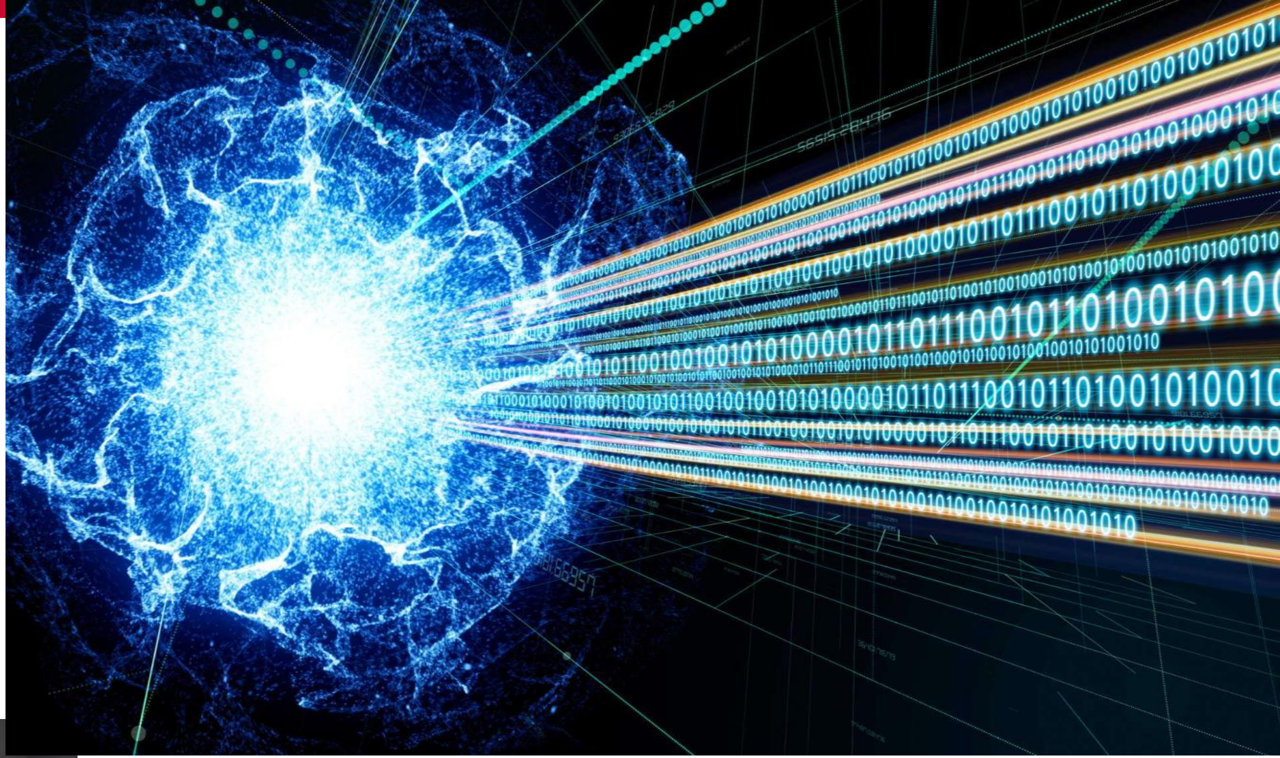
BROADCOM
MAINFRAME SOFTWARE

Quantum computing threats to cryptographic foundations

Jessica Doherty
Senior Manager, Broadcom

A new challenge is on the horizon…



Y2Q

Cryptography is Ubiquitous

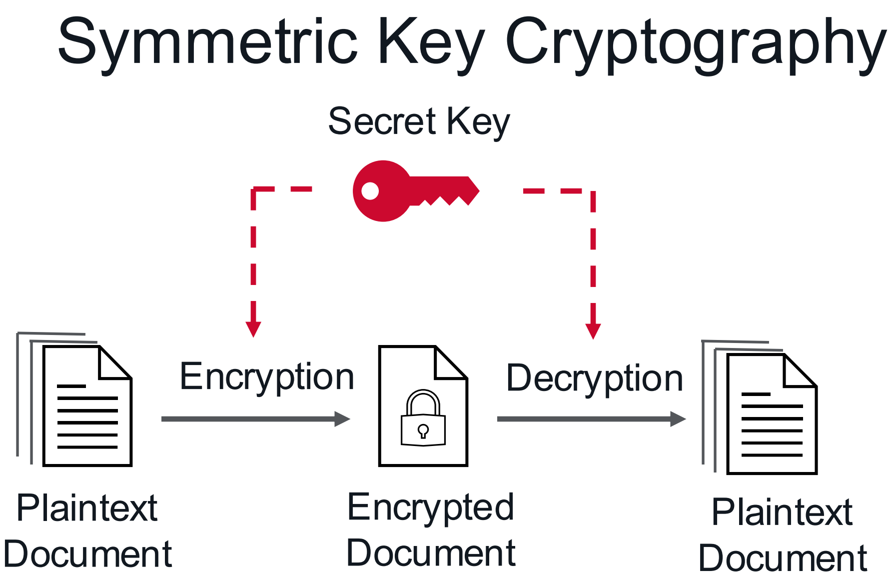
Basic Functions

- Data Confidentiality
- Data Integrity
- Authentication
- Non-Repudiation
- Digital Signatures

Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Cryptographic Hashing

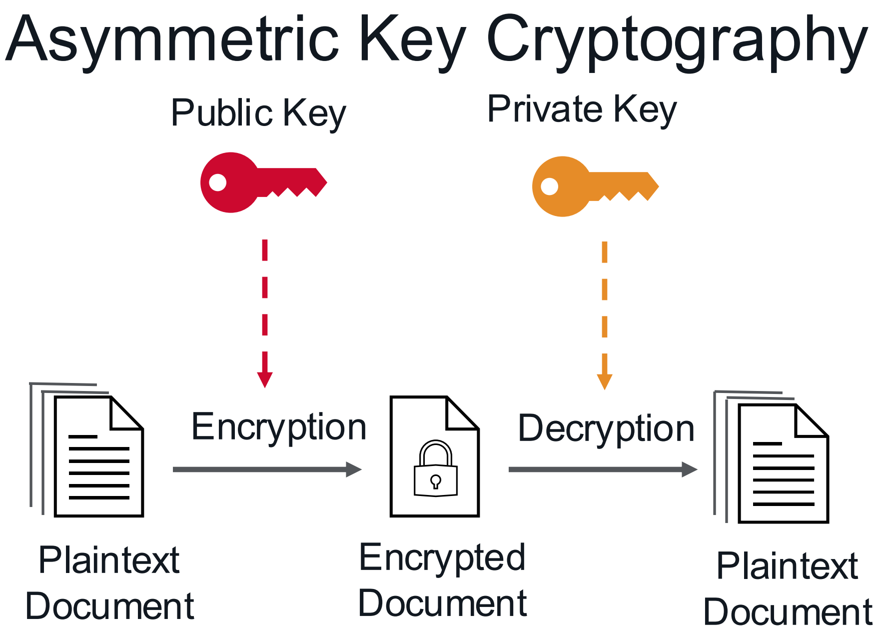
Symmetric Key Cryptography: Foundations & Use Cases



Example Use Cases

- Protection of data at-rest
- Protection of data in-flight
- Protection of card holder data
- Application encryption
- Password protection
- Message authentication

Asymmetric Key Cryptography: Foundations & Use Cases

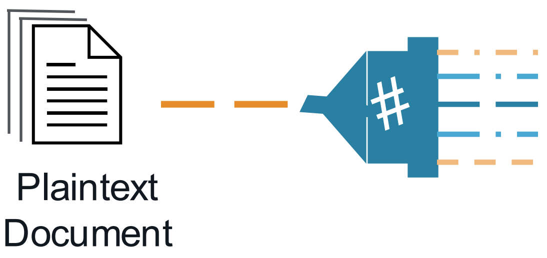


Example Use Cases

- Secure Network Communication
- Supply chain security
- Key Exchange/Management
- Secure email
- Online Banking
- Digital Currency
- Asset Tokenization
- Blockchain

Cryptographic Hashing: Foundations & Use Cases

Cryptographic Hashing



Example Use Cases

- Secure Network Communication
- Supply chain security
- Digital Signature generation and validation
- Code Validation

BROADCOM MAINFRAME SOFTWARE

What makes cryptography Secure?

Cryptography relies on complex mathematical problems that are:

- Computationally easy to solve in one direction (with the correct key)
- Computationally infeasible to solve in the other direction (without the correct key)

RSA Algorithm

Integer Factorization Problem

Elliptic Curve Algorithm

Elliptic-curve Discrete Logarithm Problem

AES Algorithm

Finding the correct key to decrypt data (without knowing the secret key)

Example: Classical Computer 2048-bit RSA

P

134326859429968865971237515160828015130176303529791700311990229884023894953454330209363238405326956563619122733992415186948198691772796005599898574682338226775537694019879689740450841380869996611857924558905560743662539607570832717254467614391977047515197914404269518189849812359398417061967386888270081363253

X

Q

142852786483485439440109784104559515049969955642910475099509825170174101898054824776053102694302138070502387418638774980058198599531468099447571980468008544514709616805793022873756221678206936193622137751154199130742454173113800452283115085480878077980038749003008078572106031985393484847905901056763881959123

=

N

19188966169146505057360226932044563428507247437672667082585537517664057655920442482178153371926802406978084823460532984561597405324257566704144336585809074732530729782200185918070252225524999644123449281672398466310803453742541083637291730588791181192993450086427041296434465684731503629903535709335495464469559358656507799294788357236337129881018599953094664584034724056918120466619750900791339514935628718075423464154976269070877321181744476214022917602869048917406697915942555970751249880972223427329830656247866362980066798002033743754545994238703037858291760069549211065889855733747256036412464755276312260307119

N

19188966169146505057360226932044563428507247437672667082585537517664057655920442482178153371926802406978084823460532984561597405324257566704144336585809074732530729782200185918070252225524999644123449281672398466310803453742541083637291730588791181192993450086427041296434465684731503629903535709335495464469559358656507799294788357236337129881018599953094664584034724056918120466619750900791339514935628718075423464154976269070877321181744476214022917602869048917406697915942555970751249880972223427329830656247866362980066798002033743754545994238703037858291760069549211065889855733747256036412464755276312260307119

=

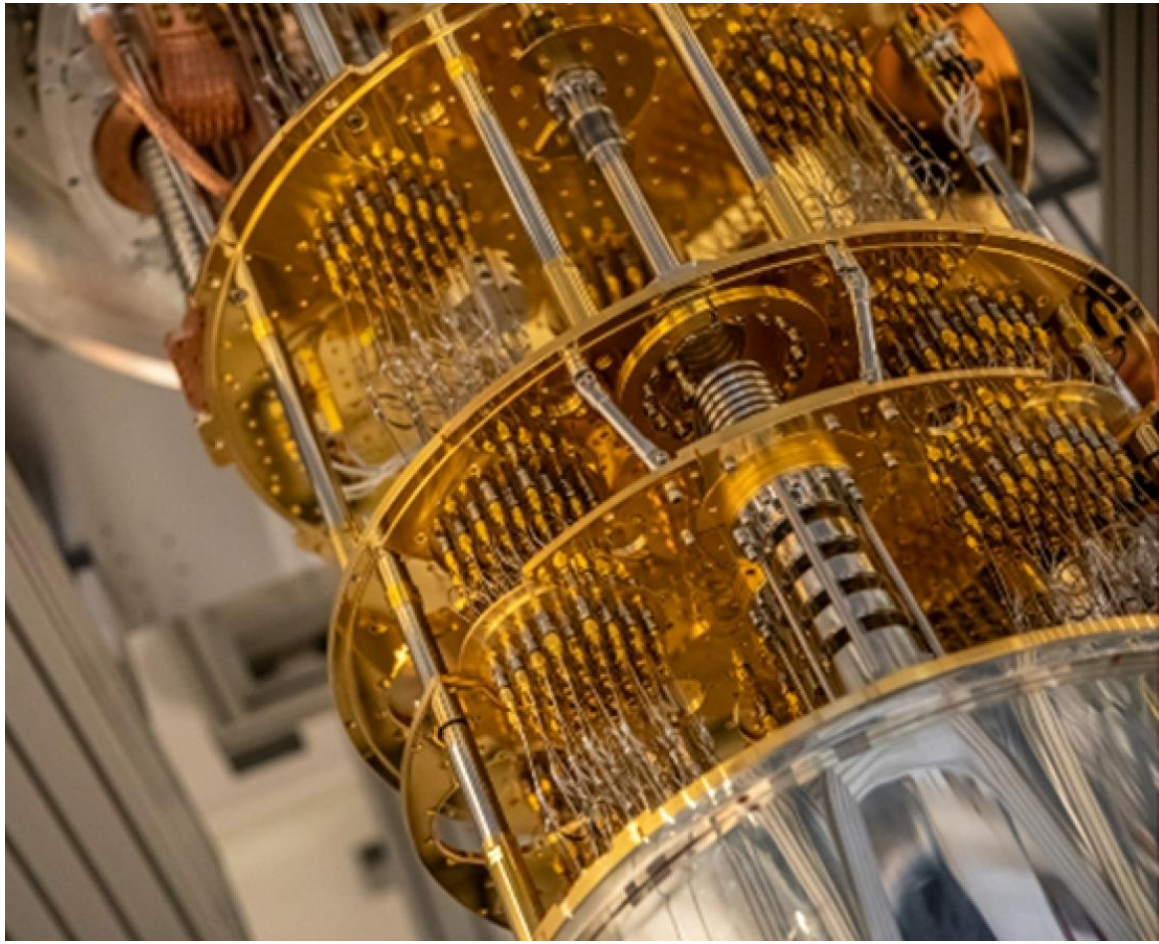
??? X ???

*It is estimated it would take a **classical computer** on the order of **BILLIONS** of years to solve this problem.*

BROADCOM
MAINFRAME SOFTWARE

How are quantum computers different?

- Only specific known algorithms run efficiently on classical binary computers
- Quantum computers represent a new paradigm of computation leveraging quantum mechanics
- Binary bits are replaced with quantum bits or qubits
- Quantum computers can use algorithms to solve problems once thought to be impossible
- *Like any new technology quantum computers can be used for good and bad...*



Shor’s Factoring Algorithm

- **Rock Star** of quantum algorithms
- Responsible for driving massive investment in quantum computing
- Can factor numbers exponentially faster than any know classical algorithm

BROADCOM MAINFRAME SOFTWARE

Example: Quantum Computer 2048-bit RSA

N

19188966169146505057360226932044563428507247437672667082585537517664057655920442482178153371926802406978084823460532984561597405324257566704144336585809074732530729782200185918070252225524999644123449281672398466310803453742541083637291730588791181192993450086427041296434465684731503629903535709335495464469559358656507799294788357236337129881018599953094664584034724056918120466619750900791339514935628718075423464154976269070877321181744476214022917602869048917406697915942555970751249880972223427329830656247866362980066798002033743754545994238703037858291760069549211065889855733747256036412464755276312260307119

=

P

134326859429968865971237515160828015130176303529791700311990229884023894953454330209363238405326956563619122733992415186948198691772796005599898574682338226775537694019879689740450841380869996611857924558905560743662539607570832717254467614391977047515197914404269518189849812359398417061967386888270081363253

X

Q

142852786483485439440109784104559515049969955642910475099509825170174101898054824776053102694302138070502387418638774980058198599531468099447571980468008544514709616805793022873756221678206936193622137751154199130742454173113800452283115085480878077980038749003008078572106031985393484847905901056763881959123

Applying Shor's algorithm using a quantum computer with ~20,000 logical qubits (~2M physical qubits) can solve this problem in
8 HOURS!!!

When should organizations begin Preparing?

Two Factors to Consider:

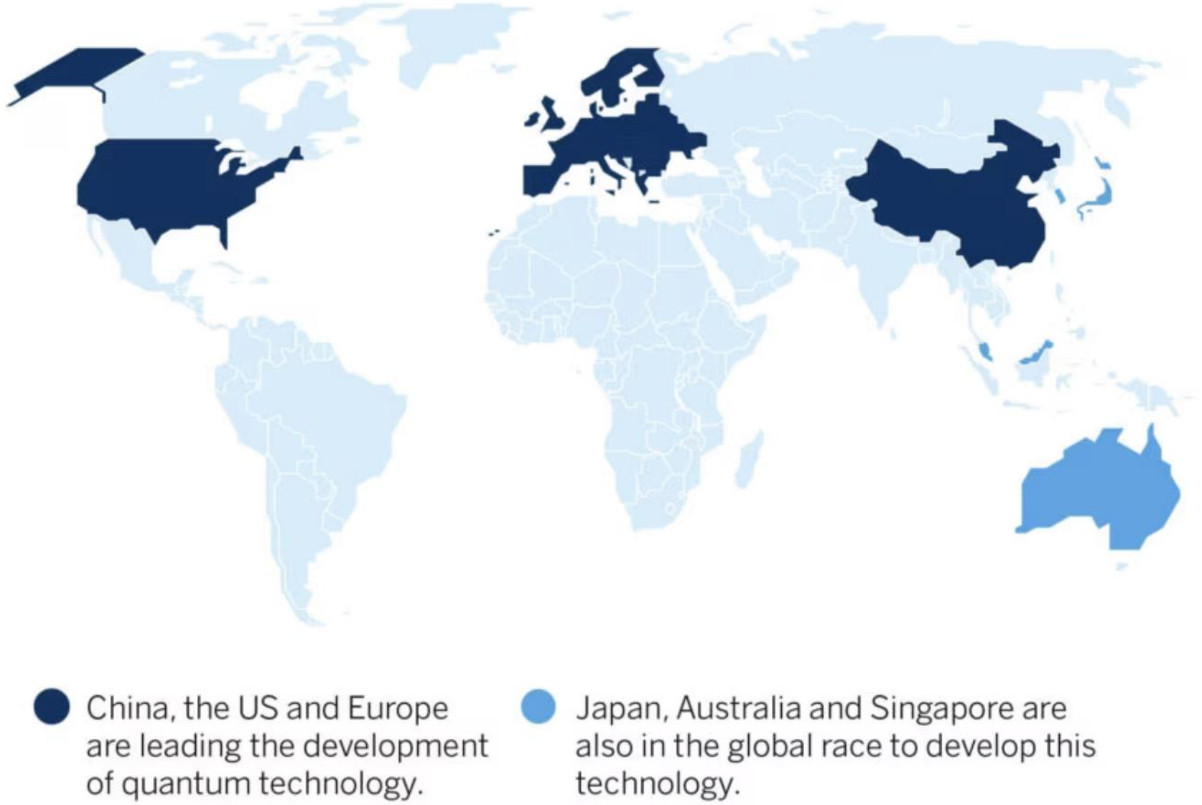
- Availability of Cryptographically Relevant Quantum Computer
  - IBM’s Quantum System II is the most powerful quantum computer today with 3 – 156 qubit processors (468 qubits) – Roadmap to get to 1000s of logical qubits 2033+ [1]
  - "*I have estimated a one in seven chances that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026 and a 50% chance by 2031.*"
    Dr. Michele Mosca, an expert from the University of Waterloo [2]
- *Harvest Now Decrypt Later*
  - *Immediate concern!*

Y2Q

1: https://newsroom.ibm.com/2025-06-23-ibm-and-riken-unveil-first-ibm-quantum-system-two-outside-of-the-u-s
2: https://www.isaca.org/resources/news-and-trends/industry-news/2024/embracing-the-future-the-quantum-computing-revolution-begins-now

Quantum Computing Global Investment

- Global investment is estimated at $55B[1]
- China leads public funding investment with over $15B[2]
- China views quantum technology as pivotal
- China leads in quantum communication
- US leads in quantum computing and quantum sensing
- EU countries are leaders in quantum research



1: https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/
2: https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

BROADCOM MAINFRAME SOFTWARE

What is the industry doing?

- Global effort - countries with national quantum strategies:
  - Australia, Canada, China, Denmark, France, Germany, Japan, India, Russia, South Korea, Netherlands, UK, and USA.
- August 2024 NIST published its first set of algorithms designed to withstand the attack of a quantum computer:
  - FIPS 203 – ML-KEM – (AKA Crystals Kyber)
  - FIPS 204 – ML-DSA – (AKA Crystals Dilithium)
  - FIPS 205 – SLH-DSA – (AKA SPHINCS+)
- NIST plans to standardize additional PQC algorithms
- February 2025 IETF published draft recommendations for hybrid key exchange and composite authentication for TLS-based applications

What can/should enterprises be doing now?

Discover and identify cryptographic usage	Applications, software, hardware, etc
Build a crypto inventory	Crypto Usage and Key Material
Create a plan for transitioning to post quantum crypto	
Address technical debt	Replace outdated algorithms |(e.g. DES, TDES), Begin migration to TLS 1.3

Learn More and Continue the Conversation

Post Quantum Crypto Resources:

- NIST PQC https://csrc.nist.gov/projects/post-quantum-cryptography
- NIST NCCoE: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
- Open Quantum Safe (OQS): https://openquantumsafe.org
  - Liboqs: https://github.com/open-quantum-safe/liboqs
- NCSC: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
- CISA https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
- BSI: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html =

Speakers:

- Jessica.Doherty@Broadcom.com

BROADCOM
MAINFRAME SOFTWARE

Thank You