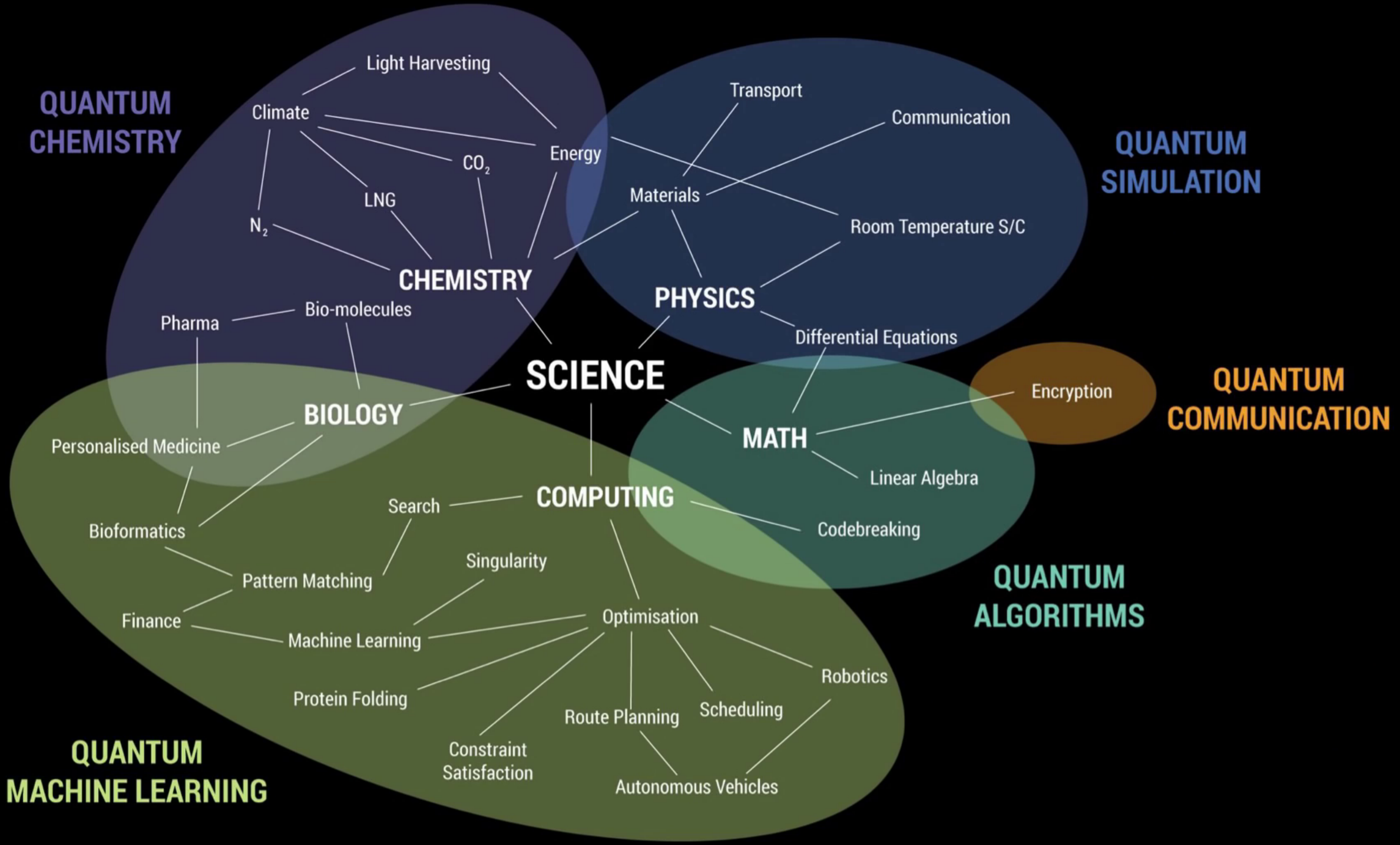
SCAsia 2019
Supercomputing
Gathering the Best of HPC in Asia

Cambridge
Quantum
Computing

IronBridge and Quantum Encryption

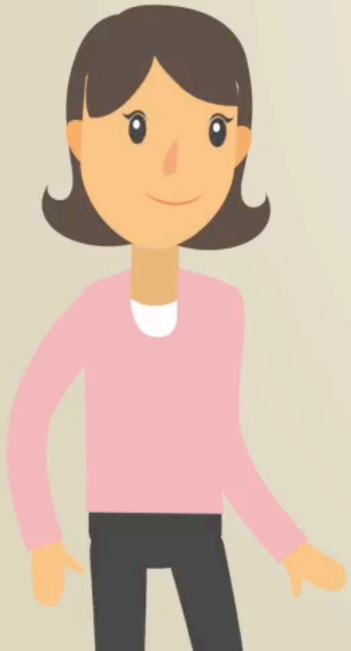
Mark Jackson, Ph.D.

14 March 2019


QUANTUM CHEMISTRY
Light Harvesting
Climate
Energy
CO_2
LNG
N_2
CHEMISTRY
Pharma
Bio-molecules
Transport
Communication
Materials
Room Temperature S/C
PHYSICS
Differential Equations
QUANTUM SIMULATION
SCIENCE
BIOLOGY
Personalised Medicine
Bioformatics
MATH
Encryption
Linear Algebra
QUANTUM COMMUNICATION
COMPUTING
Search
Codebreaking
Singularity
Pattern Matching
Finance
Optimisation
Machine Learning
Robotics
Protein Folding
Route Planning
Scheduling
Constraint Satisfaction
Autonomous Vehicles
QUANTUM ALGORITHMS
QUANTUM MACHINE LEARNING

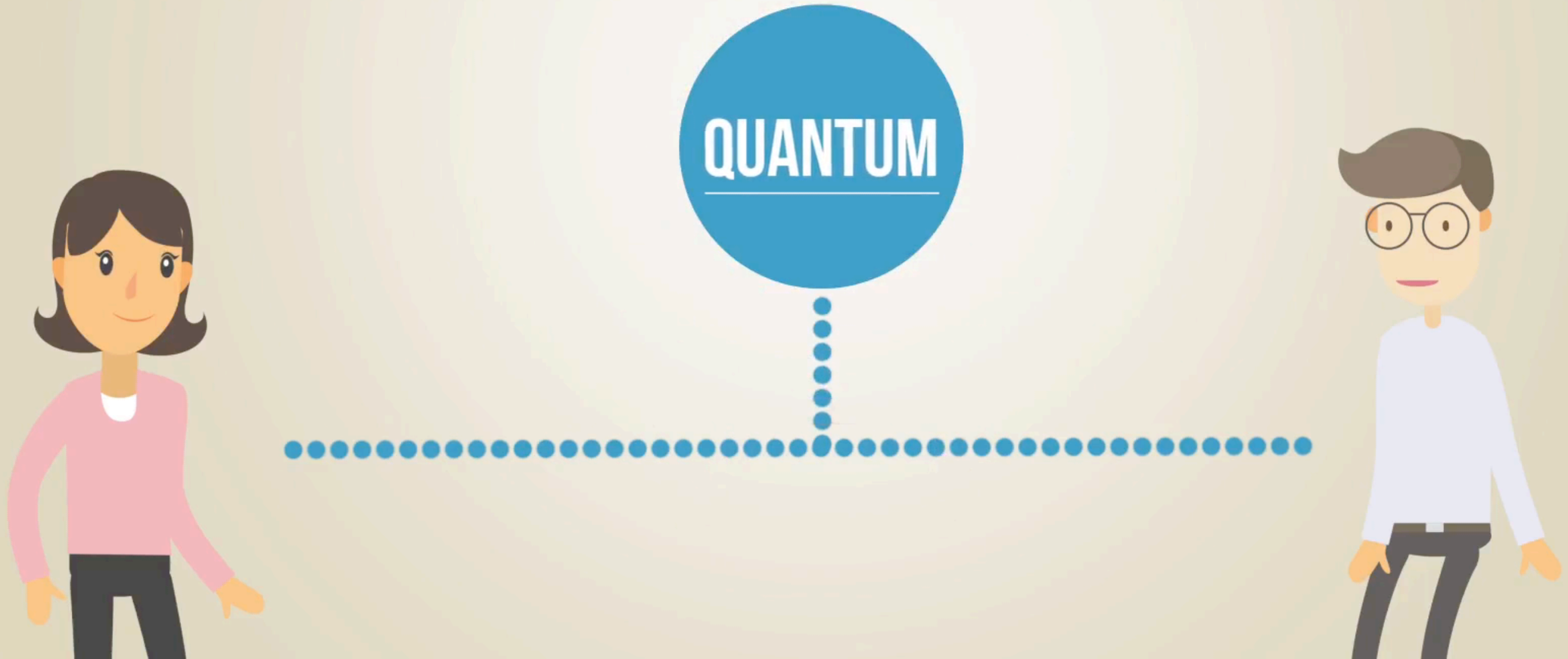
ENCRYPTION

KEY



PROTOCOL

CURRENT ENCRYPTION IS AT RISK



"POST-QUANTUM" ENCRYPTION

QUANTUM

0007635987163019235910928375019836509 1836

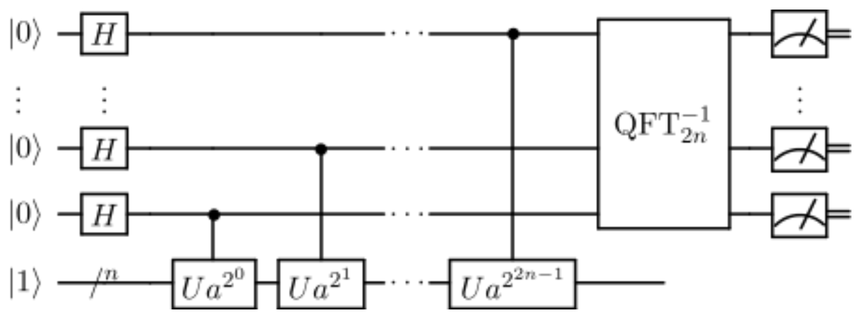
Shor's Algorithm

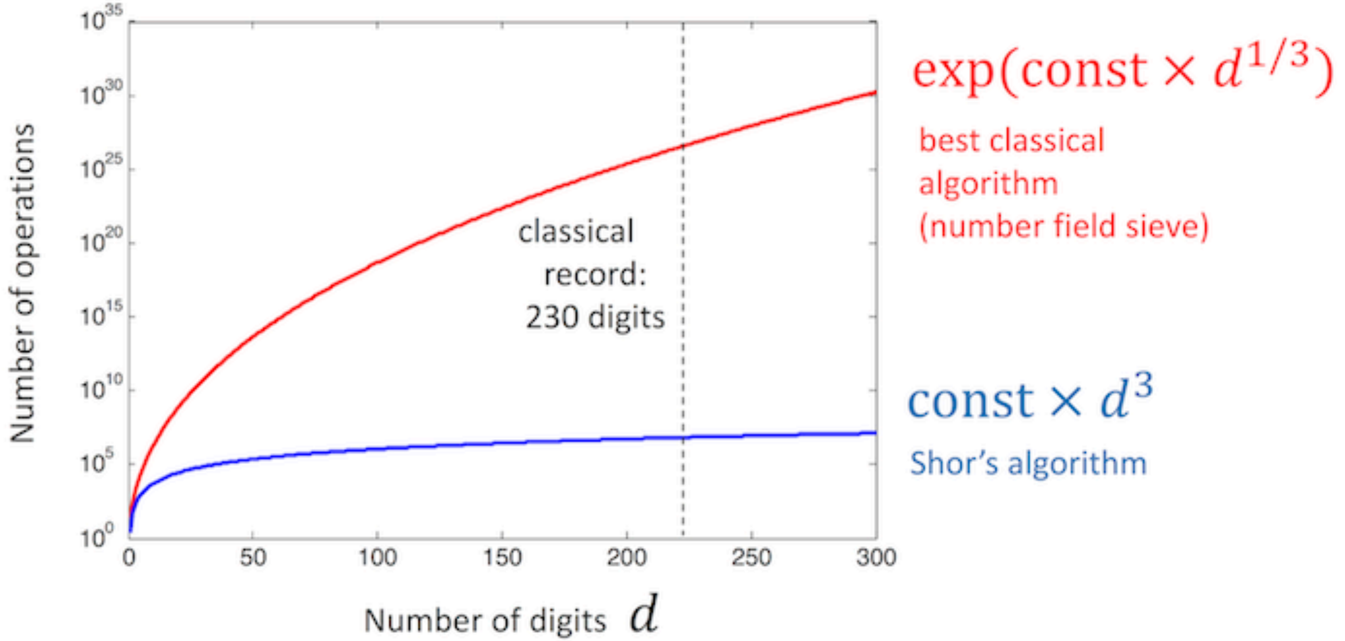
In 1994 Peter Shor discovered a very important quantum program: decomposing integers into its prime factors

easy (multiplying) →

433 x 937 = 405,721

← hard (factoring)





Post-Quantum Encryption

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

} 99% of online encryption

QUANTUM-SECURE

Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).

Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate cryptography

These schemes rely on the hardness of solving systems of multivariate polynomial equations.

NIST: National Institute for Standards and Technology

Meter

Second

Peanut Butter…?

January 30, 2019

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals’

April 11, 2018

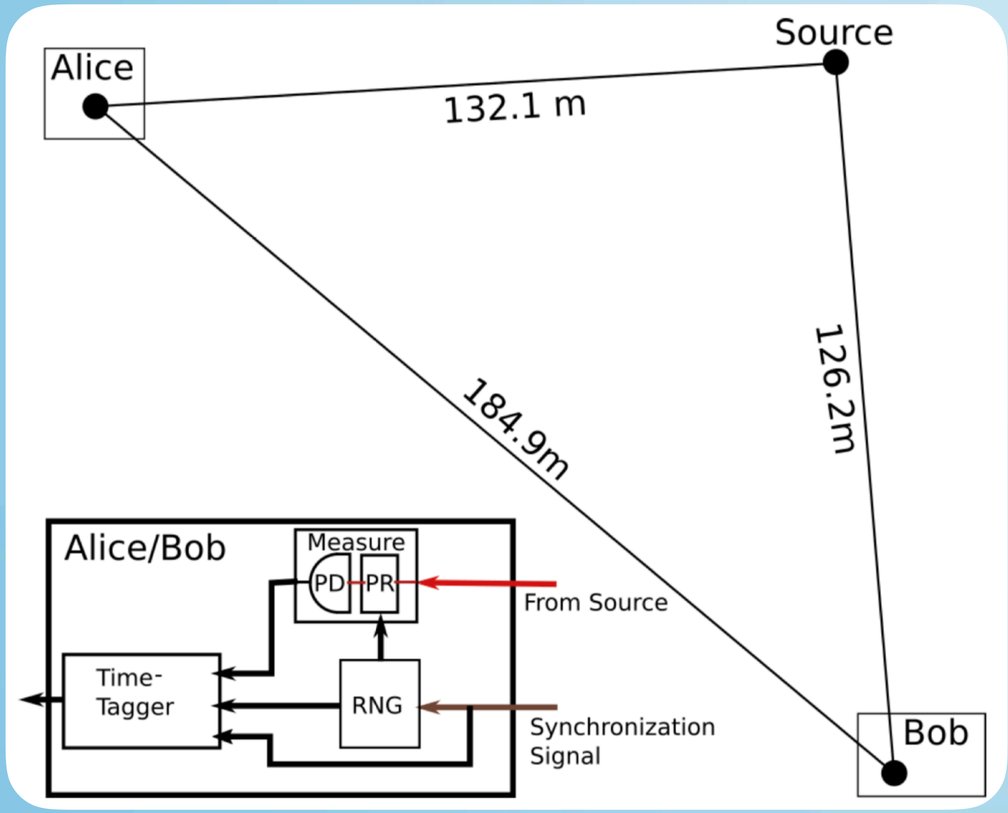
NIST’s New Quantum Method Generates *Really* Random Numbers

Producing Certifiably Random Numbers

Credit: Center for Quantum Technologies

Two problems with NIST's approach:

1) Alice and Bob need be **260 meters apart**



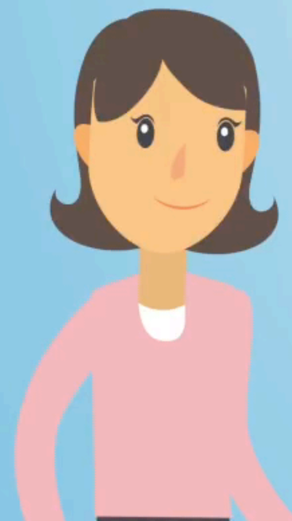
2) 132,000,000 trials - **over 4 days** - required to generate **256 random numbers**

IronBridge

Absolute Security

SECURITY AGAINST

QUANTUM HACKING THREATS

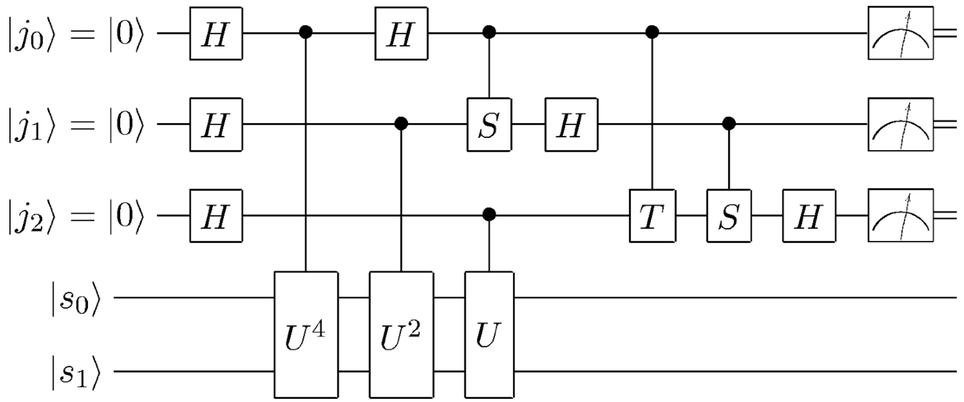


13964 13964 13964 13964 13964 13964 13964 13964

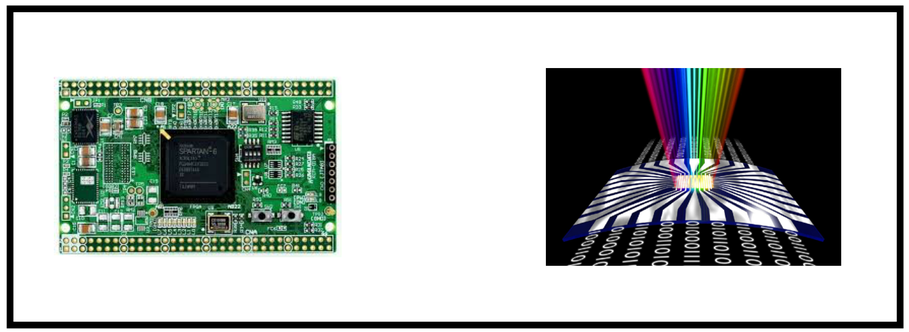
IronBridge: Encryption through Certifiable qRNG

1) Server-rack device
   Entangled photonics
   ~16 Mbps

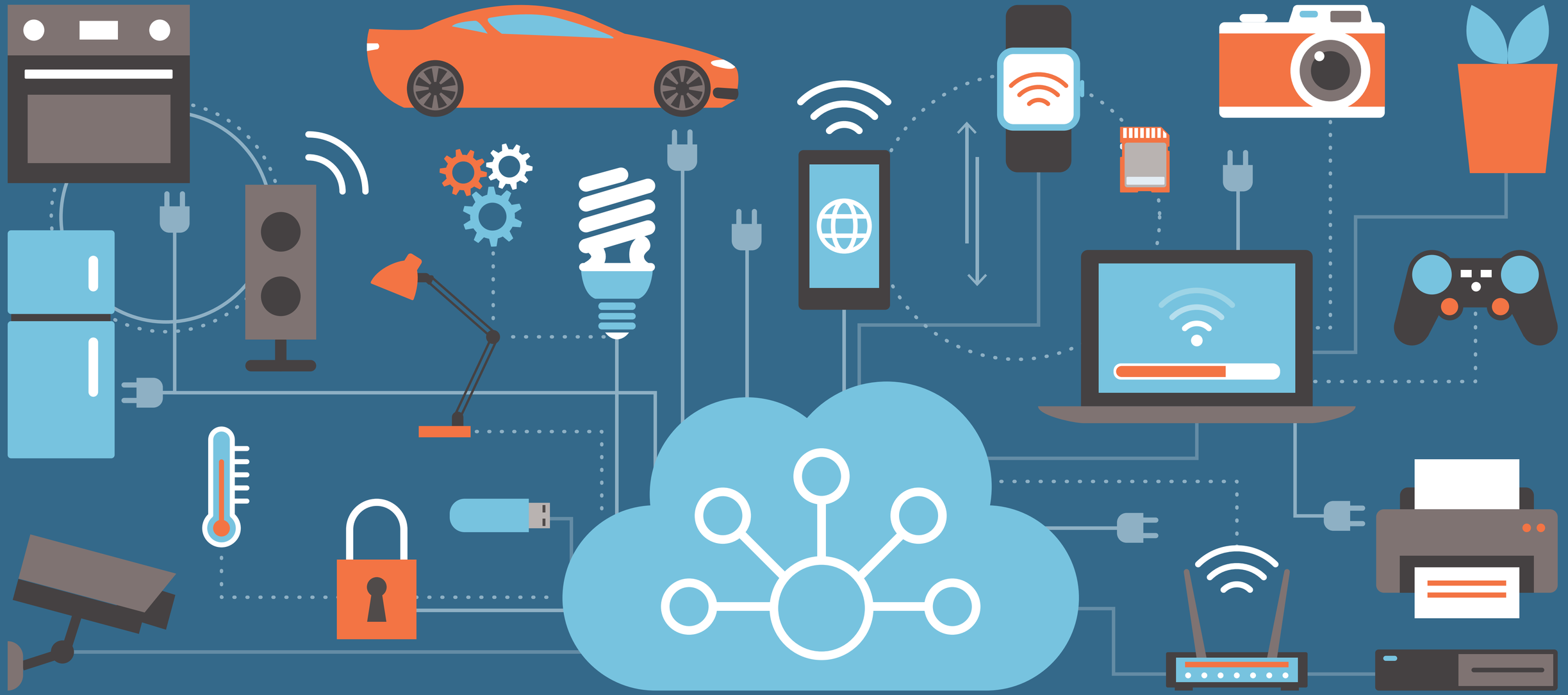
2) Quantum circuit



3) Custom Implementation
   via FPGA



Internet of Things

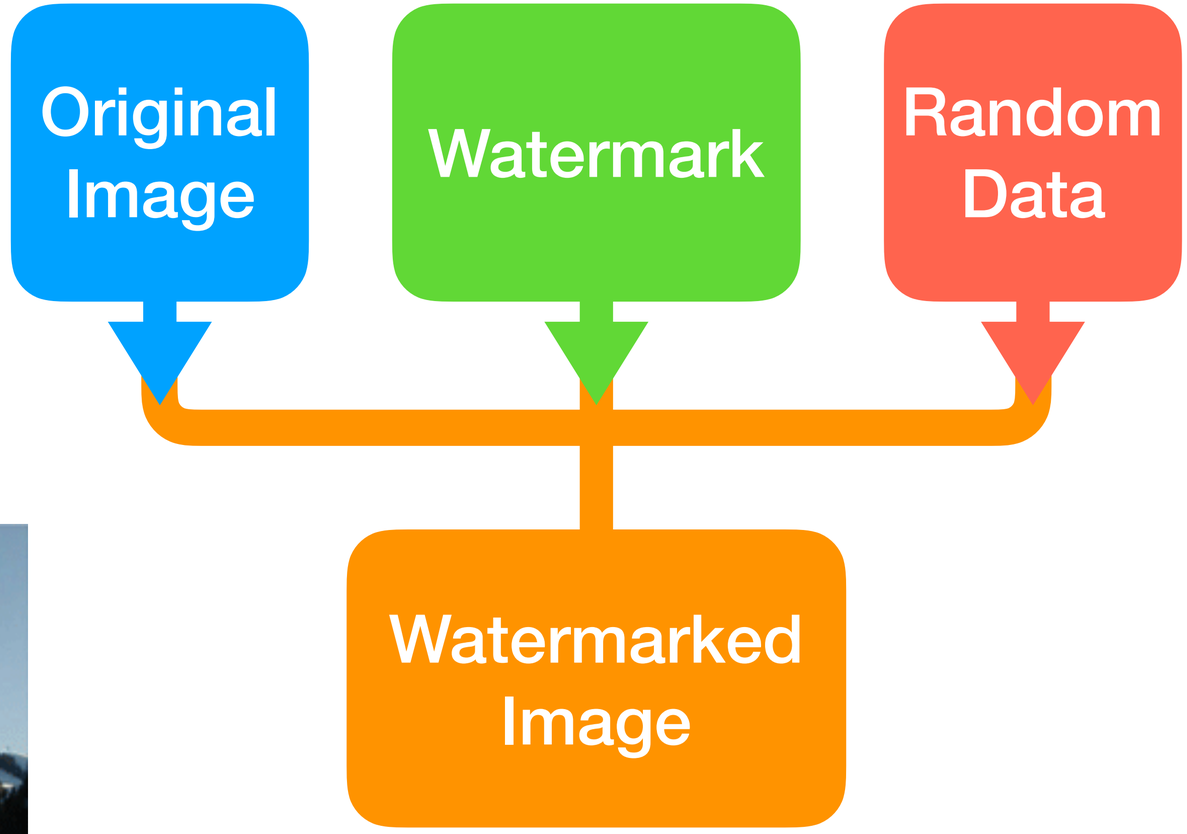



5G

Watermarking

Original

Watermarked



Watermarking Applications

Photo & Video Piracy

E-Contracts

Health Care Data

Cambridge Quantum Computing

- Cambridge Quantum Computing combining expertise in quantum encryption/security, machine learning, compilers, and chemistry
- We design solutions that will utilize quantum computing even in its earliest forms
- Leading Quantum Readiness Program in UK

London

Cambridge

Hong Kong

Berkeley

Washington

Tokyo

Bloomberg Business Innovators 2016

CB INSIGHTS