How financials can anticipate on the advent of the quantum computer

Oscar Covers

21 April 2022

Agenda

- Why the financial sector should monitor the advent of the quantum computer
- Known complications
- Known unknowns
- Comforting certainties
- Emerging threats, low regret moves and challenges

Monitoring the advent of the quantum computer for the financial sector

- Security is freedom from, or resilience against, potential harm caused by others
- Encryption is incorporated in many financial services
- Banks don’t manage state secrets
- Bank do process many transactions
- Trust is key for banking services
- Encryption raises a computational barrier

- Some unsolvable problems for the current computer can easily be solved by quantum computers!
- Two known quantum algorithms lower the security level of our current encryption

Algorithms that lower the security level of our encryption

- The algorithm of Grover weakens symmetrical encryption
  - Worst case scenario:
    - Double the key length: AES128 -> AES256
    - HASH functions: SHA256

- The algorithm of Shor breaks our current asymmetric encryption or public key encryption!

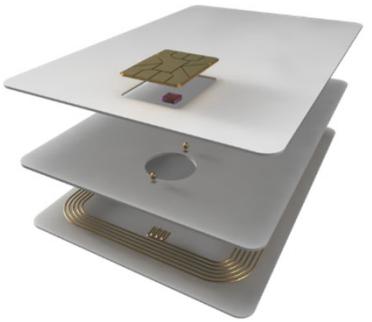
When will the generic quantum computer be available?

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

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

Known complications



Replacement crypto primitives 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 based on symmetric encryption, such as message authentication code, key generation and key derivation, remain secure
- Concepts of the “old era”, predating the use of asymmetric cryptography, remain secure.

Low regret moves

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

	encryption algorithms used	Security shelf life	quantum resistant cipher	required time for migration	Critical timeframe
Application	RSA 2048				
	Three-key TDEA Encryption	till 2023*	AES 256	12 months	
	AES 128	till 2030**	AES 256		

*NIST SP 800-131A REV. 2 (DRAFT)

**NIST SP 800-57 Pt. 1 Rev. 4

NIST post-quantum competition, Round 3 Finalists

(https://csrc.nist.gov/projects/post-quantum-cryptography)

- NIST post-quantum competition

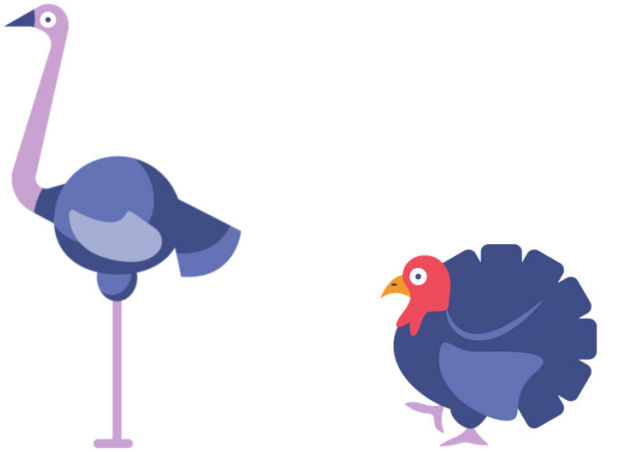
Hard problem	Signature	KEM
Lattice based	DILITHIUM, FALCON	CRYSTALS-KYBER, NTRU, SABER
Code based	X	Classic McEliece
Multivariate	~~Rainbow~~	X
Hash based	X	X
Other	X	X

- Alternate Candidates

Hard problem	Signature	KEM
Lattice based	NTRU Prime	FrodoKEM
Code based	x	BIKE, HQC
Multivariate	GeMSS	x
Hash based	Picnic, SPHINCS+	x
Other	x	SIKE

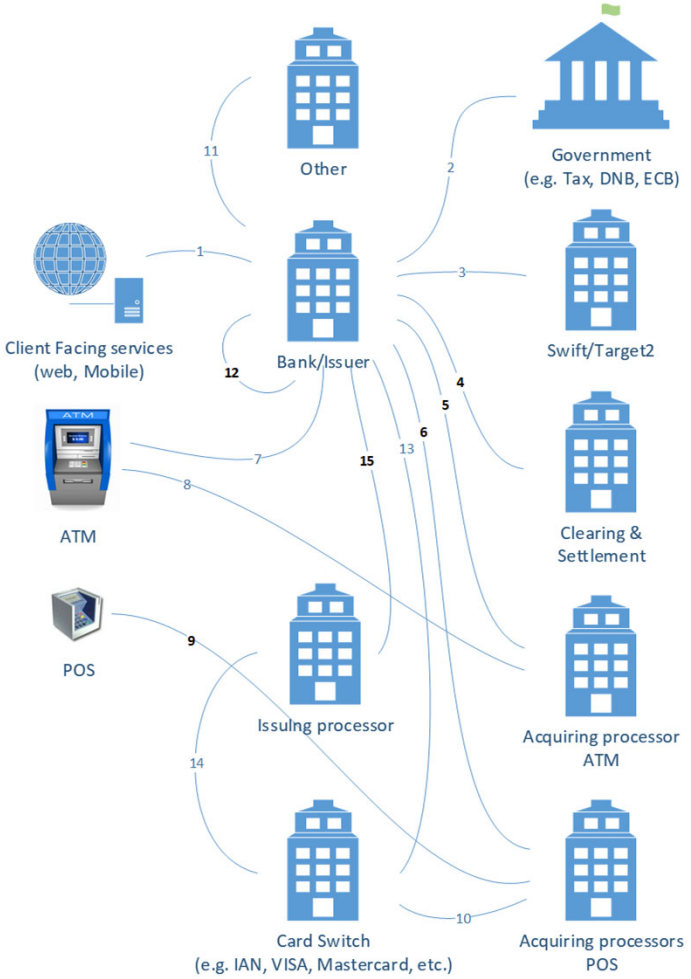
PQC Performance Considerations

- Network performance
  - Larger signature and key sizes -> more data to be transferred -> packet fragmentation -> may lead to high delays in lossy networks
  - VPN are less impacted
  - TLS
    Cloudflare

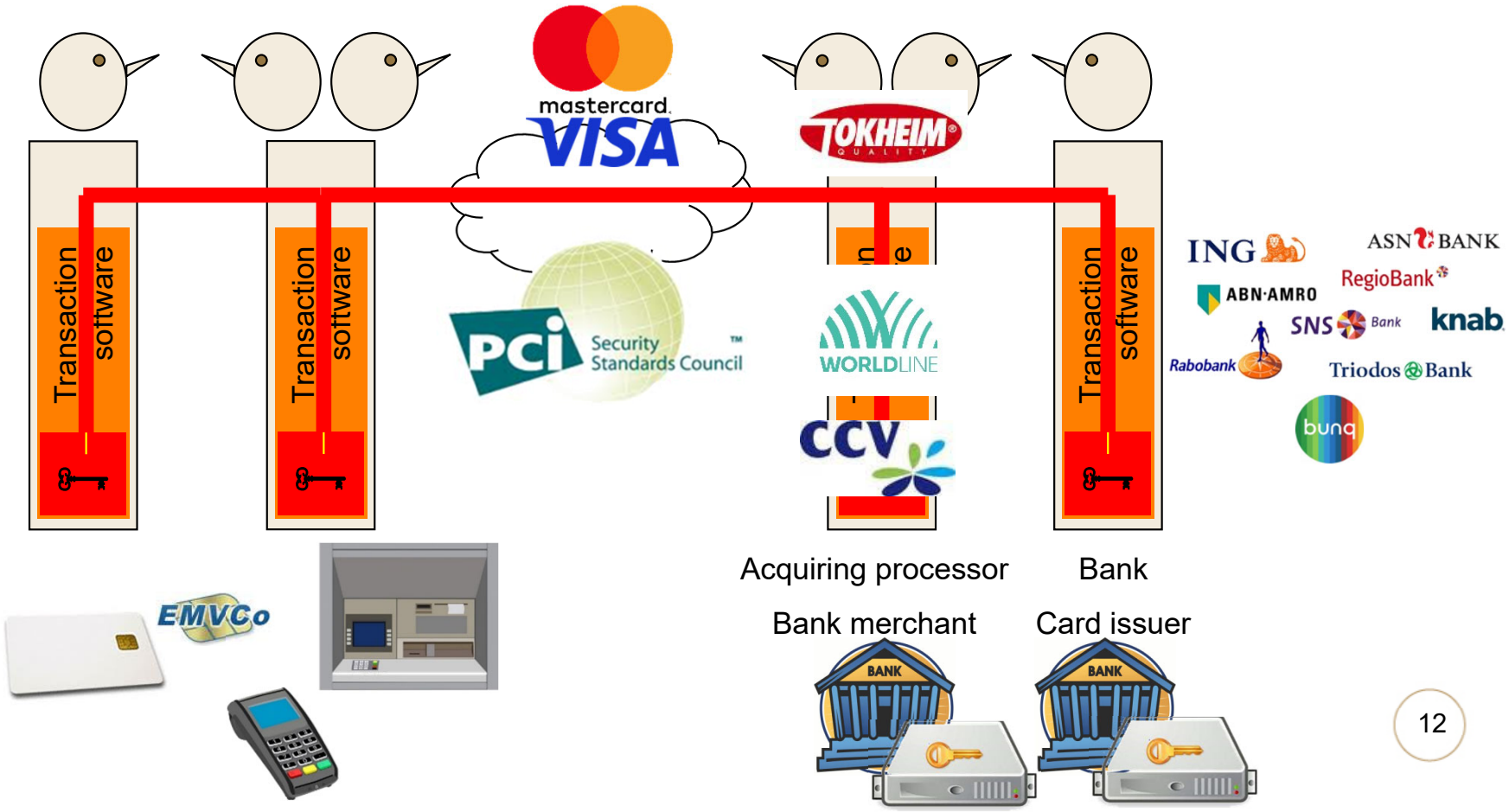


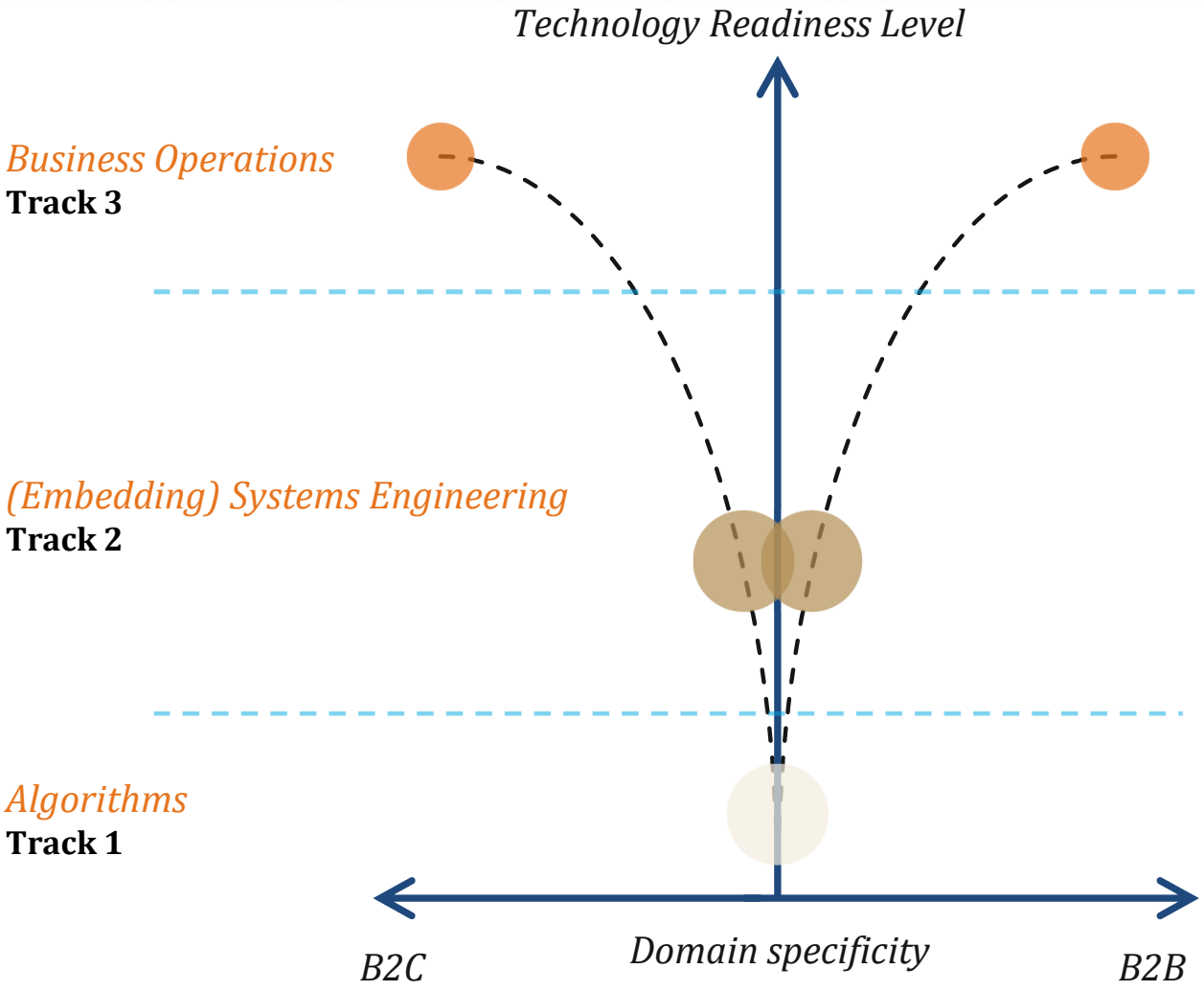
CECPQ2 = HRSS + X25519

CECPQ2b = SIKE + X25519


Other
Government
(e.g. Tax, DNB, ECB)
Client Facing services
(web, Mobile)
Bank/Issuer
Swift/Target2
ATM
Clearing &
Settlement
POS
Issuing processor
Acquiring processor
ATM
Card Switch
(e.g. IAN, VISA, Mastercard, etc.)
Acquiring processors
POS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

EFT POS/ATM and the stakeholders




Technology Readiness Level
Business Operations
Track 3
(Embedding) Systems Engineering
Track 2
Algorithms
Track 1
B2C
Domain specificity
B2B

Algorithm

- Available PQ algorithms:
  - ≥ AES 128
  - ≥ SHA-2
- PQC NIST algorithms

  Public-Key Encryption/KEMs
  - Classic McEliece
  - CRYSTALS-KYBER
  - NTRU
  - SABER

  Digital Signatures
  - CRYSTALS-DILITHIUM
  - FALCON
- Stateful Hash-Based Signature Schemes,
  - LMS
  - XMSS
  - HSS
  - XMSS^{MT}

A

SysEng B2B:

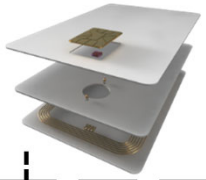
B2B

B2C

SysEng General:

- Governance Req. Eng.
- Technical Req. Eng.
- How to embed in infrastructure
- Resource costs estimation

SysEng B2C:



B2C

B.Ops B2B:

- Functional business requirements
- Timelines
- Risk management
- Who to involve

B2C

B.Ops B2C:

- Functional business requirements
- Impact
- Timelines
- Risk management
- Who to involve

Technology Readiness Level

Protocols *Embedding Systems Engineering* *Business Operations*

Low regret moves extended

3. Urge international financial organizations to prepare for the advent of the quantum computer     Ect.
4. Start the migration to AES, secure hashes and secure key derivation
5. For the card payment infrastructure develop fall-back to quantum resistant ciphers
6. For EMV smart card profile develop a profile that doesn't rely on asymmetric encryption
7. Implement the latest official TLS releases and gain experience with PQC

Questions?