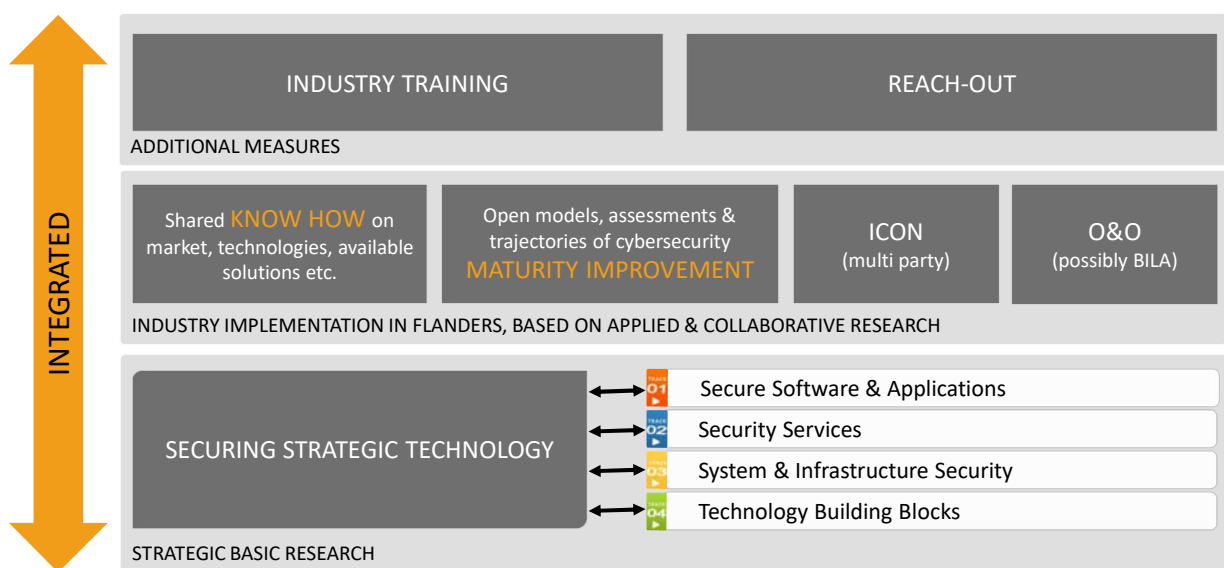




Cybersecurity Innovation Priorities, Examples and Industry Perspectives

Bart Preneel - COSIC, KU Leuven
Wouter Joosen - DistriNet, KU Leuven
Leuven, November 25 2019

THE BIGGER PICTURE – Cybersecurity Programme as a whole





Are we – Are you – loosing the race?

Why is it hard?

1. Digital (r)evolution everywhere
2. Accelerated go-to-market
3. Hyperconnected world, ultra-large scale

What if we would/could measure the total attack surface?





MUST | NICE
HAVE | IDEA

Industry Priorities?

Who dares?



7 IMPORTANT PROJECTS
IN 2020
AND BEYOND..

Not in a particular order

1. API's – "the API economy" - software composition at last
2. **Awareness** – in many ways
3. **Intelligence?** - Security Intelligence!
4. **IoT** security
5. Random number generation
6. Think long term – think **quantum**
7. **Privacy** means and requires a lot, including clever crypto



(3) INTELLIGENCE & CYBERSECURITY



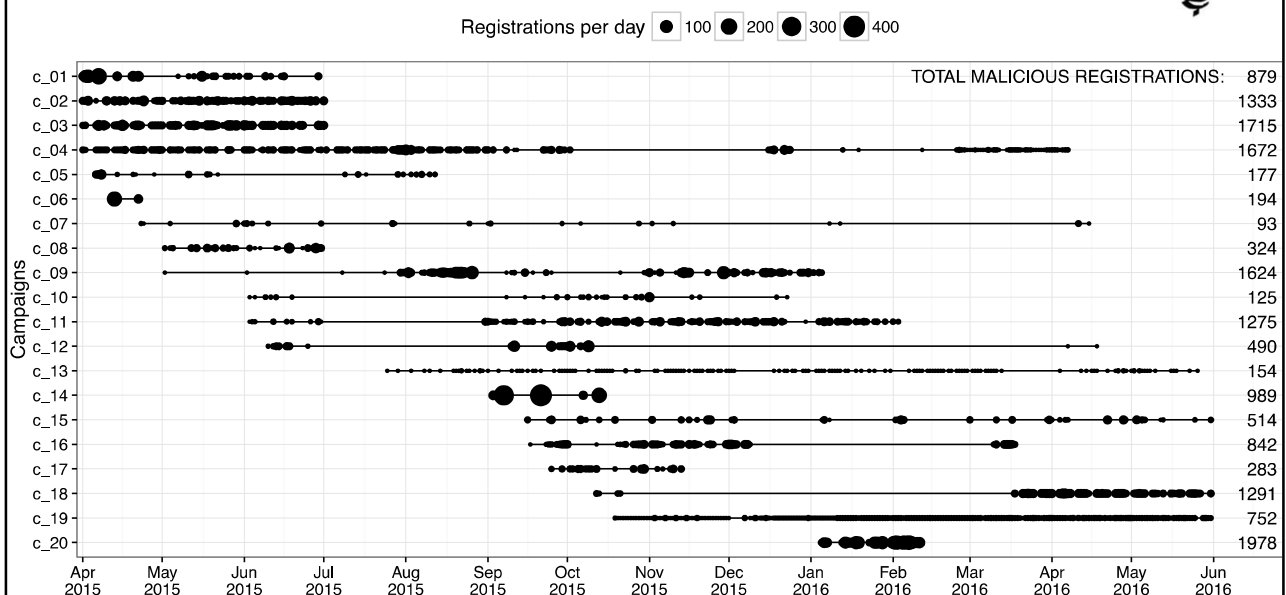
Example: malicious domain registration campaigns

- Domain names are often abused by cyber criminals
 - Spam, botnet C&C infrastructure, phishing, malware, ...
- To avoid blacklisting, malicious actors often deploy a hit-and-run strategy
- Understand the ecosystem of domain registrations in order to detect and prevent them from causing harm

Vissers et. al. Exploring the ecosystem of malicious domain registrations in the .eu TLD. RAID 2017

9

Analysis of 14 months of .eu registrations



.eu Home News Register a domain name My .eu Become a registrar WHOIS About us Contact Us

Over 25 000 domain names suspended with t identity fraud

.eu Home News Register a domain name

Over 11 000 abusive

On 29 January 2018, EURid suspe
With actions as such, our focus is
enforcement, both on a national i
towards building the most trustw
illegal activity online. "With our the
names for potential abuse, leadin
EURid Legal Manager.

In 2017, we suspended 20 126 dc
enforcement.

On 21 June 2018, EURid suspended 11 760 domain names that were registered with non-eligible registration
of which some have been reported for abuse.

With actions as such, our focus is on the safety of online consumers. Via close collaborative efforts with law
s with our registrar channel, w
pace, taking a stand against

domain names for potential
2017, where we suspended 20
abusive domain names, we're up to 36 336 abusive domain name suspensions thus far in 2018." said Geo Van
Langenhove, EURid Legal Manager.

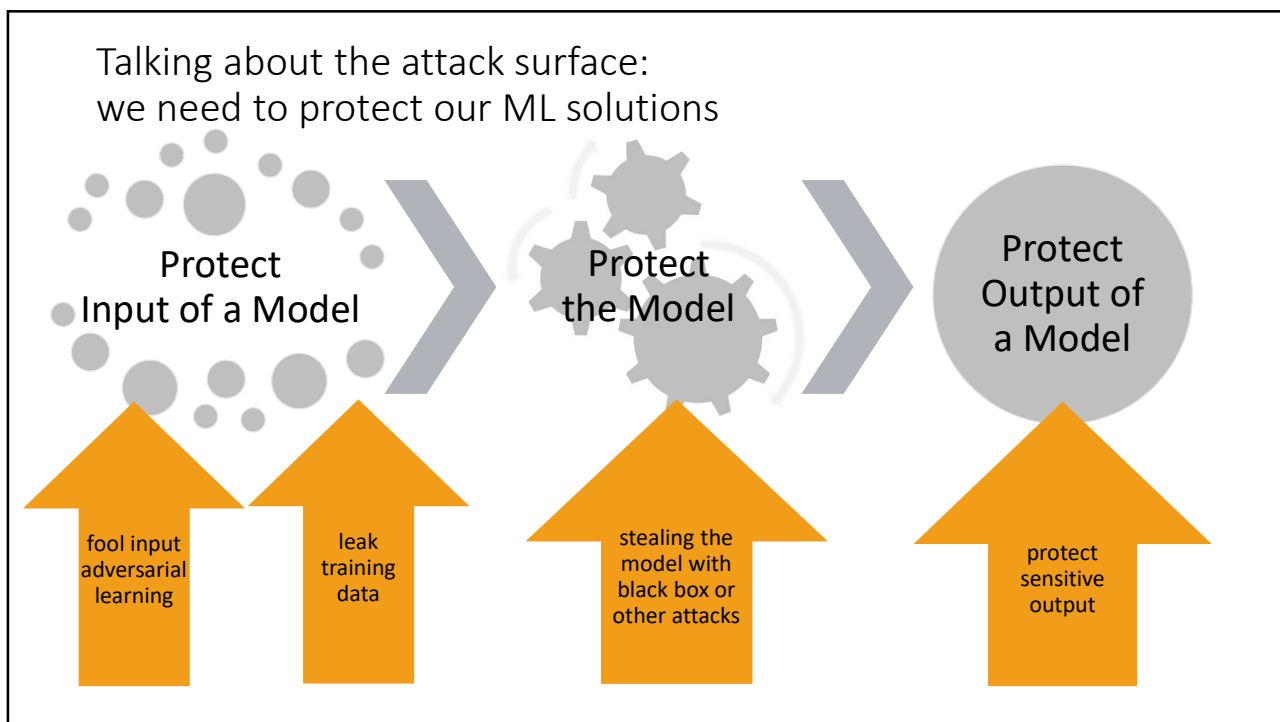
Learn more about the ways we're building a trustworthy .eu and .euo domain name space at trust.eurid.eu.

Predictive Algorithms

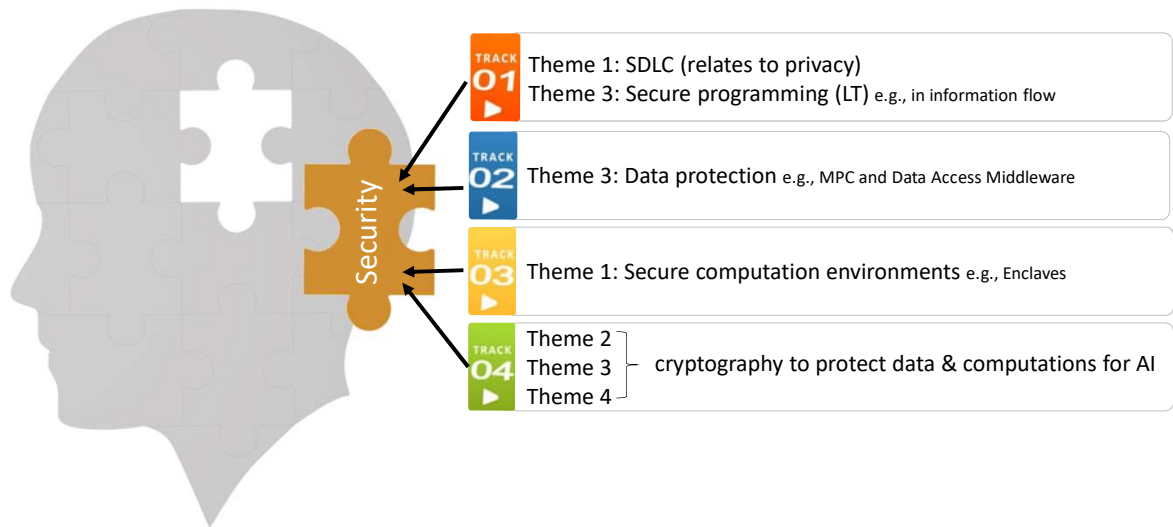
Through the use of historical data and self-learning algorithms, we are
working to predict at the time of registration whether or not a domain
name might be used in an abusive way in an effort to prevent such
malicious domain names from becoming active in the first place.

« Back to the news page

As part of the EURid's Trust & Security program,
58,966 domains were suspended in 2018.

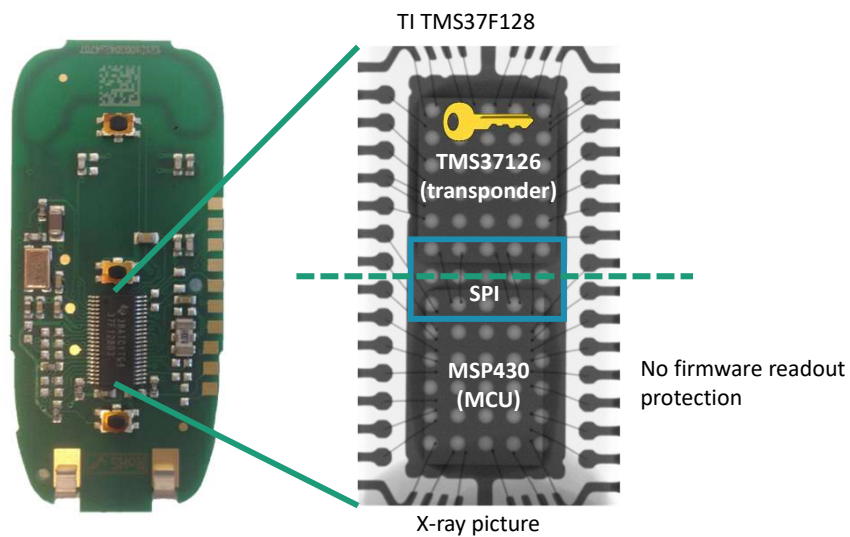


BTW: on the need for SECURITY IN ARTIFICIAL INTELLIGENCE



(4) IoT Security

The Tesla Model S key fob



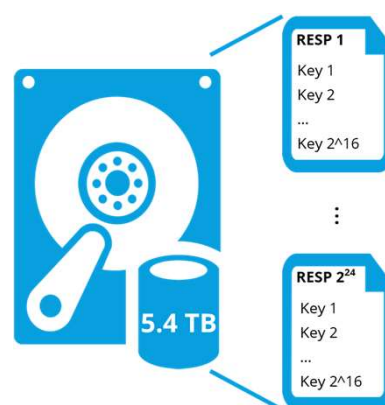
15

Findings



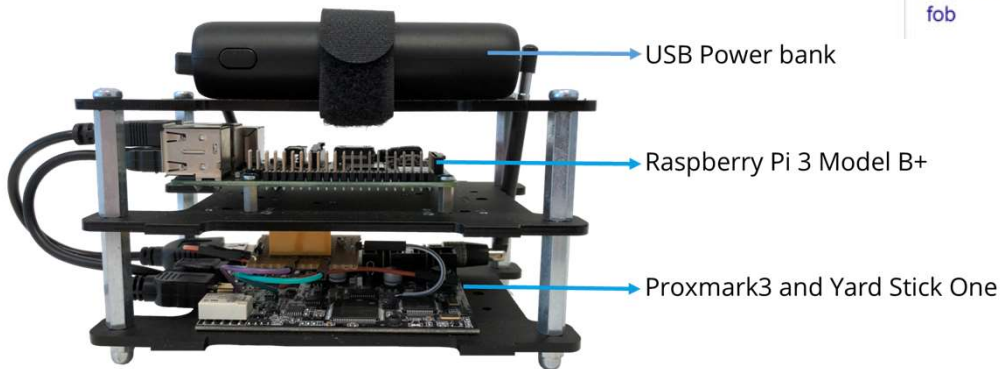
System & Infrastructure Security

- 40-bit key DST40 cipher
 - 40-bit challenge and 24-bit response
- No mutual authentication
- Time-Memory Trade-Off Table
 - Key recovery in ~2s on a Raspberry Pi



16

Proof of Concept attack

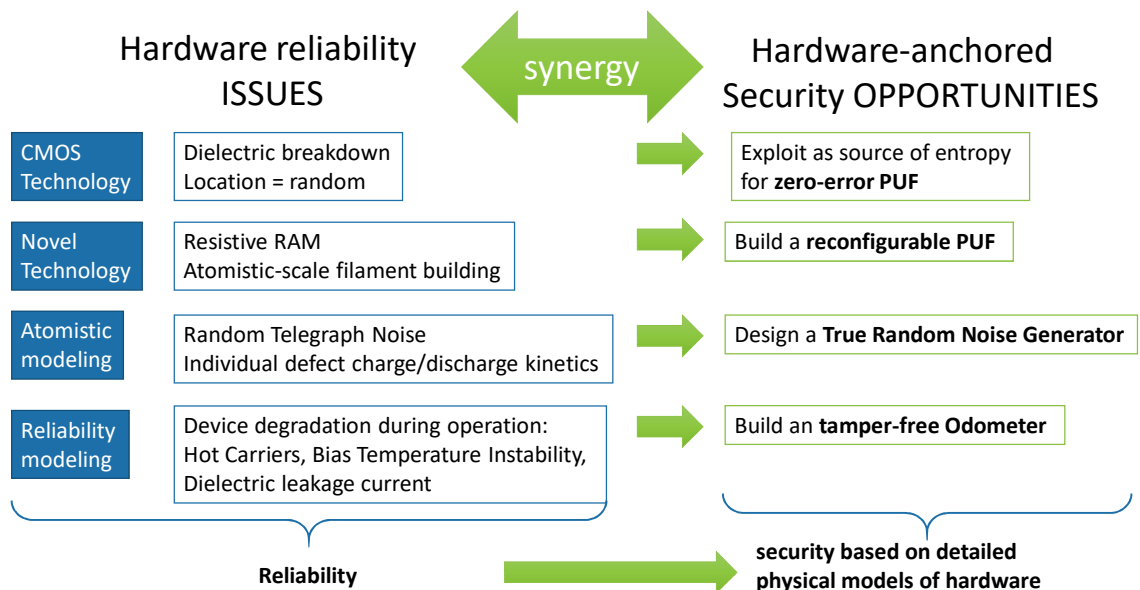


17

(5) TRUE RANDOM NUMBER GENERATORS



Reliability and security: hand in hand



19

True Random Number Generators

TRACK
04

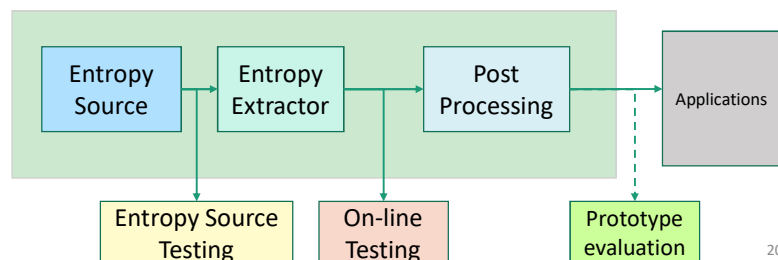
Theme 1 Secure hardware

Self-tuning TRNGs to reduce influence of technology

Novel entropy sources

Novel entropy extractors (post-processing)

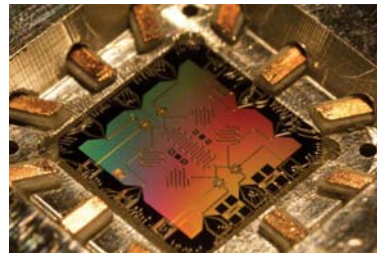
On-line test



20

(6) POSTQUANTUM CRYPTOGRAPHY

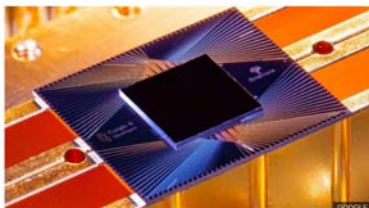
IBM 2017: 50 qubits
 IBM 2019: 53 qubits
 Google 2018: 72 qubits
 Rigetti: 128 qubits
 RSA-2048 would require 4096 ideal qubits or 20 million real qubits



Google claims 'quantum supremacy' for computer

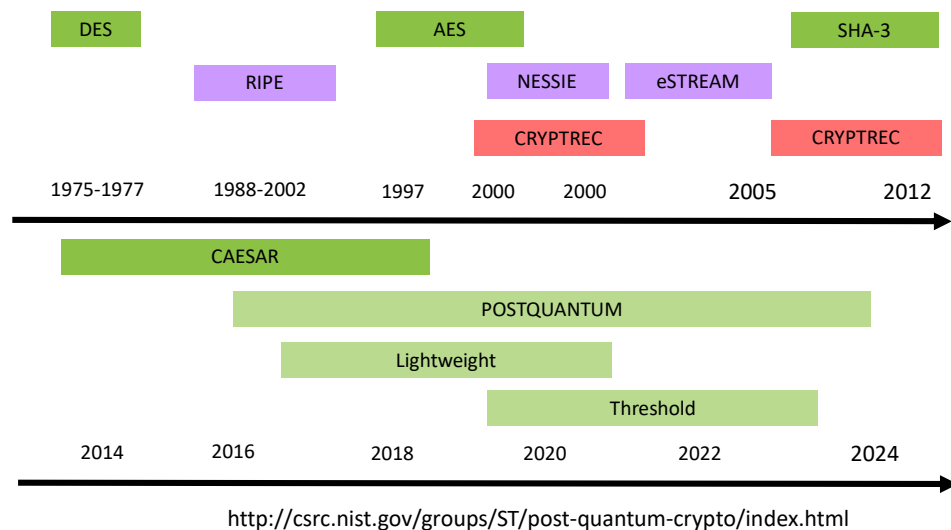
By Paul Rincon
 Science editor, BBC News website
 © 23 October 2019

[f](#)
[t](#)
[t](#)
[e](#)
[Share](#)



<http://www.qubitcounter.com/>

Open competitions



23

When to switch to quantum resistant cryptography? [Mosca]

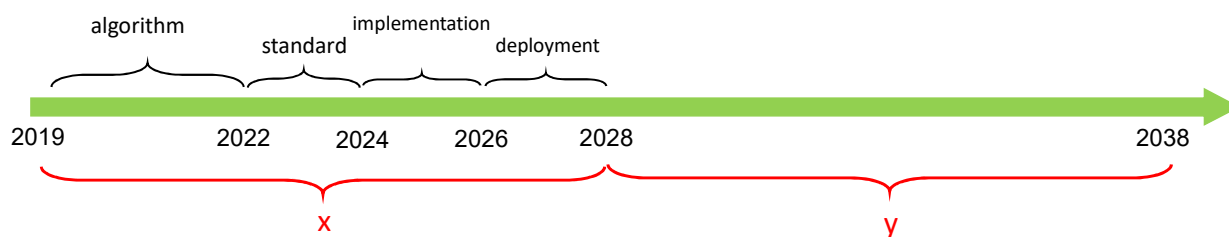
Q = #years until first large quantum computer

x = #years it takes to switch (3-12 years)

y = #years data needs to be **confidential** (10 years)

Need to start switching in the year $2019 + Q - x - y$

e.g. $Q = 20, x=10, y=10$: today!



24

NIST Post-Quantum competition

https://en.wikipedia.org/wiki/Post-Quantum_Cryptography_Standardization

- 69 complete and proper submissions
- January 30, 2019: 26 remaining (including LUOV and SABER)

	Signatures	Encryption/KEM	TOTAL
Lattice	3	9	12/28
Code	0	7	7/24
Multivariate	4	0	4/13
Hash	1	0	1/4
Other	1	1	2/13
TOTAL	9	17	26/82

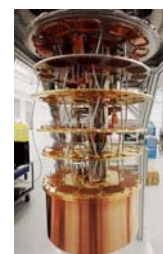
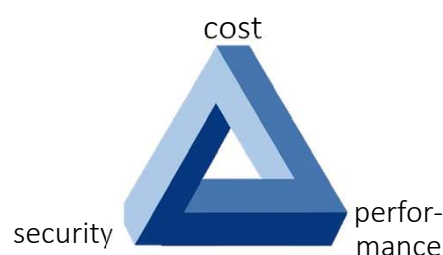
25

Cryptographic algorithms



Theme 2 Symmetric key and public-key algorithms

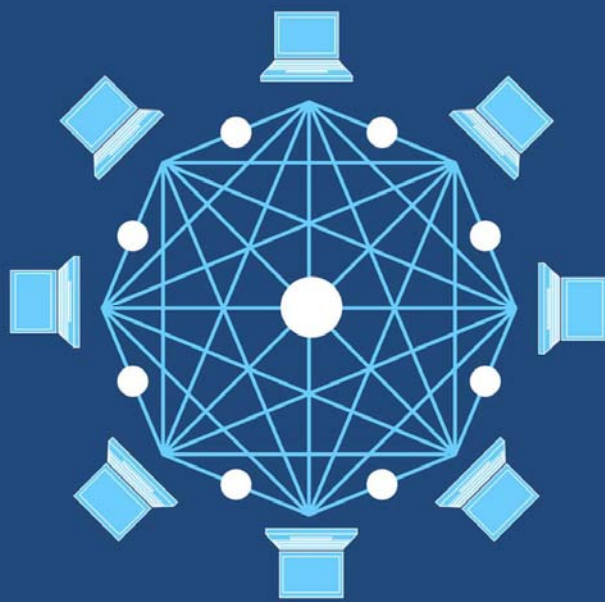
- pushing the security/cost tradeoff for cryptography to allow for ubiquitous long-term cryptographic protection of data during storage, communication and processing
- increasing the assurance and addressing the threats posed by quantum computers
- align with international standardization strategies (NIST, ISO,..)



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



26

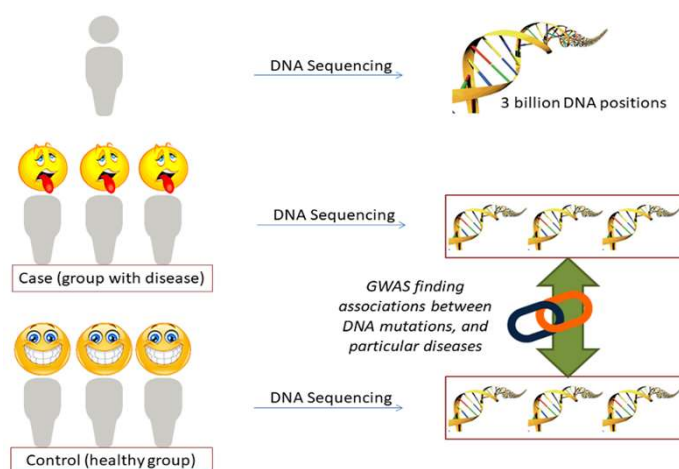


(7) COMPUTING ON ENCRYPTED DATA

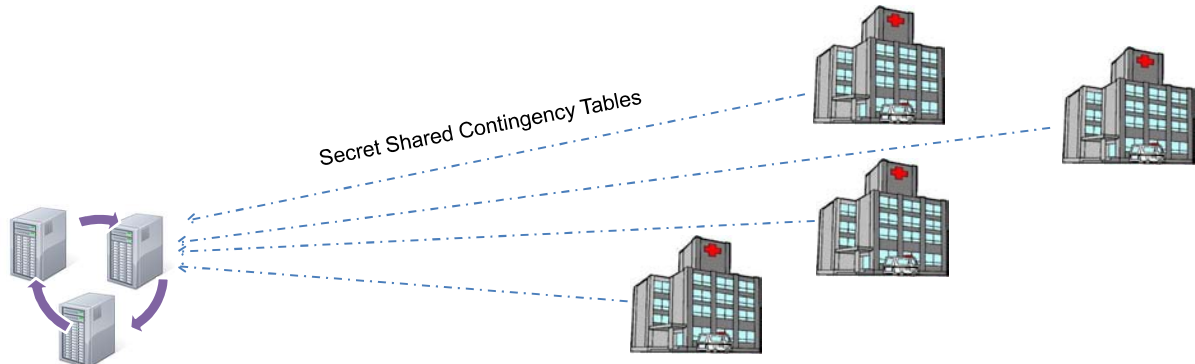
Genome Wide Association Study (GWAS) via Multi-Party Computation (MPC)



Theme 2 Cryptographic protocols



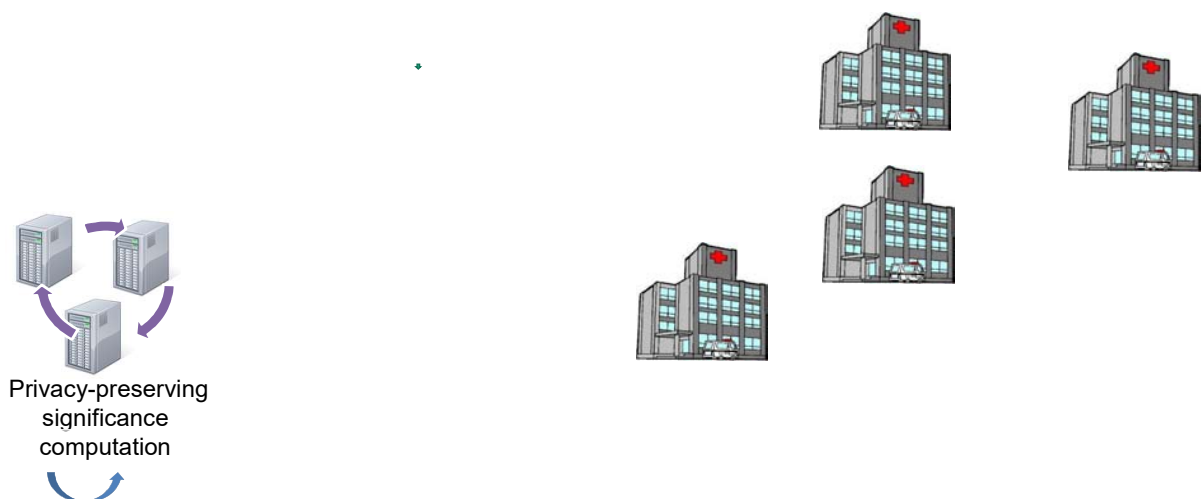
GWAS via MPC



Step 1: The hospitals secret share their contingency tables to the MPC engine

29

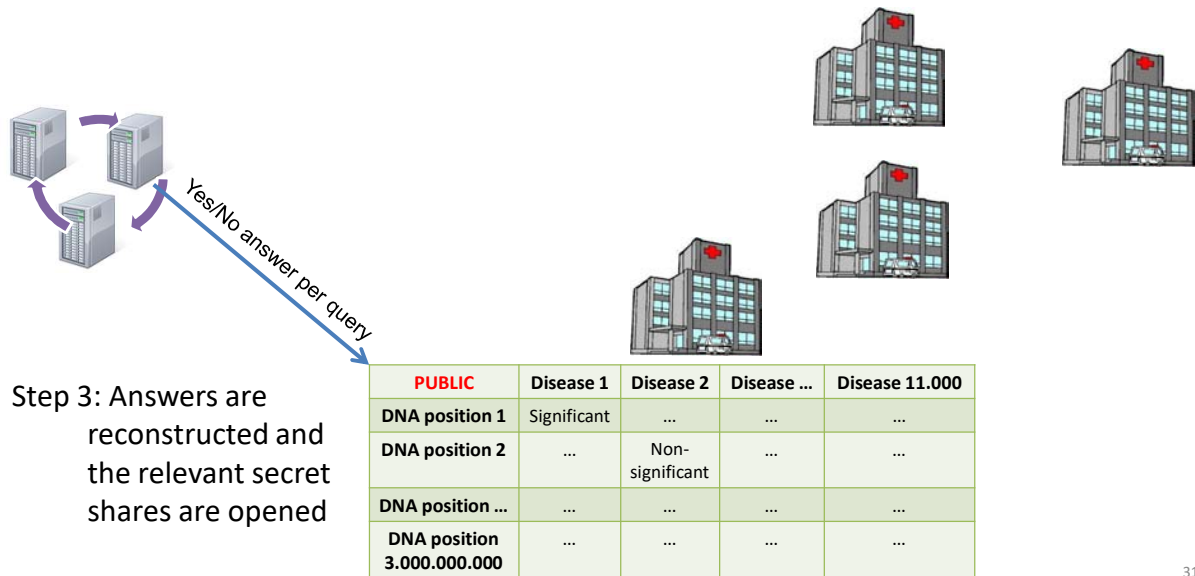
GWAS via MPC



Step 2: The MPC engine performs on the computation on the secret shared data

30

GWAS via MPC



31



What is good enough Cybersecurity?

AGILITY

BUSINESS VALUE



RESILIENCE



PROVEN SECURITY



Human Capital is the key.

A horrible trade-off



THANK YOU

Questions?