Betaalvereniging Nederland

Hoe in te spelen op de komst van de quantumcomputer?

… voor het betalingsverkeer

PvIB Platform voor InformatieBeveiliging

Oscar Covers
Risk Management

Utrecht
14 januari 2020

Agenda

Betaalvereniging Nederland

- Waarom ontwikkelingen van de quantumcomputer volgen voor bancaire sector?
- Bekende complicaties
- Bekende onbekende factoren
- Geruststellende zekerheden
- *Low regret moves* om dreigingen te mitigeren

De quantumcomputer in het nieuws

Betaalvereniging Nederland

CAIXABANK DEVELOPS THE FIRST R&D PROJECTS AIMED AT APPLYING QUANTUM COMPUTING TO FINANCIAL ACTIVITY IN SPAIN

The bank has set up a team of experts with IT technicians, mathematicians and risk analysts.

Press release from Caixabank
September 3rd 2019 | 829 readers

• The Bank has adapted a quantum algorithm such as mortgage and treasury bill portfolios.

• Quantum computing will help solve hugely c will also provide better solutions to the curren

CaixaBank has conducted the first real tests u technology within the scope of risk analysis. T Qiskit, an infrastructure that includes a simula scientific community with tools to develop and execute quantum algorithms.

Nieuws - 7 februari 2019 - 07:51

ng Willem Al

t Microsoft C

Quantum algorithms for financial derivatives

Wednesday 4 September 2019 | 08:15 AM CET

4-9-2019

***IBM Research** scientist **Stefan Woerner** reveals for The Paypers findings of a recently published paper called **Option Pricing Using Quantum Computers**, co-authored with JPMorgan*

In the finance industry, options, or more generally financial derivatives, are contracts that give their owner the right, but not the obligation, to buy or sell some underlying security or set of securities at pre-defined conditions, such as time or price. They're used in hedging strategies to manage financial risk, or to speculate on future market performance. Just in 2018, more than 13 billion option contracts were traded worldwide.

Karl Flinders
Emea Content Editor, Computer Weekly

Published: 27 Jun 2019 12:04

leeltjes.

Canadians issue digital security recommendations in the financial sector

Tuesday 27 August 2019

2

The Canadia decided t issue.

After several meetin came up with nine industry and what t recommendations in

Recommendation 1: the public safety an including internation

Recommendation 7: responsible vulnerab

Recommendation 8: approaches to lawful

Recommendation 9: to ensure all sensitiv packets are not expo

Quantum technologies + Add to myFT

Google claims to have reached quantum supremacy

Researchers say their quantum [illegible] em for ordinary machines

20-9-2019

Madhumita Murgia and Richard Waters SEPTEMBER 20 2019

162

Google claims to have built the first quantum computer that can carry out calculations beyond the ability of today's most powerful supercomputers, a landmark moment that has been hotly anticipated by researchers.

A paper by Google's researchers seen by the FT, that was briefly posted earlier this week on a Nasa website before being removed, claimed that their processor was able to perform a calculation in three minutes and 20 seconds that would take today's most advanced classical computer, known as Summit, approximately 10,000 years.

The researchers said this meant the "quantum supremacy", when quantum computers carry out calculations that had previously been impossible, had been achieved.

"This dramatic speed-up relative to all known classical algorithms provides an experimental realisation of quantum supremacy on a computational task and heralds the advent of a much-anticipated computing paradigm," the authors wrote.

"To our knowledge, this experiment marks the first computation that can only be performed on a quantum processor."

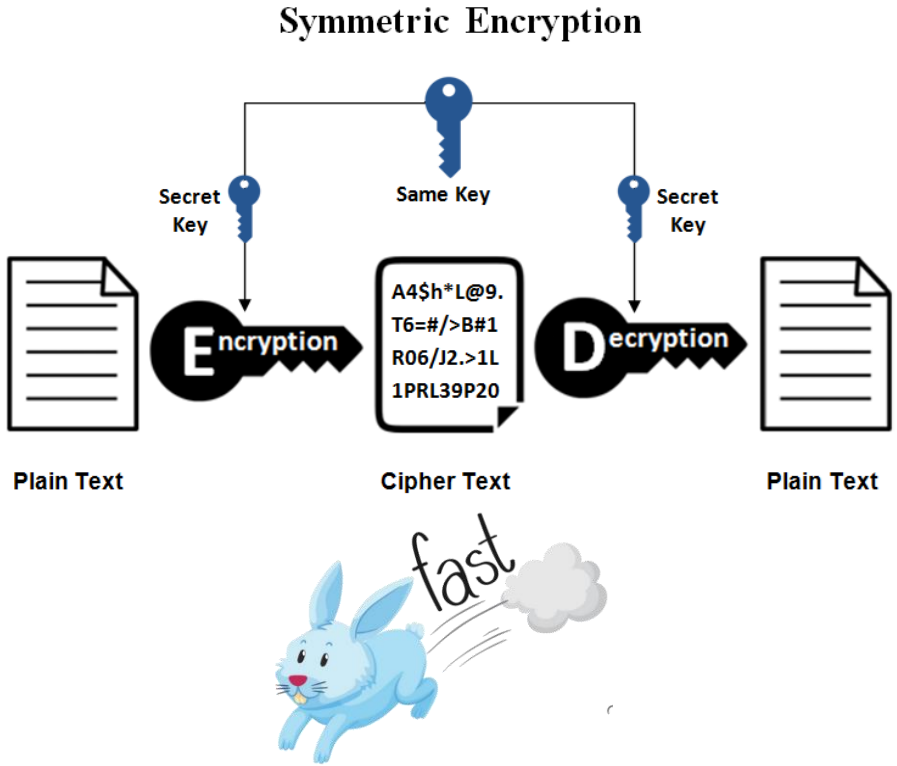
LLC,

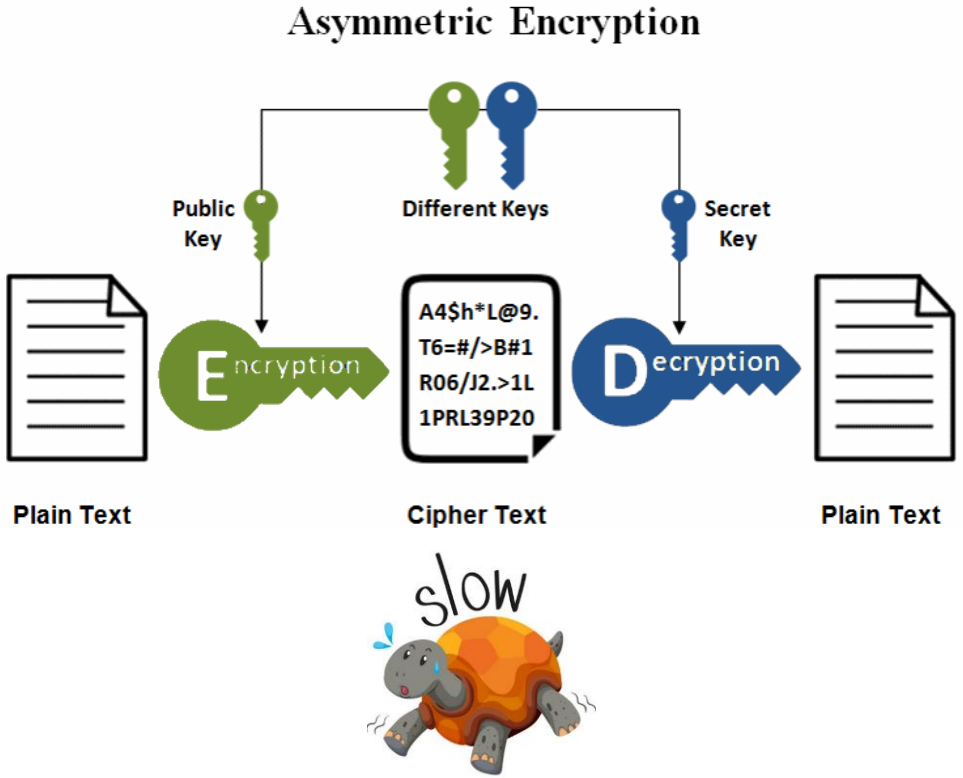
Quantum
ments key
provide volume"
layers from a
d (China),Intel
(Canada),Google
s),Cisco Systems
& Co, Inc. (United

Waarom wij ontwikkelingen van de quantumcomputer volgen voor bancaire sector

Betaalvereniging Nederland

- De beveiliging van vele bancaire diensten vertrouwt op encryptie
- Encryptie is in twee groepen onder te verdelen:





Digital signatures

Public encryption

Key exchange

Waarom wij ontwikkelingen van de quantumcomputer volgen voor bancaire sector

Betaalvereniging Nederland

- De beveiliging van vele bancaire diensten vertrouwt op encryptie
- Encryptie is in twee groepen onder te verdelen: symmetrische en asymmetrische encryptie
- De banken hebben geen staatsgeheimen, maar verwerken wel veel transacties
- Vertrouwen is erg belangrijk voor bankdiensten
- Encryptie werpt een rekenkundige barrière op

- Enkele problemen die voor de huidige computer onoplosbaar zijn, zijn voor de quantumcomputer eenvoudig op te lossen!
- Twee quantumalgoritmen verlagen het beveiligingsniveau van onze huidige encryptie

Algoritmen die beveiligingsniveau huidige encryptie verlagen

Betaalvereniging Nederland

- Het Groveralgoritme beïnvloedt symmetrische encryptie
  - Worst case scenario:
    - Verdubbel de sleutellengte: ~~3DES~~ AES
    - Verdubbel de output van HASH functies: ~~SHA-1~~ -> SHA256

- Het Shoralgorithme beïnvloedt asymmetrische encryptie of public key encryption
- Ter illustratie: factorisatie van een 2048-bits getal
- Met het beste klassieke algoritme (GNFS algoritme)

  ~ 10^{34} stappen; op klassieke THz Computer (een triljoen bewerkingen per seconde) -> ~ 317 triljoen jaar
- Met het kwantumalgoritme Shor

  ~ 10^{7} stappen; op een MHz quantumcomputer (een miljoen bewerkingen per seconde): -> ~ 10 seconden
- Voorwaarde 4099 logische qubits

Impact op cryptoalgorithmen

Het quantumalgorithme Shor heeft dus veel Qbits nodig!

Resource schattingen voor twee bekende crypto algoritmes:

- ECDSA: over n-bit finite field, require ~9n qubits and $O(n^3)$ Toffoli gates
- P-224 needs 2042 **logical** qubits and $8{,}43 \cdot 10^{10}$ Toffoli gates

- RSA: n-bit modulus N requires ~ 2n qubits and $O(n^3)$ Toffoli gates
- RSA-2048 modulus needs 4098 **logical** qubits and $5{,}20 \cdot 10^{12}$ Toffoli gates

Logical qubits ~1000 to 10000 physical qubits

Roetteler, Martin, et al. "Quantum resource estimates for computing elliptic curve discrete logarithms." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Cham, 2017.

Impact op cryptoalgorithmen

Betaalvereniging Nederland

Langdurige vertrouwelijkheid is grootste probleem

- Onderschep vercijferde communicatie en sla op
- Ontcijfer vercijferde data met terugwerkende kracht

Stelling (Mosca): Als x + y > z dan hebben we een probleem!

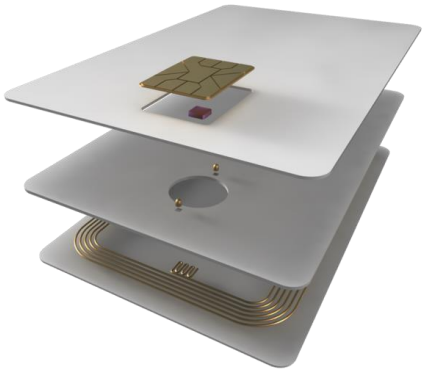
- x = houdbaarheid van de beveiliging
- y = migratietijd
- z = grote quantumcomputer is gebouwd

Mosca: 1/7 kans om RSA-2048 te breken tegen 2026 en 1/2 kans tegen 2031

Bekende complicaties

Het vervangen van crypto primitieven in het bancaire domein kent lange doorlopentijden:

- Smart card platformen gaan circa 8 tot 17 jaar mee (selectie en certificatie 3 jaar, uitgifte voor 5 jaren, toelating te verlengen tot 12 jaar)
- Serviceleven POS & ATM variëren van 5 tot 20 jaar
- In gebruik zijnde crypto primitieven laten zich niet allen eenvoudig vervangen. De PQC-alternatieven bieden geen "drop-in"-vervanging en vragen om redesign.
- Standaarden en policies voor de uitrol van PQC bestaan nog niet



De bekende onbekenden

- Dag z
- Het PQC-onderzoeksveld is nog volop in beweging
- Inventarisatie van alle bancaire processen die encryptie gebruiken ontbreekt

Geruststellende zekerheden

- Symmetrische algoritmes zoals AES (≥AES128) worden als veilig beschouwd tot 2031 en daarna
- Hashfuncties zoals (≥) SHA-2 worden als veilig beschouwd tot 2031 en daarna
- MAC, sleutelgeneratie en sleutelafleiding gebaseerd op deze functies en algoritmen blijven veilig
- De protocolconcepten uit de "oude tijd" van vóór het gebruik van asymmetrische cryptografie, blijven geldig en veilig. Echter 3DES moet vervangen worden.
- De quantumcomputer zal zijn meerwaarde eerder aantonen voor minder veeleisende toepassingen, en dit zal niet geheim blijven. Een volgende generatie quantumcomputers zal pas krachtig genoeg zijn om de cryptografie te breken.

De dreiging van de quantumcomputer en *Low regret moves*

Betaalvereniging Nederland

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
   a) Jaarlijkse workshops met brede expertgroep
   b) Met readiness projectgroep ontwikkelingen vertalen naar interbancaire acties en jaarlijks het interbancaire lange termijn plan actualiseren
   c) Onderhoud en actualiseer de Q&A om de pers te kunnen informeren

De dreiging van de quantumcomputer en *Low regret moves*

Betaalvereniging Nederland

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
2. Onderhoud en breid de huidige inventarisatie van interbancaire processen uit.

Business process	encryption algorithms used	Security shelf life	Post-quantum crypto	required time for migration	Critical timeframe
	RSA 2048		NewHope	24 months	
	Three-key TDEA Encryption	till 2023*	AES 256	12 months	
	AES 128	till 2030**	AES 256	12 months	

*NIST SP 800-131A REV. 2 (DRAFT)
** NIST SP 800-57 Pt. 1 Rev. 4

De dreiging van de quantumcomputer en *Low regret moves*

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
2. Onderhoud en breid de huidige inventarisatie van interbancaire processen uit.
3. Spoor internationale financiële organisaties aan om zich voor te bereiden op de komst van de kwantumcomputer.

Ect.

De dreiging van de quantumcomputer en *Low regret moves*

Betaalvereniging Nederland

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
2. Onderhoud en breid de huidige inventarisatie van interbancaire processen uit.
3. Spoor internationale financiële organisaties aan om zich voor te bereiden op de komst van de kwantumcomputer.
4. Voor klassieke cryptografie, start migratie naar AES, veilige hashes en veilige sleutelafleidingsalgorithmes.

De dreiging van de quantumcomputer en *Low regret moves*

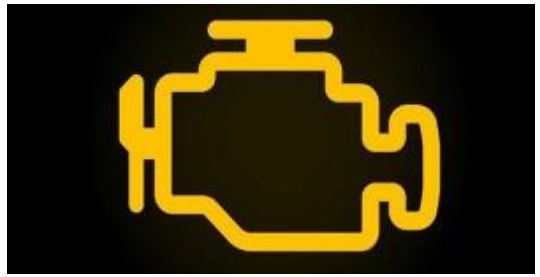
Betaalvereniging Nederland

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
2. Onderhoud en breid de huidige inventarisatie van interbancaire processen uit
3. Spoor internationale financiële organisaties aan om zich voor te bereiden op de komst van de kwantumcomputer
4. Voor klassieke cryptografie, start migratie naar AES, veilige hashes en veilige sleutelafleidingsalgorithmes.
5. Ontwikkel een fallbackscenario naar de klassieke cryptografie voor de Cards-infrastructuur. Asymmetrische encryptie wordt gebruikt voor remote sleuteldistributie en ondertekening. Hiervoor zijn ook klassieke alternatieven als MAC, challenge response en traditionele sleuteldistributie.

De dreiging van de quantumcomputer en *Low regret moves*

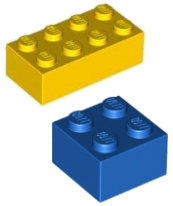
Betaalvereniging Nederland

5. Ontwikkel een fallbackscenario naar de klassieke cryptografie voor de Cards-infrastructuur.
   - Als op dag z een krachtige quantumcomputer encryptie kan breken
   - …dan moet het betalingsverkeer door kunnen gaan, desnoods tijdelijk iets minder efficiënt.
   - Voor POS & ATM lijkt een fall-back scenario haalbaar:



Block ciphers

Hash functions



→

Key generation

Key derivation

Message authentication code

Authenticatie; challenge response

Traditionele sleuteldistributie

De protocolconcepten uit de "oude tijd“ blijven veilig, zoals split knowledge/key components.
Inzet van veelbelovende PQC candidates like NewHope.

De dreiging van de quantumcomputer en *Low regret moves*

Betaalvereniging Nederland

1. Volg de ontwikkelingen op het gebied van quantumcomputing en PQC op de voet.
2. Onderhoud en breid de huidige inventarisatie van interbancaire processen uit
3. Spoor internationale financiële organisaties aan om zich voor te bereiden op de komst van de kwantumcomputer
4. Voor klassieke cryptografie, start migratie naar AES, veilige hashes en veilige sleutelafleidingsalgorithmes.
5. Ontwikkel een fallbackscenario naar de klassieke cryptografie voor de Cards-infrastructuur.
6. Ontwikkel een EMV-smartcardprofiel dat niet afhankelijk is van asymmetrische encryptie.
7. Bepaal in beleid de regel om altijd de laatste officiële TLS-versies snel te implementeren en doe ervaringen op met PQC.