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

QCrypt RTD 2010

FNSNF

QKD key distillation engine

R. Houlmann[1], J. Constantin[2], Andreas Burg [2], Fabien Vannel[3], Pascal Junod[3], Nino Walenta[1], Olivier Guinnard[1], Charles L. Ci Wen[1] and Hugo Zbinden[1]

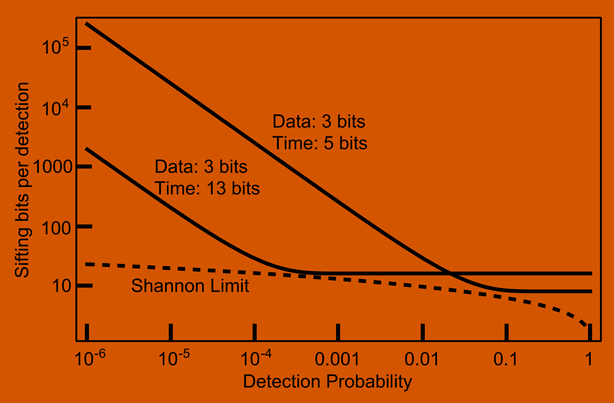
[1]GAP Optique, University of Geneva, [2]IEL EPFL Lausanne , [3]HES-SO Yverdon

Goals

- Distillation engine running with a single FPGA device (Virtex 6) on each device
- Supports high-speed coherent one-way platform (COW) support but is in principle independent of the respective QKD protocol or optical implementation
- All distillation communication over an authenticated service channel multiplexed in time
- An OTP (One-Time Pad) encryption over the classical channel
- Distillation of at least 1 Mb secret keys per second

Sifting

- Encoding of sifting information done in order to minimize the bandwidth usage on the classical channel

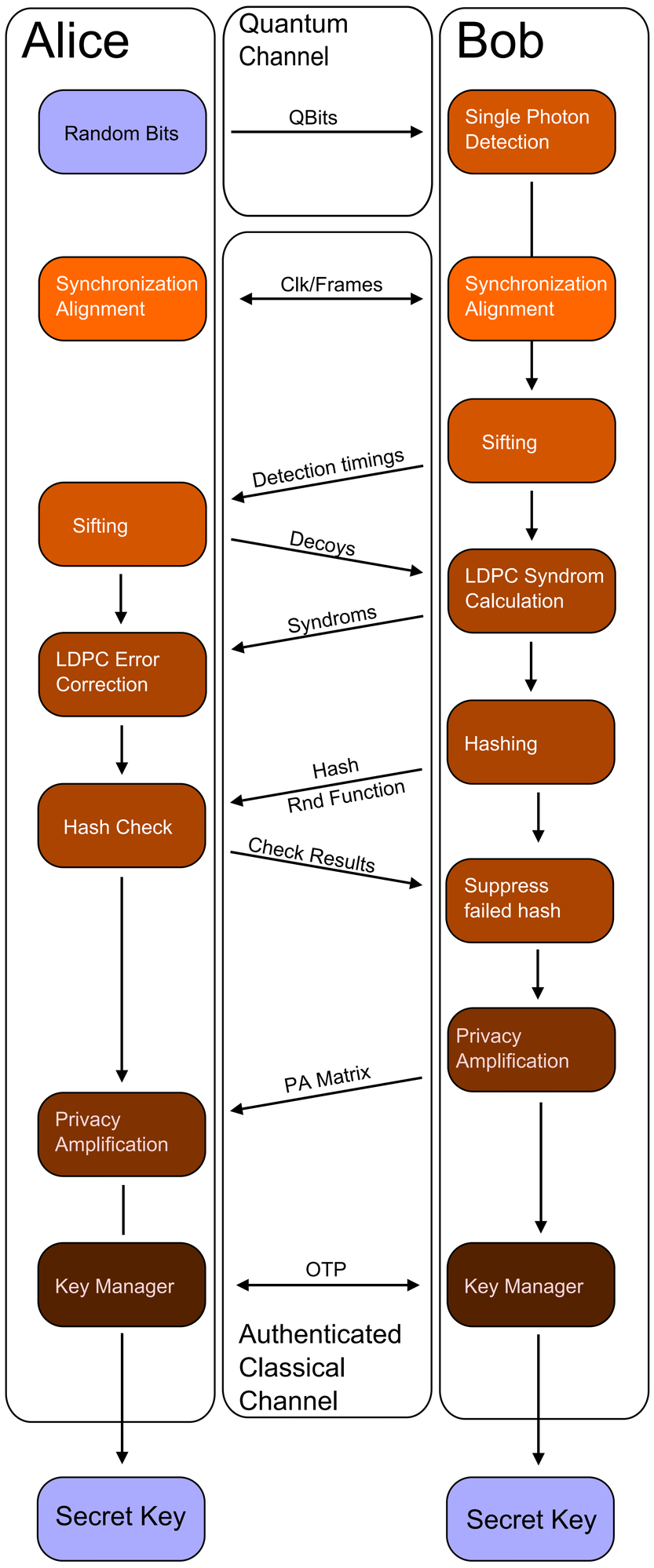


- Sifting is done in real time in order to minimize the size of Alice' buffers
- Parameter estimation selectable to evaluate QBER
- Possible configurations for different quantum protocols

Results

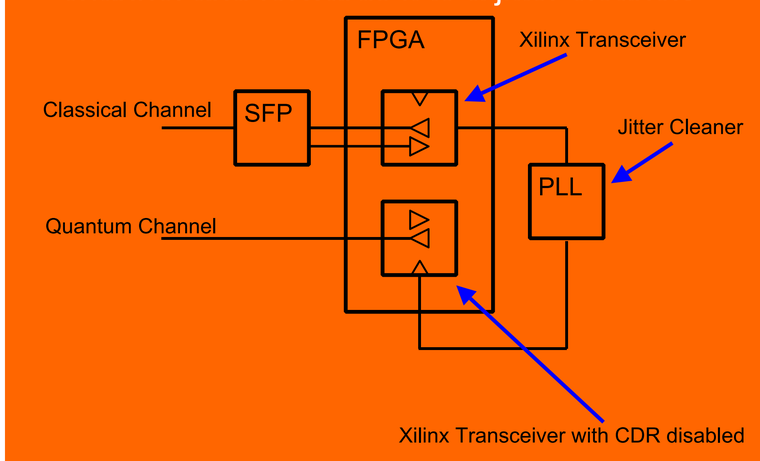
- Secret key distillation at a rate of up to 4 Mbit/s
- Implemented in a single FPGA (Virtex-6)
- OTP channel integrated to encrypt with quantum keys at the best level of security
- Classical channel fully authenticated with quantum keys
- Flexible configurations for different distances and detection rates
- Possibility to multiplex classical and quantum channel in a single fiber
- Initial entropy created with quantum random number generators
- Model parameter verification in real time to discard unsecure key bits
- Base frequency adaptable to precise interferometer disbalance length

Data Flow



Synchronization and Alignment

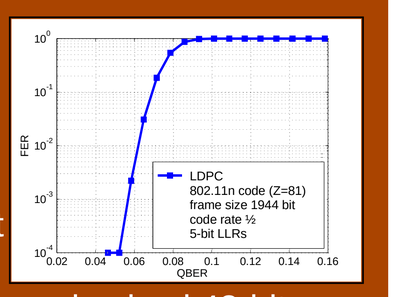
- Both machines are completely synchronous, Bob recovers Alice's clock on the classical channel and forwards it to a jitter cleaner.



- Specific frames are used to align the quantum channel with respect to the classical channel
- Data from the Quantum channel is sampled with a transceiver (Clock recovery disabled) synchronous with the emission

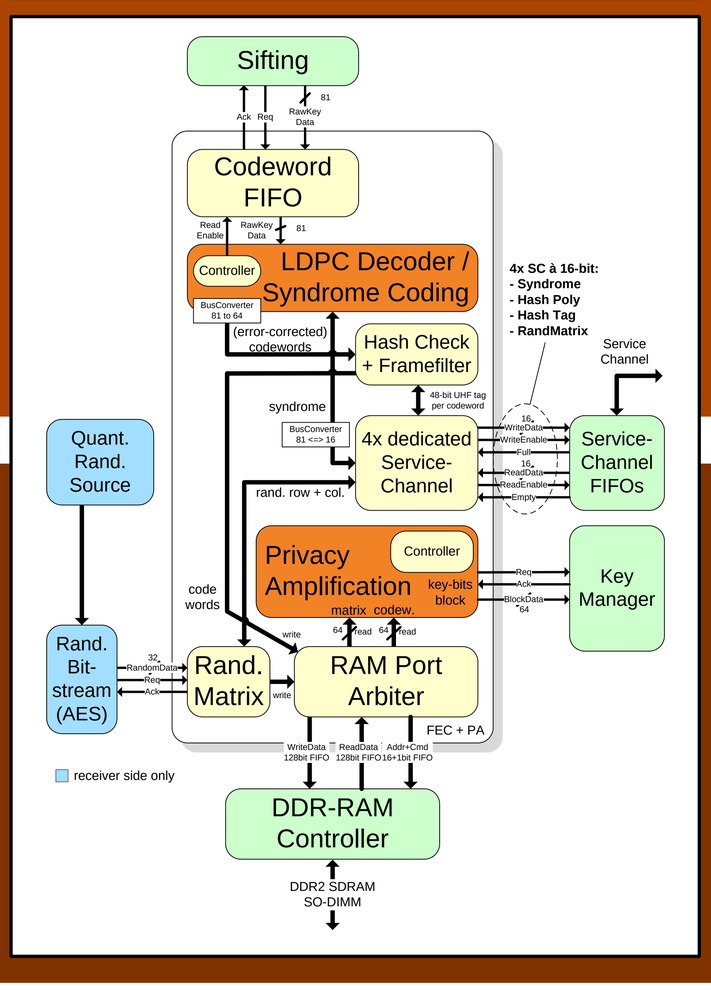
Error Correction

- Syndrome encoding
- Error correction using QC-LDPC decoder
- Flexible code rates of ½, ⅔, ¾, ⅚ allow adaptation for different QKD link distances



- Frame filtering using a randomized 48-bit universal hash function (polynomial hashing)

Residual frame error rate of only 0.5% at 6% QBER



Privacy Amplification

- Toeplitz hashing (Toeplitz matrices)
- Random matrix ($10^6 + 10^5$ random bits)
- Matrix-vector multiplication: $10^6 \times 10^5$
- Slice-based processing of multiplication inside the FPGA: 512 parallel accumulator units (rows)
- Online configurable compression ratio (0-100%)
- Output key rate of 2 or 4 Mbit/s (32-bit / 64-bit MACs)

$$A = \begin{bmatrix} a_0 & a_{-1} & a_{-2} & \dots & \dots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \ddots & & \vdots \\ a_2 & a_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{-1} & a_{-2} \\ \vdots & & \ddots & a_1 & a_0 & a_{-1} \\ a_{n-1} & \dots & \dots & a_2 & a_1 & a_0 \end{bmatrix}$$

Highly scalable and flexible PA design supporting any compression ratio

Contact:Raphael Houlmann (Raphael.Houlmann@unige.ch)