The Quantum Revolution

Making and breaking cryptography using quantum technology

About the authors

Mathis HAMMEL

@MathisHammel

Deputy Technical Director @ Sogeti
Co-founder, Challenge Designer @ h25

About the authors

Clément HAMMEL

@clement_hammel

Product Operation Manager @ PayFit
Co-founder, Challenge Designer @ h25

Introduction

“Quantum” is the “blockchain” for nerds

Introduction

“Quantum” is the “blockchain” for nerds

Introduction

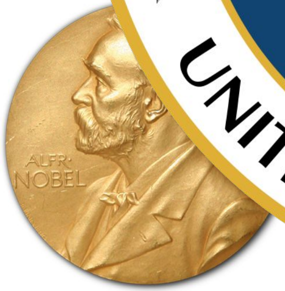
“Quantum” is the “blockchain” for nerds

Introduction

"Quantum" is the "blockchain" for nerds

Introduction

“Quant … for nerds



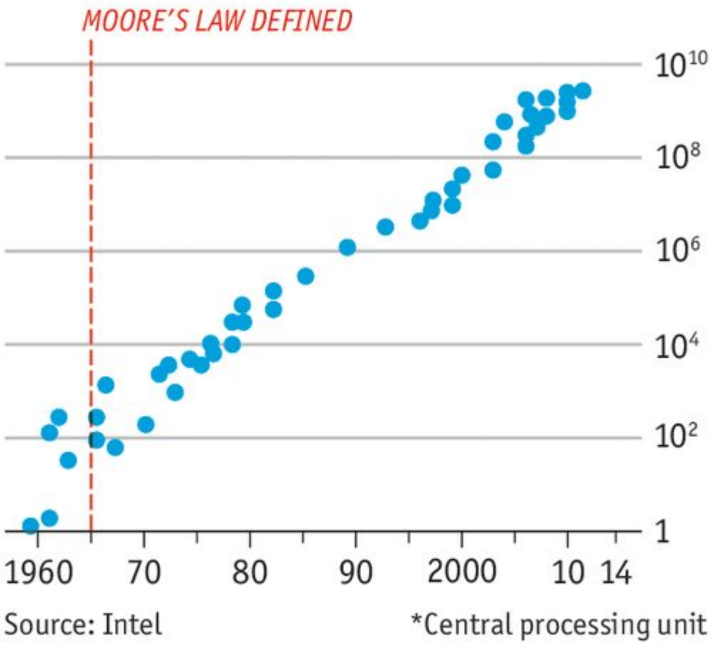
Outline

- Quantum Computing
- Breaking modern cryptography
- Defending against quantum adversaries
- Making new cryptography

Quantum Computing

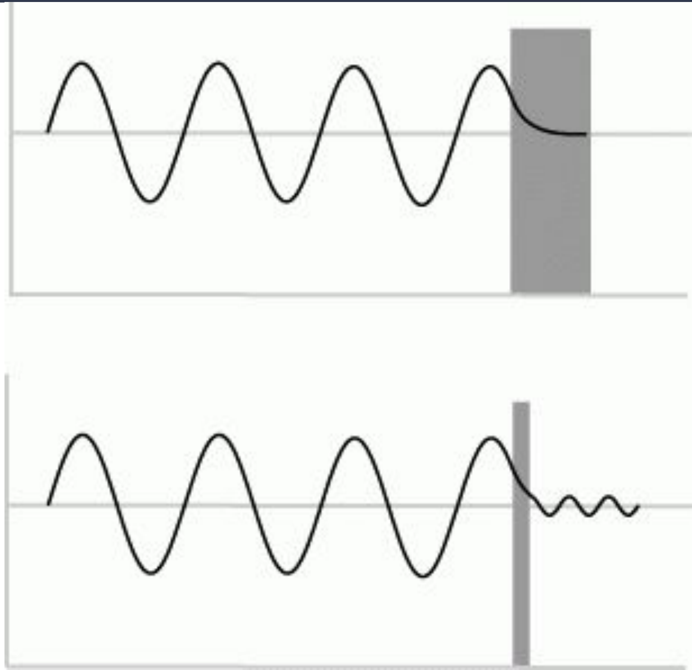
- End of Moore’s Law
- Q-Computing 101

Quantum computing - Moore’s Law



Economist.com

Quantum computing - Moore’s Law



Quantum tunneling

Quantum computing - Moore's Law

expected to end in 2025-2030

How to prevent this ?

- Manage tunneling noise
- Make more complex chips
- Use another technology

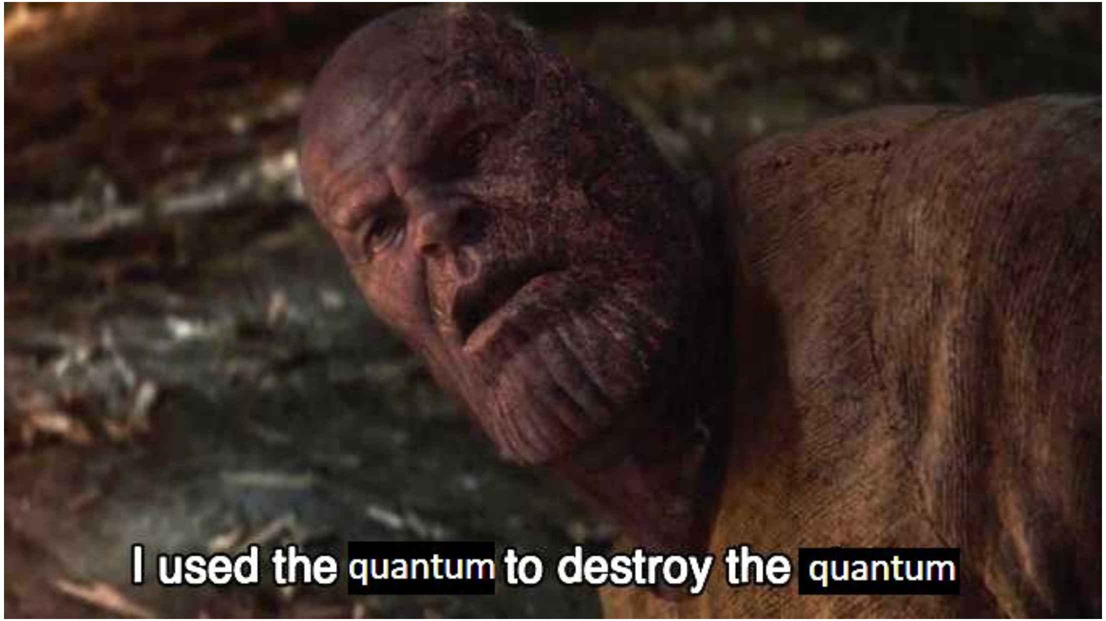
Quantum computing - Moore’s Law

expected to end in 2025-2030

How to prevent this ?

- Manage tunneling noise → Working on it
- Make more complex chips → Too expensive now
- Use another technology → Quantum ? 🤔

Quantum computing - Quantum 101

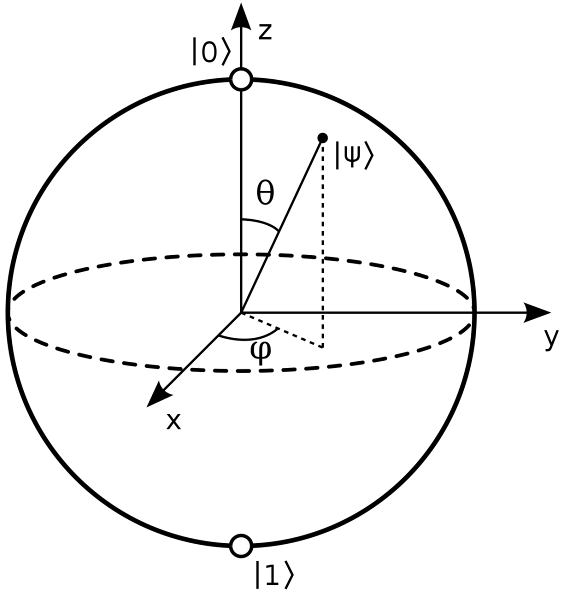


Quantum effects to get over quantum

Quantum computing - Quantum 101

Quantum vs classical, what’s the difference?

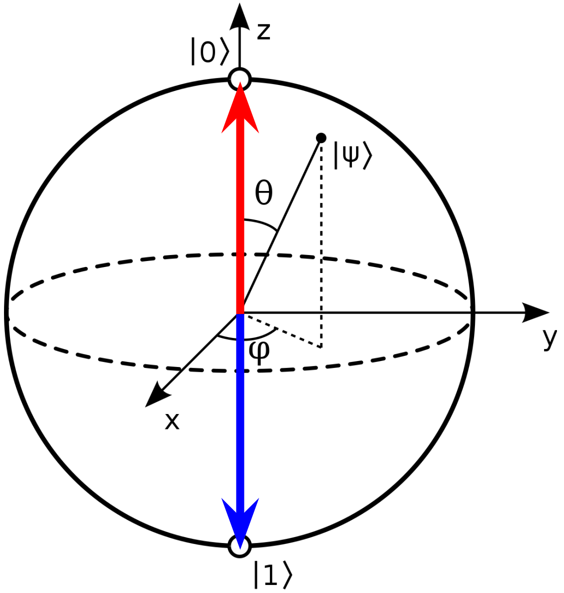
Bit = 0 or 1



Qubit = 0 and 1 combined

Quantum computing - Quantum 101

When measured, qubit collapses to 0 or 1



Qubits allow to compute both possibilities at the same time

Quantum computing - Quantum 101

2 values at the same time is only 2x speedup!

What’s so good about quantum computers?

Quantum computing - Quantum 101

Quantum intrication : when working with multiple qubits, we can link their states !

Instead of N independent qubits, we have a combination representing all 2^N bit vectors

Quantum computing - Quantum 101

1 qubit : 2 states

10 : 1024 states

100 : 1267650600228229401496703205376 states

Exponential speedup !

Quantum computing - Quantum 101

Key concepts

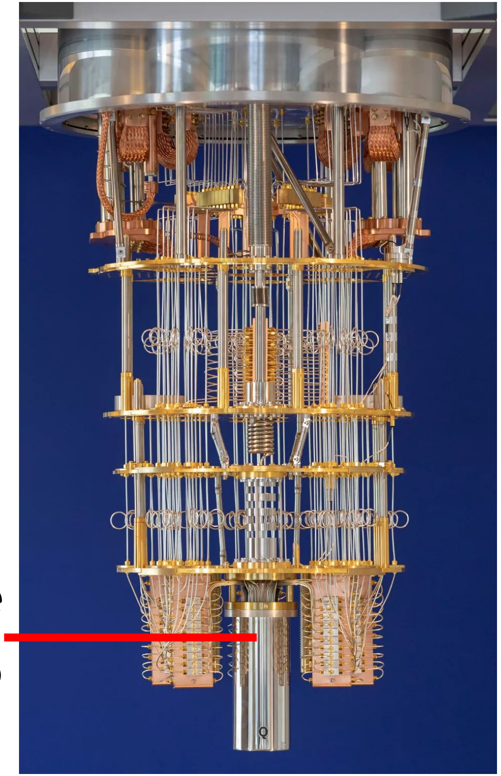
- 2^N simultaneous states
- 1 single measure

Quantum computing - What now?

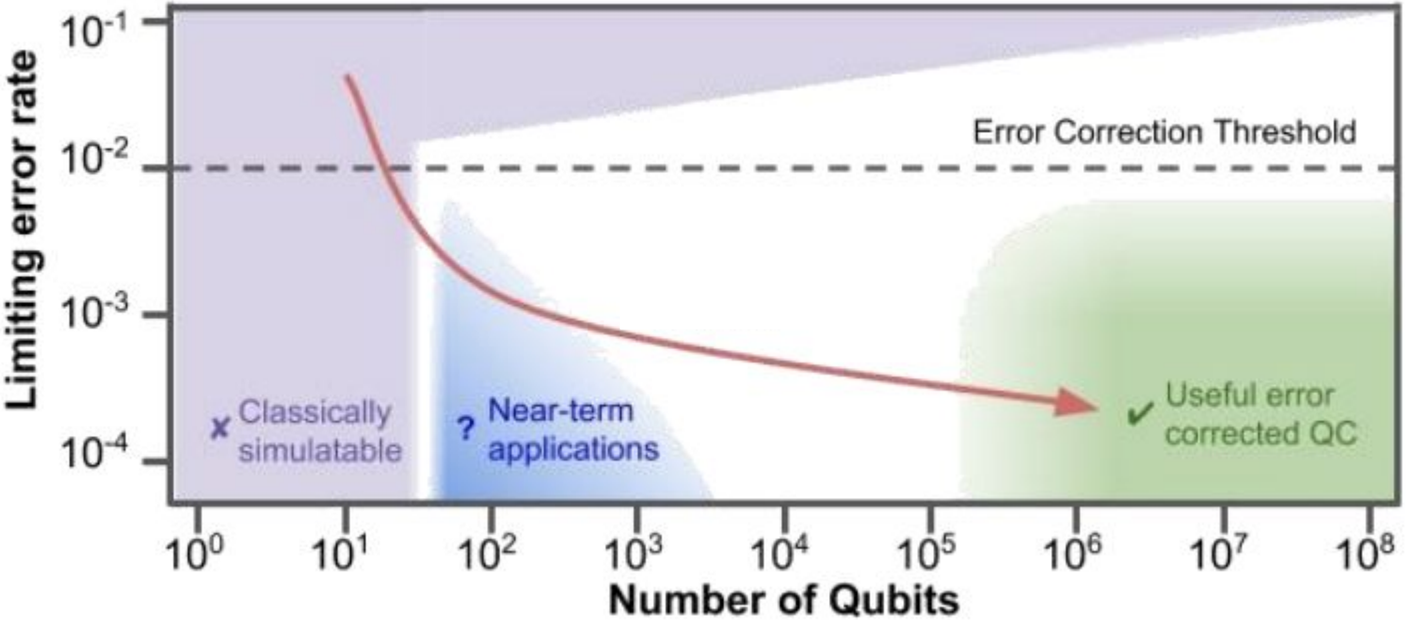
Current issues :

- Qubit are fragile
- Algorithms
- Connecting Qbits

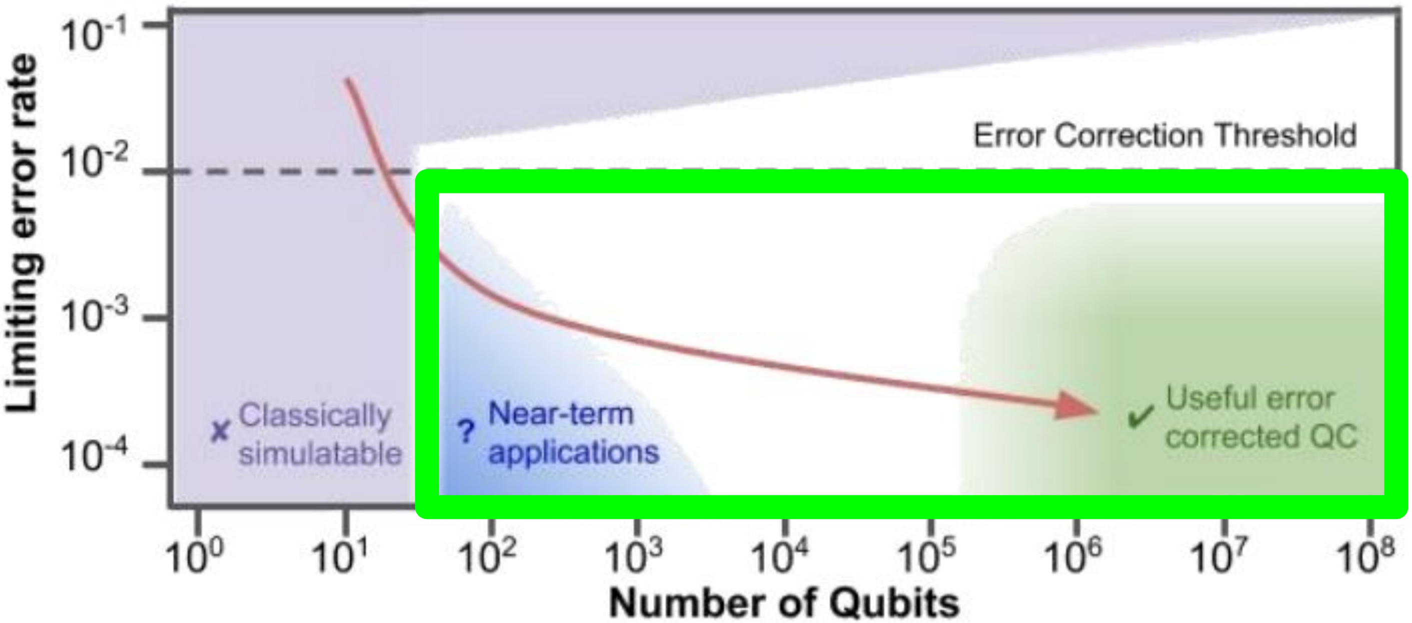
0.01°C above
absolute zero



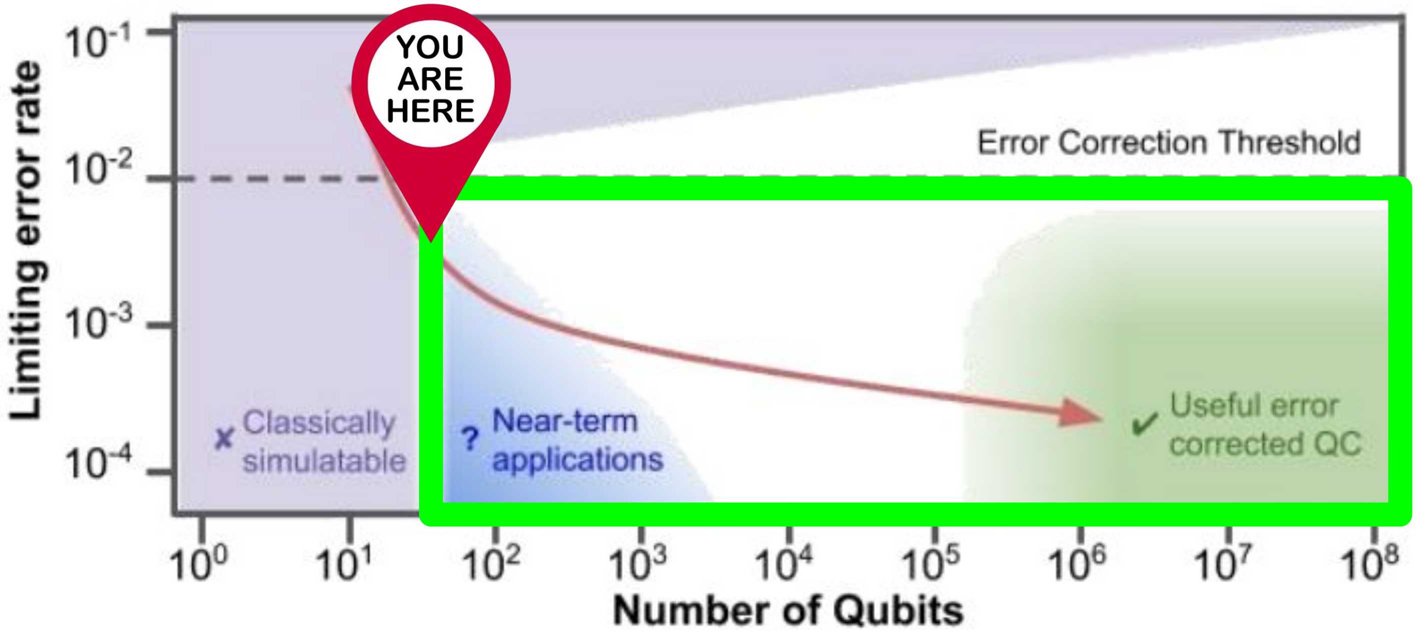
Quantum computing - What now?



Quantum computing - What now?



Quantum computing - What now?



Braking modern cryptography

Two main attacks :

- Shor’s Algorithm
- Grover’s Algorithm

Shor's Attack

$$N = p \times q$$

$$4088459 = 2017 \times 2027$$

Shor's Attack

MIT + Bell Labs

1994

Shor’s Attack

<u>Find a divisor of N ?</u>

Shor's Attack

<u>Find a divisor of N ?</u>

Shor’s Attack

Find a divisor of N ?

1. Pick a random number a

Shor’s Attack

<u>Find a divisor of N ?</u>

1. Pick a random number `a`
2. Find `p → aᵖ % N = 1`

Shor's Attack

Find a divisor of N ?

1. Pick a random number a
2. Find $p \rightarrow a^{p} \% N = 1$
3. $(a^{p/2}-1)$ or $(a^{p/2}+1)$ $\rightarrow$ 36.5% chance!

Shor's Attack

Find a divisor of N ?

1. Pick a random number a
2. Find $p \rightarrow a^p \% N = 1$
3. $(a^{p/2}-1)$ or $(a^{p/2}+1) \rightarrow$ 36.5% chance!

Shor’s Attack

$$a^p \% N = 1?$$

Shor's Attack

$$a^p \ \% \ N = 1?$$

$a^1 \ \% \ N \ = 13$

$a^2 \ \% \ N \ = 25$

…

Shor's Attack

$$a^p \% N = 1?$$

$a^1 \% N = 13$

$a^2 \% N = 25$

…

$a^p \% N = 1$

$a^{p+1} \% N = 43$

…

$a^{2p} \% N = 1$

$a^{2p+1} \% N = 43$

…

Shor's Attack

$$a^p \ \% \ N = 1?$$

$a^1 \ \% \ N = 13$

$a^2 \ \% \ N = 25$

…

$a^p \ \% \ N = 1$

$a^{p+1} \ \% \ N = 43$

…

$a^{2p} \ \% \ N = 1$

$a^{2p+1} \ \% \ N = 43$

…

1 frequency measure

Shor's Attack

Find a divisor of N ?

1. Pick a random number a
2. Find $p \rightarrow N \mid (a^p - 1)$
3. $(a^{p/2}-1)$ or $(a^{p/2}+1)$ $\rightarrow$ 36.5% chance!

Shor's Attack

$$n = p \times q$$

<u>Quantum = death of RSA, DH, El Gamal, ...</u>

Shor's Attack

N-bit prime -> ~N qubits

State of the art

4088459 = 2017 × 2027

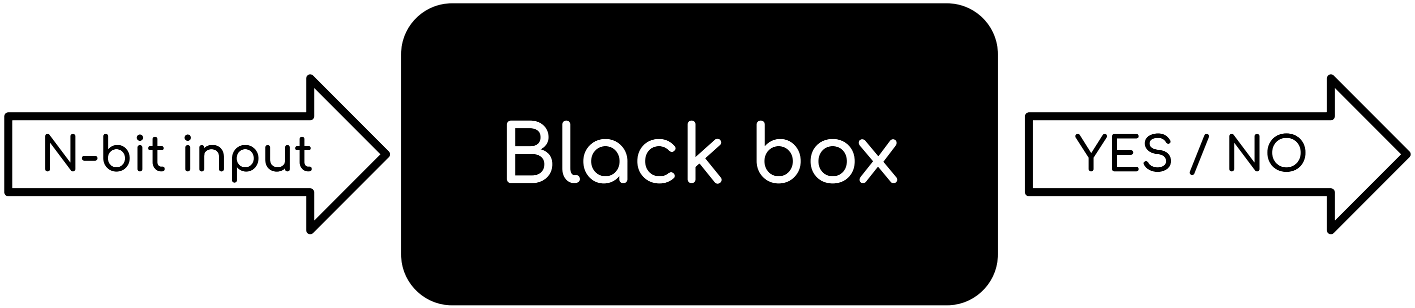
Shor's Attack

Key length	Classical CPU	Quantum CPU
N	$2^{N/2}$	N^3
64 (easy CTF)	10^{10}	10^6
2048 (ANSSI)	10^{308}	10^{10}

Solves an NP problem in polynomial time !

Grover's Attack

Versatile algorithm for search



Finds a valid input that results in YES

Grover's Attack

Can be used for bruteforce search

Reduces the search space from size K to $\sqrt{K}$

Grover's Attack

<u>Key search</u>

"Does AES key xxx give a valid plaintext ?"

<u>Hash cracking</u> (incl. Bitcoin)

"Is md5(xxx) equal to a77b94ffab... ?"

Grover’s Attack

Attacks on N-bit search space are reduced to N/2 bits

Only double key size to resist Grover’s attack, but SHA1 and AES-128 will die

Other algorithms

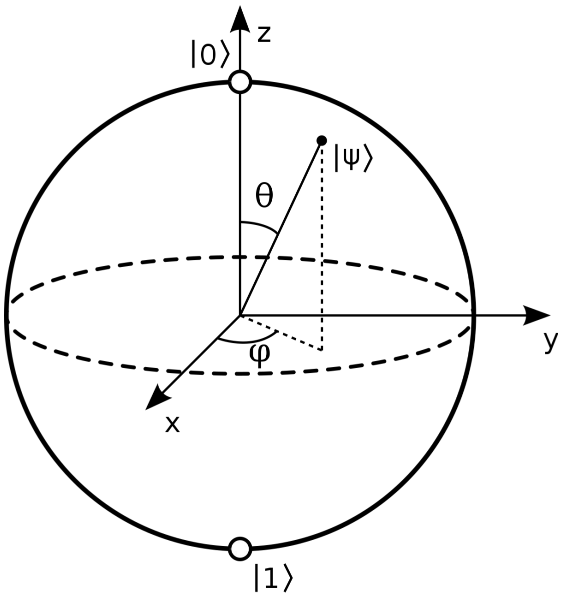
Why are quantum algorithms
so hard to make ?

Other algorithms

- Relatively new area of computer science
- Hard to simulate beyond 50 qubits
- Need to rely more on formal proofs
- Very particular end conditions needed

Other algorithms

Particular conditions



Superposition of all possible states

Measure outputs a single state, destroying intrication

Other algorithms

Output state is unreliable, will change every time

state	p(state)
000	0.24
001	0.02
010	0.06
011	0.13
100	0.16
101	0.11
110	0.18
111	0.10

Other algorithms

Output state is reliable
Run a few times to be sure

state	p(state)
000	0
001	0
010	0
011	0.01
100	0
101	0.99
110	0
111	0

Other algorithms

With many qubits, need to make every incorrect state probability very close to 0

state	p(state)
000	0
001	0
010	0
011	0.01
100	0
101	0.99
110	0
111	0

Other algorithms

Cryptography cemetery :

- RSA
- Diffie-Hellman
- SHA-1 (not only collision)
- AES-128

Are the others safe ?

Defending against quantum adversaries

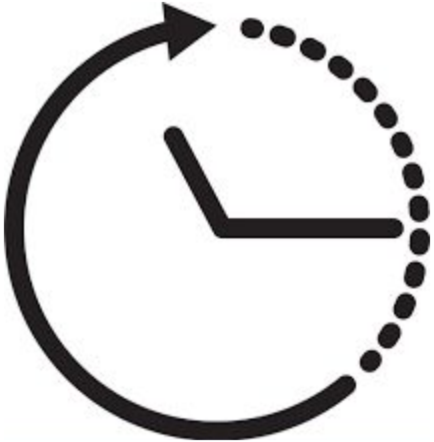
Should we panic?

Defending against quantum adversaries

Are our current communications safe?

Defending against quantum adversaries

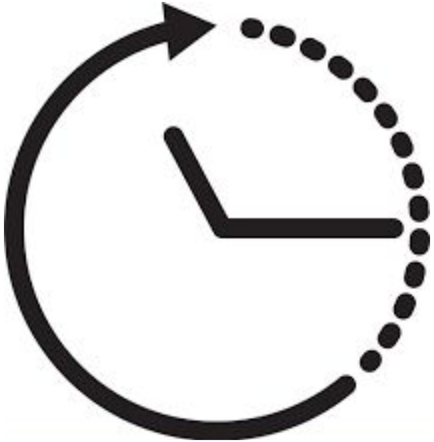
Are our current communications safe?

 +  + $$$

Defending against quantum adv

Are our current communicatior

+



+ $$$

Defending against quantum adversaries

OPEN QUANTUM SAFE

aws

NIST Contest

Defending against quantum adversaries

CLOUDFLARE®

Longer keys (~300B-1kB)
slower handshakes than TLS (~10%)

BUT It's there!

The perfect cryptosystem

How can we design a perfect cryptosystem over an unsafe channel ?

The perfect cryptosystem

- Key entropy ≥ message entropy
- Perfect key sharing scheme
- Authentication
- Perfect implementation

The perfect cryptosystem

- Key entropy ≥ message entropy

  → One-Time Pad

- Perfect key sharing scheme

  → How ?

- Authentication

  → Interesting but complex problem

- Perfect implementation (lol)

The perfect cryptosystem

How to share keys securely ?

Mainly two schemes :

- Pre-Shared Key
- Key exchange

The perfect cryptosystem

Pre-shared key is perfect but unrealistic :

- If using OTP, huge storage
- Can't communicate with new peers

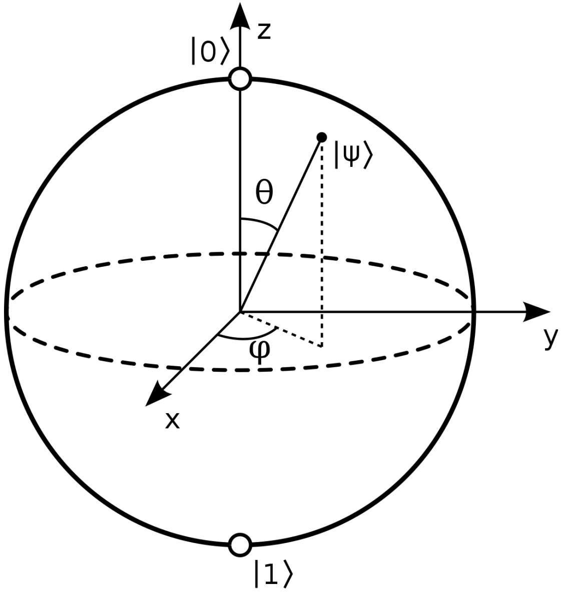
The perfect cryptosystem

What about key exchange ?

Mainly based on Diffie-Hellman, which is broken by Shor :(

The perfect cryptosystem

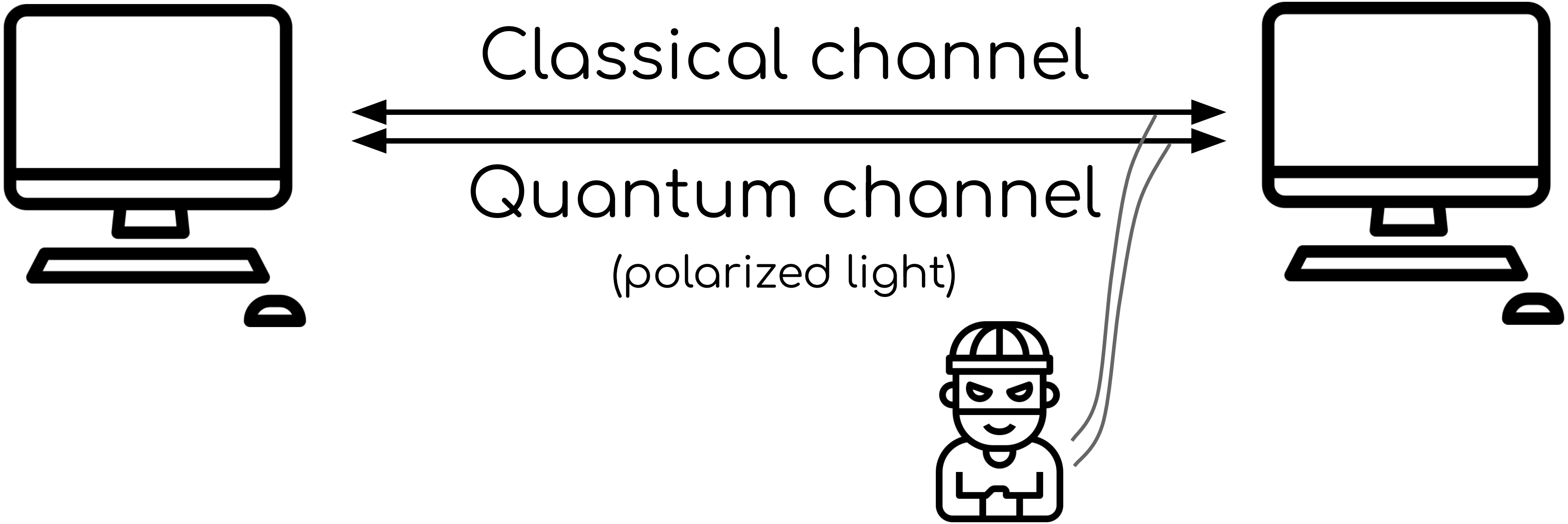
Remember this bad boy ?



We can also use quantum superposition for secure exchanges !

The perfect cryptosystem

Introducing Quantum Key Distribution, BB84



The perfect cryptosystem

Data transmitted is random

- Cannot send the message directly
- Use the shared bits as a key

The perfect cryptosystem

How does BB84 work ?

The perfect cryptosystem

Each photon carries 2 informations :

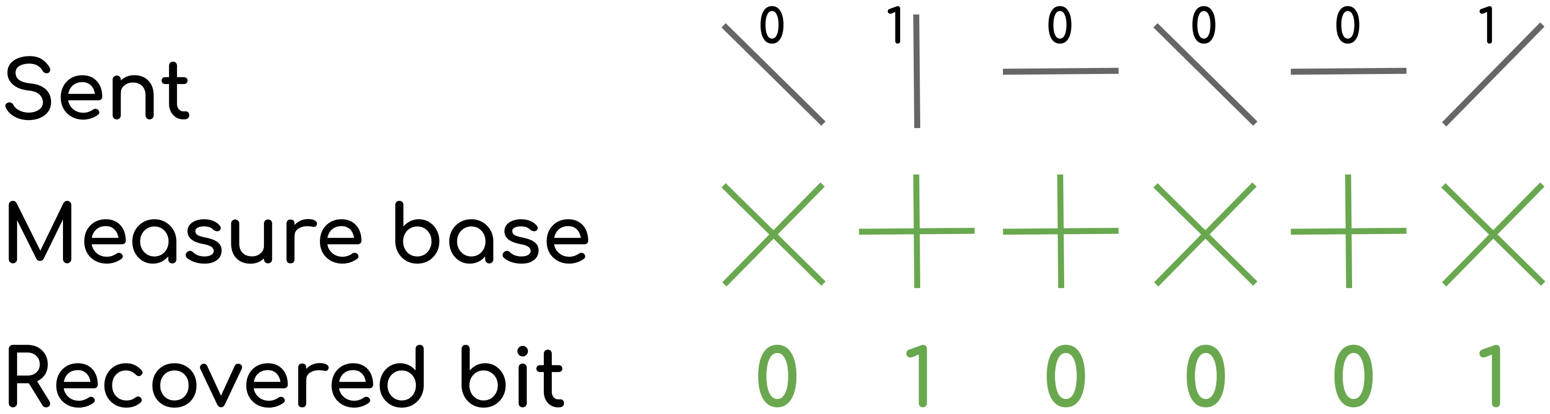
- Base
- Value

	×	+
0	╲	―
1	╱	│

The perfect cryptosystem

The receiver chooses a base randomly

If base is correct, original value recovered



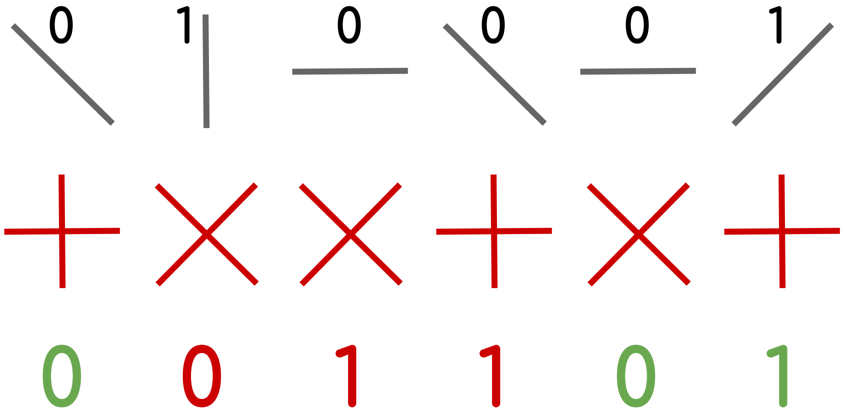
The perfect cryptosystem

If base is incorrect, random value recovered and the original value is destroyed

Sent

Measure base

Recovered bit

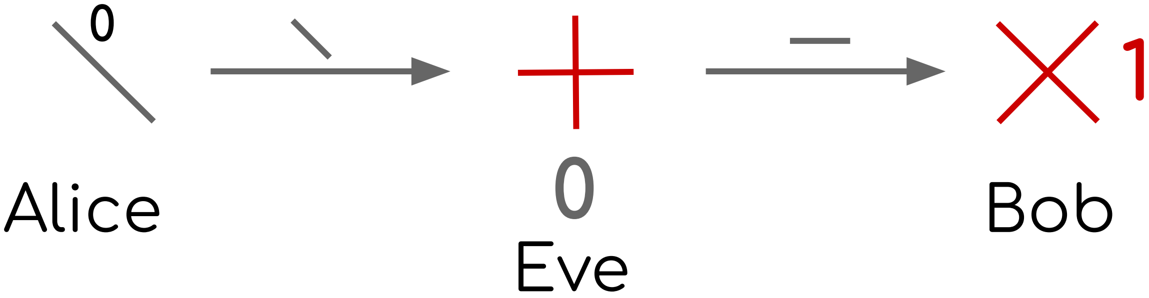


The perfect cryptosystem

Someone intercepting the exchange doesn't know the base and risks altering the bits

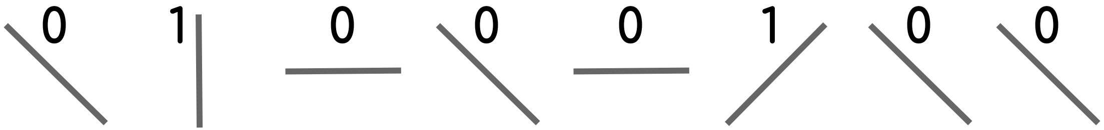
The perfect cryptosystem

Someone intercepting the exchange doesn’t know the base and risks altering the bits

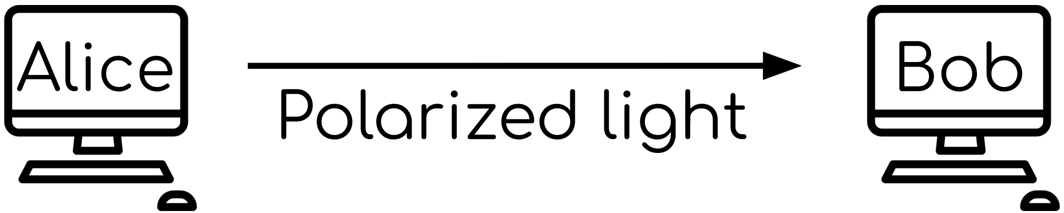


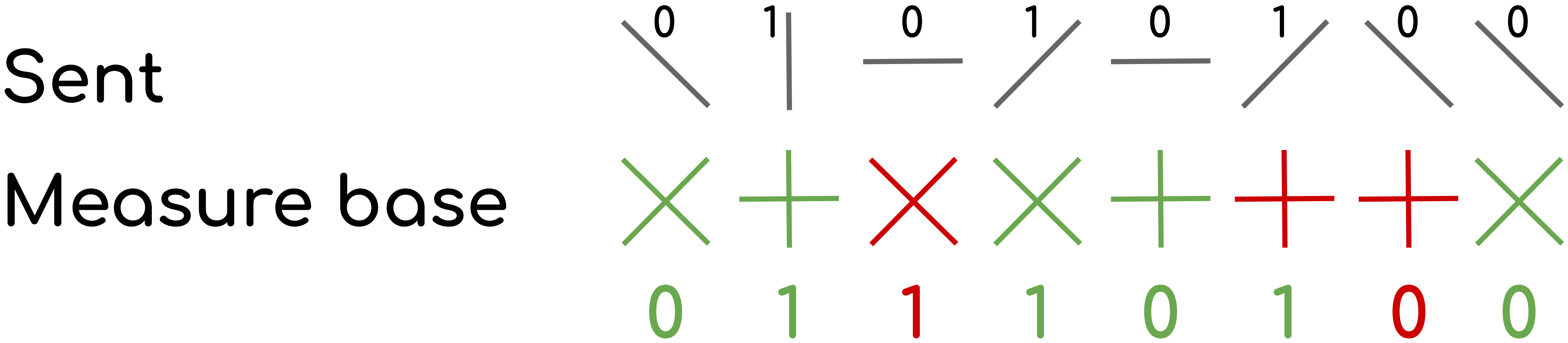
The perfect cryptosystem

Sent

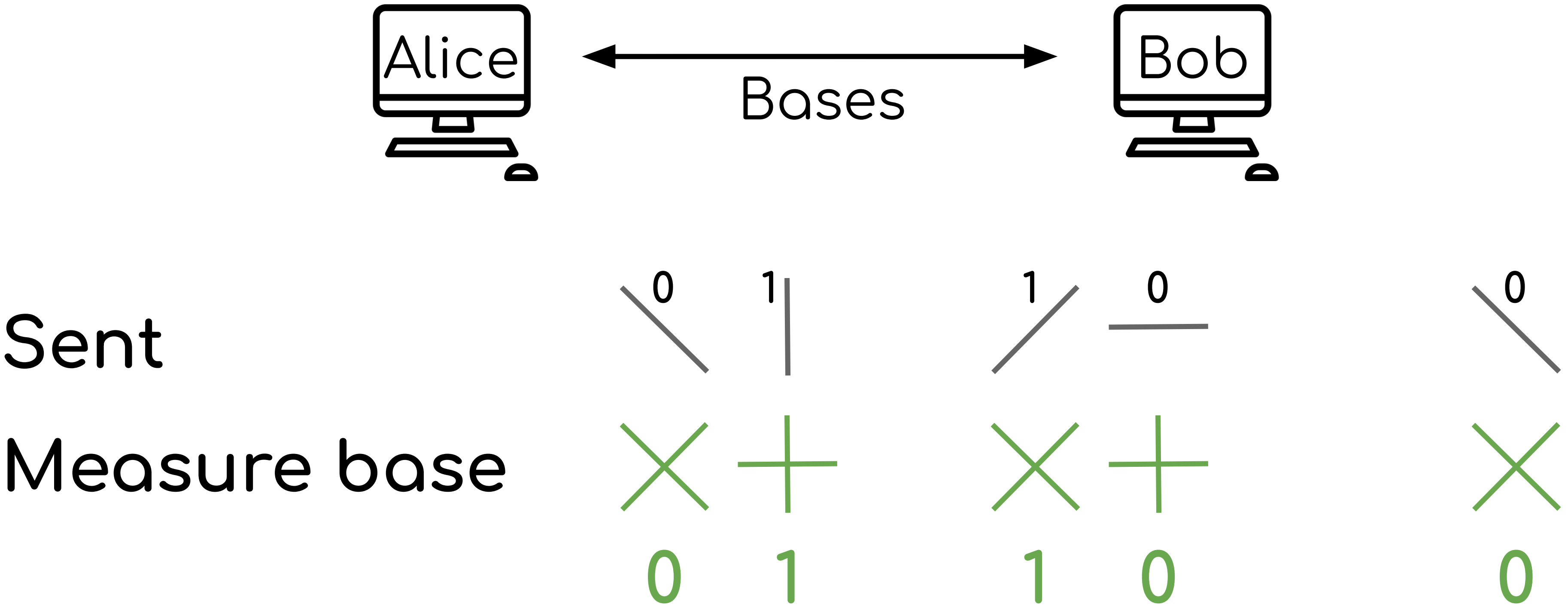


The perfect cryptosystem

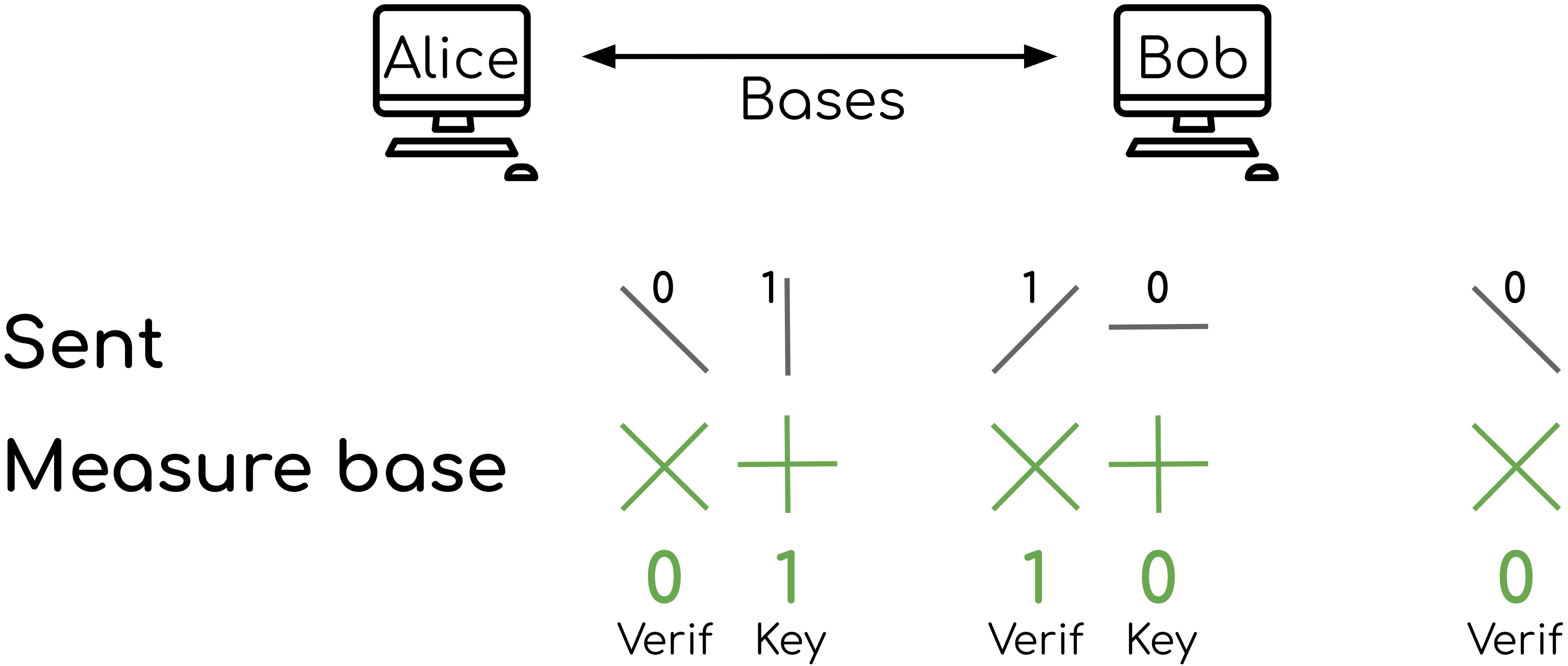




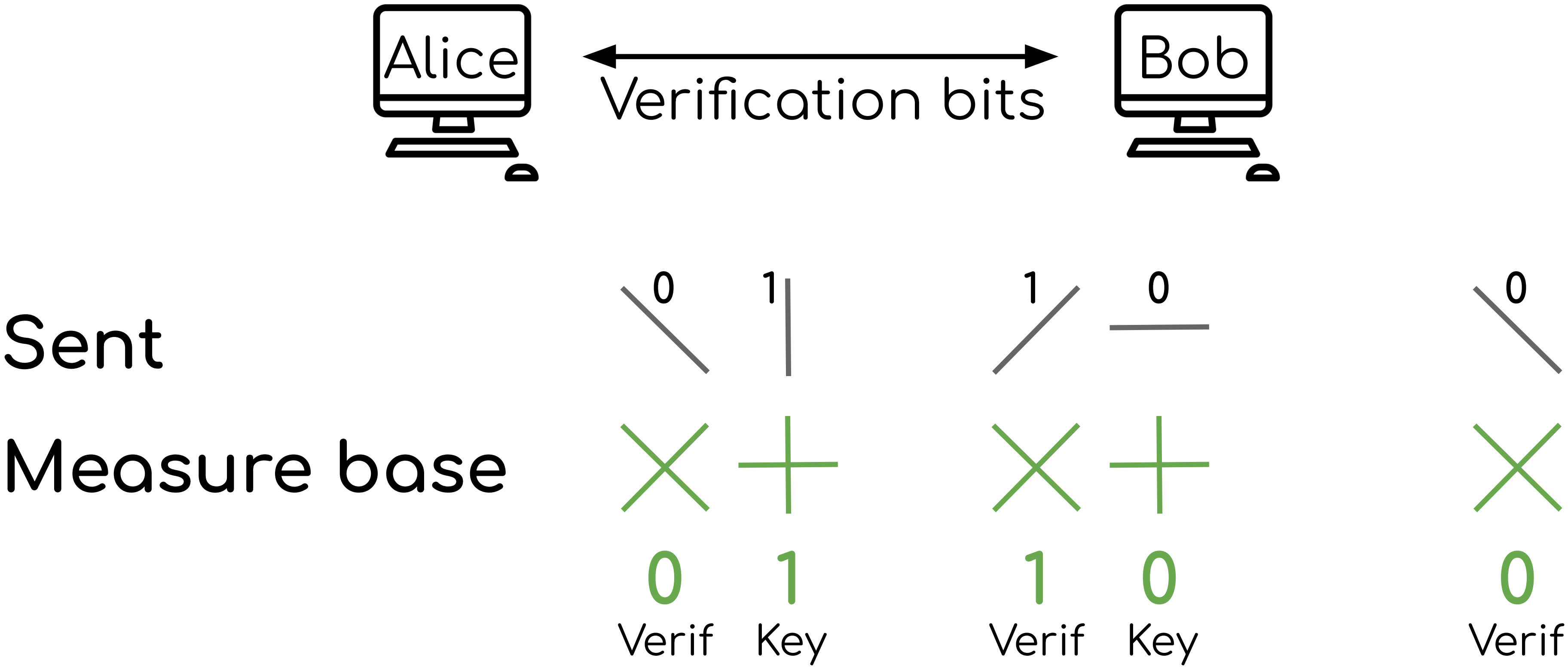
The perfect cryptosystem



The perfect cryptosystem

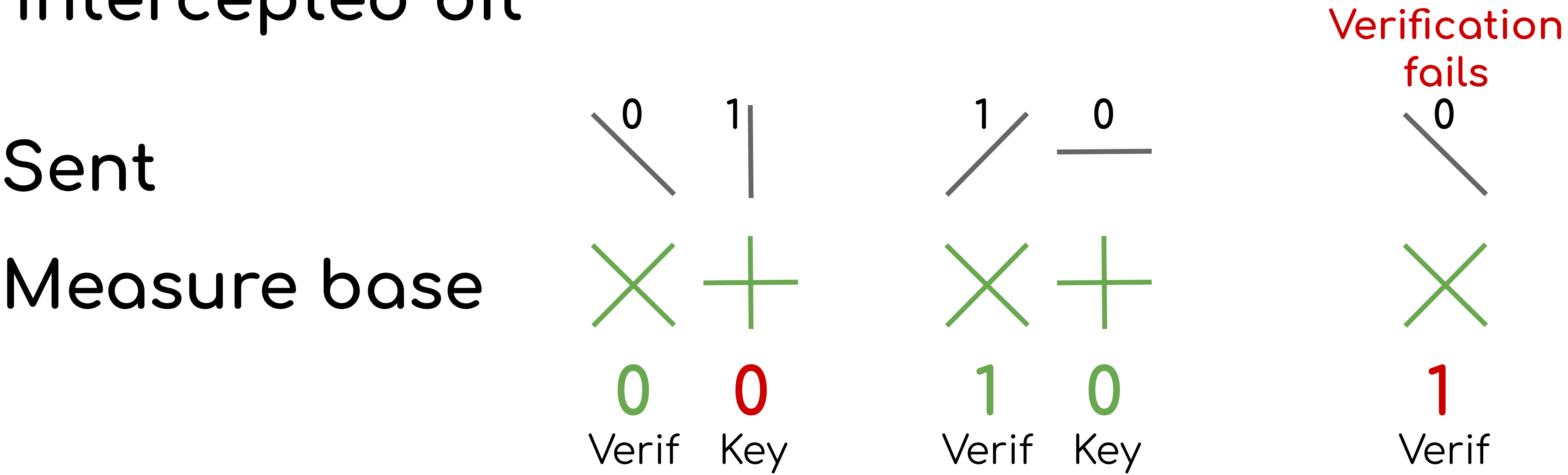


The perfect cryptosystem



The perfect cryptosystem

Attacker has a 25% chance to flip each intercepted bit



The perfect cryptosystem

With N verification bits, probability $1-0.75^N$ to discover the attack

Only 100 verification bits give the attacker a 1:3000000000000 chance of stealth

Conclusion

Many unknowns about quantum technology

Likely to be the next tech revolution

Will change the face of crypto as we know it

Take quantum as an ally

About h25

We do serious stuff

- Coding challenges
- CTFs

About h25

... but mostly fun stuff

discord.h25.io

live.h25.io

Thanks !

Any questions ?