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

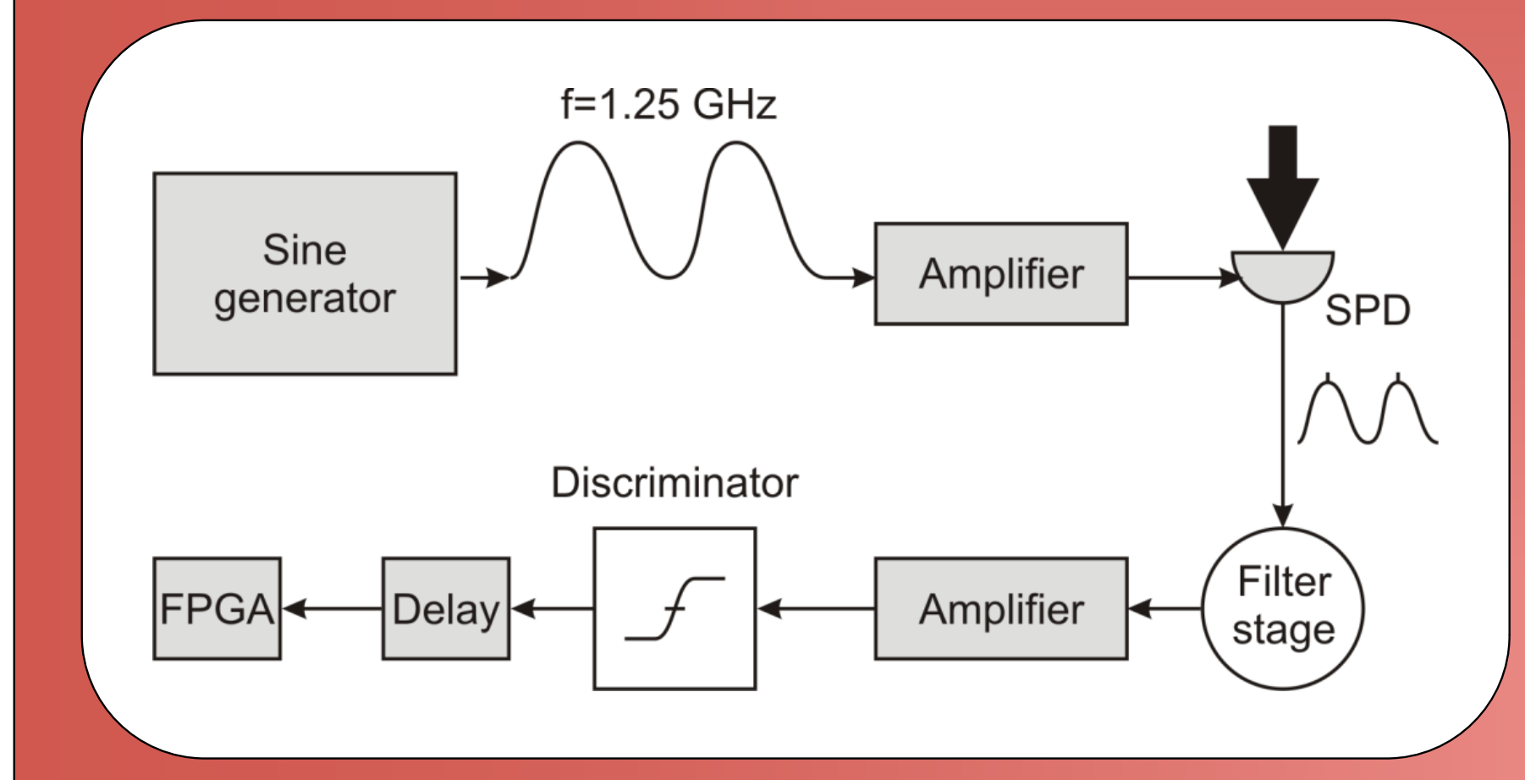
UNIVERSITÉ DE GENÈVE · ETH Zürich · EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE · Hes·so Haute Ecole Spécialisée de Suisse occidentale · IDQ

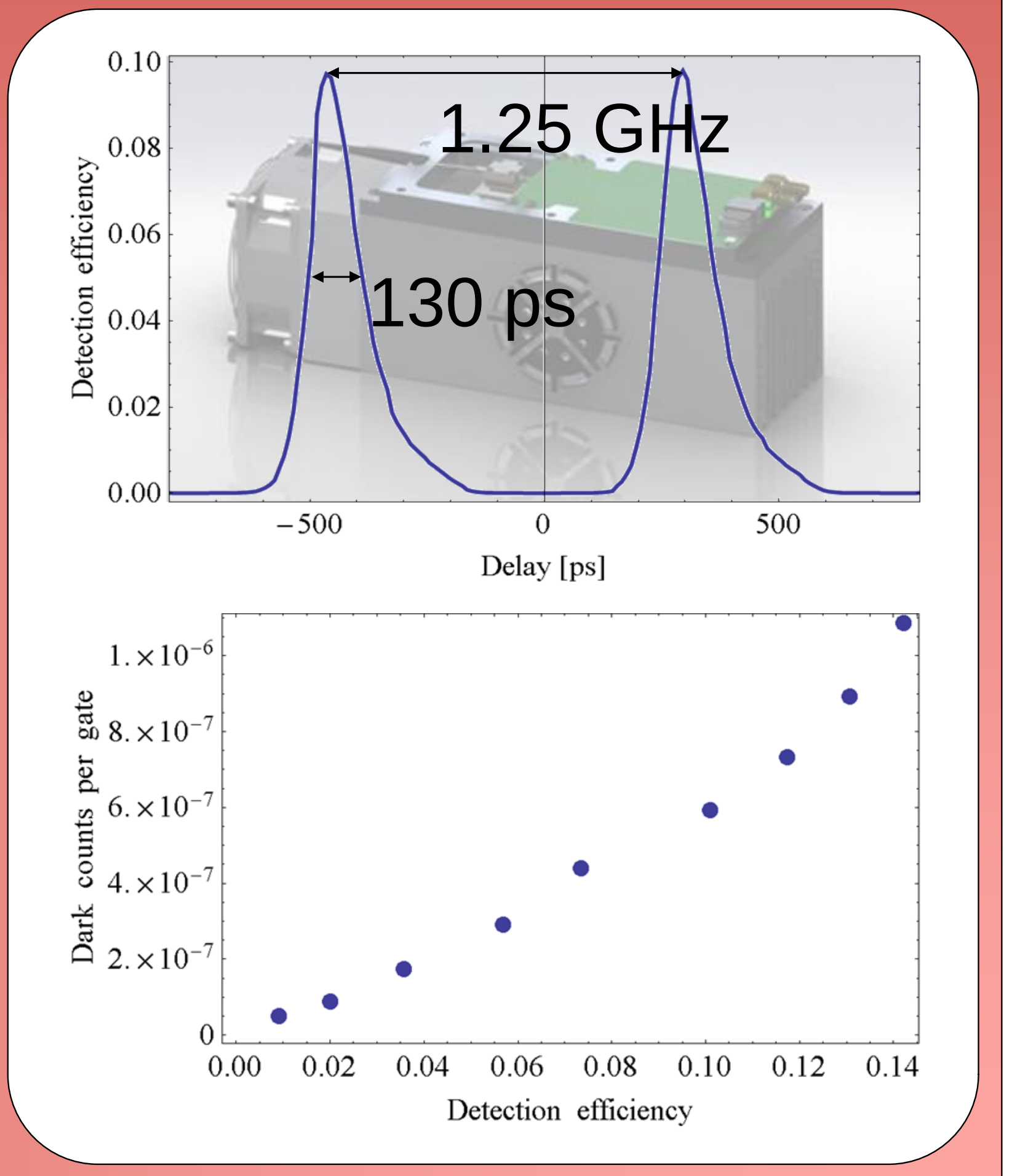
Introduction

Quantum key distribution (QKD) is the most complex and advanced application of quantum physics adopted commercially today. We currently develop a high speed QKD enhanced encryption engine based on a modified 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. To potentially relax the hardware requirements in a finite key scenario we improved the finite key security proof for BB84.

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.



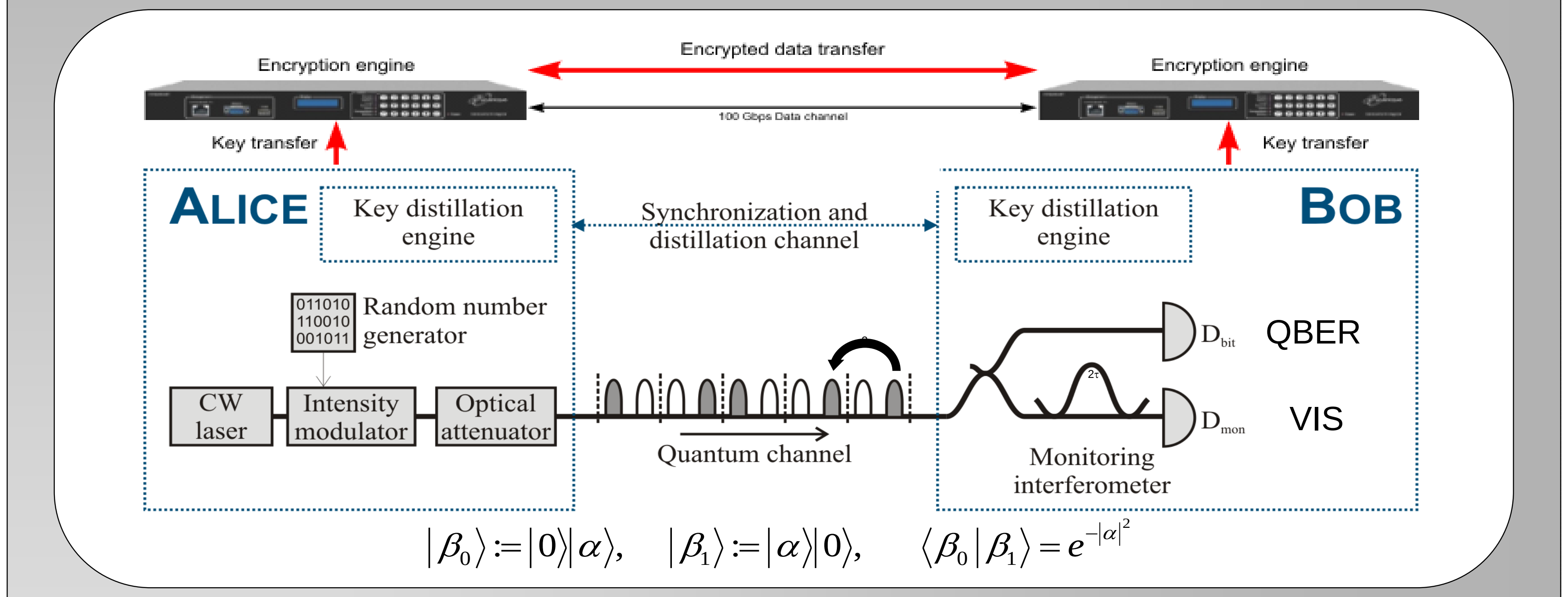


Characteristics

- High gate frequencies up to 2.3 GHz
- at η = 10% ↔ p_{dark} = $6{\cdot}10^{-7}$ per gate
- Low afterpulse probability < 1%
- Low dead time of 8 ns
- High detection rates > 33 MHz
- Compact design

High rate coherent one-way QKD system

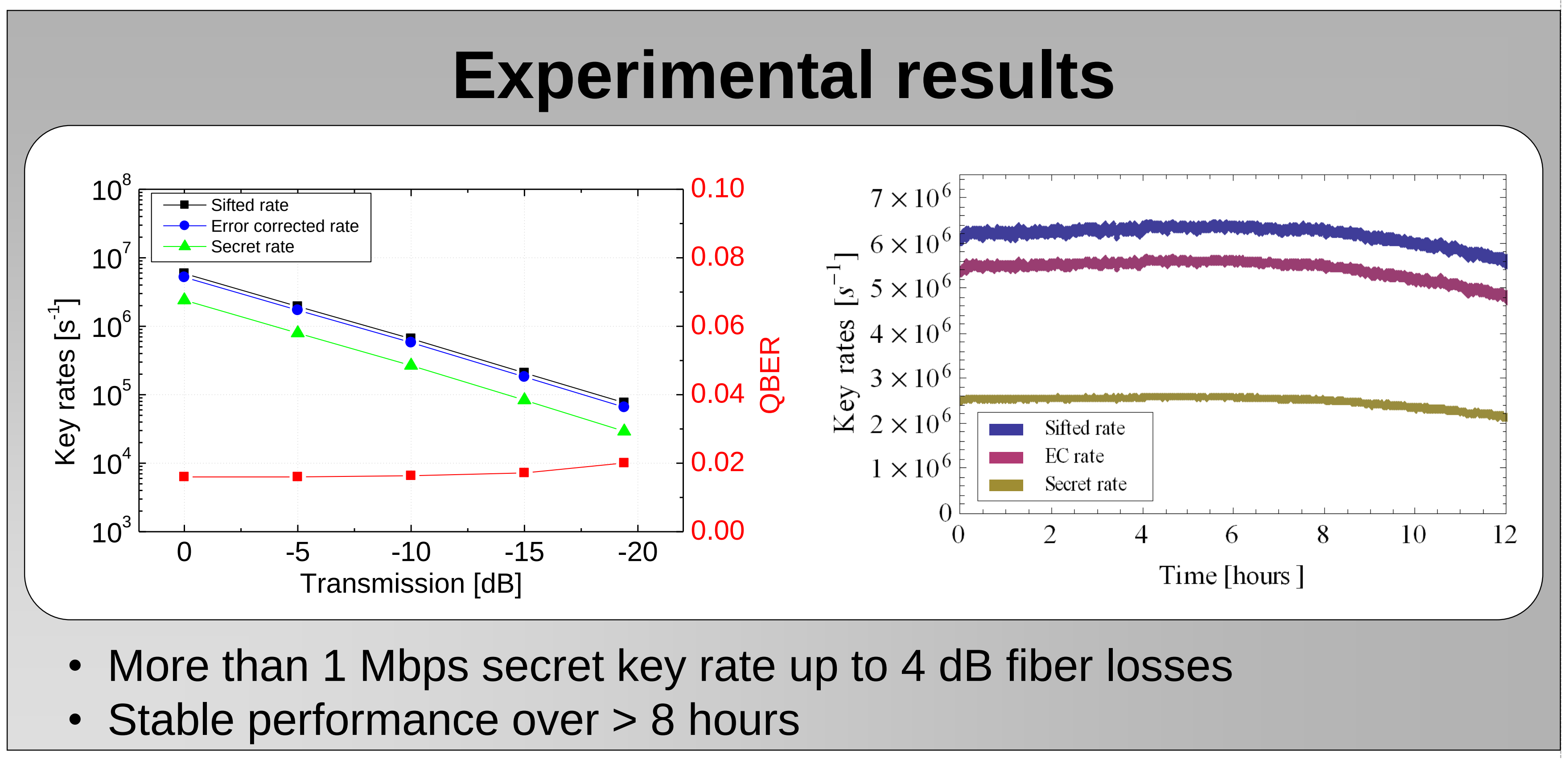
- High-speed Quantum key distribution (QKD) based on the Coherent One-Way protocol
- 1 Mbps one-time pad encryption (OTP)
- Wavelength-division multiplexing over a single fibre



$$|\beta_0\rangle := |0\rangle|\alpha\rangle, \quad |\beta_1\rangle := |\alpha\rangle|0\rangle, \quad \langle\beta_0|\beta_1\rangle = e^{-|\alpha|^2}$$

- 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

Experimental results



- More than 1 Mbps secret key rate up to 4 dB fiber losses
- Stable performance over > 8 hours

Tight finite key analysis

Most pre-existing security proofs require the assumption of asymptotically large statistics! Previous known results indicates that practical QKD is not feasible unless one processes large block of data (~10^6). Moreover, it is only valid for a restricted class of attacks.

In our work, we prove a finite-key security proof framework that allows one to consider all attacks and only data size of (~10^4) is required.

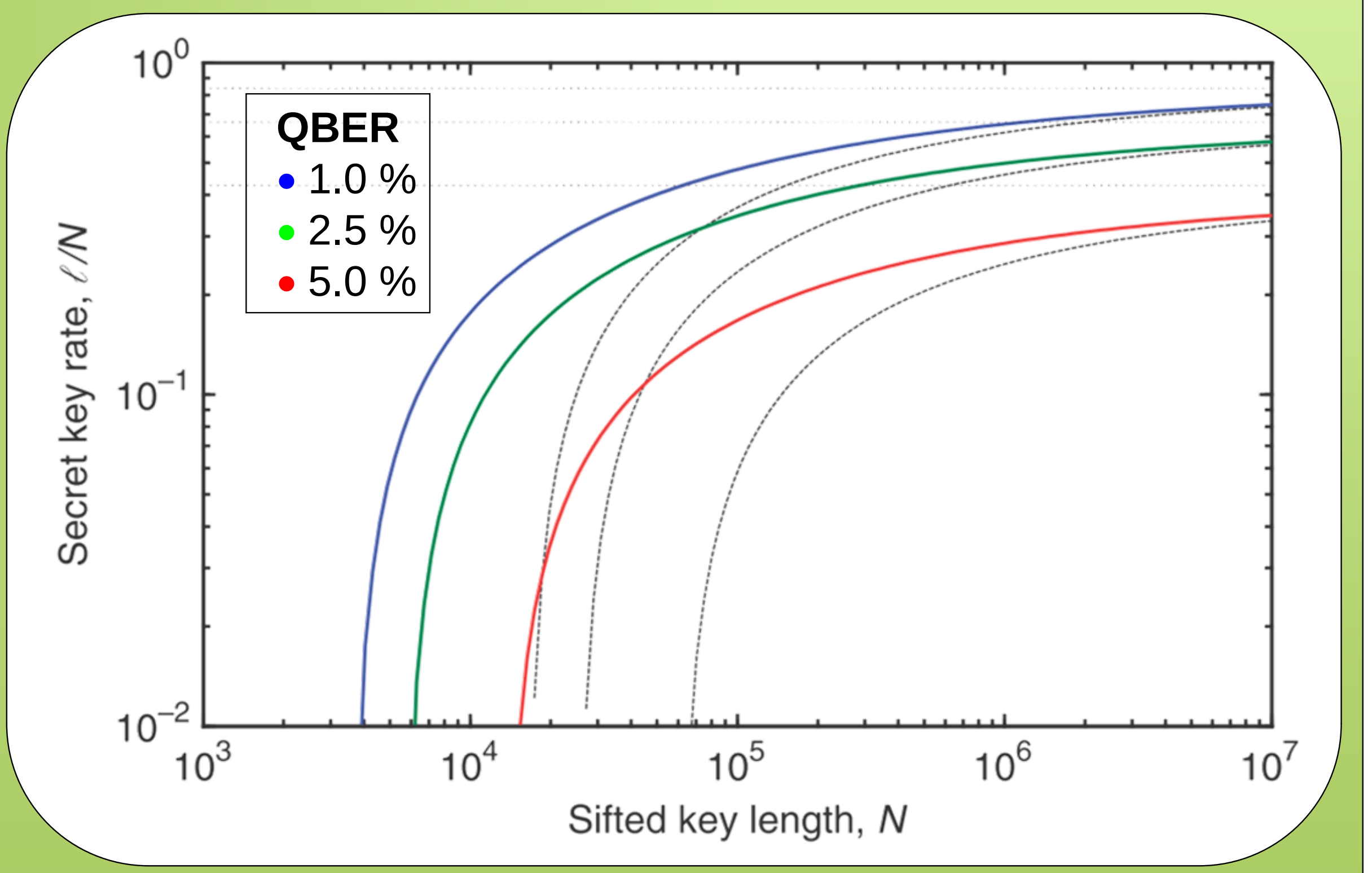
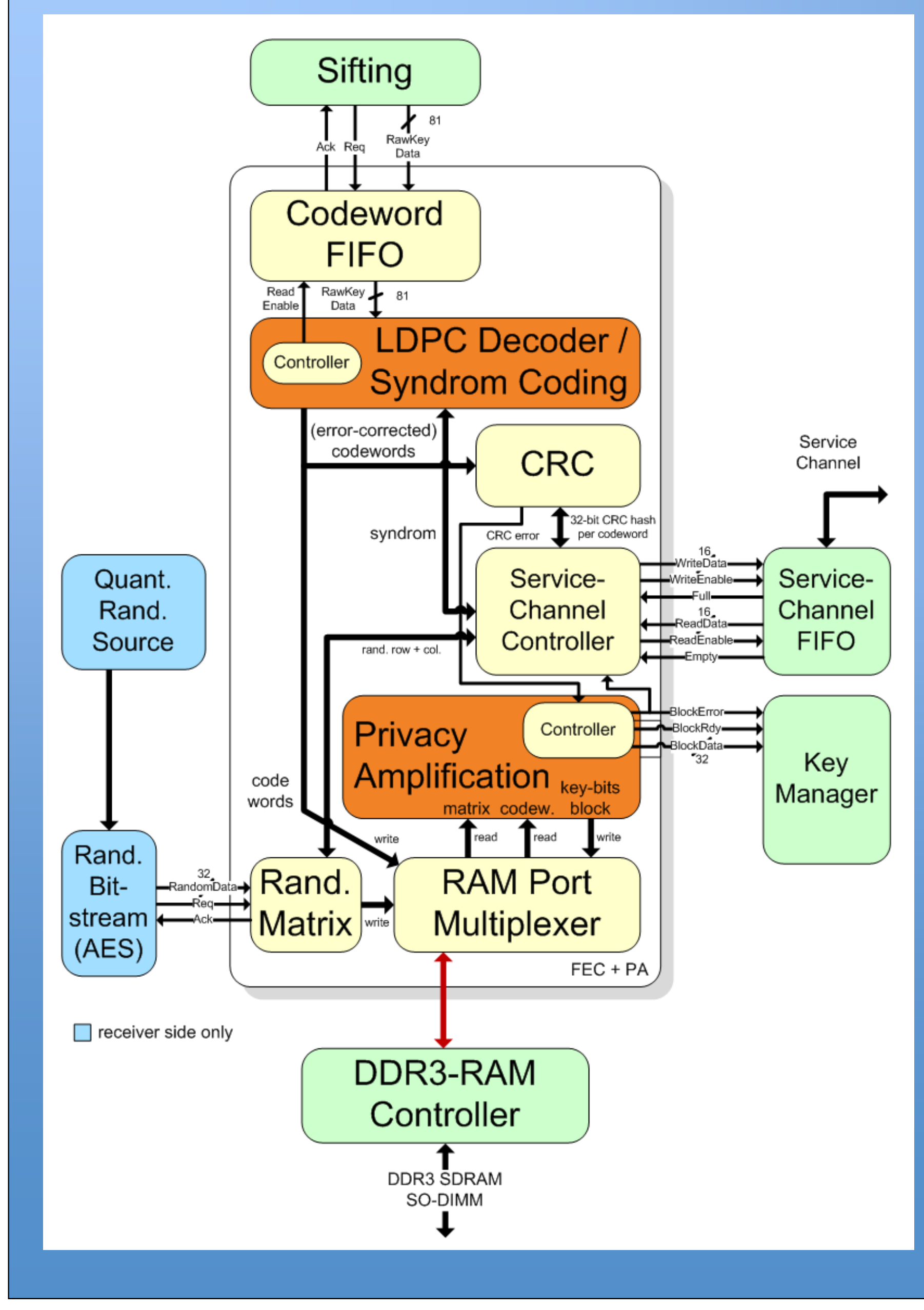
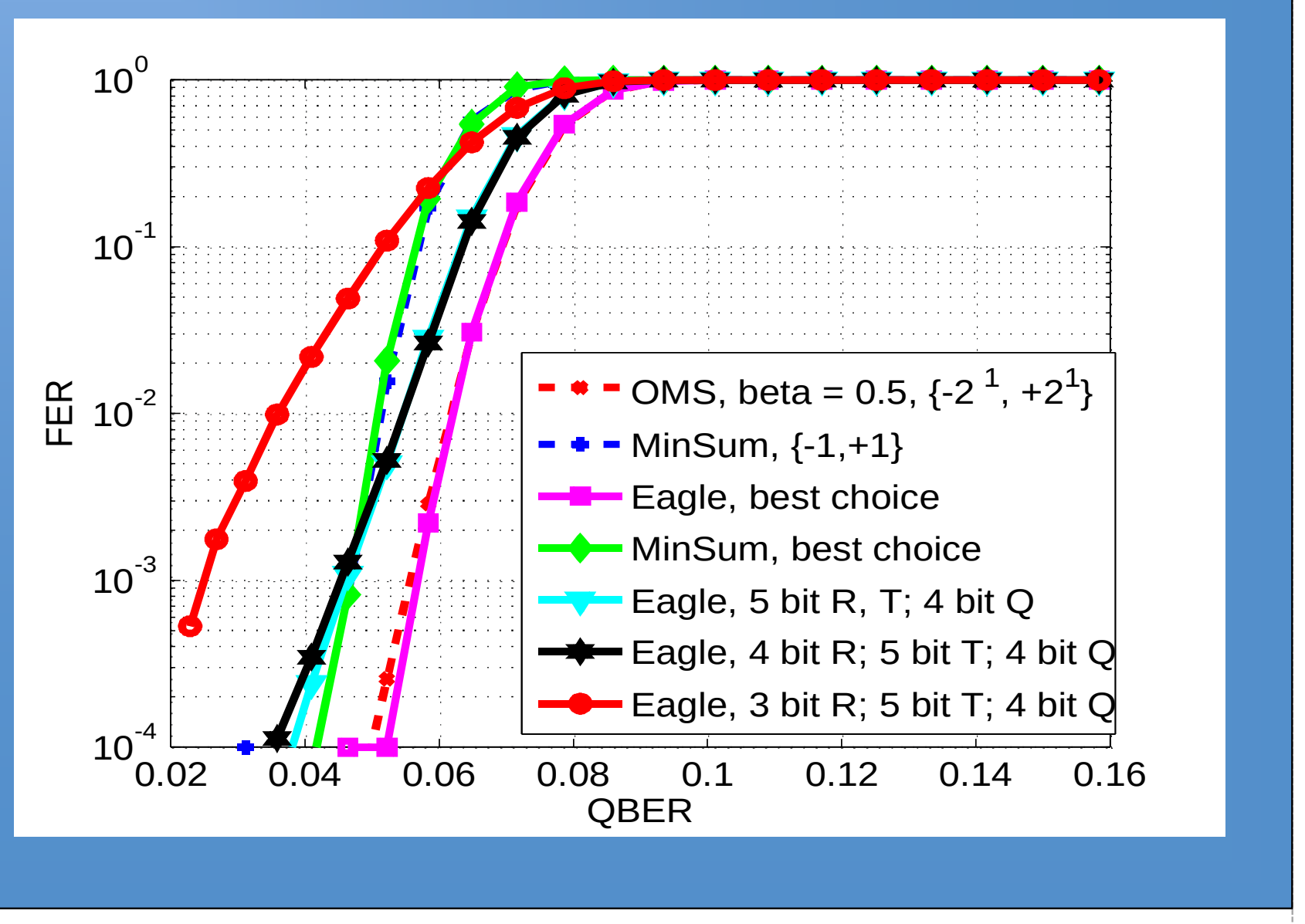


Fig: The colour lines are given by our finite-key security framework, with the error rates given by: top to bottom (1%, 2.5%, 5%). The dashed lines represent the previous known results.

Quantum key distillation process



- **Forward error correction** using **LDPC** codes
  - QC code based on 802.11n
  - syndrom encoding
- Flexible code rates (½, ⅔, ¾, ⅚)
- Throughput decrease of **0.5%** at 6% QBER
- **Privacy Amplification** using Toeplitz matrices
  - Matrix-vector product **10^6**x**10^5**
- PA ratio is adjustable



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

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