ANALYSIS AND IMPLEMENTATION OF SECURITY STANDARDS FOR CRITICAL INFRASTRUCTURES IN THE POST-QUANTUM ERA

Niki - Aikaterini Kyriakatou, Kyriaki Tsantikidou, Nicolas Sklavos

SCYTALE Group,

Computer Engineering and Informatics Department,

University of Patras, Greece

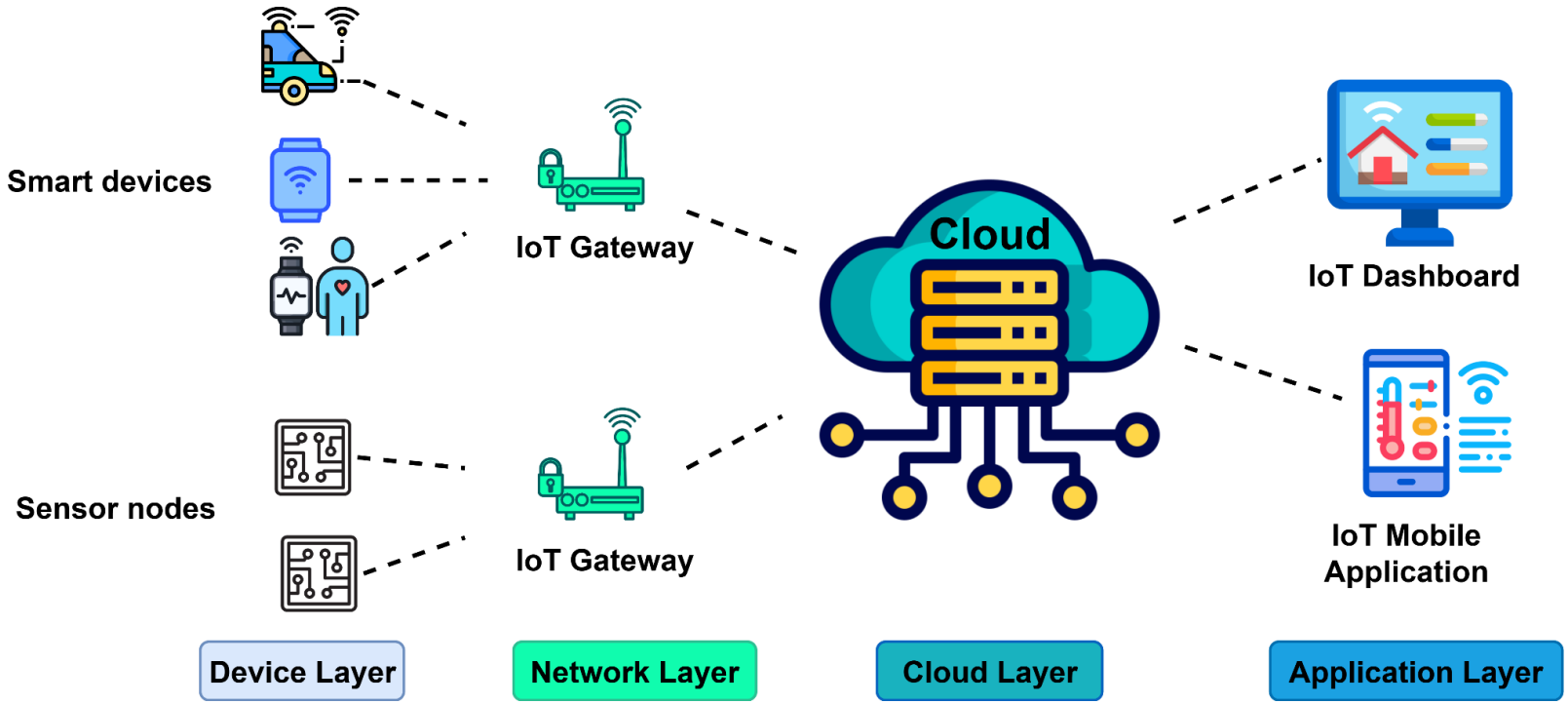
Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- Privacy-Enhancing Cryptography.
- Discussion of Experimental Standardized Framework.
- Conclusions.

Why security in IoT matters?

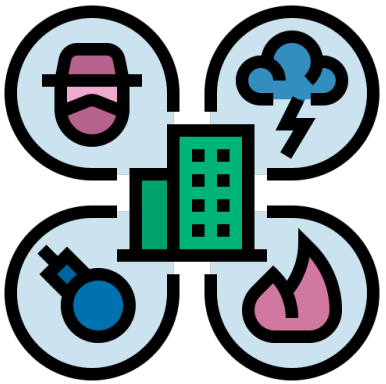
Over **billions of IoT and edge devices** are projected in 5G/6G ecosystems spanning from wearable and vehicles to industrial control systems.

The scale and heterogeneity of IoT ecosystems pose unprecedented security challenges.



Critical Infrastructures at Risk

- **Critical Infrastructure Dependency:**
  - **Healthcare,**
  - **transportation,**
  - **energy,**
  - **defense and national security.**



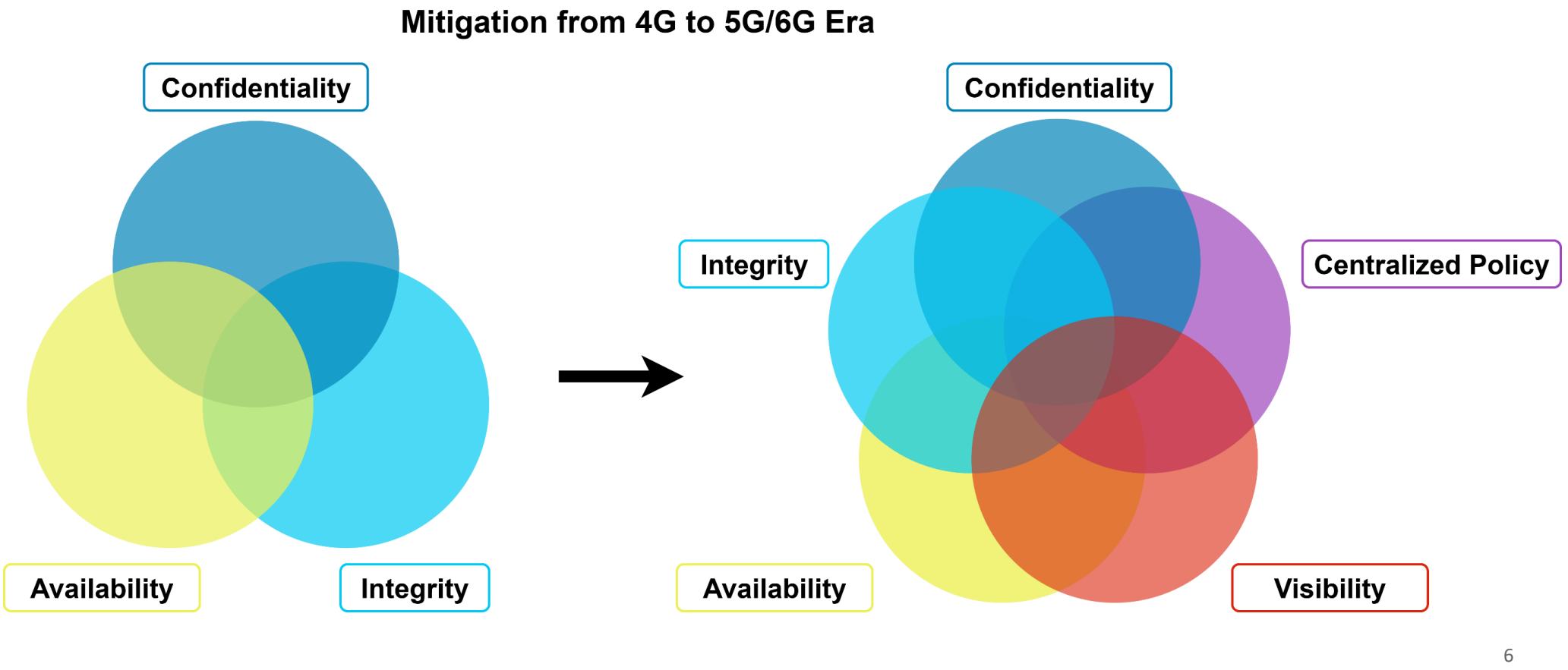
- **High-Stakes Consequences:**
  - Downtime: economic disruption and loss of trust.
  - Safety risks in life-critical systems.
  - Privacy breaches on a massive scale.

The Weakest Link Problem

- **Expanded attack surface:**
  - **Edge nodes** with limited resources are easy entry points.
  - **Smart devices** often lack strong cryptography.
  - **Gateways** act as single points of compromise.

A system as secure as its weakest layer. One compromised node can undermine the entire infrastructure.

Security Model Evolution: From 4G to 5G/6G



Quantum Threats to Classical Cryptography

- **Shor's algorithm** can compromise public-key cryptosystems, such as RSA, DSA and ECC, by solving the underlying factorization and discrete logarithm problems in polynomial time.

- **Grover's algorithm** reduces symmetric key strength by a square root factor undermining symmetric key cryptosystems such as AES.
- Long term confidentiality of current encrypted data is threatened. Data harvested today could be decrypted in the future ("**harvest now, decrypt later**").
- As a result, there is an urgent need to adopt **Post-Quantum Cryptography** (PQC).

Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- Privacy-Enhancing Cryptography.
- Discussion of Experimental Standardized Framework.
- Conclusions.

Core Pillars of Post-Quantum Cryptographic Design

Key Encapsulation Mechanisms (KEM):

- Facilitate secure symmetric key exchange over untrusted channels.
- Form the foundation of hybrid and quantum-resilient communication protocols.

Digital Signature Schemes:

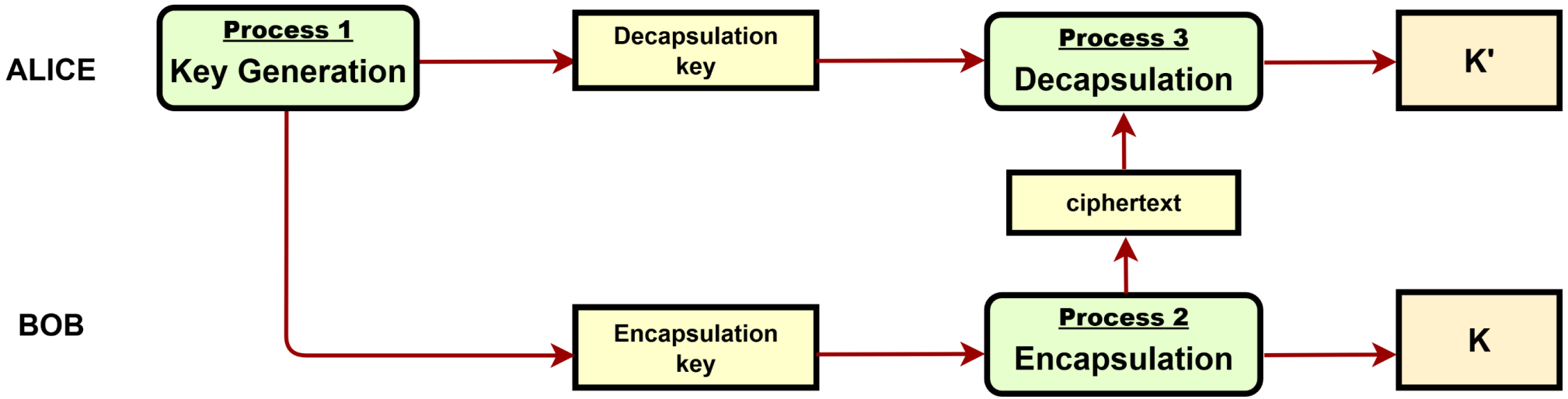
- Provide authenticity, integrity, and non-repudiation of data and software.
- Crucial for firmware updates, digital identities, and blockchain resilience.

Hash-Based Cryptographic Primitives:

- Offer resistance against Grover's preimage attacks and enable stateless verification.
- Underpin quantum-resilient signature schemes and authentication protocols.

FIPS 203 – Module Lattice KEM

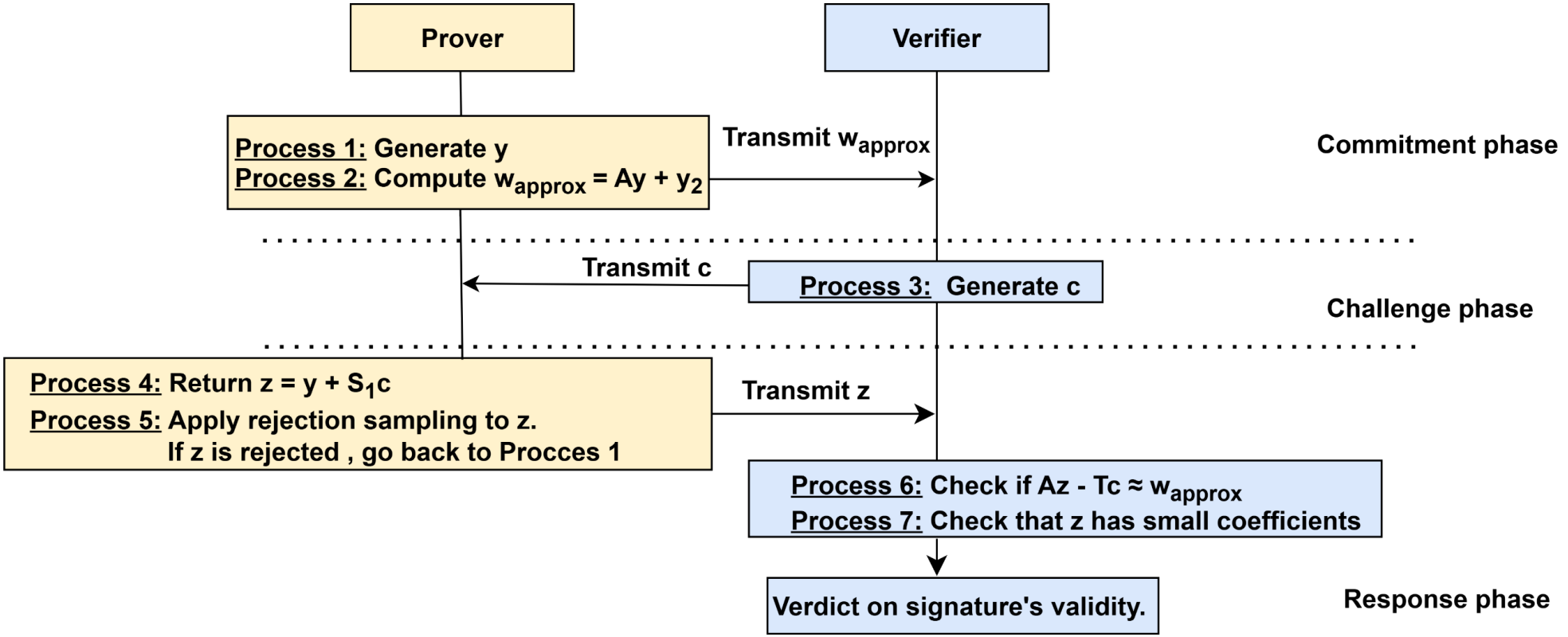
FIPS 203 enables the secure establishment of a shared secret key between two parties over a public channel.



FIPS 203 – Module Lattice KEM

Version	Key Sizes	Mitigation	Security Mechanisms
ML-KEM-512 (128 bits)	**Encaps:** 800 B **Decaps:** 1632B **Cipher:** 768B **SSKey:** 32 B	• IND-CCA2	1)MLWE Problem 2)Fujisaki-Okamoto Transform
ML-KEM-768 (192 bits)	**Encaps:** 1184 B **Decaps:** 2400 B **Cipher:** 1088B **SSKey:** 32 B		
ML-KEM-1024 **(**256 bits)	**Encaps:** 1568 B **Decaps:** 3168 B **Cipher:** 1568B **SSKey:** 32 B		

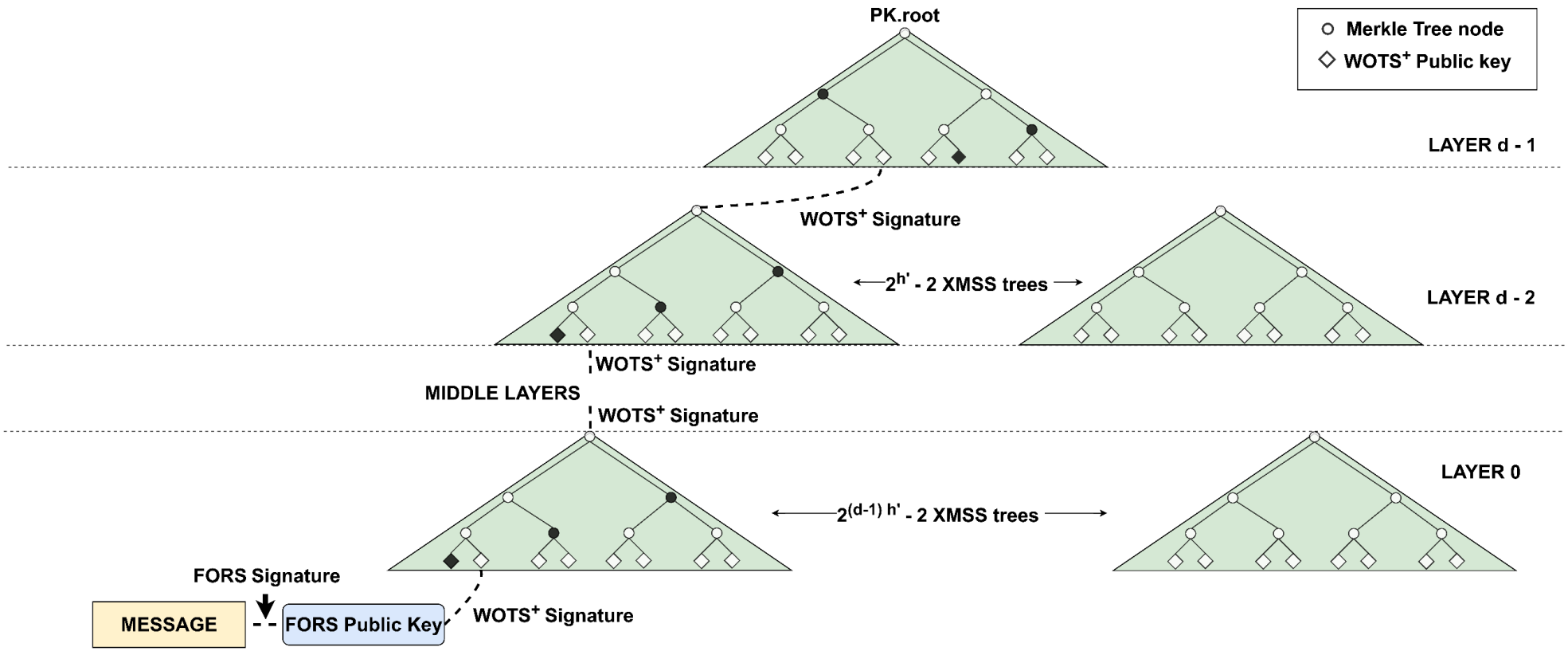
FIPS 204 – Interactive protocol



FIPS 204 – Module Lattice Digital Signature

Version	Key Sizes	Mitigation	Security Mechanisms
ML-DSA-44 (128 bits)	**PKey:** 2560 B **SKey:** 1312 B **Sign:** 2420 B	• SUF-CMA • Exclusive Ownership • Message Bound • Non-re-signability	1)MLWE Problem 2)Self-Target-MSIS 3)ZKPoP /Fiat-Shamir with abords
ML-DSA-65 (192 bits)	**PKey:** 2560 B **SKey:** 1312 B **Sign:** 2420 B		
ML-DSA-87 (256 bits)	**PKey:** 2560 B **SKey:** 1312 B **Sign:** 2420 B		

FIPS 205 – Structure



FIPS 205 – Stateless Hash-based Digital Signature

Version	Key Sizes	Mitigation	Security Mechanisms
SHA2-128s **SHAKE-128s**	**PKey:** 32B **Sign:** 7856 B	• EUF-CMA • Message Bound	1) Forest of Random Subsets (FORS) 2) Winternitz One Time Signature Plus (WOTS+) 3) eXtended Merkle Signature Scheme (XMSS)
SHA2-128f **SHAKE-128f**	**PKey:** 32 B **Sign:**17088 B		
SHA2-192s **SHAKE-192s**	**PKey:** 48 B **Sign:** 16224 B		
SHA2-192f **SHAKE-192f**	**PKey:** 48 B **Sign** 35664 B		
SHA2-256s **SHAKE-256s**	**PKey:** 64B **Sign:** 29792 B		
SHA2-256f **SHAKE-256f**	**PKey:** 64 B **Sign:** 49856 B		

The Lightweight Gap in PQC

- **PQC ≠ Universally Deployable:**
  FIPS 203, 204, and 205 offer strong post-quantum guarantees. Yet, their **large key/ ciphertext sizes** and **computational demands** limit applicability in constrained environments.

- **Constrained Platforms Rising:** Systems like **IoT nodes**, **RFID tags**, and **sensor networks** demand cryptographic efficiency in:
  - Memory footprint
  - Power consumption
  - Real-time responsiveness

Challenge: Design of cryptographic standards that **remain secure under real-world adversaries** while staying deployable on **embedded platforms**.

Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- Privacy-Enhancing Cryptography.
- Discussion of Experimental Standardized Framework.
- Conclusions.

Ascon: Tailored Cryptography for Constrained Platforms

Version	Key Sizes	Mitigation	Security Mechanisms
Ascon-AEAD-128 (128 bits)	**SKey:** 128 bits **Nonce:** 128 bits **A:** variable length **Tag:** $64 \leq \tau \leq 128$ **Cipher:** Text+τ bits	• State reuse and replay-based attacks • Collision-based forgery attacks	Double-keyed initialization and finalization Duplex construction
Ascon- Hash-256 (128 bits)	**M:** Variable length **Digest:** 256 bits	• Collision resistance • Preimage resistance • Second preimage resistance	Sponge based construction
Ascon-XOF-128 (min(L/2,128) bits)	**M:** Variable length **Digest:** L bits		
Ascon-CXOF-128 (min(L/2,128) bits)	**M:** Variable length **Z** $\leq$ 2048 bits **Digest:** L bits		

Ascon – Efficient Architecture

Design Insights:

- **Unified 320-bit permutation** across all modes: minimizes code & logic redundancy.
- **Single-pass, online encryption** avoids buffering full messages in memory.
- **Forward-only architecture:** no inverse needed. It is built using only **bitwise XORs**, **ANDs and rotations.**
- Built on **Boolean logic primitives**, enabling **bit-sliced execution** and compact code footprint.

Efficiency-Oriented Enhancements:

- Optional **truncation & nonce masking** for bandwidth-constrained use cases.
- **Little-endian alignment** matches common microcontroller architectures.

The limits of Ascon

Attack scenario:

An adversary with **quantum capabilities** targets a healthcare IoT network.

- At a **sensor level** Ascon ensures **fast, energy-efficient authenticated** encryption.
- At a **gateway/cloud level** the same lightweight hashes are deployed.

Adversarial power:

- **Brassard-Høyer-Tapp (BHT)** and related **quantum algorithms** executed on **quantum computers.**

Not every key fits every lock

Outcome:

- The adversary may exploit the reduced hardness of lightweight hash functions.
- This undermines the integrity of digital signatures, enabling forged updates, unauthorized commands, and system wide compromise.

Key Insight: The security of Ascon is not compromised by design but by **misapplication.** It is perfect for constrained nodes, yet **weak** to withstand quantum powered adversaries in more resource-rich layers.

To seal the system:

- **Ascon→ edge devices**.
- **PQC → gateways and cloud** infrastructures.

Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- **Privacy-Enhancing Cryptography.**
- Discussion of Experimental Standardized Framework.
- Conclusions.

Beyond Security: Privacy-Enhancing Cryptography

Integrity and confidentiality have been reinforced against classical and quantum threats.

Is this sufficient to achieve trust without sacrificing privacy?

Security ≠ Privacy

Attack scenario:

A cloud-based AI service processes encrypted healthcare IoT data utilizing only PQC.

- **PQC in place:** Keys are quantum safe, and signatures validated.
- **Weakness:** Data must be decrypted during computation, exposing sensitive content.

Adversarial power:

- Insider abuse within the cloud provider.
- Quantum-enabled adversaries exploiting decrypting states.

Security ≠ Privacy: Outcome

Outcome:

- Decryption at the computational layer exposes raw data to protentional adversaries within the cloud.
- Despite secure communication and storage, **privacy collapses at the point of computation.**
- Exposure of medical records undermines trust and may trigger catastrophic failures in safety and compliance.

Key insight:

- PQC seals data in transit and storage.
- PEC keeps data private even while being used.
- Robust Systems **combine PQC with PEC** to ensure **end-to-end protection,** even during computation or collaboration.

Overview and application domains of PEC Standards

	Security Basis	Primary Functionality	Complexity/ Cost	Application Domain
ZKPoP	Proof of knowledge over a secret without its disclosure.	• Structured reference strings (SRS) • Hash functions	Depends on the proof system.	• Privacy enabled databases • Privacy on blockchain systems • Secure communication protocols
MPC	Joint private computation.	• Secret sharing • Homomorphic encryption • Garbled circuits	High protocol complexity and communication overhead.	• Privacy preserving vote systems • Joint analytics/ collaborative computations • collaborative ML
FHE	Computation on Encrypted data.	• LWE • Ring-LWE	Very high due to bootstrapping.	• Encrypted cloud computing • Healthcare data analytics.

PEC – Enabling Visibility and Policy Enforcement

Privacy-Enhancing Cryptography (PEC) tools extend post quantum cryptography by securing how data is used and verified.

- **Visibility through proofs:**
  - **ZKPoP:** Verifiable actions without exposing raw data.
  - Auditable compliance with preserved confidentiality.
- **Centralized policy enforcement:**
  - **FHE:** Encrypted data remains usable under strict policies.
  - **MPC:** Enforces collaborative rules across distributed entities.

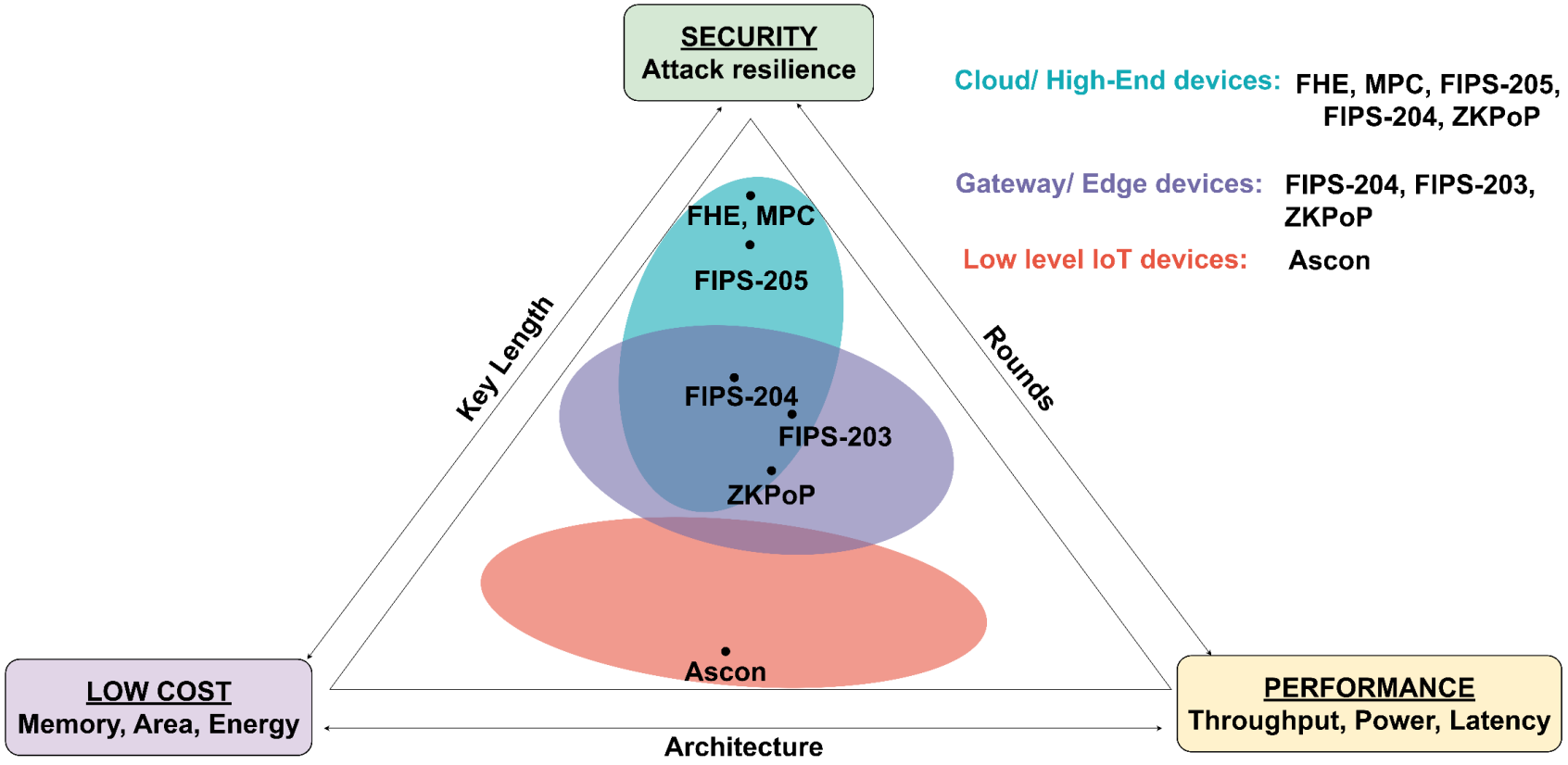
Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- Privacy-Enhancing Cryptography.
- Discussion of Experimental Standardized Framework.
- Conclusions.

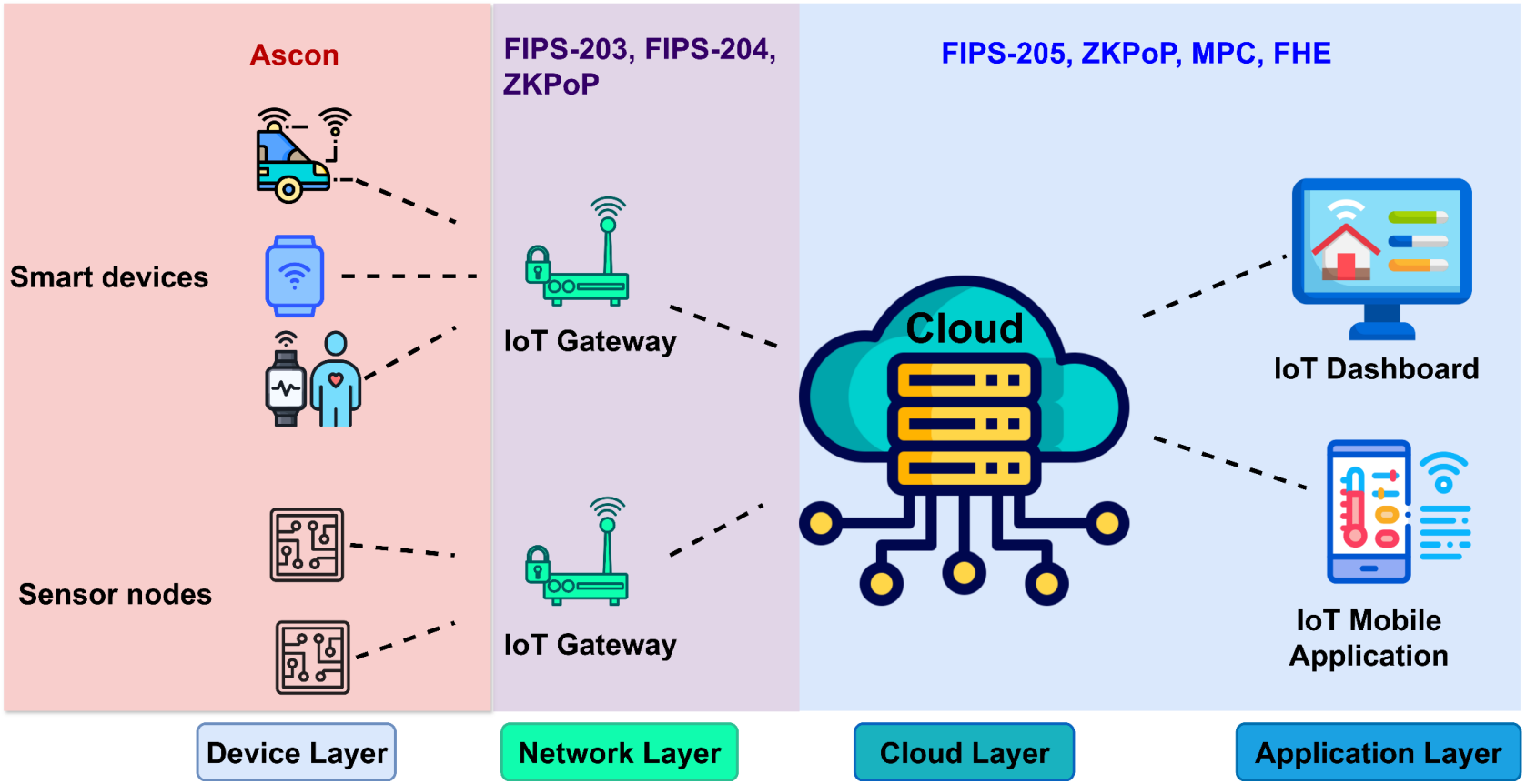
Hardware Cost Spectrum Across Standards

	Hardware cost
Ascon	Very Low / Minimal memory, CPU, and footprint.
FIPS 203	Moderate/ Requires polynomial arithmetic CPU, memory usage.
FIPS 204	Moderate/ Balanced trade-off of size vs. speed. NTT accelerates performance.
ZKPoP	Variable/ Cost depends on the proof system (e.g. Bulletproofs vs. zk-SNARKS).
FIPS 205	High / Large signature sizes
MPC	Very high/ Heavy protocol
FHE	Very high/ Bootstrapping dominates cost

Cryptographic Orchestration: Context-aware by Design



Sealed Layered Systems Framework



Presentation Outline

- Introduction and Motivation.
- PQC Standards.
- Lightweight Cryptography (Ascon suite).
- Privacy-Enhancing Cryptography.
- Discussion of Experimental Standardized Framework.
- Conclusions.

Conclusions: Interoperability over Isolation

Coordinating PQC and LWC:

- Standards are Complementary, not Competing**.** Their strength lies not in **universal deployment, but in coordinated coexistence.**
- **Hybrid deployments** like FIPS 203 and Ascon AEAD reflect real-world layered stacks (e.g., TLS 1.3).

Deployment Principle:

- PQC and LWC are not interchangeable but interdependent**.** A secure system must **map cryptographic roles to device capabilities,** forming an **adaptive and layered architecture.**

Privacy Dimension:

- PEC extends this model, ensuring trust is preserved not only through security, but also through **data confidentiality in use.**