QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

From Quantum Threats to Quantum Shields

A comprehensive guide to Post-Quantum Cryptography

Panagiotis (Panos) Vlachos
PhD Researcher CSIT, QUB

Outline

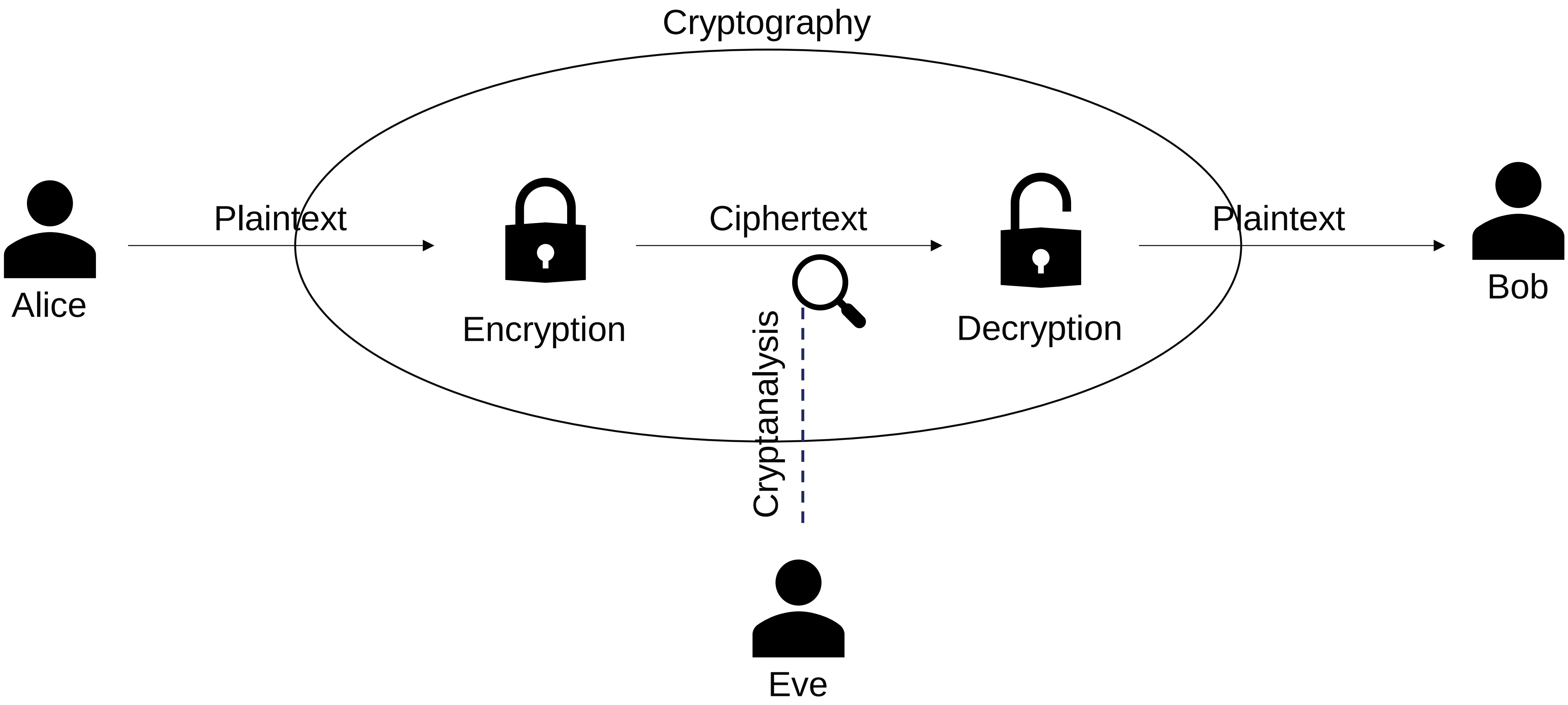
1. Conventional cryptography
2. Quantum Computing & Quantum Threat
3. Post-Quantum Cryptography – Responding to the Quantum Threat
4. Post-Quantum Cryptography – Latest advancements
5. Applications of PQC

Conventional Cryptography

Basic Terms

- **Cryptography** is the practice and science of securing Confidentiality, Integrity & Authenticity of information, by transforming it into an unreadable format.
- **Plain-text** is human readable text / message in its original format.
- **Cipher-text** is encrypted text that has been transformed using a cipher or encryption algorithm
- **Cryptanalysis** is the science of analyzing and breaking cryptographic codes and ciphers.
- **Post-Quantum/Quantum-Resistant Cryptography (PQC)** cryptographic methods & algorithms that remain secure, even against quantum attacks, while functioning effectively with classical computers.

Cryptography



Symmetric & Asymmetric Cryptography

Symmetric Cryptography

- Same key for encryption & decryption
- Algorithms that transform plain to ciphertext using a secret key
- Keeping the secret key secret

Cryptanalysis

- Brute-force
- Attacks aimed at the cipher

Asymmetric Cryptography

- Key pair (public, private)
- Mathematical Foundation
    - Large-number factorization (RSA)
    - Discrete logarithm problem (DH, ECC)
- Computational Difficulty

Cryptanalysis

- Mathematical attacks
- Quantum attacks

Quantum Computing

Quantum Computing & Quantum Threat

Traditional Computing

- Bit {0,1}
- Single path

Quantum Computing

- Qubit {0,1, both 0 and 1 simultaneously (superposition)}
- Entanglement – “information telepathy”
- Multiple paths

”Quantum Computers are not faster – just weirder”

— *Prof. Martin Albrecht*

Impact on current cryptographic systems

Shor's Algorithm

- Efficient computations on quantum machines
- Large-number factorization & discrete logarithms in polynomial time
- Targets asymmetric cryptography (RSA, ECC, DSA, …)

Grover's Algorithm

- Efficient search with quantum machines
- Reduces the time complexity of brute-force attacks
- Targets symmetric cryptography (AES, SHA, …)

What can we do?

Symmetric Cryptography

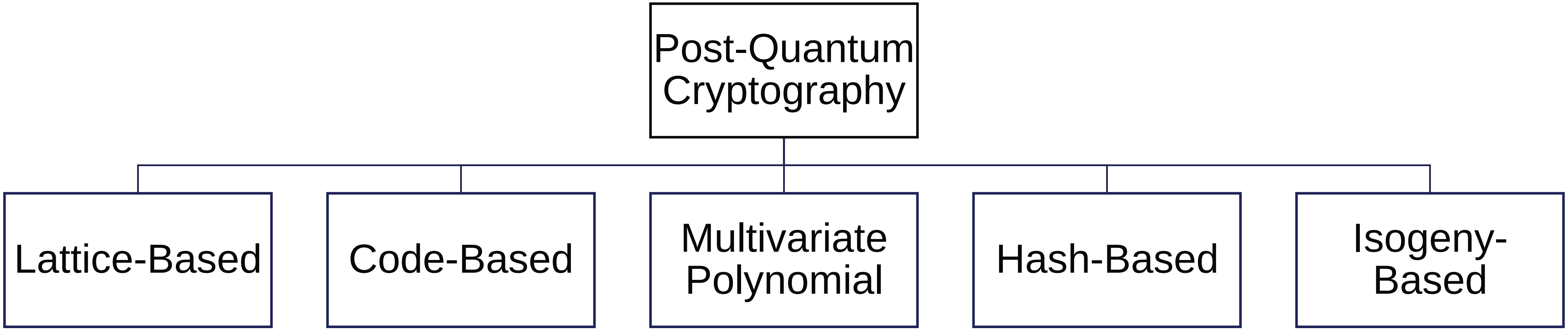
- Grover's algorithm, halves the security level
  - 128-bit → 64-bit security against Grover's attacks
- **Doubling the key length**
  - Impacts on computational load, memory requirements, latency, energy consumption

Asymmetric Cryptography

- Shor's algorithm attacks the underlying mathematical problems
- No simple solution…

Post-Quantum Cryptography (PQC)

PQC Families



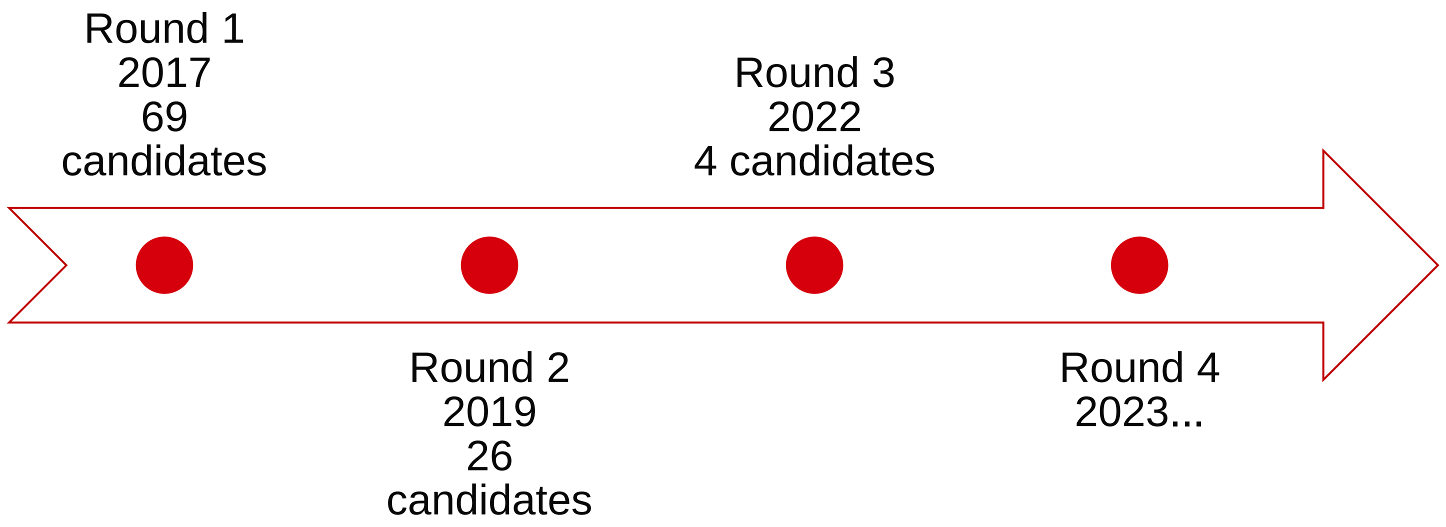
PQC Standardisation Process

NIST Standardization Process

National Institute of Standards and Technology (NIST)

Standardization process

1. Algorithm submissions
2. Evaluation of submitted algorithms
3. Selection for standardization



Standardization Process Rounds

Algorithm Name	Cryptographic Family	Purpose	Additional Notes	
CRYSTALS-KYBER	Lattice-Based	PKE/KEM	FIPS-203	Round 3
CRYSTALS-Dilithium	Lattice-Based	Signatures	FIPS-204	
SPHINCS+	Hash-Based	Signatures	FIPS-205	
FALCON	Lattice-Based	Signatures	*Draft FIPS-206 TBA*	
HQC	Code-Based	PKE/KEM	Selected for standardization (11/03/2025)	Round 4
Classic McEliece	Code-Based	PKE/KEM	Long-standing security record	
BIKE	Code-Based	PKE/KEM	Error-correcting codes	
SIKE	Isogeny-Based	PKE/KEM	Proven insecure in 2022; included in the 4th round for academic visibility	

Current Status - Selected Algorithms

Algorithm Name	Cryptographic Family	Purpose	Additional Notes
CRYSTALS-KYBER	Lattice-Based	PKE/KEM	FIPS-203
CRYSTALS-Dilithium	Lattice-Based	Signatures	FIPS-204
SPHINCS+	Hash-Based	Signatures	FIPS-205
FALCON	Lattice-Based	Signatures	*Draft FIPS-206 TBA*
HQC	Code-Based	PKE/KEM	Selected for standardization (11/03/2025)
Classic McEliece	Code-Based	PKE/KEM	Long-standing security record
BIKE	Code-Based	PKE/KEM	Error-correcting codes
SIKE	Isogeny-Based	PKE/KEM	Proven insecure in 2022; included in the 4th round for academic visibility

Standardised (CRYSTALS-KYBER, CRYSTALS-Dilithium, SPHINCS+)

Selected for standardization (FALCON, HQC)

Under evaluation (Classic McEliece, BIKE)

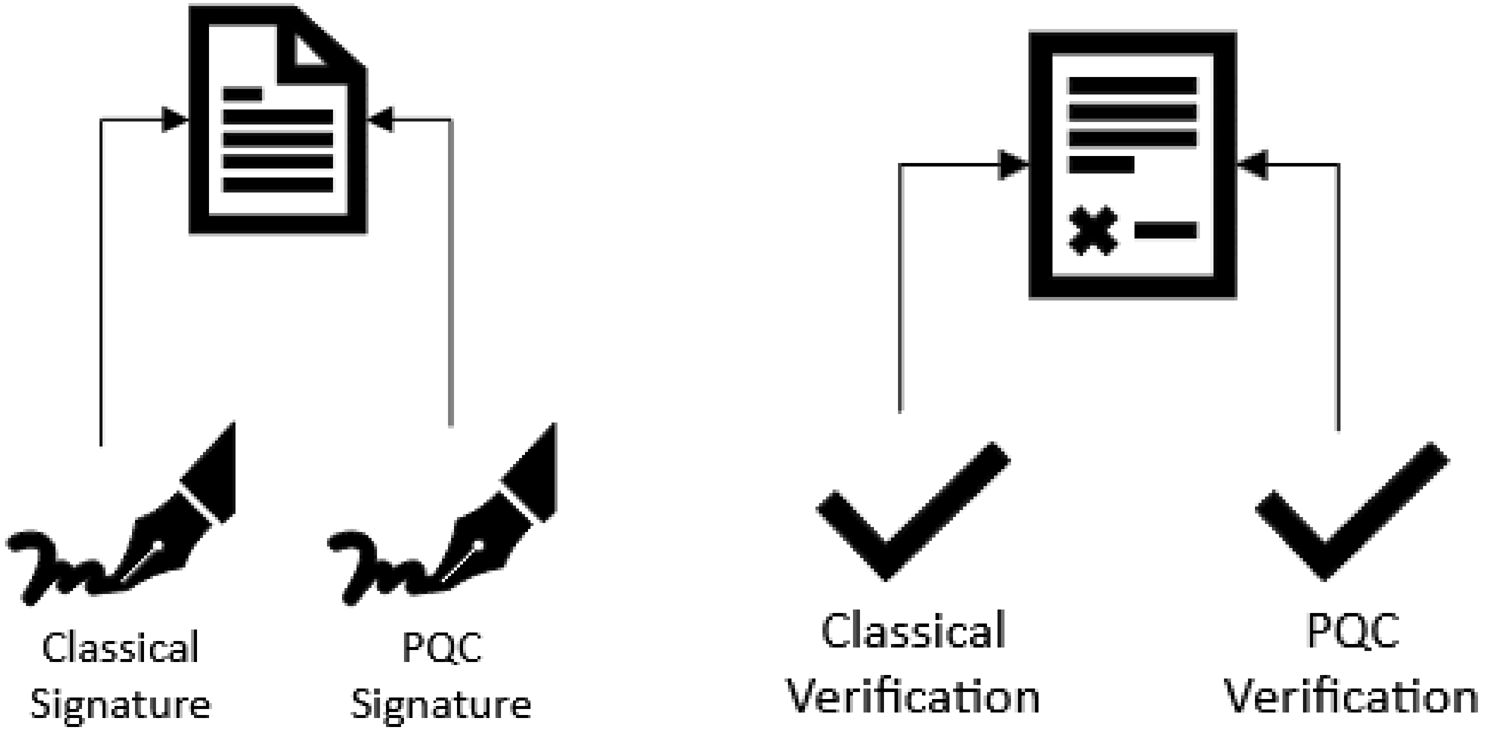
Migrating to PQC

Global Policy Landscape

- USA
  - **NIST Standardization Process** – Algorithms vetted to protect against quantum threats.
  - **Presidential Memorandum (2022)** – US Federal Agencies to adopt PQC by **2030** (NASA, Department of Defense)
- Australia
  - **ACSC** (Australian Cyber Security Centre) – **phasing out** legacy cryptosystems by **2030**
- Europe
  - **ENISA** (European Union Agency for Cybersecurity) – collaborating with the **European Commission** to guide PQC implementation across member states.
  - UK's **NCSC** (National Cyber Security Centre) – full migration to PQC by **2035.**
- Asia
  - **Japan**'s **CRYPTREC** Guidelines – advisory body for PQC transition recommendations for the next years, includes banking & public services
  - **South Korea**'s **roadmap** for PQC adoption, targets pilot implementations by **2025**, focus on areas like smart cities, fintech and autonomous vehicles.
    KPQC research group.

Hybrid PQC

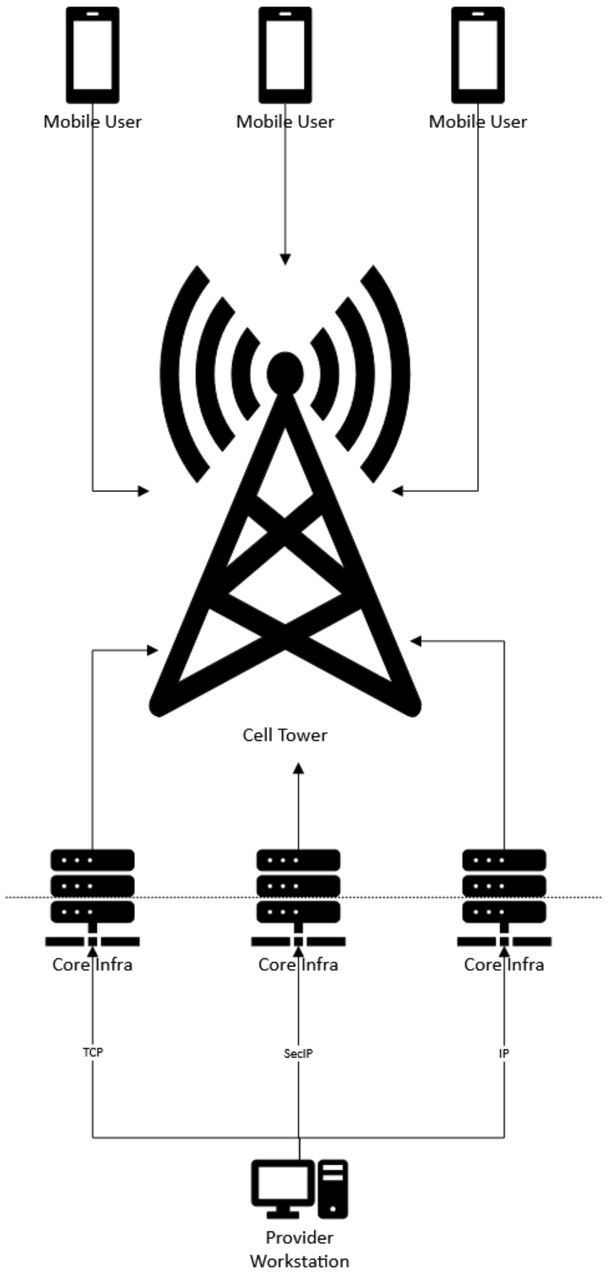
- PoC vs Production
- Conventional & Post-quantum → Hybrid implementation
  - Dual Protection
  - Gradual transition
  - Interoperability



Applications of PQC

Areas of application

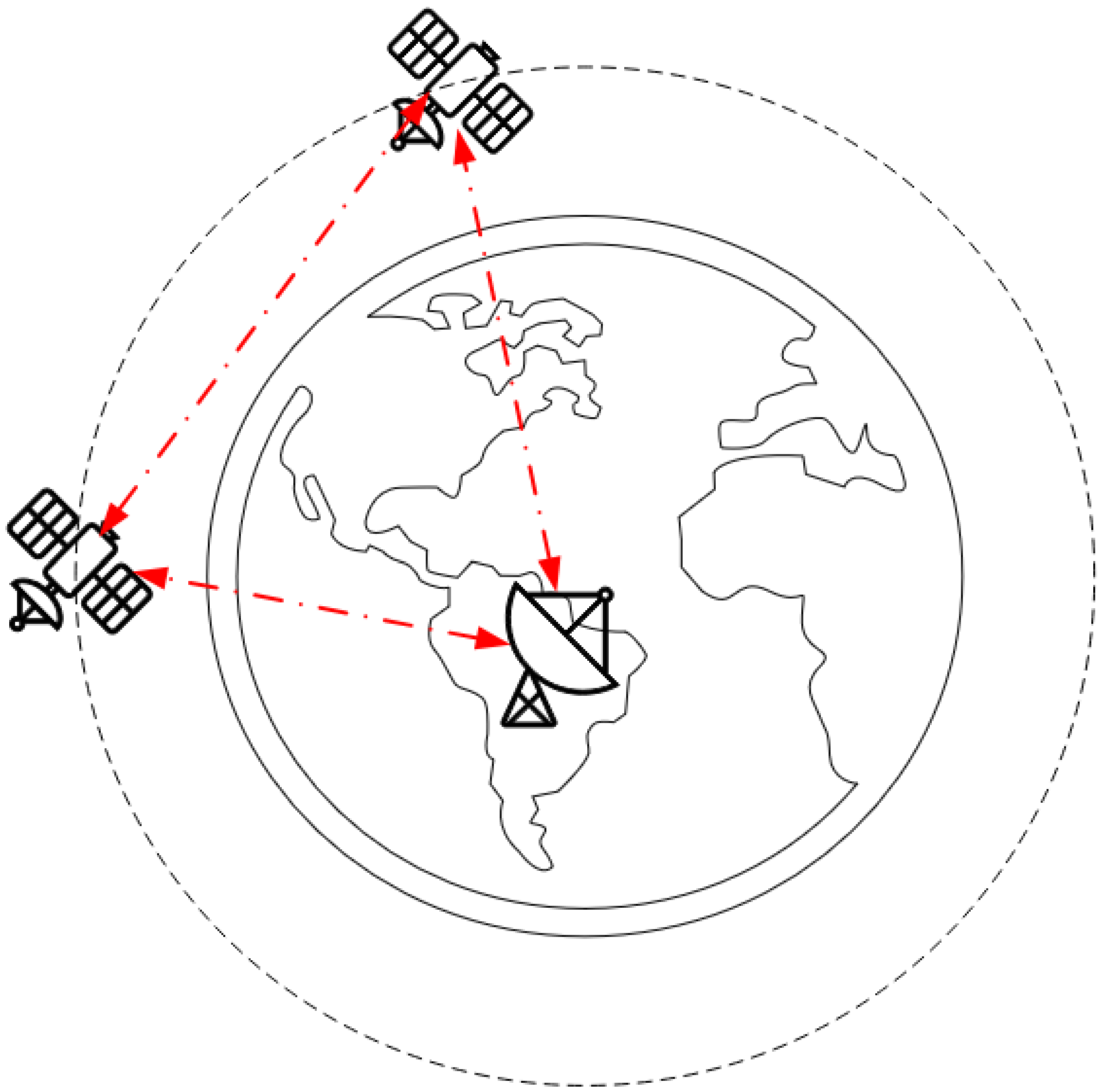
- Emerging Technologies - 6G
  - Previous infrastructure
  - Identity Concealment
  - **Hybrid approach**
  - **Synergies**



Read more here.

Areas of application

- Space Systems
  - Symmetric Cryptography
  - Future Challenges:
    - Satellite Constellations
    - Mesh networks
  - Decade-long lifespan
  - Safety & Security



Read more here.

Takeaways

Takeaways

- High level understanding of Quantum Threat & PQC
- Monitor advancements in both areas & stay curious
- Keep track of what you’re using


H & W
H & W
WHITE STAR HOUSE
Thank you!

Panagiotis (Panos) Vlachos

pvlachos01@qub.ac.uk