Cybersecurity Today and Tomorrow:

Assurance or Insurance?

Apostol Vassilev, Ph.D.
Research Lead - STVM, CSD, NIST

(HOST 2016, May 3-5, The Ritz-Carlton, McLean, VA)

A look at the challenges today

- **Key facts in the Verizon 2016 Report**

most attacks exploited known vulnerabilities where a patch has been available for months, often years.

no one is immune

most breaches are about money

main reason - 58% of business don't have "mature" patch management processes

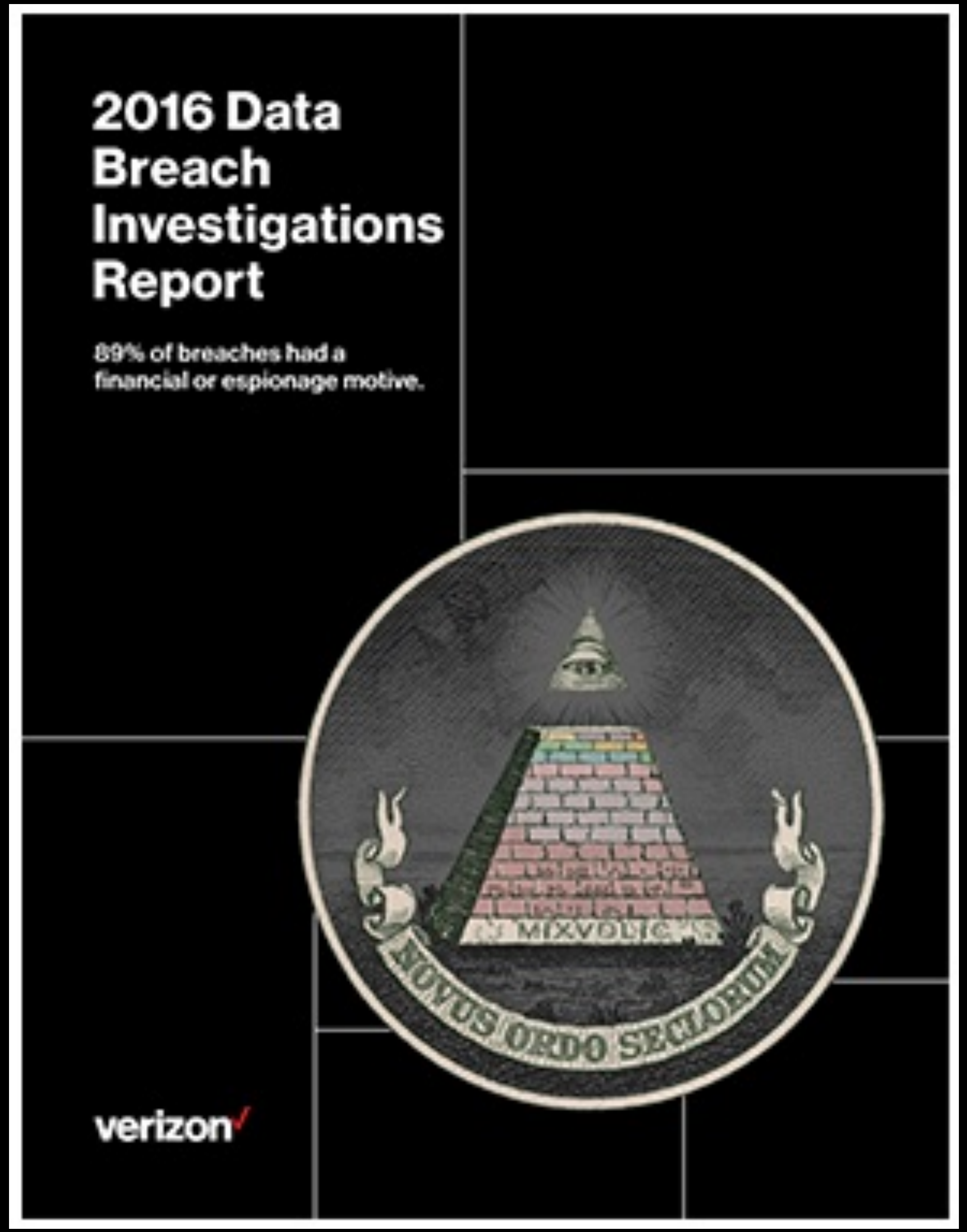


Image Courtesy: verizonenterprise.com/verizon-insights-lab/dbir/2016/

The root cause

- The economy of cybersecurity slow to emerge

a market failure in cybersecurity
www.economist.com/sites/default/files/20140712_cyber-security.pdf

<u>main reason</u> - the way computer code is produced

Cryptography is not immune

- Cryptography is fundamental for cybersecurity
    - by far the dominant means for protecting data in transit and at rest

- Susceptible to issues plaguing general computer code

- … but there are special areas of concerns, especially when implemented in hardware

The case of modern crypto

Courtesy of XKCD, https://en.wikipedia.org/wiki/Xkcd

- **The algorithms are well-known:**
  - **e.g., RSA, AES**

- **Security depends largely on the black box principle:**
  - **e.g., secrecy of keys and internal state**

  - must be (nearly) impossible to guess

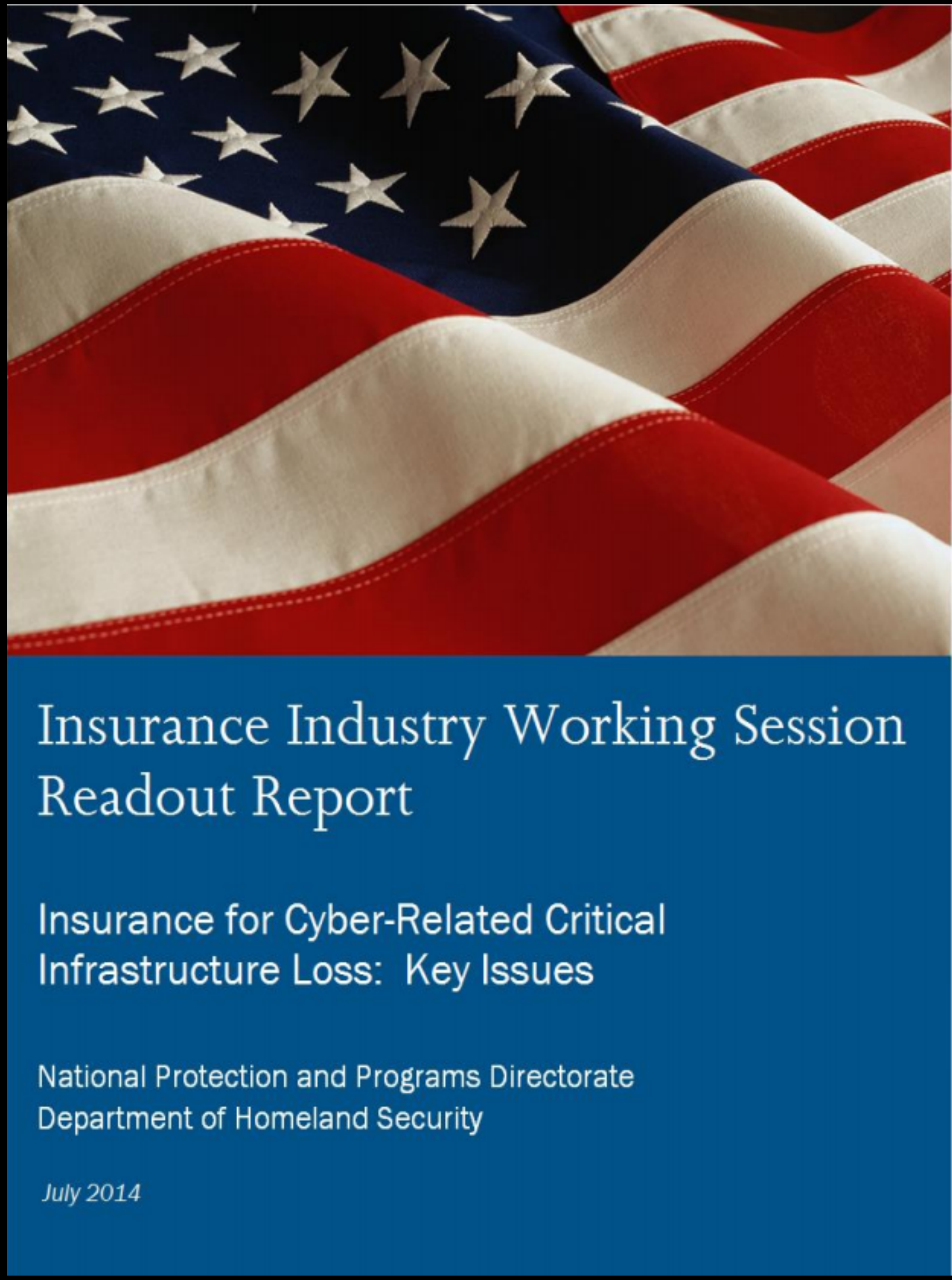
- Side-channel leakage is very problematic for H/W
  - due to inherent properties of algorithms

  - <u>undermines the assurances</u> from crypto

The insurance case

- The cybersecurity insurance market is a nascent one

  - Carriers cited several reasons for this:
    - a lack of actuarial data;
    - aggregation concerns;
    - the unknowable nature of all potential cyber threat vectors.



www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf

Assurance or Insurance today?

Courtesy of Wikipedia

Odysseus facing the choice between Scylla and Charybdis

A useful example

- **Automotive industry experience**

    - **turning car safety into a competitive advantage**

        the Volvo effect

Ad, 1973

An approach for getting strong assurances from cryptography

- Develop modern standards for cryptography and security
- Provide powerful incentives to the industry to adopt them
- Improve conformance testing to guarantee assurances

Traditional Conformance Testing

Example: FIPS 140-2

Intended to improve the security and technical quality of cryptographic modules employed by Federal agencies (U.S. and Canada) and industry by

- leveraging accredited independent third-party testing laboratories

Issues w/ Laboratory Testing

- **Labs burdened with labor-intensive and ineffective test methodology**
  - **having trouble testing in depth, w.r.t. state-of-the-art in security testing**
  - **rely on the English essay model for reporting test results**

- **Labs' competency in challenging technical areas**
  - **entropy & physical security testing**
    competency unevenly distributed among labs

- **Labs' business conflicts of interest**
  - **operate w/ own revenue and profit targets**
  - **enter in paid contracts w/ industry clients**

The metamorphosis effect

Module validated <u>without</u> a single implementation change

Test report review uncovers <u>significant</u> discrepancies

documentation-only metamorphosis

A systemic problem casting doubts on security assurances due to lack in trust in laboratory testing

Automate as much as possible


C. Chaplin, “Modern times”, 1936

- Reduce the validation cycle length;
- Enable Just-In-Time validations;
- Reduce the validation costs;
- Introduce a three-tier assurance model with trusted vendors;
- Refocus laboratories on testing beyond what is already tested by industry vendors.

Powerful economic incentives for the industry

Research and Innovation

- **Help the industry meet difficult security requirements through technology innovation**
  - Entropy as a Service (EaaS)
  - Advanced physical security
  - IoT security

  - Working w/ leading academic institutions

    University of Florida & FICS

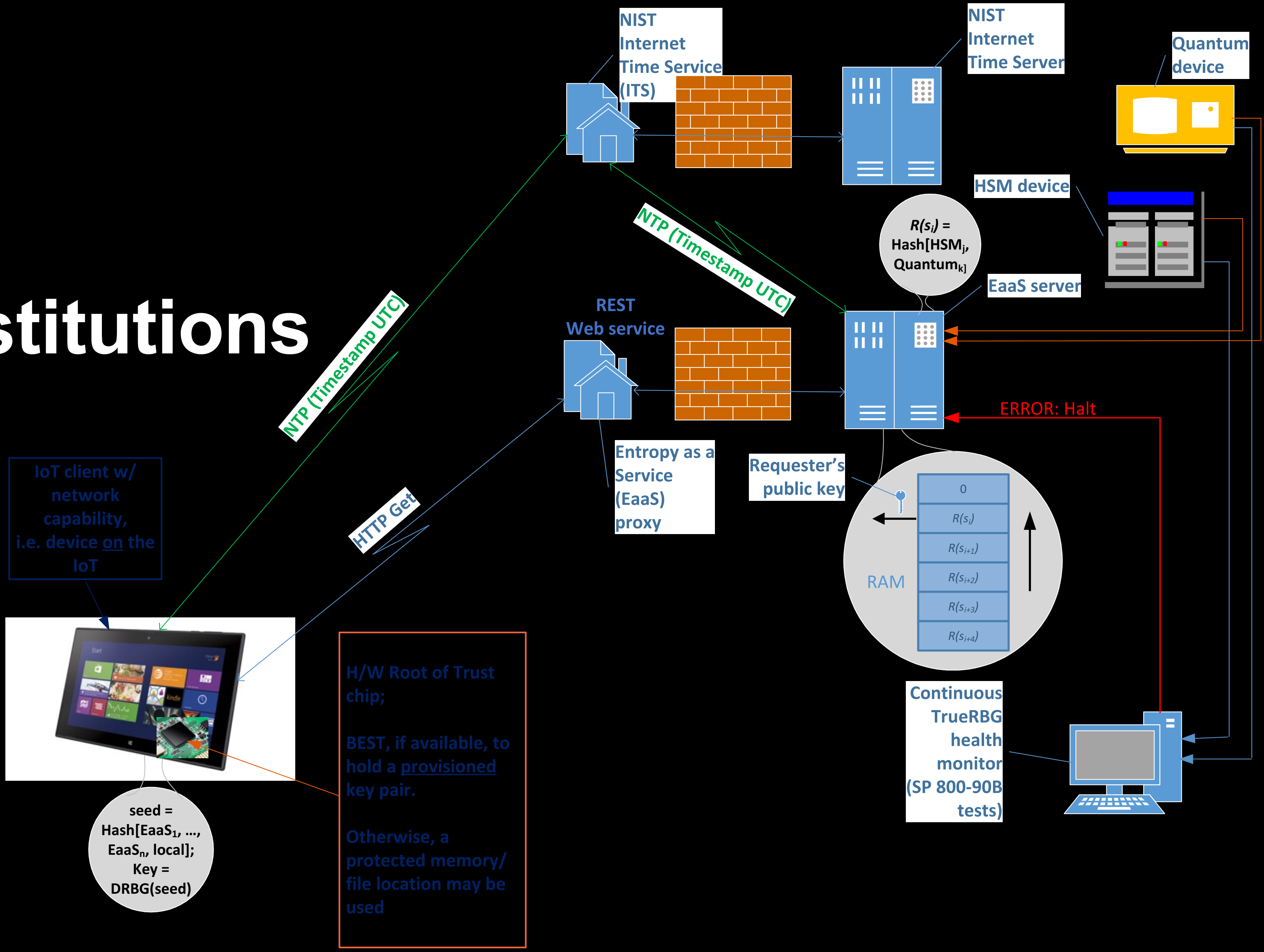
    EaaS, IoT, H/W testing

    KU Leuven, Belgium

    Leakage-resistant crypto for H/W

    University of Maryland

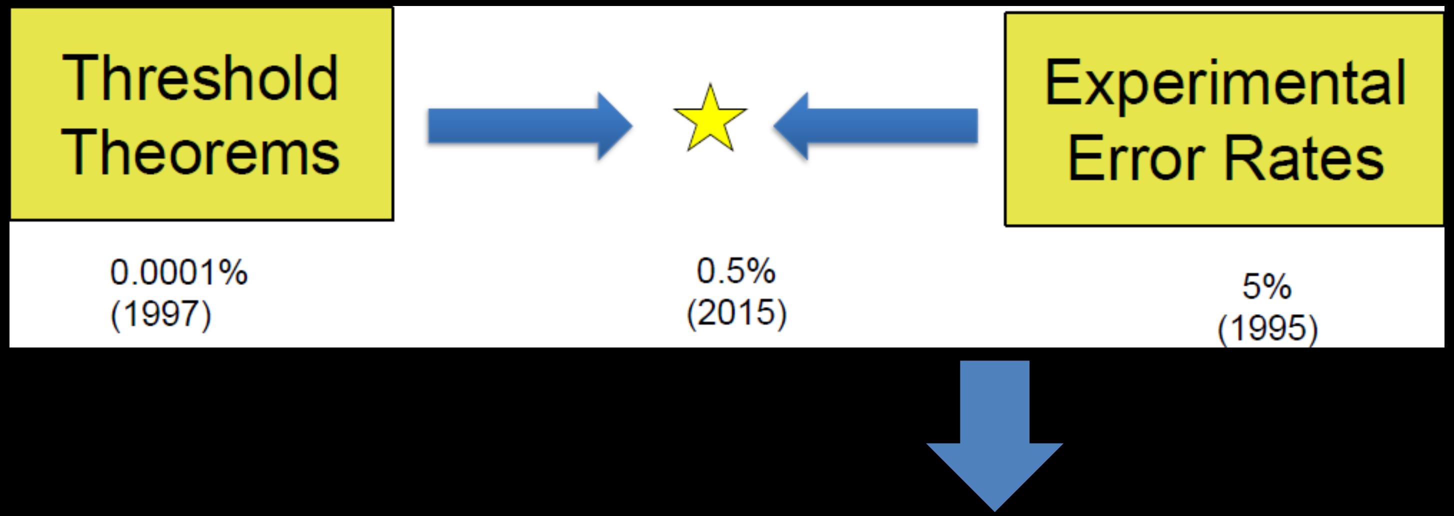
    PQC, EaaS, lightweight crypto for IoT

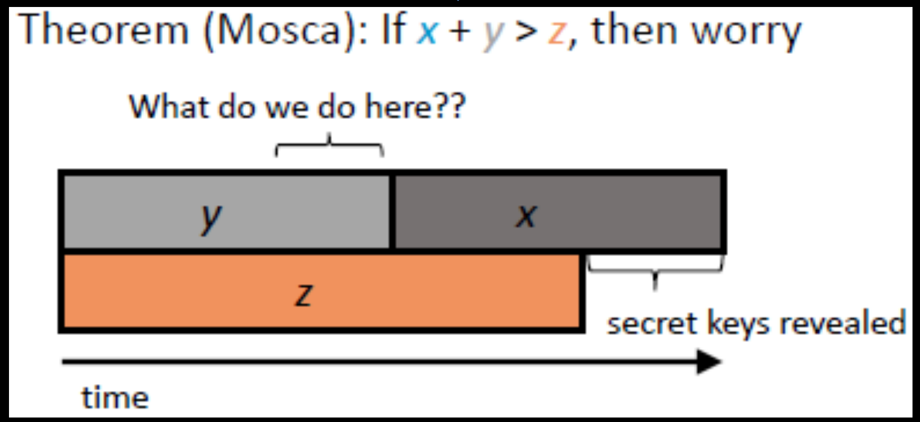


The PQC Challenge

Quantum computers are 25 years in the future and always will be. ?

Error rate halves every ≈11 months





x **– years information to stay secure**
y **– years to retool infrastructure**
z **– years to large-scale QC**

How about a hybrid approach for the interim?

Encrypt: a message or a key K is randomly split to two shares
K = K1 XOR K2.
K1 is encrypted by an approved algorithm (e.g., RSA, DH)
K2 is encrypted by a PQC method (e.g., NTRU).
The receiver decrypts both shares to recover K.

Sign: a message M is signed by two signature schemes
one approved alg Sig_1, (e.g., ECDSA)
another is a PQC signature, Sig_2 (e.g., hash-based Sig)

The signature of M is Sig_1(M) ∧ Sig_2(M).

Trading performance for security

Courtesy of: Stephen Jordan, Yi-Kai Liu & Lily Chen, NIST PQC Team

Putting it all together

The Royal Society for
Putting Things on
Top of Other Things

Monty Python, 1970

Assurance/Insurance tomorrow?

- Assurances from crypto are fundamental
  - Industry responding well to the call for action
    - started an Industry Working Group in December 2015 to rebuild crypto validation program and standards
    - great level of participation from all
- Crypto assurances help quantify cyber risks
  - A prerequisite for growing the cyber-insurance market
  - The Volvo effect?
- Assurance or Insurance – not an exclusive choice
  - The enterprise of tomorrow will likely need a blend of both

Questions?

A perspective: cryptography evolves very fast to provide security in the IoT

Emerging crypto technologies
- lightweight crypto
- lighter versions of legacy protocols
  - tinyDTLS, lightweight DTLS
- post-quantum cryptography (PQC)

New crypto is cool but have we solved all known problems with conventional crypto?