nano-tera.ch
swiss scientific initiative in health / security / environment systems

QCRYPT RTD 2010

Continuous coherent one-way QKD and data encryption at up to 100 Gbit/s

GAP Optique (University of Geneva); IIS (ETH Zurich); TCL (EPFL); INIT, IICT and REDS (HESSO); ID Quantique SA

Introduction

Quantum key distribution (QKD) is the most complex and advanced application of quantum physics adopted commercially today. We developed a high speed QKD enhanced encryption engine based on the Coherent one-way (COW) protocol. To support its high rates we implemented a 1.25 GHz sine gating technique for InGaAs avalanche photodiodes (APDs) and a hardware key distillation engine based on FPGAs which allows a continuous distillation of secret keys. We employ dense wavelength-division multiplexing to send the quantum channel and all classical communication channels over one single common fiber.

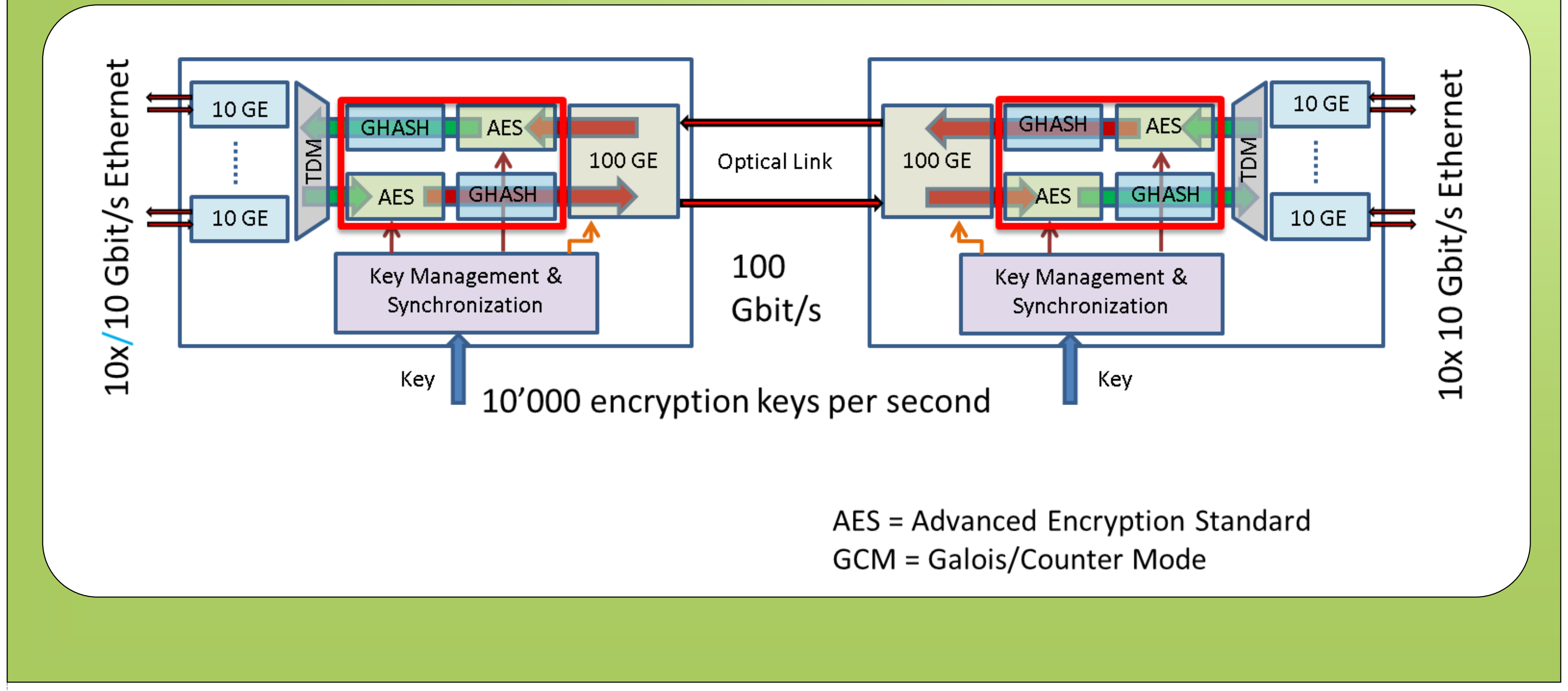
Hardware key distillation engine

Sifting	Timing and base information
Error estimation	Direct comparison or sampling
Error correction	LDPC forward error correction
Error verification	Universal hashing
Privacy amplification	Toeplitz hashing
Authentication	Polynomial hashing

- Distillation engine running on a single FPGA device (Virtex 6) for each device
- Secret key distillation at a rate of up to 4 Mbit/s
- Flexible configurations for different distances and detection rates
- Error correction using LDPC with flexible code rates allows adaptation for different QKD link distances
- Scalable and flexible privacy amplification based on Toeplitz matrices supporting any compression ratio
- Classical channel fully authenticated with quantum keys
- Initial entropy created with quantum random number generators (Quantis, IDQ)
- Integrated OTP encryption using quantum keys for highest level of security

High speed encryption devices

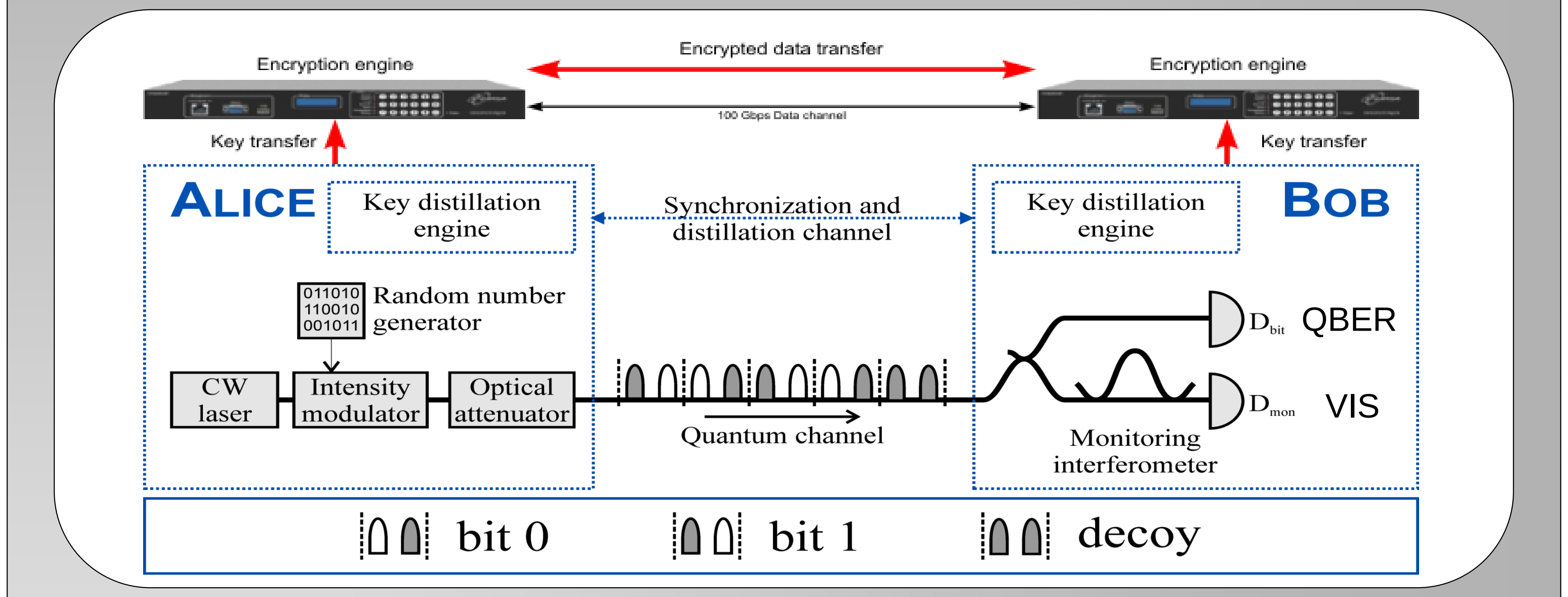
- Secure 40 and 100 Gb/s networks require to en- and decrypt terabits of data in hardware
- 40 nm Field Programmable Gate Arrays (FPGA) technologies



AES = Advanced Encryption Standard
GCM = Galois/Counter Mode

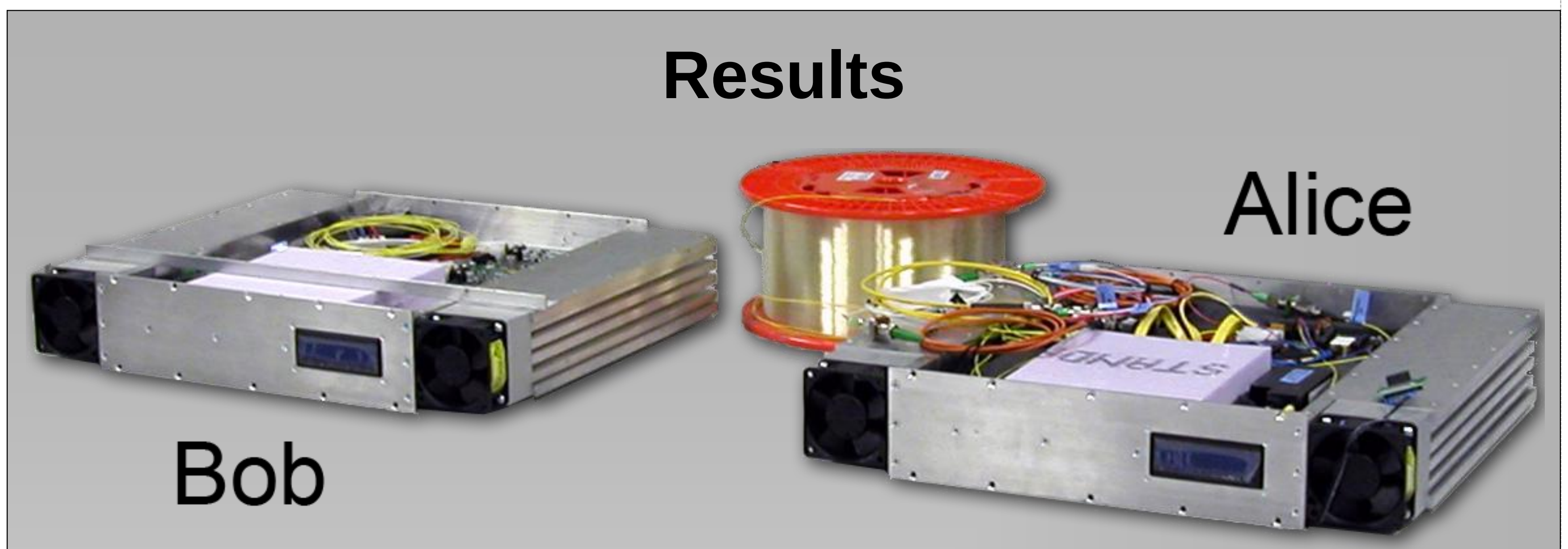
High rate coherent one-way QKD system

- High-speed Quantum key distribution (QKD) based on the Coherent One-Way protocol
- 1 Mbps one-time pad encryption (OTP)
- Wavelength-division multiplexing over a single fibre

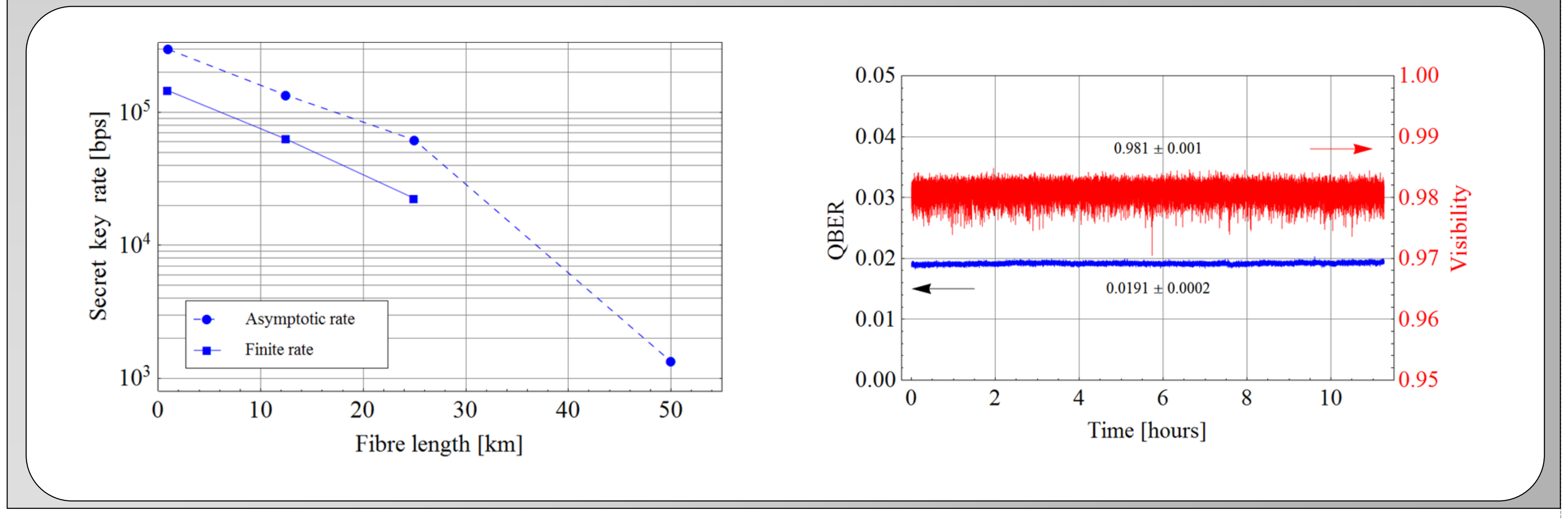


- Simple data channel with no active elements at Bob
- Interference visibility as measure of eavesdropper's information
- No QBER induced by reduced interference visibility
- Robust against USD and PNS attacks

Results



- Sine gating data detector and free-running monitor detector
- Wavelength multiplexing of all communication channels
- Hardware distillation engine with 10^6 bits post-processing block size
- Total security parameter $\varepsilon = 4 \cdot 10^{-9}$
- Stable performance over > 10 hours



Conclusions

We realized a compact and versatile implementation of the coherent one-way QKD protocol based on a hardware key distillation engine, dense wavelength-division multiplexing and fast sine gated detectors. We demonstrated up to 146 kbps secret key rate in finite key scenarios, and 298 kbps asymptotic secret key rate. Over 50 km fibre length, we obtained 1 kbps asymptotic secret key rate. The whole system is compactly integrated in 19" housing racks.

Contact: Nino Walenta (Nino.Walenta@unige.ch)
Hugo Zbinden (Hugo.Zbinden@unige.ch)

Visit the IDQ boot to watch a live-demonstration of the system !