# Nothing Lives Forever. Especially Unsupported Devices

How lifecycles can undermine security and trust

Jan Dušátko
jan.dusatko@cryptosession.cz

# Lifecycle management is a security problem

Technically, assets can survive decades. But would you like to use it?

- Lifecycle is matter of security, not accounting
- In a connected world, only support provided will decide about lifetime
- Risk analysis for devices without support is an equivalent of robbery

*"Nothing says ‘robust cybersecurity’ like a Windows Server old enough to vote."*

# Your Assets Has Better Persistence Than Your Security Team

Vulnerability growth over time

- Lack of support for assets with geological lifespans
- Devices become forgotten and Shadow IT rises
- Security controls become incompatible
- Cryptography becomes unsupported
- Supply-chain dependency problems grow

*"Temporary exception approved in 2010. Still temporary in 2025."*

# Motivation and misconception

What is a motivation for device replacement?

- Could be one or more from list:
  TCO, PUE, availability, stability, safety, price, simplicity, user interface
  in rare cases - support
- Everyone forgot security

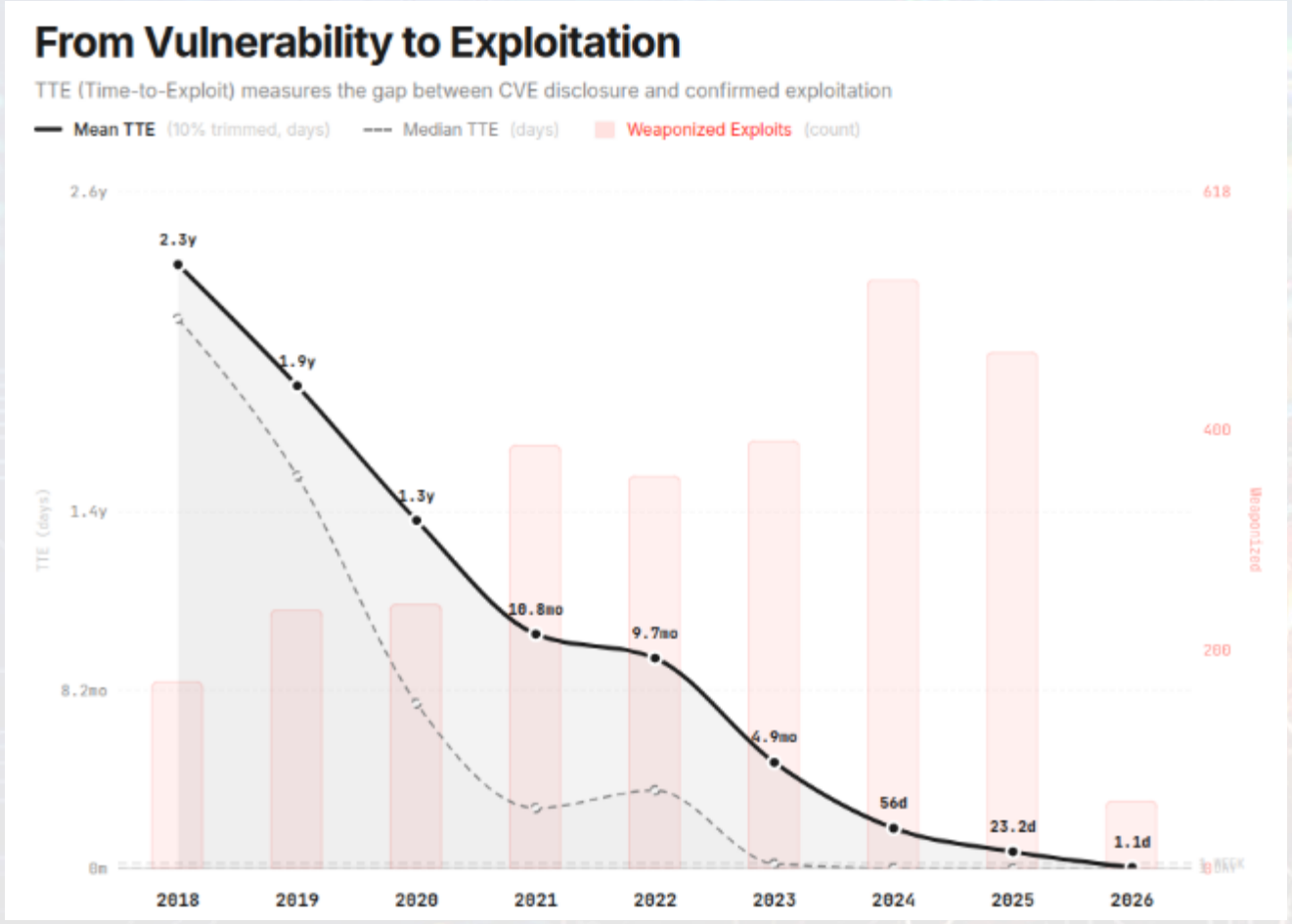
Beware:

- Extended Support Is Not Resurrection
- Risk Acceptance Is Not Risk Elimination

# If It Cannot Be Patched, It Becomes Malign

- Unsupported systems become systemic risk.
- Lifecycle management is security governance.
- EoL planning must exist before deployment.

# Cybercrime and AI twist the game




- 2026 - 1 day *(actually 10 hours)*
- 2027 - 10 minutes
- 2028 - 1 minute !!!

Source: https://zerodayclock.com/

# Agile Cryptography

You can’t spell Cryptography without “cry” …



ARROW

# Mosca's theorem

$$X + Y > Z$$

X Migration time 🛠

Y Security shelf life 📚

Z Time to compromise 🕐

☠ Secret keys compromised

Withdraw timescale in cryptography is usually about 10-15 years!

# Record, Measure, Evaluate, Manage …

- Unknown assets are just future incident reports
- If you do not measure and evaluate it, attackers probably already did
- Cryptoagility: Change in minutes, not months

What else required?

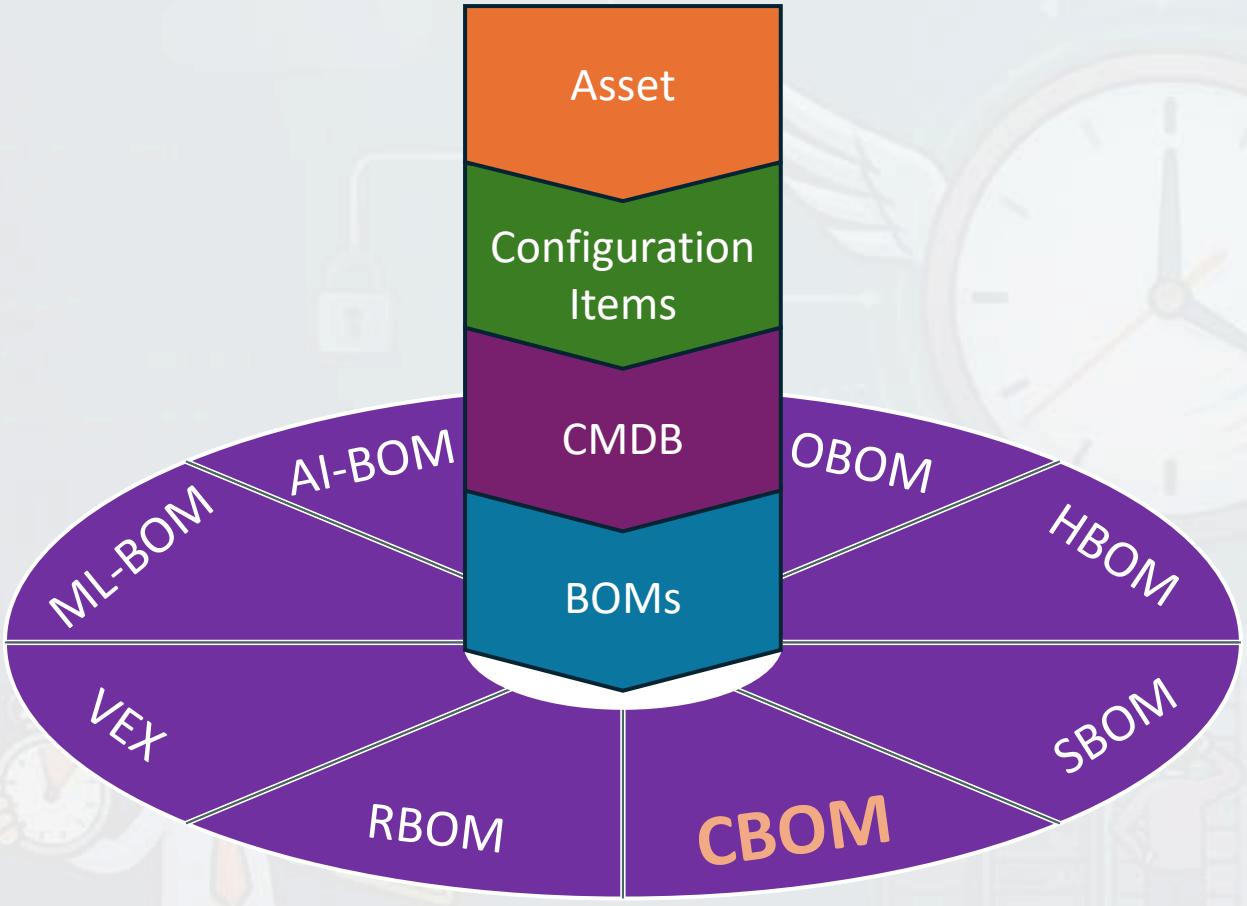
# Cryptoagility and technology

- Separate cryptography from business logic.
  *Replacing one cipher should not require rewriting whole history.*
- Cryptographic policies must be centrally managed.
  *Developers should not “express themselves” through custom crypto settings.*
- Cryptography must be continuously tested.
  *“It encrypted something” is not a successful test result. Who will decrypt it?*
- Key rotation and crypto migration must be automated.
  *Expired certificates remain one of humanity’s favorite outage generators.*
- Plan for cryptographic replacement before disaster happens.
  *Attackers usually do not wait for your next maintenance window.*

# CBOM and measurement

- Not providing a CBOM is still a strategy. For now.
- “Military-grade encryption” stops sounding impressive once someone asks for metrics.
- Relax. It’s only statistics deciding your security posture.

# Explaining Why “One More Migration” Is Actually a Feature



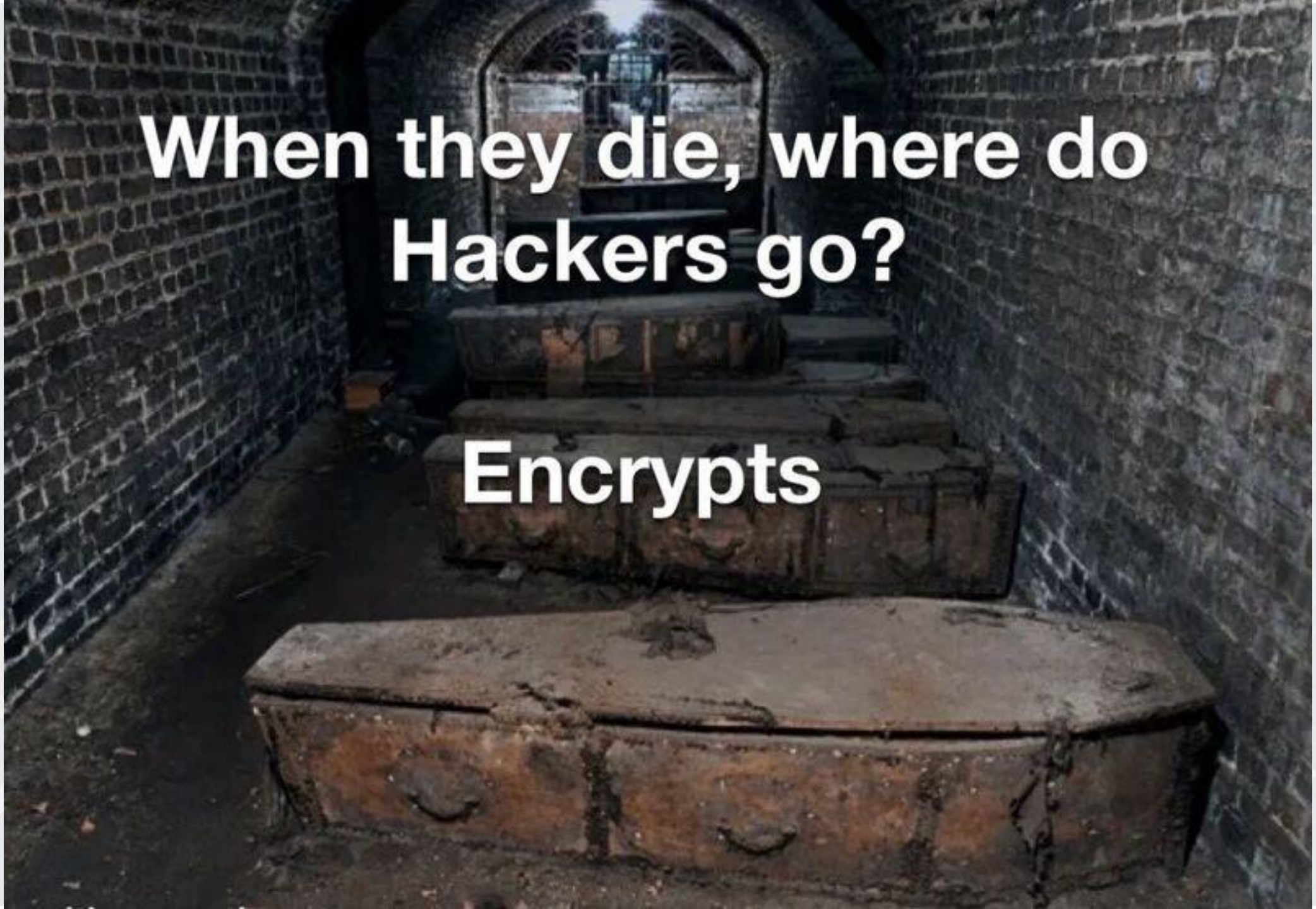

**CBOM** (**C**ryptography **B**ill **o**f **M**aterials)

Consist:

- Libraries
- Protocols
- Algorithms
- Key materials

Scopes:

- Capability
- Dependencies
- Default configuration
- Used settings


When they die, where do Hackers go?
Encrypts

# Side-Channel Attack or Sith Side Attack?

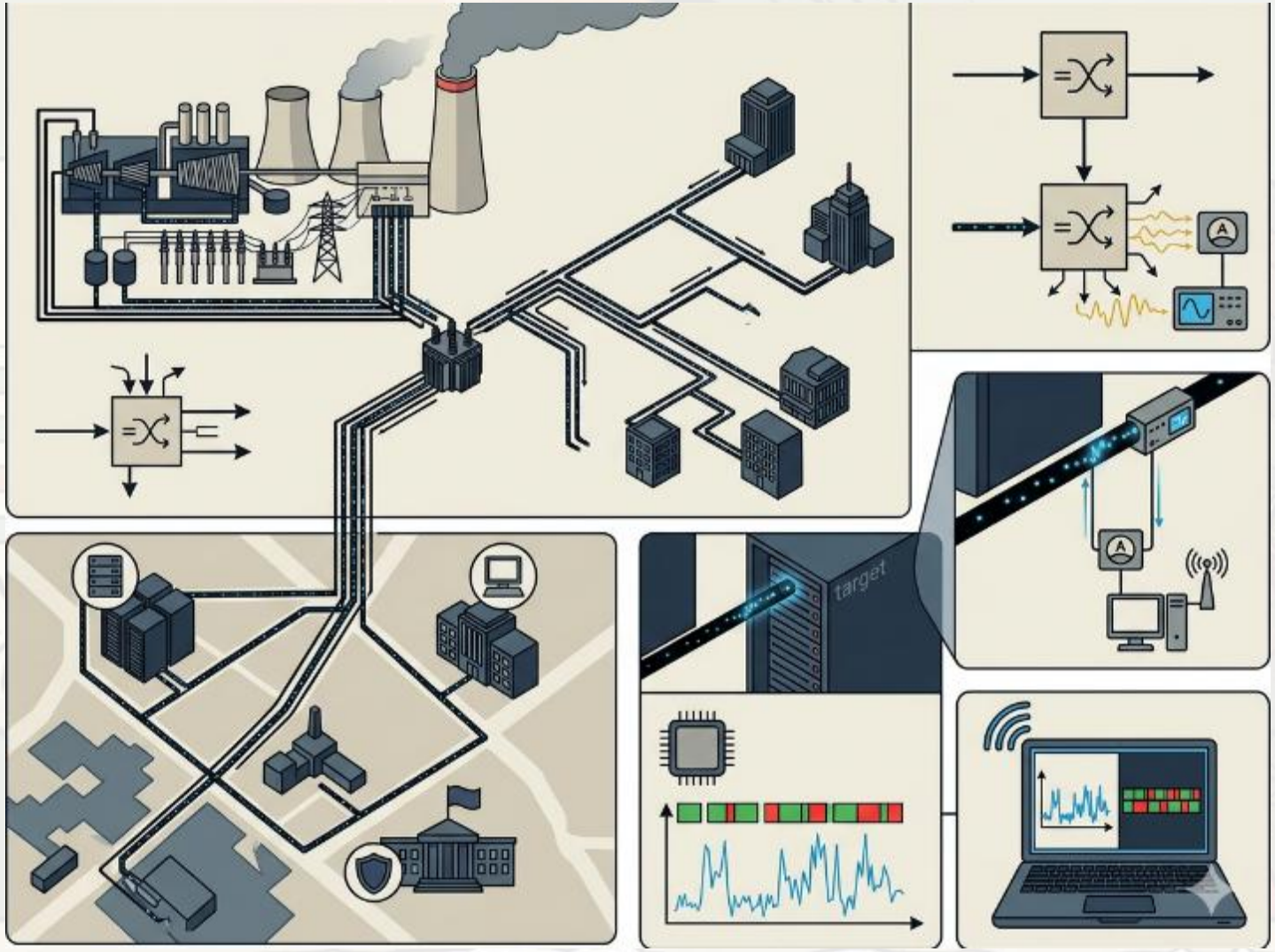
Secure in Theory, Leaking in Practice

# The encryption survived. The physics testified against it.

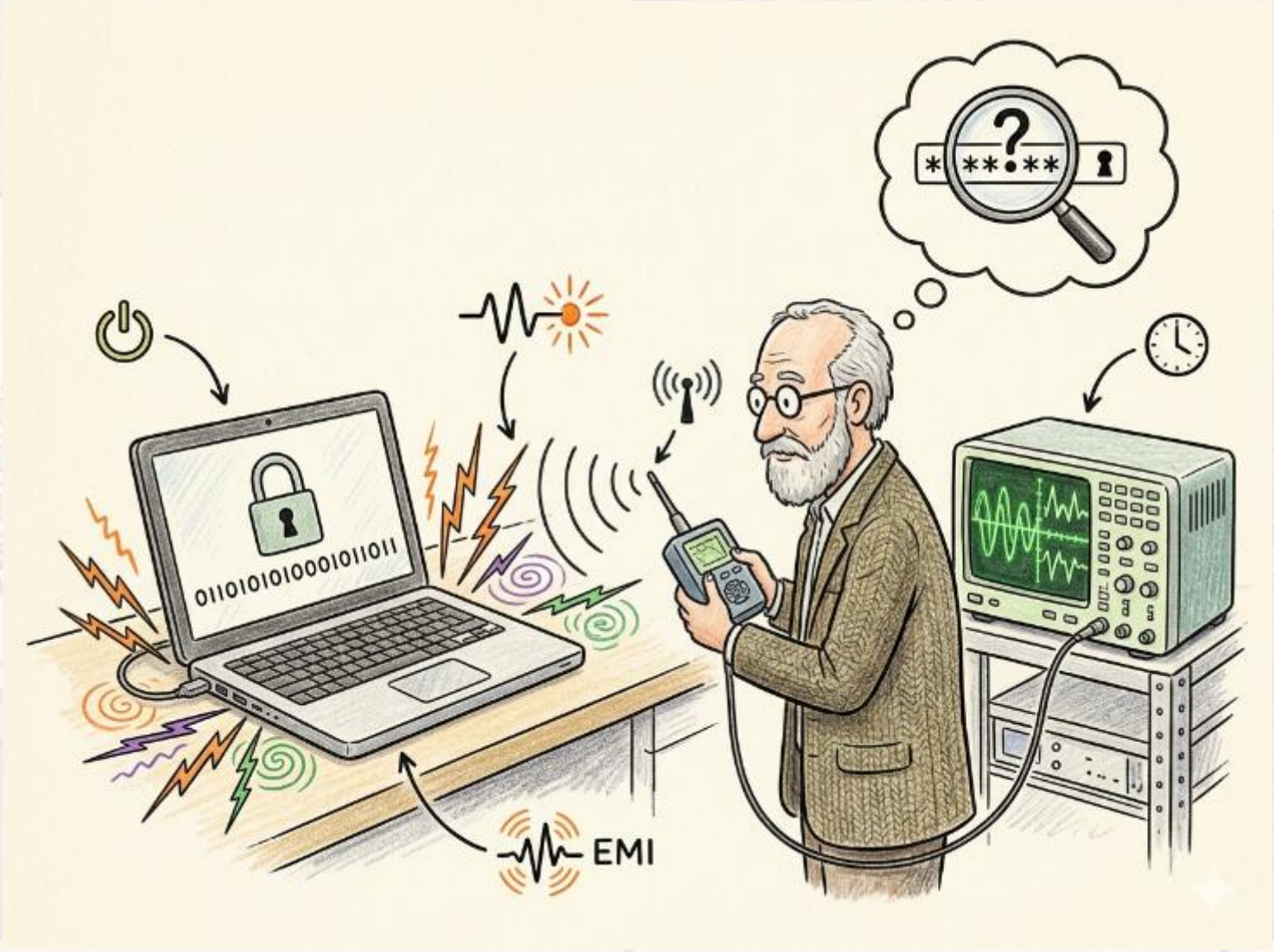
- Timing: Measuring your mistakes in nanosecond scale
- Power: Power plant is now part of your threat model
- EMI: Dr. Oscilloscoppy can witness
- Cache: The cache is not exactly your friend.
- Acoustic: When encryption speaks out loud.
- Optical: Device decided to become a lighthouse.

# Timing: Measuring your mistakes in nanosecond scale

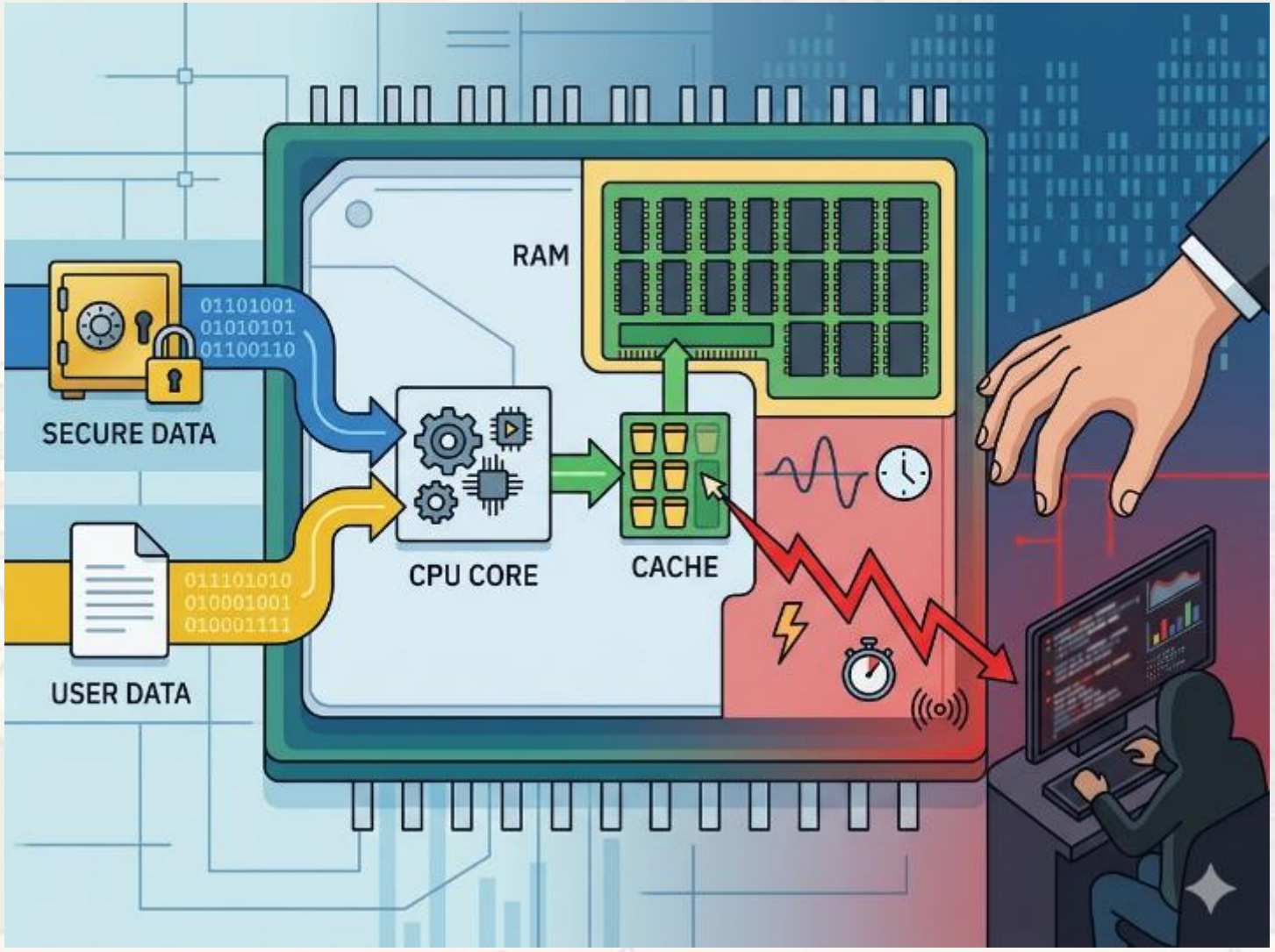
# Power: Power plant is now part of your threat model



# EMI: Dr. Oscilloscoppy can witness



# Cache: The cache is not exactly your friend.



# Acoustic: When encryption speaks out loud.

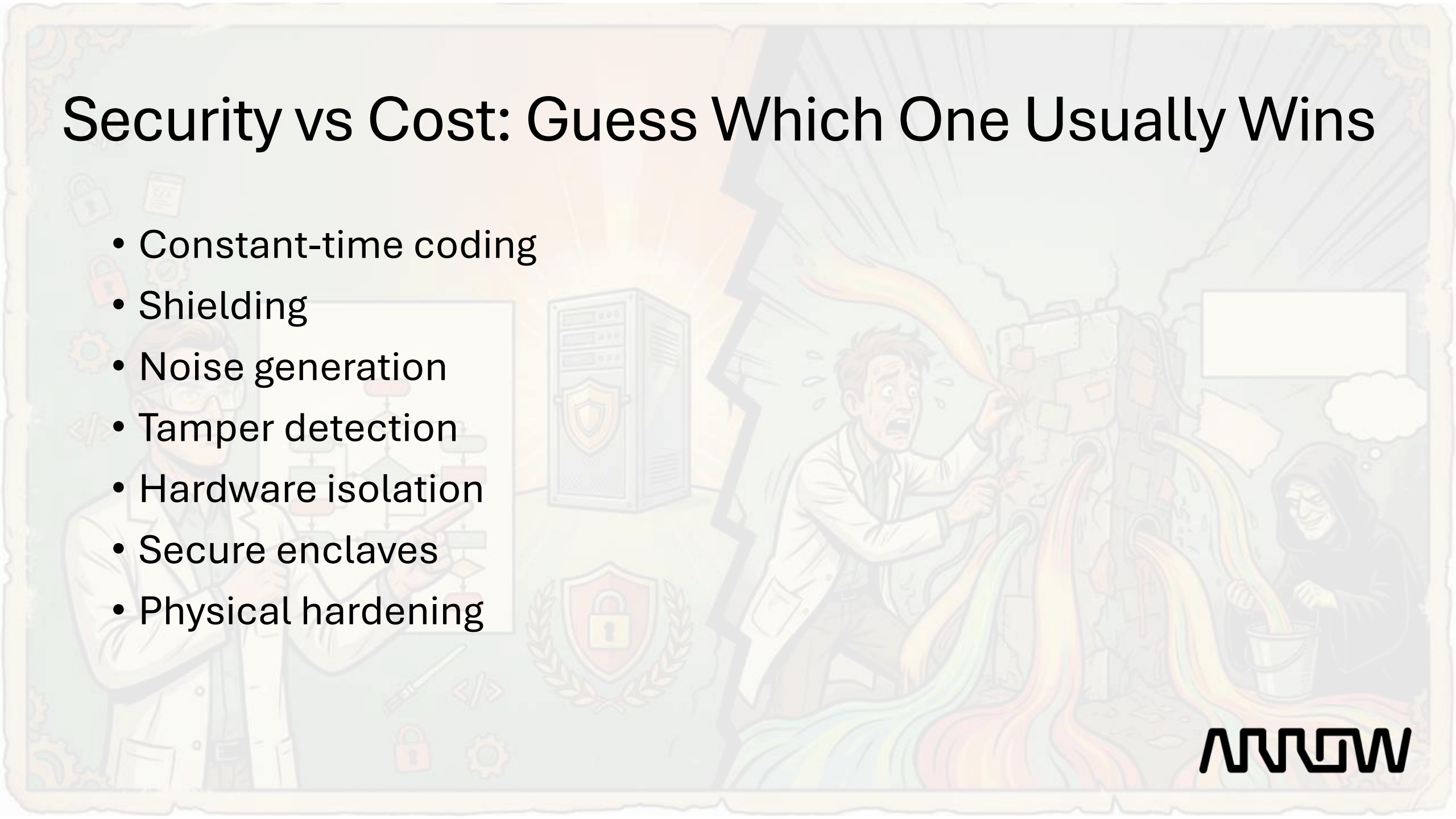
# Optical: Device decided to become a lighthouse.

# Important and Overlooked Part

- Performance versus latency
- Price versus security

# Security vs Cost: Guess Which One Usually Wins

- Constant-time coding
- Shielding
- Noise generation
- Tamper detection
- Hardware isolation
- Secure enclaves
- Physical hardening




I.O.T.
DID YOU KNOW THE 'S' IN I.O.T. IS FOR SECURITY?
BUT... THERE IS NO 'S' IN I.O.T. ?!
EXACTLY MY POINT.'
Hello...
dcypher Symposium 2017
MEDIAPLAZA-Utrecht
ATARI

# Post-Quantum Cryptography

Quantum Computing: Because Classical Problems Were Too Easy

# PQC and QRC

- Difference between classical and quantum computation.
- Why cryptography is affected.
- Long-term confidentiality risks.
- Key Facts
- Quantum computers threaten asymmetric cryptography most severely.

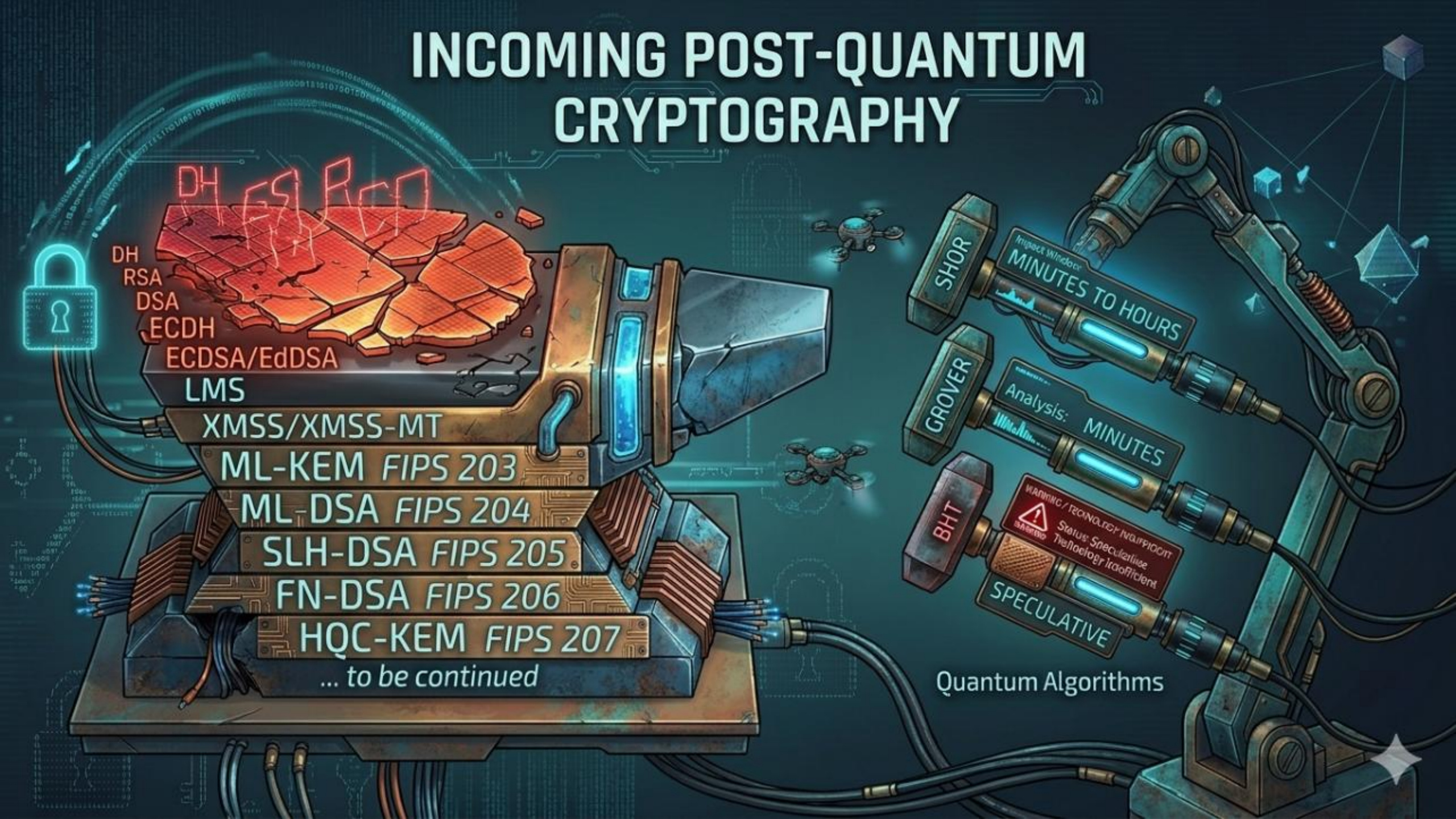
*"RSA had a good run. Roughly 47 years."*

# Designing Cryptography for the Next 20 Years

- Quantum computers are not the only thing trying to break your cryptography
- Future-proof implementations require algorithm agility and measurable security properties
- Your hardware will likely outlive your current threat model

Solution?

Same interface. Same controls. More capabilities where needed.

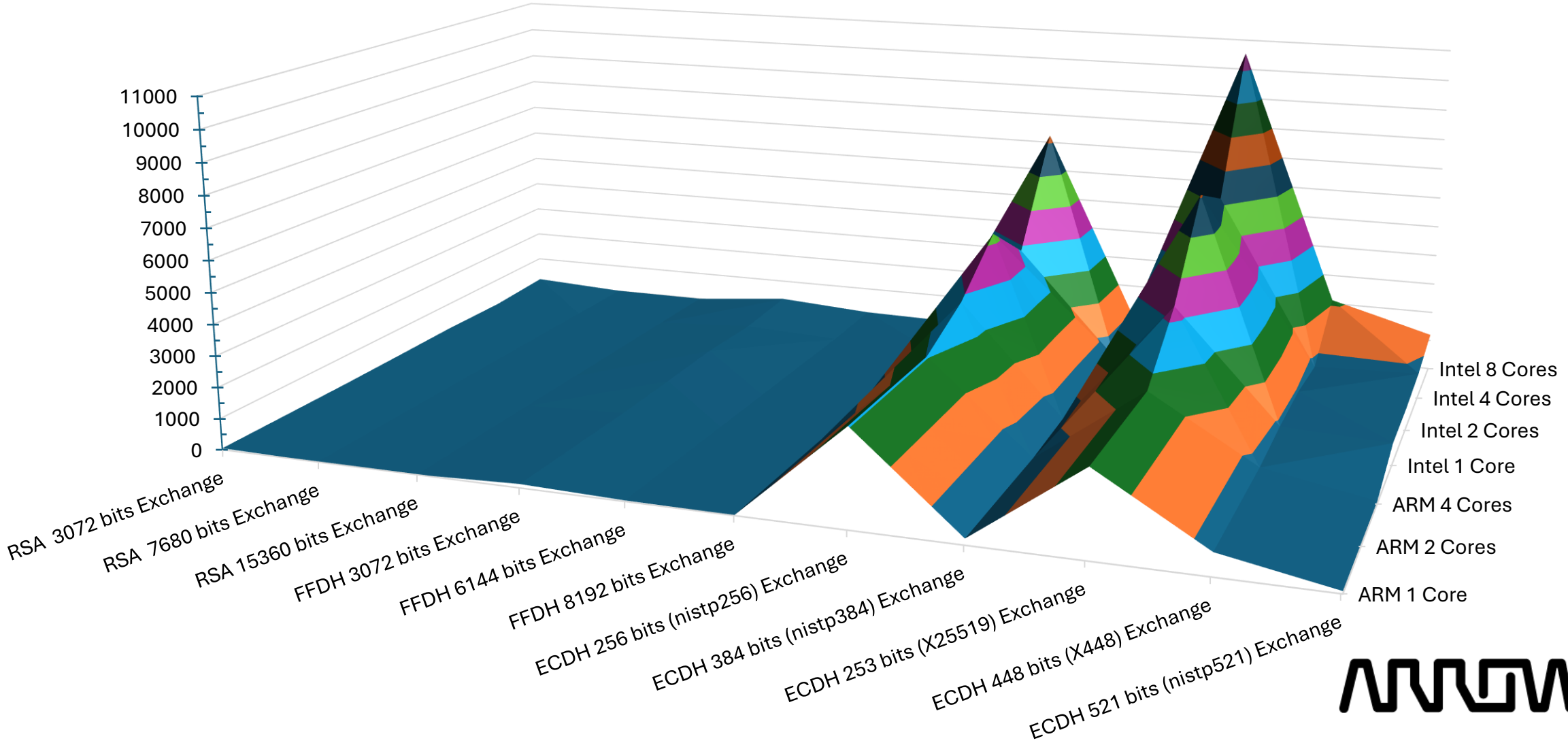

INCOMING POST-QUANTUM CRYPTOGRAPHY
DH
RSA
DSA
ECDH
ECDSA/EdDSA
LMS
XMSS/XMSS-MT
ML-KEM FIPS 203
ML-DSA FIPS 204
SLH-DSA FIPS 205
FN-DSA FIPS 206
HQC-KEM FIPS 207
... to be continued
SHOR
MINUTES TO HOURS
GROVER
Analysis: MINUTES
BHT
SPECULATIVE
Quantum Algorithms

# Post-quantum cryptography does not simply replace RSA with “RSA but newer.”

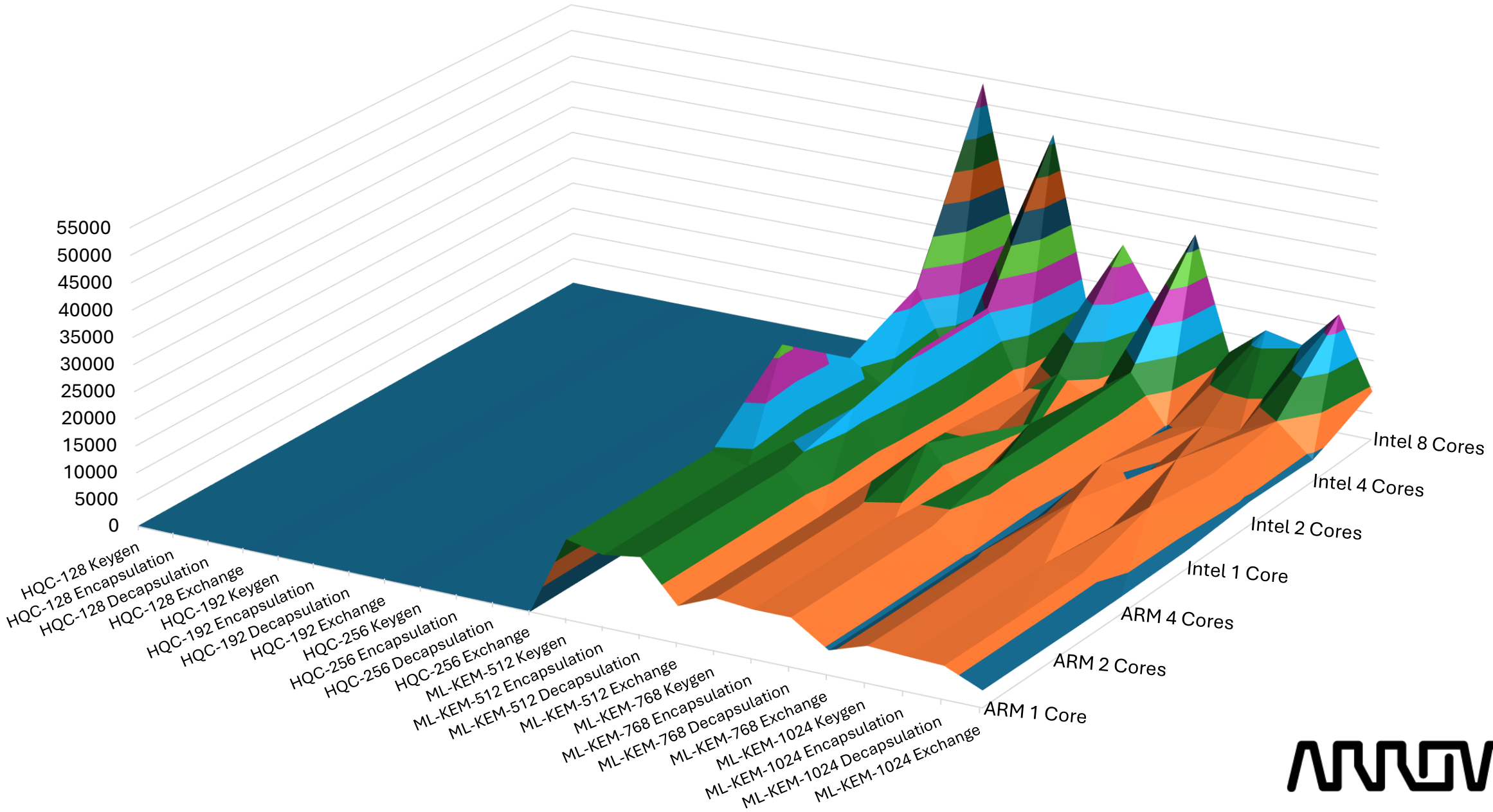
- Despite all that complexity, many of them still outperform today’s “modern” cryptography in selected scenarios.
- The migration is not only cryptographic. It is architectural, operational, and sometimes painfully organizational.

*This is not a crypto refresh. It is an infrastructure personality change.*

# Performance of classical cryptography, normalization to 1GHz



# PQC KEM - normalization to 1GHz CPU, impact of cores, HT and instruction sets




Jan Dušátko
jan.dusatko@cryptosession.cz