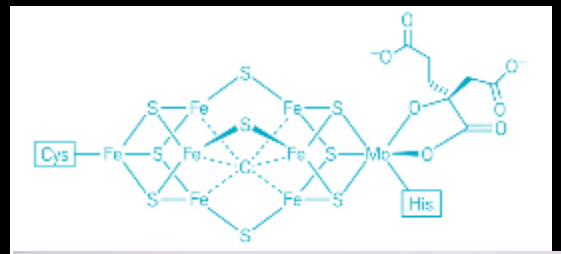
Security Hybridization: Towards Quantum-secure Communication Systems

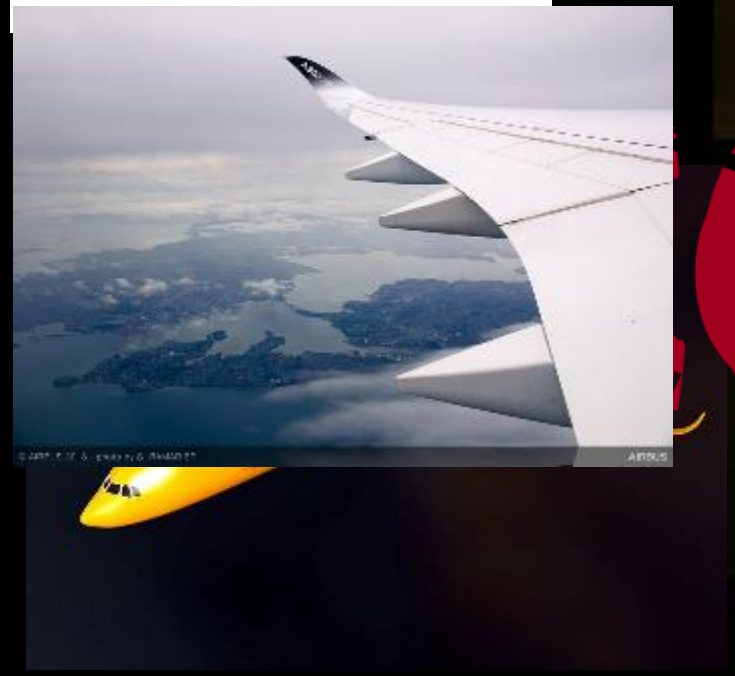
DEFENCE AND SPACE

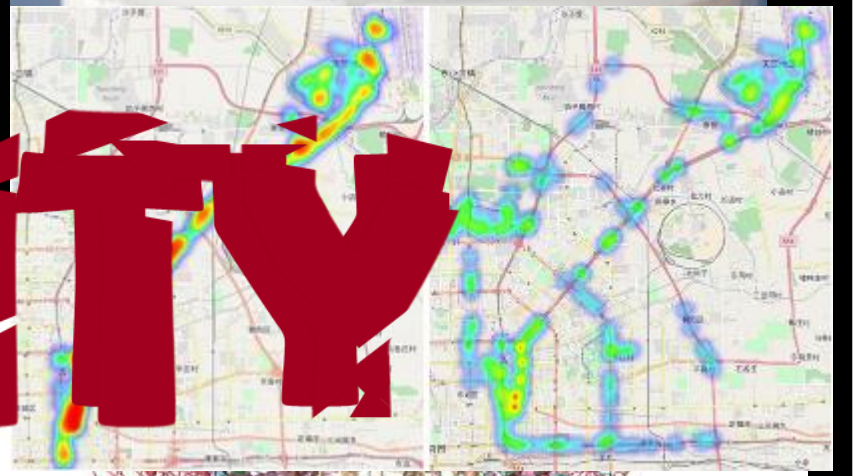
Johanna Sepúlveda, Ph.D.
Expert Post-Quantum Secure Communications
Chief Engineer Quantum Secure Communications

AIRBUS

Quantum Computer



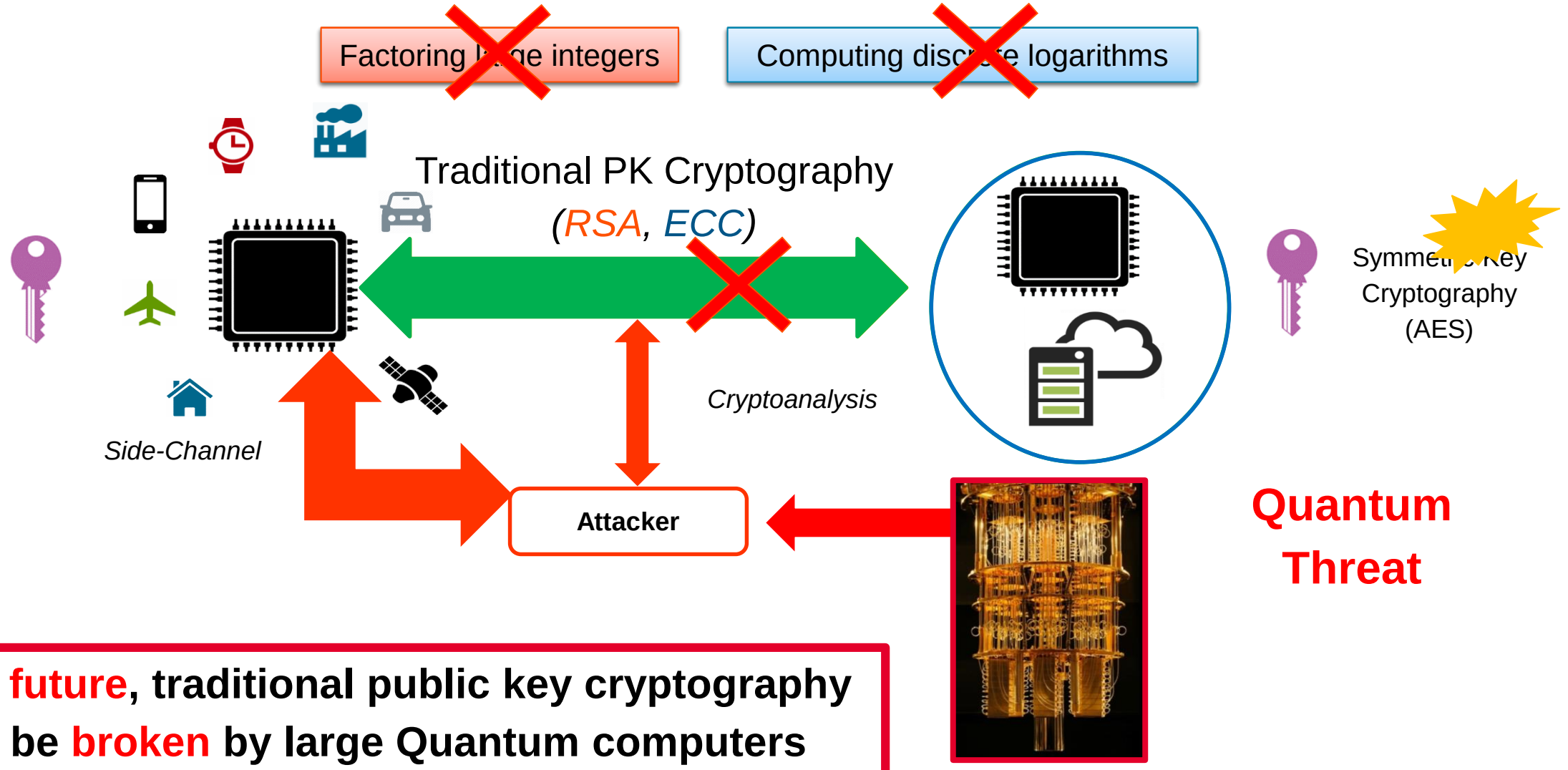




CURITY

AIRBUS

Traditional Security is under Threat



In the future, traditional public key cryptography will be broken by large Quantum computers

Security Challenges

Quantum-Secure Solutions are required

Require long term security

Criticality

Heterogeneity

Different Communication capabilities and needs

Quantum Key Distribution (QKD)

Still Immature (TRL5 2024)

Quantum-Secure Technologies

- **PQC** and **QKD are not competing**
- **PQC** and **QKD** can **work together**
- Two security technologies with different properties
- They can cover the security needs of a **wide variety of applications**

How?

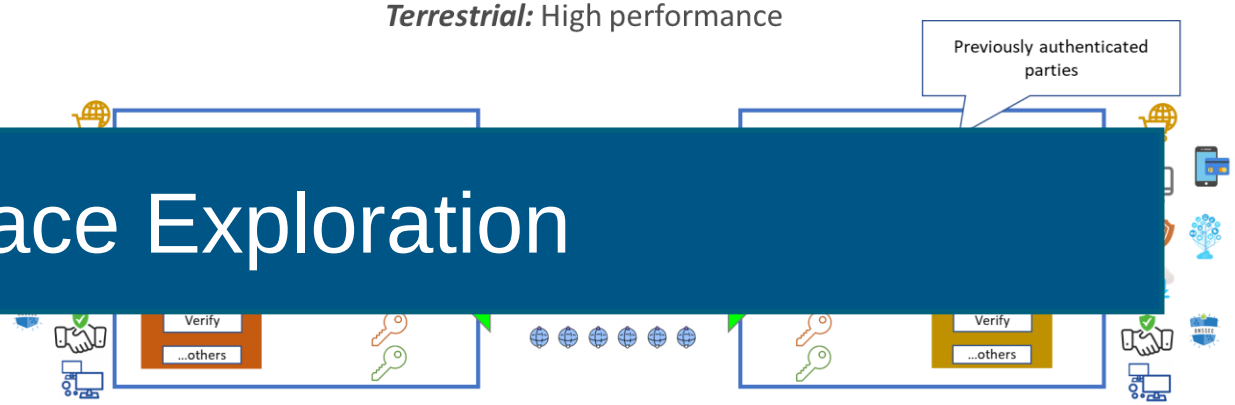
Quantum-Key-DIstribution

Quantum-Key-Distribution (QKD)

- QKD is one part of the overall information security infrastructure:
  - Two parties can agree upon a shared key
  - protocol
- QKD creates random, independent session keys
- Public key cryptography for authentication and QKD for key agreement can lead to very strong long-term security
- Performance: **QKD link technology** and **post-processing**

Space: High range

Terrestrial: High performance



K_A , K_B : Final QKD keys on Alice and Bob's sides

Authentication:

- ✓ **Public key authentication** (CA)
  - PQC, Hybrid
- ✓ **Symmetric** (pre-shared secret)
  - Based on unconditionally secure message authentication code (Wegman-Carter)
  - Use QKD for QKD (QKD Composability)

Wide Design Space Exploration

Quantum-Key-Distribution (QKD): System Level View is Relevant

- System level exploration is mandatory and critical (E2E secure communication)

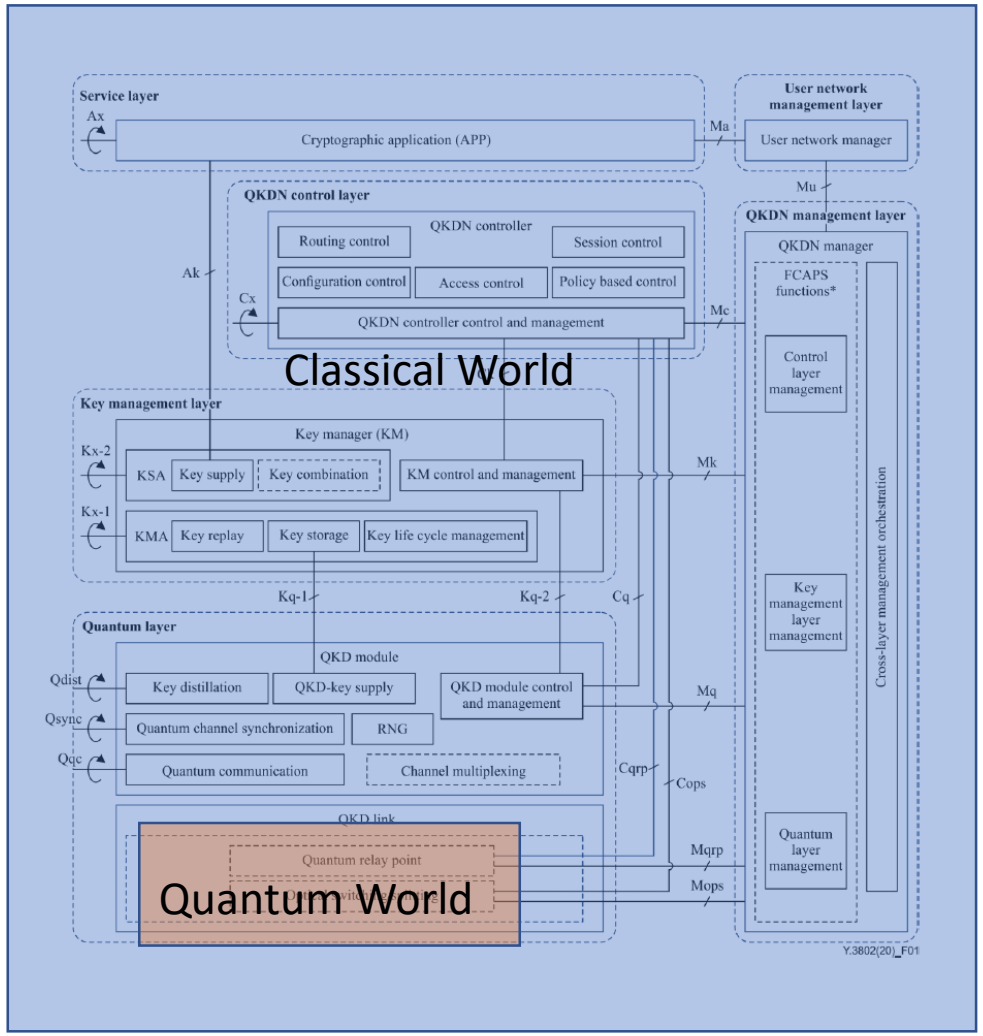
Interoperability

System Security

System Performance

System Reliability

Cryptoagility



From ITU Y-3802

AIRBUS

Quantum-crypto at **AIRBUS: EuroQCI (EC) and SAGA (ESA)**

2019 **2021** **2024** **2026** **2027** **2035**

Preparatory activities EU funded research projects

Two Commercial concept studies ***« High level Architecture »***

AIRBUS

Two studies ***« Detailed Design »***

AIRBUS

« QKD EU National Deployments » x27

EuroQCI Coordination

AIRBUS *(partner)*

QKD Operational system

Quantum Internet Operational system

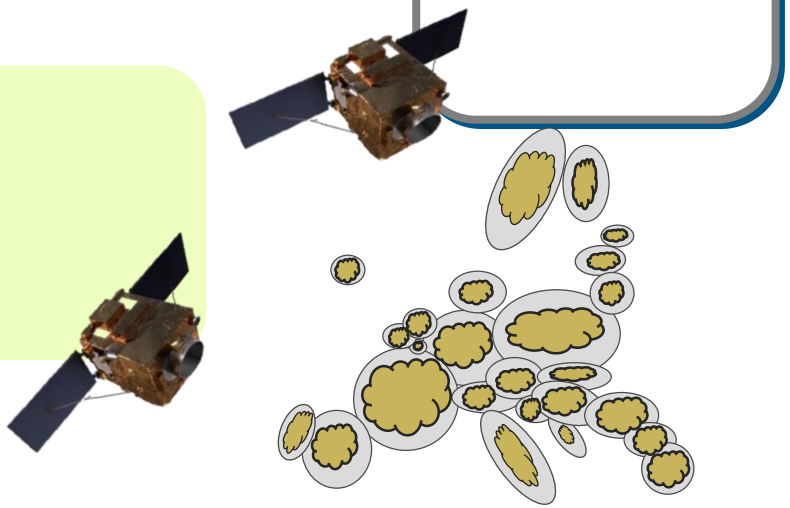
SAGA I

AIRBUS

SAGA II

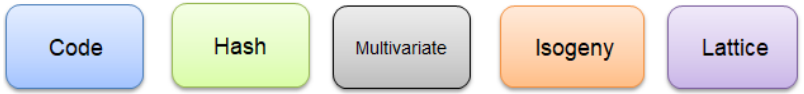
AIRBUS

QKD Space backbone



Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) Types



Code-based

(e.g. McEliece, Bike)

Pros:

- Well studied error correcting codes
- Multipurpose
- Fast

Cons:

- Very large key sizes

Hash-based

(e.g. SPHINCS+, XMSS, LMS)

Pros:

- Security relies on hash functions
- Very efficient

Cons:

- No encryption schemes
- Track of signed messages

Multivariate

(e.g. Rainbow)

Pros:

- Multipurpose
- Very efficient for signature schemes

Cons:

- Most public key schemes are broken

Isogeny

(e.g. SIKE)

Pros:

- Elliptic-based
- Smallest key sizes

Cons:

- Low efficiency
- Difficult to construct

Lattice-based

(e.g. Kyber, Dilithium, Falcon)

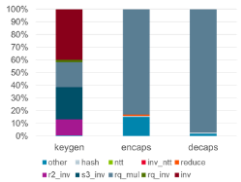
Pros:

- Efficient
- Public key, digital signatures, FHE, IBE

Cons:

- Key sizes when compared to classical crypto

NIST PQC Roadmap and Airbus Footprint



Apr.16: NISTIR 8105 report

Dec.17: First-round candidates announced

Airbus: First PQC-codesign HW/SW (Crypto-agility)

Jul.19: Second-round candidates announced

Jul.20: Third-round candidates announced

Airbus: Design 1st Chip with EU processor with PQC

Jul.22: Selected PQC announced; Round four begins

Aug.23: First PQC draft Published

Airbus: Record implementation of advanced PQC crypto-primitives

2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | Future

Dec.16: Formal call for submissions

Nov.17: Deadline for submissions

Apr.18: First NIST PQC Workshop

Aug.19: Second NIST PQC Workshop

Jun.21: Third NIST PQC Workshop

Jul.22: Formal call new signature

Jun.23: Deadline for submissions new signatures

Airbus: Ultra-constrained PQC solution

Airbus: First PQC-enhanced Wireless sensor network

Airbus: Record on PQC Implementation (performance, power, memory footprint)

Airbus: Demonstration PQC on the field Secure Drone Connectivity

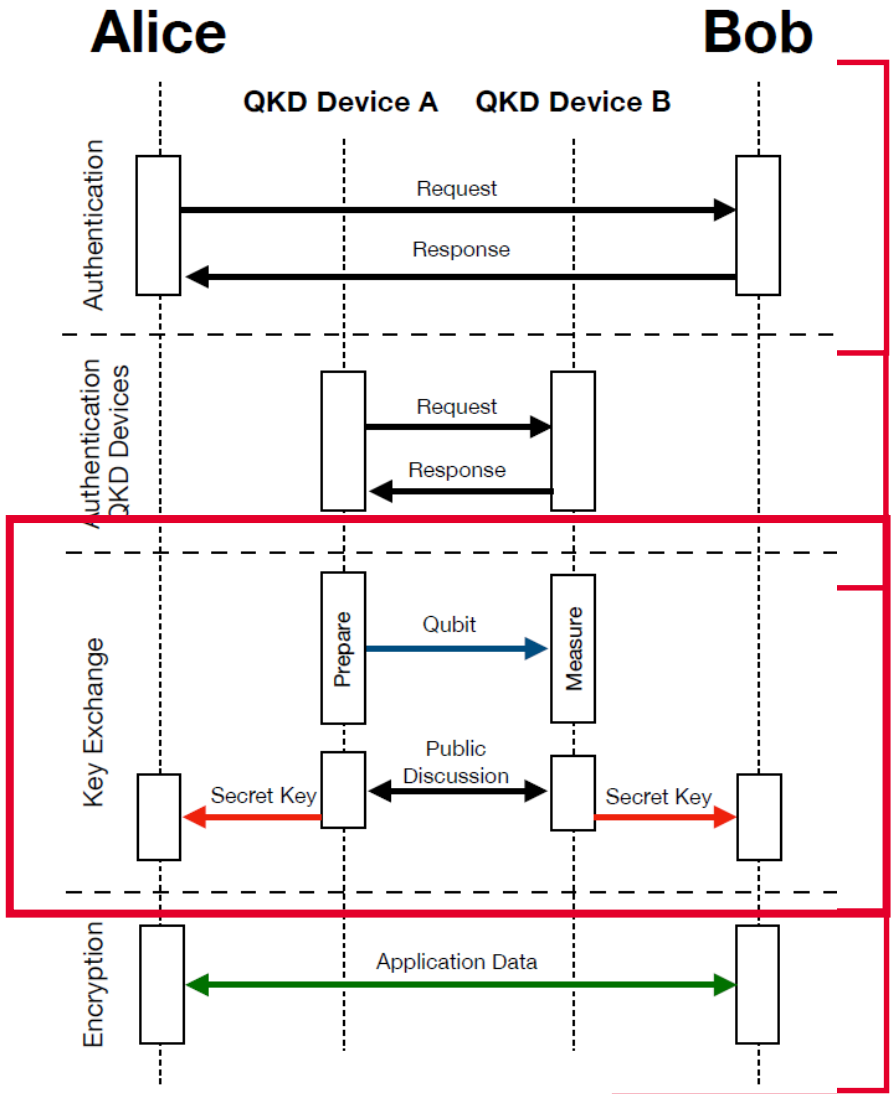
Airbus: Development of advanced PQC-enhanced systems Space, dynamic networks, PQC-secured Blockchain

E2E Quantum-secured communication

Quantum-Secure Communication

Purpose is to ensure Quantum Secure Communication between two parties

Quantum Layer



1) Authentication of Alice and Bob using PQC Algorithms

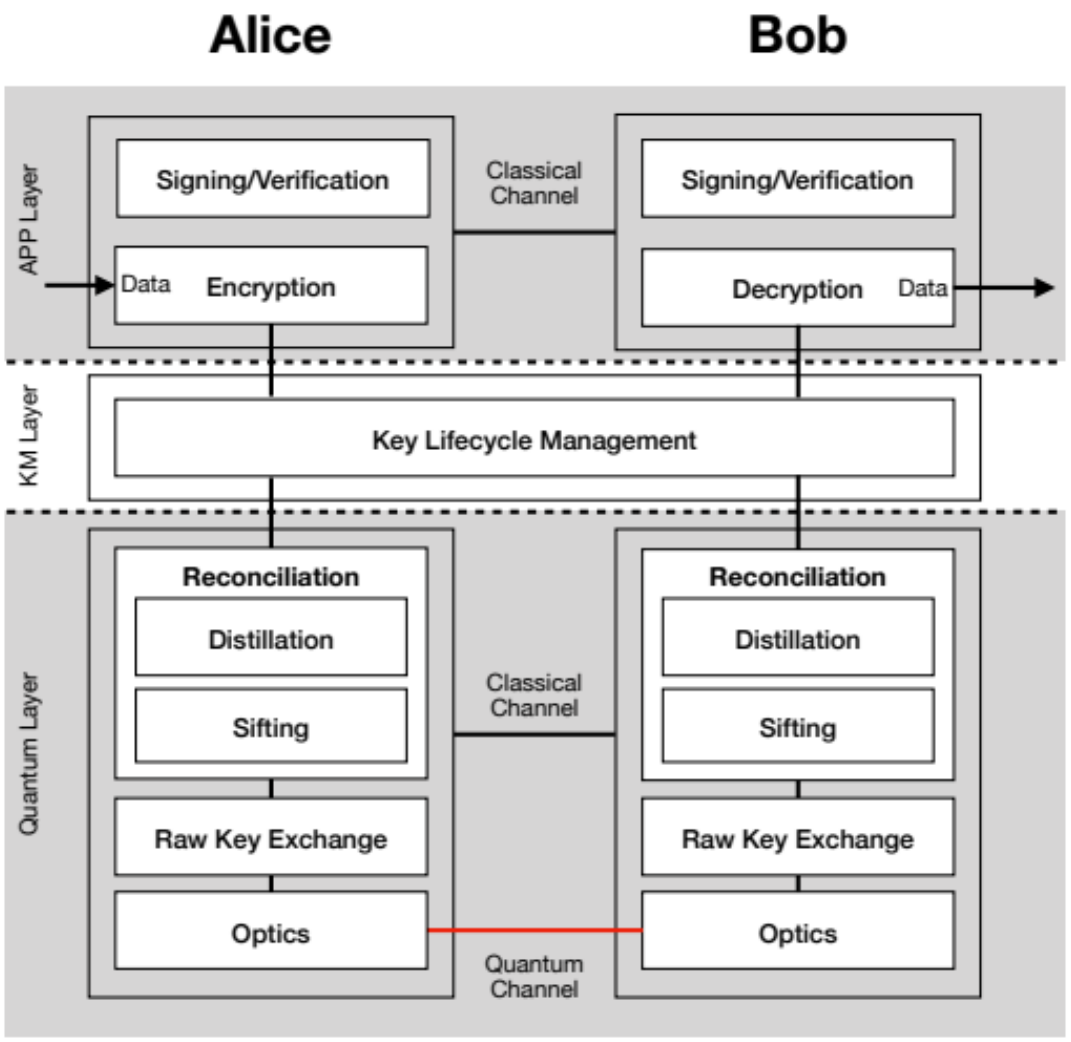
2) Authentication of QKD Devices

3) Quantum Key Exchange

4) Encryption using QKD Key

AIRBUS

Software Implementation



Fast prototyping tool (Python)

PQC:

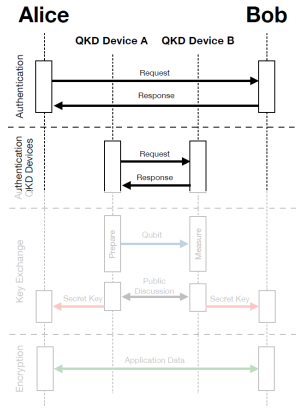
- Secure PQC implementation (liboqs, pqclean)
  Baseline, time-protected, masked implementations
- Low and high processing capabilities

Quantum:

- Quantum virtual private Network (**QVPN**) point-to-point link
- Validated models and configurations with physical setups
  - QKD **Fibre model**
  - Protocols: **decoy-BB84** and **T12**

Post-Quantum Cryptography

Authentication



- **NIST PQC algorithms:**
  - PQC signature selection: Dilithium, Falcon, SPHINCS+
  - Stateful **XMSS** (NIST SP 800-208)
- **Pre-shared Keys**

Key Sizes in Bytes

SIG Parameter Set	Public key	Secret key	Signature
Falcon-512	897	1281	690
Falcon-1024	1793	2305	1330
Dilithium2	1312	2528	2420
Dilithium3	1952	4000	3293
Dilithium5	2592	4864	4595
SPHINCS+-SHA256-128s-simple	32	64	7856
SPHINCS+-SHA256-192s-simple	48	96	16224
SPHINCS+-SHA256-256s-simple	64	128	29792
XMSS	67	67	2564

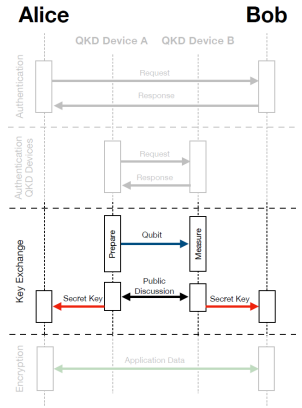
Performance

SIG Parameter Set	$t_{Raspi}[ms]$	$t_{PC}[ms]$
Falcon-512	170.04	5.13
Falcon-1024	454.71	14.78
Dilithium2	10.73	0.14
Dilithium3	16.81	0,22
Dilithium5	26.71	0.28
SPHINCS$^+$-SHA256-128s-simple	8674.60	200.09
SPHINCS$^+$-SHA256-192s-simple	15076.81	385.69
SPHINCS$^+$-SHA256-256s-simple	16056.43	301.41
XMSS	18197,.6	2246.93
Pre-Shared keys	0.091	0.0056

Parameters

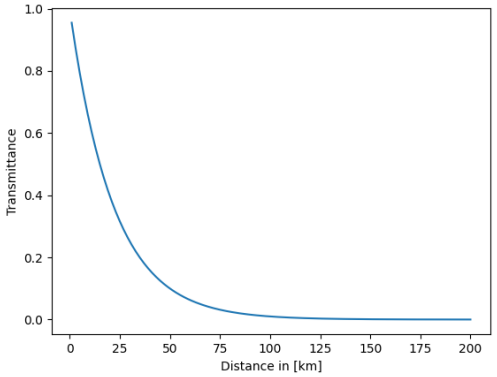
Decoy BB84, T12

Key Exchange

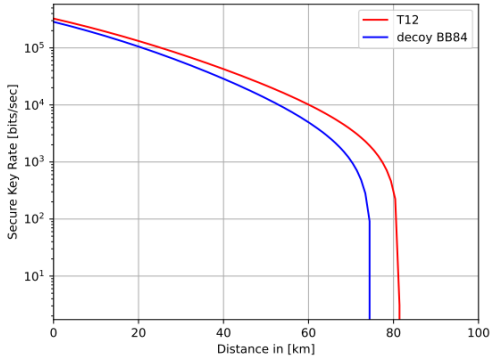


Param.	Description	Value
μ_u	intensity signal state	0.425
μ_v	intensity decoy state	0.044
μ_w	intensity vacuum state	0.0001
p_v	probability sending decoy state	0.3
p_w	probability sending vacuum state	0.1
α	attenuation coefficient [1/km]	0.2
d	fibre dispersion coefficient[ps/(km*nm)]	4
t_b	internal receiver loss[dB]	0.4
λ_q	signal frequency[nm]	1550
n	detection efficiency[-]	0.20
f	pulse generation rate [MHz]	500
ρ_{AP}	after-pulsing probability [-]	0.0525
t_{dead}	dead time of APD detectors[s]	$1 * 10^{-6}$
p_{dc}	dark-count probability[-]	$2,1 * 10^{-5}$

Fiber properties



QKD



QKD Parameter	skr [bit/sec]	$skr_{256}[key/sec]$	$t_{key}[ms]$
decoy-state BB84 - 10 km	179,749	702	1.42
T12 - 10 km	213,239	832	1.20
decoy-state BB84 - 50 km	12,762	49	20.06
T12 - 50 km	21,504	84	11.90

Experimental Results and Conclusions

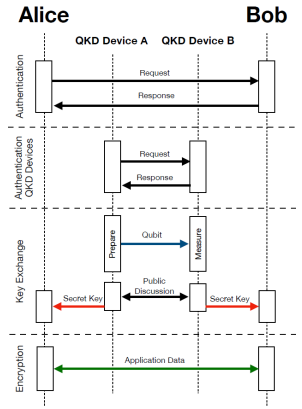
Performance results in [ms]

System	t_{Raspi}	t_{PC}
10 km - PSK - T12 - AES-256-CBC	4.8	4.7
10 km - Dilithium2 - T12 - AES-256-CBC	415.5	4.8
10 km - Dilithium3 - T12 - AES-256-CBC	421.6	4.9
10 km - Dilithium5 - T12 - AES-256-CBC	431.5	4.9
10 km - Falcon-512 - T12 - AES-256-CBC	575.8	9.8
10 km - Falcon-1024 - T12 - AES-256-CBC	859.5	19.4
10 km - SPHINCS$^+$-128 - T12 - AES-256-CBC	9,079.4	204.8
10 km - SPHINCS$^+$-192 - T12 - AES-256-CBC	15,481.6	390.4
10 km - SPHINCS$^+$-256 - T12 - AES-256-CBC	16,461.2	306.1
50 km - PSK - T12 - AES-256-CBC	15.5	15.4
50 km - Dilithium2 - T12 - AES-256-CBC	426.2	15.5
50 km - Dilithium3 - T12 - AES-256-CBC	432.3	15.6
50 km - Dilithium5 - T12 - AES-256-CBC	442.2	15.6
50 km - Falcon-512 - T12 - AES-256-CBC	585.5	20.5
50 km - Falcon-1024 - T12 - AES-256-CBC	870.2	30.1
50 km - SPHINCS$^+$-128 - T12 - AES-256-CBC	9090.1	215.5
50 km - SPHINCS$^+$-192 - T12 - AES-256-CBC	15492.3	401.1
50 km - SPHINCS$^+$-256 - T12 - AES-256-CBC	16471.9	316.8

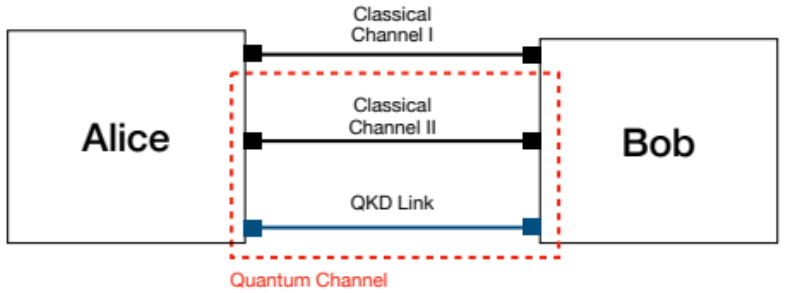
Authentication

Key Exchange

Encryption



Conclusions



- **System-level** quantum-secure communication is relevant
- Hybrid approaches are key for deploying the QKD in real applications and to ensure the E2E quantum-secure communication
- The **design space of the overall system is wide** and must be explored: Performance, security, reliability, etc.
- Classical component of the QKD systems might have a strong impact on the overall performance and security
- Major time for executing was consumed by the **PQC authentication**

Thank you

Johanna.sepulveda@airbus.com