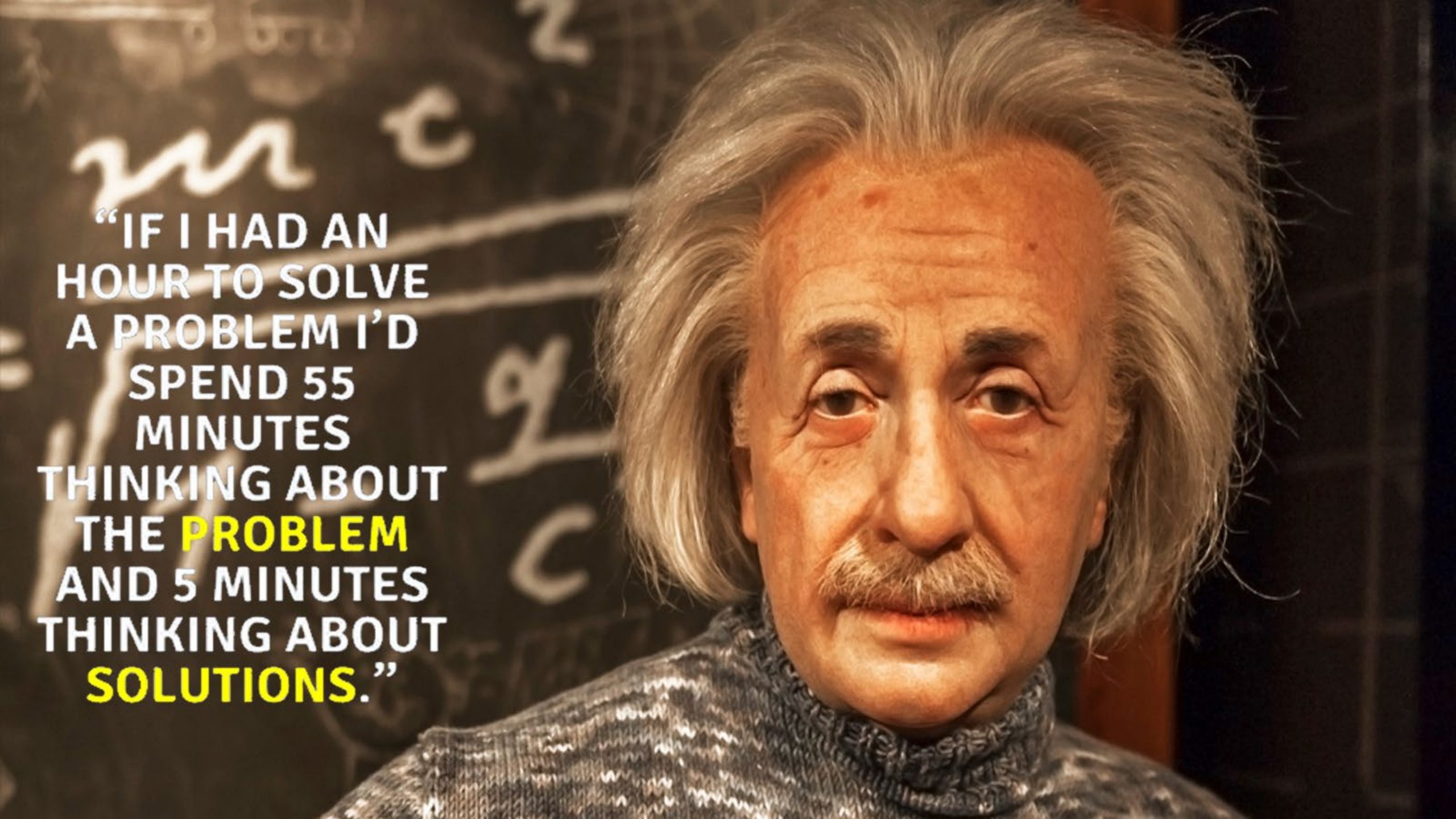
DEPARTMENT OF
COMPUTER
SCIENCE

QGP: A Novel Quantum Good Privacy for Enhanced Security, Privacy, and Authentication

Paul Wang, Ph.D.

Morgan Quantum Computing Group
- Computing, Cryptology, Cryptography, and Security


"IF I HAD AN HOUR TO SOLVE A PROBLEM I'D SPEND 55 MINUTES THINKING ABOUT THE PROBLEM AND 5 MINUTES THINKING ABOUT SOLUTIONS."

Color

Vulnerabilities

Cybersecurity

Buffer overflow

Injection attacks

Artificial Intelligence/ Machine Learning

Non-bias, equitable, responsible

ethical, trustworthy

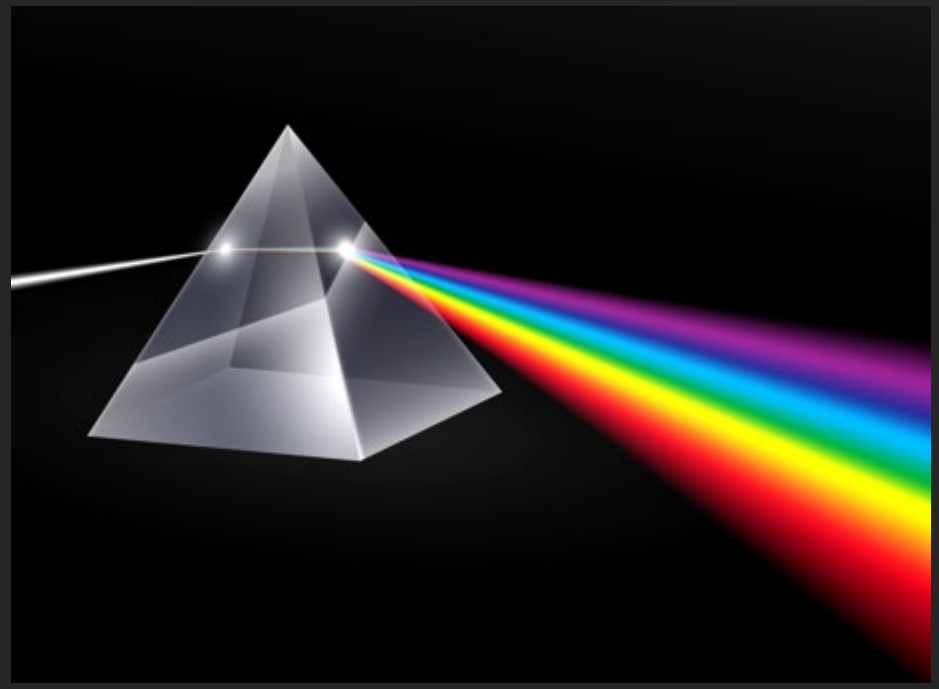
Secure Coding

Bugs

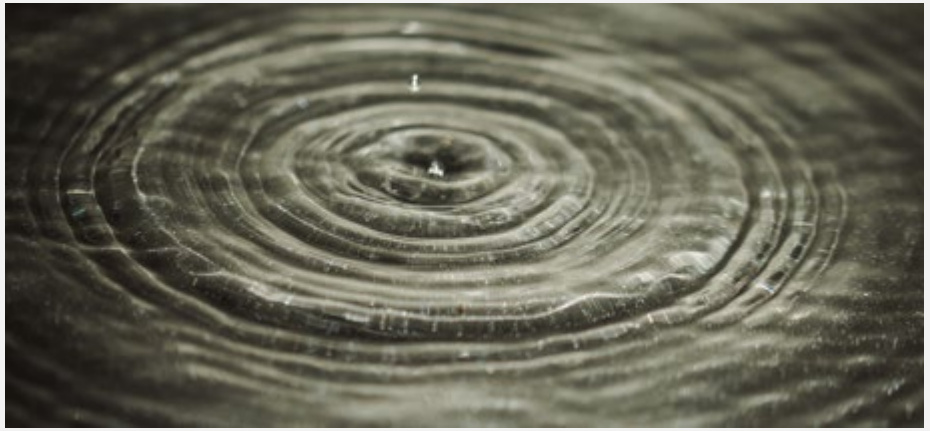
Logic flaws

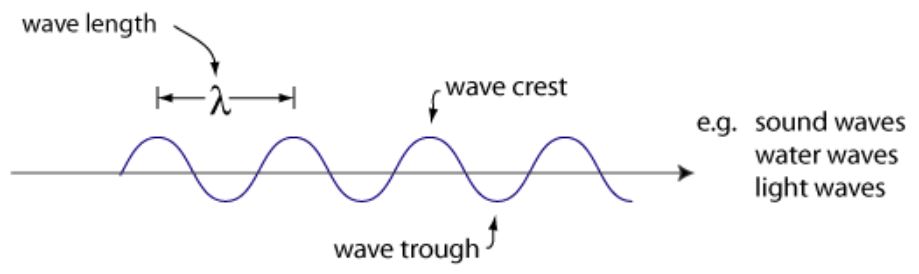
Exploitable

Light, *Quantum Theory of*



- **Light** is composed of particles called **photons**.
- **Matter** is composed of particles called electrons, **protons**, and neutrons.
- It's only when the mass of a particle gets small enough that its **wavelike** properties show up.





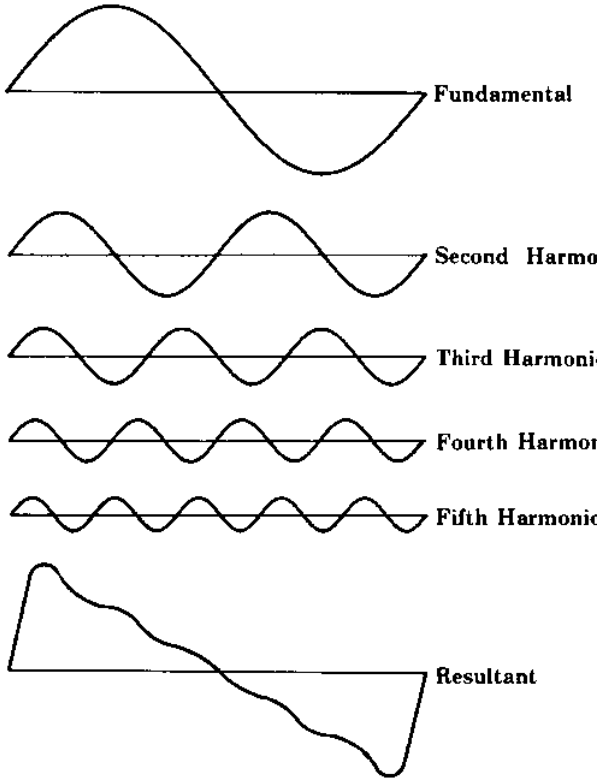
In the 1600s, Christiaan Huygens, a Dutch physicist, showed that light behaves like a wave.

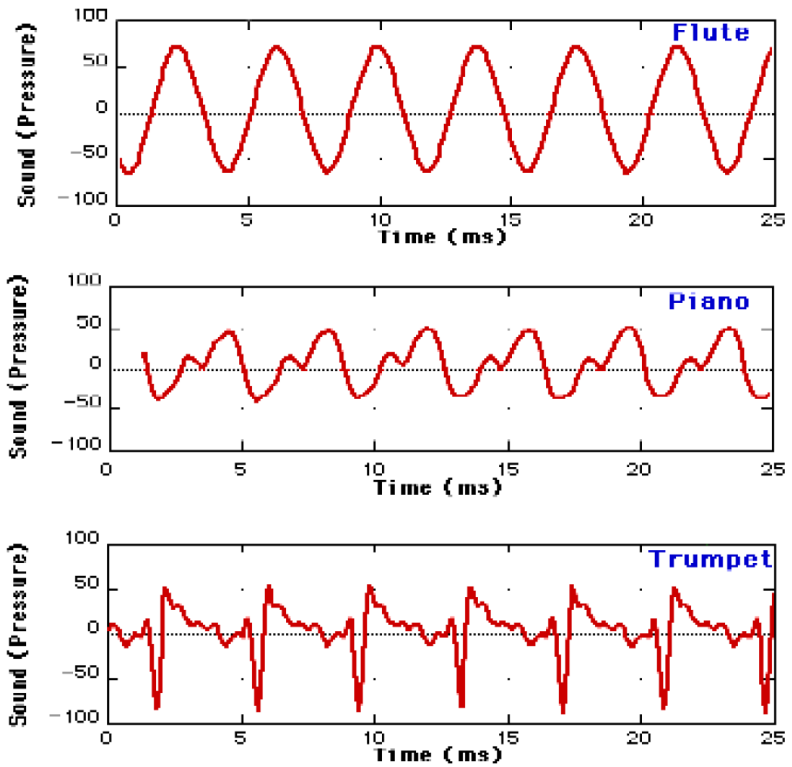
Waves – Cycles

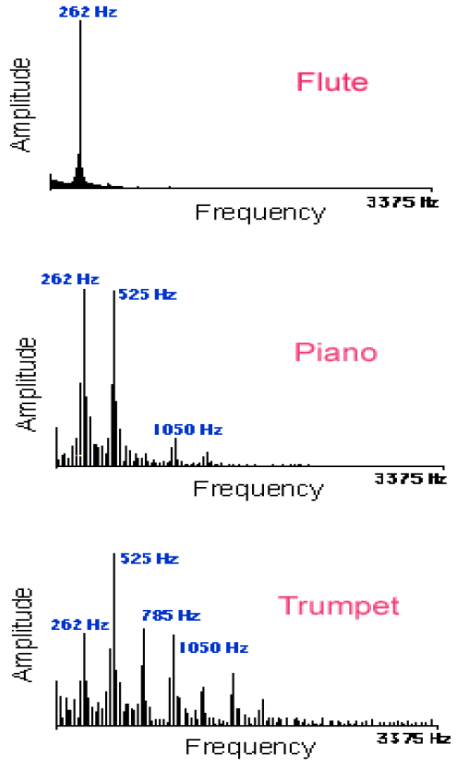
Karaoke, Voice Cancellation

$262\ Hz = (440 * \sqrt[12]{2} * \sqrt[12]{2} * \sqrt[12]{2}) / 2$

note *C*







Davis, 2002

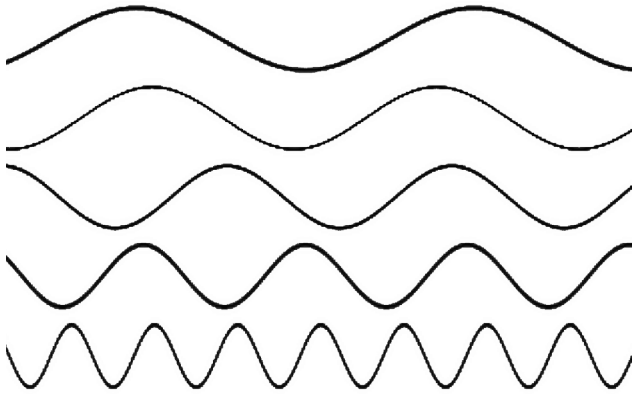
Period and Transform

$$e^{ix} = \cos x + i\sin x,$$

Clock

Piano, 7, 12, 26, 400

Pi or e (??)



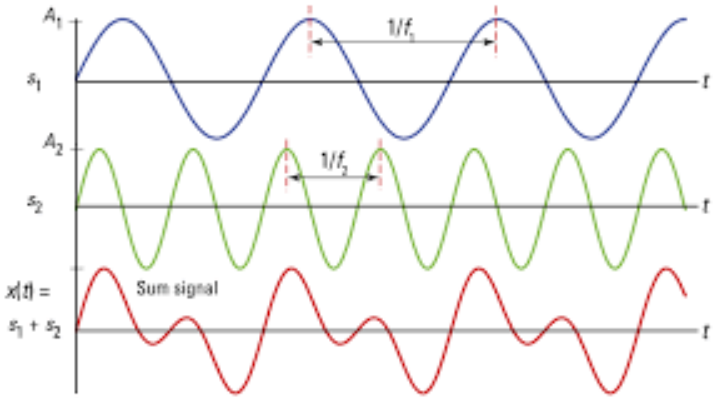
XOR

9 + 6 = 3 mod 12

3 + 6 = 9 mod 12

5 + 3 = 2 mod 7

25 + 2 = 1 mod 26




UNITED STATES NAVY


AIR AR FORCE

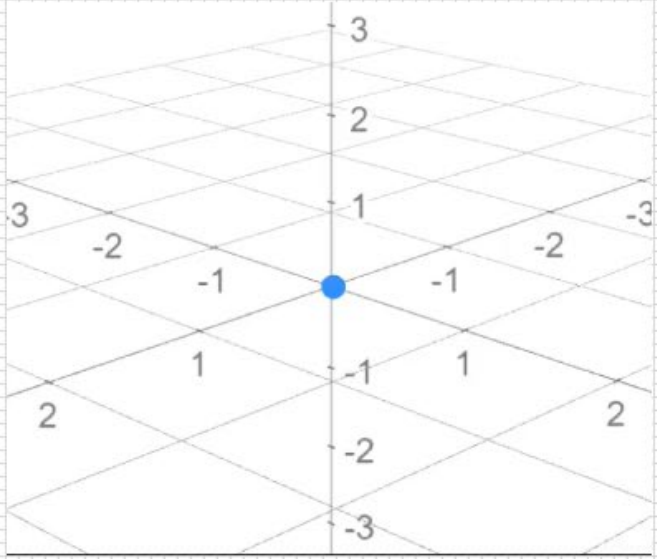

GOD SAVE THE KING


Slient Night

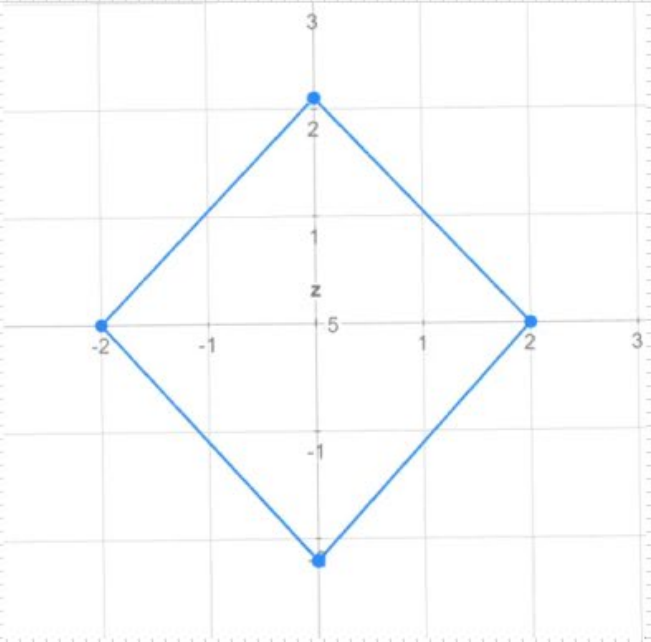

NEW WORLD
SYMPHONY


GRAND
OLE OPRY

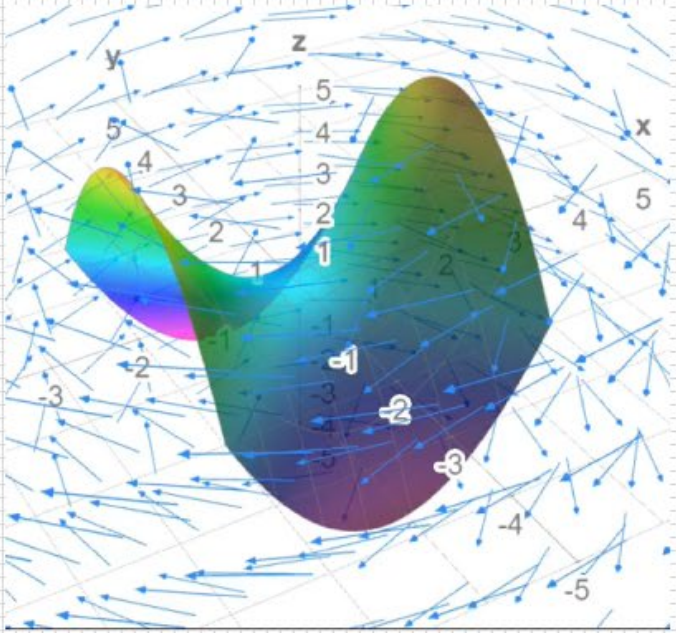
The Beauty of **Transform**



A point or a line?

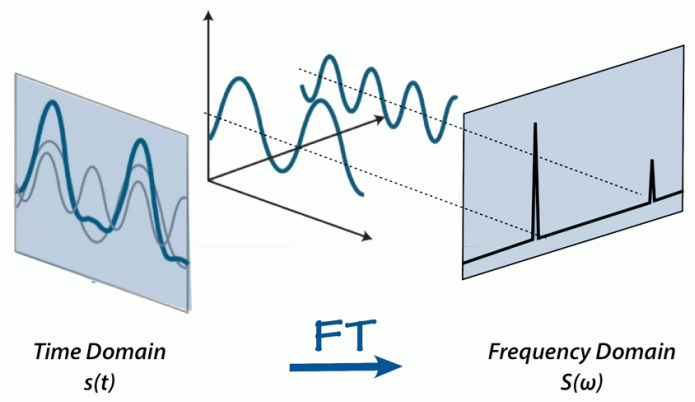


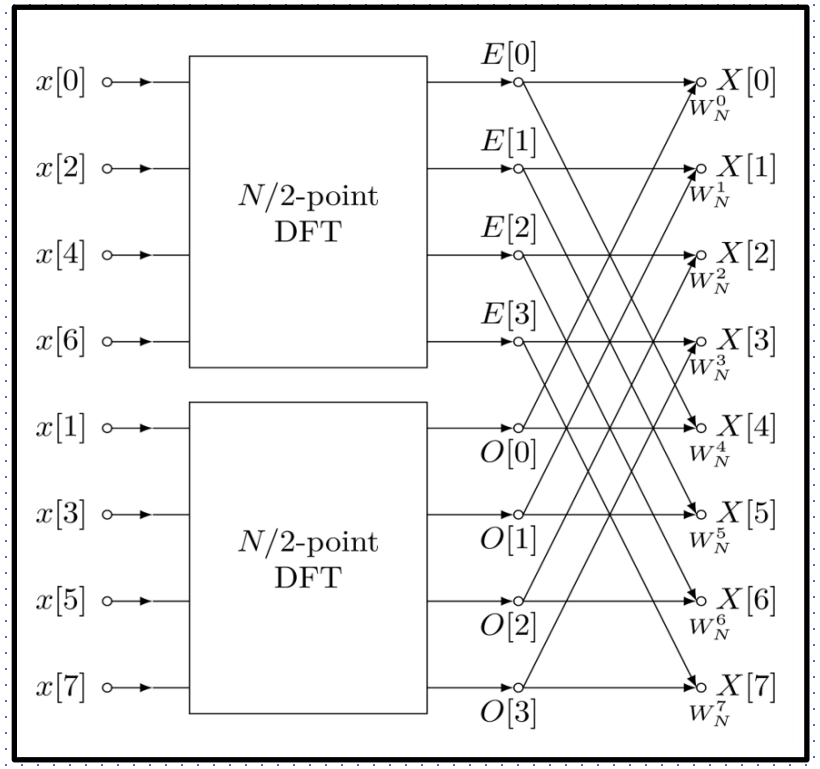
2D or 3D space?



Random or patterns?

The Beauty of Transform – FFT

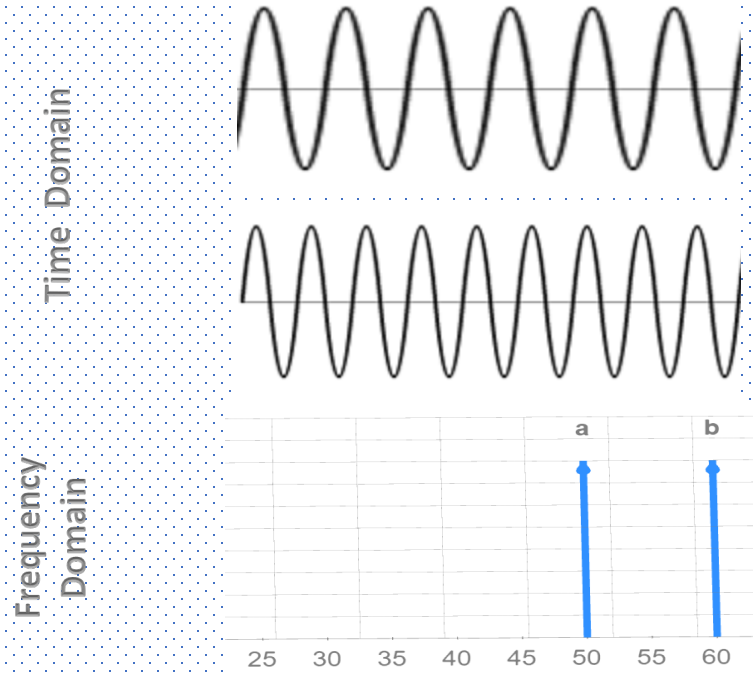




N-point DFT

Butterfly

Recursion!



A FFT algorithm on $n = 2^p$ inputs with respect to a primitive n-th root of unity $\omega_n^k = e^{-\frac{2\pi i k}{n}}$ relies on $o(n \log_2 n)$ butterflies of add & sub

Shor’s Algorithm

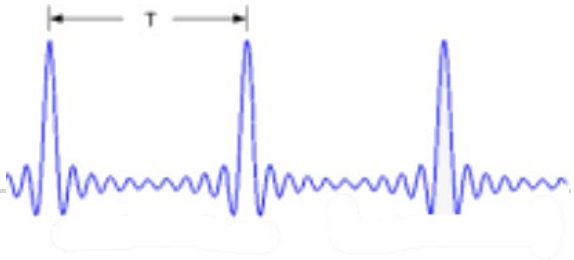
- Shor’s algorithm, 1994
- Implementation
  - 15 = 3x5, 2001 and 2012
  - 21 in 2019
  - 35 failed due to errors

```
In [1]: N = 10403
        for x in range (2, N):
            for y in range (2, N):
                if x*y == N:
                    print ("x=", x, "y=", y)

x= 101 y= 103
x= 103 y= 101
```

- The core is factoring sth. like x^2 = (x+1)(x-1) = 0 *mod* N
  - **Period**
  - **Transform**

Period in RSA Algorithm



Modular Exponentiation: $f(x) = a^x \mod N$

where $a \neq p, q$ is an integer number, the modulus $N = pq$

Number Theory: $f(x)$ is periodic with period r

Period: $r = (p-1)(q-1)$ **Hard** if finding r from only N – **order finding**

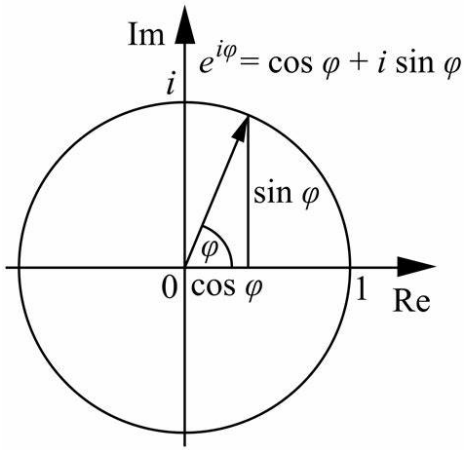
Key Pair: Public key: e, N; Private key: d, N

e Satisfies: 3 <= e <= N – 1, gcd (e, r) = 1 (coprime)

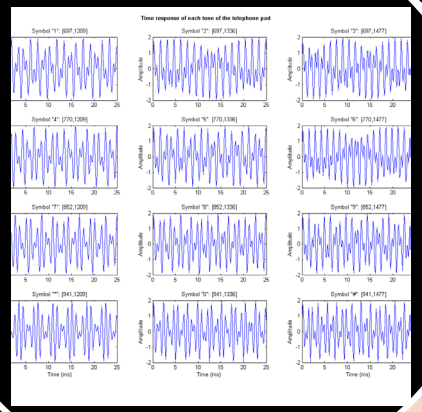
d = Inverse e: $d = e^{-1} \mod r$

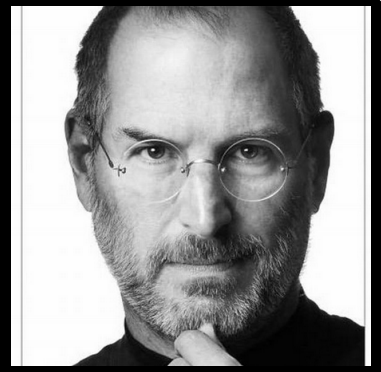
Encryption: $c = m^e \mod N$

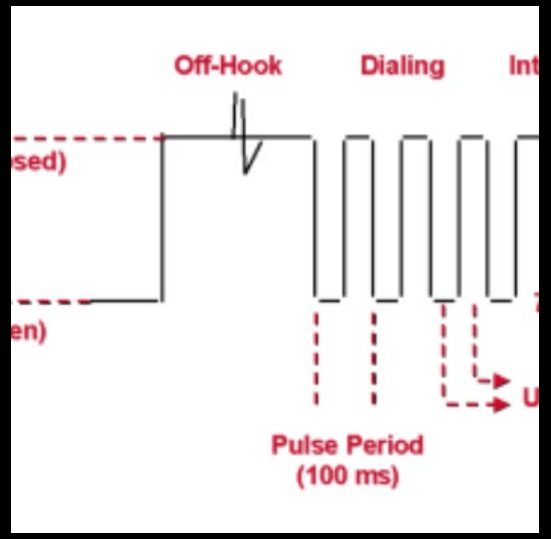
Decryption: $c^d \mod N = (m^e)^d \mod N = m$



Bluebox vs. “Greenbox”





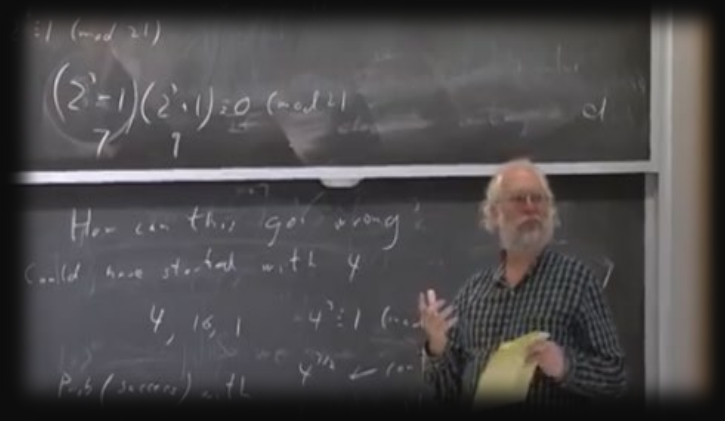


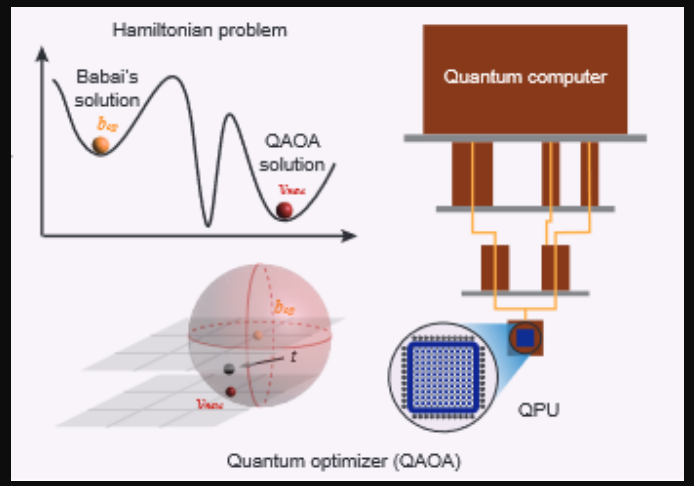
How Secure Are We Now?

Shor: exponential speed up, mathematically

# of qubits?

Circuit depth?





RSA 2048: 372 qubits with thousands of depth

- IBM: 127 qubits, 433 qubits

https://arxiv.org/abs/2212.12372

RSA Backdoor?

Hour much trust to the third party?

Key-Splitting

A key can be crafted using modular arithmetic such that a third party can decipher without requiring the private key.

Could this have been already embedded in RSA?

An **exercise** for interested people.

A new idea for RSA backdoors (arxiv.org)

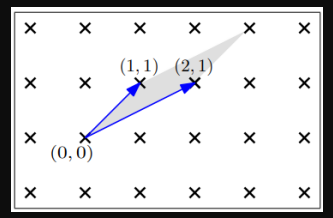
How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer (cloudflare.com)

Report: NSA Paid RSA $10M to Create 'Back Door' in Encryption Software | PCMag

Post Quantum Cryptography

Encryptions and Key Establishment

- CRYSTALS-Kyber
- Asymmetric Algorithm
- Module Lattice, LWE (Learning With Errors) Based



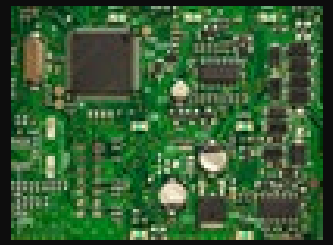
$\mathbb{R}^2$ vs. $\mathbb{R}^{400}$

Digital Signatures

- CRYSTALS-Dilithium-AES
- Asymmetric Algorithm

Side-Channel Attacks

- Timing Attacks, Power, Electromagnetic, Fault Attacks
- RISC-V PQC ISA



eprint.iacr.org/2021/1021.pdf

Worry Free With PQC?

Worry Free !?

Enigma: needs 100 years to break – T/F?

- Statistical analysis

DES – 1976

- 3DES to store government document to 2030 – T/F?
- DES cracker – 1998, NSA involvement, AES – 2002

RSA – 1977

- 300 trillion years to break RSA-2048 – T/F?
- Never been approved for no short cut
- Vulnerable to quantum attacks

PQC – 2023

- Secure against any computers – T/F?

Worrisome QKD

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

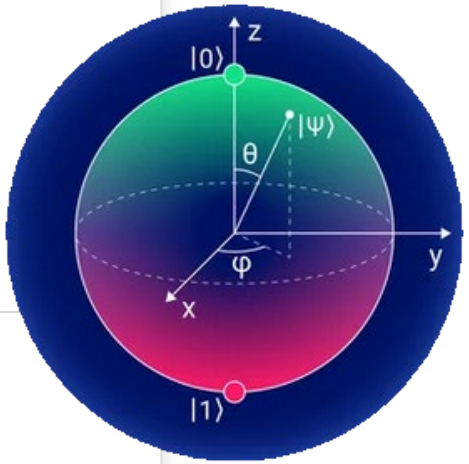
SWEDISH ARMED FORCES

- Need for specialized hardware and high costs
  - Single photon sources and detectors
  - Eavesdropping, interference →**DoS**
- Distance limitations and end-to-end security
  - Currently hundreds km
  - Need **trusted notes** for longer distance, thus **end-to-end** vulnerable
  - Key rate is limited. Satellite?
- Reliance on classical cryptography for peer authentication
  - Authentication: pre-shared keys must be present at both ends before running QKD protocol
  - The secret key must be distributed and then periodically renewed in a secure manner

Mistakes Made in History

What we thought was a strong crypto algorithm may not be that strong when looking from a **new** perspective.

QFT Speed Up



Initialization

Recursion

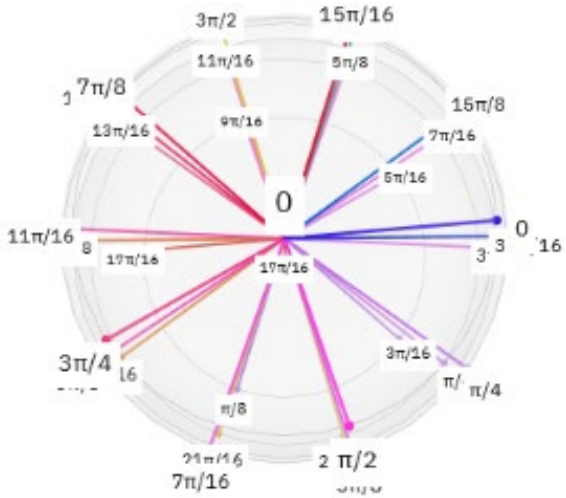
QFT

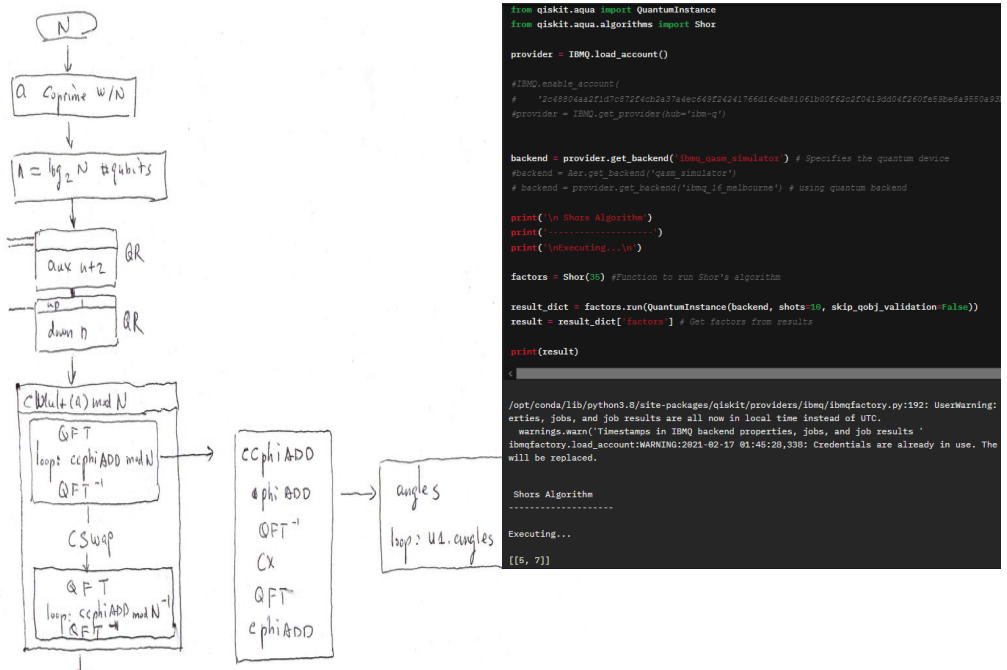
Modular ADD (phi)

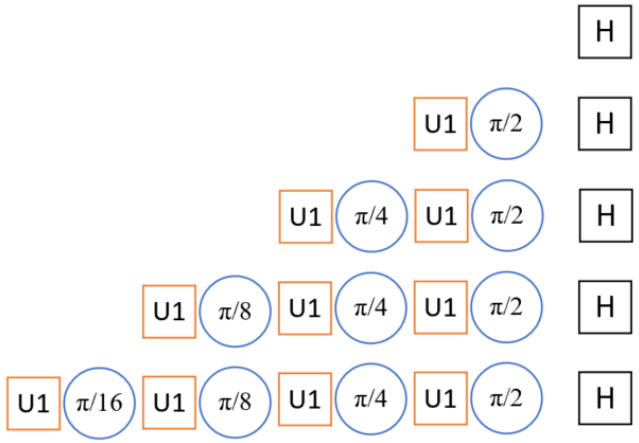
QFT^{-1}

Measure

Calculate factors







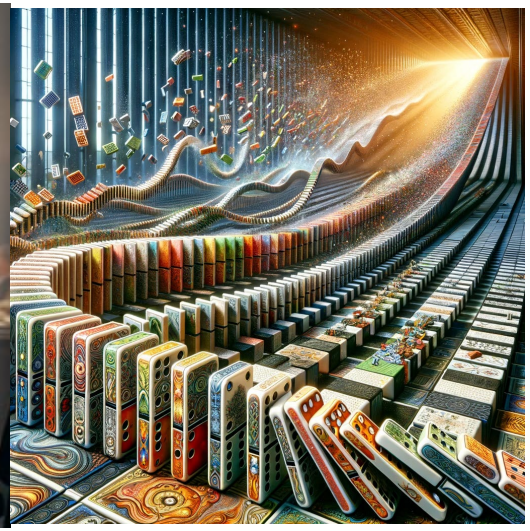
Exp to Add/Sub With Additional Polynomial Overhead

Quantum Computing

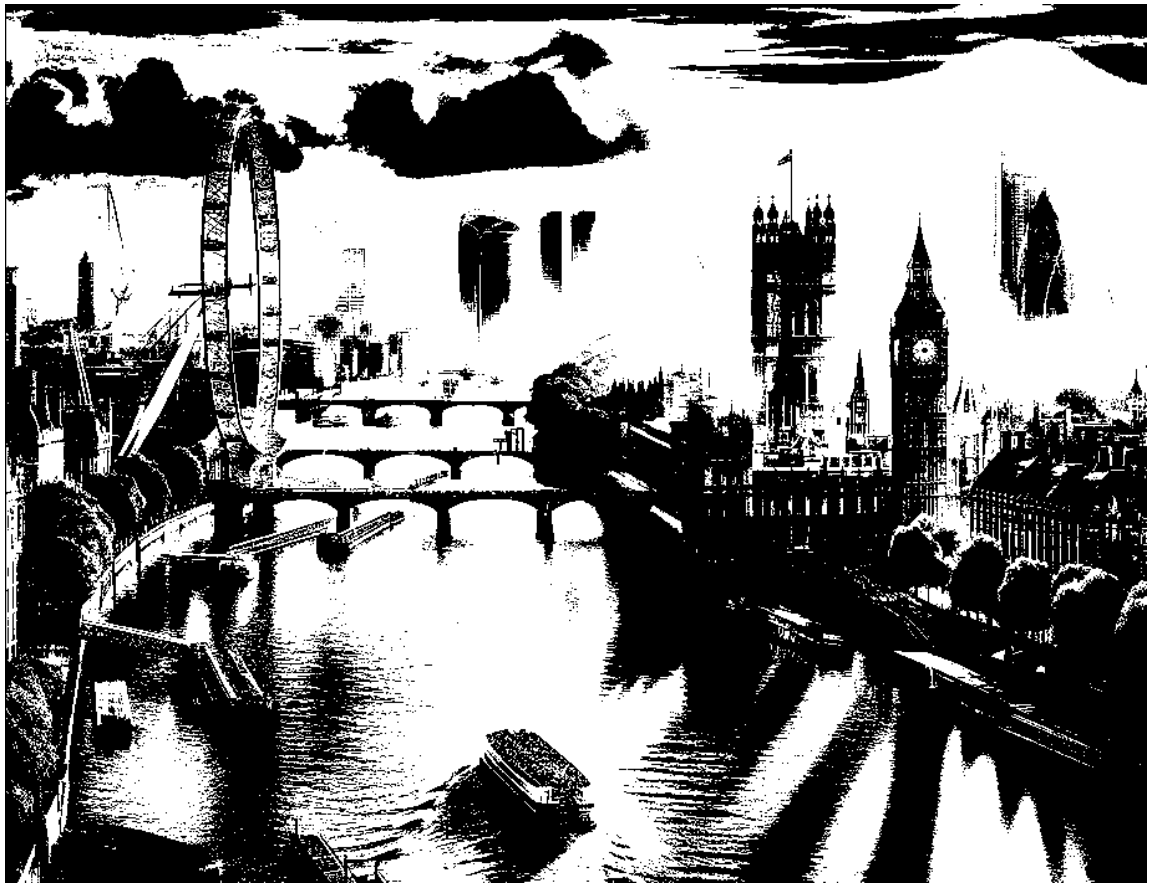
Superposition

```
For each apple on the apple tree
  if color == green then continue
  else "red apple found"
```

Entanglement



Interferences



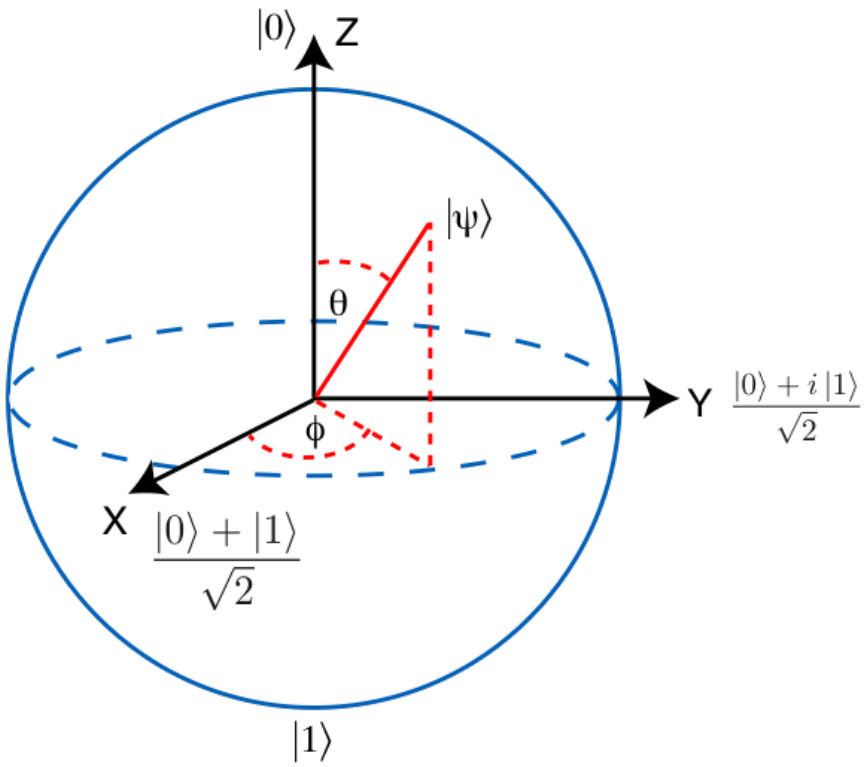
Why Binary?

Base 2 vs. Base N

π music

O(time) Analysis

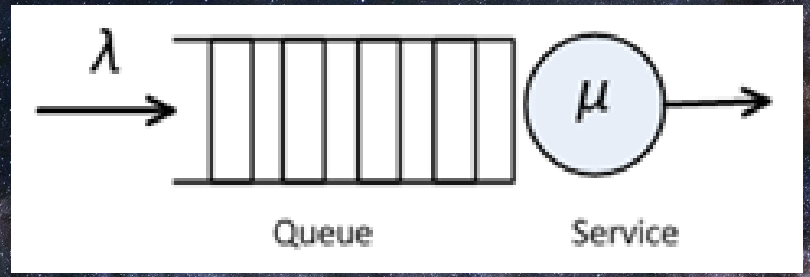
- 1D time domain signal
  - Compress/stretch a signal in <u>time</u> domain: **hard**
  - Compress/stretch in <u>frequent</u> domain: easy
- 2D time domain signal
  - Process in <u>time</u> domain: **slow** (n X n for image processing)
  - Process in <u>frequency</u> domain: fast (n log n)
- e^x (nD) time domain signal
  - **Impossible** to process due to time
  - QFT to frequency domain to perform add/sub

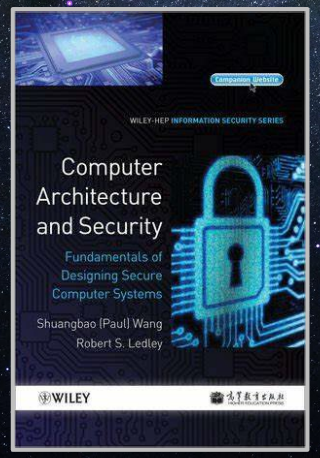


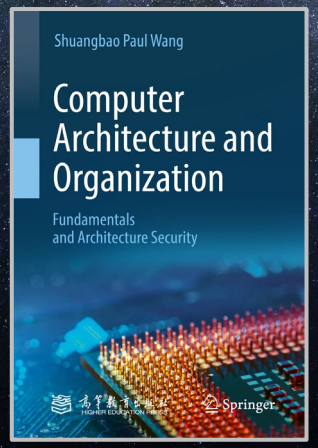
Quantum Internet

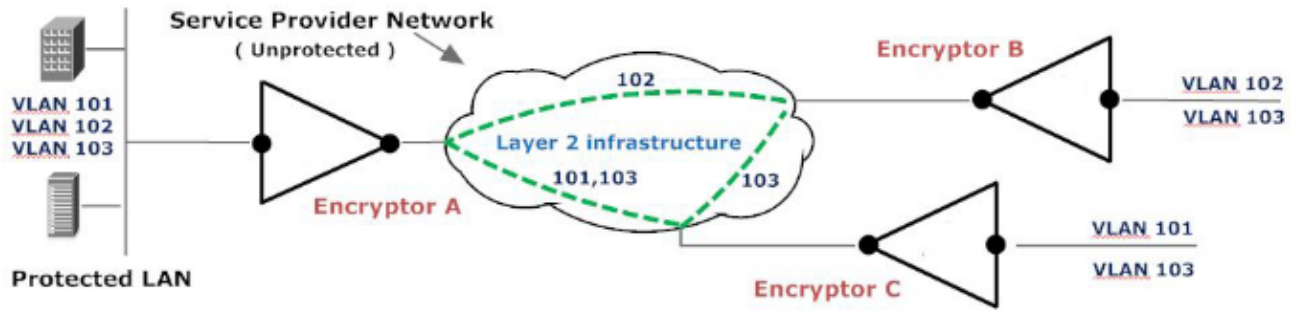
Security Enhancement

- Networking protocol: TCP/IP
  - 7 layers: APSTNDP
- Routers and switches
  - Quantum **memory**
- Encryption key distribution
  - Asymmetric key encryption (RSA)
  - Digital signatures

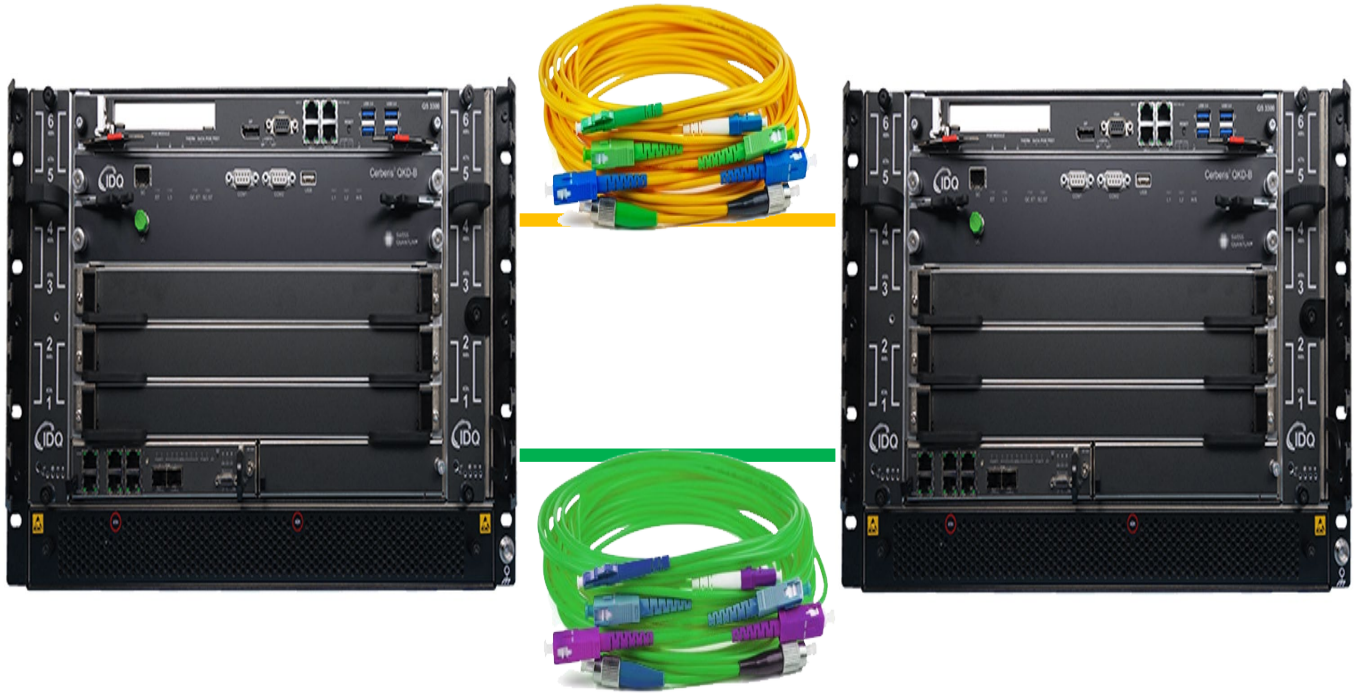




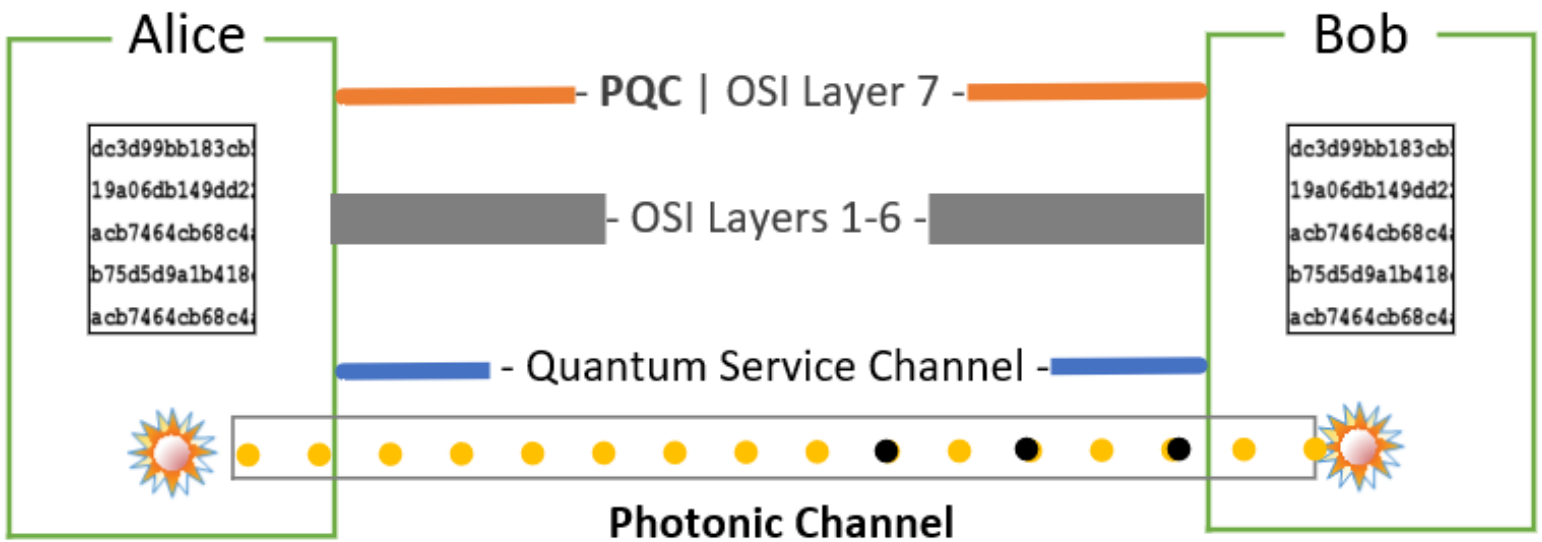


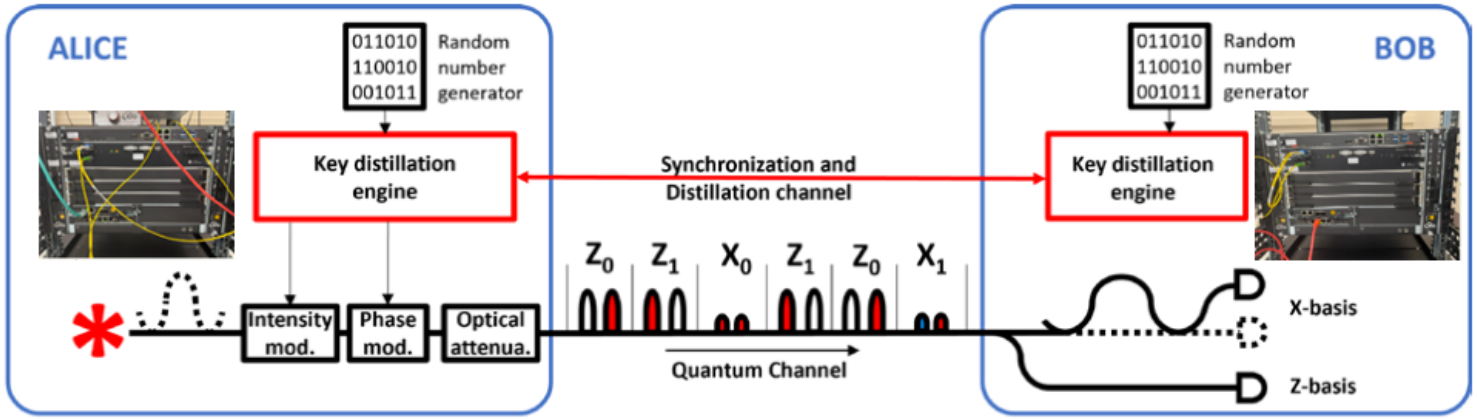

Service Provider Network
(Unprotected)
VLAN 101
VLAN 102
VLAN 103
Protected LAN
Encryptor A
102
Layer 2 infrastructure
101,103
103
Encryptor B
VLAN 102
VLAN 103
Encryptor C
VLAN 101
VLAN 103


CENTAURIS
LOCAL
NETWORK
ALARM
SECURE
LAN — MANAGEMENT — CON
POWER

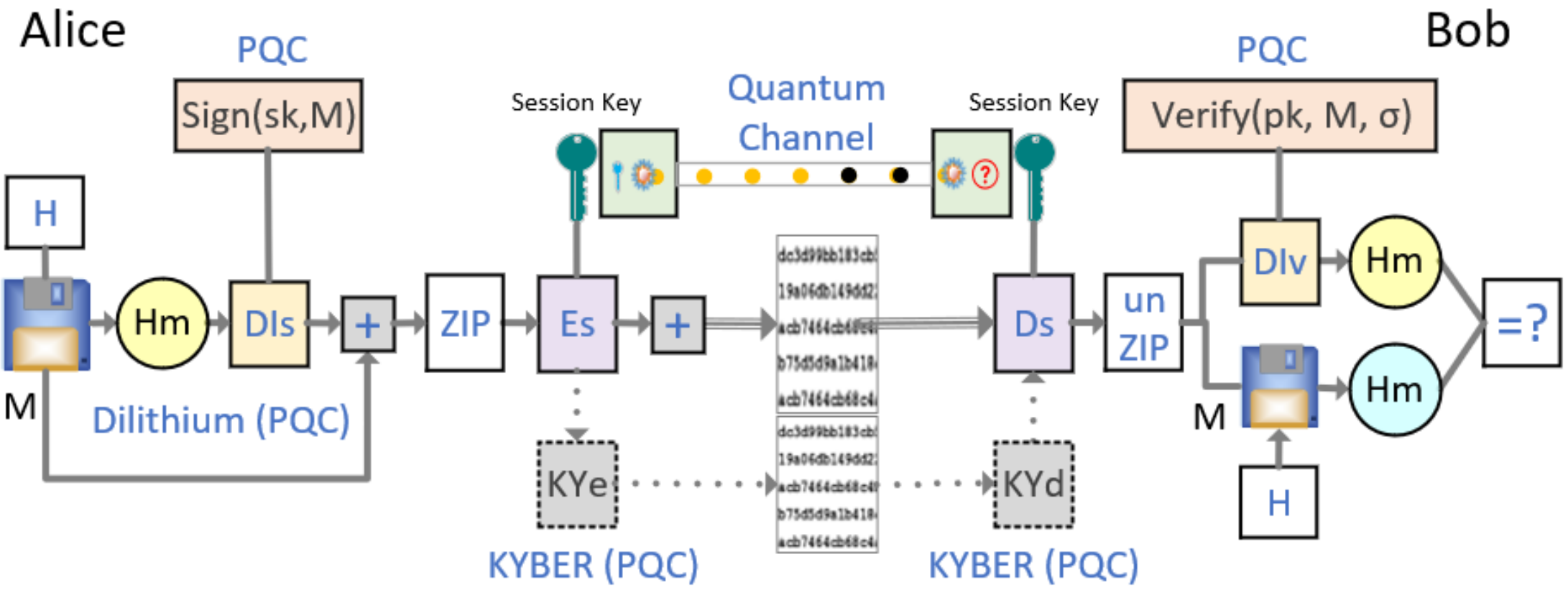


Adding Layer 0 and Modified Layer 7





QGP – Quantum Good Privacy



https://www.blogger.com/blog/post/edit/5367145941120044372/4774259468001993828

To Build a Quantum Internet Testbed

Quantum computing is the future

Quantum cryptography is now

“Cyber attacks present the greatest threat to our national and economic security today, and the magnitude of the threat is growing. This bill is an important step toward curbing these dangerous cyber attacks.”

Senate Intelligence Committee
Cybersecurity Bill – 2014

Paul Wang
https://www.linkedin.com/in/paulwangedu