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:

Comunicaciones Cuánticas Seguras

Gustavo Moreira Lima

UDEC/MIRO/SeQure

Objetivo

. Promover el desarrollo de equipos propios, basado en nuevas tecnologías cuánticas, para la seguridad incondicional de enlaces ópticos de comunicación en Chile.

. Creando así una infraestructura de comunicación chilena moderna, de alta capacidad, que fortalece la seguridad nacional.

Pertenecía secretamente a la CIA

1970 – 2018 (?)

HAGELIN-CRYPTOS
CRYPTO AG

Empresa SUIZA

Sabotajes en:
. Hardware
. Algoritmos
. Software

Clientes:
. América Latina
. Irán
. Israel
. India

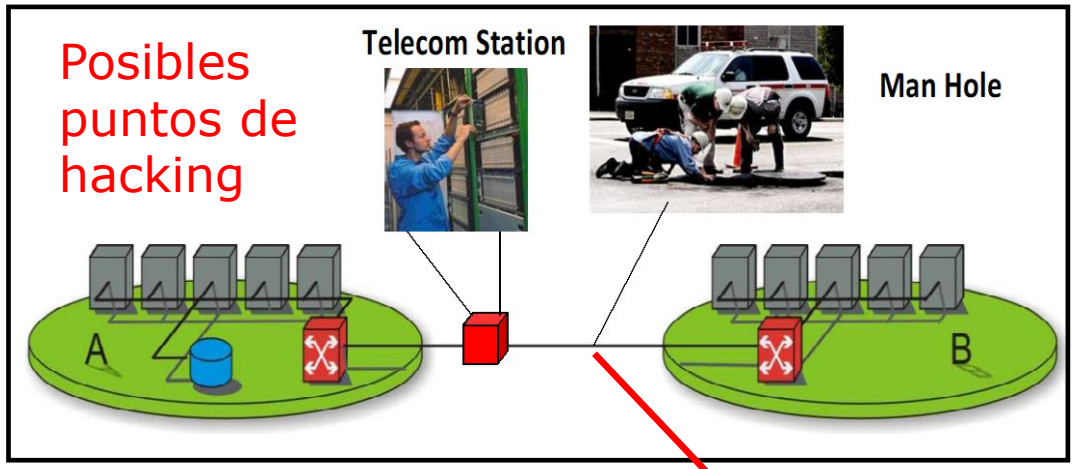
Resultados:

. Inteligencia contra las fuerzas militares argentinas en la guerra de las Malvinas.

. Monitoreo de regímenes militares, etc…

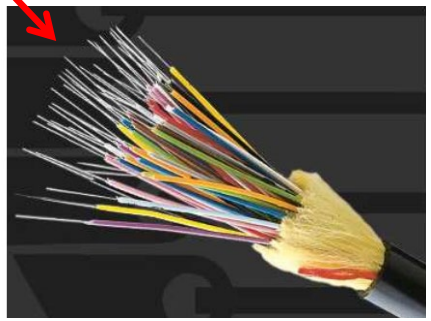
Porque NO es segura la red clásica de comunicación?

1) Vulnerabilidade física para copia de sinales transmitidos



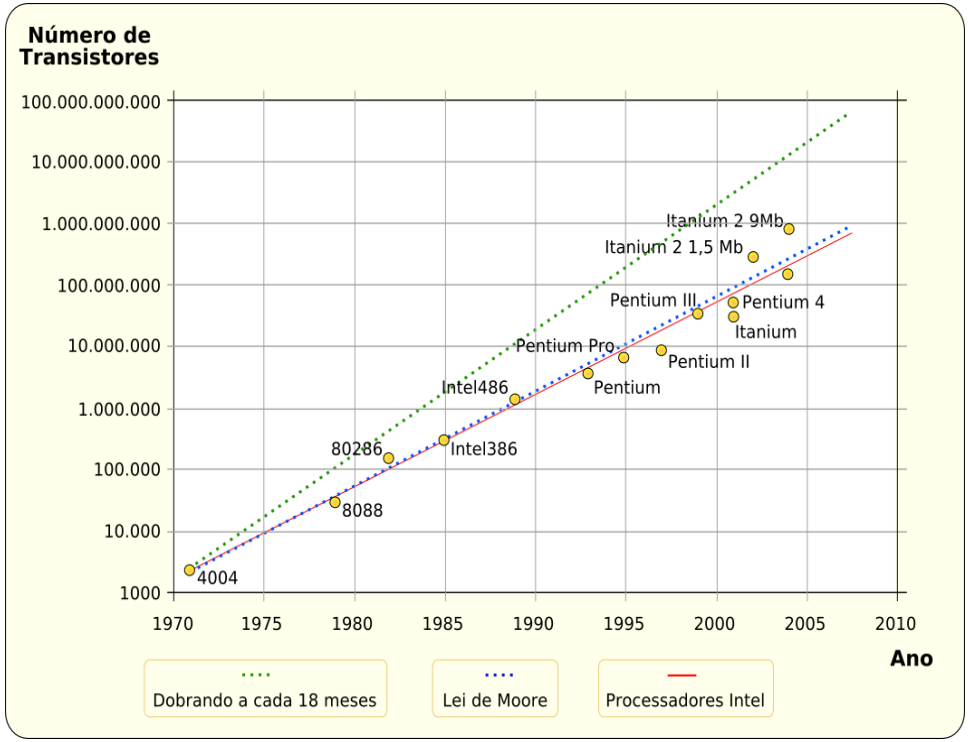
Posibles ataques

Acoplador óptico



2) Sinales copiados son hackeables en escalas de tempo relativamente cortas

Moore's law



En enlaces de comunicaciones cuánticas, la seguridad es garantizada por las leyes de la física cuántica. **La seguridad es incondicional.**

Ventajas de la Comunicación Cuántica

1) Ocupa la misma rede de fibras ópticas actual. Cambios menores de hardware en el transmisor.

Quantum Transm.

Quantum Receiver

2) Se basa en el cifrado simétrico de llaves, que son distribuidas de forma segura (QKD).

$|\psi\rangle$

Espia

Seguridad de la distribución de llaves

$\nexists$ "Máquina de clonaje":

Mediciones → Errores →

Presencia del Espía detectada!

La criptografía en la era de los Computadores Cuánticos

The beginning of the end for encryption schemes?

New quantum computer, based on five atoms, factors numbers in a scalable way.

Cryptography will rely on:

1) Quantum-resistant classical cryptographic algorithms

- For everyday users
- For sensitives documents of big corporations

2) Quantum cryptography

- Unconditional security

Escenarios Industriales Relevantes para QC

1. Banking Industry: Protecting sensitive client information

ID Quantique (IDQ) has successfully demonstrated the use of quantum communications in the banking industry to secure data.

2. Financial Industry: Safeguarding critical business data

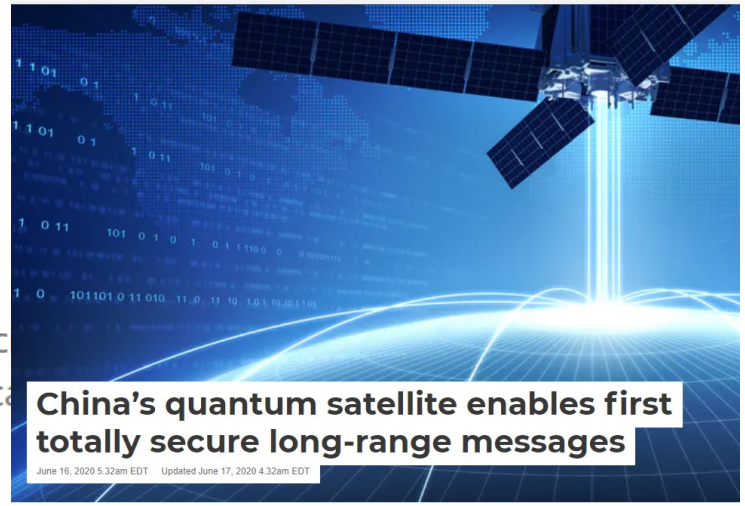
Quantum communications have been employed for high-security networks in the financial industry. IDQ, working with the United Kingdom's Colt Technologies and Services Group

-
-
-

4. Government and defense industry

Quantum communications will be tremendously beneficial for governments and defense agenc
amounts of classified data with long-term sensitivity, both inside the country and on a global sc

-
-
-



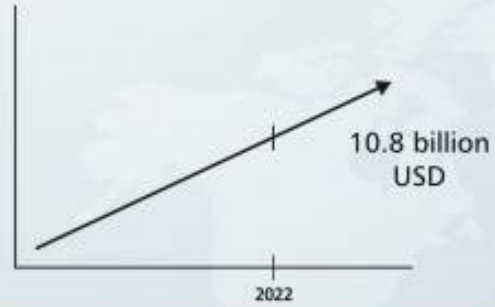
Source: Quantummxc.com

Proyección Mercado Tecnologías Cuánticas

QUANTUM COMPUTING TECHNOLOGY INNOVATIONS LANDSCAPE

pintels™

Quantum Computing Market Size



Top Players

- IBM
- Google
- Nokia
- ID Quantique
- KPN
- Fujitsu
- Intel
- Microsoft
- Magiq
- Quintessence Photonics
- D Wave
- Evolution
- Lockheed Martin

Key Market Segments by Technology

- ☐ Superconducting loops technology
- ☐ Trapped ion technology
- ☐ Topological Qbits technology

Market Segmentation

By End User

- Aerospace and defense
- Federal Government
- IT and Telecomm
- Transportation
- Healthcare
- Chemistry

By Applications

- Optimization
- Quantum encrypted Communications
- Artificial Intelligence
- Smart Manufacturing and Logistics
- Quantum Computing devices

Equipos para comunicaciones cuánticas ya están disponibles en el mercado desde 2007

- Distancia máxima lograda: 500 Km en fibras

Creemos que Chile puede tener una penetración importante en este segmento del mercado en LATAM

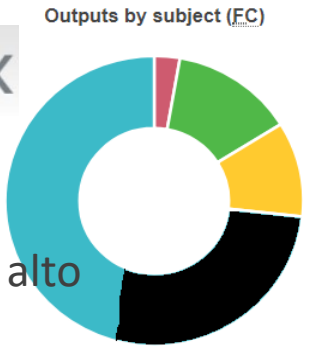
Comunicaciones Cuánticas UDEC

- **Equipo multidisciplinario especializado, de alta productividad científica y conectado internacionalmente**
- **Capacidades de frontera en instrumentación**
- **Experiencia en transferencia tecnológica e innovación**

AC	FC
50	5.60

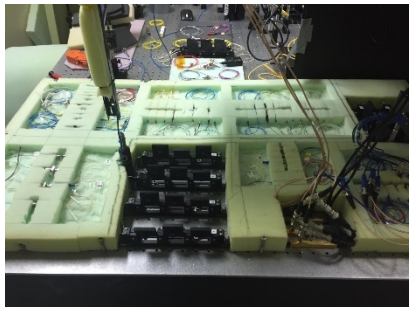
nature INDEX
2018

30%
Publicaciones de alto impacto UdeC



milenio INICIATIVA CIENTÍFICA

CONICYT Ministerio de Educación Gobierno de Chile



300 millones anuales

Empresa asociada Spin-off

SeQure

Quantum Technologies for the Future

Experiencias en innovación colaborativa

Equipo comercial en desarrollo: Generador cuántico de números aleatorios auto-certificable en tiempo real

Empresas Involucradas:

SeQure

Loteria

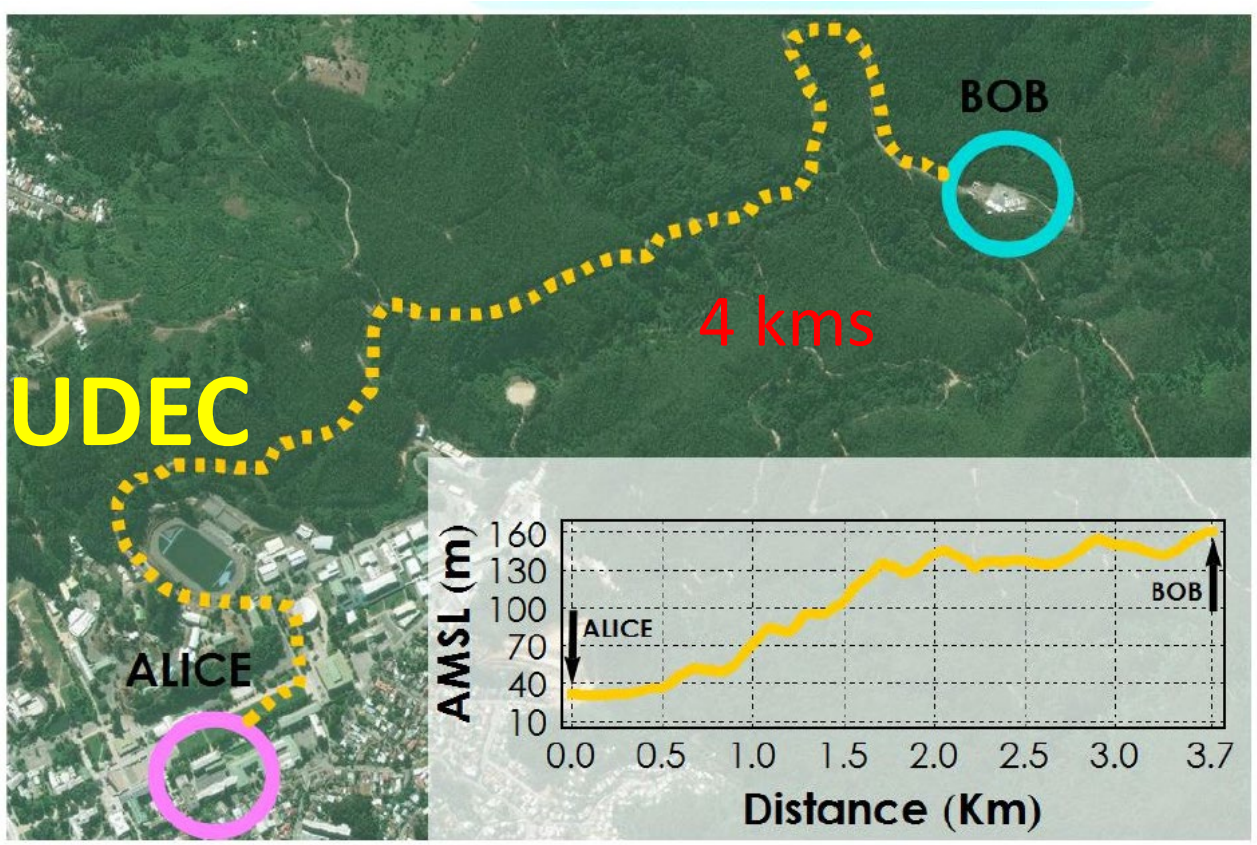
Serpel

Solicitud Patente Internacional:

Solicitud PCT/PL2020/050032 titulada "*Method for quantum generation of random numbers especially in lotteries and gaming and device for quantum generation of random numbers*"

- Inventores: Dr. Gustavo Moreira Lima (UdeC) y Dr. Marcin Pawlowski (U Gdansk)
- Fecha presentación: 24 de abril de 2020
- Oficina receptora: Patent Office of The Republic of Poland
- Titularidad: 50% UdeC | 50% U Gdansk

Desarrollos Tecnológicos en Comunicaciones Cuánticas



. Generación de claves ultra-secretas en la red actual de telecomunicaciones.

Permite:

Transmisión de información de forma incondicionalmente segura entre distintos edificios de industrias y agencias gubernamentales.

Desarrollos Tecnológicos en Comunicaciones Cuánticas

2) Desarrollo de equipos en comunicaciones cuánticas

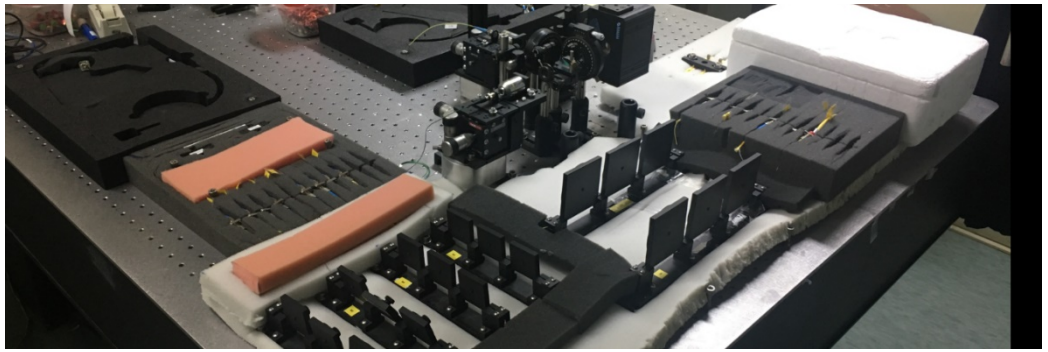
Transmisor Receptor

Equipo Avanzado en Fase TRL 7 (prototype demonstration in a relevant environment)

. Generación de claves ultra-secretas en **distancias metropolitanas**.

Key Rate: 10 Kbit/s over 48 km.

3) Nuevo proyecto: TRL 4 (Validated in laboratory)



Newly developed devices

. Generación **RAPIDA** de claves ultra-secretas en **distancias metropolitanas**.

Expected Rate: 1 Mbit/s over 50 km.

GRACIAS !

Contacto:

- Gustavo Moreira Lima

glima@udec.cl