APSIA
Preparing for a Quantum-Resistant Era

Aditya Damodaran, Georgios Fotiadis, Peter Y. A. Ryan
SnT, University of Luxembourg

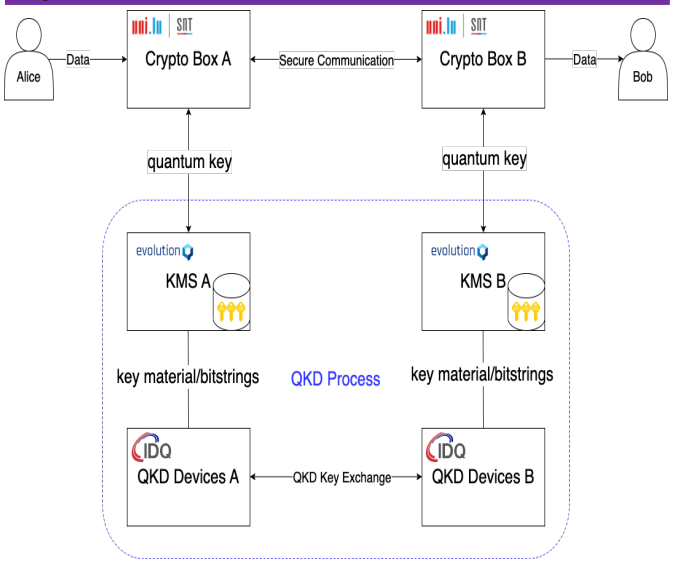
APSIA/Quantum Lab
url: apsia.uni.lu

APSIA/APSIA Q Lab

APSIA is part of SnT/University of Luxembourg, headed by **Prof. Dr. Peter Y. A. Ryan** and specialising in:

- ✓ Design/analysis of primitives, protocols
- ✓ Quantum crypto and Quantum Key Establishment
- ✓ Quantum Information Theory
- ✓ Post-Quantum Cryptography (PQC)
- ✓ Efficient/side-channel resistant PQC implementations

CryptoBox: End-to-end secure communication



*A **software-based solution** ensuring confidentiality, authentication and integrity **using QKD-derived keys**. Developed by **APSIA** for the ESA project INT-UQKD.*

Quantum-Resistant Era

Threat: *The advances of quantum computing pose **significant threats** to cryptography. **All current public key cryptosystems will be broken by quantum computers**.*

The Solution: Quantum-Resistant Crypto

Quantum Key Distribution (QKD)

Post-Quantum Crypto (PQC)

NIST National Institute of Standards and Technology

Projects

LuxQCI (ESA) - Q Communication Testbed

INT-UQKD (ESA) - Operational QKD services

Lux4QCI (EU/SnT) — National QKD deployment

FutureTPM (EU) — PQ Trusted Platform Modules

FuturePass (FNR) — PQ authentication ciphersuites

EquiVox (FNR) — PQ eVoting schemes

Q-CoDe (FNR) — (Deniable) Q Communication

FP2 (FNR) - Future-Proofing Privacy in Secure eVoting

Contact

aditya.damodaran@uni.lu, georgios.fotiadis@uni.lu, peter.ryan@uni.lu

Partners

The Government of the Grand Duchy of Luxembourg — Ministry of State — Department of Media, Connectivity and Digital Policy
LUXCONNECT
LUXTRUST — Enabling a digital world
infineon
Royal Holloway University of London
HUAWEI
SES TECHCOM
SPECTRAL
RHEA GROUP
HITEC LUXEMBOURG
POST LUXEMBOURG
INDEV
UBITECH ubiquitous solutions
evolution
INCERT
esa
IBM Research
Suite5 — We Deliver Intelligence
Technical University of Denmark
DTU
SCCS Surrey Centre for Cyber Security
restena réseau · sécurité · .lu
itrust consulting
Abstractions Lab
IDQ
TECHNIKON
inesc id lisboa
UNIVERSITY OF BIRMINGHAM
UNIVERSITY OF PIRAEUS