How to Anticipate on the Advent of the Quantum Computer

Oscar Covers, Chairman of the European Cards Payments Association Security Working Group (ECPA SWG)

Topics to be Discussed

- Introduction
- What is a quantum computer
- Why should we monitor the quantum computing developments?
- Known complications
- Known unknowns
- Comforting certainties
- Low regret moves

Introduction

Who is Oscar Covers

- Active in payments since August 2001 and was for over 12 years responsible for the security certification of Dutch POS terminals.

- Cyber Security Analyst
- Chairman of the Dutch interbank security working group
- Member of the Curriculum Committee - course Applied Cryptography

- Chairman of the ECPA SWG,
  on behalf of the Dutch Payments Association
- Member of the PCI PTS working group (PCI PTSwg),
  on behalf of the Dutch Payments Association

The Quantum Computer

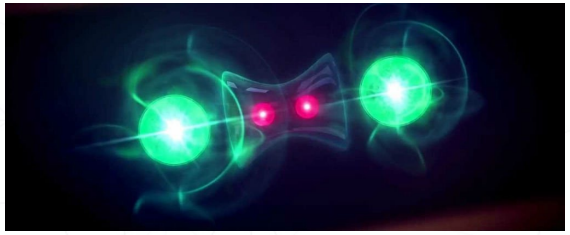
The Most Important Quantum Mechanics Concepts

To understand quantum computing:

- Superposition

- Interference

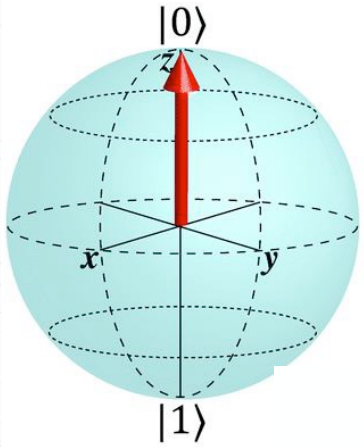
- Entanglement

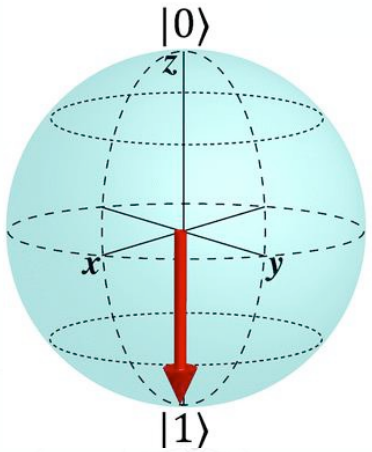


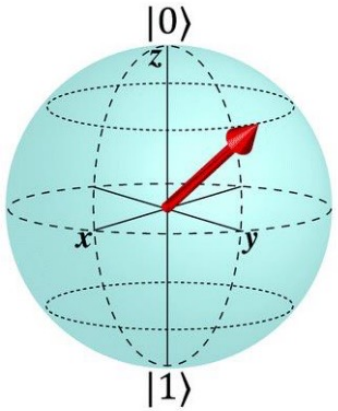
Superposition

Current computers work with bits: 0 of 1

The quantum computer uses Qubit (*quantum bits*):







With each Qubit, the information that is included in the calculation doubles!

The Quantum Computer Will Be a Disruptor

A quantum computer can simulate the properties and behavior of molecules and take chemistry to a new level

Nitrogen Fixation

Industrial Manufacturing

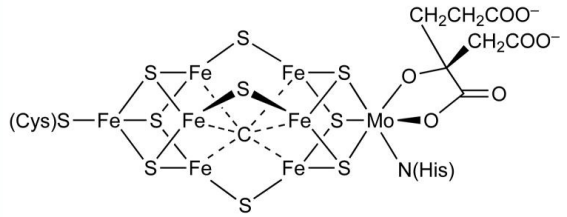
Industry uses a process that operates at 500ºC, 20 Mpa and consumes 2% of the world's annual energy consumption!

Natural Production

Bacteria outperform this process[1] at 25ºC and atmospheric pressure (0,1 MPa)

Quantum Computational Chemistry

The chemical reaction mechanism for FeMoCo driven nitrogen fixation is not understood and cannot be simulated on a classical computer

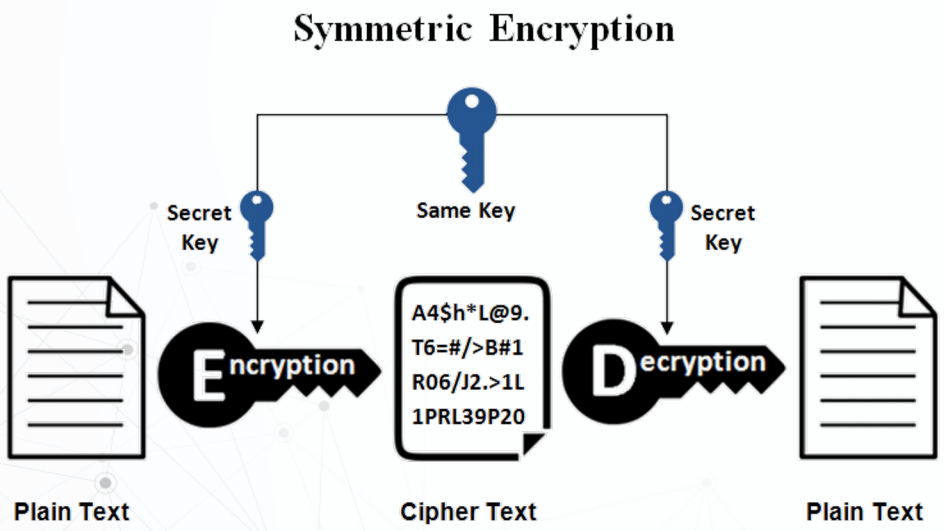


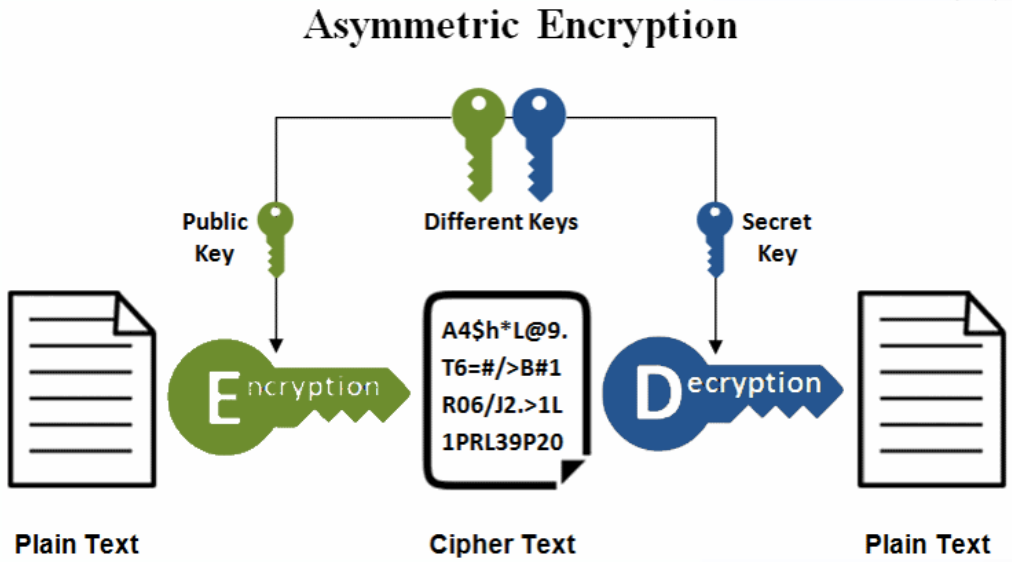
However, in 2016, Reiher et al.2 showed how a quantum computer with 111 qubits can be used to simulate (understand) this chemical reaction

[1] Active site of Mo-dependent nitrogenase: iron molybdenum cofactor (FeMoco), splits the dinitrogen triple bond
[2] https://arxiv.org/abs/1605.03590

Why Monitor the Quantum Computing Developments?

Encryption is incorporated in many business processes





Digital signatures

Public encryption

Algorithms That Lower the Security Level of Our Encryption

The algorithm of Grover weakens symmetric encryption

- Worst case scenario: The effective key strength is halved

  Migrate to AES

  HASH functions: SHA256

Lov Grover

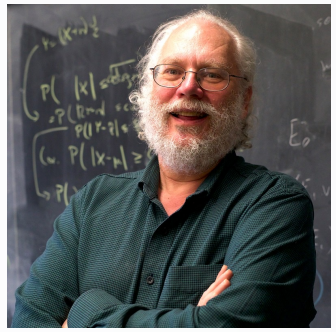
The algorithm of Shor weakens asymmetric or public key encryption!

- As an example: Factor a 2048-bit number into prime numbers
- With the best classical algorithm (GNFS algorithm)

  ~ 10^{34} steps; on supercomputer (one trillion operations per second) -> ~ 317 trillion years

- With the quantum algorithm Shor

  ~ 10^{7} steps; on a quantum computer (one million operations per second) -> ~ 10 seconds



Peter-Shor

Condition: 4099 logical qubits (1 logical qubits ~1000 to 10.000 physical qubits)

Impact on Crypto Algorithms

Long term confidentiality biggest problem

- Intercept and store encrypted communication
- Decrypt retroactively, much later

Theorem (Mosca): If x + y > z then we have problem!

- x = security shelf life
- y = migration time
- z = quantum computer is built

Post Quantum Cryptography - Classical cryptosystems resistant against quantum computer attacks

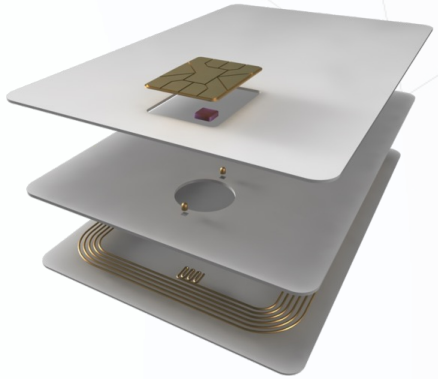
Mosca[1]: 1/7 chance of breaking RSA-2048 by 2026 and 1/2 chance by 2031

[1] NIST Workshop on Cybersecurity in a Post-Quantum World, April 2015.

Known Complications

Replacement crypto primitives for the banking industry has long lead times

- Service life smart card platforms ranging from 8 to 17 years
- Service life POS & ATM ranging from 5 to 20 years
- Not all crypto primitives in use can easily be replaced. Post Quantum Crypto alternatives do not offer simple drop-in replacements and require redesign.
- Standards and policies for rollout of PQC are lacking



Some Comforting Certainties

- Symmetric encryption is considered safe (≥AES128)
- Hash functions are considered safe (≥SHA-2)
- Functions and algorithms, like message authentication code, key generation and key derivation remain secure if previously mentioned algorithms are used
- Protocol concepts of the “old era”, that predate the use of asymmetric cryptography, remain valid and secure.

Known Unknowns

- Day z is unknown
- The field of quantum computing and the PQC standardization is still highly in flux
- Missing inventory of all business processes that use encryption

Low Regret Moves

1. Monitor developments in quantum computing and PQC closely
2. Maintain and expand inventory of interbank processes

	Encryption Algorithms Used	Security shelf life	Post-quantum crypto	required time for migration	Critical timeframe
Application	RSA 2048		NewHope	24 months	
	Three-key TDEA Encryption	till 2023*	AES 256	12 months	
	AES 128	Beyond 2030**	AES 256	12 months	

*NIST SP 800-131A REV. 2 (DRAFT)
* * NIST SP 800-57 Pt. 1 Rev. 5

Low Regret Moves

1. Monitor developments in quantum computing and PQC closely
2. Maintain and expand inventory of interbank processes
3. Ask international financial organizations to prepare for the advent of the quantum computer

Etc.

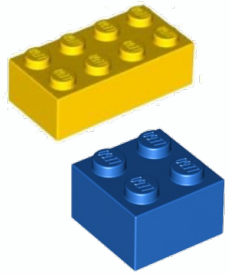
4. For symmetric cryptography, start the migration to AES, secure hashes and secure key derivation immediately
5. For the card payments infrastructure develop a fallback that does not rely on asymmetric encryption

Low Regret Moves

5. For the card payments infrastructure develop a fallback that does not rely on asymmetric encryption
   - For POS & ATM a fall-back scenario seems feasible:

Block ciphers

Hash functions



Message authentication code

Key generation

Key derivation

We can also use the PQC candidate CRYSTALS-KYBER for key-establishment.

   - It starts with the foundation, a quantum resistant secure bootloader.

Low Regret Moves

1. Monitor developments in quantum computing and PQC closely
2. Maintain and expand inventory of interbank processes
3. Ask international financial organizations to prepare for the advent of the quantum computer
4. For symmetric cryptography, start the migration to AES, secure hashes and secure key derivation immediately
5. For the card payments infrastructure develop a fallback that does not rely on asymmetric encryption
6. For EMV smart card profile develop a profile that does not rely on asymmetric encryption
7. Enforce a policy to swiftly implement the latest official TLS releases and gain experience with PQC in High-assurance implementations

ECPA

European Card Payment Association

THANK YOU FOR YOUR ATTENTION

Further reading and more background suggestions

How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure (2020)