24/ NOV/ 2020

DE 09.00 A 11.00 HRS.

SEMINARIO

EL FUTURO DE LA SEGURIDAD EN LAS COMUNICACIONES DIGITALES

Universidad de Concepción

ALIANZA CHILENA DE CIBERSEGURIDAD

ORGANIZAN:

MIRO

ACTI

SeQure

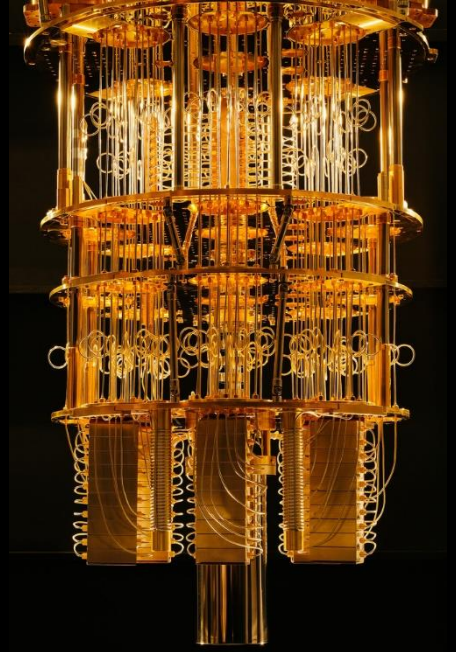
COLABORAN:

Transmisión segura de datos con tecnologías post-cuánticas

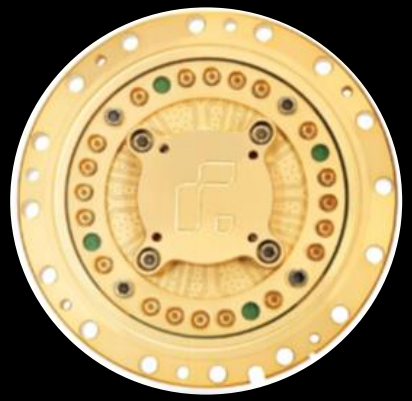
Dr. José M. Brito

CSO - GoQuantum

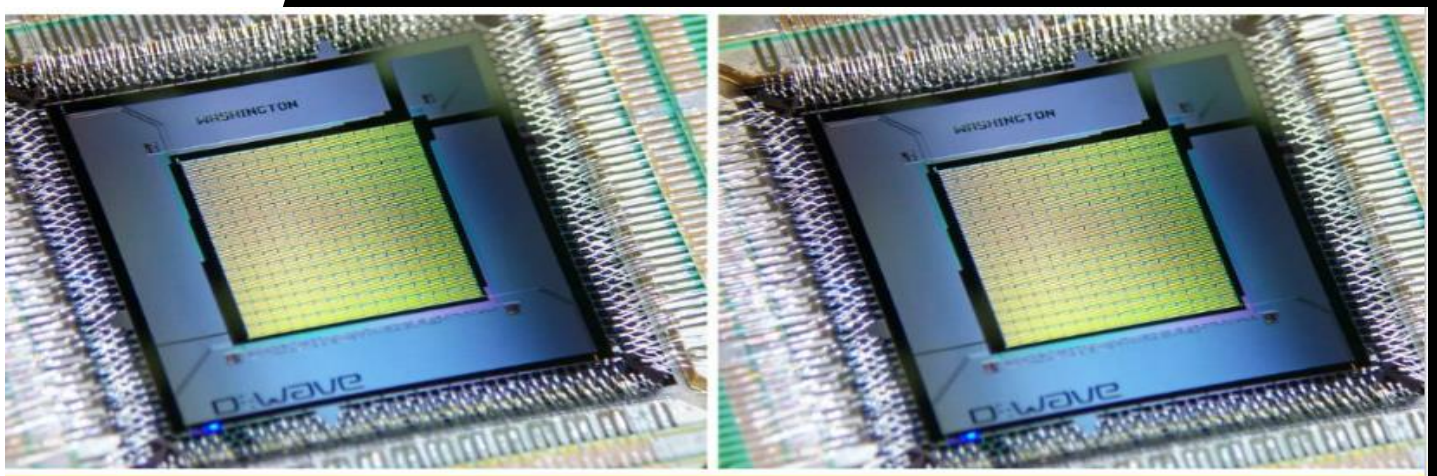
Computación Cuántica



IBM’s Q Computer



Rigetti’s Quantum chip

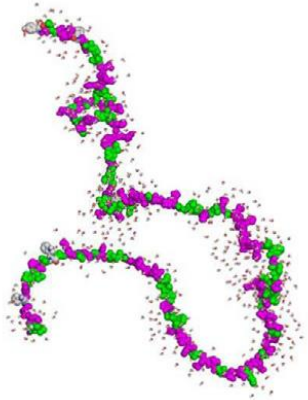


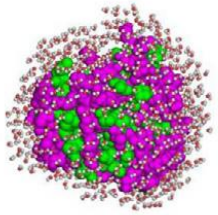
D-Wave

TECH

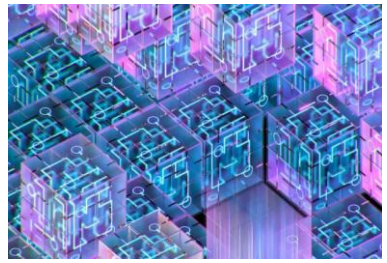
Google's Quantum Computer Is 100 Million Times Faster Than Your Laptop

DAVID NIELD 10 DEC 2015

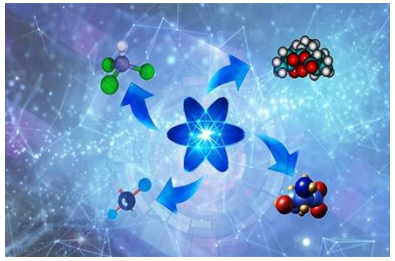




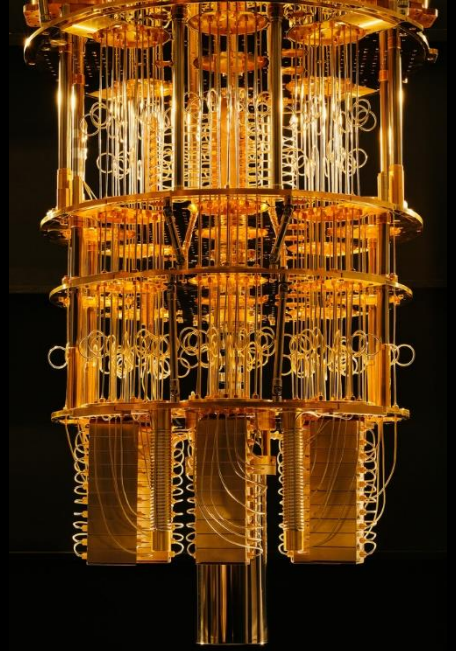
Secuenciado ADN



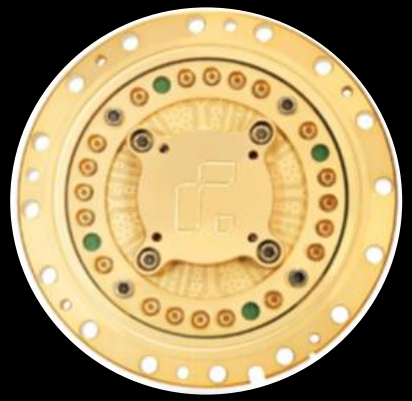
Machine Learning



Medicamentos



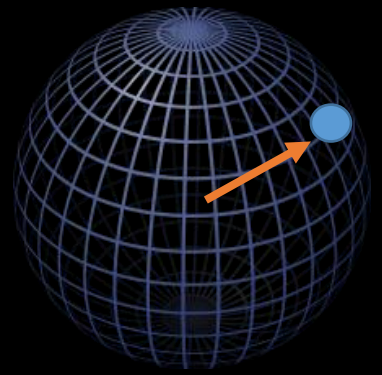
IBM’s Q Computer



Rigetti’s Quantum chip

Bit cuántico - Qubit

$|0\rangle$



$|1\rangle$

$$\Psi = \alpha|0\rangle + \beta|1\rangle$$

- Estado de Superposición (Vector)
- Diferentes implementaciones físicas posibles (superconductores - átomos)

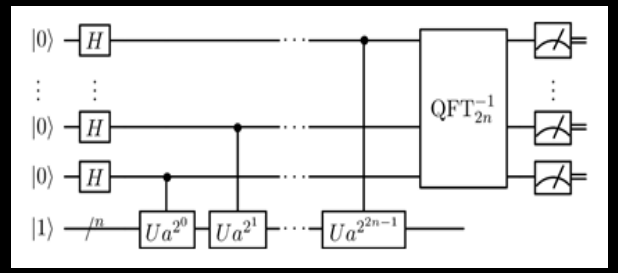
Un (gran) problema: Algoritmos cuánticos

Seguridad actual basada en Hard - Problems

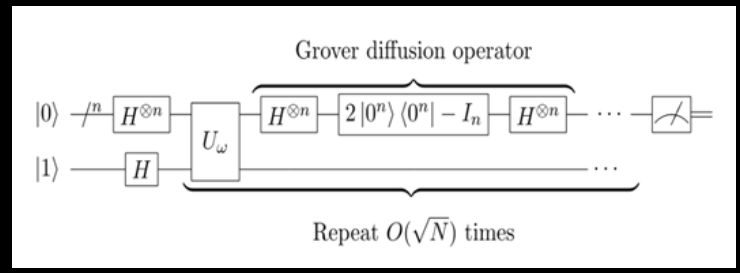
Algoritmos cuánticos: Shor – Grover afectan fuertemente la criptografía estándar y sus llaves.

Shor: 1000 años vs 1 día para factorizar un número de 650 bits [VanMeter2013]

Shore : Factorización



Grover: Búsqueda



Un (gran) problema: Algoritmos cuánticos

Seguridad actual basada en Hard - Problems

Algoritmos cuánticos: Shor – Grover afectan fuertemente la criptografía estándar y sus llaves.

(computación cuántica) … afectará seriamente **la confidencialidad e integridad de las comunicaciones digitales** en internet y en general…

Reporte Criptografía PostQuantum NIST NISTIR 8105
US National Standards Institute

Algoritmos más usados para proteger comunicación digital (móvil,internet,etc) !!

CRYPTOGRAPHIC ALGORITHM	TYPE	PURPOSE	Impact from large-scale quantum computer
AES	Symmetric Key	Encryption	**Large key sizes needed**
SHA-2, SHA-3	---------	Hash functions	**Large output needed**
RSA	Public Key	Signatures, Key establishment	**No longer secure**
ECDSA, ECDH (Elliptic Curve Cryptography	Public Key	Signatures, Key exchange	**No longer secure**
DSA (Finite Field Cryptography)	Public Key	Signatures, Key exchange	**No longer secure**

Campagna et al, (2014) **Quantum Safe Cryptography and Security, ETSI Report (22 Experts panel, European Telecommunications Standards Institute)**

EDITION: US

ZDNet

VIDEOS 5G WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS

JUST IN: Quora discloses mega breach impacting 100 million users

IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.

By Tom Foremski for Tom Foremski: IMHO | May 18, 2018 -- 18:24 GMT (11:24 PDT) | Topic: Security

BBC Sign in News Sport Weather Shop Earth Trav

NEWS

Home Video World UK Business Tech Science Magazine Entertainme

Business Market Data Markets Economy Companies Entrepreneurship

Quantum computing: Game changer or security threat?

By Zoe Thomas
Technology of Business reporter

5 April 2016 | Business

MIT Technology Review

Topics+ Top Stories

Connectivity

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption—but doesn't yet know what to do about that problem.

by Tom Simonite February 3, 2016

CSO

OPINION

The quantum computing cyber storm is coming

What cyber leaders need to know now to protect their critical data in the quantum era.

By Alan Usas, Contributor, CSO | JUL 9, 2018 12:45 PM PT

Opinions expressed by ICN authors are their own.

MORE LIKE THIS

How quantum computers will destroy and (maybe) save cryptography

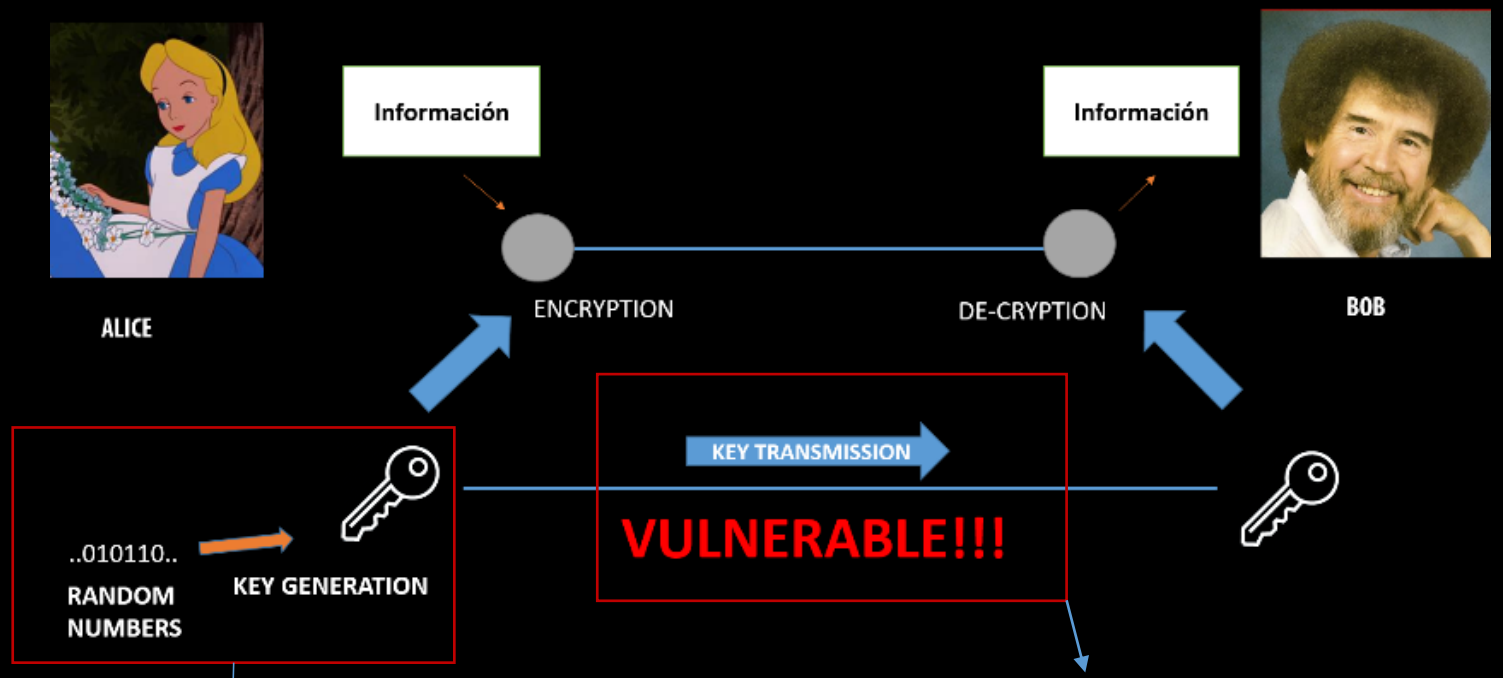
Gran problema actual: Colección de Datos

- **La c. cuántica aun requiere tiempo para madurar (10-20 años)**
- **Harvest&Decrypt => Almacenar, luego desencriptar**
- **Cambiar a nueva criptografía requiere tiempo!**
- **Nuevas necesidades de hardware- compatibilidad**

NSA Data Center - 10^6 TERABYTES

Países inviertiendo intensivamente para proteger u información: EEUU, EU, CHINA

Vulnerabilidades



2 Grandes vulnerabilidades

Distribución de llave pública

Gen . Segura (privada) de llaves

- Generación pseudo aleatoria

- Hardware intervenible

Nuevas Posibilidades: Tecnologías Cuánticas

Quantum Key Distribution (QKD) : Encriptación de estados cuánticos

Desventajas

- Necesidad de redes de fibra -> NO compatible con todas las tecnologías
- Ordenes de mangitud diferencia en Costo

Change, before you have to.

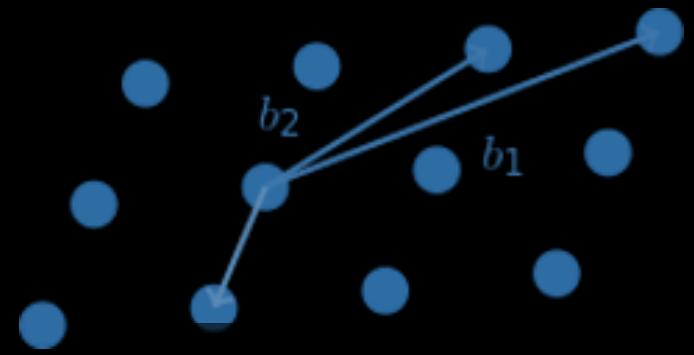
– Jack Welch

Post-quantum Secure Data Transmission Devices

Criptografía post-cuántica

Criptosistemas CLÁSICOS basado en problemas también complejos para computadores cuánticos.

- **Lattice-based Crypto →SVP Problem**



- **Multivariate polynomials Crypto**

- **Code-based (linear) Crypto**

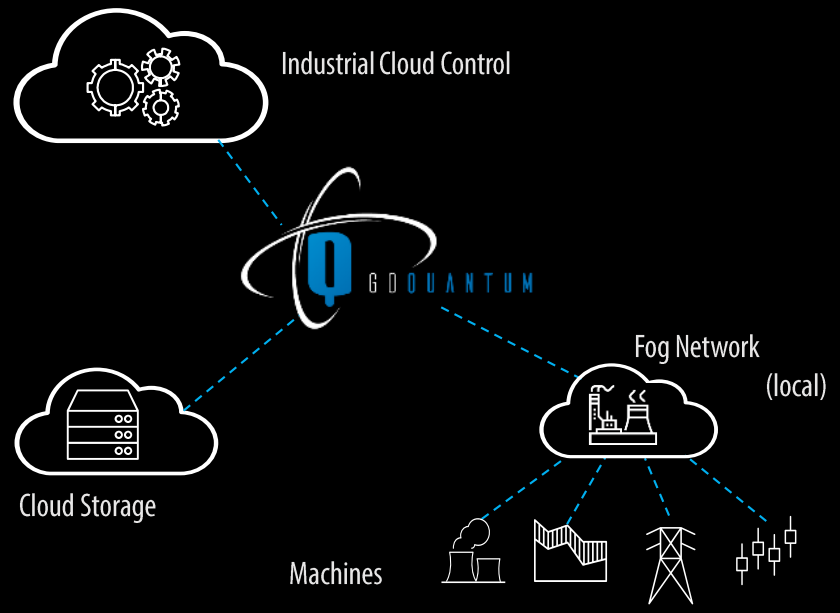
- **Supersingular elliptic curve isogeny Crypto**

- **Hash-based Crypto (Hash-trees)**

GOQUANTUM

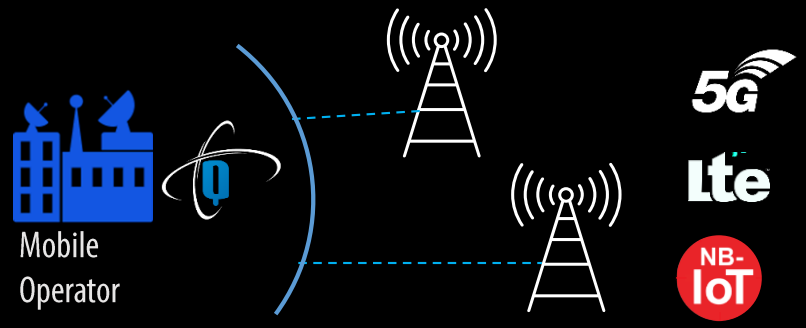
USE CASES

Post-Quantum IoT Edge



Post-Quantum Telecom

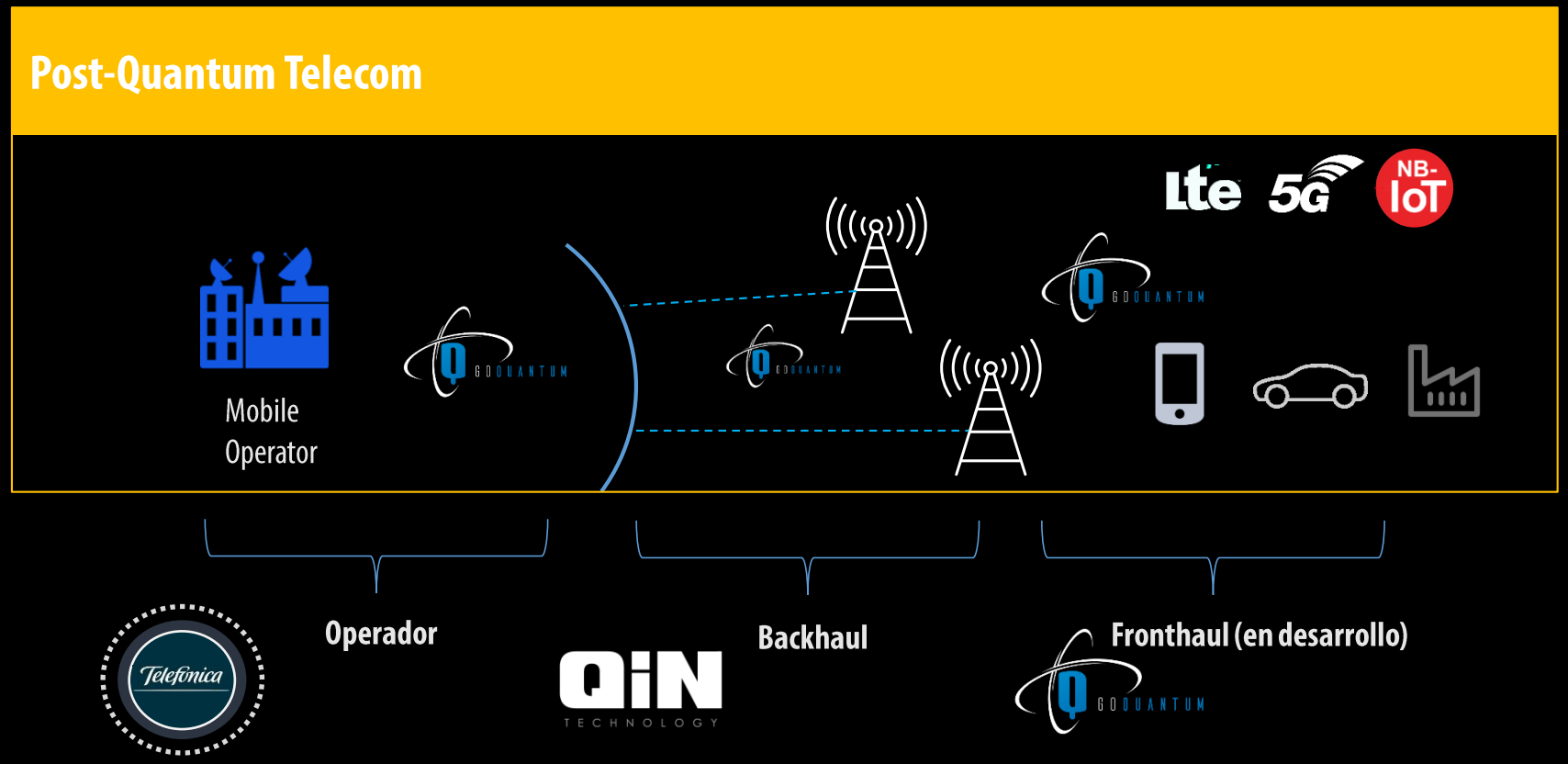
-Backhaul
-RAN



Post-Quantum Safe Personal VPN

GOQUANTUM

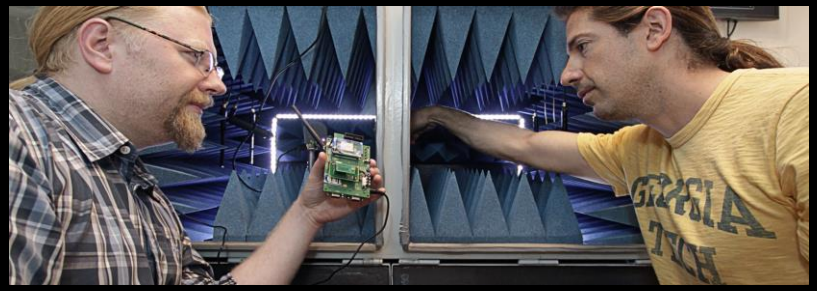
USE CASES



Protección de comunicaciones

Conclusiones

- Computación cuántica debe ser considerada
- Estrategias de adaptación toman tiempo, actuar ahora!
- Tecnologías cuánticas y post-cuánticas son necesarias
- Es posible realizar implementaciones con tec. actual



Contacto

José M. Brito

E: jose@goquantum.tech | **W:** goquantum.tech

Chile: Santiago | **Germany: Berlín**