The Impact of Quantum Technology on Cybersecurity

RVAsec

June 2023

Qrypt

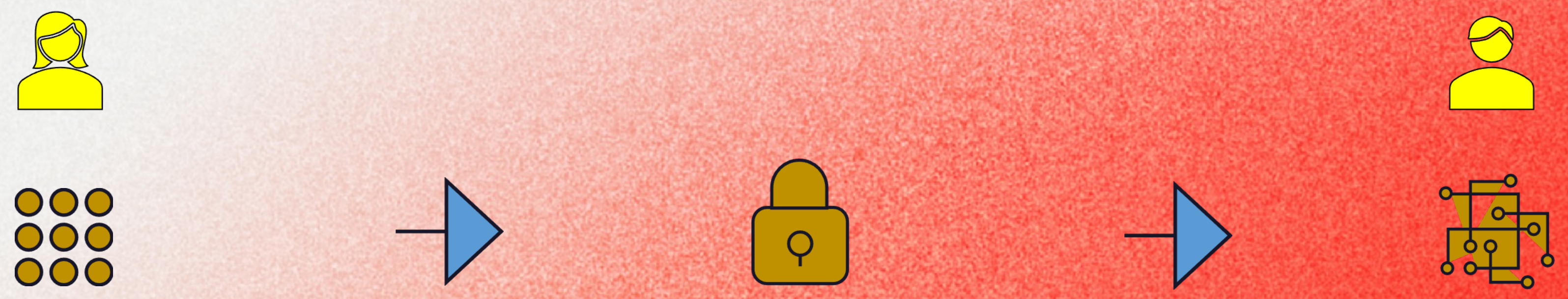
Denis Mandich

CTO and Co-founder of Qrypt
Founding member of the Quantum Economic Development Consortium (QED-C)
Industry Advisory Board – Center for Quantum Technology
Founding member of the Mid-Atlantic Quantum Alliance (MQA)
ANSI Accredited Standards Committee X9
ITU Telecommunications Standardization Sector (ITU-T)
Forbes Technology Council
Former Quside board member
20-year USIC veteran
Physicist

Qrypt

Cryptography Basics

- Cryptography is the use of codes to secure communications over an insecure medium
- Must provide **Secrecy** and **Authenticity** even when the adversary controls the channel
- Security proofs depend on the secrecy of a randomly generated key which may be shorter or longer than the message.



Brief History of Cryptography – “How we got here”

- Caesar cipher, Vernam, 1970s to today
- Asymmetric/Symmetric
- Information theoretic secure/computationally theoretic secure
- Quantum-safe/quantum-secure difference
- Suite A/Suite B/CNSA
- No *“security through obscurity”* – publish everything

Suite A

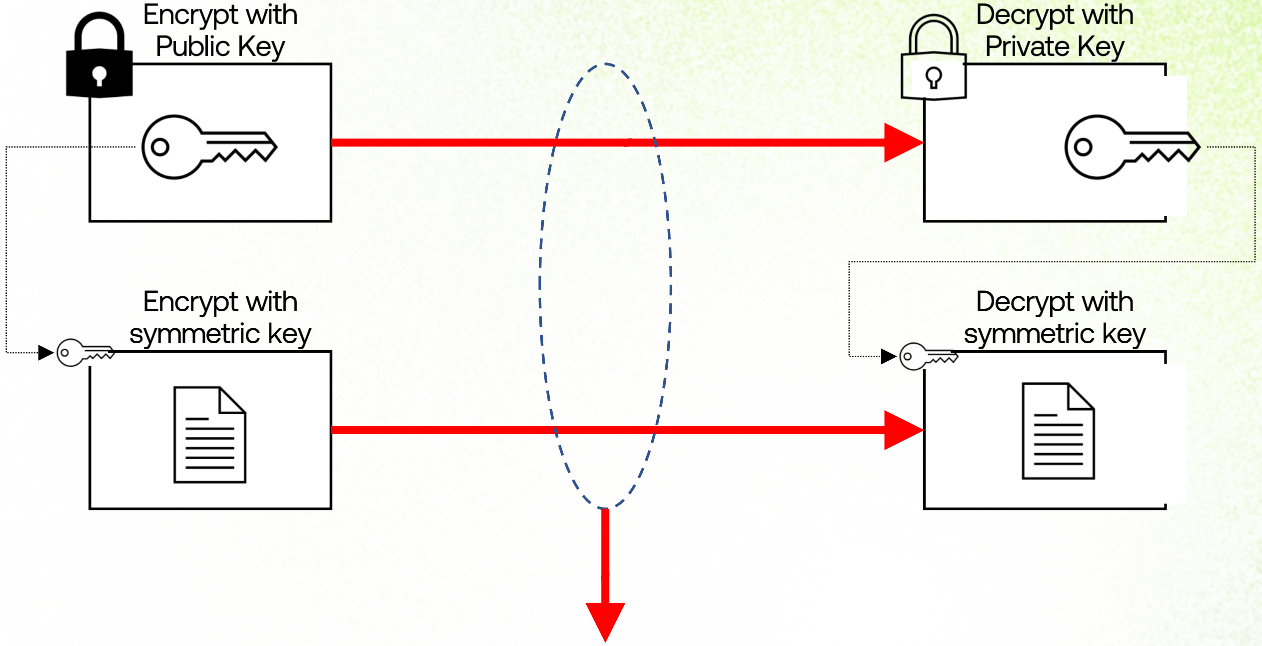
Suite B

Qrypt

Public-Private key pairs are used to exchange symmetric keys to both encrypt and decrypt data:

1. Transmit keys

2. Transmit data

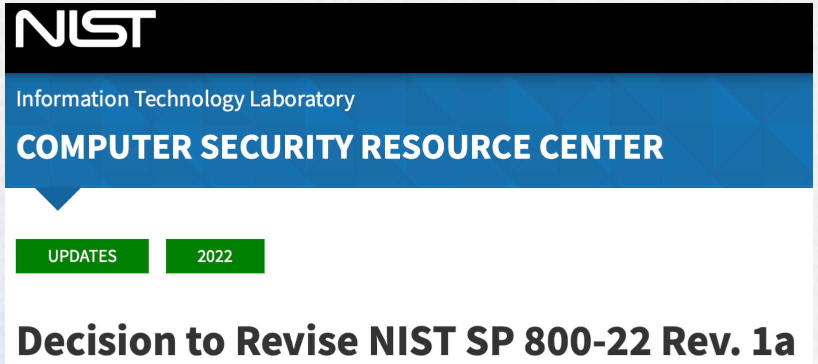


Quantum computers will be able to decrypt key transmission, which makes encrypted data accessible.

Qrypt

Public Key Infrastructure, E2E

- The internet is fragile as are all apps for banking, privacy, health records, govt, etc
- PKI was never completed and continues to grow in complexity and management challenges
- Zoom, Yubikey examples; FedRamp, FIPs certifications

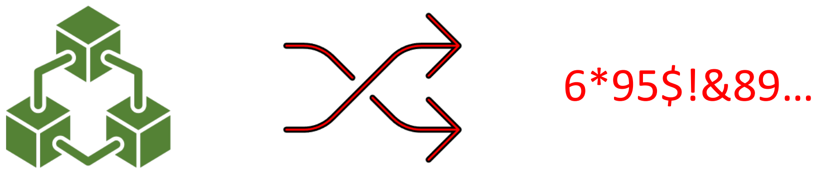


...rejecting its use for assessing cryptographic random number generators

Qrypt

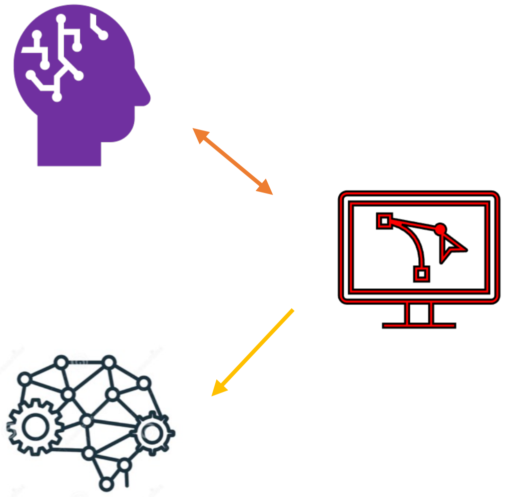
Where is encryption used?

- Bank transactions, ATMs, https, e-commerce, PCI
- Cryptocurrency, digital wallets and assets
- Cloud infrastructure, virtual networks
- Ubiquitous, always-on systems and sensor networks



Where are the greatest threats?

- Integrity of automated and interconnected systems
- Trust in the financial industry and data exchanges
- Security of deposits, trading strategies, M&A
- Risk to operational AI and ML infrastructure



Qrypt

Persistence of classical vulnerabilities

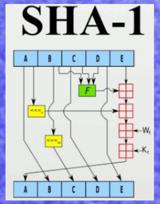
SIKE – NIST PQC Finalist

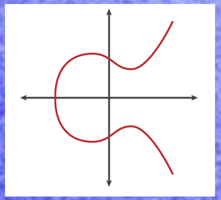
- Broken by a 2010 desktop computer with a Xeon processor
- What if this wasn't discovered for 5-10 years after implementation?

Intel SGX enclaves – the encryption keys to the kingdom

- Cornerstone of a trusted execution environment, even when the operating system is compromised
- Multiple types of flaws discovered over four years, new CacheOut attack

SHA-1, Dual_EC_DRBG, Heartbleed, Spectre, Meltdown, PacMan…

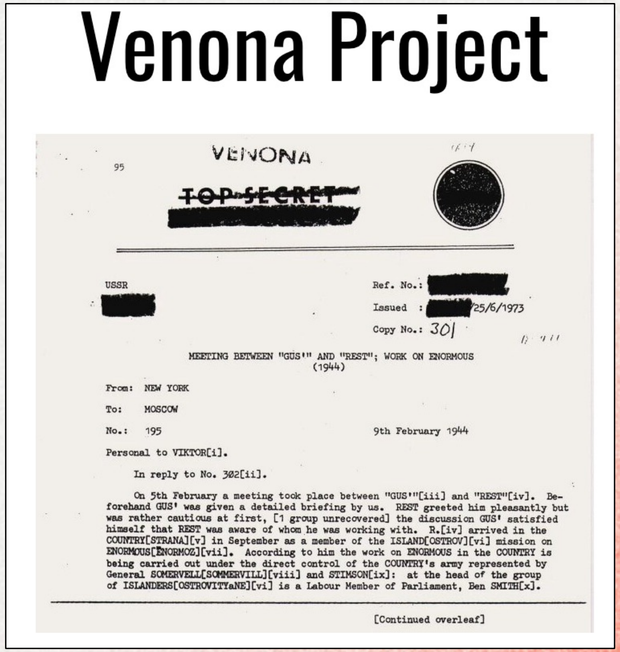





Qrypt

“Harvest now, decrypt later”

- **Venona** project, China today, low/no cost for storing, high potential benefit
- Real world examples, Rosenbergs, IoT
- Change in data theft priorities, targeting strongly encrypted data



Venona Project

VENONA

95

TOP SECRET

[redacted]

USSR

[redacted]

Ref. No.: [redacted]

Issued : [redacted]/25/6/1973

Copy No.: 301

MEETING BETWEEN "GUS'" AND "REST"; WORK ON ENORMOUS (1944)

From: NEW YORK

To: MOSCOW

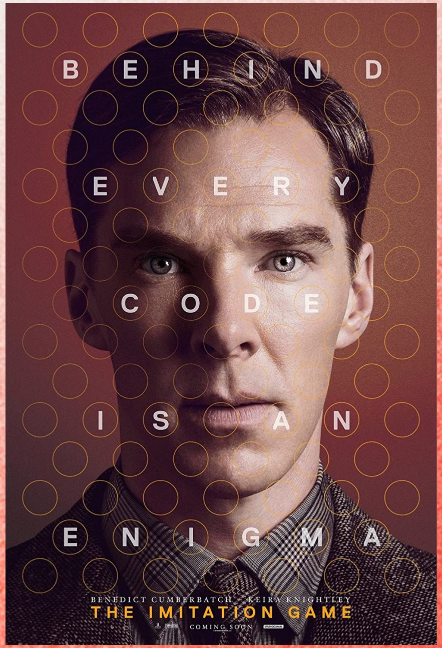
No.: 195 9th February 1944

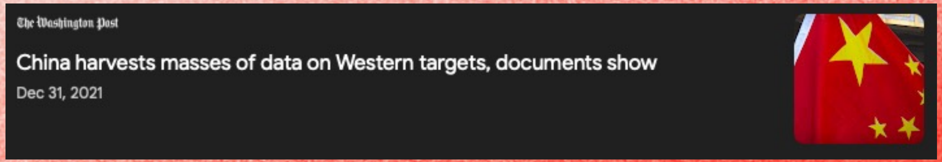
Personal to VIKTOR[i].

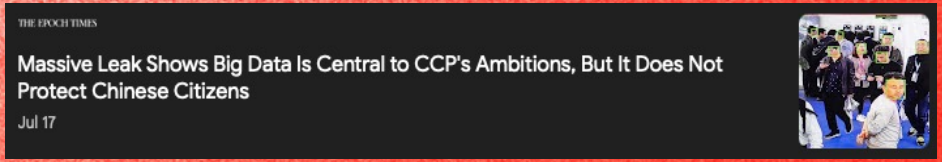
In reply to No. 302[ii].

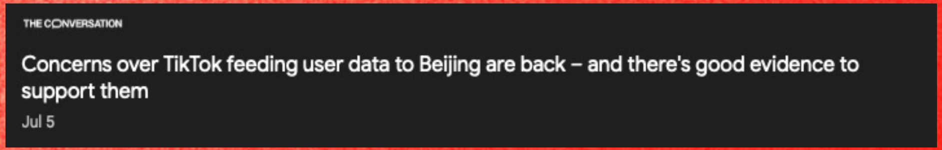
On 5th February a meeting took place between "GUS'"[iii] and "REST"[iv]. Beforehand GUS' was given a detailed briefing by us. REST greeted him pleasantly but was rather cautious at first, [1 group unrecovered] the discussion GUS' satisfied himself that REST was aware of whom he was working with. R.[iv] arrived in the COUNTRY[STRANA][v] in September as a member of the ISLAND[OSTROV][vi] mission on ENORMOUS[ENORMOZ][vii]. According to him the work on ENORMOUS in the COUNTRY is being carried out under the direct control of the COUNTRY's army represented by General SOMERVELL[SOMMERVILL][viii] and STIMSON[ix]: at the head of the group of ISLANDERS[OSTROVITYaNE][vi] is a Labour Member of Parliament, Ben SMITH[x].

[Continued overleaf]









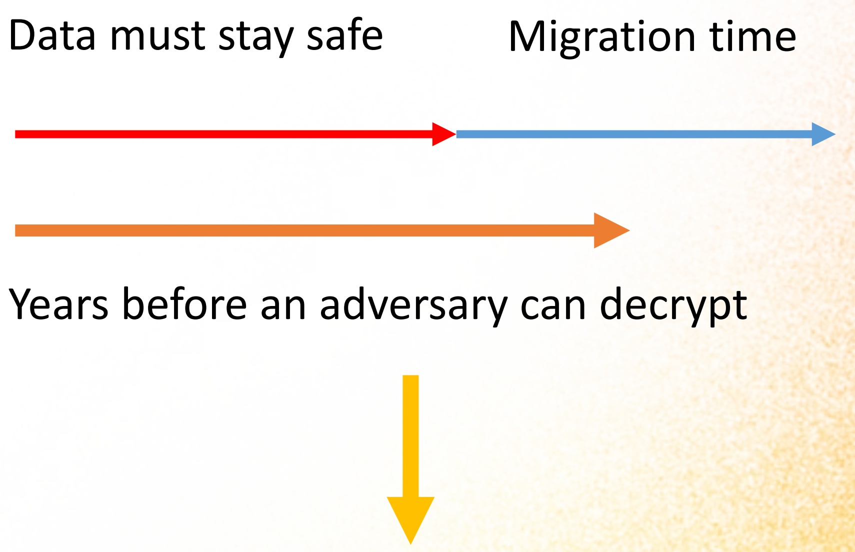
Qrypt

When quantum is here, it will be too late. Your data is ready for decryption.

Harvest Now, Decrypt Later means adversaries are storing your encrypted data *today*.

Waiting for NIST PQC algorithms isn't enough.

- All of today's stolen data can be decrypted when **Y2Q** hits
- If/when future PQC algorithms fail, that data will also be vulnerable

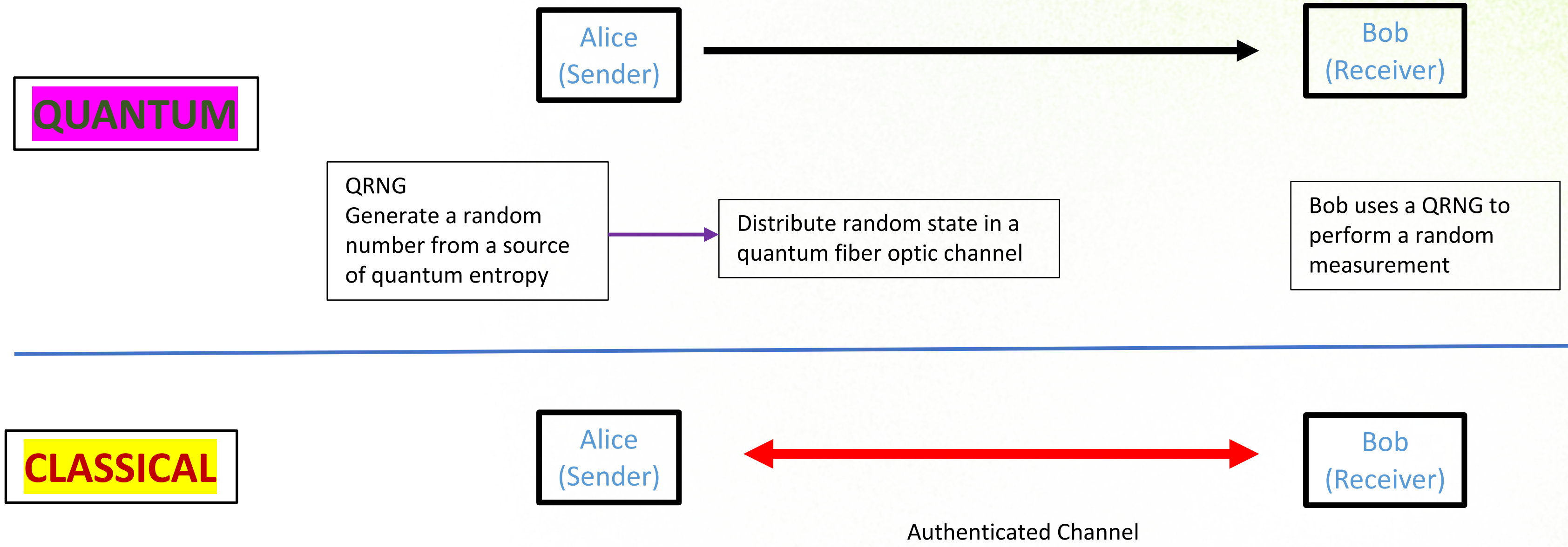


We have today problem.

Qrypt

What makes cryptography quantum?

- Keys must be generated from a source of quantum **entropy**, <u>not</u> electronic noise
- Identical quantum keys must reach multiple endpoints to be useful
- SneakerNet, DI-QKD, BB84, E91 – all rely on inescapable classical assumptions
- **NSA** affirmed <u>rejection</u> of **QKD**:



Alice and Bob each have a random number, but they don't **MATCH**!

Alice and Bob use the <u>internet</u> to agree on which numbers can be used as secret keys

**Still uses classical information so what was gained by sacrificing redundancy?*

Qrypt

The core issues with QKD and variants:

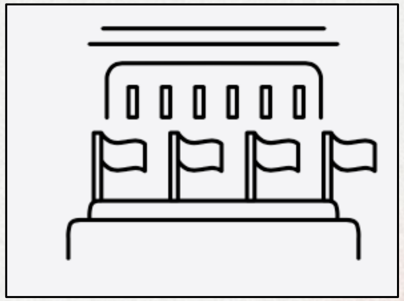
- Trusted node network until we have reliable and scalable quantum repeaters and quantum memory
- Expensive physics appliances at the endpoints – still need to get keys to clients (iPhones, laptops, etc)
- Centralized point of attack and failure for denial-of-service, accidents (shovels and backhoes!)
- Requires authenticated classical channels so what's the point? Just use PQC instead?
- NSA repeatedly stated their position: **"It's a HARD NO!"**

The "must-haves" in quantum cryptography to make it commercially viable and deployable:
- QRNGs to make random numbers/states [SOLVED]
- Redundancy and decentralization – must be resilient, no single point of failure
- Leverage existing massive global communications infrastructure (not physical security)
- Accessible by any classical device endpoint, *not just datacenter-datacenter*

Qrypt

What is the best solution?

- Pre-shared key, OTPs, quantum keys, send data in the clear with no risk
- Random number generator stations example during the cold war
- Embassies communication over adversarial controlled comms



The spooky world of the 'numbers stations'

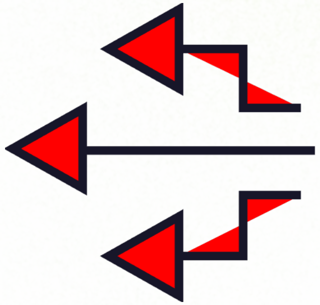
By Olivia Sorrel-Dejerine
BBC News Magazine

16 April 2014

THINKSTOCK

What if we didn’t distribute keys?

- Simultaneously generate them at the endpoints
- **HNDL** issue is eliminated
- Cryptographic channel, not the same as the data channel - **decoupling**
- Cloud-enabled, simplified implementation on modern infrastructure

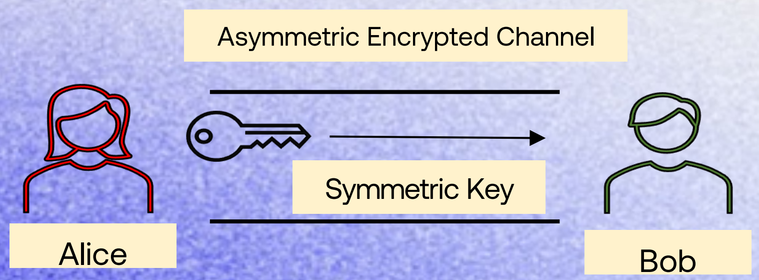


Qrypt

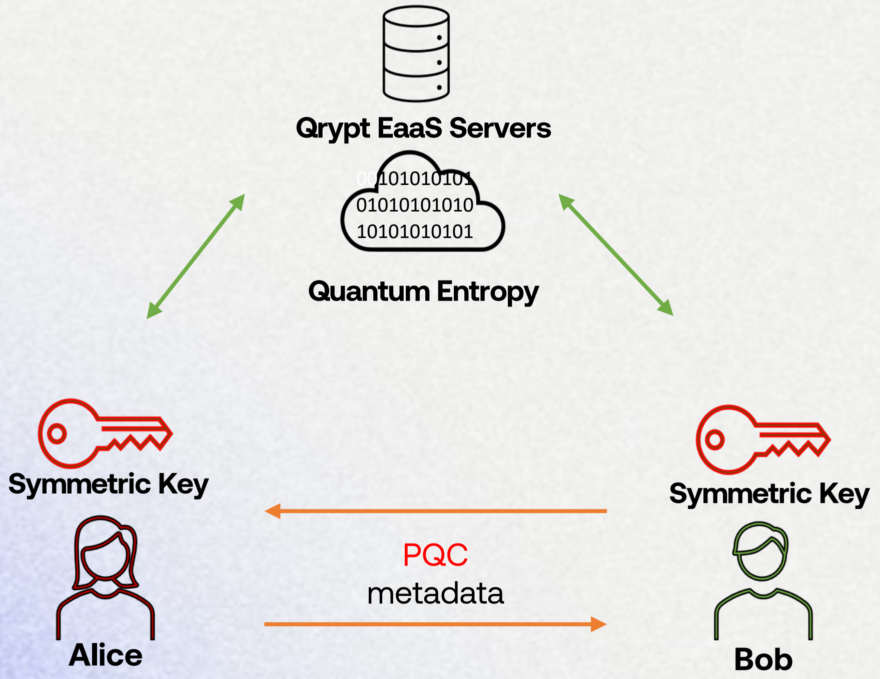
A quantum solution

- Cryptographic extractors, metadata and sample implementation
- The cloud service nor the app should be capable of recovering the keys
- PQC is not used to exchange keys
- Benefits/cost

Traditional Distribution of Symmetric Keys



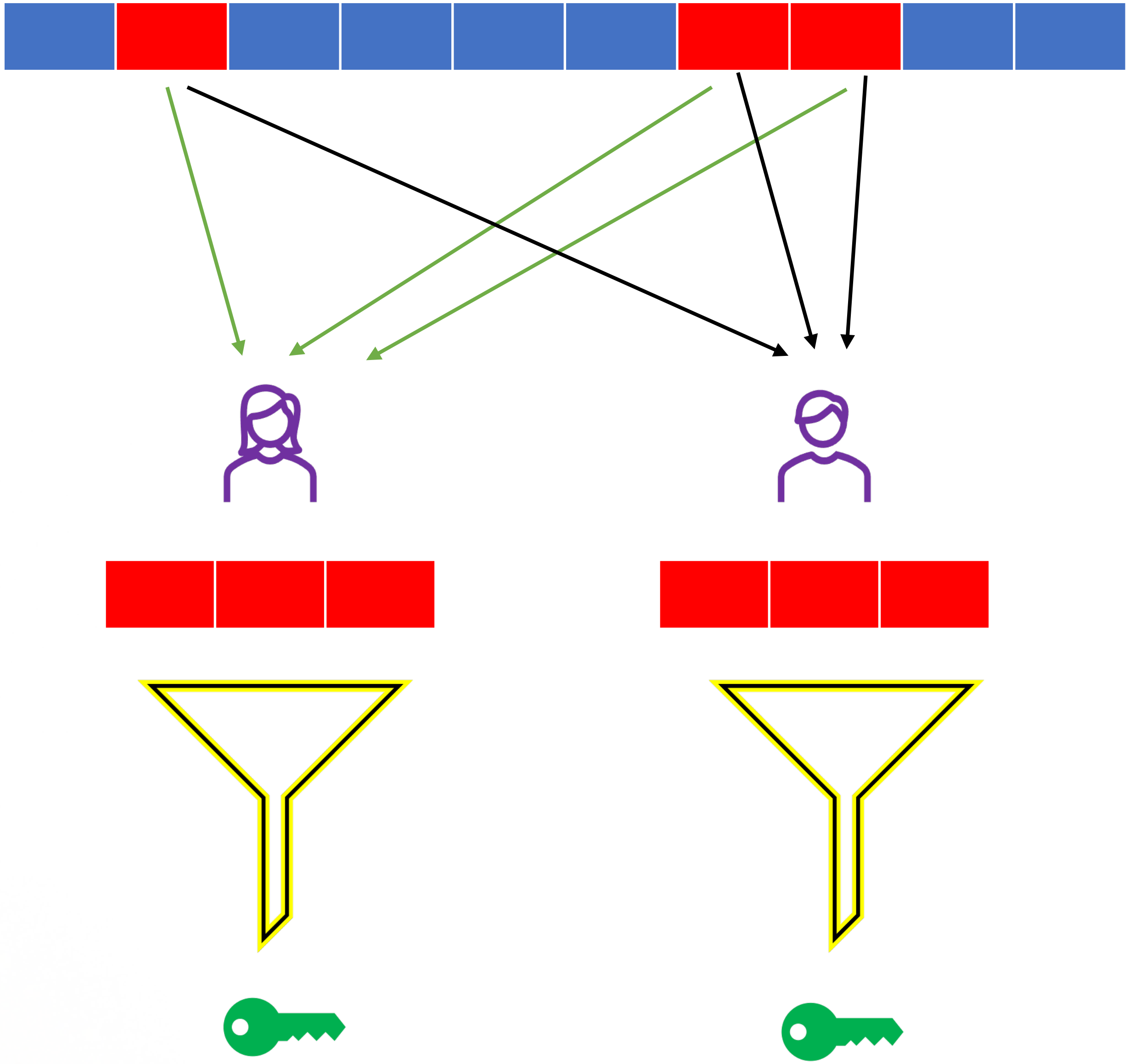
An observer can harvest now and decrypt later if the channel is monitored.



Keys are never distributed.

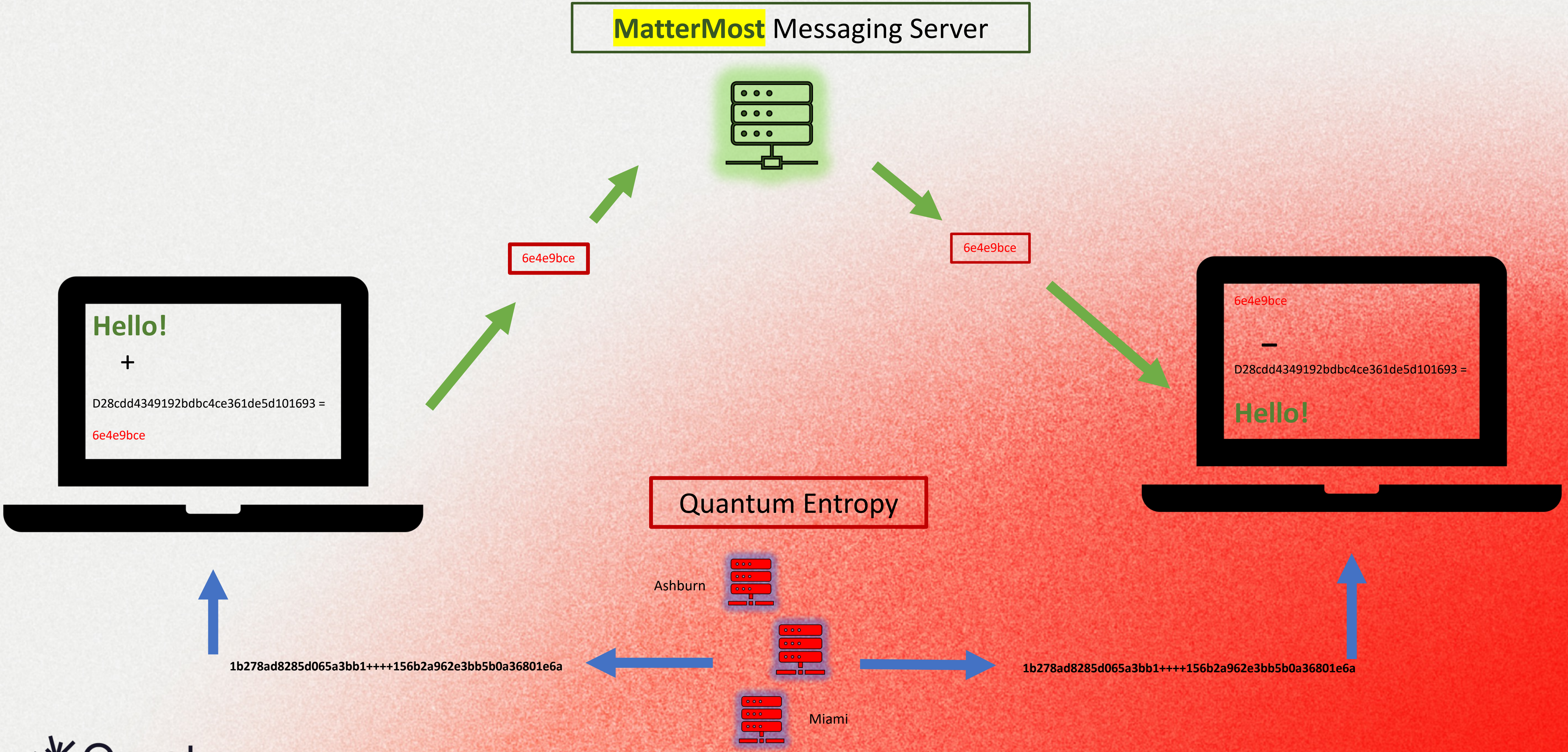
Sample then Extract

- Stateless and locally computable
- Preserve quantum entropy
- Force the attacker to compromise decoupled systems, but get nothing
- Compatible with PQC, but provides additional protections in a **crypto-agile** world even when new algorithms are compromised



Qrypt

Quantum security for any application – MatterMost



Qrypt

No free lunches

- If an attacker is on the endpoint/client, no encryption can help
- Compatible with PQC, but provides additional protections in a "crypto-agile" world
- "Trust no one" or leave vulnerabilities
- *USG key escrow and backdoors never work*

✳Qrypt

NIST process for PQC algorithm standardization

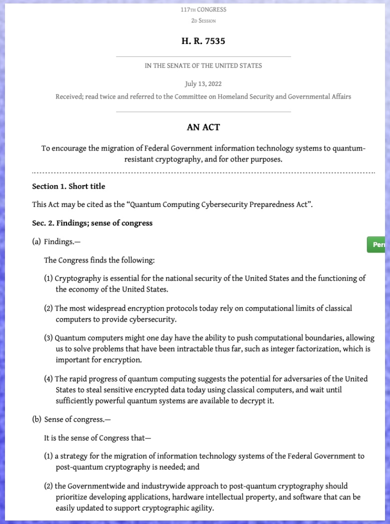
- Remaining candidates for 2024, possible issue with signatures, request for new submissions
- Assume another transition is coming, SIKE has fallen, potential weakness found in Kyber
- MFA analogy and trajectory

Public Key/KEMs	**Digital Signatures**
Finalists for standardization	
Kyber	Dilithium Falcon SPHINCS+
4th round in reserve	
BIKE HQC McEliece ~~SIKE~~	*????? Nothing yet!!!*

Qrypt

USG Directives, government is leading the way

- NSMs, EOs, HR, Senate, near full bipartisan support
- Message is clear: industries doing govt business must implement PQC
- National Security implications and changes to data governance



117th CONGRESS
2d Session

H. R. 7535

IN THE SENATE OF THE UNITED STATES

July 13, 2022

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.

Section 1. Short title

This Act may be cited as the "Quantum Computing Cybersecurity Preparedness Act".

Sec. 2. Findings; sense of congress

(a) Findings.—

The Congress finds the following:

(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

(b) Sense of congress.—

It is the sense of Congress that—

(1) a strategy for the migration of information technology systems of the Federal Government to post-quantum cryptography is needed; and

(2) the Governmentwide and industrywide approach to post-quantum cryptography should prioritize developing applications, hardware intellectual property, and software that can be easily updated to support cryptographic agility.

Executive Order 14073 National Quantum Initiative Advisory Committee (4 May 2022)
2022-10076.pdf (govinfo.gov)

NSM-8 NATIONAL SECURITY MEMORANDUM (4 May 2022)
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House

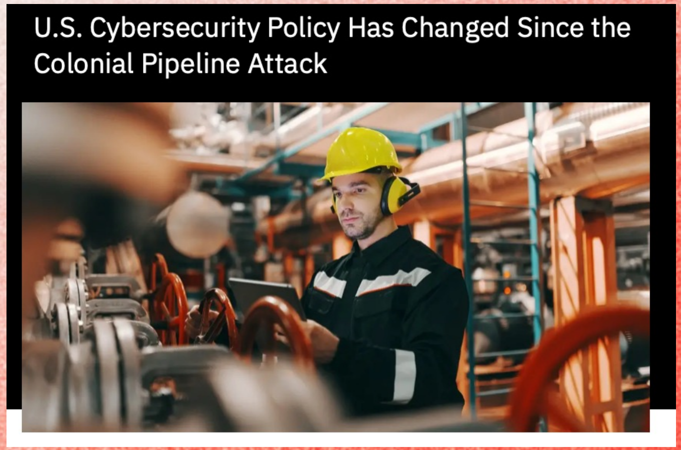
HR 7535 Quantum Computing Cybersecurity Preparedness Act (18 April 2022)
Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress

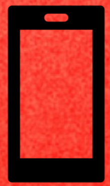
Executive Order 14028 (12 May 2021) Improving the Nation's Cybersecurity
Executive Order on Improving the Nation's Cybersecurity | The White House
Executive Order 14028: Improving the Nation's Cybersecurity | GSA

National Quantum Initiative (NQI) (21 December 2018)
About the National Quantum Initiative - National Quantum Initiative

This will be a long process, decades of insecurity

- PQC is not a permanent fix, especially for long lived devices (SCADA, vehicles)
- QKD is unsuitable for the vast majority of applications
- Always on internet, 5G, IoT, all have new requirements
- Design considerations and project planning





"If all of mathematics disappeared, physics would be set back by exactly one week."– Richard Feynman

Thank you.

denis@qrypt.com

Qrypt