Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXV cycle

Supervisor
Prof. Antonio Lioy

# Cybersecurity and Quantum Computing: friends or foes?

PhD Candidate: Ignazio Pedone

## 1. Introduction

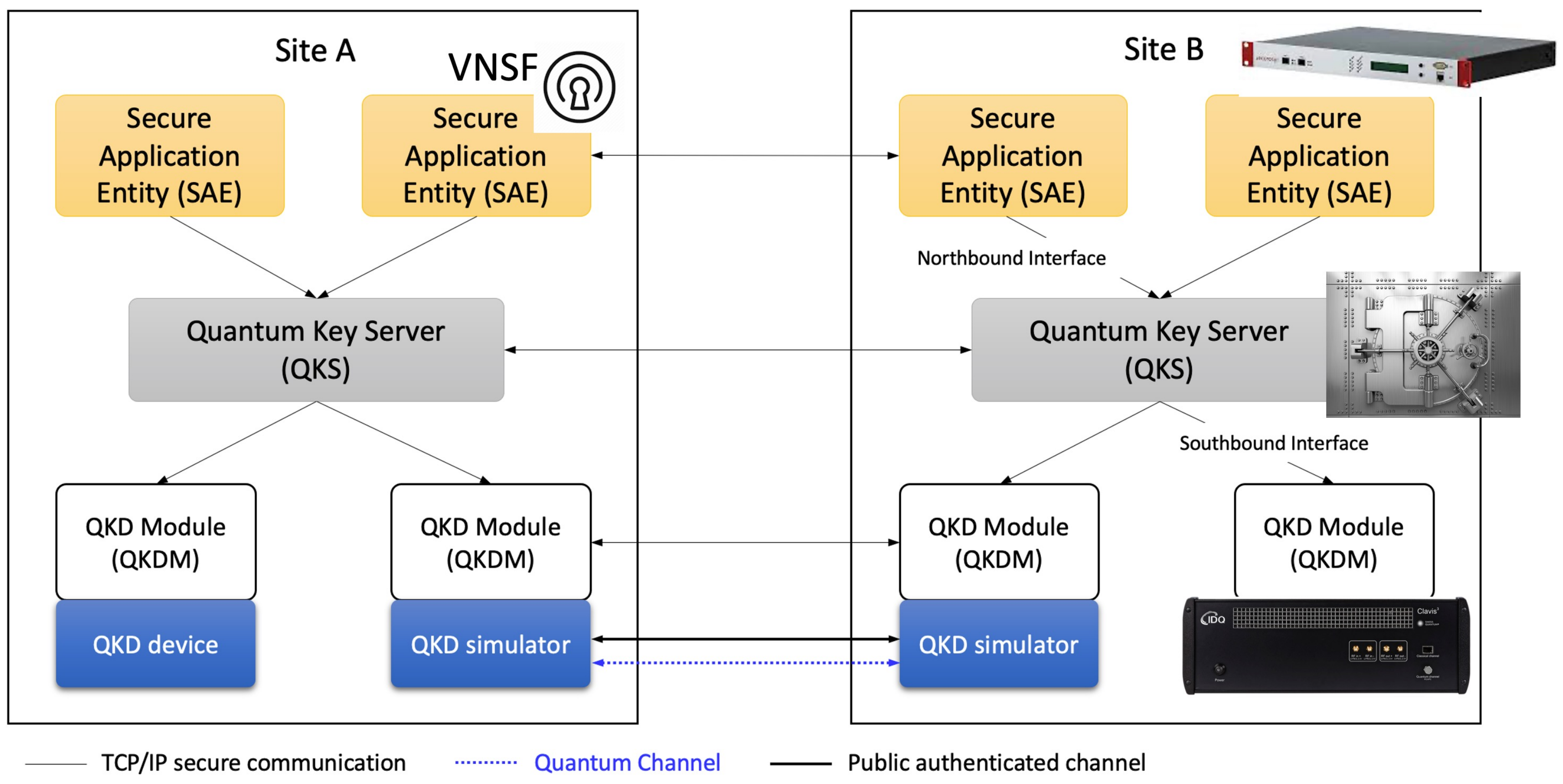
Quantum Computing jeopardises current public key cryptography algorithms that are widely used by security protocols (e.g., TLS, IPsec) adopted in modern software-defined infrastructures.

## 2. Goals

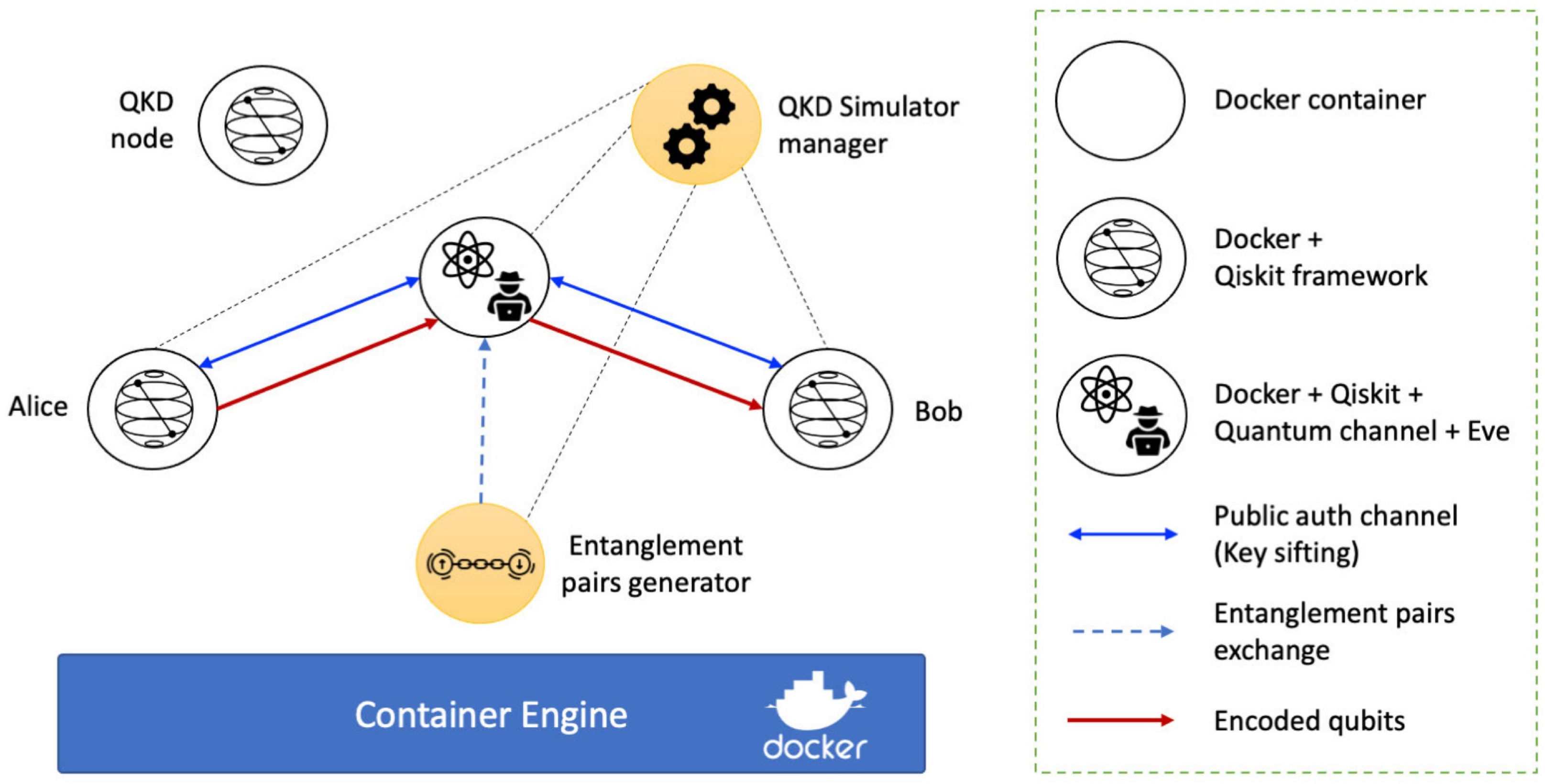
- Perform an in-depth analysis of Shor's algorithm and estimate quantum resources needed to break modern cryptosystems;
- provide effective integration of Quantum Key Distribution (QKD) in software-defined infrastructures and implement tools for simulating QKD protocols;
- apply Quantum Annealing techniques to optimize management and orchestration of modern Security-as-a-Service (SECaaS) frameworks.

## 3. Quantum Software Stack (QSS)

The QSS is a cloud-native application capable of easing the integration of QKD in software-defined infrastructures.

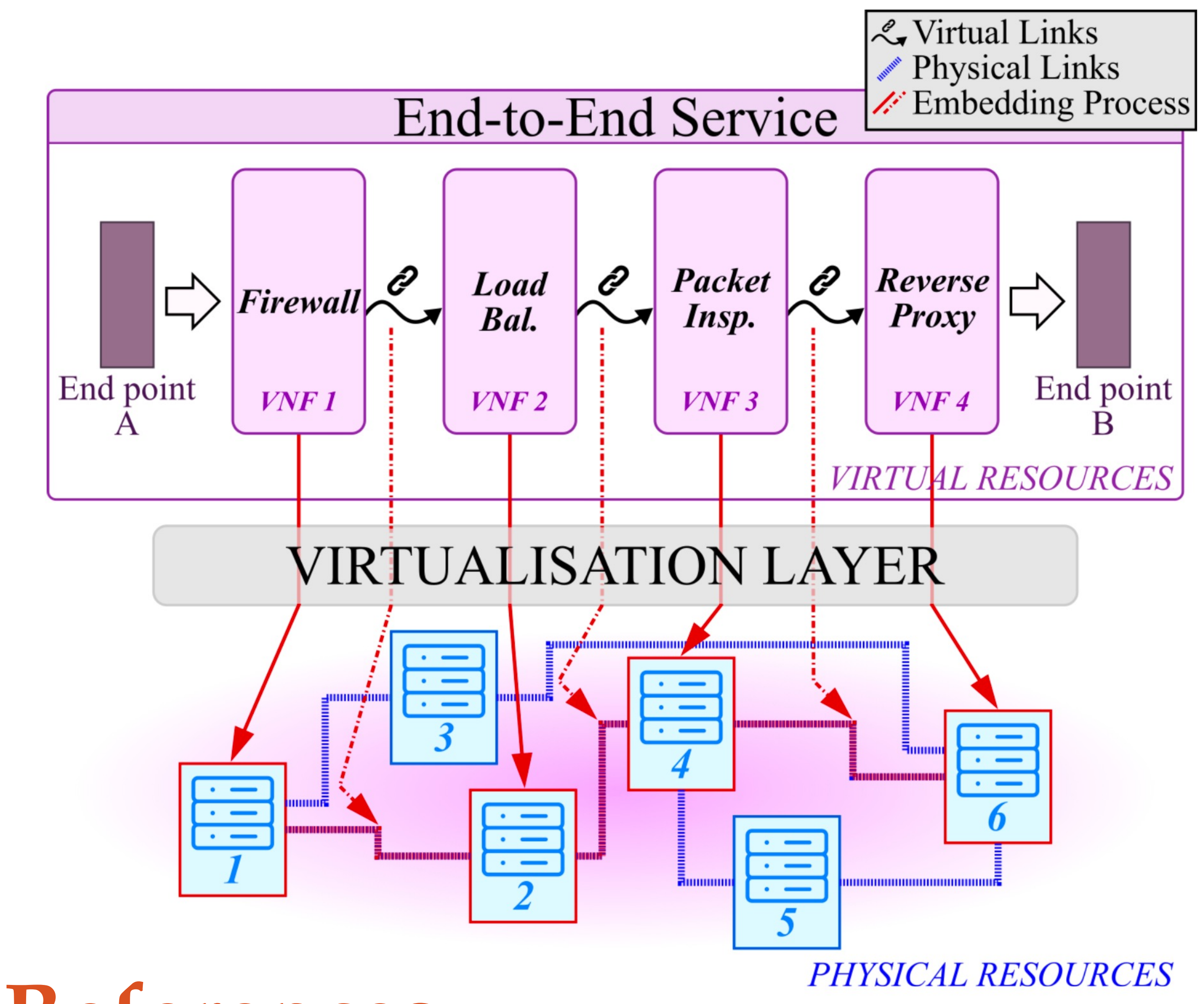


The QSS includes a QKD simulator that simulates point-to-point QKD exchanges over distributed infrastructural nodes.


QKD node
QKD Simulator manager
Alice
Bob
Entanglement pairs generator
Container Engine
docker
Docker container
Docker + Qiskit framework
Docker + Qiskit + Quantum channel + Eve
Public auth channel (Key sifting)
Entanglement pairs exchange
Encoded qubits

## 4. Quantum Annealing for VNFEPs

Quantum Annealing is a promising approach to solve Virtual Network Function Embedding Problems (VNFEPs) that are usually NP-hard. This work shows how to derive a generic QUBO formulation of a VNFEP and find optimal solutions on the D-Wave quantum annealer. The study also compares the QPU solver with Tabu Search and Simulated Annealing.



## 5. References

1. Pedone, I., Atzeni, A., Canavese, D., & Lioy, A. (2021). Toward a complete software stack to integrate quantum key distribution in a cloud environment. *IEEE Access*, *9*, 115270-1
2. Pedone, I., & Lioy, A. (2022). Quantum Key Distribution in Kubernetes Clusters. *Future Internet*, *14*(6), 16
3. Chiavassa, P., Marchesin, A., Pedone, I., Dacrema, M. F., & Cremonesi, P. (2022). Virtual Network Function Embedding with Quantum Annealing. In IEEE International Conference on Quantum Computing and Engineering (pp. 1-10).