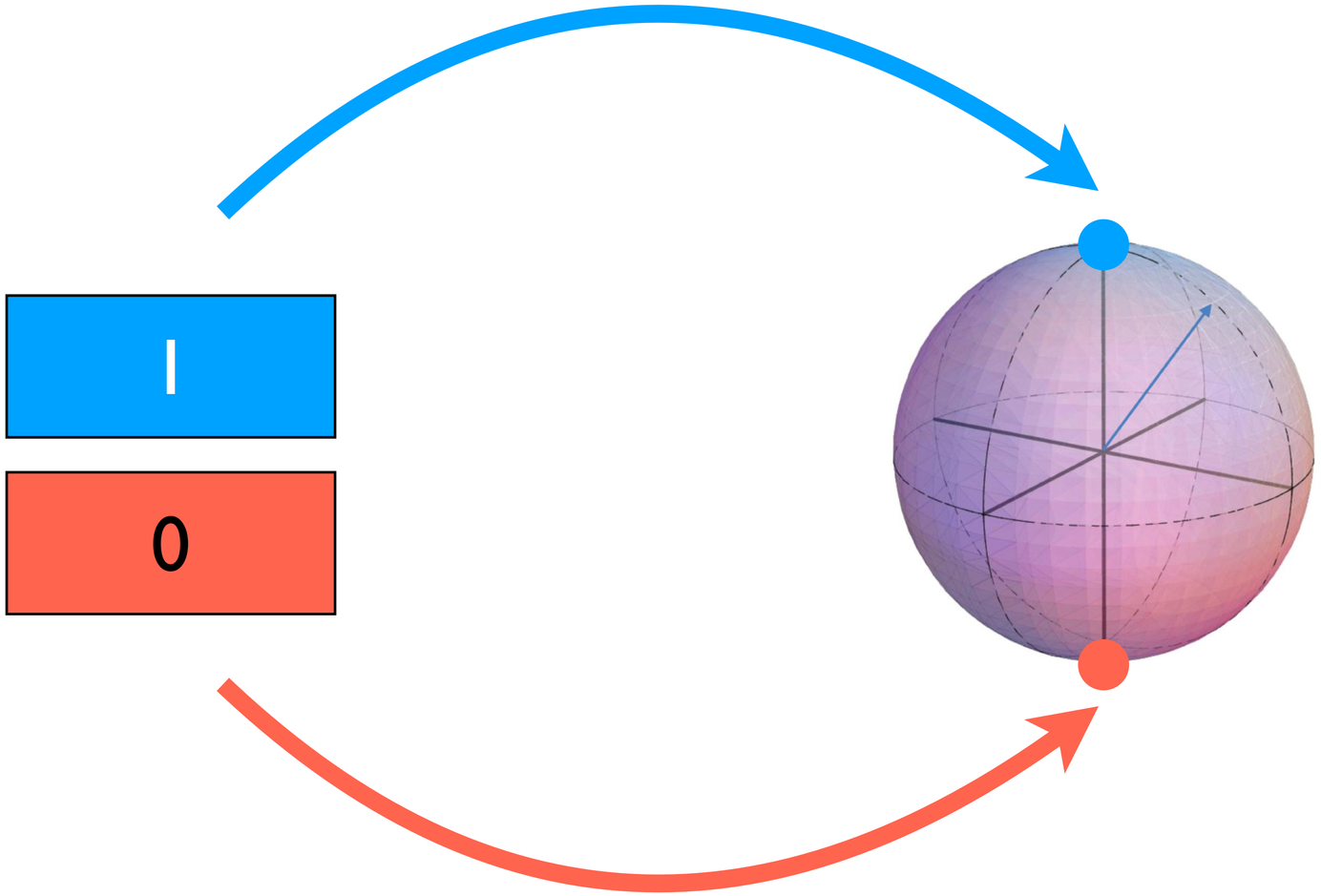
Cambridge Quantum Computing

Quantum Computing and the Future of Content Security

Mark Jackson, Ph.D.

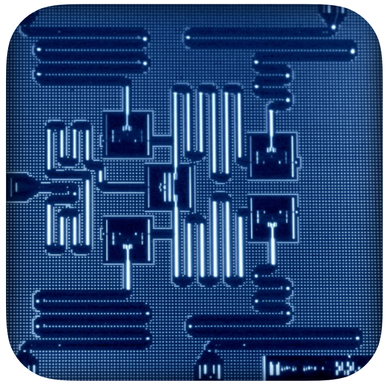
7 April 2019

Bit becomes Quantum Bit



Currently 80+ Quantum Computing Hardware Groups

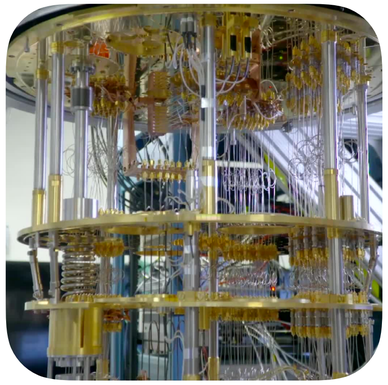
Google



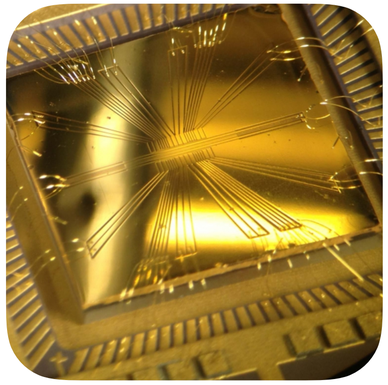
IBM

intel

Microsoft

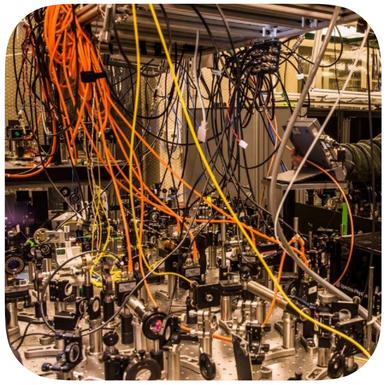


rigetti

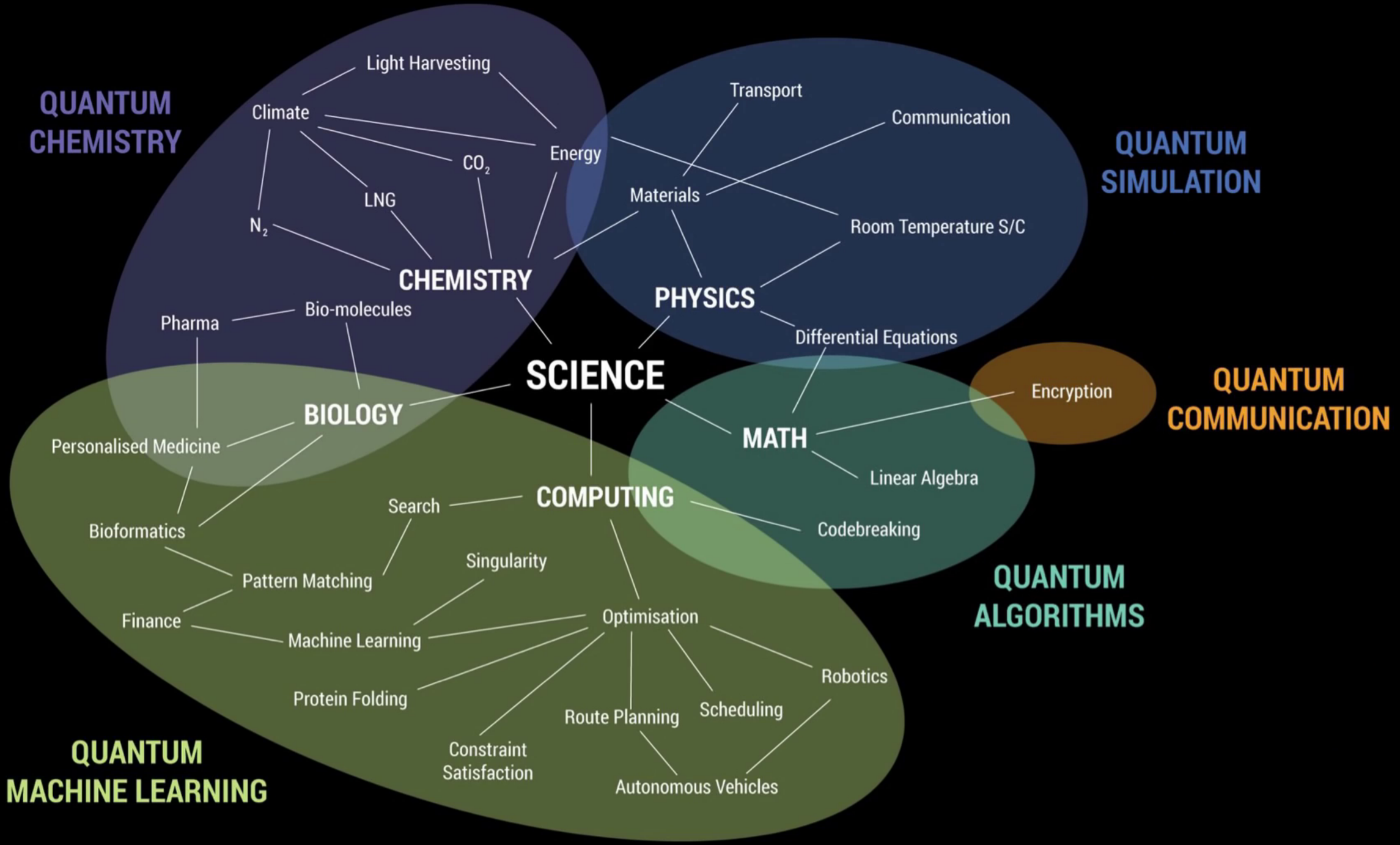


NQIT

Honeywell

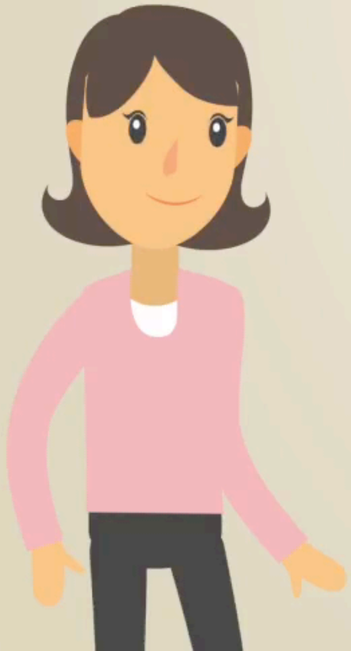


IONQ


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

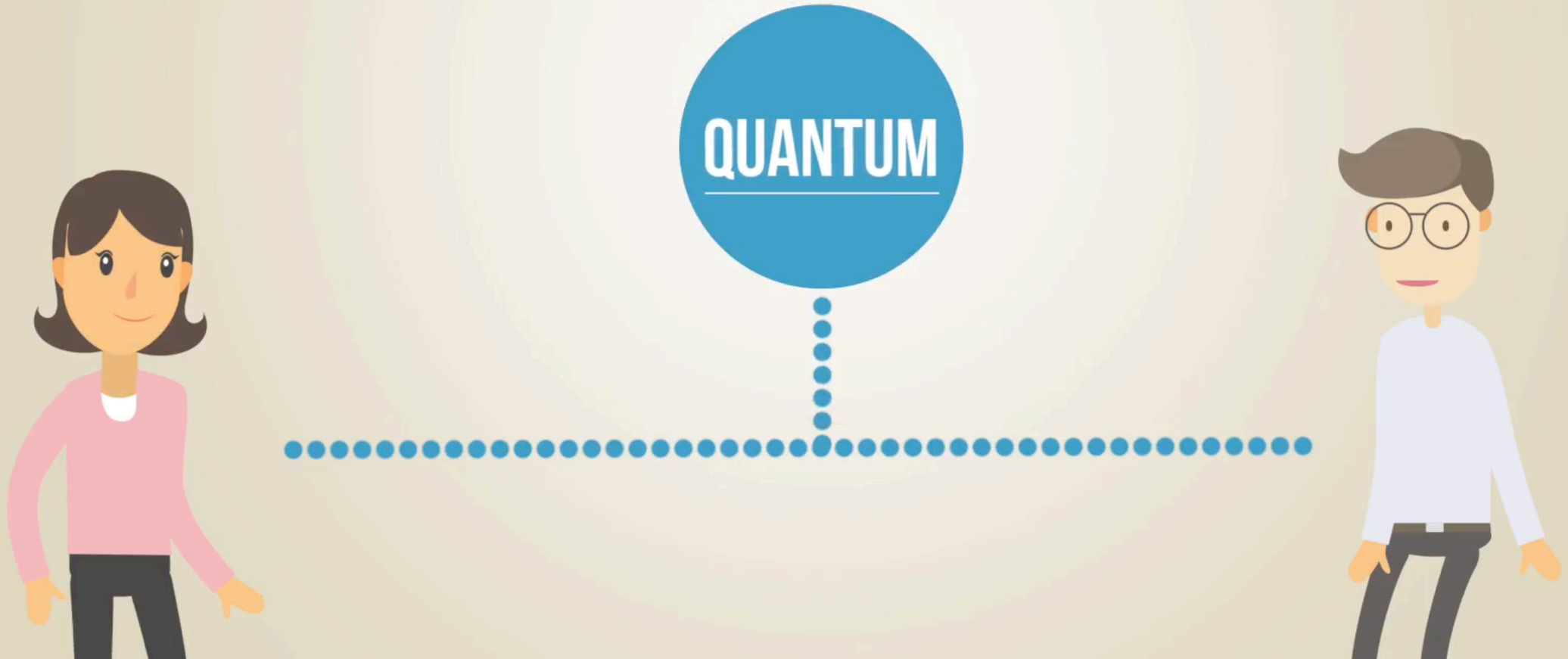
ENCRYPTION

KEY



PROTOCOL

CURRENT ENCRYPTION IS AT RISK



Post-Quantum Encryption

QUANTUM-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

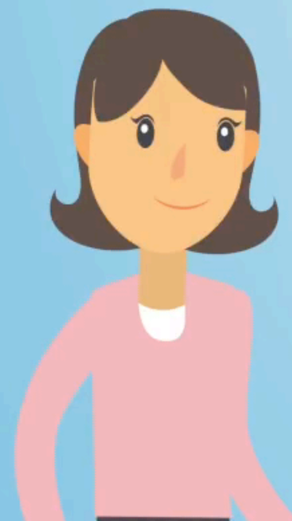
These schemes rely on the hardness of solving systems of multivariate polynomial equations.

IronBridge

Absolute Security

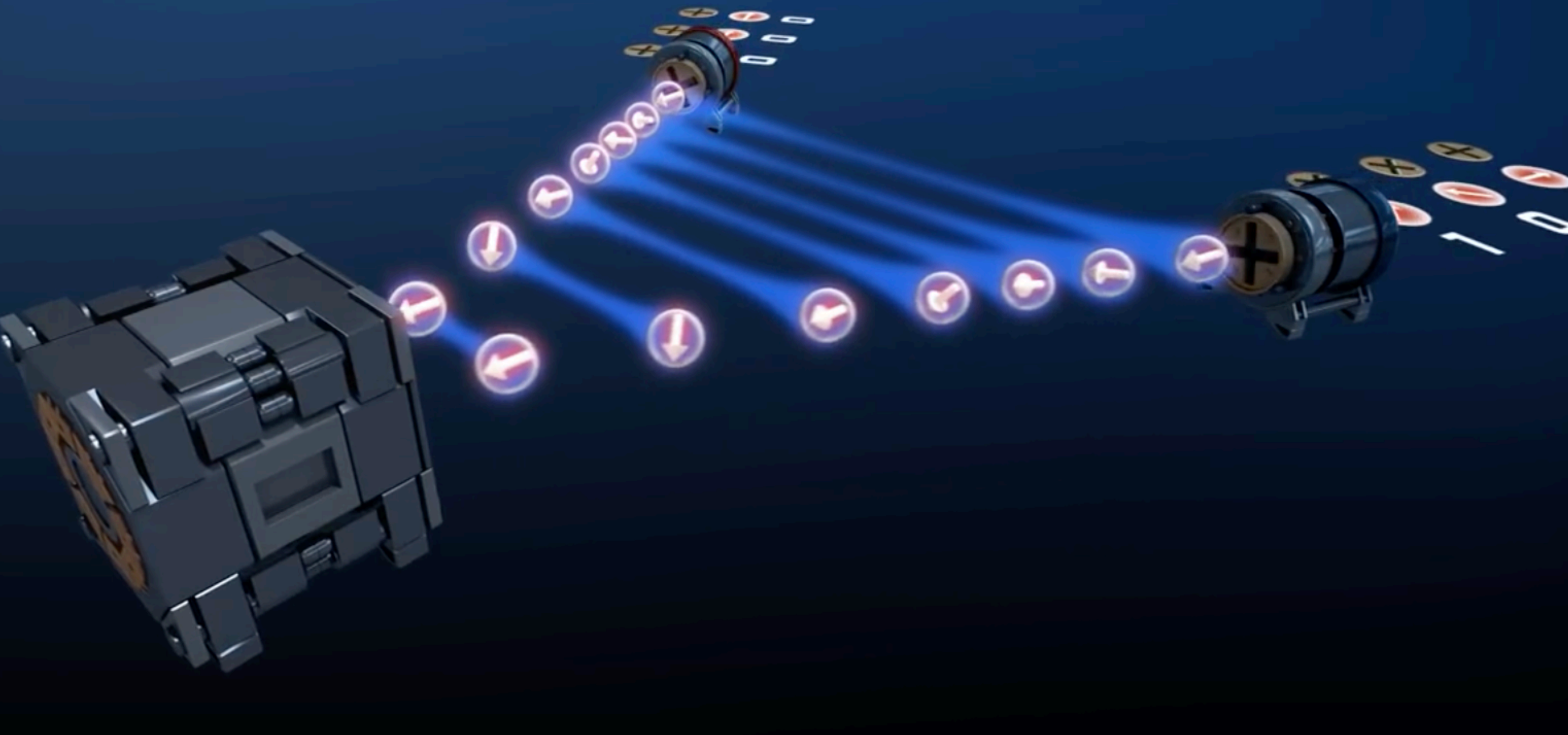
SECURITY AGAINST

QUANTUM HACKING THREATS



13964 13964 13964 13964 13964 13964 13964 13964

Quantum Entanglement

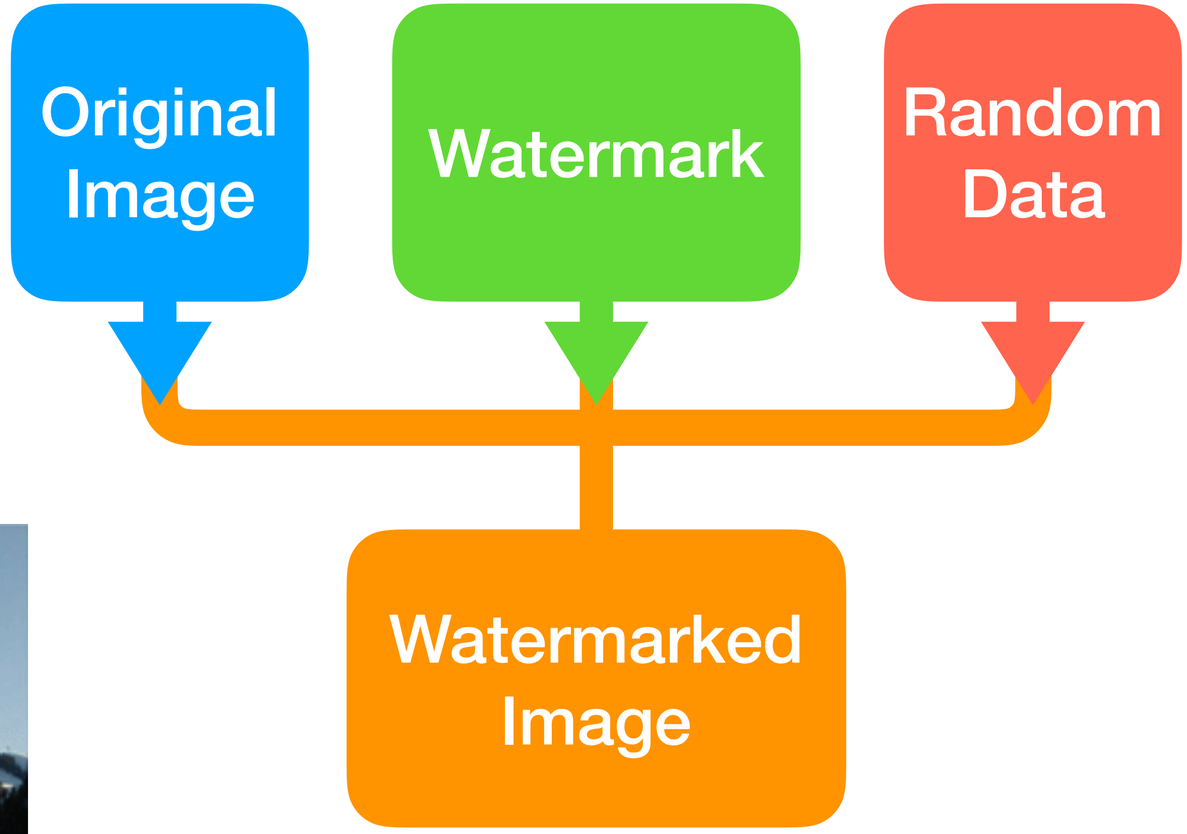



PKI Automation
for Mixed Endpoint Environments
FEITIAN
WE BUILD SECURITY
www.ftsafe.com
CenturyLink
GlobalSign
Email
Server Comms
Smart Devices
Mobile
Users
Code
10100
00011
10100
Documents
Data Transmissions
Servers
bridge Quantum
puting
Cambridge
Quantum
Computing
QE SYSTEM
EXHIBITOR

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