Cryptography in 6G: Challenges and Opportunities

Iko Keesmaat, Sandesh Manganahalli Jayaprakash, Tiia Ojanperä, Thom Sijpesteijn

Thomas Attema | CWI & TNO

19 January 2024

Confidential 6G Project

- https://confidential6g.eu/

- Horizon Europe project
  - 2023 – 2024
  - 13 partners

- Focus:
  - Post-Quantum Security
  - Confidential Computing / Privacy Enhancing Technologies

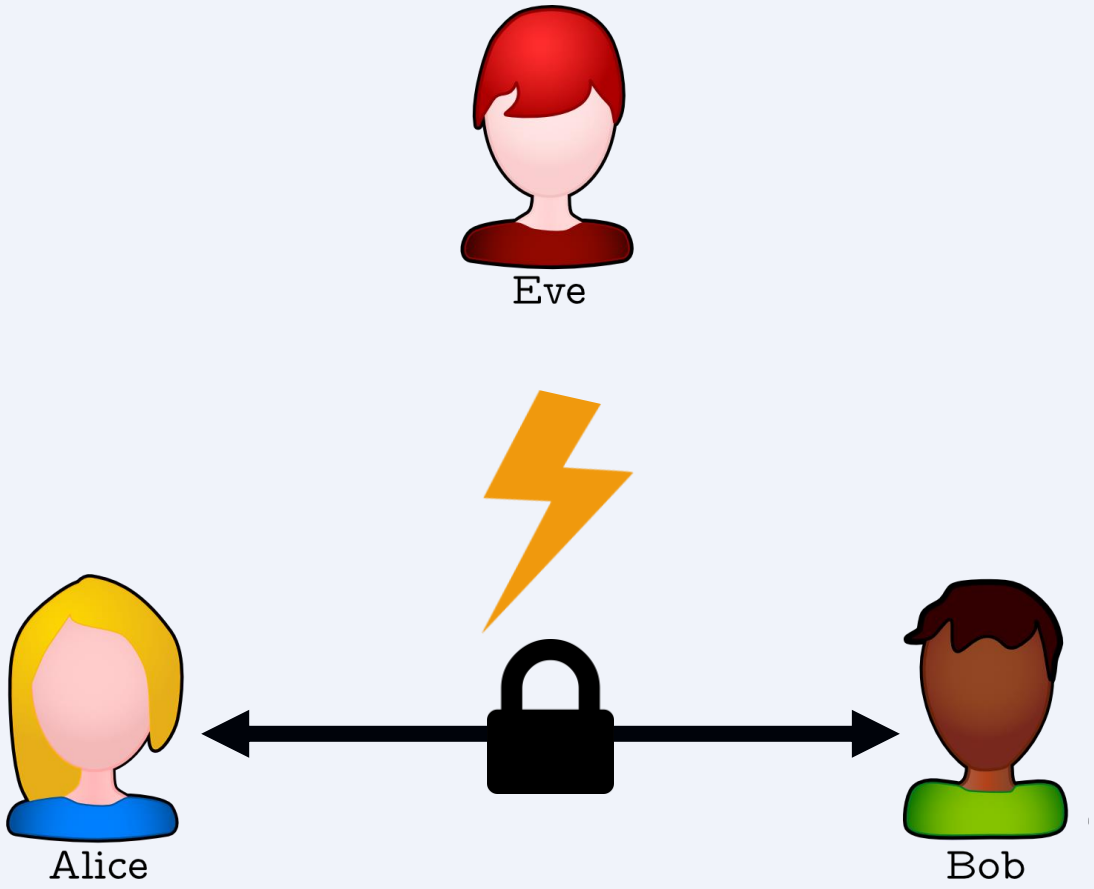
... in 6G

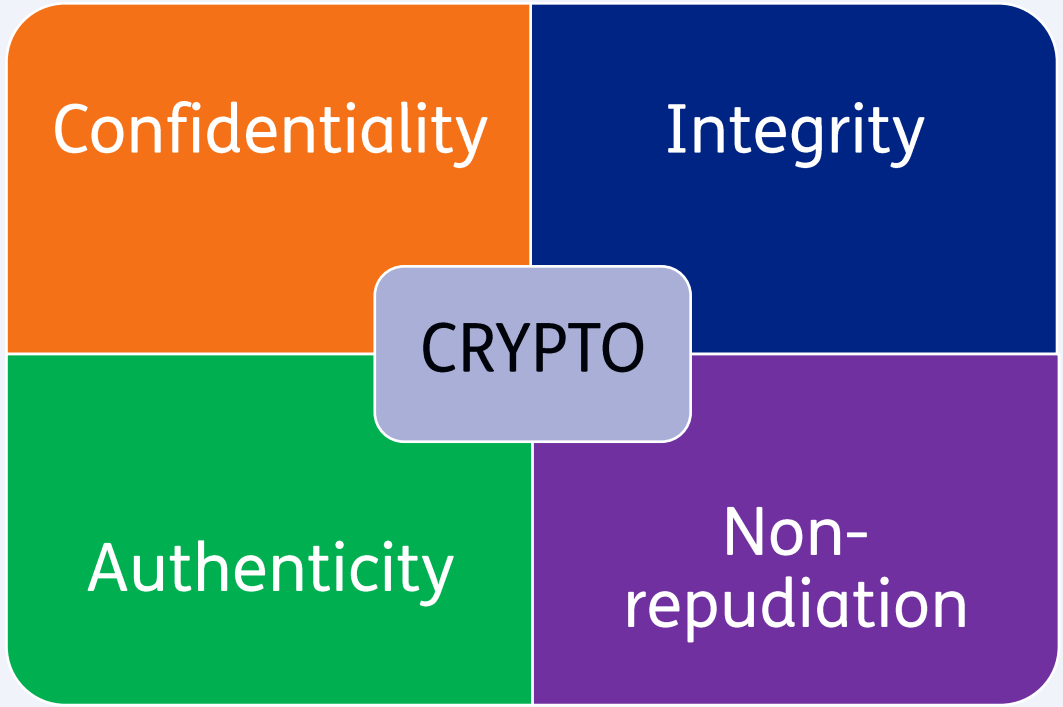
Agenda

Part I: Mitigating the Quantum Threat

Part 2: Privacy Enhancing Technologies

Cryptography

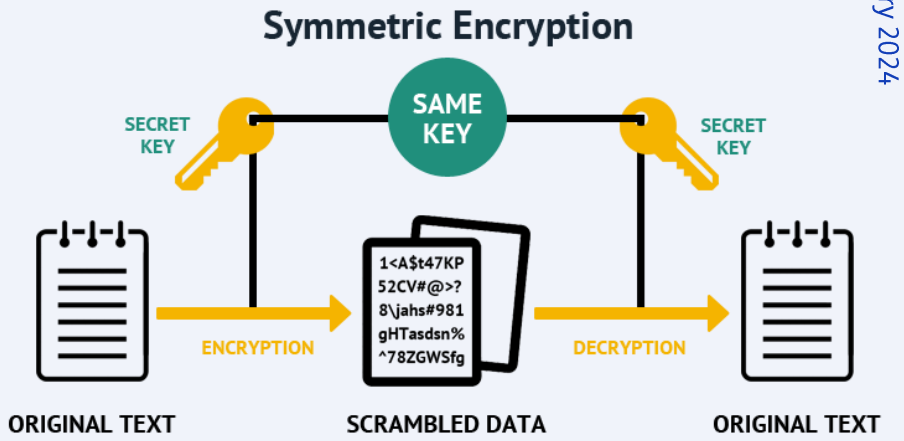




Cryptography – Two Categories

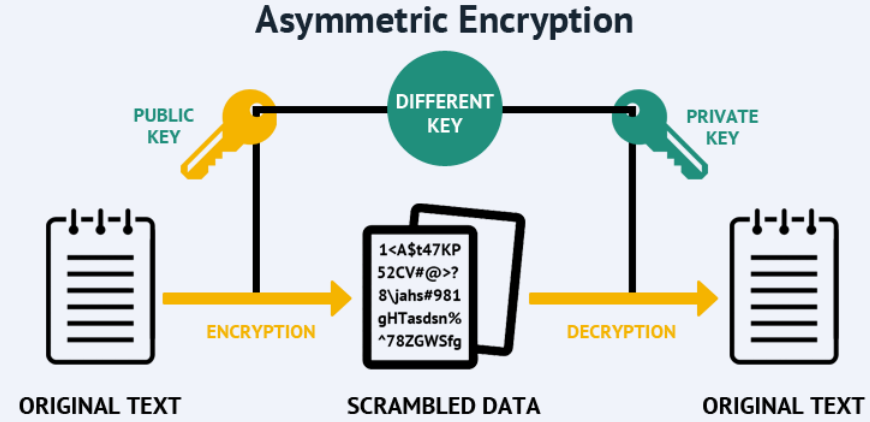
Symmetric Cryptography

- One key for both encryption and decryption
- Requires pre-arranging a shared secret key
- Examples: *AES, DES, Blowfish, Salsa20, ChaCha20*



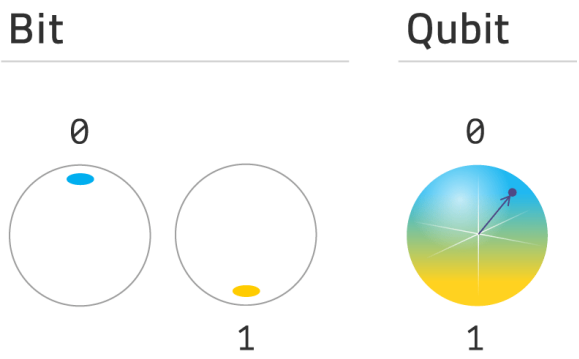
Asymmetric ("Public-Key") Cryptography

- Different keys for encryption (*public key*) and decryption (*private key*)
- Security based on "hard" mathematical problems
- Often used for exchanging/establishing symmetric key
- Examples: *RSA, DSA, ECDSA, Diffie-Hellman*



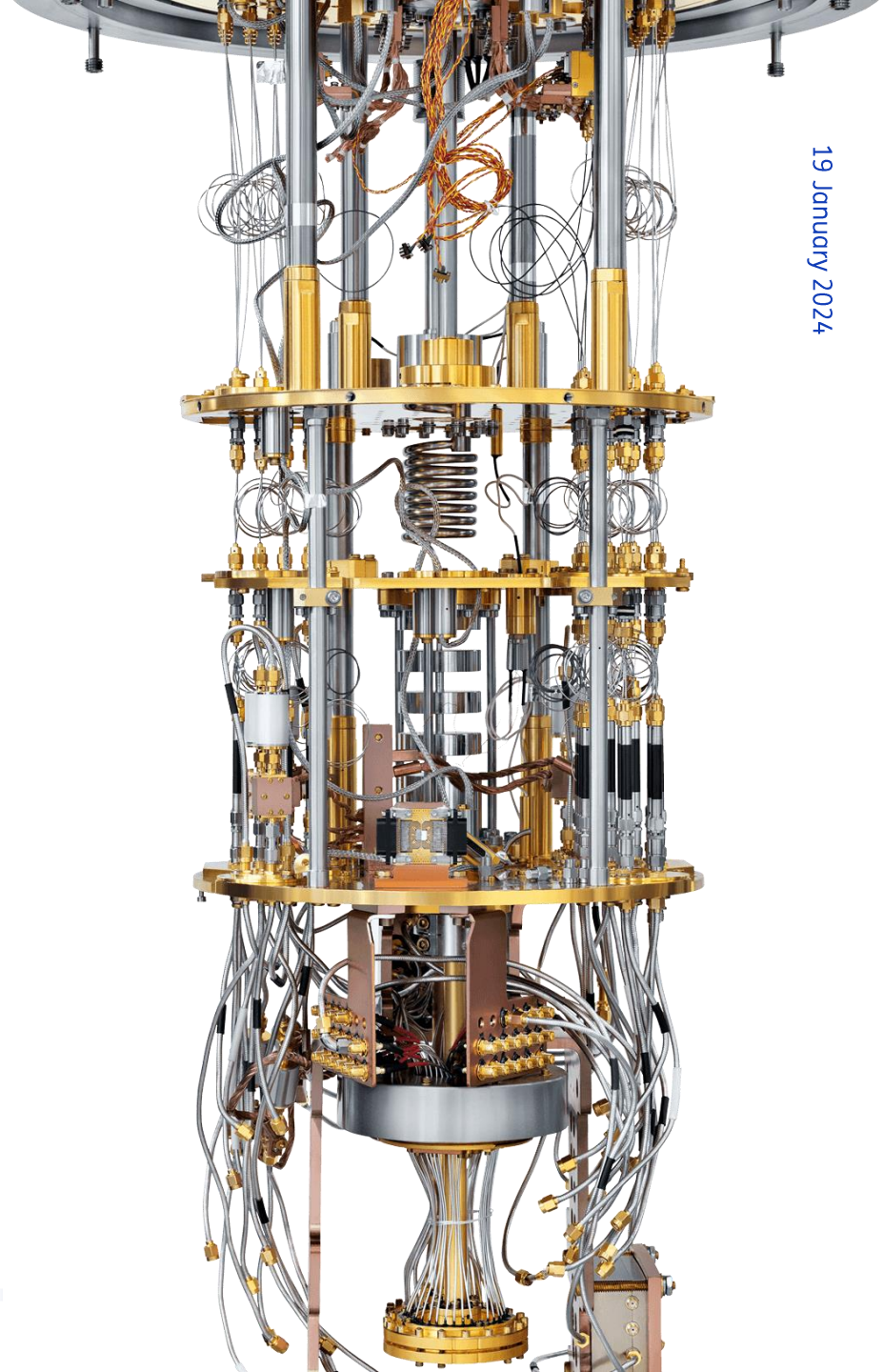
Quantum Computing

- Fundamentally different way of computation
- Makes use of so-called qubits rather than bits



- Various challenges: coherence, stability, scalability, error-correction
- Redefines which computational problems are “hard”

Quantum computer ≠ Supercomputer

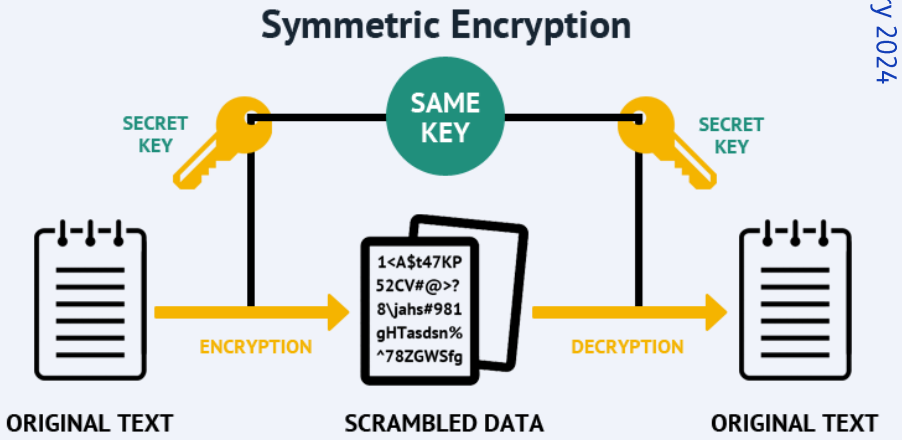


Cryptography – Two Categories

Symmetric Cryptography

- One key for both encryption and decryption
- Requires
- Examples: *AES, DES, Blowfish, Salsa20, ChaCha20*

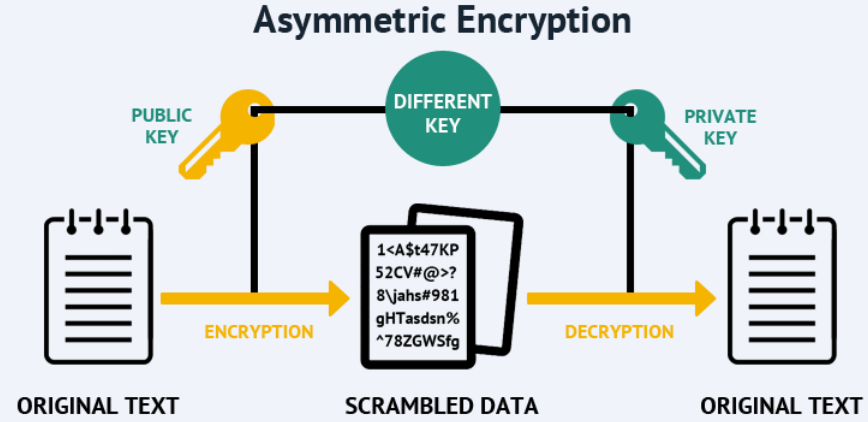
Weakened by quantum attacks (Grover's algorithm)



Asymmetric ("Public-Key") Cryptography

- Different keys for encryption (*public key*) and decryption (*private key*)
- Security based on mathematical "hard"
- symmetric key
- Examples: *RSA, DSA, ECDSA, Diffie-Hellman*

Completely broken by quantum attacks (Shor's algorithm)



Dealing with the Quantum Threat

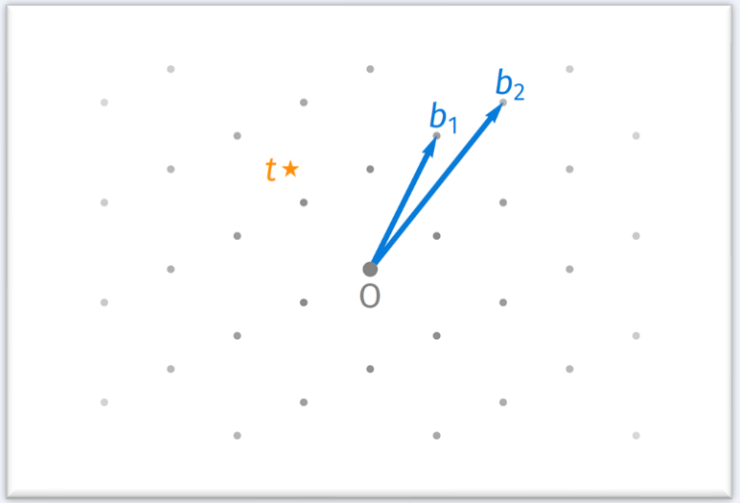
Symmetric Cryptography

- Only weakened by quantum attacks
- Doubling key length mitigates the threat posed by Grover's algorithm
- …and doubling key length is usually considered an "easy migration"

	Key Length (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Asymmetric ("Public-Key") Cryptography

- Introducing: **post-quantum cryptography**
- Based on different computational problems, believed to be quantum-hard
  - *Lattices, codes, hash functions, multivariate, isogenies, …*
- Generally not as efficient as classical cryptography: no drop-in replacement
- Migration to PQC is considered a large challenge



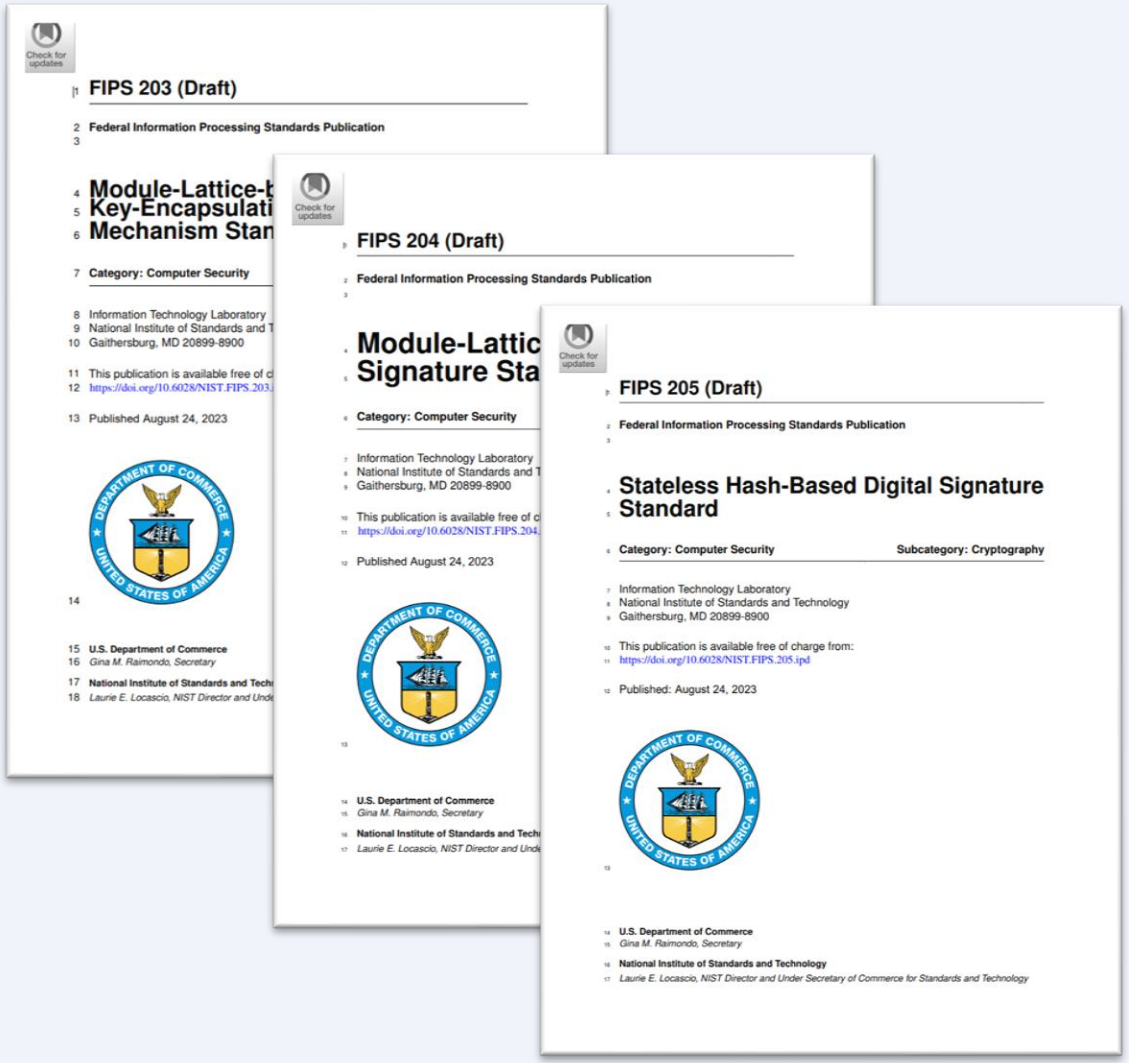
NIST Post-Quantum Standardization Competition

Timeline (2016 – present)

- **2016:** NIST call for submissions
- **2017:** Round 1: 69 candidates
- **2019:** Round 2: 26 candidates
- **2020:** Round 3: 7 finalists, 8 alternates
- **2022**: Announcement of
  - 4 winners (1 KEM, 3 SIG)
  - 4 alternates proceed to Round 4 (all KEMs)
  - New competition for additional SIG algos
- **2023**: First set of draft standards released

Future Timeline

- **2024**: First set of standards to be published
- **Later:** Additional standards (R4 + follow-up SIG)



Standardisation: Not Straightforward!

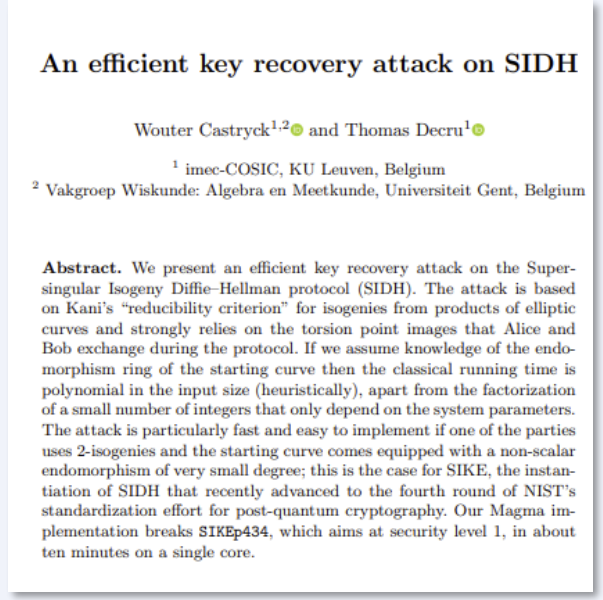
- The NIST Standardisation effort has been ongoing for since 2016
- Researchers have been validating the security of proposed schemes, yet:

July 2022

- SIKE was **completely broken** after being selected to pass to the 4th round for additional schemes
- Surprising: 6 years (!) after the start of the NIST procedure

December 2023

- *KyberSlash:* Side-channel attack on Kyber
- Not a fundamental flaw => vulnerability in some implementations
- For application in TLS with ephemeral keys, the problem does not constitute an immediate vulnerability

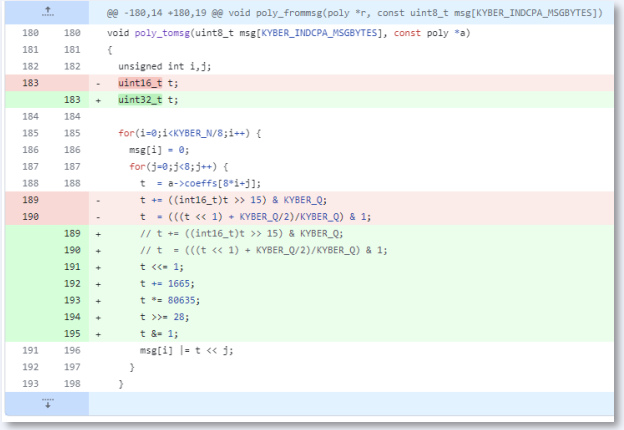


An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

Abstract. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH). The attack is based on Kani's "reducibility criterion" for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve then the classical running time is polynomial in the input size (heuristically), apart from the factorization of a small number of integers that only depend on the system parameters. The attack is particularly fast and easy to implement if one of the parties uses 2-isogenies and the starting curve comes equipped with a non-scalar endomorphism of very small degree; this is the case for SIKE, the instantiation of SIDH that recently advanced to the fourth round of NIST's standardization effort for post-quantum cryptography. Our Magma implementation breaks **SIKEp434**, which aims at security level 1, in about ten minutes on a single core.

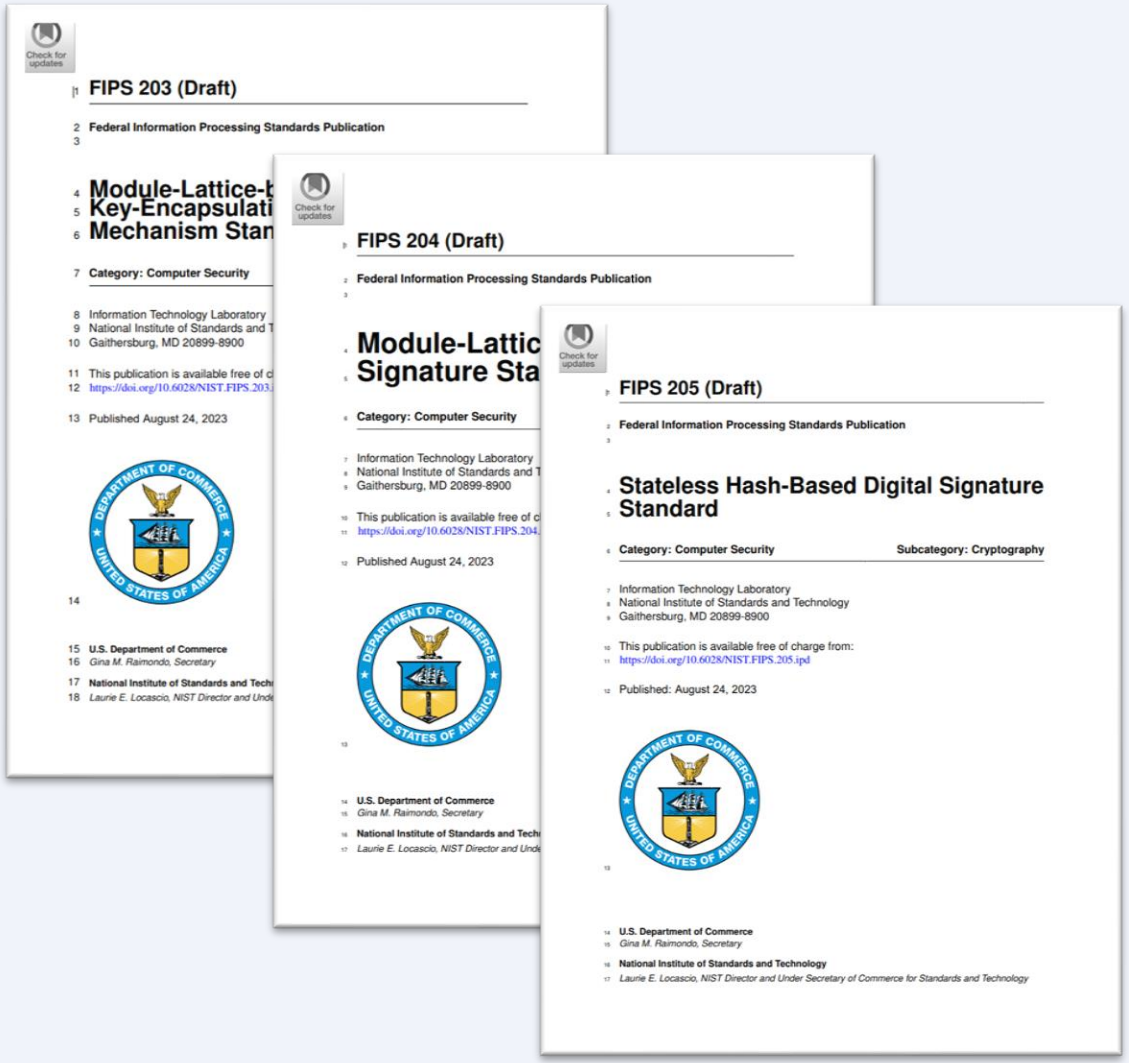


```
@@ -180,14 +180,19 @@ void poly_frommsg(poly *r, const uint8_t msg[KYBER_INDCPA_MSGBYTES])
180 180  void poly_tomsg(uint8_t msg[KYBER_INDCPA_MSGBYTES], const poly *a)
181 181  {
182 182    unsigned int i,j;
183     -  uint16_t t;
    183 +  uint32_t t;
184 184
185 185    for(i=0;i<KYBER_N/8;i++) {
186 186      msg[i] = 0;
187 187      for(j=0;j<8;j++) {
188 188        t  = a->coeffs[8*i+j];
189     -      t += ((int16_t)t >> 15) & KYBER_Q;
190     -      t  = (((t << 1) + KYBER_Q/2)/KYBER_Q) & 1;
    189 +      // t += ((int16_t)t >> 15) & KYBER_Q;
    190 +      // t  = (((t << 1) + KYBER_Q/2)/KYBER_Q) & 1;
    191 +      t <<= 1;
    192 +      t += 1665;
    193 +      t *= 80635;
    194 +      t >>= 28;
    195 +      t &= 1;
191 196        msg[i] |= t << j;
192 197      }
193 198    }
```

Do we really have to migrate to PQC?

- The timelines for *cryptographically relevant quantum computers* are still very unclear
- Some quantum sceptics even doubt whether we'll ever see a sufficiently stable and large quantum computer at all

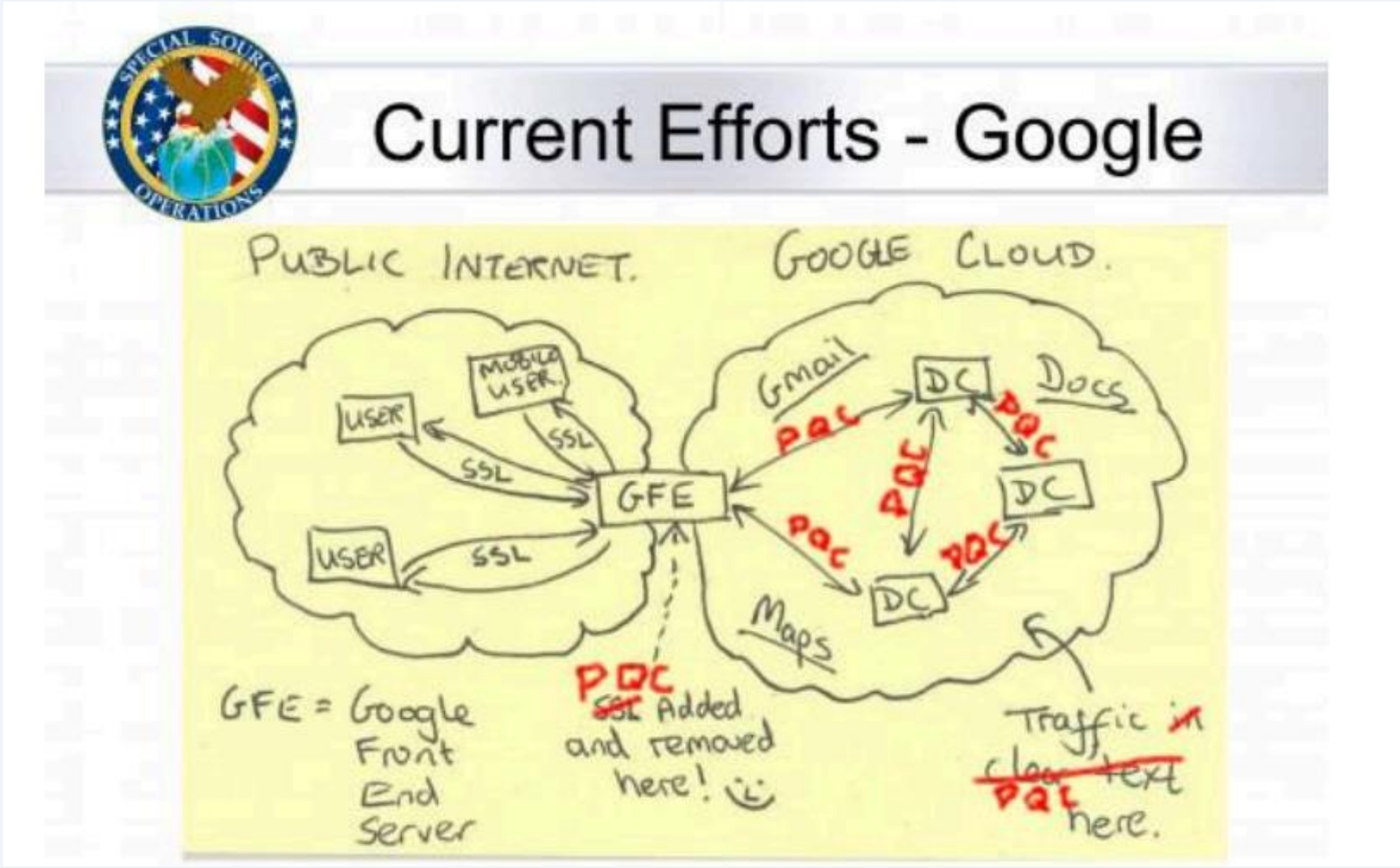
- **BUT:**
  - Impact of cryptographically relevant QC is huge
  - *Store now, decrypt later* attacks
  - Long-lived systems (e.g., 6G) must consider future threats
  - Compliance - standards are coming
  - Interoperability - large organisations (e.g. Google, Cloudflare) are already moving



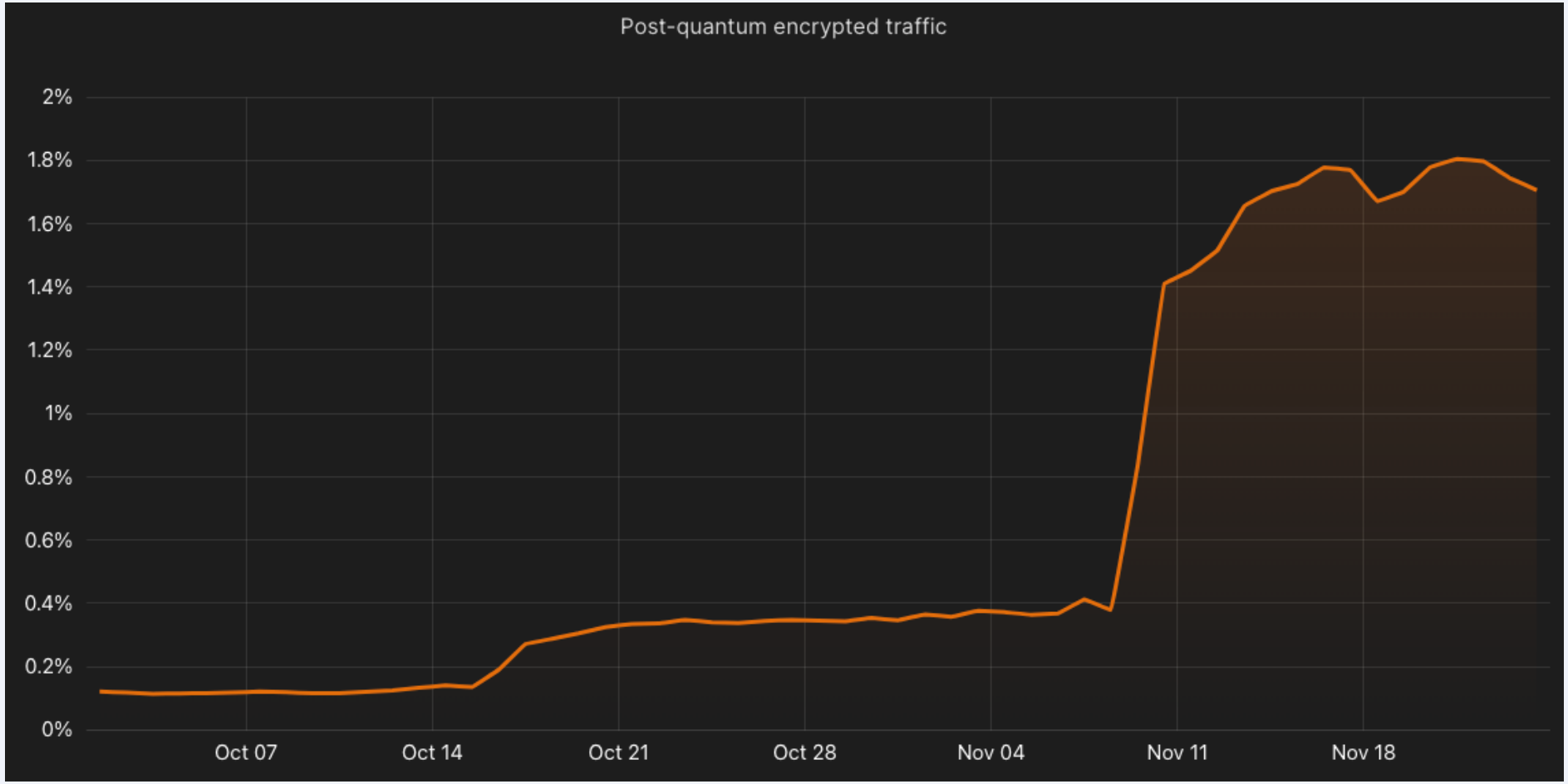
2022: US White-House Memorandum

- *May 2022*
- *“It directs specific actions for agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography”*

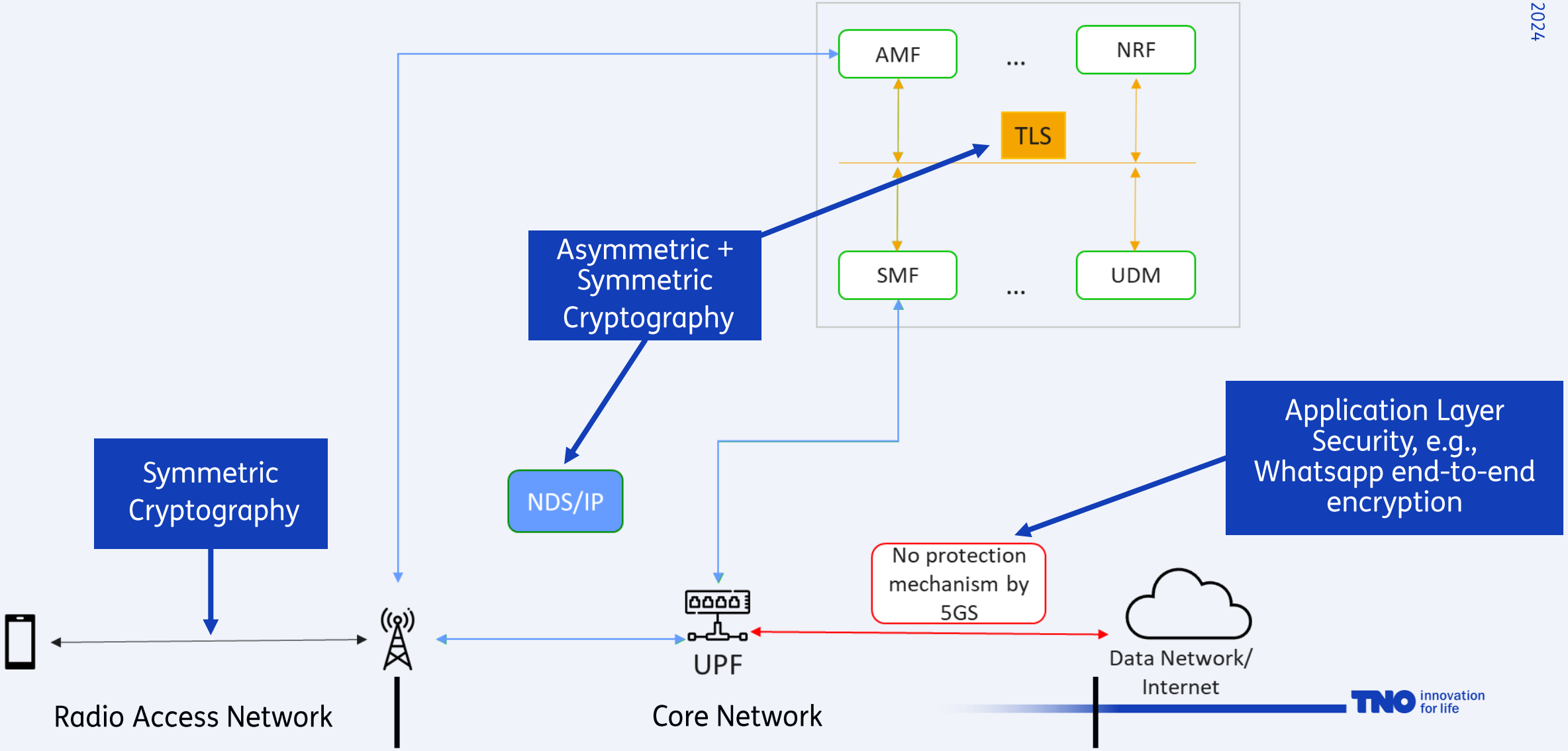
2022: Google's Internal Network uses PQC



12-2023: Cloudflare 1.7% of TLS 1.3 Connections Uses PQC



Non-Roaming 5G Architecture



Symmetric Key Cryptography

- Replacing 128 bit scheme with 256 bit is not a simple switching activity within 5G. It comes up with a need for detailed work.
- Currently this is being pursued in 3GPP standardisation within SA3 group.

3GPP TSG-SA3 Meeting #113
Chicago, USA, 6 - 10 November 2023

S3-235091
(revision of S3-234517)

Source:	**KDDI Corporation**
Title:	**New SID on study on enabling a cryptographic algorithm transition to 256-bits**
Document for:	**Approval**
Agenda Item:	**6.2**

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: Study on enabling a cryptographic algorithm transition to 256-bits

Supporting IM name
KDDI
BSI
Deutsche Telekom
Motorola Solutions
Nokia
US NSA
Lenovo
NCSC
MITRE
Samsung
NDRE
Ericsson
THALES
Johns Hopkins University APL
Apple
Huawei
KPN
IDEMIA
NIST
BMWK

3GPP TSG-SA3 Meeting #113
Chicago, US, 6 - 10 november 2023

S3-235072
(revision of S3-234681)

Source:	**Thales, Idemia, NIST, ORANGE, Nokia, Telecom Italia**
Title:	**New WID on Milenage-256 algorithm**
Document for:	**Approval**
Agenda Item:	**6.2**

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title:

New WID on addition of Milenage-256 algorithm

Asymmetric Cryptography Requires New Primitives

	Features			Speed			Memory		
	QUANTUM-SAFE?	STANDARD-ISED	CONFIDENCE[1]	KEY GEN	ENCRYP-TION/ SIGNING	DECRYP-TION/ VERI-FICATION	PUB KEY	PRIV KEY	CIPHERTEXT/ SIGNATURE
RSA (KE)									
Elliptic-curve (KE)									
CR.-KYBER (KE)									
FrodoKEM (KE)									
McEliece (KE)									
BIKE (KE)									
HQC (KE)									
CR.-DILITHIUM (DSS)									
FALCON (DSS)									
SPHINCS+ (DSS)									

19 January 2024

Part II:

Privacy Enhancing Technologies

6G Developments and Their Impact to Privacy/Confidentiality

6G Developments	Privacy/Confidentiality Concerns
• Higher throughput/lower latency • Simplifies data sharing	Potential increased sharing of sensitive/confidential information

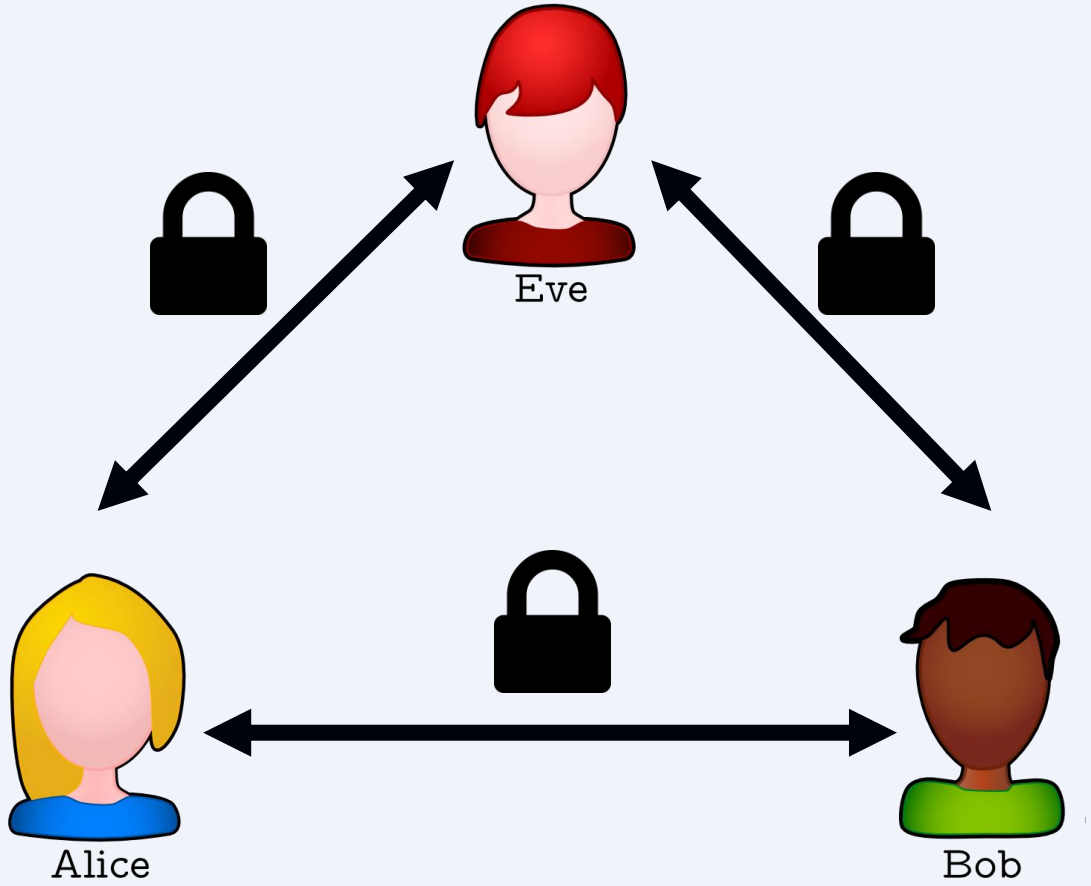
• Edge computing
  • Low latency
  • Less resources required => reduce energy consumption
	Edge nodes may not be trusted

• AI-powered networks
  • Advanced AI algorithms optimizing network management/routing
  • E.g., network data analytics function (NWDAF)
	AI algorithm consumes user data

Privacy Enhancing Technologies

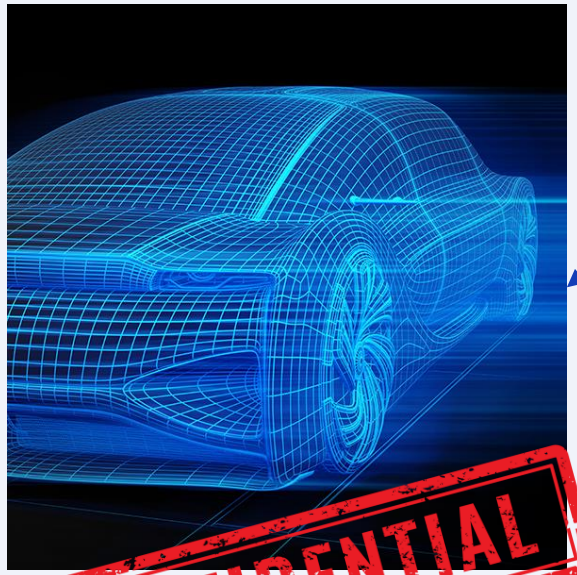
- Collaborate with untrusted parties

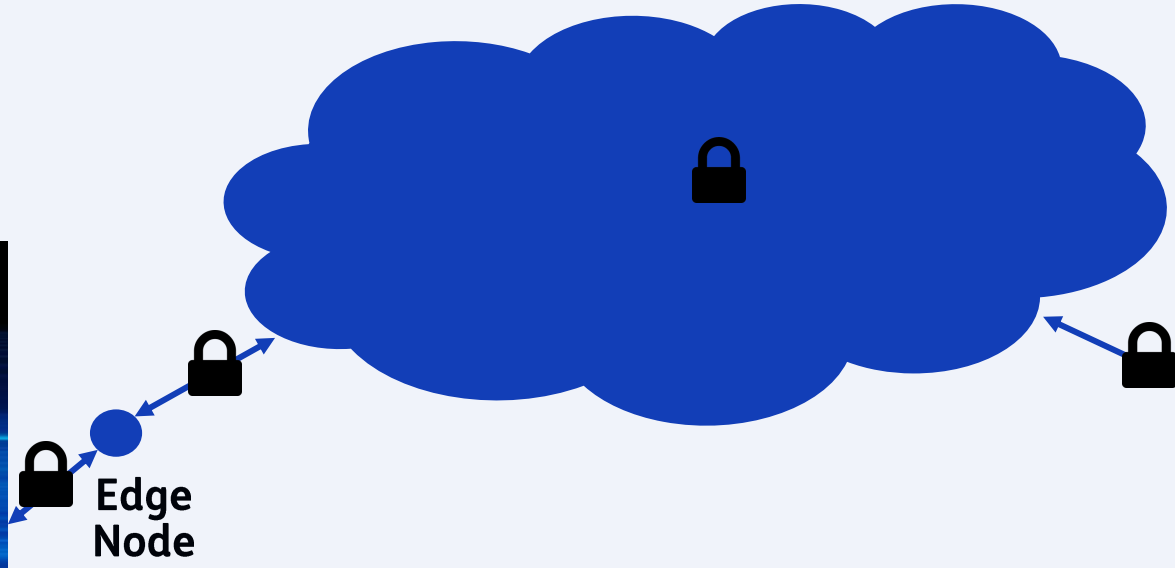
- Many different techniques
  - (Fully) Homomorphic Encryption
  - Multi-party computation
  - Federated Learning
  - Trusted Execution Environments
  - …



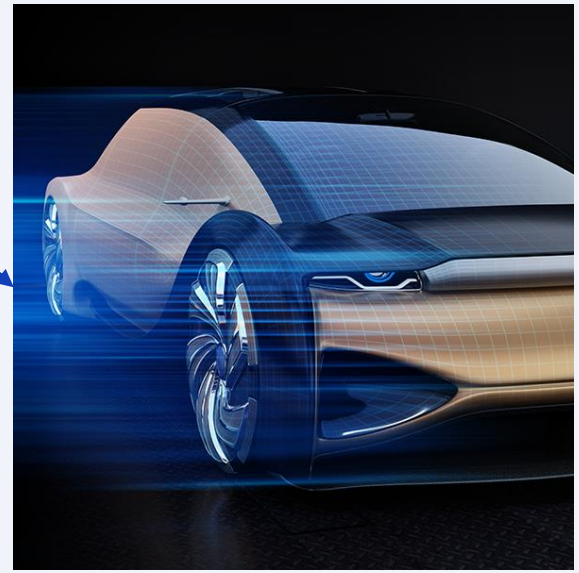
Digital Twin for (Predictive) Maintenance

Digital Twin - Manufacturer





Physical Car – (Predictive) Maintenance



"Traditional" Solution:
end-to-end encryption

Appears incompatible with edge computing

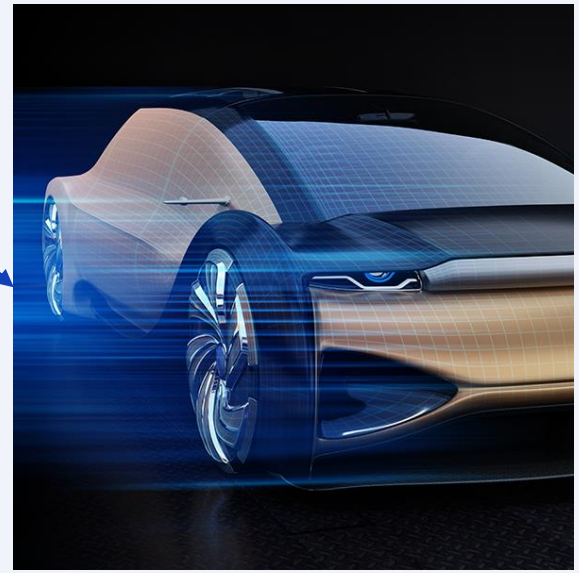
Digital Twin for (Predictive) Maintenance Edge Computing

Digital Twin - Manufacturer

Edge Node

Edge Node

Physical Car – (Predictive) Maintenance



Only applicable if edge node is trusted

Research Question:

Can we use PETs in case of untrusted edge nodes?

Concluding Remarks

- 6G should accommodate post-quantum cryptography (PQC)
  - PQC may impact performance
  - PQC standards will be ready soon, but many more developments may be expected

    => aim for cryptographic agility

- 6G introduces new privacy/confidentiality concerns
  - Privacy Enhancing Technologies may offer solutions

Questions?

TNO innovation for life