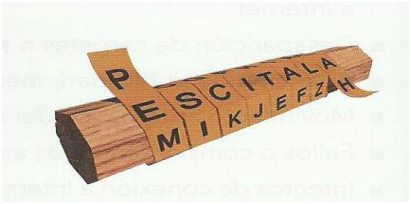
ARSAT

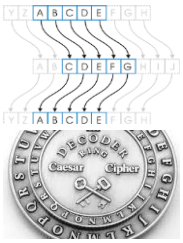
INVAP

CRIPTOGRAFÍA MILITAR: evolución de las comunicaciones secretas

Hugo D.Scolnik

Las comunicaciones secretas son **absolutamente vitales** para el desarrollo de actividades militares y diplomáticas.

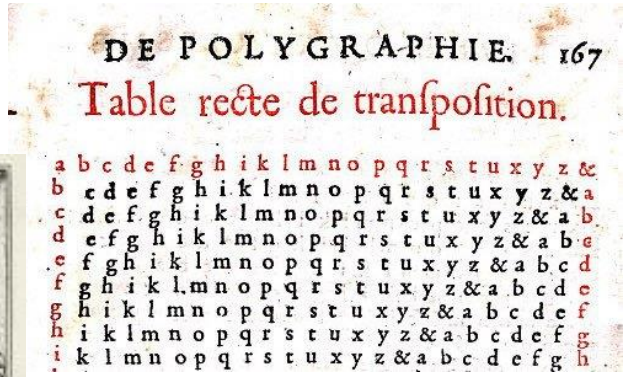


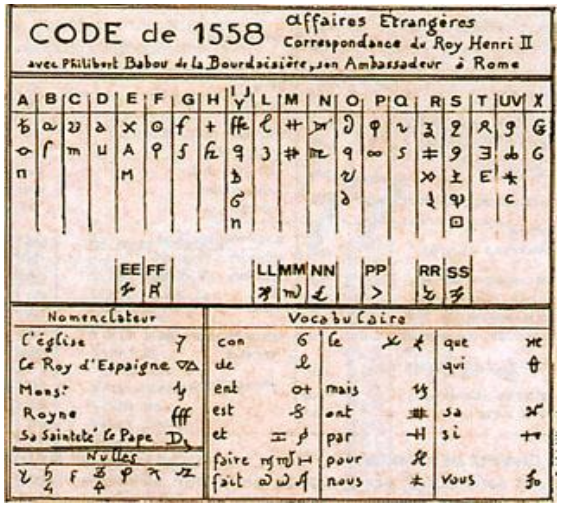


CRIPTOGRAFÍA SIMÉTRICA:

Más de 4.000 años de historia de intercambio de textos secretos lo avalan, pero siempre compartiendo claves, **con la obvia inseguridad** que conlleva.

Hubo grandes e ingeniosos desarrollos de criptosistemas entre los siglos XV y XVII, como los sistemas homofónicos y los de sustitución polialfabética, todos **muy superiores** a los métodos usados en la antiguedad

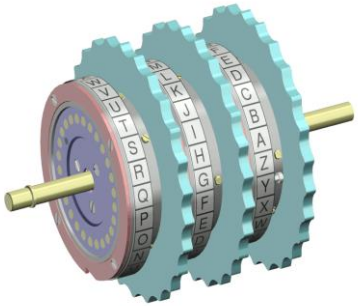


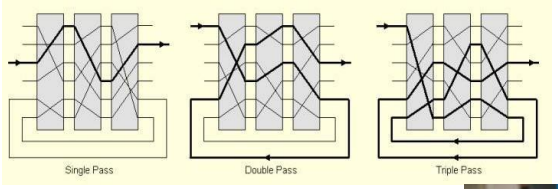


Vigenère Cipher

Plaintext	A	T	T	A	C	K	A	T	D	A	W	N
Key	L	E	M	O	N	L	E	M	O	N	L	E
	A+L	T+E	T+M	A+O	C+N	K+L	A+E	T+M	D+O	A+N	W+L	N+E
Ciphertext	L	X	F	O	P	V	E	F	R	N	H	R


Aparece la radio
con su potencial
uso militar y
recrudece el
problema de
distribuir claves

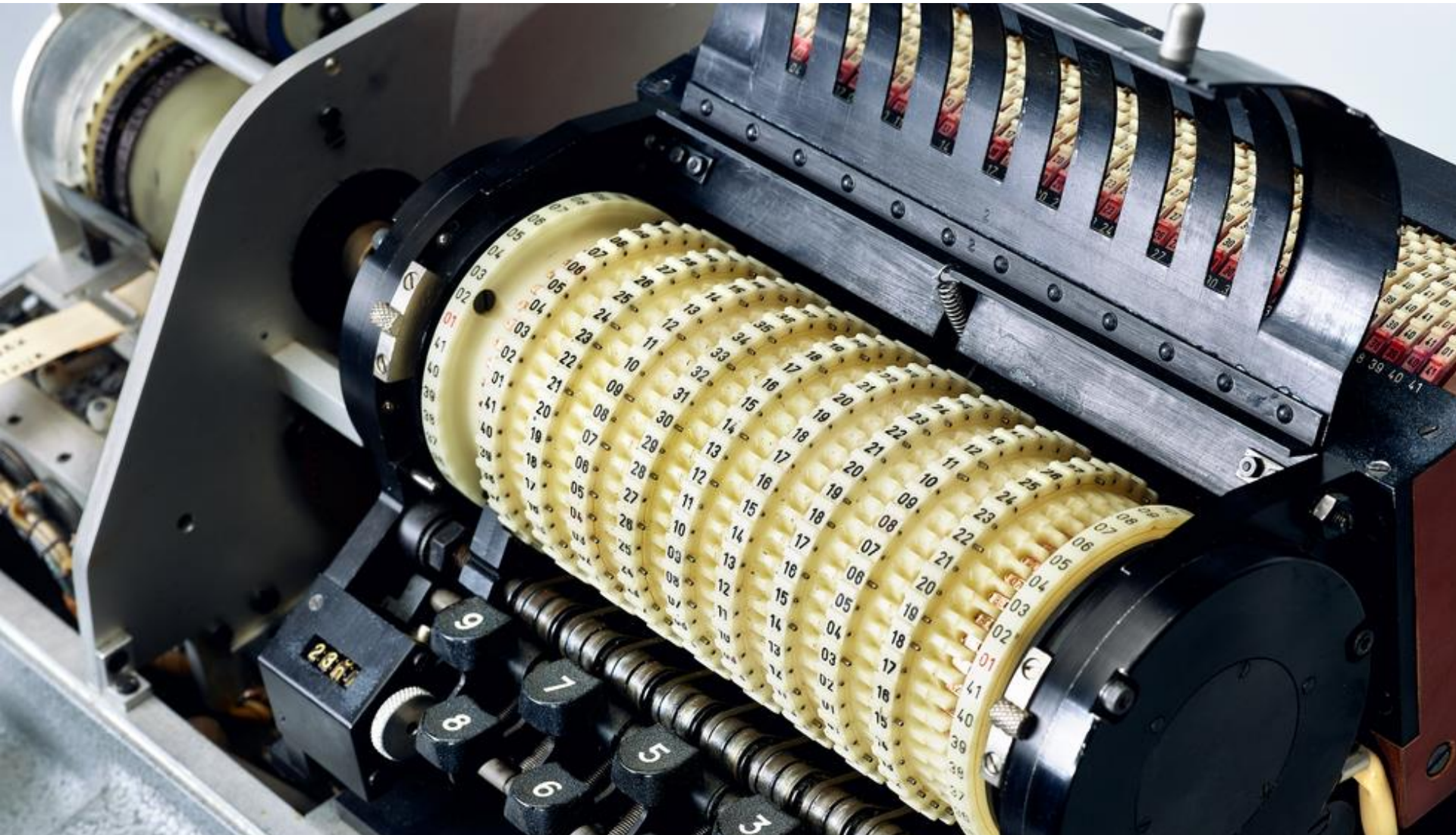




Máquinas de rotores. Quiebre de la Enigma por los matemáticos polacos. Transferencia del know-how a Inglaterra. Turing aprende de los polacos.

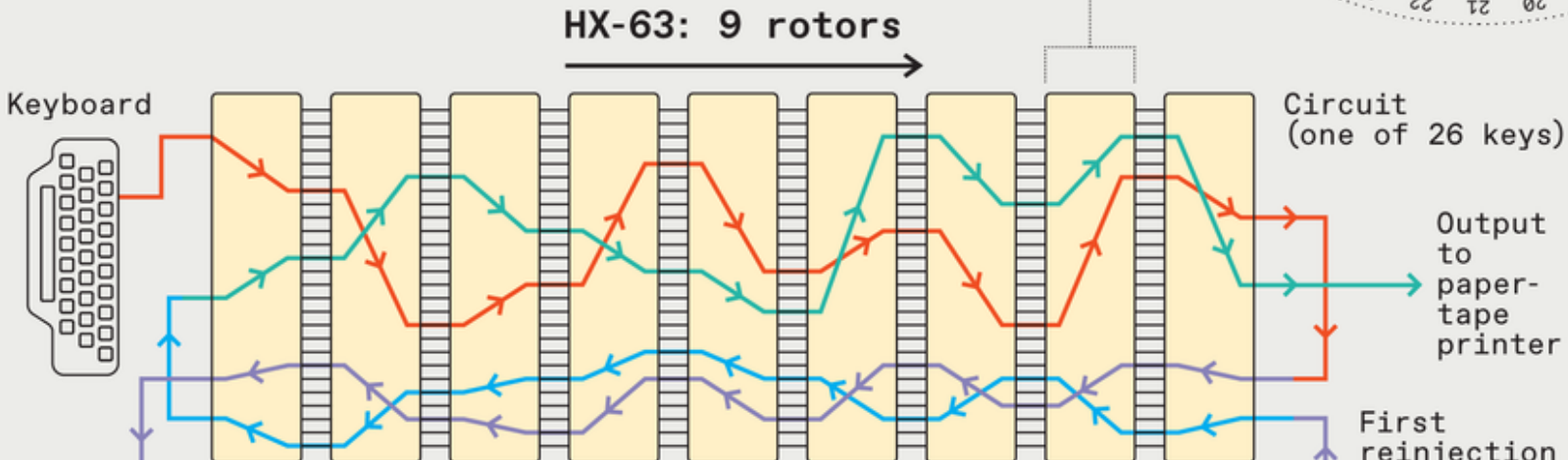
Fialka: Una máquina de 10 rotores que nunca se quebró

La máquina HX-63 de 9 rotores tan segura que nunca la dejaron vender (10^{600} claves posibles)



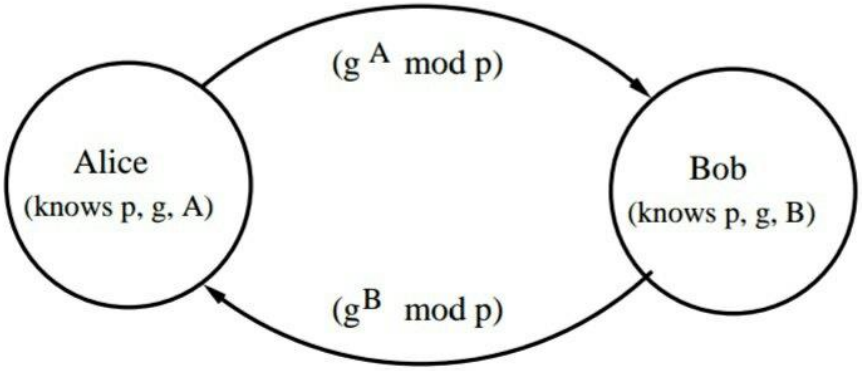
WHEELS WITHIN WHEELS: WHY THE HX-63 IS SO SECURE

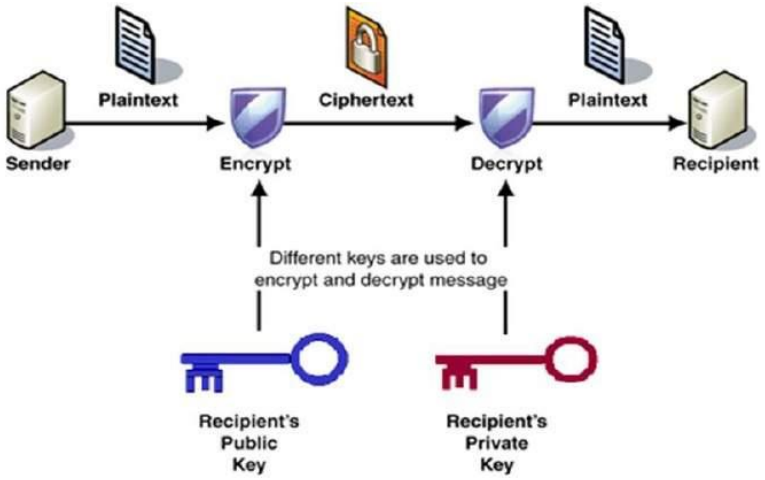
The HX-63 has nine rotors and also uses a technique called reinjection. Each rotor has a set of conductors that connect each and every electrical contact on one side of the rotor with a different contact on the other side. For every rotor the pattern of these connections is unique. When the operator strikes a key on the keyboard, representing one of 26 letters, current travels through the set of nine rotors twice, once in each direction, and then through a separate set of 15 rotor contacts at least two times. This reinjection technique greatly increases the complexity of the cipher.



CRIPTOGRAFIA ASIMÉTRICA O DE CLAVE PÚBLICA:

1945. Inglaterra encomienda a matemáticos de Cambridge el desarrollo de un método de clave pública (Ellis,etc). Se mantiene como secreto de guerra hasta que en 1976 aparece el método de Diffie-Hellman, Pohlig-Hellman, RSA,…

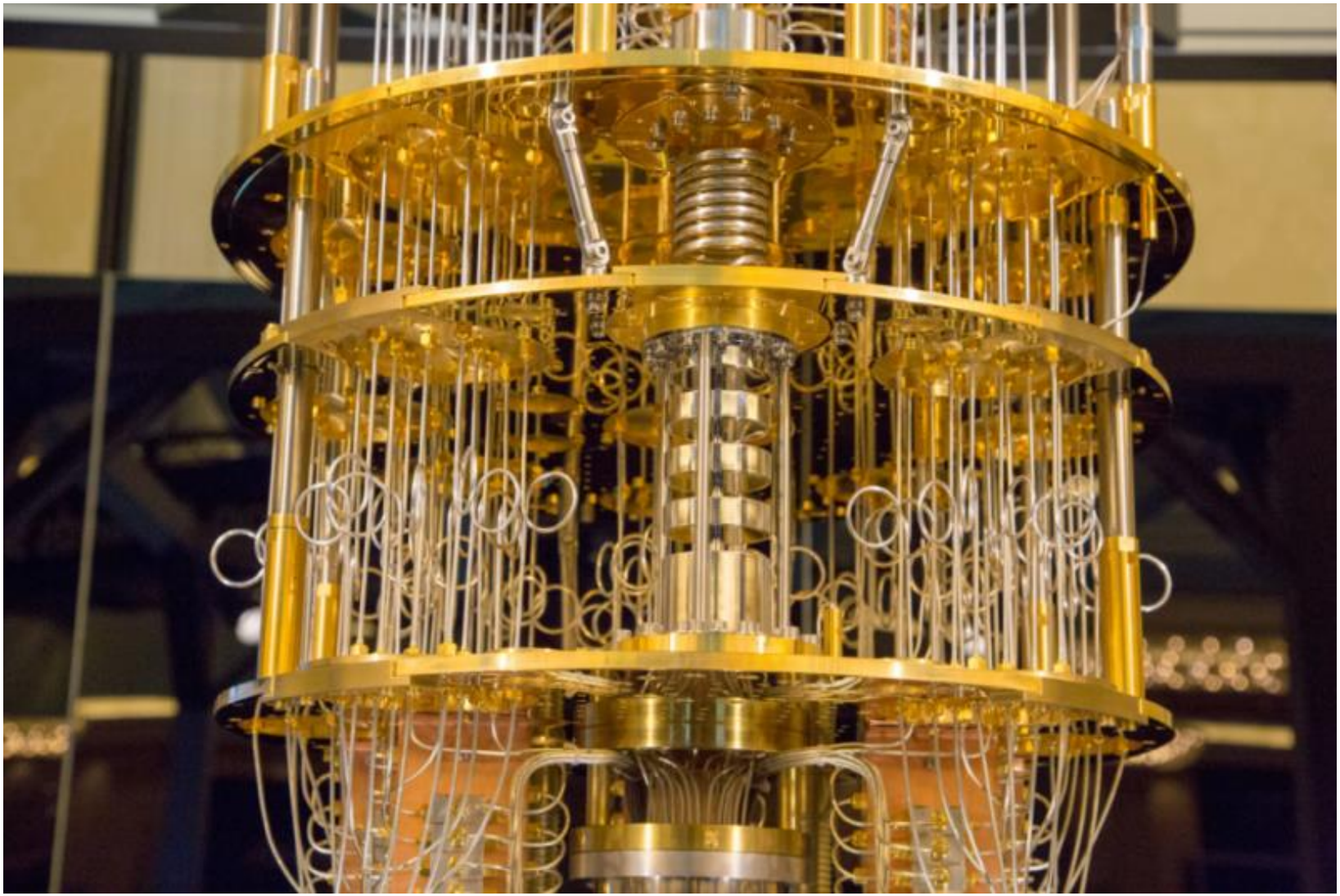




Junto al desarrollo de la tecnología informática, la criptografía avanza con nuevos protocolos simétricos y de clave pública.

Los métodos de **clave pública** basan su seguridad en la imposibilidad de resolver ciertos problemas matemáticos con las computadoras actuales. Por ejemplo factorizar:

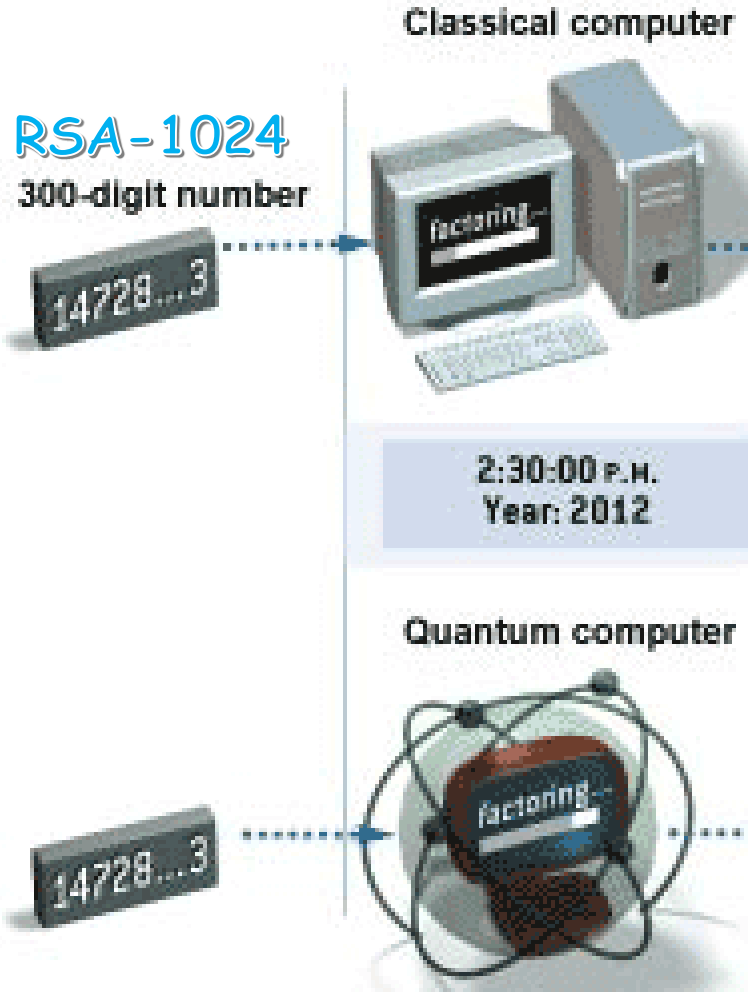
Un nuevo actor aparece en escena y quiebra este equilibrio de seguridad, la **computadora cuántica**.



30.000 años

0.000001 seg

Quiebre RSA



Impacto cuántico

Name	Function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128	block cipher	128	64
AES-256	block-cipher	256	128
Salsa20	stream cipher	256	128
GMAC	MAC	128	**64**
Poly1305	MAC	128	128
SHA-256	hash function	256	128
SHA-3	hash function	256	128
Public-key cryptography			
RSA-3072	encryption	128	broken
RSA-3072	signature	128	broken
DH-3072	key exchange	128	broken
DSA-3072	signature	128	broken
256-bit ECDH	key exchange	128	broken
256-bit ECDSA	signature	128	broken

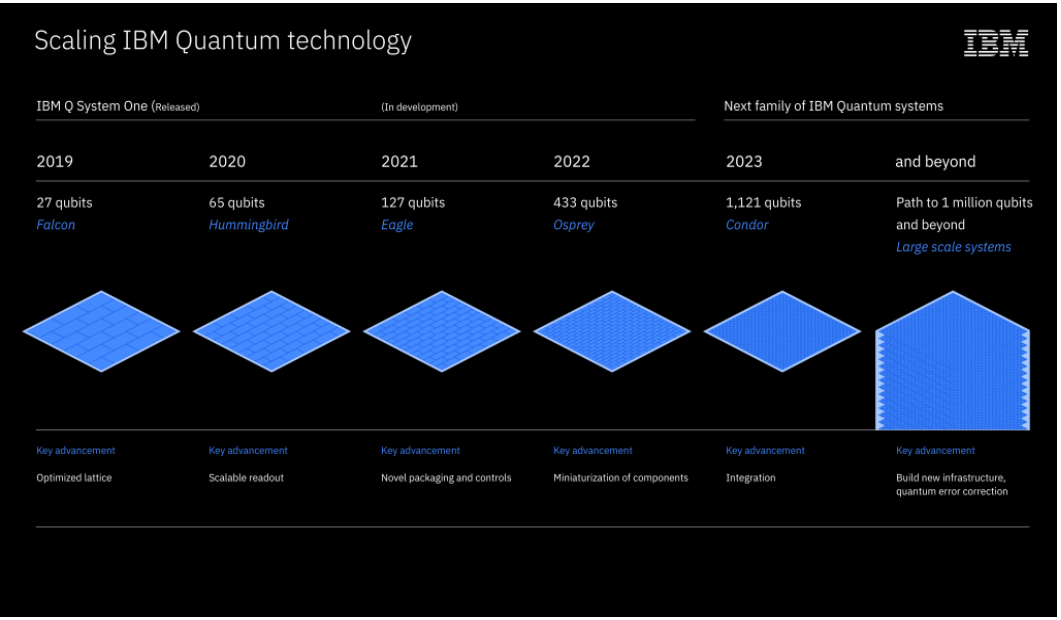
Source: University of Illinois, Bernstein & Lange

El algoritmo Grover reduce la complejidad cuadráticamente

El algoritmo Shor destruye estos algoritmos

IBM 1000 qubit computer para 2023

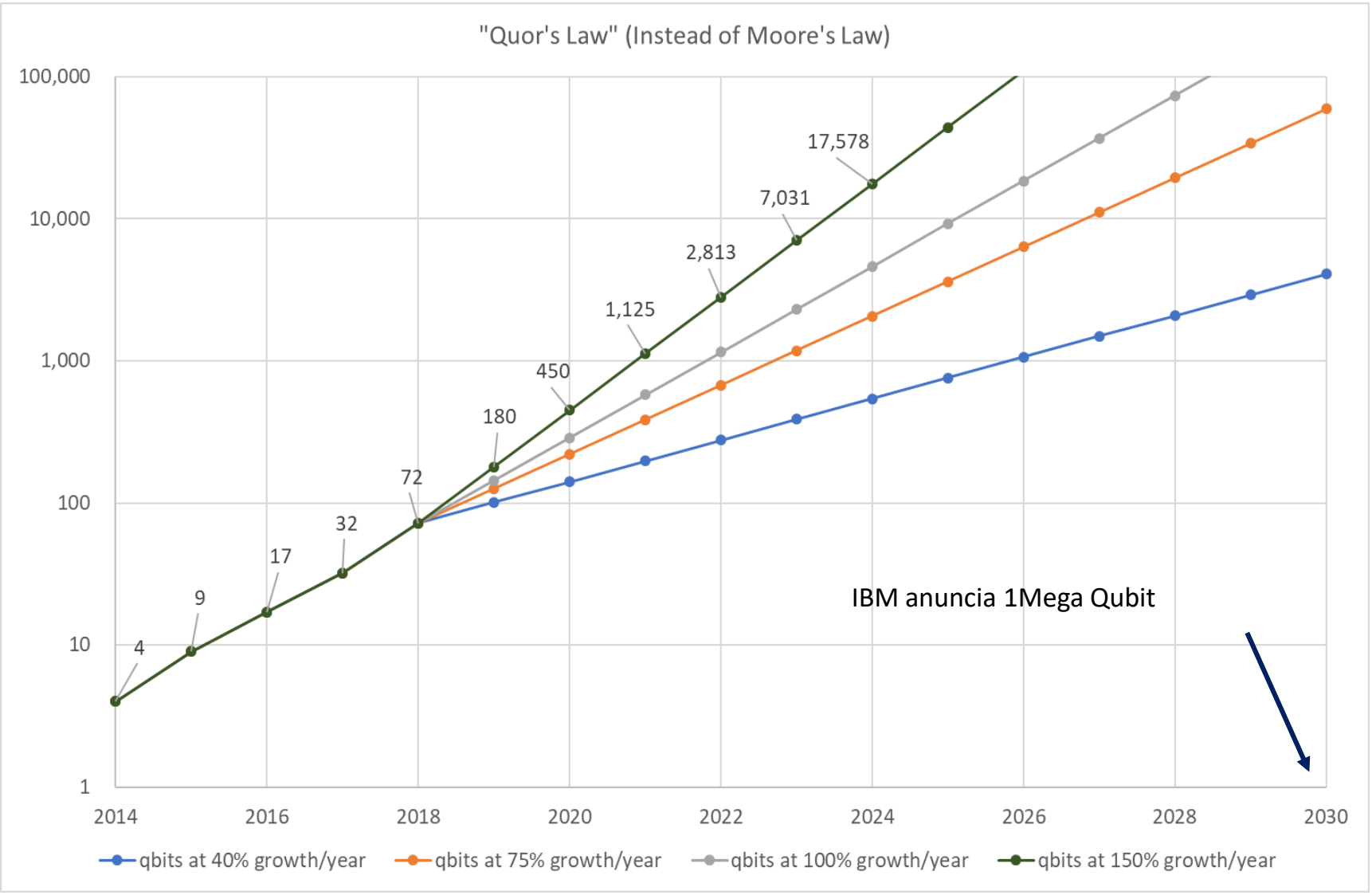
https://techcrunch.com/2020/09/15/ibm-publishes-its-quantum-roadmap-says-it-will-have-a-1000-qubit-machine-in-2023/

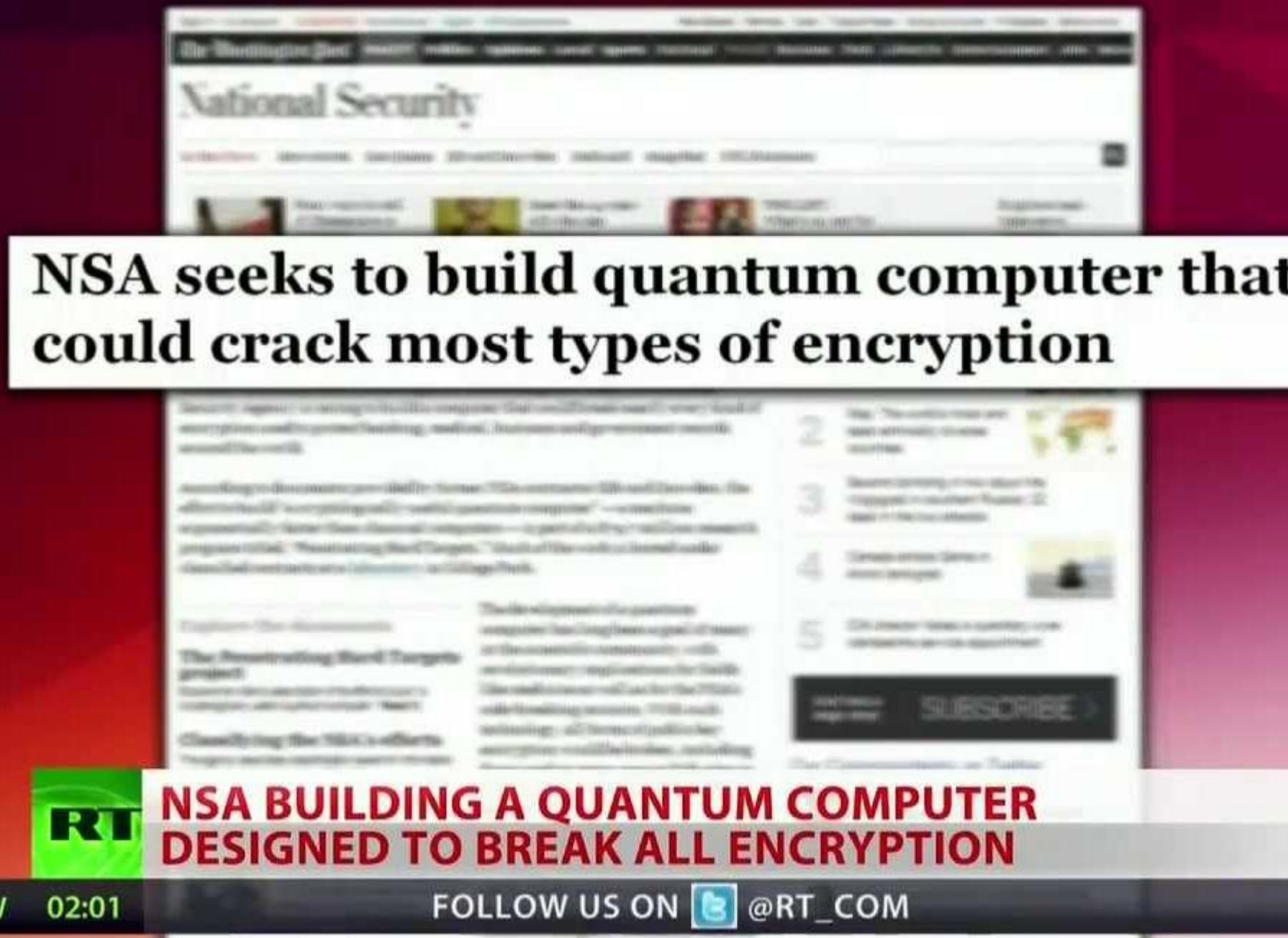


IBM 1.000.000 qubit computer para 2030

https://fortune.com/2020/09/15/ibm-quantum-computer-1-million-qubits-by-2030/

Predicciones de escala en QC




National Security
NSA seeks to build quantum computer that could crack most types of encryption
RT
NSA BUILDING A QUANTUM COMPUTER DESIGNED TO BREAK ALL ENCRYPTION
02:01
FOLLOW US ON @RT_COM

Long Reads

Inside big tech's high-stakes race for quantum supremacy

Quantum computers used to be an impossible dream. Now, after a decade of research by some of the world's biggest tech companies, they're on the verge of changing everything

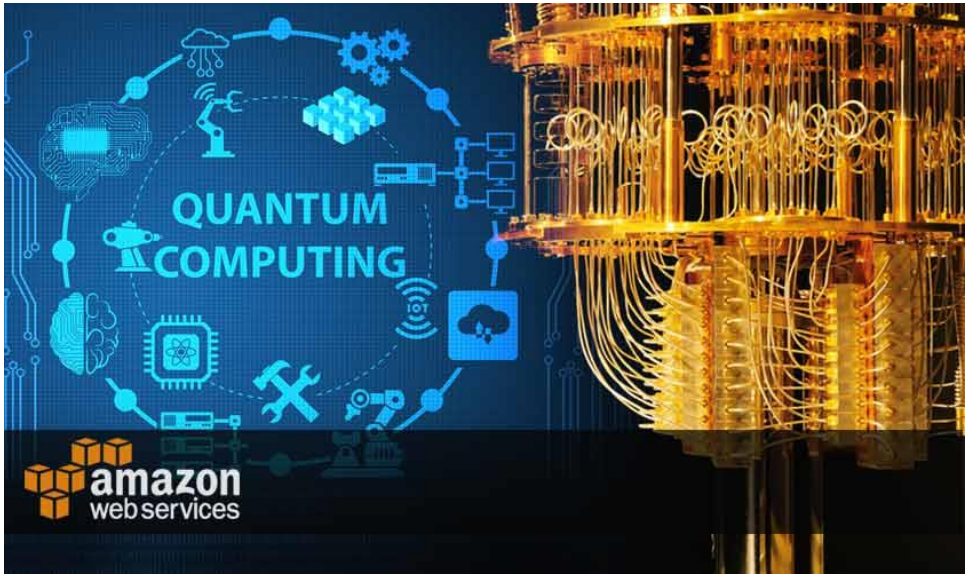
A cryostat at Google's quantum computing lab near Santa Barbara, California designed to keep a quantum chip at t

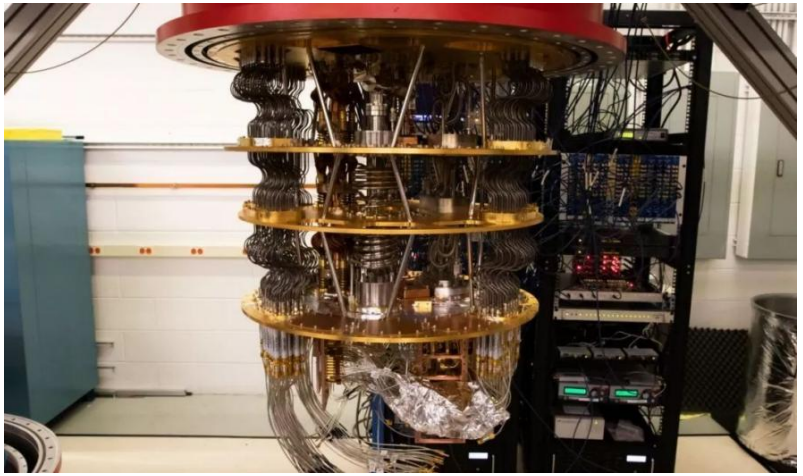
Credit: Jason Koxvold

By AMIT KATWALA

Monday 18 May 2020

On June 4, 2019, Sergio Boixo gathered his colleagues on Google's quantum research team together for an urgent meeting. The group, split across two sites in southern California, had spent the better part of a decade trying to build a working quantum computer – a revolutionary type of device that works according to the laws of quantum mechanics.





En el campo de la ciencia y la tecnología cuánticas, China resultó ser otra gran potencia, que dejó directamente a Estados Unidos muy rezagado. Resulta que el ordenador cuántico de China ha hecho un gran avance esta vez. Con millones de qubits, reescribirá directamente la historia de la supercomputación humana en el futuro.

La criptografía post-cuántica (PQC)

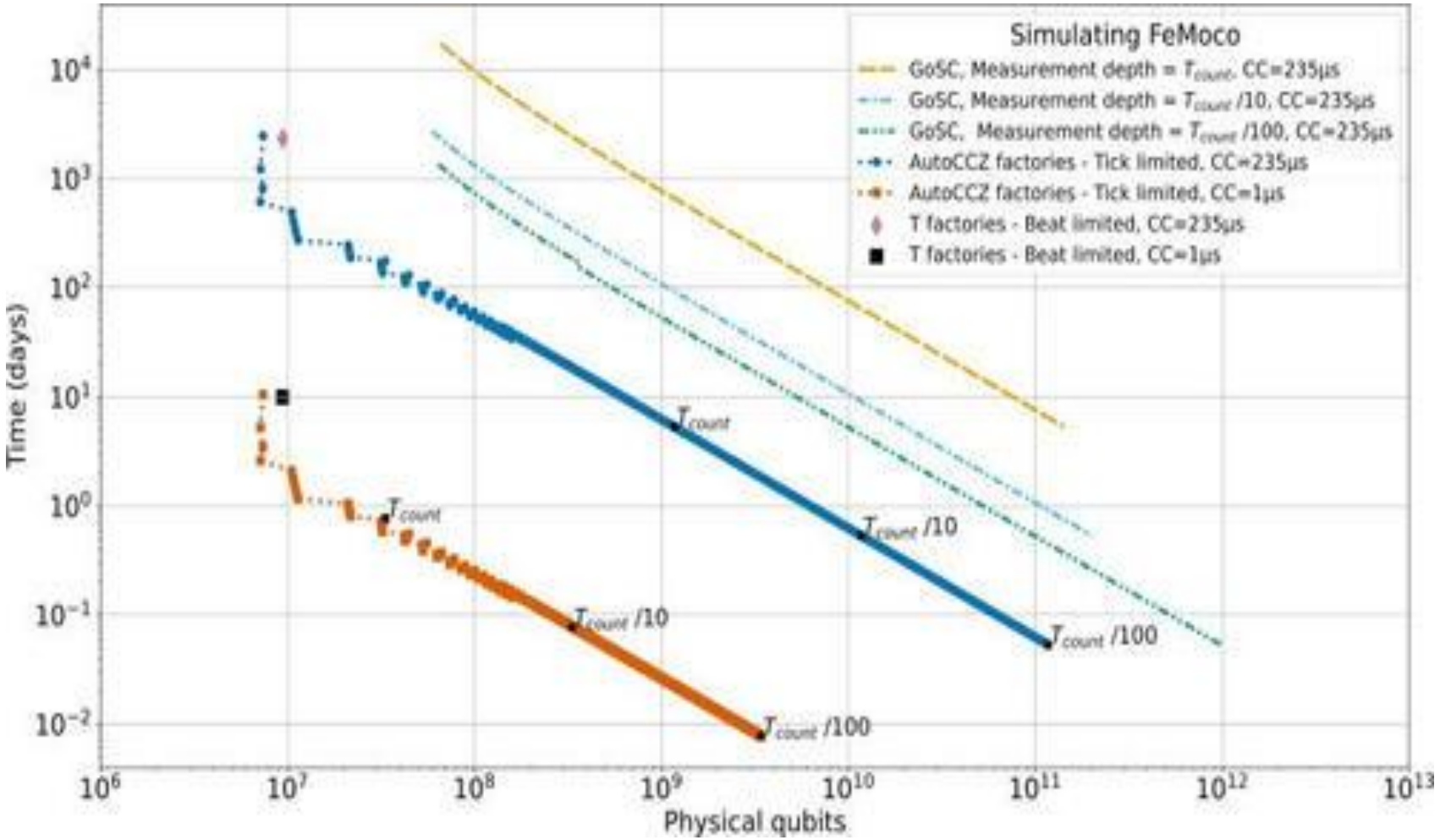
Su objetivo es generar sistemas criptográficos resistentes a los ataques cuánticos. Dada la creciente evolución en el desarrollo de computadoras cuánticas, esa amenaza ya no es virtual y se impone adoptar esta tecnología para proteger nuestras comunicaciones y los activos del País, única vía de cimentar la Ciberseguridad y Ciberdefensa Nacional.

El universo post-cuántico (PQC)

Hay una buena posibilidad de que los ordenadores cuánticos sean capaces de descifrar el RSA-2048 en un plazo de cinco a diez años (se necesitan unos 8.000 qubits en un ordenador cuántico universal para hacerlo). Algunos datos encriptados tienen una vida útil de más de diez años. Puede llevar diez años pasar a un nuevo esquema de cifrado, por lo que las empresas y los gobiernos están luchando para averiguar qué hacer. La totalidad de los cifrados que se usan hoy en día ya no son seguros en un mundo cuántico. Si alguien ha estado grabando una sesión de https, digamos, puede que no sea capaz de desencriptarla ahora, pero sí dentro de unos años.

predicción de la relación qubits-tiempo necesarios para quebrar ECC-256 bits

(usado en la red Bitcoin)



AVS Quantum Sci. 4, 013801 (2022); https://doi.org/10.1116/5.0073075

Para implementar un sistema de comunicaciones seguras en este momento hay que hacerlo basado en métodos post-cuánticos para obtener inviolabilidad por muchos años.

No sirve recurrir a recursos físicos y lógicos del extranjero, hay innumerables ejemplos de puertas traseras ocultas que vulneran esa seguridad.

Afortunadamente tenemos recursos humanos nacionales para afrontar el desafío.

ARSAT

INVAP

Sistema PQC CRYPTOCOMM

ARSAT desarrolló con criptógrafos argentinos un sistema de comunicaciones inviolables de mensajes y archivos. La existencia de las computadoras cuánticas y su enorme capacidad asociada, amenaza destruir la confidencialidad vigente en la actualidad tanto en Internet (TLS) como en las estructuras de firma digital. Las vulnerabilidades se verían primordialmente sobre los métodos asimétricos (RSA, ElGamal, Curvas Elípticas, DSA, etc.) pero también afectarían a los algoritmos simétricos como AES al reducir la complejidad de los ataques por fuerza bruta.

Este panorama condujo a que se generen distintas investigaciones para lograr métodos postcuánticos (PQC) que resistan los ataques mediante computadoras tanto normales como cuánticas. En este caso, se trata de un sistema basado en algoritmos postcuánticos originales. Consta de un cifrador simétrico de alta velocidad (con claves de 318 bits) , el cual puede usarse eficazmente en sistemas de comunicaciones. También desarrollamos una nueva tecnología postcuántica de generación de claves privadas/públicas y de certificados digitales.

Hay dos versiones:

El sistema en versión "S" permite el intercambio de archivos y mensajes mediante software. Luego se lanzará la versión "H", que implementará el sistema mediante un hardware especializado desarrollado entre ARSAT e INVAP. Adicionalmente, se agregará la funcionalidad de realizar transmisiones de voz y video en tiempo real.

DESCRIPCIÓN FUNCIONAL

Se adapta al estándar de red cero confianza (ZTN) https://csrc.nist.gov/publications/detail/sp/800-207/final bajo el cual cada equipo, usuario y mensaje se certifica con criptografía asimétrica. Por otra parte, el aplicativo puede utilizar credenciales de correo o hacer uso de servicios en la nube.

La versión "S" se ofrece para LINUX y WINDOWS

Los equipos de la red se autentican sitio a sitio, usando un empaquetador que protege al ejecutable estático o en operación contra ingeniería reversa usando tecnología estado-del-arte.

Cada miembro opera con juegos de claves público-privadas, y las públicas sólo se pueden usar si poseen un certificado digital emitido por la Autoridad Certificante de la comunidad (AC).

Los mensajes se cifran con criptografía híbrida (simétrica y asimétrica). La parte asimétrica permite definir claves simétricas infraguables sin intercambios previos, lo que acelera el tráfico.

Los mensajes pueden estar formados por uno o más archivos que se empaquetan en forma automática, y se protegen con el certificado digital de la AC. Cada receptor verifica la validez del certificado digital antes de la apertura de cada mensaje.
Se planea incorporar la capacidad de mandar mensajes desde cualquier entidad emisora hacia un número arbitrario de receptores de una comunidad (broadcast).

La interfaz gráfica del sistema es absolutamente simple e intuitiva, permitiendo su uso por parte de personal sin experiencia informática.

cryptocomm

Cryptocomm

un producto de Arsat

Descargar tarjeta de contacto

HD - hscolnik@gmail.com

Recibidos | Enviados | Nuevo mensaje

ARCHIVO ADJUNTO

No se eligió ningún archivo.

Destinatario

+ SELECCIONAR CONTACTO

sin asunto

CIFRAR SIN ENVIO DE CORREO | ENVIAR CORREO

Gracias por su atención.

Si está interesado en probar el sistema y/o tiene preguntas escribir a

hscolnik@arsat.com.ar

PQC desarrollo Argentino: escudo tecnológico para la Ciberdefensa Nacional…