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

QCRYPT RTD 2010

FNSNF

A high speed QKD prototype based on the coherent one-way protocol

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

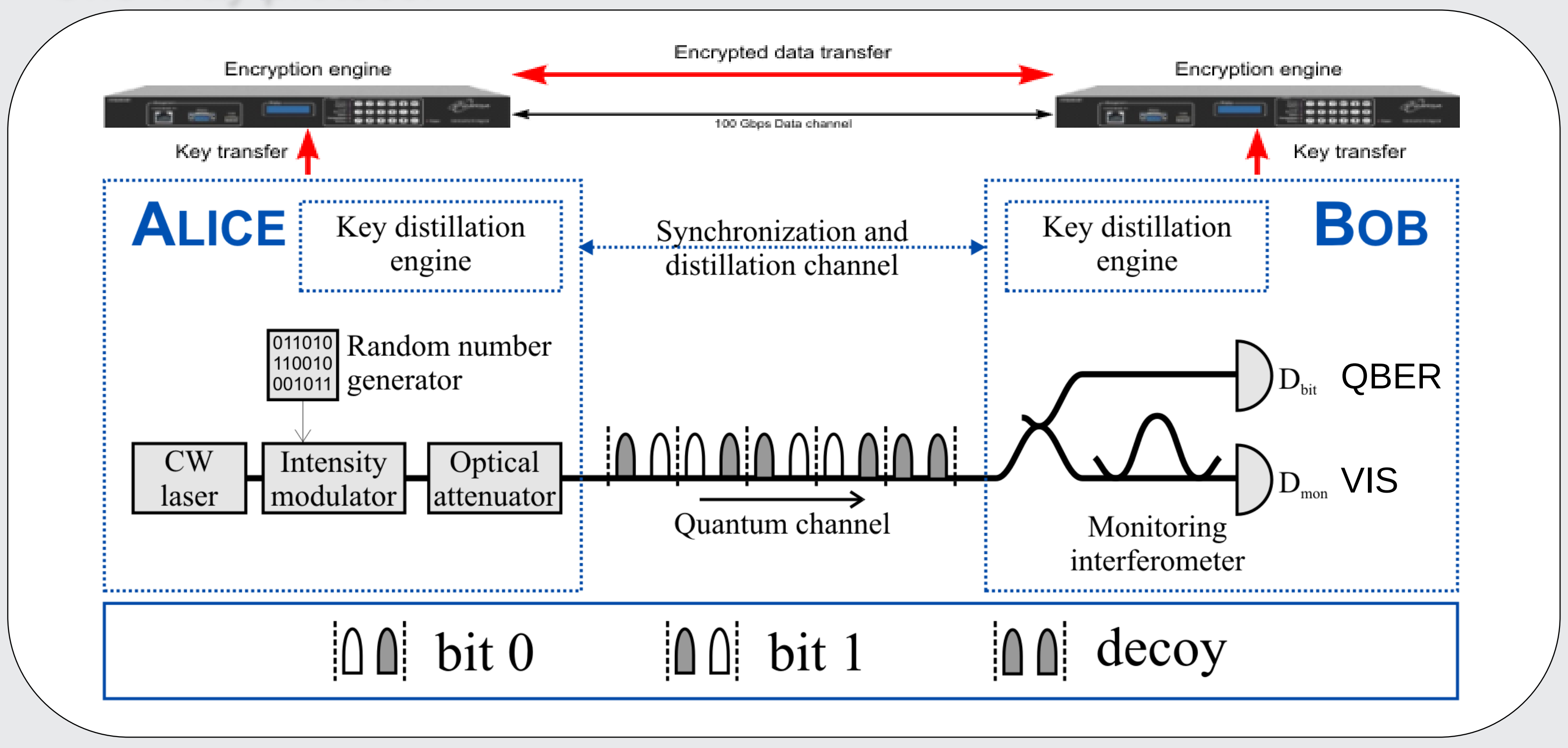
UNIVERSITÉ DE GENÈVE — ETH Zürich — ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE — Hes·so Haute Ecole Spécialisée de Suisse occidentale — IDQ

Introduction

Quantum key distribution (QKD) is the most complex and advanced application of quantum physics adopted commercially today. In scope of the Nano-Tera *QCrypt* project we implemented a flexible 625 MHz QKD platform especially suited for the Coherent one-way (COW) protocol. To support its high key rates we developed rapid 1.25 GHz gated InGaAs single photon detectors, and a hardware key distillation engine based on FPGAs which allows a continuous distillation of secret keys. Our QKD platform is compatible with external high-speed network encryptors developed in parallel to provide them continuously with secret keys for highly secure network communication.

High rate coherent one-way QKD system

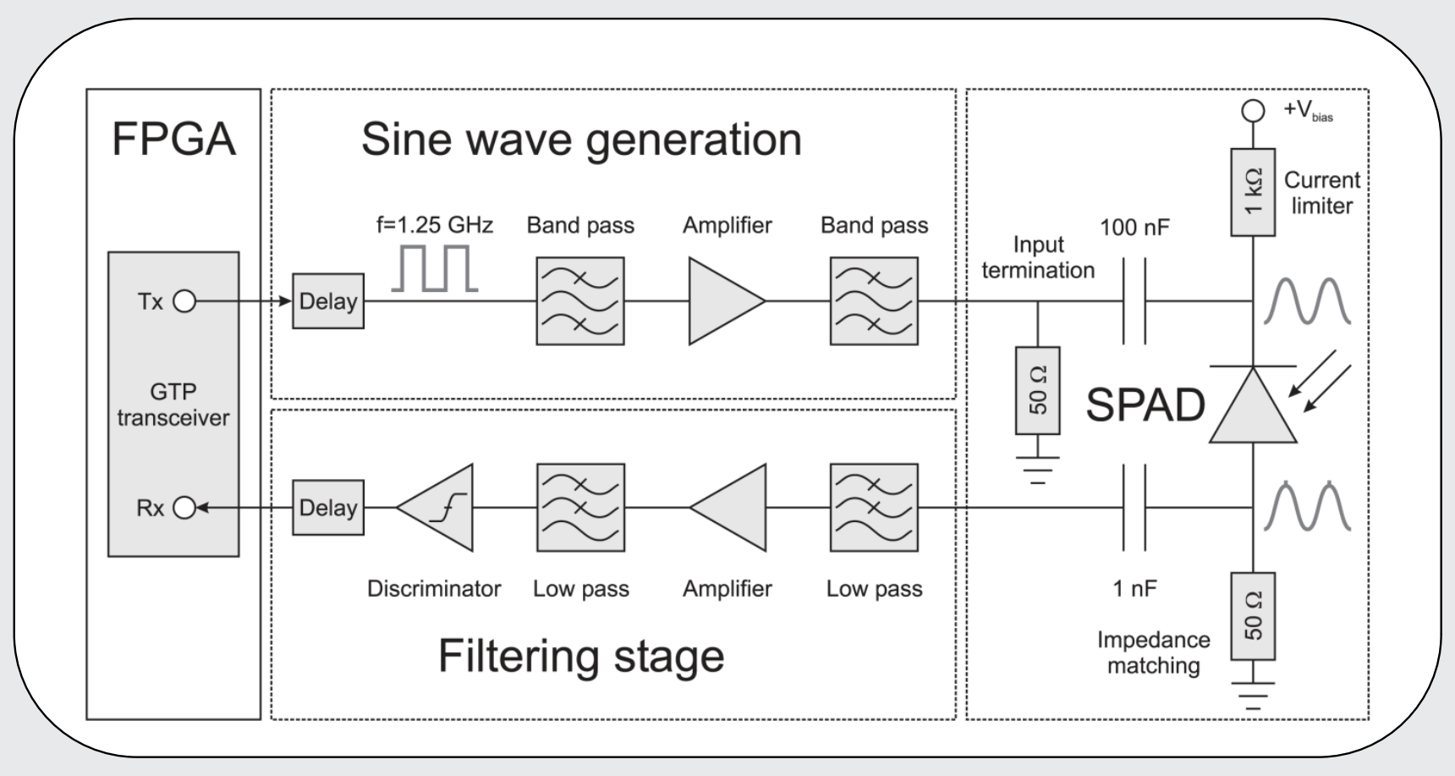
- High-speed Quantum key distribution (QKD) based on the Coherent One-Way protocol

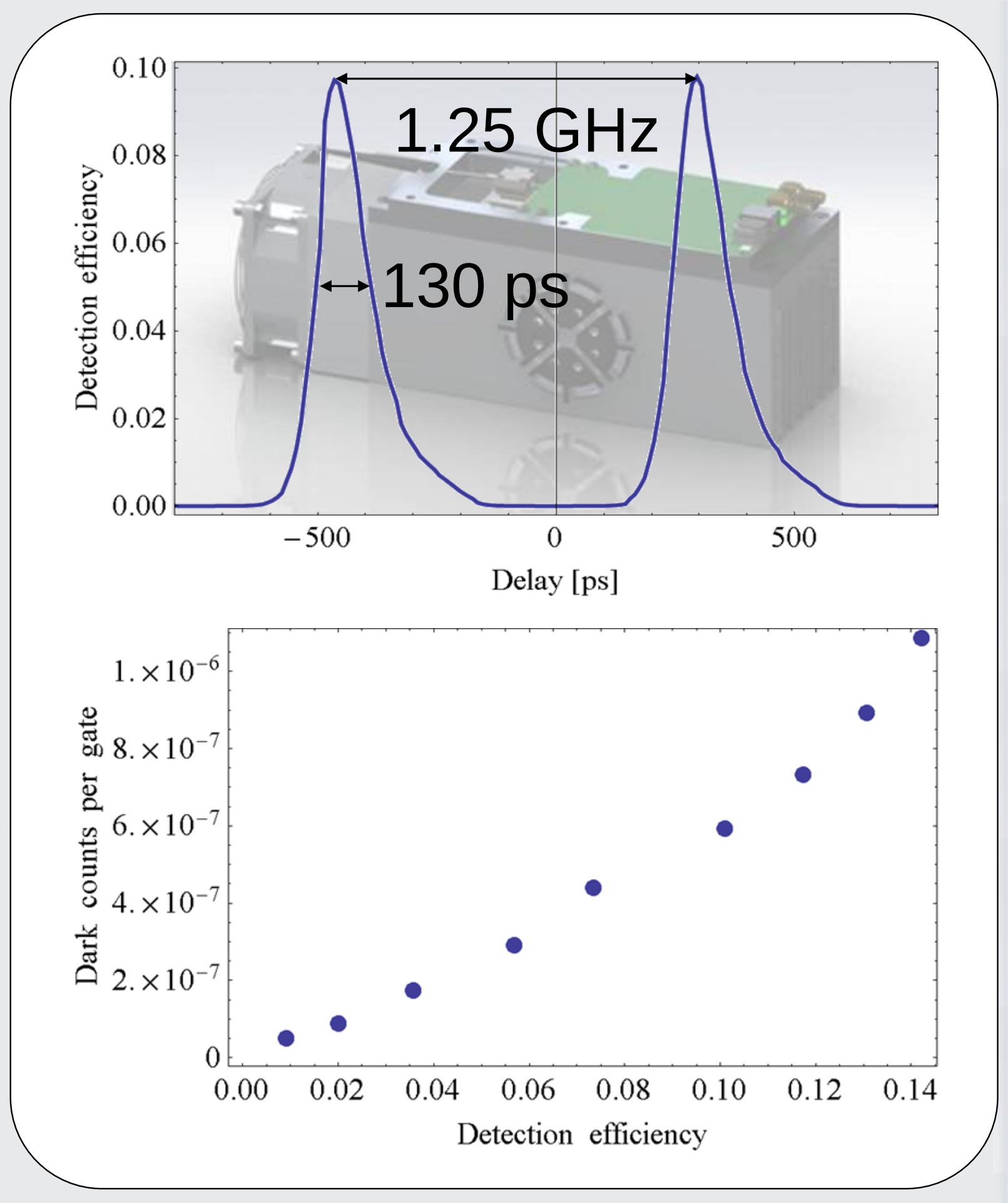


- Robust but simple bit measurement without active elements at Bob
- Interference visibility as measure of eavesdropper's information
- Robust against USD and PNS attacks

Fast single photon detectors

We implemented a gate technique where a pure sinusoidal gate with fix frequency is applied to the APD. After a photon detection, the avalanche is filtered from the sine signal and subsequently amplified and discriminated.



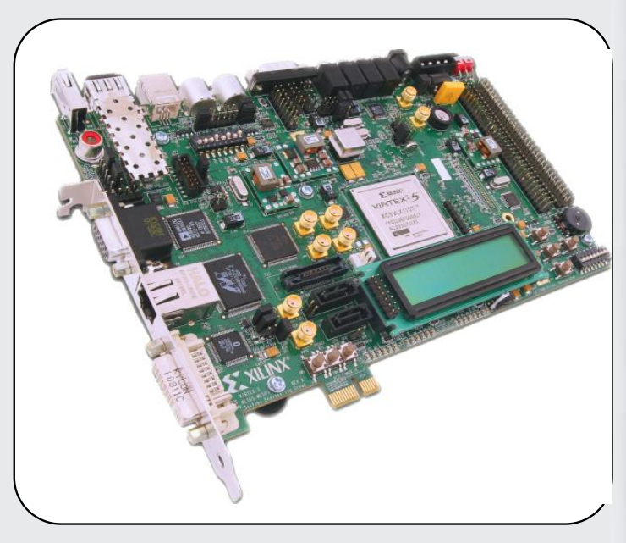


Characteristics

- High gate frequencies up to 2.3 GHz
- at η = 10% ↔ pdark = 6·10-7 per gate
- Low afterpulse probability < 1%
- High detection rates > 33 MHz
- Room temperature operation
- Compact design

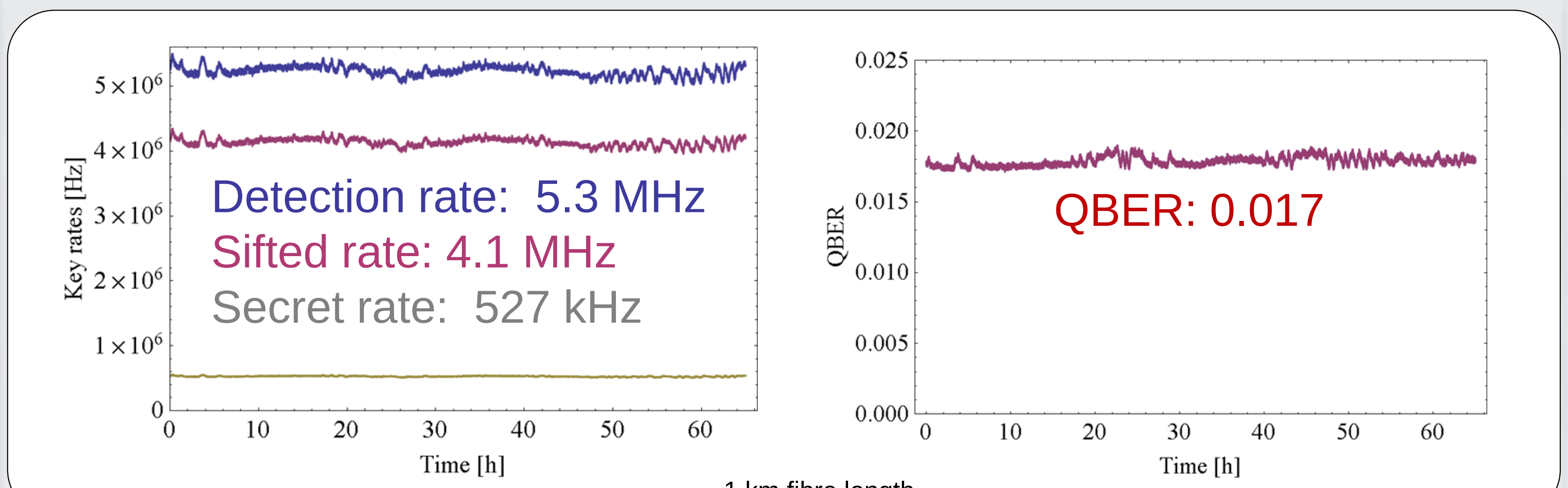
Hardware key distillation

- Sifting: Optimized for different fiber transmission losses
- Parameter estimation: 12.5 % random sampling or by direct comparison
- Error correction: Low density parity checks (LDPC) with flexible code rates (1/2, 2/3, 3/4, 5/6)
- Error verification: Universal hashing
- Privacy amplification: Toeplitz hashing over 995,328 bits
- Authentication: Polynomial hashing with QKD key reuse

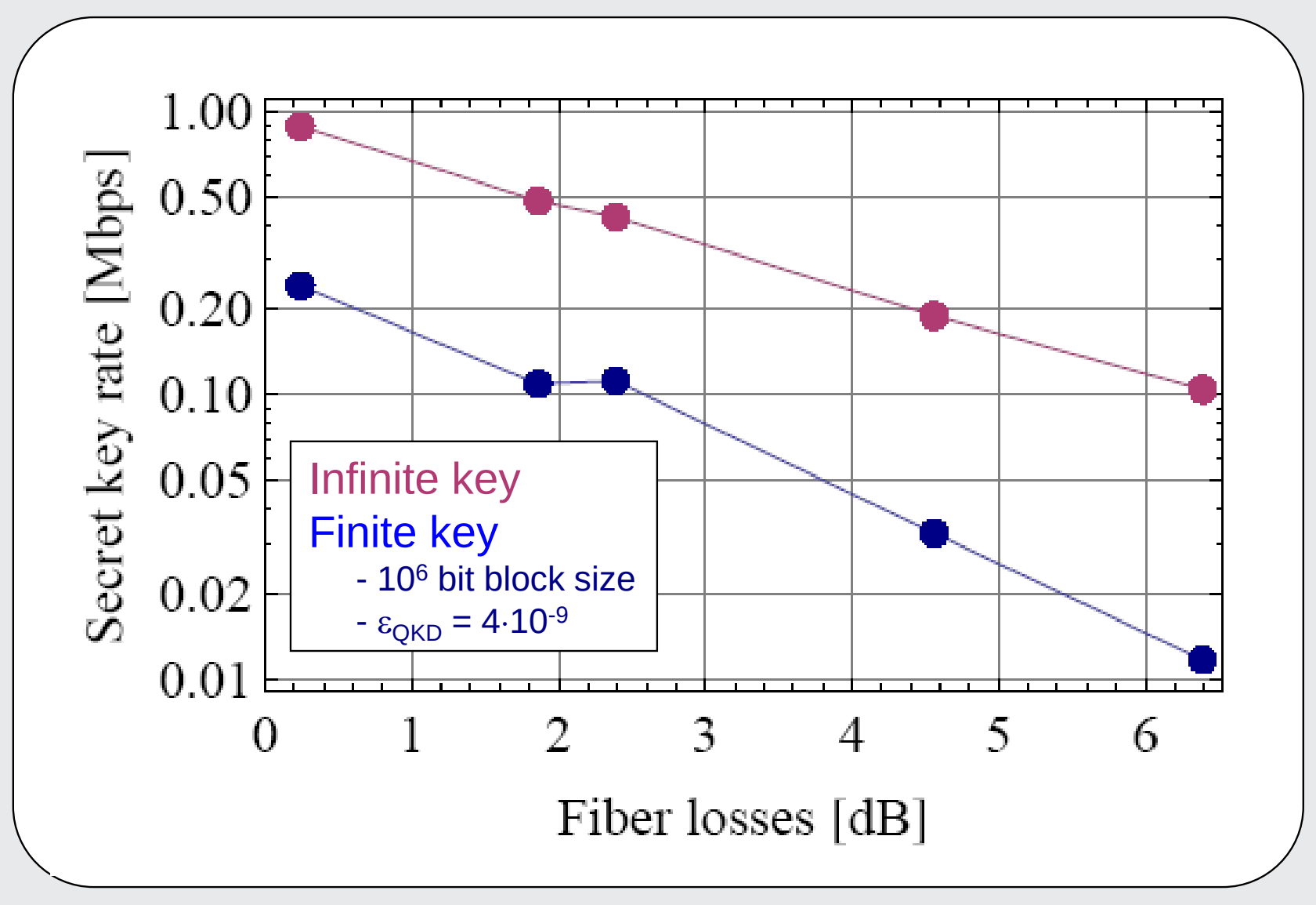


Results

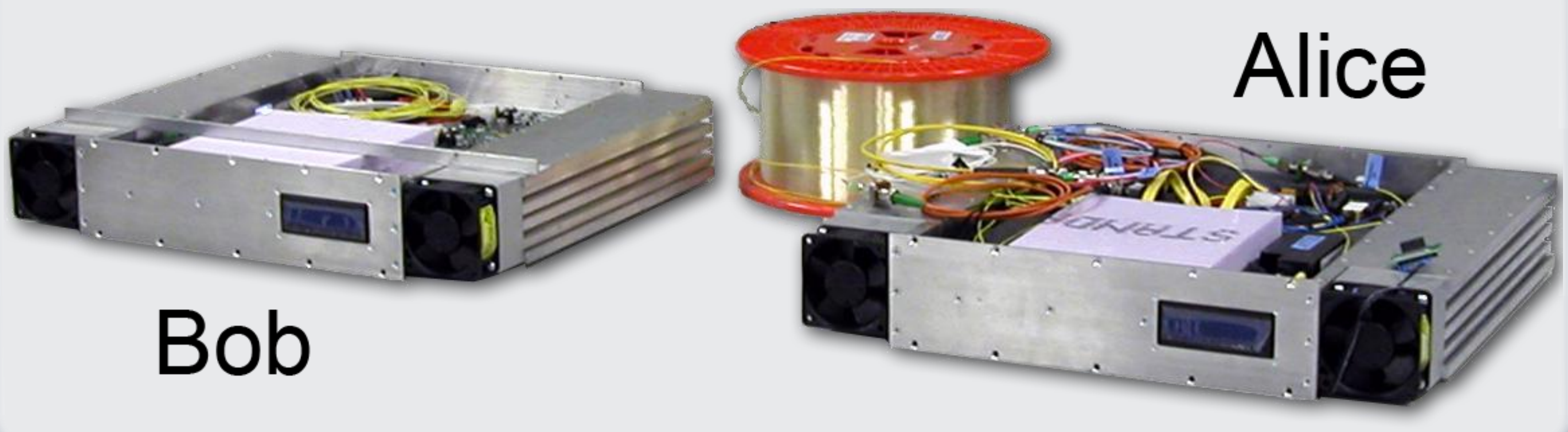
- Sine gating data detector and free-running monitor detector
- Wavelength multiplexing of all communication channels over a single fibre
- Hardware distillation engine:
  - 10^6 bit post-processing block size
  - Security parameter $\varepsilon_{QKD} = 4{\cdot}10^{-9}$



1 km fibre length



- Up to 890 kbps for short distances (250 kbps with finite key security)
- More than 100 kbps over 20 km (12 kbps with finite key security)
- Low QBER down to 1.7 %
- Stable performance over > 60 hours
- Compact tamper proof housing



Principal investigator: Nicolas Gisin (Nicolas.Gisin@unige.ch)

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