The Importance of Cryptographic Agility in the Banking Sector

Gergely Zsolt Kovács

Date

20 July, 2025

Introduction

- PhD student at Eötvös Loránd University
- Cooperative Doctoral Program (KDP)
- Cybersecurity researcher at OTP Bank

ELTE-OTP Cybersecurity Lab (Kiberlab)

- Since 2023
- 30 BSc, MSc students
- Practical cybersecurity research topics
- Both university and industry mentors

Post-Quantum Transition

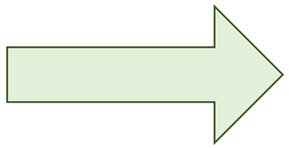
- Need is well understood
- Timeline uncertain
- Operational / reputational / compliance risk
- When to start?
- Where to start?

Post-Quantum Cryptography Topic Kiberlab

- One of the first efforts in the Bank to tackle this challenge
- BSc students
- Research externally (also to familiarize themselves)
- Consult with experts inside the Bank
- Produce a report on the main risks (protocols, algorithms, existing solutions)

Transition Challenges

- Cryptography is everywhere
- Hard coded algorithms
- Legacy software
- Baked into hardware

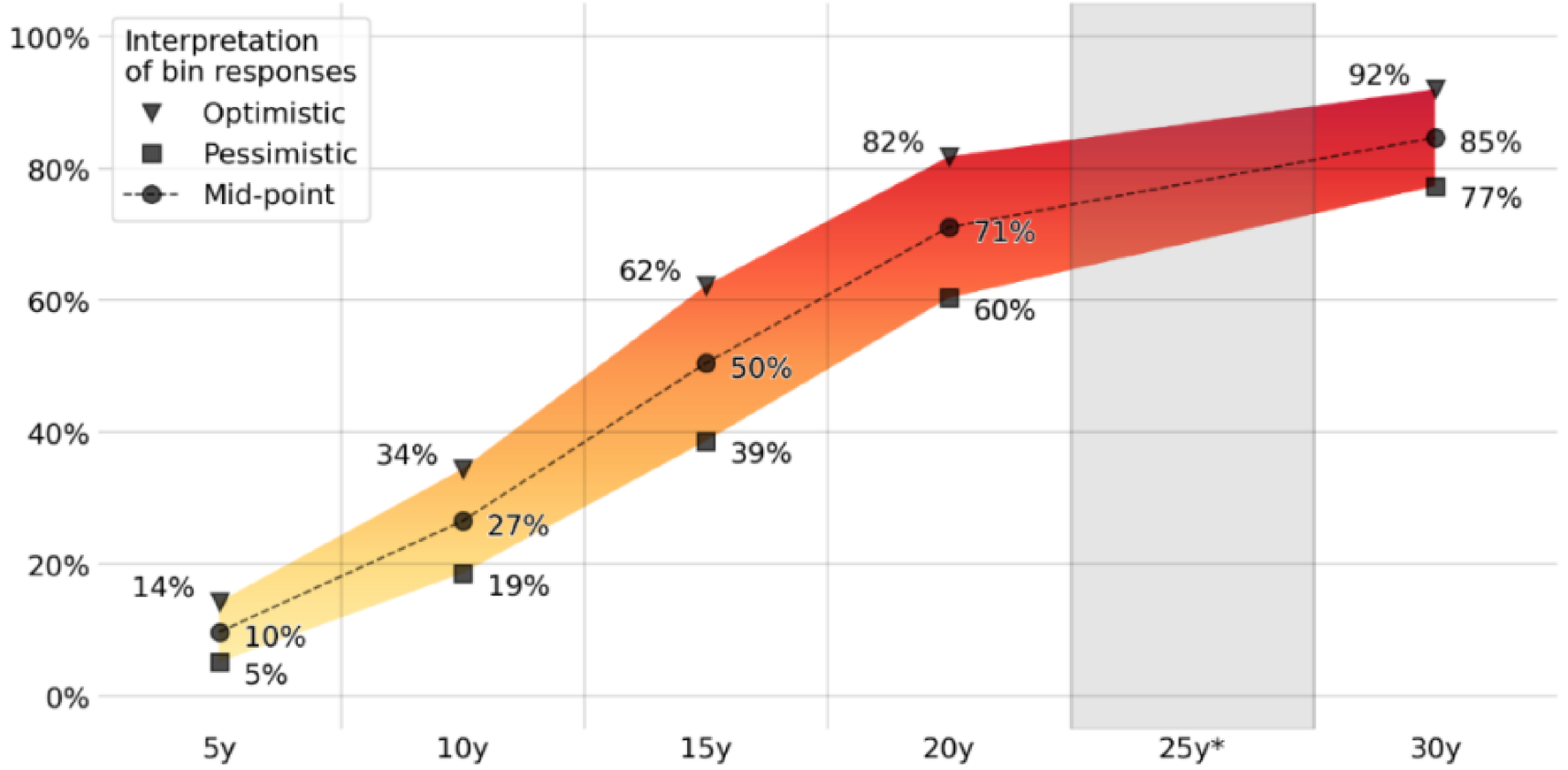


Migration is **costly** and **time consuming**

But urgency is not clear

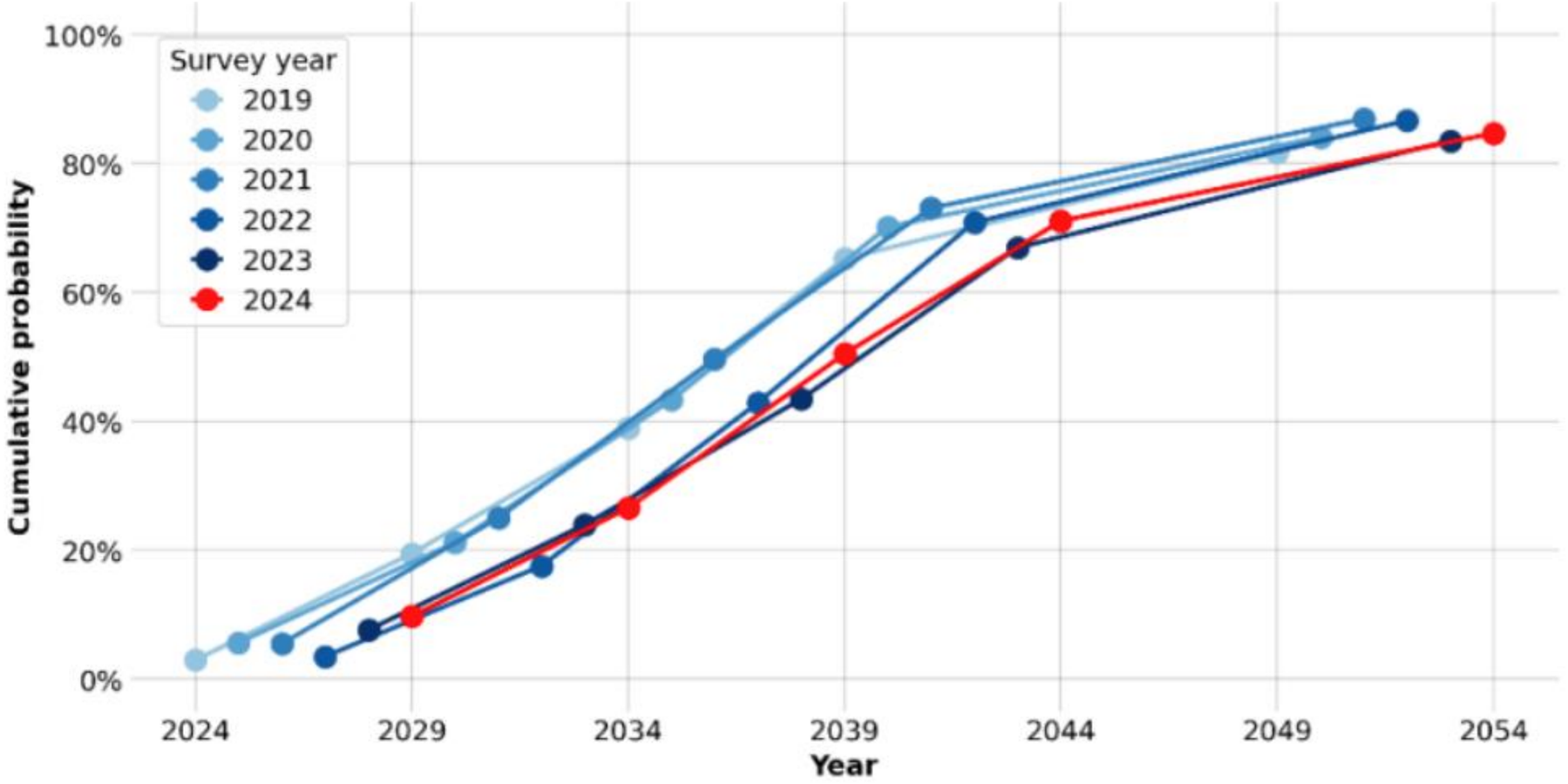
2024 OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the estimates indicated by the respondents, and mid-point. [*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]



OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: intermediate interpretation of the estimates indicated by the respondents. The estimates have been shifted based on the year of the survey.



Quantum Threat Timeline Report 2024 – Global Risk Institute

Timelines

BSI:

- The **most sensitive use cases** […] should be protected against ‘store now, decrypt later’ attacks as soon as possible, latest by the end of **2030**.

NIST:

- 112 bits of security deprecated after 2030
- All disallowed after 2035

Table 4: Quantum-vulnerable key-establishment schemes

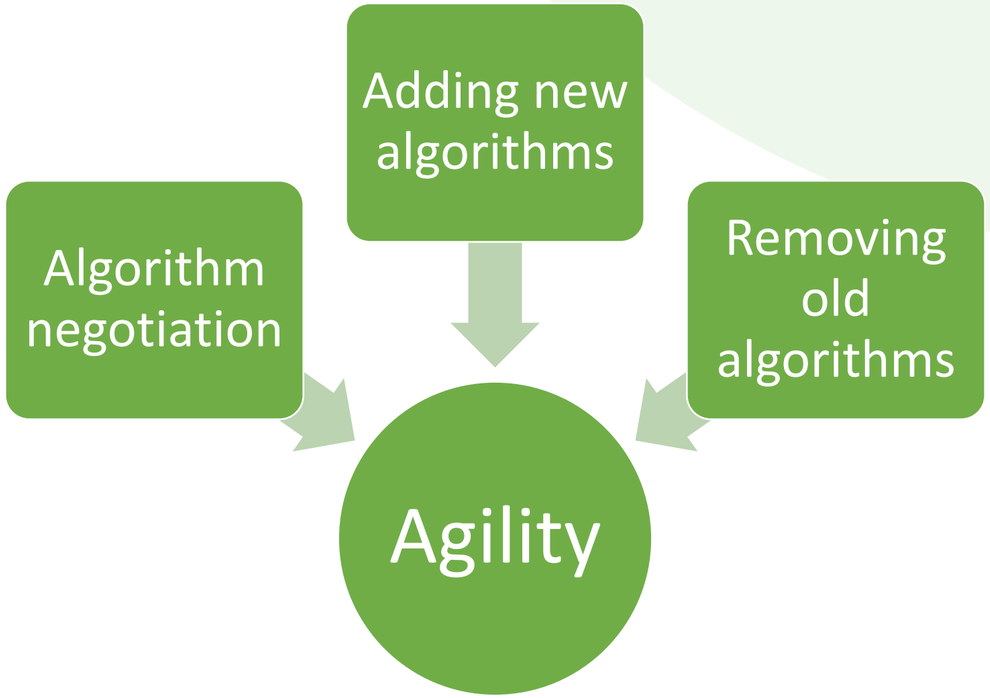
Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

NIST IR 8547: Transition to Post-Quantum Cryptography Standards (2024)

Cryptographic Agility

NIST describes crypto agility as:

- *The ability for machines to select their security algorithms in real time and based on their combined security functions;*
- *The ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features; and*
- *The ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete.*



The Need for Agility

- Algorithms getting broken
- Regulatory divergence
- Interoperability

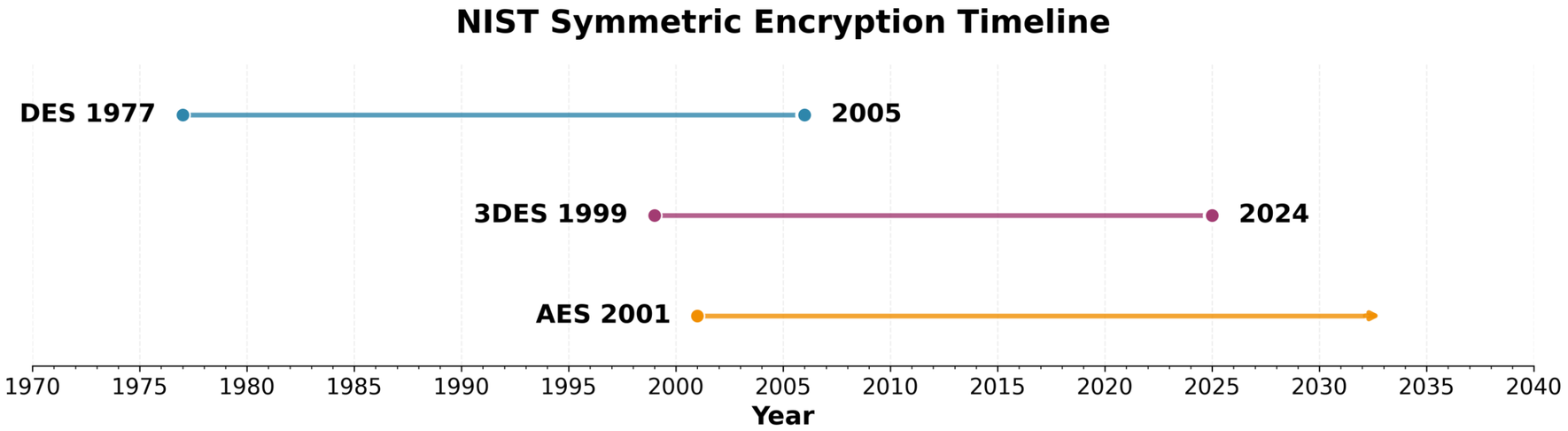
BSI:

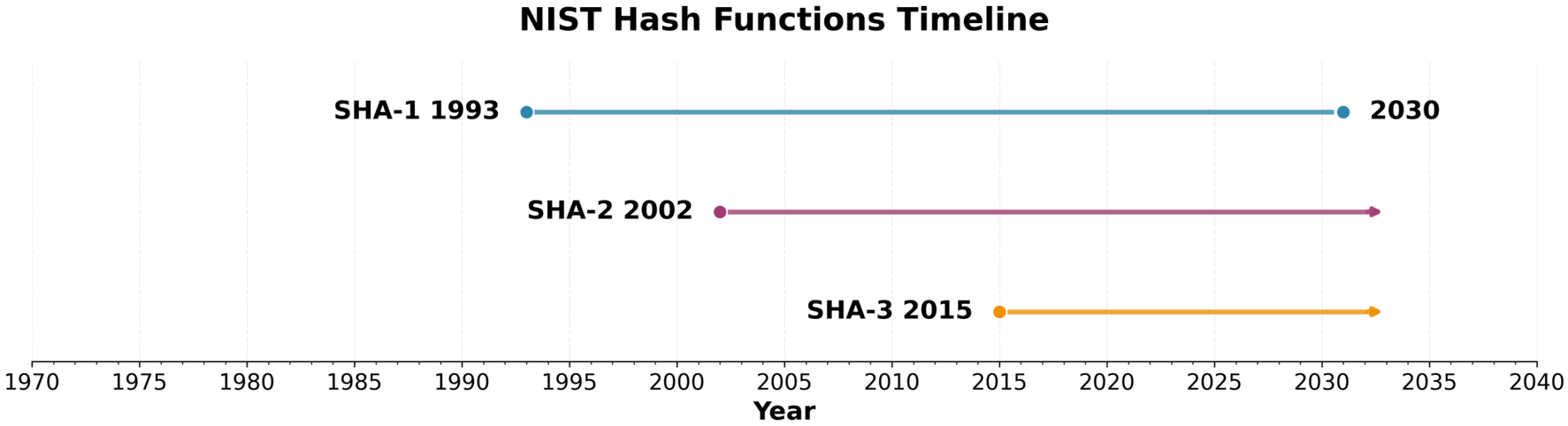
- Second core message is agility

NIST:

- Publication in March on Crypto Agility

Past Transitions





How to Achieve Agility

otpbank

- Modular software design
  - Crypto API
- Protocols should define cipher suites
- Algorithms should be negotiated
- Enable potentially increased future resource usage (3072 bit RSA ≈ 19360 bit ML-DSA)
- Reusable hardware accelerators

Risks from Agility

otpbank

- Increased complexity
  - Rarely used protocols – undiscovered bugs?
- Downgrade attacks
  - Negotiation has to be integrity protected

Challenges

- Vendor dependencies
  - Cloud providers
  - Mobile networks
  - Hardware

Current Efforts

otpbank

- Collect and maintain CBOM (Cryptographic Bill of Materials)
- Update policies
- Coordinate with suppliers

- Google: Tink cryptographic library (PQC WIP)

Questions?

Thank you!