


# Dutch Microsoft & Security Meetup



  
**FUJITSU**

**Welcome!**

# Who we are?



- We have been in the business for 84 years and do everything in ICT
- We use our experience and ICT to shape the future of society with our customers
- Japan's largest IT services provider and no. 5 in the world
- 140,000 Fujitsu people support customers in more than 100 countries
- Over 18,500 employees are engaged in R&D within the Fujitsu Group and 1,400 researchers in the Fujitsu Laboratories Group
  
- **Culture:** Invest in long-term relationships and technological innovation
- **Management:** Involved, autonomous and locally responsible
- **Approach:** Adding value for the customer through sincere interest
- **Method:** International standards, tailored to local specific customer needs, supported by a global organization

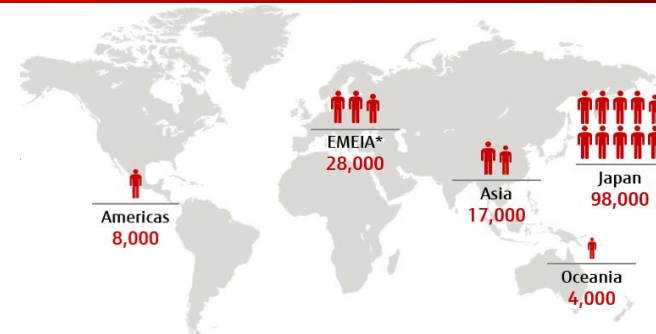
# Fujitsu's Global Footprint



## Global Product portfolio



## Global Workforce



## Global DC Infrastructure



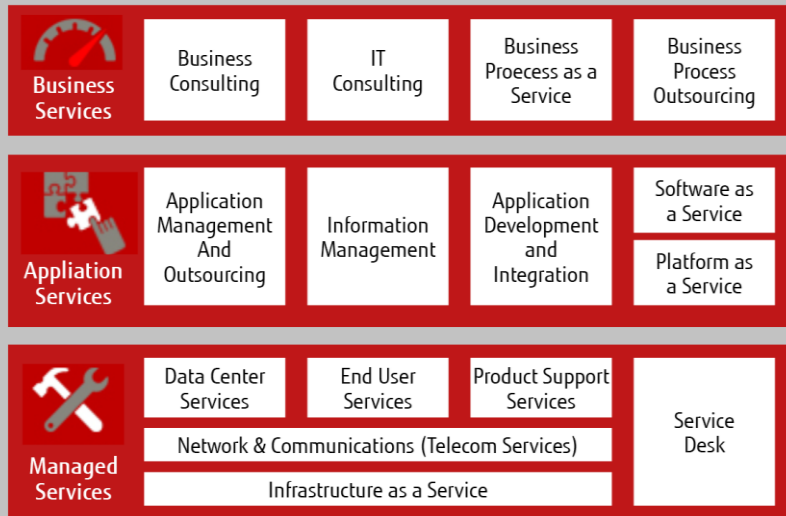
## Global on-site services ('Follow the sun')



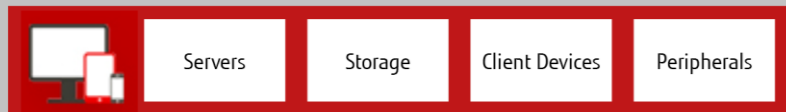
# IT Portfolio



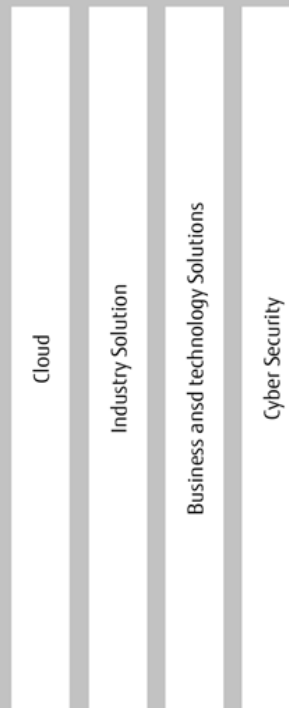
## Services



## Products



## Solutions



## Strategic Partners



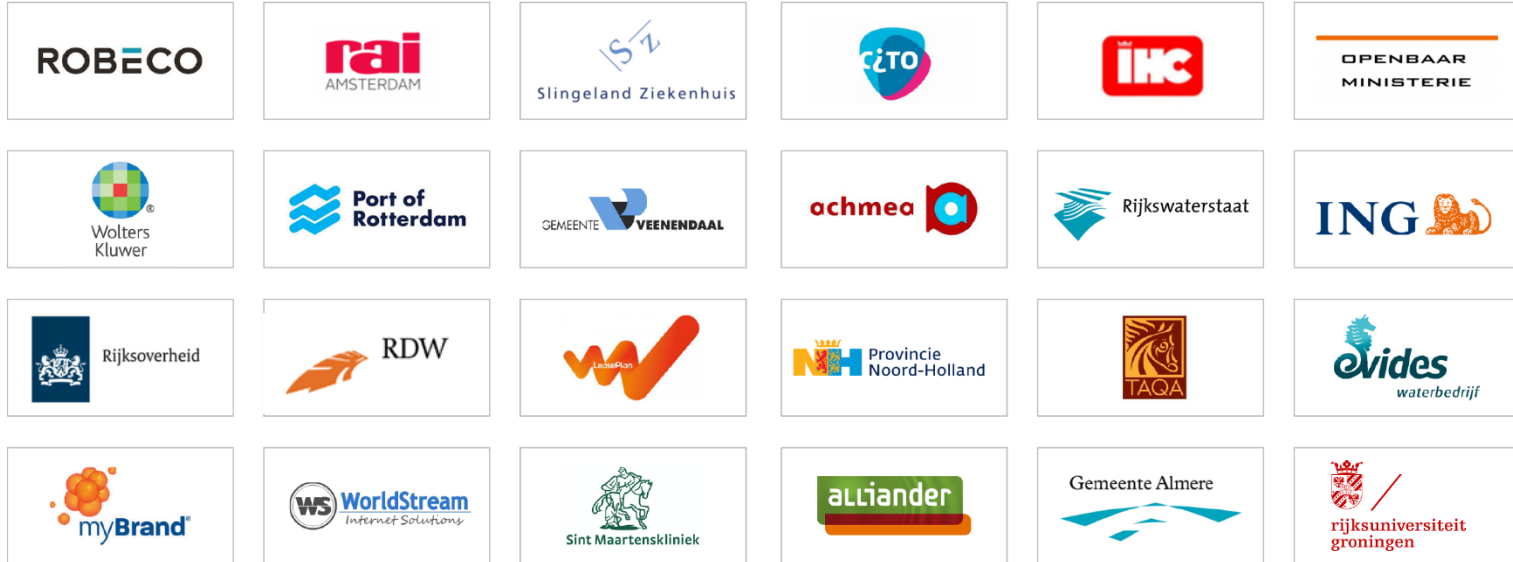
Azure  
Expert  
MSP



servicenow




# Our customers



# Experience center 'the Bridge'







# Cracking Enigma in the Quantum Era

Microsoft and Security  
Meetup April 16th

FUJITSU

shaping tomorrow with you

Human Centric Innovation

Co-creation  
for Success

# A Test – Part 1

$$D = 110 - \left( 110 \times 1 - e^{\frac{t - \sqrt{w}}{-2\pi}} \right)$$



“Deze wiskundige formule berekent de perfecte panty” – James Hind, University of Nottingham





[natgeotv.com](http://natgeotv.com)

# It Started with Enigma

- *Rotors and sequence (60 possibilities)*
- *Ring setting*
- *Orientation of rotors (17 576 possibilities)*
- *Setting of connector board with six wires (6,4 trillion possibilities)*



Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	$4.2 \times 10^9$
56-bit (DES)	$7.2 \times 10^{16}$
64-bit	$1.8 \times 10^{19}$
128-bit (AES)	$3.4 \times 10^{38}$
192-bit (AES)	$6.2 \times 10^{57}$
256-bit (AES)	$1.1 \times 10^{77}$

*AES based on Rijndael algorithm:*

- *Keylength*
- *Blocks*
- *Rounds*
- *Subbytes*
- *Shiftrow*

## Agenda

- The Quantum Era
- A Test
- A Deeper Look at Encryption
- Recent Studies
- Post-Quantum Initiatives
- Back to Enigma

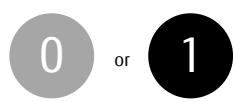






# The Era of Quantum

Technology utilizing quantum mechanics phenomena

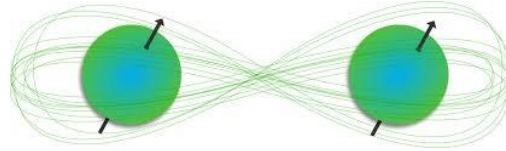


"0" or "1"  
DIGITAL STATE

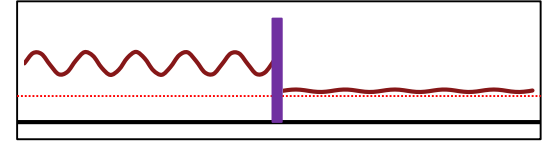


"0" and "1"  
QUANTUM STATE

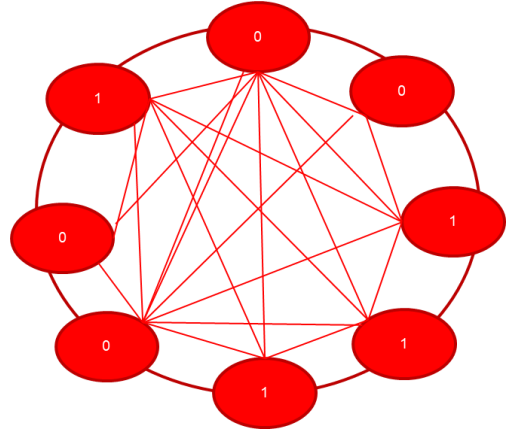
Superposition



Entanglement



Quantum tunneling







# The Impact of Quantum: Opinions

📰 NOT SO FAST: South Korea 5G rollout faces delays

## 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 (19:24 BST) | Topic: Security

The easy part is something that you are probably already doing. [Attacks](#) that can run on quantum computers simply divide the number of bits of security that an AES key provides by two—a 256-bit AES key will provide 128 bits of security, etc. So if you are already using AES-256, you are already using an encryption algorithm that will provide an adequate level of security against quantum computers. If you are using AES-128, just move to AES-256 and you will be using a quantum-safe algorithm. It is that easy.



Don't panic!

**Is quantum computing the end of security as we know it?**

The background is a solid dark red. Overlaid on this are several elements: a series of white binary digits (0s and 1s) arranged in a perspective that recedes into the distance, creating a sense of depth; a bundle of white, fiber-optic-like lines that fan out from the bottom left corner towards the center; and a few larger, stylized white circles and vertical bars scattered throughout the composition.

The Question: Does Quantum Require  
New Types and Forms of Encryption?

# A Test – Part 2

## Calculating Prime

1 person: Calculate the prime factorization of 300

1 group: Calculate the prime factorization of 640

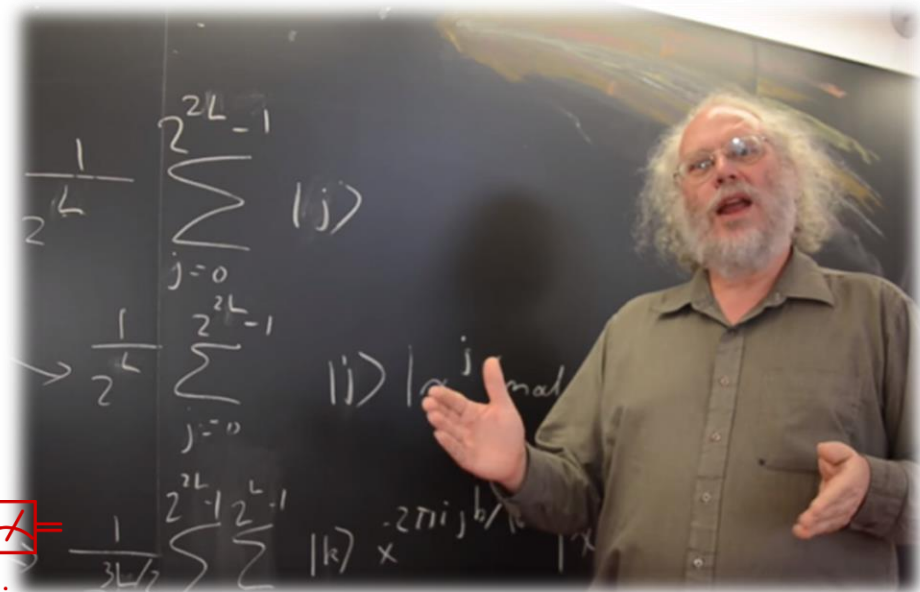
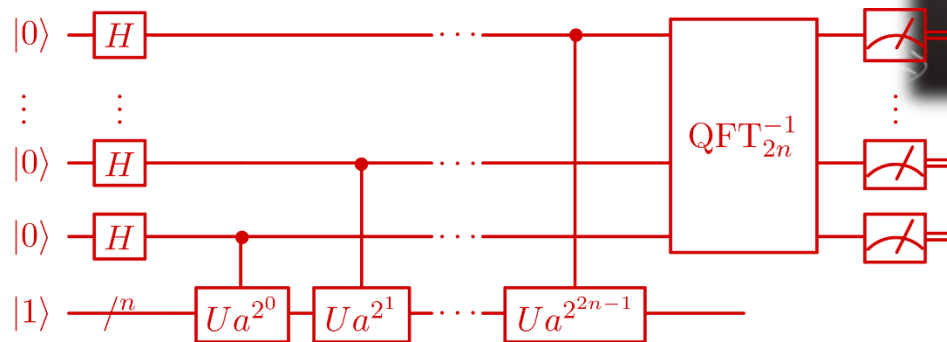
2 groups: Calculate the prime factorization of 820



# What we just did

## Shor's Algorithm

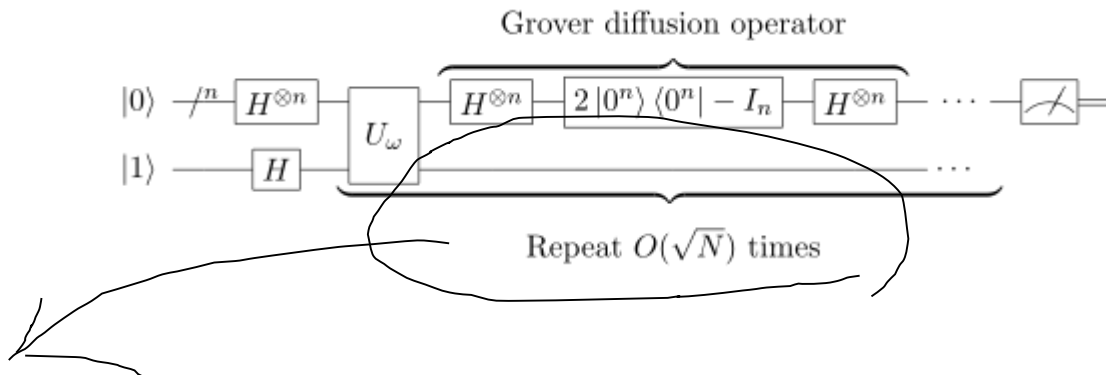
- Based on calculating prime factorization
- Quantum computers will definitively be able to use Shor's algorithm to crack public keys





# Grover's Algorithm

You are given a list of elements, and you know that one element satisfies a certain condition, while the other elements don't. Basically, this is an **algorithm** for finding a specific element in an unordered list.



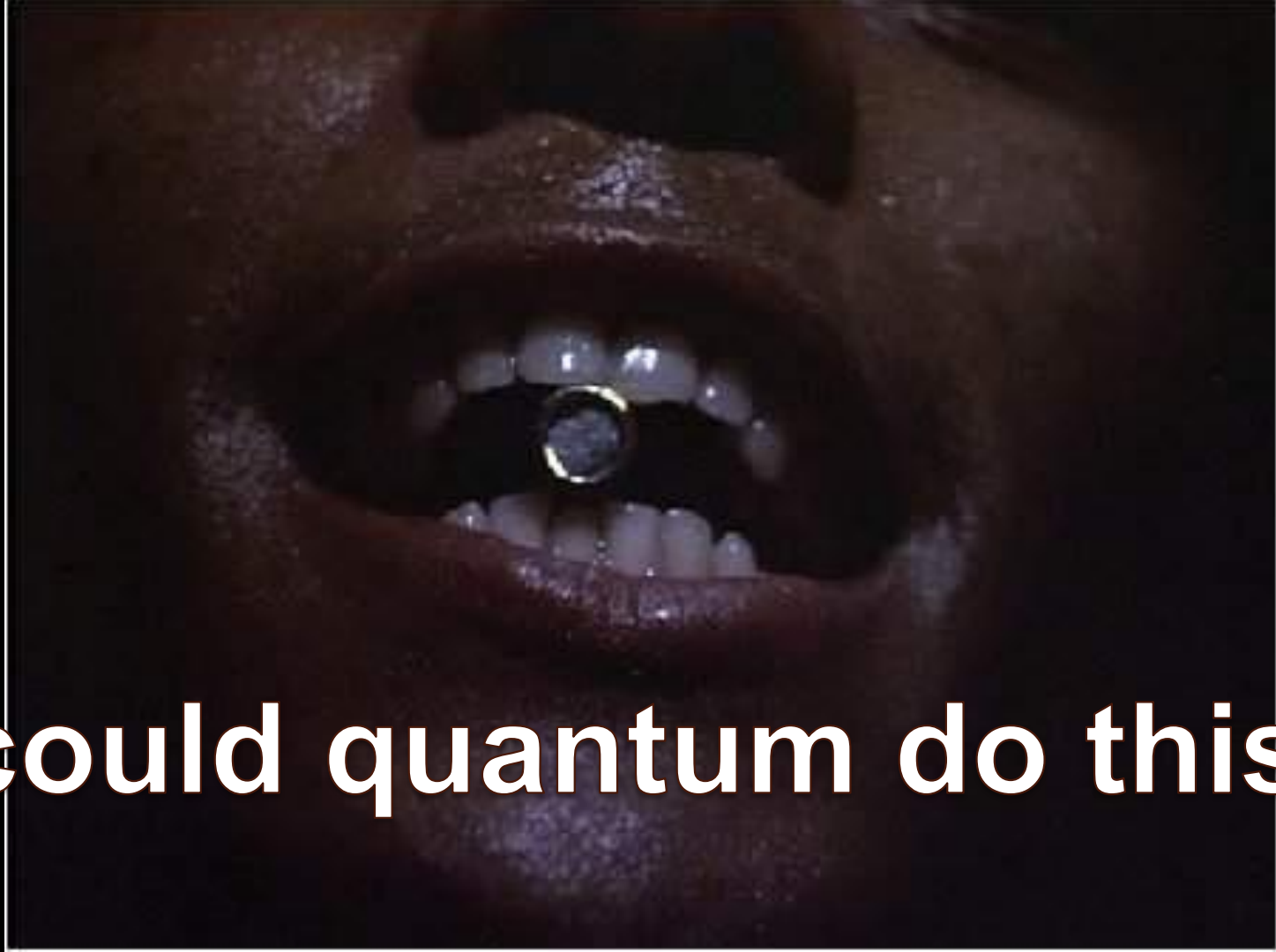
$$\langle \omega | s \rangle = \langle s | \omega \rangle = \frac{1}{\sqrt{N}},$$

$$\langle s | s \rangle = N \cdot \frac{1}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} = 1,$$

$$U_{\omega} | s \rangle = (I - 2|\omega\rangle\langle\omega|) | s \rangle = | s \rangle - 2|\omega\rangle\langle\omega| s \rangle = | s \rangle - \frac{2}{\sqrt{N}} |\omega\rangle,$$

$$\begin{aligned} U_s \left( | s \rangle - \frac{2}{\sqrt{N}} |\omega\rangle \right) &= (2|s\rangle\langle s| - I) \left( | s \rangle - \frac{2}{\sqrt{N}} |\omega\rangle \right) = 2|s\rangle\langle s| s \rangle - | s \rangle - \frac{4}{\sqrt{N}} | s \rangle \langle s | \omega \rangle + \frac{2}{\sqrt{N}} |\omega\rangle \\ &= 2|s\rangle - | s \rangle - \frac{4}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} | s \rangle + \frac{2}{\sqrt{N}} |\omega\rangle = | s \rangle - \frac{4}{N} | s \rangle + \frac{2}{\sqrt{N}} |\omega\rangle \\ &= \frac{N-4}{N} | s \rangle + \frac{2}{\sqrt{N}} |\omega\rangle. \end{aligned}$$





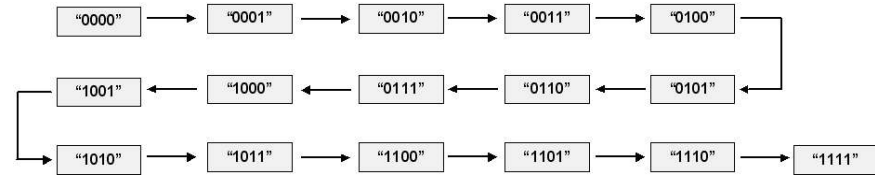
**could quantum do this?**

# Cracking AES: Brute Force

## The Principle

Brute-force attack involves systematically checking all possible key combinations until the correct key is found.

4 bits: 16 rounds to check all possible key combinations starting with 0000



Fujitsu K-Computer (Kobe, Japan): 705,024 cores, 10,51 petaflops

Time estimated to crack AES-256 based on 1000 flops per combination check (brute force): ... infinite (Fujitsu Labs, Tokyo)

Key size	Time to Crack
56-bit	399 seconds
128-bit	$1.02 \times 10^{18}$ years
192-bit	$1.872 \times 10^{37}$ years
256-bit	$3.31 \times 10^{56}$ years

# Brute Force at Quantum Rate



*If you know the probabilities that a particle is in one of multiple states, you can think of that particle as simultaneously being in all of those states at the same time.*

*Extending this idea to qubits, you can use  $N$  qubits to simultaneously store the probabilities that your system is in any of the possible  $2^N$  states. This is often interpreted as meaning that with  $N$  qubits, you can store all  $2^N$  possible  $N$ -bit values at once.*





# Q: AES 256 is Quantum Secure?

*Prof. Dr. T. Lange: „Unless a large group of people have overlooked something, an attack based on Grover would result in  $2^{128}$  operations on 256bit-AES. However, I would never call something quantum secure.”*



***„I would never call  
something quantum secure.”***







# Recent Study (2018)

(IJACSA) International Journal of Advanced Computer Science and Applications,  
Vol. 9, No. 3, 2018

## The Impact of Quantum Computing on Present Cryptography

Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang  
Department of Informatics, University of Oslo, Norway  
Email(s): {vasileim, kamerv, mateusdz, josang}@ifi.uio.no

TABLE I. IMPACT ANALYSIS OF QUANTUM COMPUTING ON ENCRYPTION SCHEMES (ADAPTED FROM [14])

Cryptographic Algorithm	Type	Purpose	Impact From Quantum Computer
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
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

# Recent Study (2019)

## Quantum Security Analysis of AES

Xavier Bonnetain<sup>1,2</sup>, María Naya-Plasencia<sup>2</sup> and André Schrottenloher<sup>2</sup>

<sup>1</sup> Sorbonne Université, Collège Doctoral, F-75005 Paris, France

<sup>2</sup> Inria de Paris, France

{xavier.bonnetain, maria.naya\_plasencia, andre.schrottenloher}@inria.fr

„We consider the secret key setting and, in particular, AES-256, the recommended primitive and one of the few existing ones that aims at providing a post-quantum security of 128 bits.”

„This cryptanalysis can be quantumly improved as shown in [xx], **so the necessity to combine AES with an improved secure mode of encryption is sharpened when taking into account quantum attacks.**”

<https://eprint.iacr.org/2019/272.pdf>



# Recent Study

- Grover's algorithm used
- Quantum time calculated
- Based on 1200 qubits
- 40 qubits per s-box

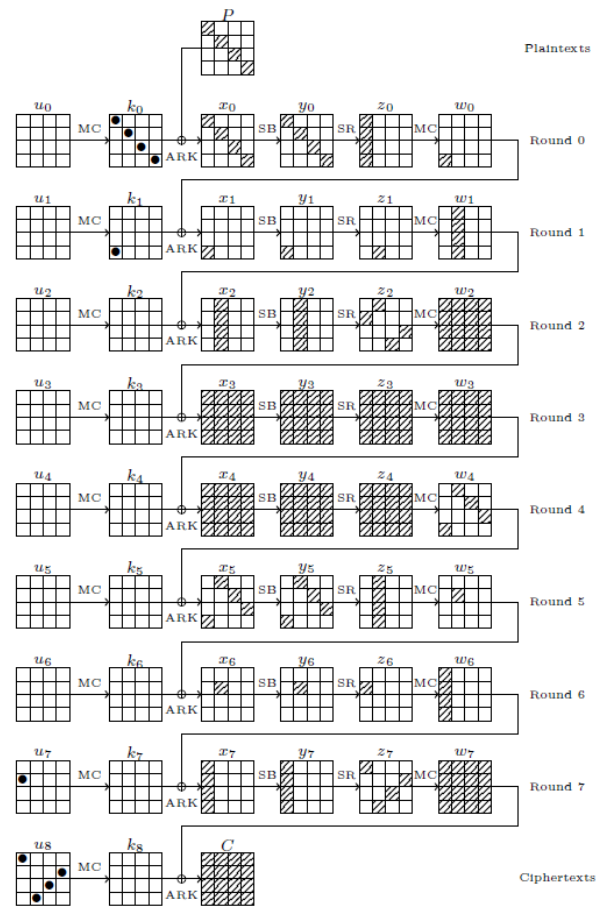


Figure 4: Full differential path used in the quantum attack. Key bytes guessed in the outer Grover procedure are denoted by ●.

# Post-Quantum Startups and Big Tech

## A selection of interesting companies



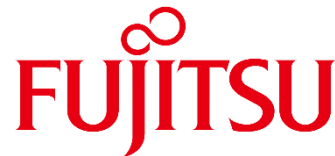
qStream: Quantum True  
Random Number Generator  
(QRNG)



ID Quantique: QRNG and  
'quantum key distributor'



Quantum Resistant Encryption  
NTS: Never The Same  
encryption



# Lattice-based Cryptography

$$L = \left\{ \sum a_i \mathbf{b}_i : a_i \in \mathbb{Z} \right\}$$

## Unbreakable by Quantum (public key)

„...mathematically has been proven to be resistant to quantum computing attacks.

So far, no known algorithms can break this method of encoding data.”

*Arvind Krishna, director of IBM Research*

- Lattice math as used in linear algebra, only with a random vector added in large dimension matrices, using the shortest vector problem (SVP)
- Lattice-based primitives are efficient and have already been successfully plugged into the TLS and Internet Key Exchange (IKE) protocols
- Lattice-based cryptography provides fast, quantum-safe, fundamental primitives and allows for constructions of primitives that were previously thought impossible.
- Lattice-based cryptography “one of the most fascinating research fields with potential to become the backbone of real-world cryptography in the near future”

(IJACSA) International Journal of Advanced Computer Science and Applications,  
Vol. 9, No. 3, 2018

### The Impact of Quantum Computing on Present Cryptography

Vasileios Mavroudis, Kamer Vishi, Mateusz D. Zych, Audun Josang  
Department of Informatics, University of Oslo, Norway  
Email(s): {vasileim, kamerv, mateusdz, josang}@ifi.uio.no

**In conclusion, among all the lattice-based candidates mentioned above NTRU is the most efficient and secure algorithm making it a promising candidate for the post-quantum era.**

# NIST Project and Pqcrypto

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.

Round 2 submissions, announced January 30, 2019

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt
- NewHope
- NTRU
- NTRU Prime
- NTS-KEM
- Rollo
- Round5
- RQC
- Saber
- SIKE
- Three Bears



Initial recommendations of long-term secure post-quantum systems

„Under Grover’s attack, the best security a key of length  $n$  can offer is  $2^{n/2}$ , so AES-128 offers only 264 post-quantum security. PQCRYPTO recommends thoroughly analyzed ciphers with 256-bit keys to achieve 2128 post-quantum security:

- AES-256
- Salsa20 with a 256-bit key.”

<https://pqcrypto.eu.org/docs/initial-recommendations.pdf>

# Microsoft on Post-Quantum Encryption

„Working with academia and industry on four candidates for cryptography systems that can both withstand quantum computer capabilities, while still working with existing protocols.”

Any new cryptography has to integrate with existing protocols, such as TLS. A new cryptosystem must weigh:

- The size of encryption keys and signatures
- The time required to encrypt and decrypt on each end of a communication channel, or to sign messages and verify signatures, and
- The amount of traffic sent over the wire required to complete encryption or decryption or transmit a signature for each proposed alternative.

## FrodoKEM

FrodoKEM is based upon the Learning with Errors problem, which is, in turn, based upon lattices.

## SIKE

SIKE (Supersingular Isogeny Key Encapsulation) uses arithmetic operations of elliptic curves over finite fields to build a key exchange.

## Picnic

Picnic is a public-key digital signature algorithm, based on a zero-knowledge proof system and symmetric key primitives.

## qTESLA

qTESLA is a post-quantum signature scheme based upon the Ring Learning With Errors (R-LWE) problem.

*<https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/>*



So: how bad is it really?





# A Matter of Time?



We must do all this quickly because we don't know when today's classic cryptography will be broken.

It's difficult and time-consuming to pull and replace existing cryptography from production software.

Add to all that the fact that someone could store existing encrypted data and unlock it **in the future** once they have a quantum computer, and our task becomes even more urgent.

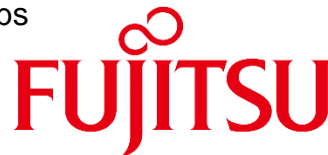
<https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/>



People should be aware of the fact that data that they store and encrypt right now, is already being collected at large scale. If you want to **keep this data safe for a longer period of time**, then basically it's already too late. – Christian Schaffner, UvA and QuSoft/CWI

<https://tweakers.net/reviews/5885/all/de-dreiging-van-quantumcomputers-en-de-noodzaak-van-resistente-encryptie.html>

To convey information that needs to be protected over a **relatively long period of several tens of years or more** such as genetic information, the need is felt for more advanced cryptography. – Shimoyama et al, Fujitsu Labs



# Quantum Azure



Quantum

Why Microsoft

Team

Technology

Resources

All Microsoft

## The only scalable quantum solution

Quantum computing promises a revolution in how we solve the world's most complex problems. Fully realizing this promise requires a scalable quantum solution that anyone can start exploring. From breakthroughs in physics and nanomaterials to seamless integration with Azure and familiar developer tools, Microsoft is leading the way to scalable, accessible quantum computing.

[Read more >](#)

<https://docs.microsoft.com/en-us/quantum/?view=qsharp-preview>

<https://github.com/Microsoft/Quantum>



## Advanced code optimization in a simulated environment

Set breakpoints, step into the Q# code, debug line-by-line, and estimate the real-world costs to run your solution. Simulate quantum solutions requiring up to 30 qubits with a local simulator, or use the Azure simulator for large-scale quantum solutions requiring more than 40 qubits.

# Back to Enigma

## How much time would it take to crack Enigma today?

1. Turing did not use 'brute force' to solve Enigma
2. Enigma: 15,354,393,600 combinations
3. 2017: DigitalOcean copied the work of Turing with 2,000 VM's and a piece of Python code (single thread): 13 mins of work. Cost 7\$.
4. Code worked through combinations 'one by one'
5. With Quantum... it doesn't get faster (not depending on hardware)
6. Using Shor's algorithm and parallel computation – it does.
7. A 30-qubit quantum computer would equal the processing power of a conventional computer that could run at 10 **teraflops** (trillions of floating-point operations per second)
8. So... cracking Enigma with 40 qbits would be like 0,00000000000..... 1 second.
9. **TO BE VALIDATED! (And I will write about it ☺ Need to learn Q# first)**

<https://blog.digitalocean.com/how-2000-droplets-broke-the-enigma-code-in-13-minutes/>



# Who was this guy?

Jeroen Mulder

Lead Architect

Hybrid IT and Emerging Technology

+ Azure Nerd

CISA

[Jeroen.Mulder@ts.fujitsu.com](mailto:Jeroen.Mulder@ts.fujitsu.com)

@Jeroen1511

Latest blog on

<https://blog.global.fujitsu.com/fgb/2019-04-05/go-cloud-native-or-dont-go/>

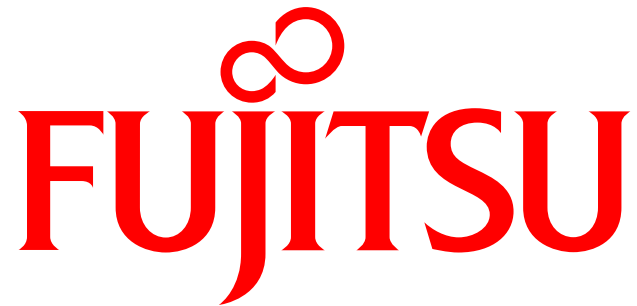


# Graag tot ziens!



- Bedankt voor jullie komst
- Vragen?
  - Bob de Vries – Microsoft practice lead, [bob.devries@ts.fujitsu.com](mailto:bob.devries@ts.fujitsu.com)
  - Hanin el Farissi – Head of Hybrid IT, [hanin.elfarissi@ts.fujitsu.com](mailto:hanin.elfarissi@ts.fujitsu.com)
  - Jeroen Mulder – Architect/Azure Lead, [jeroen.mulder@ts.fujitsu.com](mailto:jeroen.mulder@ts.fujitsu.com)
  - Anouk Deneer – Marketing Netherlands, [anouk.deneer@ts.fujitsu.com](mailto:anouk.deneer@ts.fujitsu.com)
  - Theo Wakkermans - Head of Architecture & Consultancy, [theo.wakkermans@ts.fujitsu.com](mailto:theo.wakkermans@ts.fujitsu.com)
- @Fujitsu\_NL      #Fujitsu\_NL
- [www.linkedin.com/company/fujitsu-nederland](https://www.linkedin.com/company/fujitsu-nederland)





shaping tomorrow with you