POST-QUANTUM CRYPTOGRAPHY

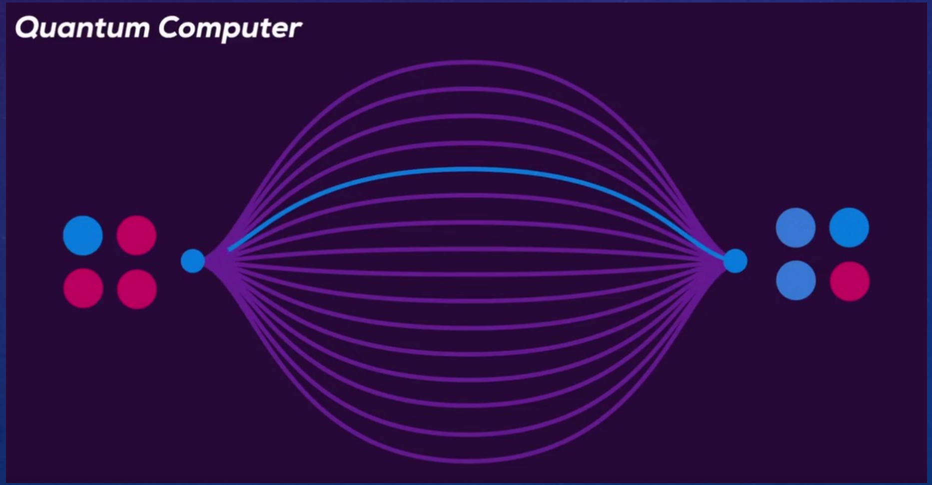
MADE BY: ROBIN VAN GRINSVEN.

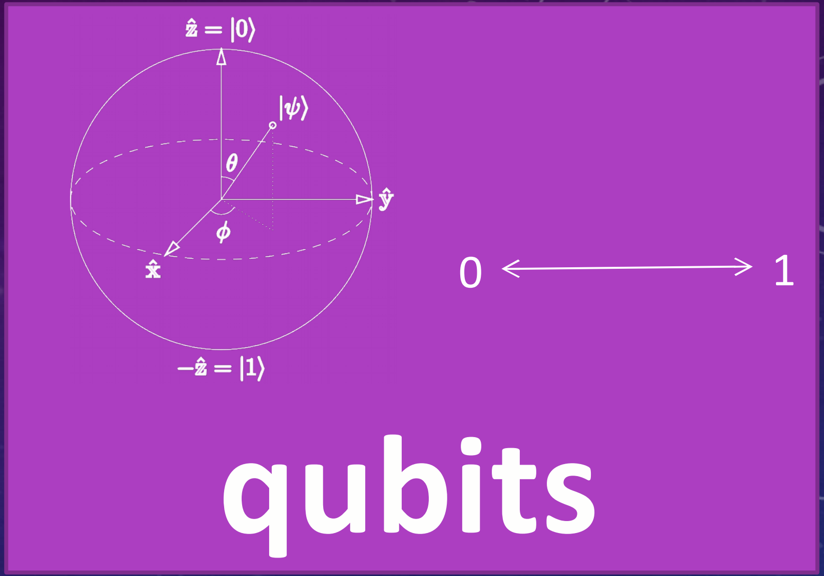
NHTV/IADE/EUROPEIA

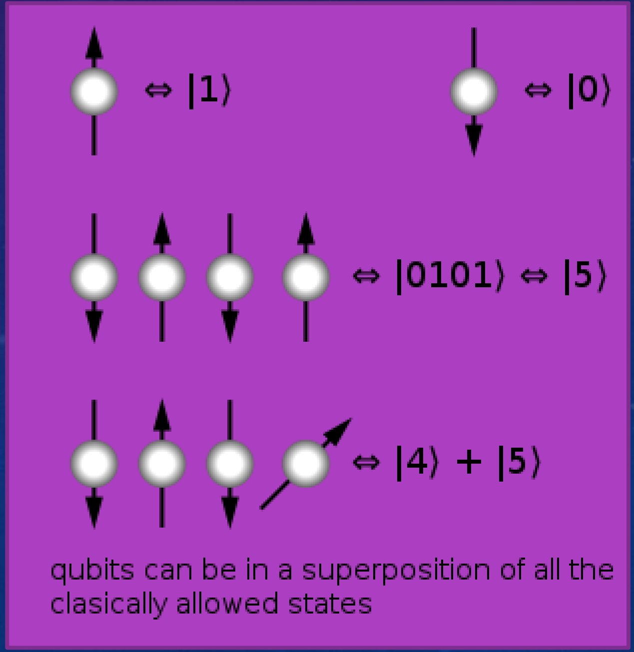
QUANTUM COMPUTING

- Niels Bohr: "Anyone who is not shocked by quantum theory has not understood it.“
- Richard Feynman The Character of Physical Law - (Anon 2014) :"If you think you understand quantum mechanics, you don't understand quantum mechanics.“

- Runs many questions at once. But once looked gives 1 answer. (parallel paths 1 answer)
- Orientation changers are it manipulators instead of (X)or/(x)and gates
- 50 qubit.





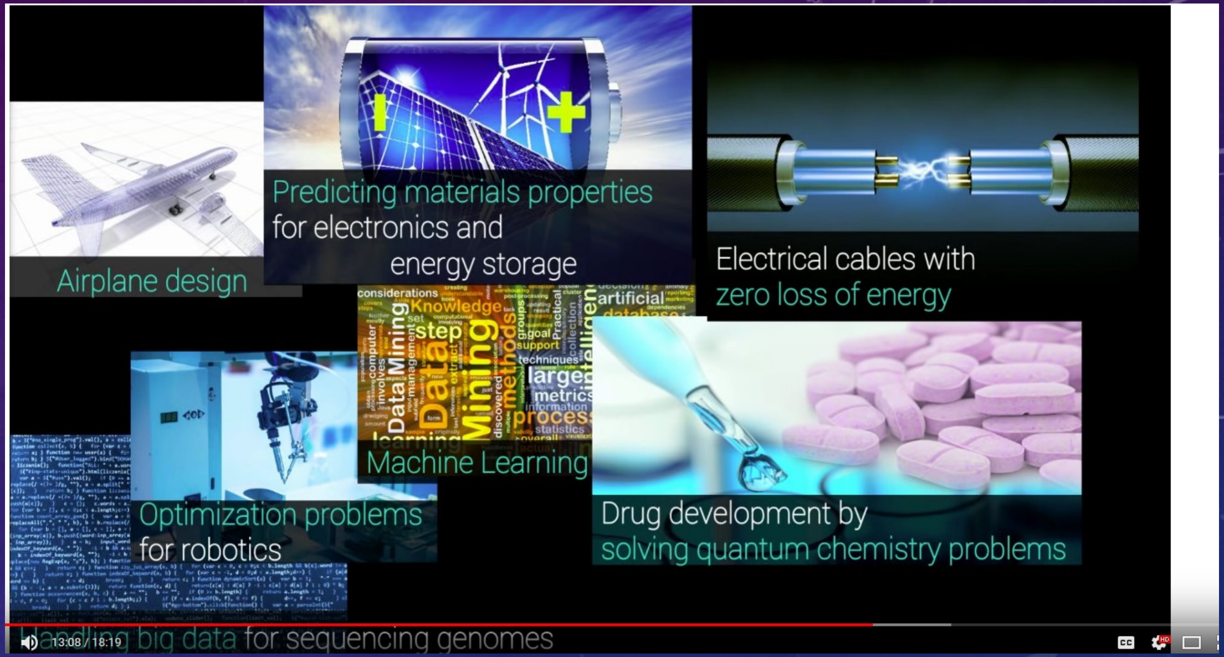


CURRENT PROBLEMS

- scalable physically to increase the number of qubits;
- qubits that can be initialized to arbitrary values;
- quantum gates that are faster than decoherence time;
- universal gate set;
- qubits that can be read easily.
- Control 5-10 cubits(2015).
- Currently solve the substitute of 15(5X3).
- Making a quantum computer 2 times faster requires 1 qubit. 2n.

INDUSTRIES

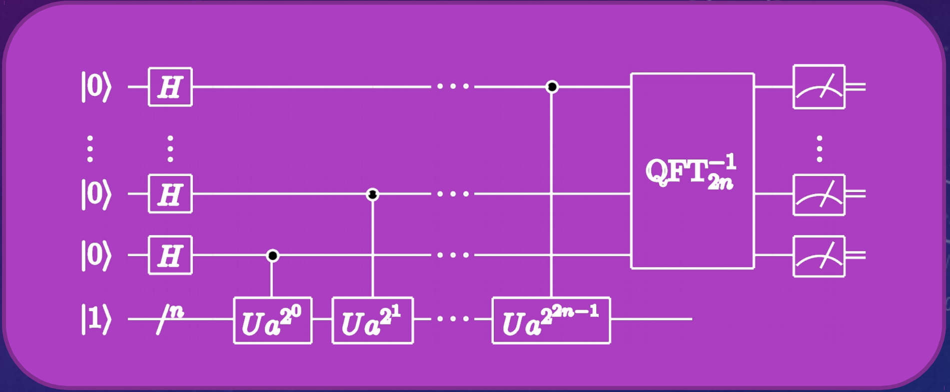
- Astrophysics.
- Pharmaceuticals/Chemistry.
- Weather forecasting.
- Nanotechnology.
- Any simulation.
- Data base theory.(Grover's Algorithm)
- Encryption/Decryption.
- And anything with these problems:
  - guess answers repeatedly and check them.
  - possible answers are equal to the amount of inputs.
  - Every answer takes equal amount of time to check.
  - There are no clues about which answers might be better: generating possibilities randomly is just as good as checking them in some special order.



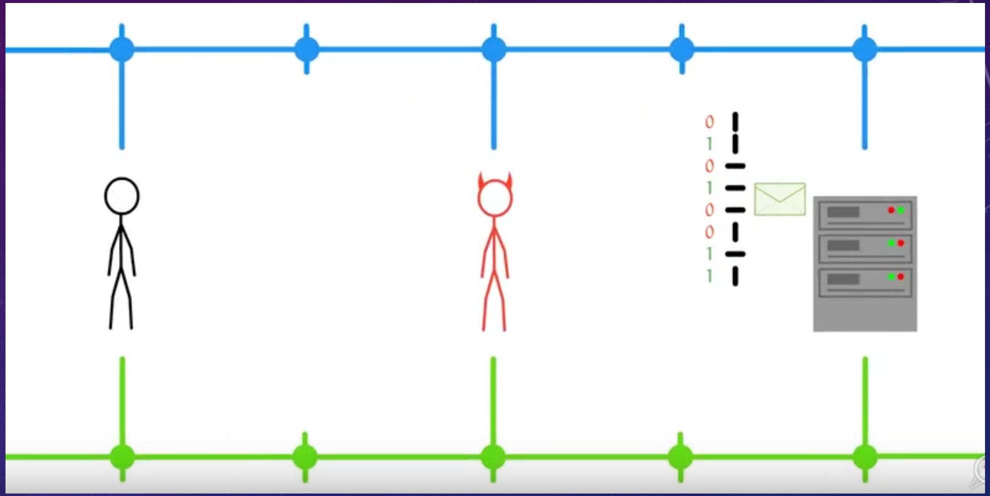
https://www.youtube.com/watch?v=aUuaWVHhx-U

SHOR'S ALGORITHM

- Peter shor(1994)
- Great for finding the prime factors of a number.(RSA)
- Current performance is 143=11*13(done on 5 atoms)
- Makes the problem lay in BQP



QUANTUM DEFENSE



- Quantum to beat quantum
- Exploit the “look” mechanic of quantum
- Need a quantum connection
- Chances are quantum computers will not be in ordinary households.

CLASSIC COMPUTER DEFENSES

implementations

- ring Learning with Errors key exchange
- McEliece cryptosystem
- GoldRiech -Goldwasser- Halevi scheme
- superSingular IdoGeny Diffie helleman key exchange

concepts

- Lattice Cryptography
- Multivariate cryptography
- Hash-based cryptography
- Code-based cryptography (1971-encoding)
- Supersingular elliptic curve isogeny cryptography
- Symmetric key quantum resistance

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt[34]	Lattice	6130 B	6743 B	
Streamlined NTRU Prime	Lattice	1232 B		
Rainbow[35]	Multivariate	124 KB	95 KB	
SPHINCS[18]	Hash Signature	1 KB	1 KB	41 KB
BLISS-II	Lattice	7 KB	2 KB	5 KB
GLP-Variant GLYPH Signature[10][36]	Ring-LWE	2 KB	0.4 KB	1.8 KB
New Hope[37]	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece[14]	Code-based	1 MB	11.5 KB	
Random Linear Code based encryption[38]	RLCE	115 KB	3 KB	
Quasi-cyclic MDPC-based McEliece[39]	Code-based	1232 B	2464 B	
SIDH[40]	Isogeny	751 B	48 B	
SIDH (compressed keys)[41]	Isogeny	564 B	48 B	
3072-bit Discrete Log	**not PQC**	384 B	32 B	
256-bit Elliptic Curve	**not PQC**	32 B	32 B	

CODE-BASED CRYPTOGRAPHY

- Key size problem pre quantum security 1024 Kb
- Recommened stategery : McEliece with binary Goppa

Parity check matrix ($n = 7, k = 4$):

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

An error-free string of 7 bits $\mathbf{b} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6)$ satisfies these three equations:

$$\begin{aligned} b_0 + b_1 + b_3 + b_4 &= 0 \\ b_0 + b_2 + b_3 + b_5 &= 0 \\ b_1 + b_2 + b_3 + b_6 &= 0 \end{aligned}$$

LWE TECHNIC

- Know to resist quantum computers.
- Part of a solution.
- Inherited in lattice problem

P = G*S+E
S = 5
E = 12

Message = 12

G =[5 , 8 , 12 , 16 , 2 , 6 , 11 , 3 , 7 , 10]

T =[37 , 52, 72 , 92 ,22,42, 67 ,27, 47,62]

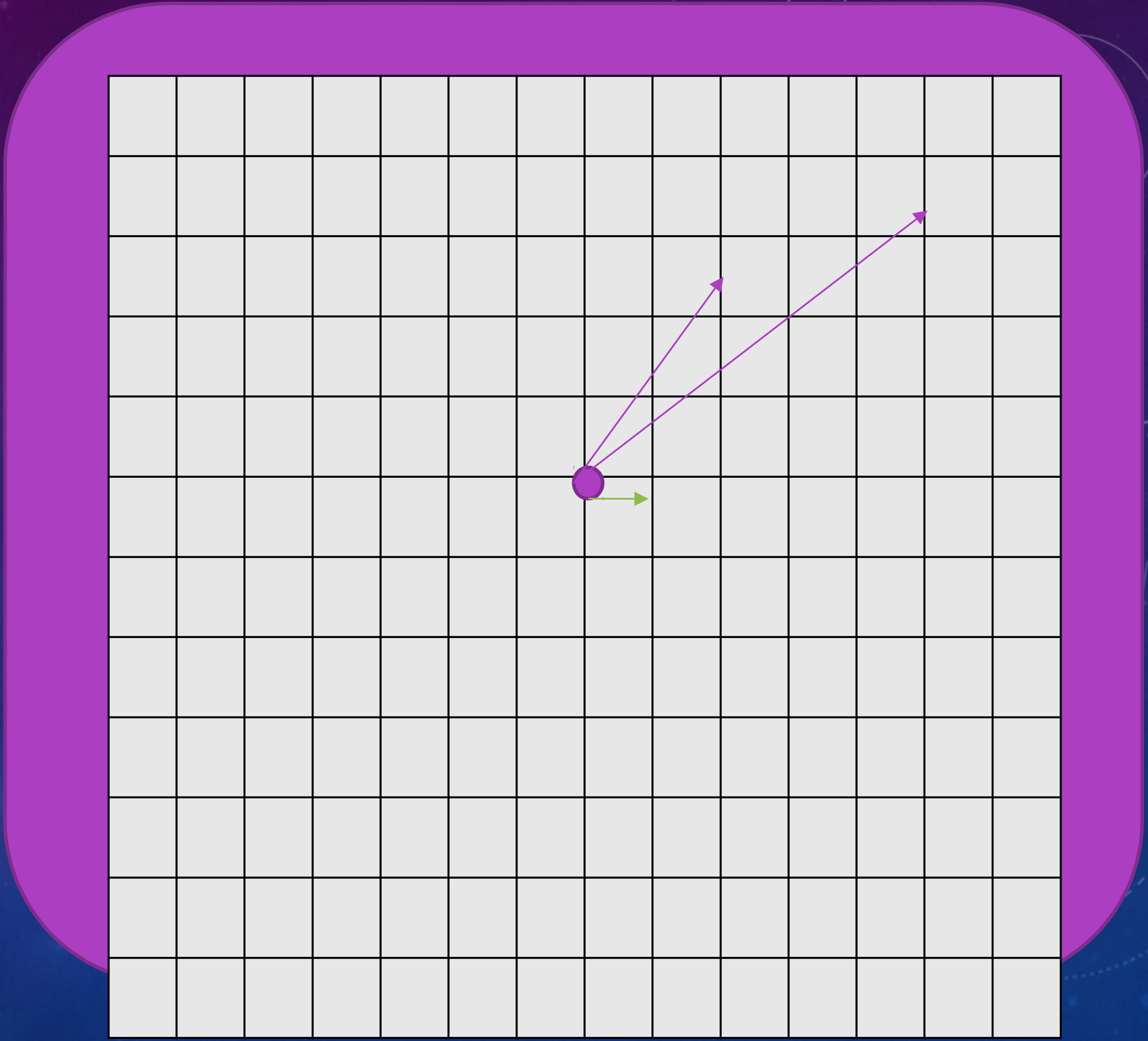
Picked values: [52,27,92,42,62]

Sum up: 275
Encrypt : sum + message
Encrypt : 287

LATTICE CRYPTOGRAPHY

- Multi dimension geometry based cryptography.
- Shortest vector problem (SVP)
- Closest vector problem(CVP)
- SVP/CVP is know as NP hard.
- NTRU(public key)
- Faster encrypt and decrypt then RSA
- Ideal lattice
- Worst-case
- Struggle … nd security

	N	q	p
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3



LATTICE CRYPTOGRAPHY

It has the following applications:

Public key encryption

CCA-Secure PKE

Identitybased encryption

Oblivious transfer

Circular secure encryption

Leakage resilient encryption

Hieracrhical identity based encryption

Fully homomorphy encryption(cloud service use)

Learning thoery

HASH-BASED CRYPTOGRAPHY

- Lamport signatures
- Started by ralph merkle in 1970
- Limit amount of numbers of signatures.
- No patent

END

“Cryptography is a endless battle between the breakers and the builders.

Or is it ending?”:quote myself.