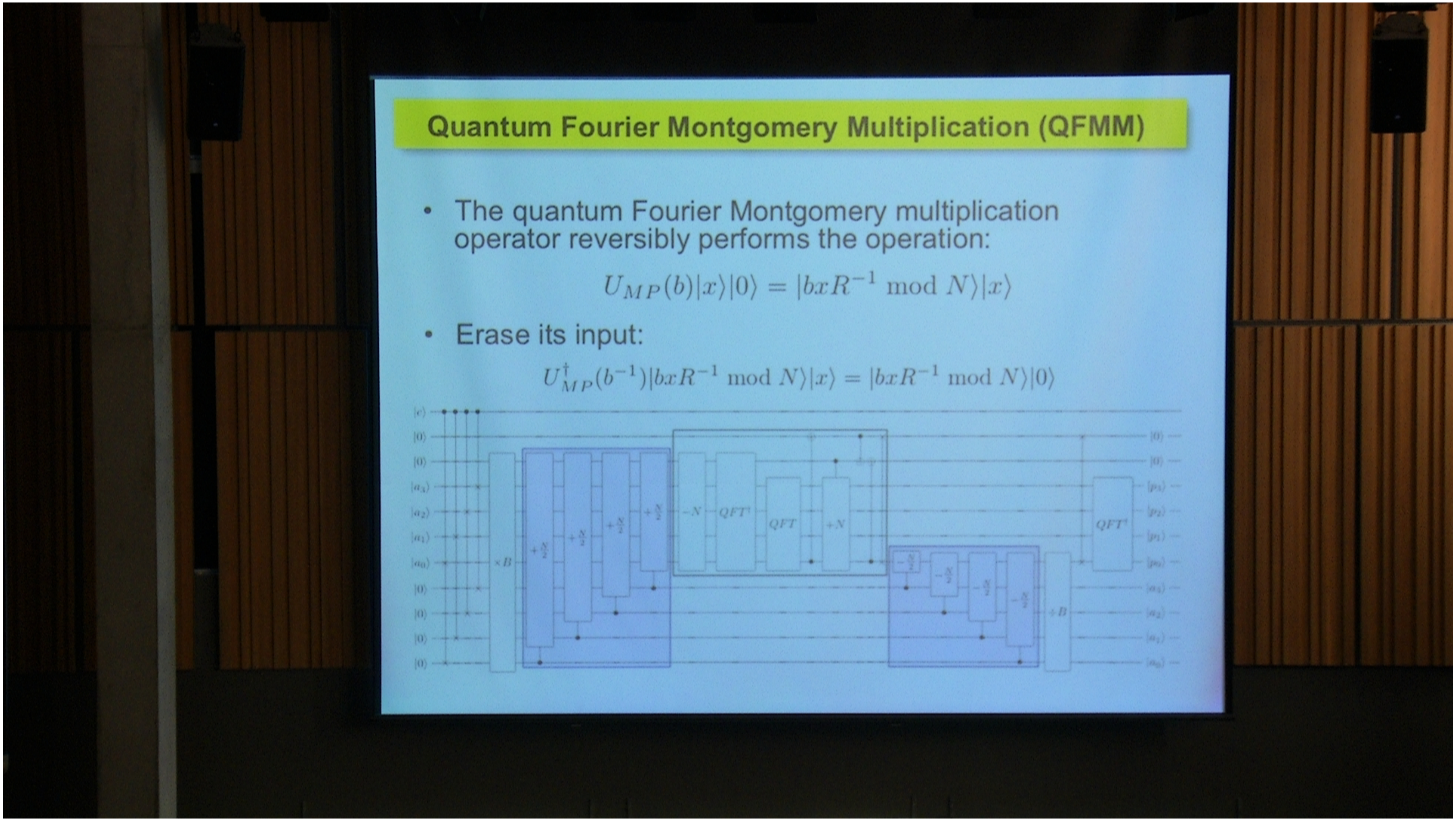
- The quantum Fourier Montgomery multiplication operator reversibly performs the operation:

$$U_{MP}(b)|x\rangle|0\rangle = |bxR^{-1} \bmod N\rangle|x\rangle$$

- Erase its input:

$$U^{\dagger}_{MP}(b^{-1})|bxR^{-1} \bmod N\rangle|x\rangle = |bxR^{-1} \bmod N\rangle|0\rangle$$




Quantum Fourier Montgomery Multiplication (QFMM)
• The quantum Fourier Montgomery multiplication operator reversibly performs the operation:
$U_{MP}(b)|x\rangle|0\rangle = |bxR^{-1} \bmod N\rangle|x\rangle$
• Erase its input:
$U^{\dagger}_{MP}(b^{-1})|bxR^{-1} \bmod N\rangle|x\rangle = |bxR^{-1} \bmod N\rangle|0\rangle$
QFT
QFT
QFT†
+N
−N
×B
÷B

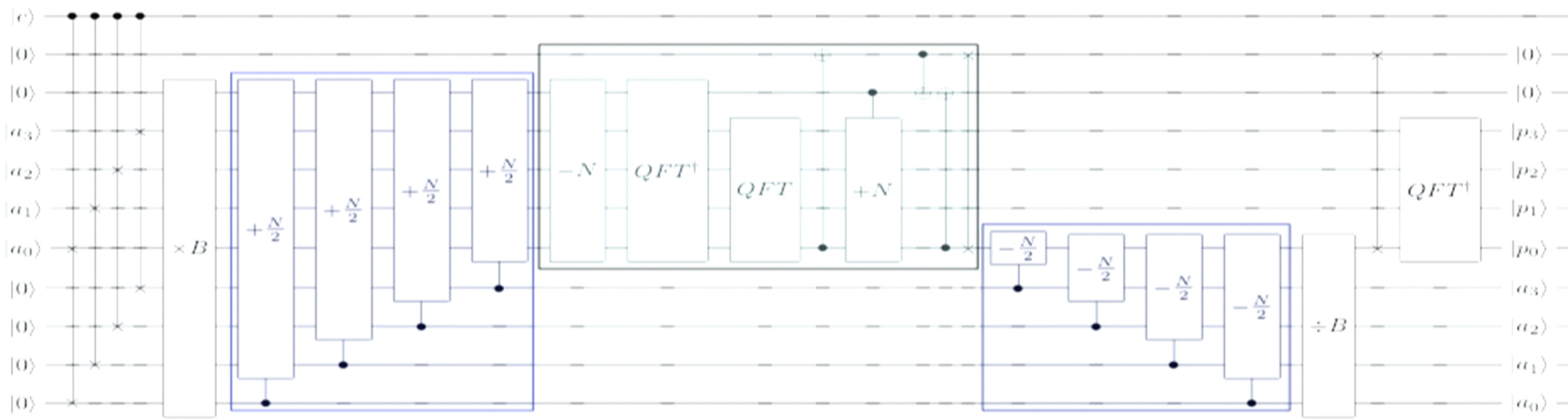
Quantum Fourier Montgomery Multiplication (QFMM)

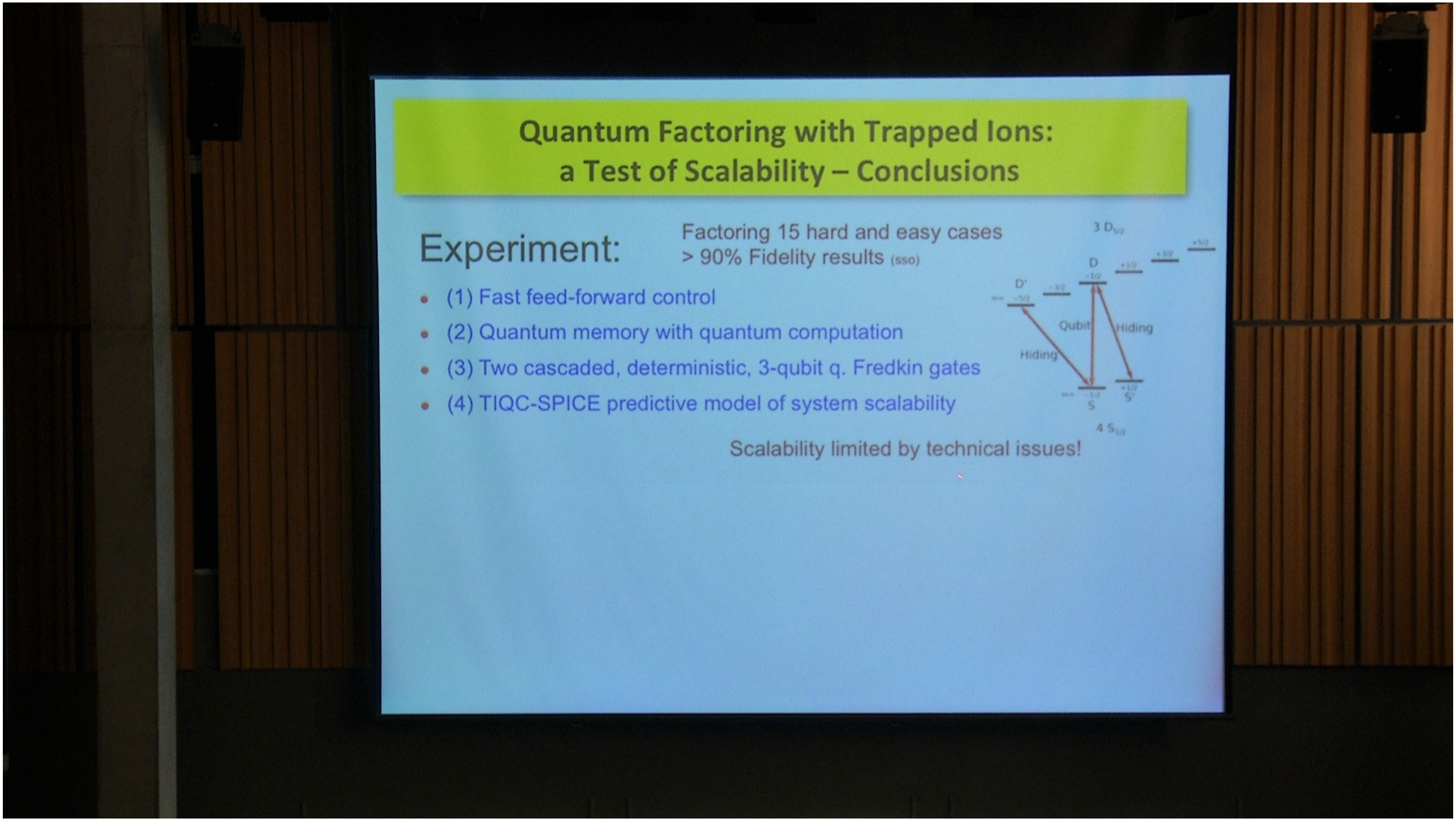
- The quantum Fourier Montgomery multiplication operator reversibly performs the operation:

$$U_{MP}(b)|x\rangle|0\rangle = |bxR^{-1} \bmod N\rangle|x\rangle$$

- Erase its input:

$$U^{\dagger}_{MP}(b^{-1})|bxR^{-1} \bmod N\rangle|x\rangle = |bxR^{-1} \bmod N\rangle|0\rangle$$




Quantum Factoring with Trapped Ions:
a Test of Scalability – Conclusions
Experiment:
Factoring 15 hard and easy cases
> 90% Fidelity results (sso)
(1) Fast feed-forward control
(2) Quantum memory with quantum computation
(3) Two cascaded, deterministic, 3-qubit q. Fredkin gates
(4) TIQC-SPICE predictive model of system scalability
Scalability limited by technical issues!
3 D5/2
D
D'
Qubit
Hiding
Hiding
S
S'
4 S1/2