FS Club

News Events Partnerships

Quantum-Resistant Encryption

Webinar

Friday 19 June 2020

FS Club

News Events Partnerships

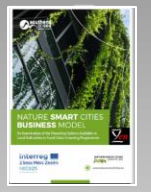
A Word From Our Chairman

Professor Michael Mainelli

Executive Chairman

Z/Yen Group






FS Club

Platinum Sponsors

Invest Northern Ireland
Red Hat
CDI China Development Institute
GIFT Gujarat International Finance Tec-City
Seoul Together we stand
LuxembourgforFinance Agency for the Development of the Financial Centre
Casablanca Finance City القطب المالي للدار البيضاء
BIFC Busan International Finance Center
GT
AIFC
Finance Montréal
Abu Dhabi Global Market
Dubai International Financial Centre

Gold Sponsors

PEERNOVA
Aptitude Software
BRIDGEWORKS
FEATURE SPACE
OUTSMART RISK
ARBORETUM
Crown Agents Bank

Silver Sponsors

P2 CONSULTING
InfrasoftTech Fintech Digital Solutions
Bottomline
BCS CONSULTING Expect Excellence
PRAXITY Empowering Business Globally
ESTATES AND INFRASTRUCTURE EXCHANGE®
The Technium Global SERVICE WITH INTEGRITY

Bronze Sponsors

Profile Software
(expleo)
CONTACT PARTNERS
alyne

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI Global Legal Entity Identifier Foundation
cuffassociates
GPS global processing services
The Transparency Task Force
CYGNETISE
Catalina Consulting
AMSOM
Gibraltar Stock Exchange
Volanté

Agenda

FS Club

News Events Partnerships

12:00 – 12:05	Chairman's Introduction
12:05 – 12:30	Keynote Address
12:30 – 12:45	Questions & Answers

FS Club

News Events Partnerships

Quantum-Resistant Encryption

Maury Shenk

Managing Director

Lily Innovation

The Post-Quantum Cryptography Problem

FS Club

3 2 4

Large-scale quantum computers would pose ***a serious***

1

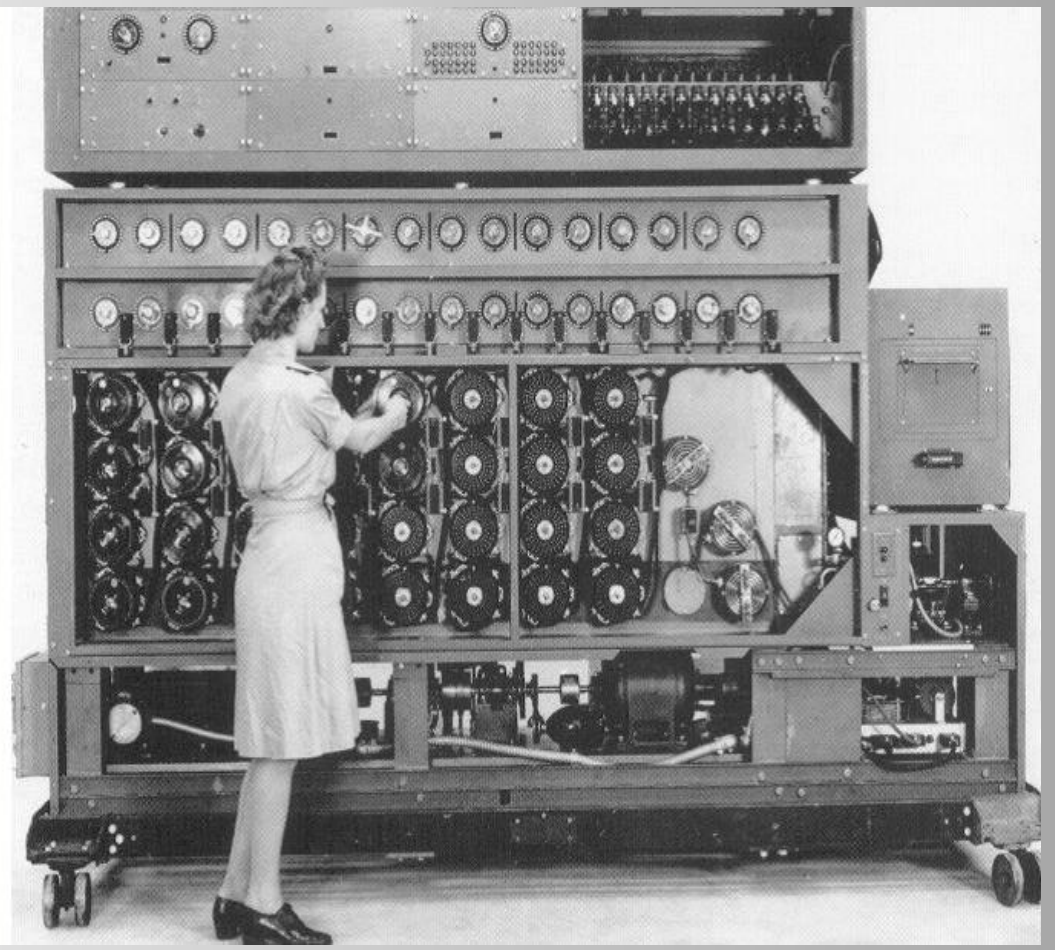
threat to the security of ***public key cryptography***

6 5

So ***what should affected entities do***, and ***when***?

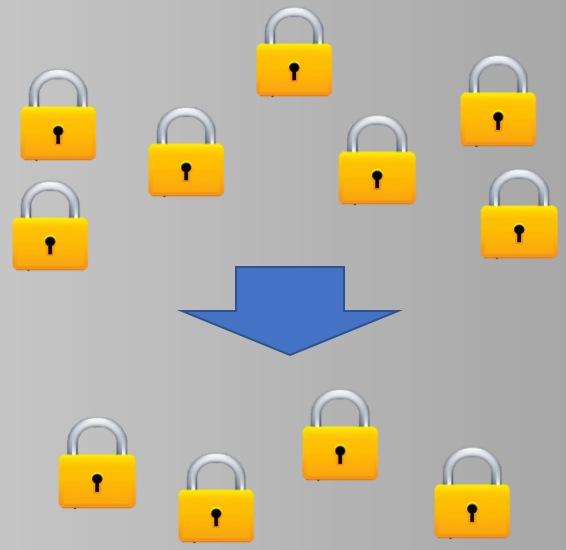
Symmetric Cryptography

FS Club



Public Key Cryptography

- Uses public and private keys for each communication, avoiding need for key exchange
- Based on problems that are “hard” in one direction (eg knapsack problem or integer factorisation)
- Secures many aspects of electronic communications and authentication



Technique	Sender Uses	Recipient Uses	Why It Works
Public key secure communication	Recipient’s public key	Recipient’s private key	Only recipient (using her private key) can read messages encrypted with her public key
Public key digital signature	Sender’s private key	Sender’s public key	Only sender can sign with her private key, and recipient can use the sender’s public key to confirm signature

The Post-Quantum Cryptography Problem

FS Club

3 2 4

Large-scale quantum computers would pose ***a serious***

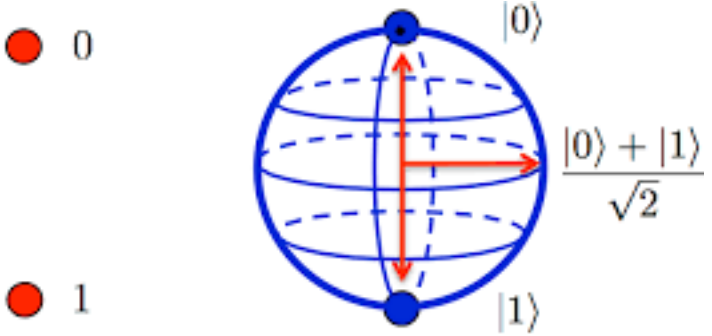
1

threat to the security of ***public key cryptography***

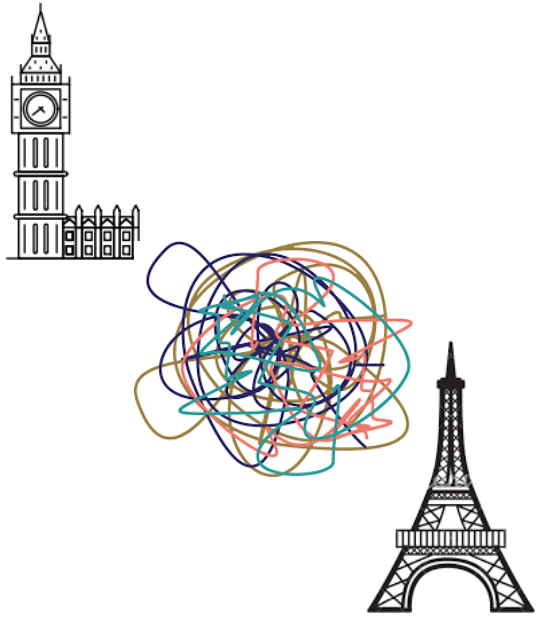
6 5

So ***what should affected entities do***, and ***when***?

Quantum Phenomena



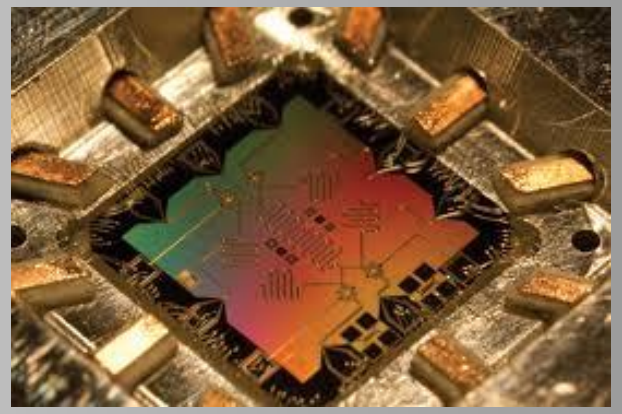
Classical Bit Qubit

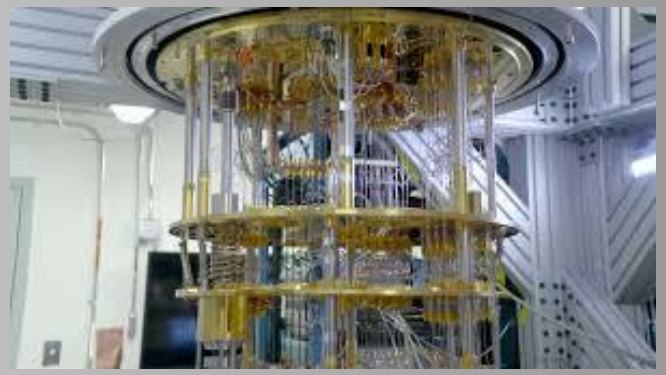


Superposition Entanglement

Quantum Computers

- Proposed by Richard Feynman in 1981
- Progress with entangled qubits
  - 1998 – 2 (Oxford)
  - 2011 – 14 (academics in Austria and Canada)
  - 2018 – 72 (Google)
- Physical qubits (the numbers above)
  - Low-temperature devices showing quantum effects
  - Decoherence – ~100 microseconds for operational quantum computers
- Logical qubits (do not exist yet)
  - Stable computing devices
  - ~1000 - 10,000 physical qubits required for one logical qubit
  - 3000-5000 logical qubits required to attack current public key cryptography





The Post-Quantum Cryptography Problem

FS Club

3 2 4

Large-scale quantum computers would pose ***a serious threat*** to the security of ***public key cryptography***

1

6 5

So ***what should affected entities do***, and ***when***?

The Quantum Threat

FS Club

- The new math!
- Shor's algorithm
  - Discovered in 1994 at Bell Laboratories
  - Would allow a sufficiently powerful quantum computer to solve quickly the hard problems underlying the most common public key cryptography algorithms (including RSA, ECDSA, Diffie-Hellman)
    - RSA is commonly used for securing web connections
    - ECDSA is standard algorithm for blockchain signatures
    - "Sufficiently powerful" means about 3000-5000 logical qubits for RSA-2048
  - Prompted increased interest in quantum computers
- Grover's algorithm
  - Discovered in 1996 at Bell Laboratories
  - Provides quadratic speed-up for attacking symmetric cryptography and hash algorithms (used for authentication, including on blockchains)
- But there are good alternatives that avoid these threats

The Post-Quantum Cryptography Problem

FS Club

3 2 4

Large-scale quantum computers would pose ***a serious***

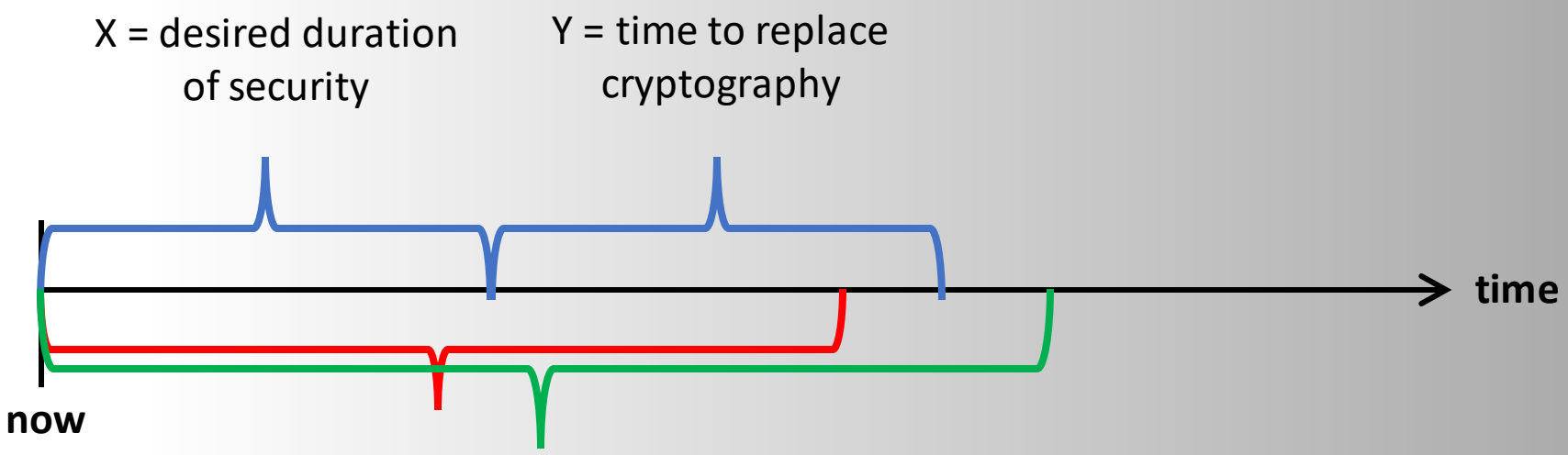
1

threat to the security of ***public key cryptography***

6 5

So ***what should affected entities do***, and ***when***?

Symmetric Cryptography



- For each system:
  - If X + Y < Z, there is time to act
  - If X + Y > Z, it may already be too late to entirely avoid the post-quantum cryptography problem
- Some systems may fall into the second category, especially where X is very large – e.g. blockchain / Smart Ledgers, life insurance, bonds

The Post-Quantum Cryptography Problem

FS Club

3 2 4

Large-scale quantum computers would pose ***a serious***

1

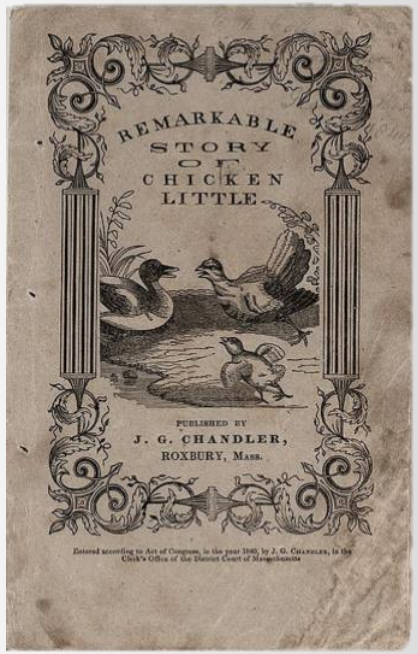
threat to the security of ***public key cryptography***

6 5

So ***what should affected entities do***, and ***when***?

Don’t Panic

- Is this like the Y2K problem? – but no certain deadline
- Maybe more like climate change? – uncertainty as to timing and impacts

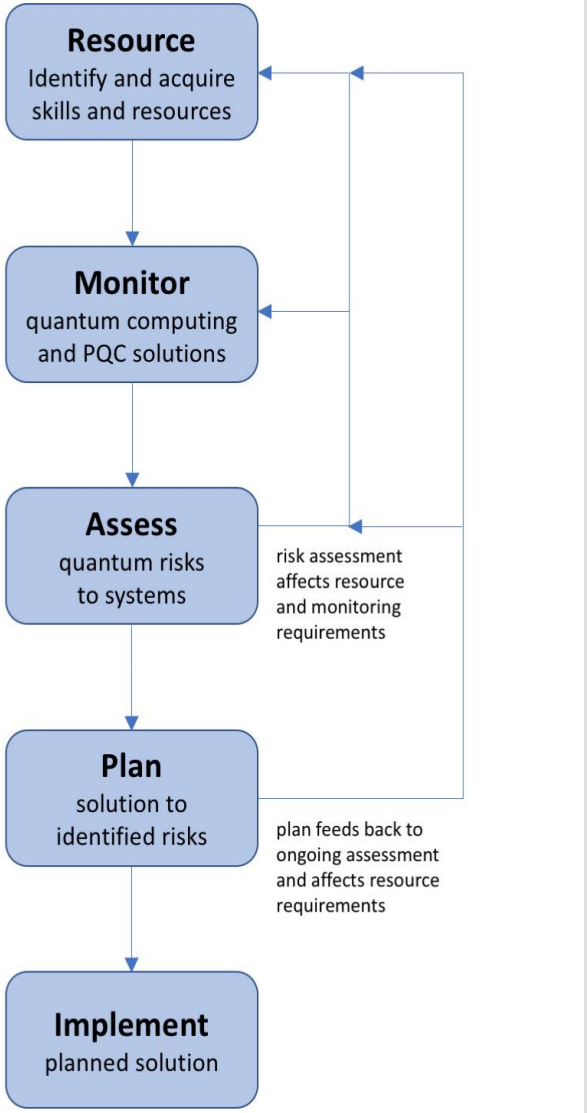


Symmetric Cryptography

FS Club

- EU PQCRYPTO recommendations (2015)
- US National Institute of Standards and Technology competition (launched 2016)
  - 69 Round 1 submissions in early 2018
  - Round 2 candidates announced Feb. 2019 – 17 public key confidentiality algorithms and 9 digital signature algorithms
  - Expected to conclude between 2022 - 2024
- Promising families of quantum-resistant algorithms
  - Lattice
  - Signature-based
  - Code-based
  - Multivariate
  - Supersingular elliptic curve isogeny

A Programme of Action



An obvious conclusion?

- New systems should be quantum resistant from the start, to avoid risks (and costs of re-engineering)
- But many new systems are not taking this approach, including because most familiar / off-the-shelf components are not quantum-resistant

Questions, Comments & Answer(s)?

FS Club

FS Club

Platinum Sponsors

Invest Northern Ireland
Red Hat
CDI China Development Institute
GIFT Gujarat International Finance Tec-City
Seoul Together we stand
LuxembourgforFinance Agency for the Development of the Financial Centre
Casablanca Finance City القطب المالي للدار البيضاء
BIFC Busan International Finance Center
GT
AIFC
Finance Montréal
Abu Dhabi Global Market
Dubai International Financial Centre

Gold Sponsors

PEERNOVA
Aptitude Software
BRIDGEWORKS
Feature Space
Outsmart Risk
Arboretum
Crown Agents Bank

Silver Sponsors

P2 Consulting
InfrasoftTech Fintech Digital Solutions
Bottomline
BCS Consulting Expect Excellence
PRAXITY Empowering Business Globally
Estates and Infrastructure Exchange
The Technium Global Service with Integrity

Bronze Sponsors

Profile Software
expleo
Contact Partners
alyne

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI Global Legal Entity Identifier Foundation
cuffassociates
GPS global processing services
The Transparency Task Force
CYGNETISE
Catalina Consulting
AMSOM
Gibraltar Stock Exchange
Volanté

Thank You

Forthcoming Webinars

22 June 2020 (15:30)	Accreditation – Facilitating Trade & Supporting UK plc: UKAS – The UK's Best-Kept Secret Weapon
23 June 2020 (09:00)	Financial Centres Of The World 2020: Focus On Tokyo
24 June 2020 (12:00)	How To Ensure All-Employee Share Plans Remain Relevant
25 June 2020 (12:00)	FSG Anti-Money Laundering (AML) Task Force – The Curious Case Of Money-Laundering Controls

Visit https://fsclub.zyen.com/events/webinars/

More added every day..