Law and Policy for the Quantum Age

Chris Jay Hoofnagle

UC Berkeley
School of Law
LIR series Technology, Law, and Society

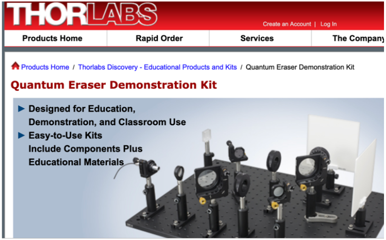
March 8, 2020

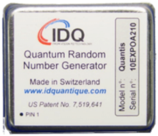
QIS project

- Joint work with Simson Garfinkel
- Forthcoming as Law and Policy for the Quantum Age (Cambridge U Press 2020)
- I am not a physicist
- Quantum Information Science (QIS)
- Quantum technologies (QT)
  - Metrology & sensing
  - Communications
  - Computing
- What policy choices?

QT: why now?

- China & EU investment explicitly to leapfrog over U.S.
    - Major scientific advances at TU-Delft (Microsoft)
    - U.S. response: $1.2bn authorized
    - Limit is talent
- Electronic warfare / MASINT
- Tech fundamentals easier: commercial products can produce quantum effects
- Some quantum effects do not require supercooling





Quantis RNG OEM component

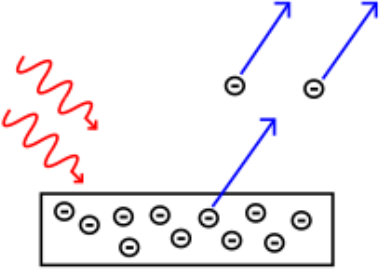
- Highly resilient to environmental perturbations
- Designed for mounting on PCB for embedded systems
- Instant entropy with high bit-rate of 4Mbits/sec
- Affordable, compact and reliable
- Uses quantum optic process to create true quantum randomness

Quantum effects

- Merger of quantum mechanics and information theory
- At quantum scales, nature is probabilistic and objects have attributes of both waves and particles
  - Nitrogen atoms used for sensing have a diameter of 1.12Å —alternatively a radius of 56 picometers (pm), 0.056 nanometers (nm) or 5.6 x 10^{-11} meters.

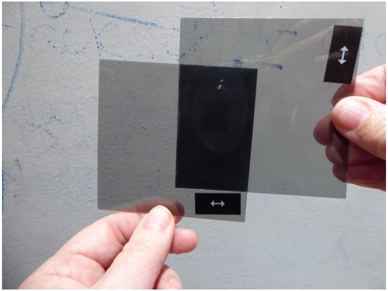
Waves and Particles

These colors are created by interference between two wave fronts: the light reflecting off the front side and the back side of the soap film.

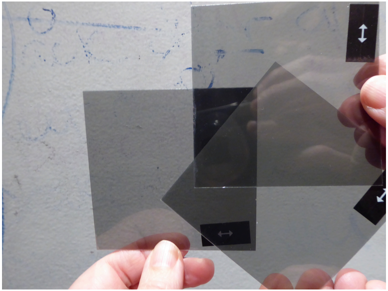


Yet, the Suns ultra-violet light can dislodge electrons from the surface of metal, producing a slight voltage, while light from the red end of the spectrum can't

Uncertainty



$\updownarrow \leftrightarrow 0^\circ + 90^\circ =$ all light blocked



$\updownarrow \nwarrow\!\!\!\searrow \leftrightarrow$ Notice the blackest block is $0^\circ + 90^\circ$; introducing $45^\circ = 12\%$ transmission!

Three quantum effects underly QT

- Superposition
  - Particles can be in an indeterminate state–0 or 1 or between
- Entanglement
  - When particles are entangled, measurement of one causes the other to act in a predictable fashion, even when separated by great distances
- No cloning
  - At quantum scales, "observation" is a physical act that influences the quantum state

Quantum sensing

- Most mature QT
  - Atomic clocks, MRI, NMR measure quantum effects
  - Most commonly rely on quantum entanglement and superposition
- Some do not require supercooling
- Nitrogen vacancy chambers as a promising medium
  - These are imperfections in diamonds, places where a single nitrogen atom is trapped by the strong bonds of neighboring carbon atoms
  - The nitrogen atom can be manipulated to produce quantum effects, even at room temp
  - Shining a laser at the nitrogen atom causes it to emit light that reveals subtle variations in the Earth's magnetic field.

Sensing implications

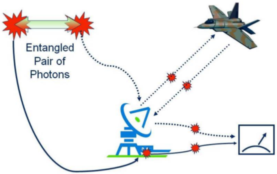
- Electronic warfare driven
- Quantum radar
- Ghost imaging, see through smoke, around corners
- SIGINT to MASINT
- Interferometry

Charting a New Course: Celestial Navigation Returns to USNA

Story Number: NNS151015-27 Release Date: 10/15/2015 3:34:00 PM

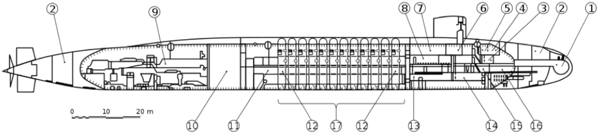
By Lt. j.g. Devin Arneson, U.S. Naval Academy Public Affairs

ANNAPOLIS, Md. (NNS) -- Picture this: A naval vessel is navigating the high seas thousands of nautical miles from land. Suddenly all navigation systems become inoperable. What happens next? What does this mean?



Quantum sonar

- Wu et al (2016) use a magnetic gradient tensor device, a SQUID—superconducting quantum interference device, suspended from a helicopter
- 2000 measurements/second. 1 microsecond time sync between devices in matrix
- If you know the strength and direction of a magnetic field with great precision, what can you find?
  - Mineral deposits, tunnels (including activity in them), infrastructure, hidden matériel
- What does this mean for submarine stealth?

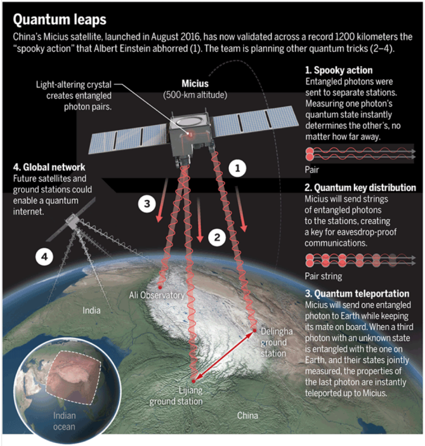


Quantum communication

- Quantum-enhanced classical encryption
    - Quantum key distribution (QKD), because of no cloning, you can tell if your key has been intercepted
    - Quantum random number generation (QRNG), because of quantum randomness, you get enough security to defend against quantum computer cryptanalysis
    - Communication can proceed over standard channels typically with AES
- Quantum communications
    - Uses quantum effects — such as the spin of particles — to communicate information
    - Because of no cloning, one will know if a listener is present
    - Could change the "place" communications happens because of entanglement (but this is still sci fi)

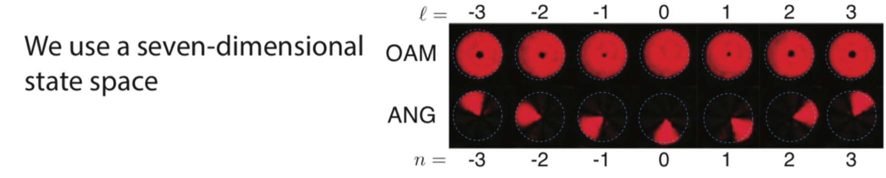
QKD & China

- Relies on entanglement, no cloning
- Distribute AES keys based on quantum randomness, invulnerable to even quantum computers
- Consequential development: China QKD by satellite = OTP distribution
- Strategy to address "pre-positioned devices"
- QKD has been around since the 1990s, why hasn't it taken off commercially?



Quantum internet — 2 fascinating ideas

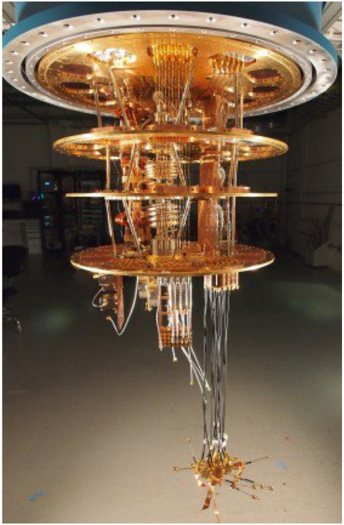
- First, use quantum effects to communicate
- Boyd (University of Rochester) working on photon's spin/orbital momentum to communicate therefore more than 1 bit per photon



- Second, notion of "teleportation"
- We would need quantum memory (to overcome no cloning) + entanglement (Wehner et al. Science 2018)

Quantum computing basics

- Qubit (2^n power)
  - Many kinds — superconducting, trapped ion, photonic, quantum dot
- Three types of QC
  - Simulation
  - Annealers (leader is D-Wave)
  - NISQs
- Uses
  - Possible answer to slowdowns in classical
  - Optimization
  - Simulation of complex physical processes
  - ML
  - Discover nature of P, NP

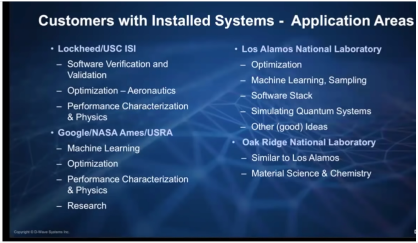


QC Challenges

- QC faces difficult challenges
- Mastery of superposition, entanglement
- Most qubits dedicated to error correction
- Keep an eye on Microsofts “topological qubit” — involves splitting electrons!
- Decoherence measured in microseconds
- Many QCs require supercooling (15 millikelvin)(annealing, superconducting, but not ion traps, photonics)
- Error correction complicated by continuous variables
- + Software, control systems, etc
- Current NISQs will not scale to general purpose computers
- Significant minority warns of quantum winter

Keep an eye on D-Wave's annealer

- Qualified claims: "In half of 150 applications, performance/quality approaching/occasionally better than classical"
- Satellite placement
- Vehicular traffic analysis
- Aircraft gate assignment
- Placement of antennae
- Robot picking in warehouse
- Election modeling



Webinar: Quantum Experiences: Applications and User Projects on D-Wave

Quantum cryptanalysis

- State of the art in factoring
  - 20-bit number using D-Wave 2000 annealer (using 89 qubits) — this is a surprise because annealers were thought to be more limited in function
  - Next gen will have 5,000 qubits
  - 768 bit number using classical computers
- NAS: RSA collapse not likely in the next decade
  - But the problem is transition period to post-Q crypto
- Google: to factor a strong key in a day, "would take 100 million qubits, even if individual quantum operations failed just once in every 10,000 operations."
- Realistic uses (not your CC numbers)

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM [5]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} yrs 1.97×10^{22} yrs 2.29×10^{32} yrs	
RSA [6]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,290 4,338 8,434	2.56×10^6 6.2×10^6 1.47×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[c] [7,8]	Asymmetric encryption	256 386 512	128 192 256	Shor's algorithm	2,330 3,484 4,719	3.21×10^6 5.01×10^6 7.81×10^6	10.5 hours 37.67 hours 95 hours	Move to NIST-selected PQC algorithm when available
SHA256 [9]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations[d]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

QT & Policy

- What policy issues with QTs force us to confront?
- What are the strategic consequences of QT?
- What are the indications/warnings that an adversary possesses QT?
- How is the technology likely to diffuse?
- What QT countermeasures will arise?
- How to foster a QIS workforce?
- Industrial policy
- Privacy

QIS Research

Nation	Estimated Number of Papers
China	8006
US	6071
European Union + national	5819
EU alone	2520
Japan	1491
Canada	1425
UK	894
Germany	785
Foundations	618
Australia	598

Going Deeper?

- Pay attention to the dramatic developments in sensing. these are not as hyped yet are strategically consequential and data intensive
- Find ways to start practicing (remember the talent limit)
  - Academic partners
  - Most basic level: free accounts on D-Wave, IBM
- Post quantum encryption + (AES 256)