nano-tera.ch

QCRYPT

1 Mbps coherent one-way QKD with dense wavelength division multiplexing and hardware key distillation

Nino Walenta

University of Geneva, GAP-Optique

Singapore, 11.09.2012

UNIVERSITÉ DE GENÈVE

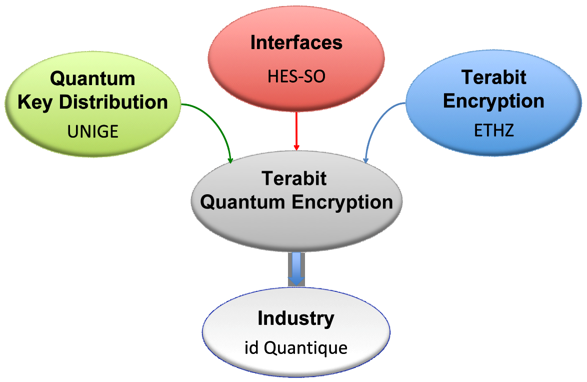
EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

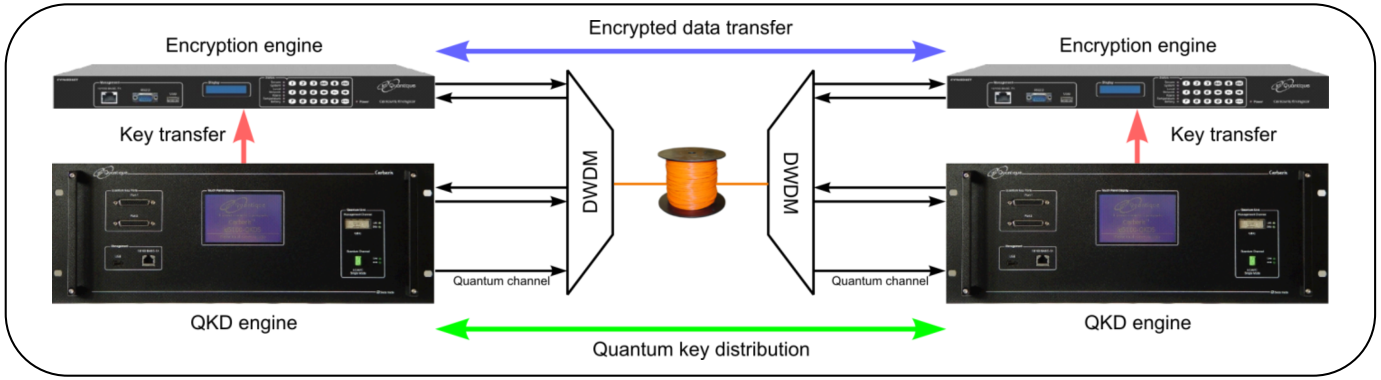
ETH Zürich

Hes·so Haute Ecole Spécialisée de Suisse occidentale

IDQ FROM VISION TO TECHNOLOGY

The Nano-Tera QCrypt project





Nino Walenta, Charles Lim Ci Wen, Tomasso Lunghi, Raphael Houlmann,
Olivier Guinnard, Christopher Portmann, Hugo Zbinden, Rob Thew, Nicolas Gisin

Etienne Messerli, Pascal Junod, Gregory Trolliet, Fabien Vannel, Olivier Auberson, Yann Thoma

Norbert Felber, Christoph Keller, Christoph Roth, Andy Burg

Patrick Trinkler, Laurent Monat, Samuel Robyr, Lucas Beguin, Matthieu Legré, Grégoire Ribordy

UNIVERSITÉ DE GENÈVE

EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

ETH Zürich

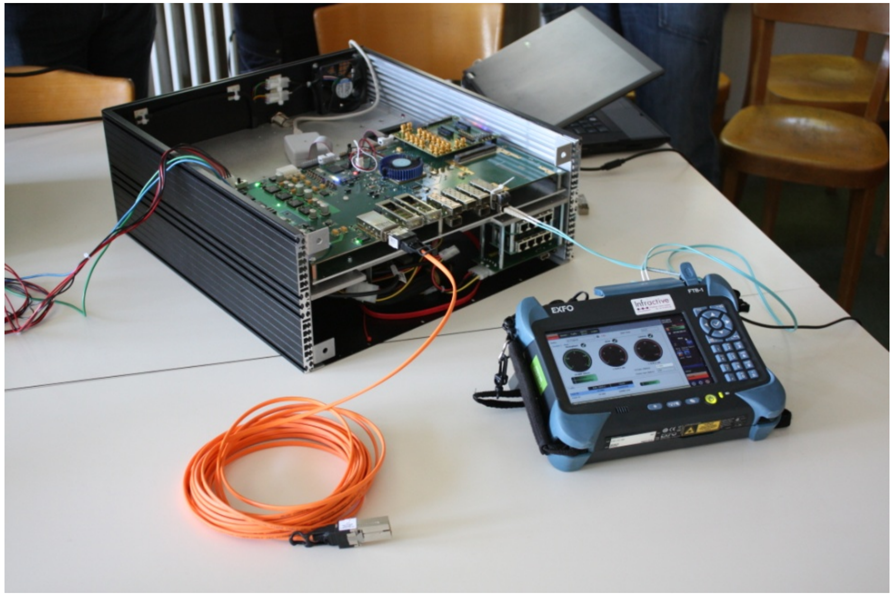
Hes·so Haute Ecole Spécialisée de Suisse occidentale

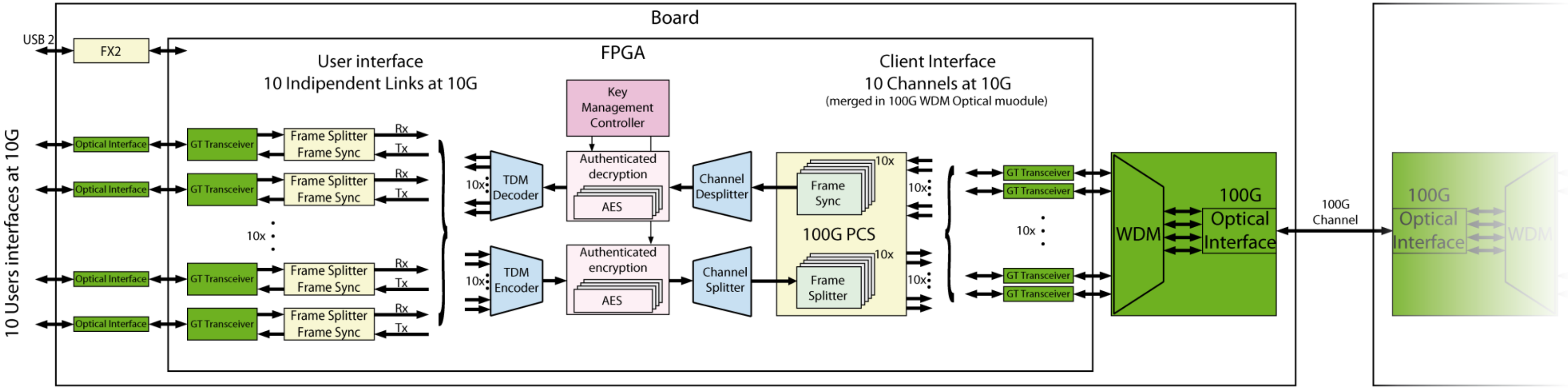
IDQ FROM VISION TO TECHNOLOGY

100 Gbit/s Encryption engine

FPGA design and 100 Gbps Interface

- User side: 10 x 10 Gbit/s Ethernet channels through 10 SPF+ optical modules
- Client side: 1 x 100 Gbit/s channel over a single fibre using 10 x 10 Gbit/s WDM optical modules
- Tamper proof
- Certification

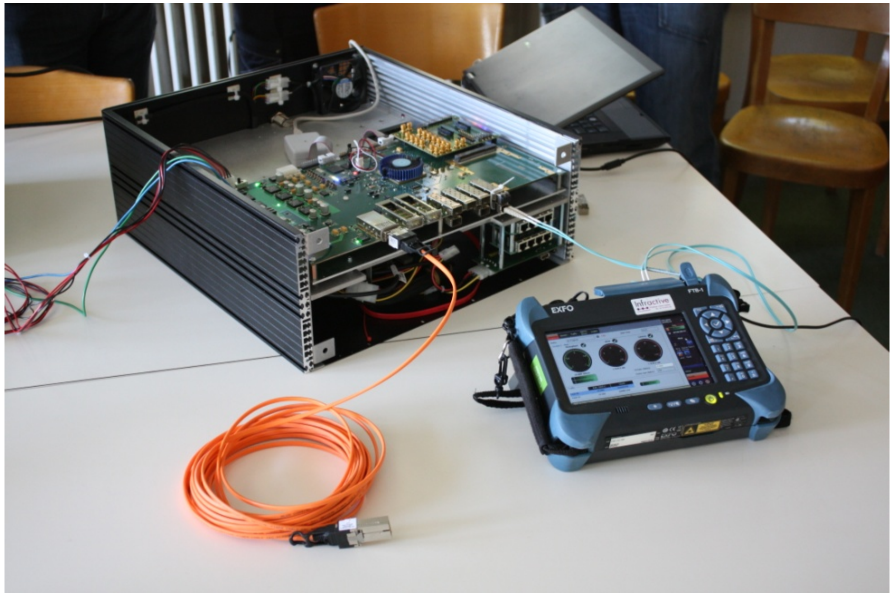




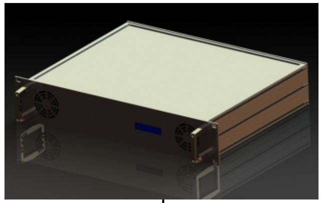
100 Gbit/s Encryption engine

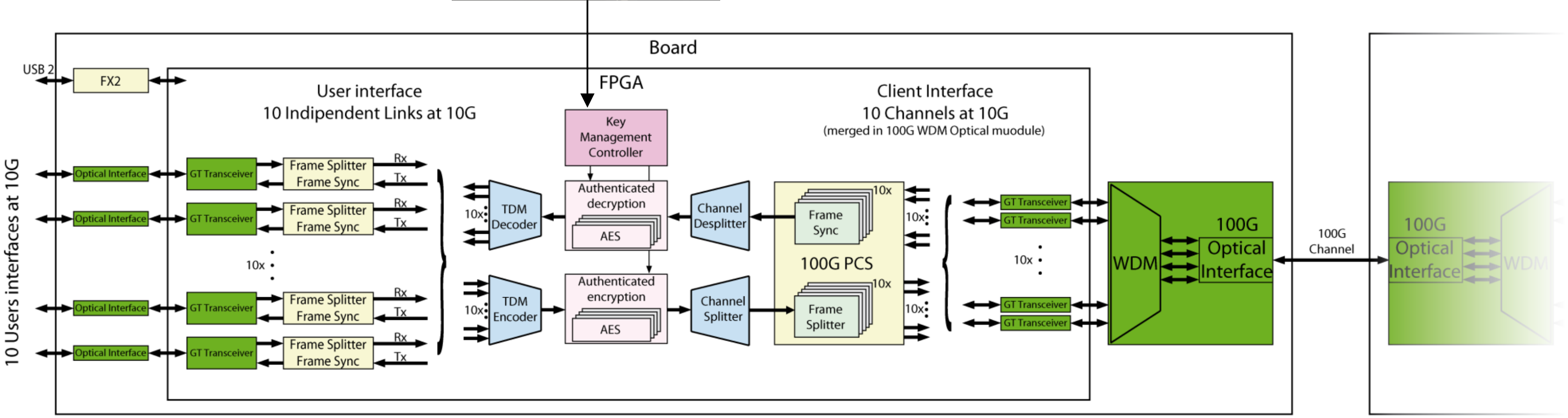
FPGA design and 100 Gbps Interface

- User side: 10 x 10 Gbit/s Ethernet channels through 10 SPF+ optical modules
- Client side: 1 x 100 Gbit/s channel over a single fibre using 10 x 10 Gbit/s WDM optical modules
- Tamper proof
- Certification



QKD Engine





nano-tera.ch

QCRYPT

Fast coherent-one way quantum key distribution and high-speed encryption

1. The COW QKD platform
2. The hardware key distillation engine
3. Telecom single photon detectors
4. Finite key results
5. Outlook and conclusions

UNIVERSITÉ DE GENÈVE

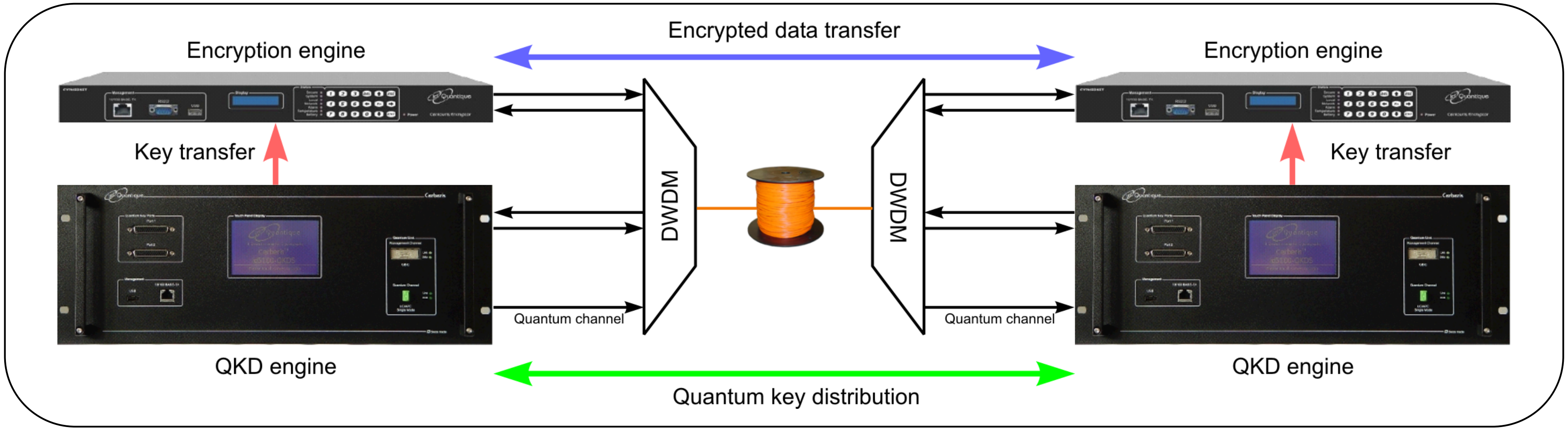
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

ETH Zürich

Hes·so Haute Ecole Spécialisée de Suisse occidentale

IDQ FROM VISION TO TECHNOLOGY

QCrypt Specifications



1 Mbps QKD platform

- 625 Mbps clocked QKD
- 1.25 GHz Rapid gated single photon detectors
- Hardware key distillation
- 1 Mbps One-Time-Pad encryption
- 1-fibre DWDM configuration
- Continuous operation

100 Gbps Encryptors

- 10 Ethernet channels at 10 Gbps
- 100 Gbps AES encryption engine
- 100 Gbps data channel over a single fiber

- Tamper proof
- Certification

UNIVERSITÉ DE GENÈVE

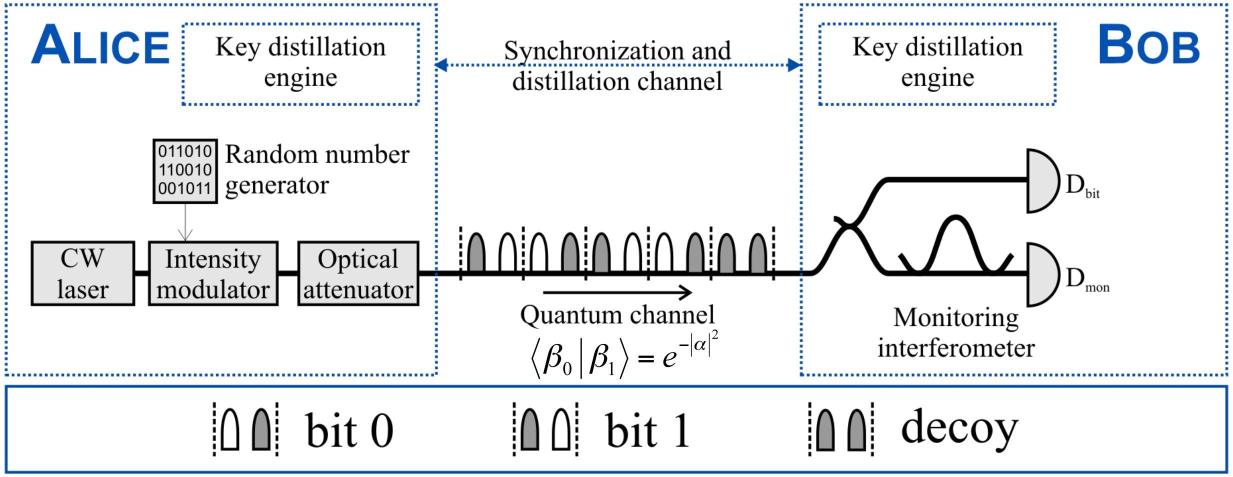
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

ETH Zürich

Hes·so Haute Ecole Spécialisée de Suisse occidentale

IDQ FROM VISION TO TECHNOLOGY

Coherent One-Way quantum key distribution



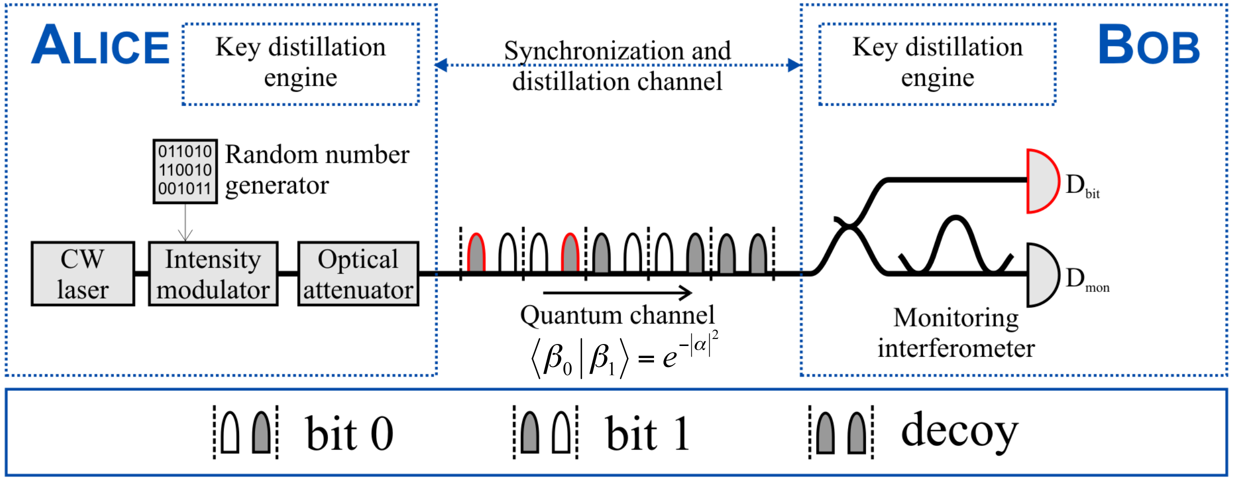
Characteristics

- No active elements at Bob
- Robust bit measurement basis
- Robust against PNS attacks
- Security proof for zero error attacks and some collective attacks

Poster 24: C. W. Lim. *Finite-key security analysis of a simple and efficient one-way quantum cryptography system.*

Poster 51: T. Moroder et al. *Security of distributed-phase-reference quantum key distribution.* arXiv:1207.5544v1 [quant-ph].

Coherent One-Way quantum key distribution



→ QBER

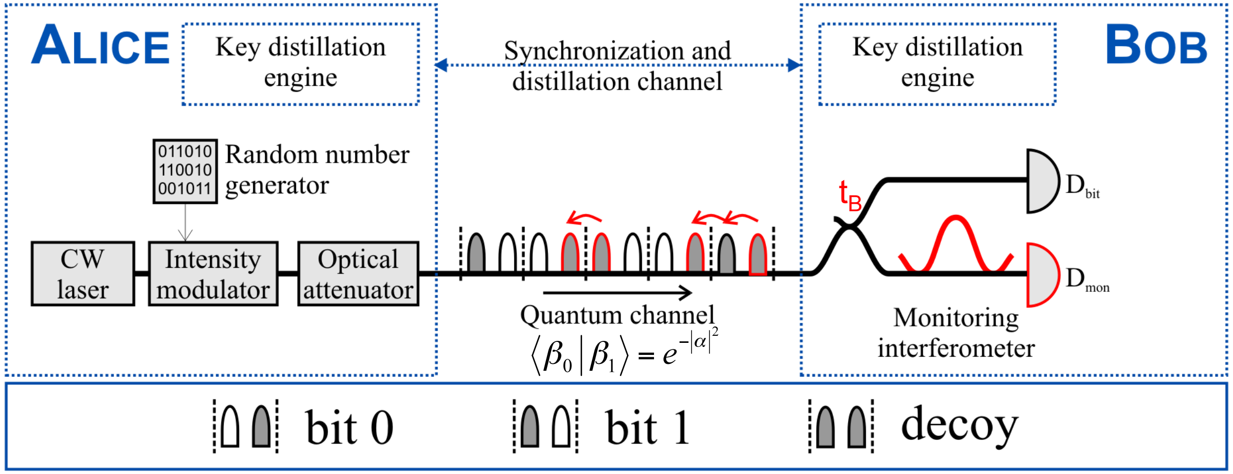
Characteristics

- No active elements at Bob
- Robust bit measurement basis
- Robust against PNS attacks
- Security proof for zero error attacks and some collective attacks

Poster 24: C. W. Lim. *Finite-key security analysis of a simple and efficient one-way quantum cryptography system.*

Poster 51: T. Moroder et al. *Security of distributed-phase-reference quantum key distribution.* arXiv:1207.5544v1 [quant-ph].

Coherent One-Way quantum key distribution



→ **QBER**

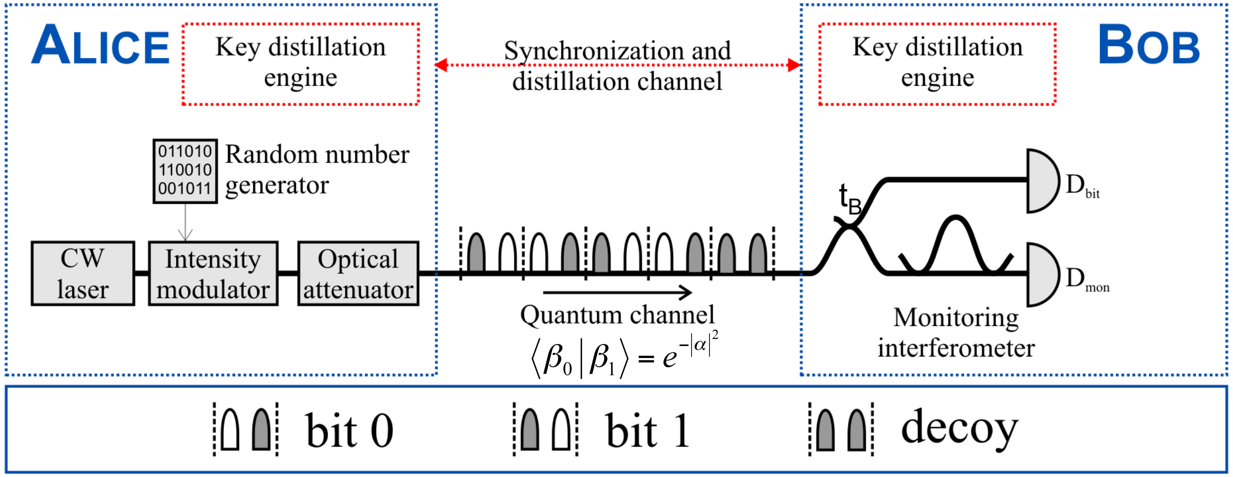
→ **Visibility**

Characteristics

- No active elements at Bob
- Robust bit measurement basis
- Robust against PNS attacks
- Security proof for zero error attacks and some collective attacks

Poster 24: C. W. Lim. *Finite-key security analysis of a simple and efficient one-way quantum cryptography system.*

Poster 51: T. Moroder et al. *Security of distributed-phase-reference quantum key distribution.* arXiv:1207.5544v1 [quant-ph].



→ **QBER**

→ **Visibility**

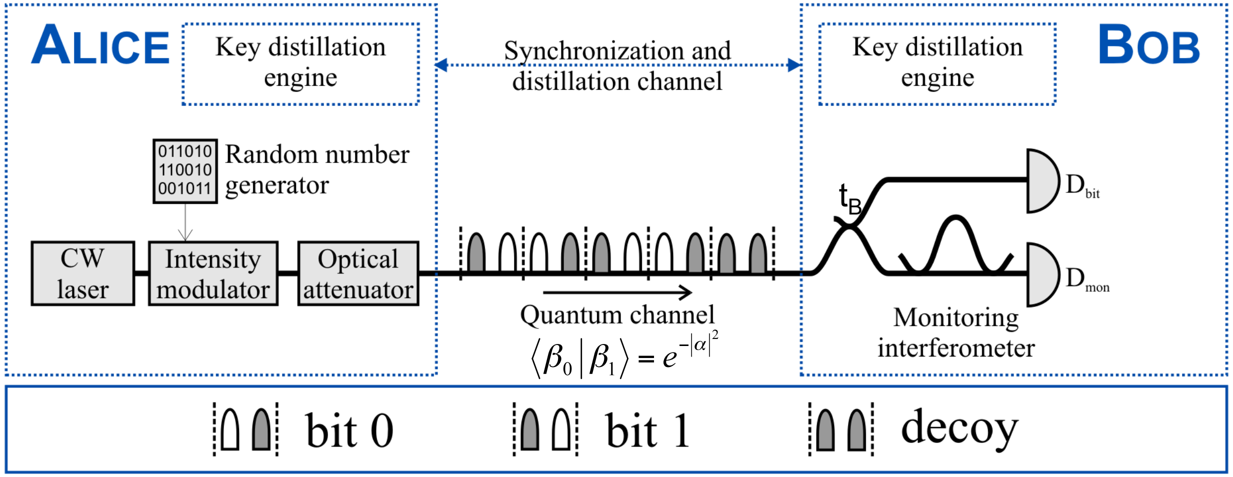
Characteristics

- No active elements at Bob
- Robust bit measurement basis
- Robust against PNS attacks
- Security proof for zero error attacks and some collective attacks

Poster 24: C. W. Lim. *Finite-key security analysis of a simple and efficient one-way quantum cryptography system.*

Poster 51: T. Moroder et al. *Security of distributed-phase-reference quantum key distribution.* arXiv:1207.5544v1 [quant-ph].

The key distillation process



12.5 % random sampling

LDPC forward error correction

CRC sum

Toeplitz hashing

Polynomial hashing

Raw detections

Sifted key

Parameter estimated key

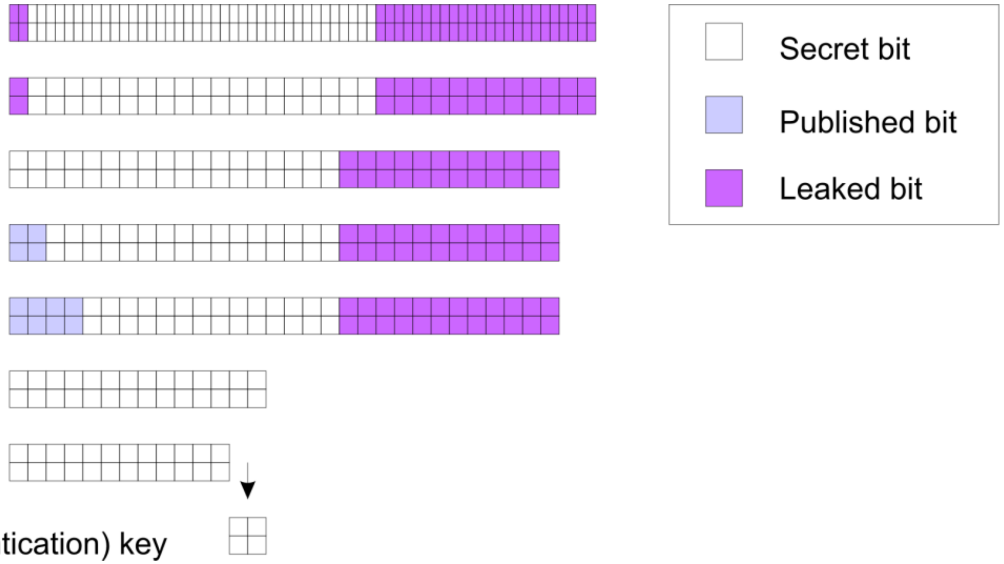
Error corrected key

Verified key

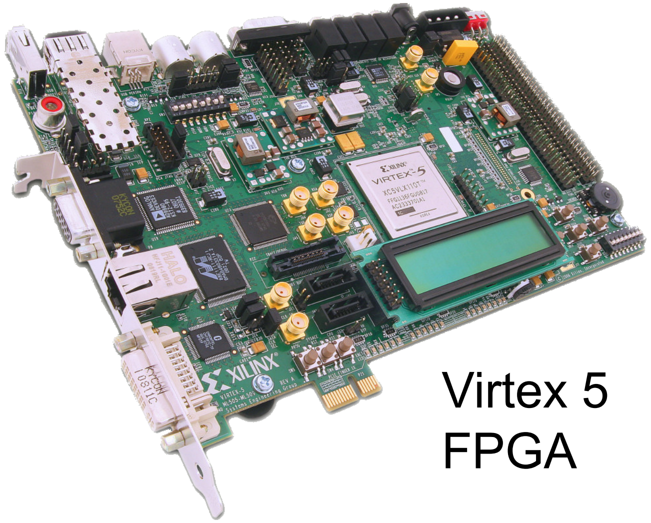
Privacy amplified key

Authenticated secret key

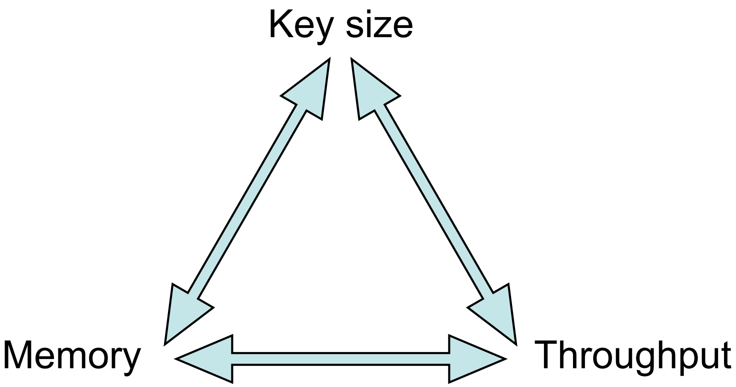
Next round secret (authentication) key

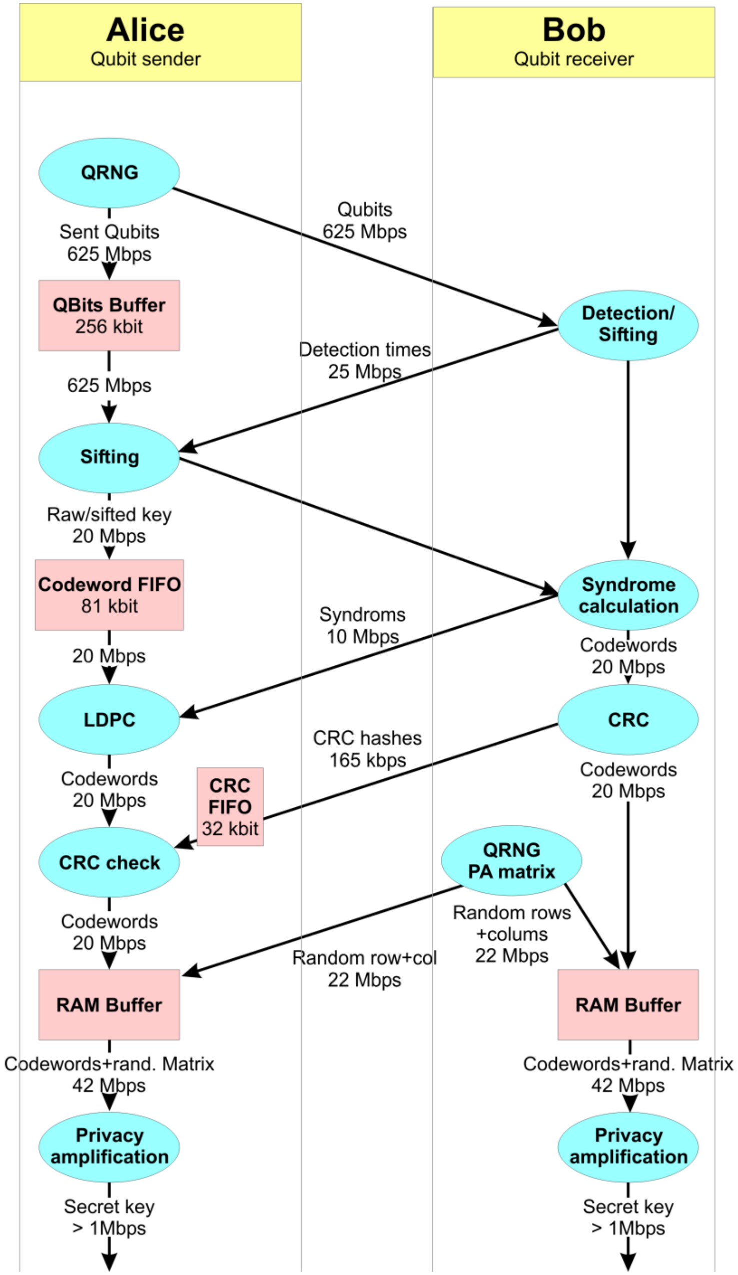


Distillation Flow



Virtex 5 FPGA





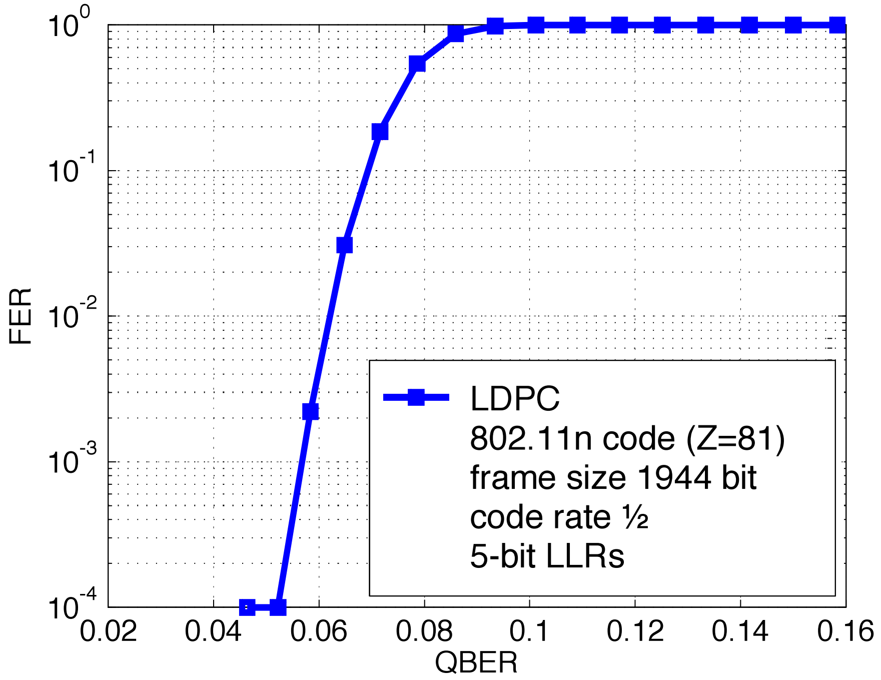
Challenges

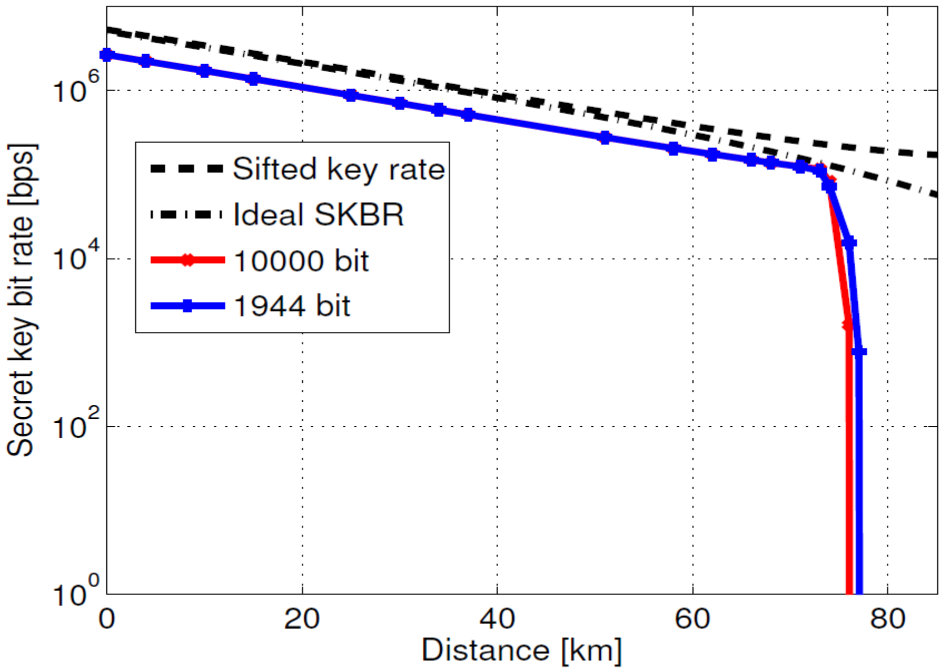
- Efficient sharing of available hardware ressources
- Minimizing amount of classical communication to safe authentication keys

Forward Error Correction (FEC)

Low-density parity-check codes implementation

- Error correction using LDPC decoder
- Standard IEEE 802.11n LDPC code, often used in communication applications (wireless)
- Syndrome encoding, calculated by receiver
- Flexible code rates: ½, ⅔, ¾, ⅚
- Throughput decrease of 0.5 % at 6 % QBER





C. Roth, P. Meinerzhagen, C. Studer, A. Burg. "A 15.8 pJ/bit/iter quasi-cyclic LDPC decoder for IEEE 802.11n in 90 nm CMOS," Solid State Circuits Conference (A-SSCC), 2010 IEEE Asian, (2010)

Privacy amplification

- Privacy amplification using Toeplitz matrices
    - Random matrix (10^6 + 10^5 random bits) with diagonal structure
- Flexible compression ratio in 0.05% steps
- Slice-based processing of multiplication inside the FPGA: 512 parallel accumulator units (rows)

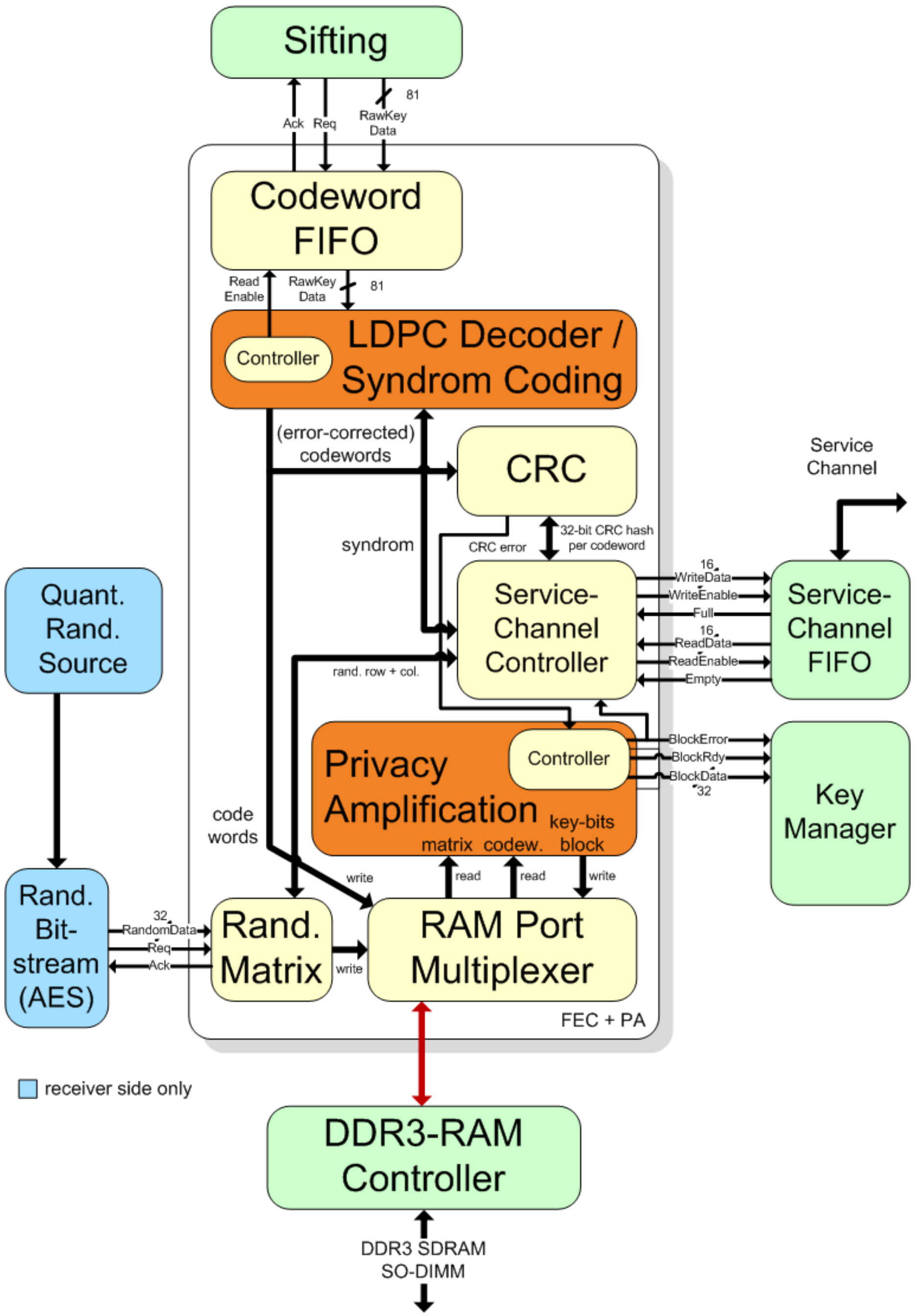
$$A = \begin{bmatrix} a_0 & a_{-1} & a_{-2} & \cdots & \cdots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \ddots & & \vdots \\ a_2 & a_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{-1} & a_{-2} \\ \vdots & & \ddots & a_1 & a_0 & a_{-1} \\ a_{n-1} & \cdots & \cdots & a_2 & a_1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

$$\mathscr{H}^{\diamondsuit} = \{\mathsf{h}_T(\boldsymbol{x}) = T\boldsymbol{x} : \boldsymbol{x} \in \mathrm{GF}(2)^m\}$$

- Storing of data to process inside the FPGA not feasible → computation done in slices (length 512 rows)
- Tradeoff between number of required processing cycles, used on-chip (FPGA) memory and memory bandwidth
- Result: high memory bandwidth requirements
- More hardware ressources (FPGA LUTs / slices) → more parallelism easily makes PA scalable

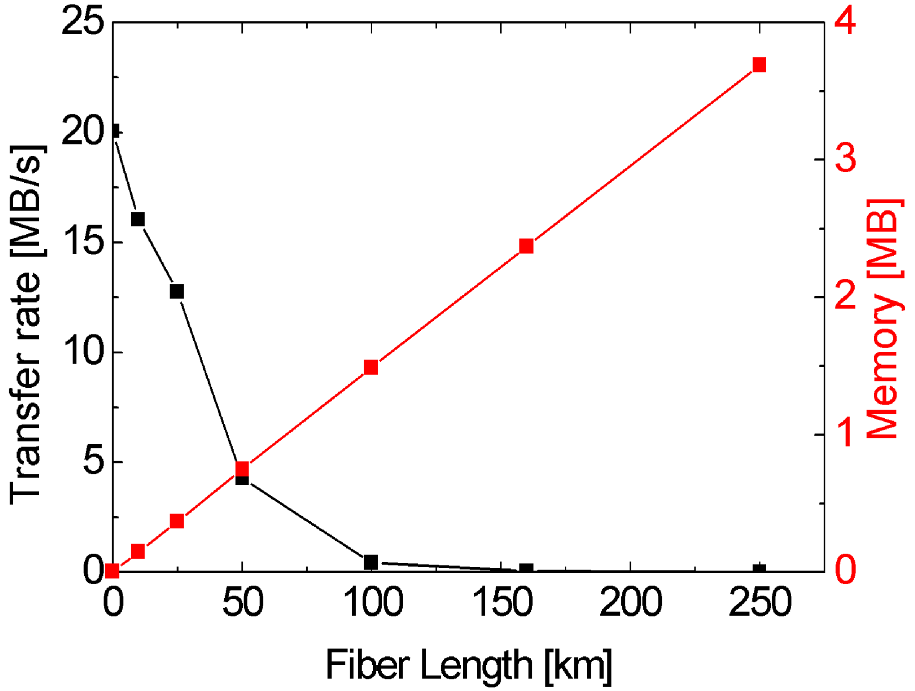
H. Krawczyk. LFSR-based hashing and authentication. Lecture Notes in Computer Science **839** (1994)

FEC and Privacy amplification: System architecture

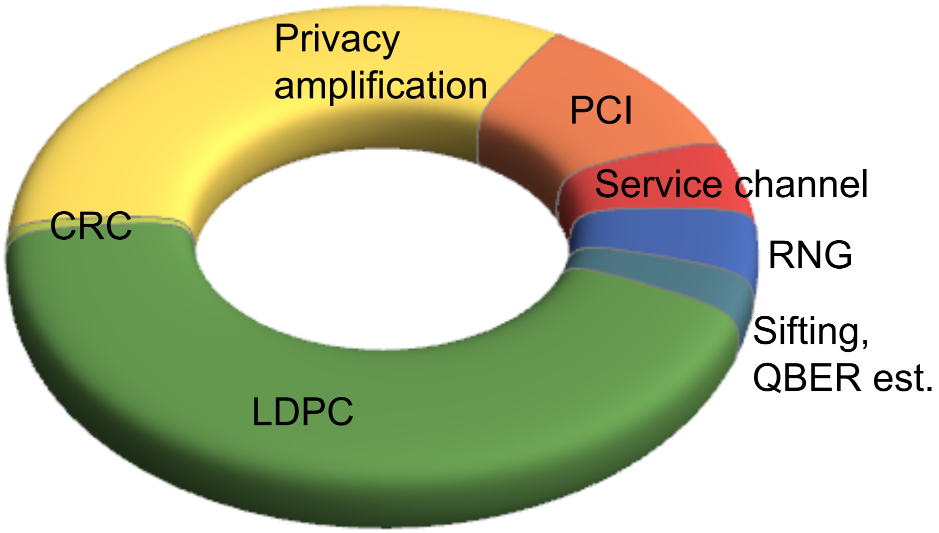


- RAM interface (DDR) with high bandwidth requirements for privacy amplification
- Maximal throughput limit of hardware architecture:
  - 4.11 Mbit/s output key rate at 10 % compression ratio and 40.8 Mbit/s input sifting rate

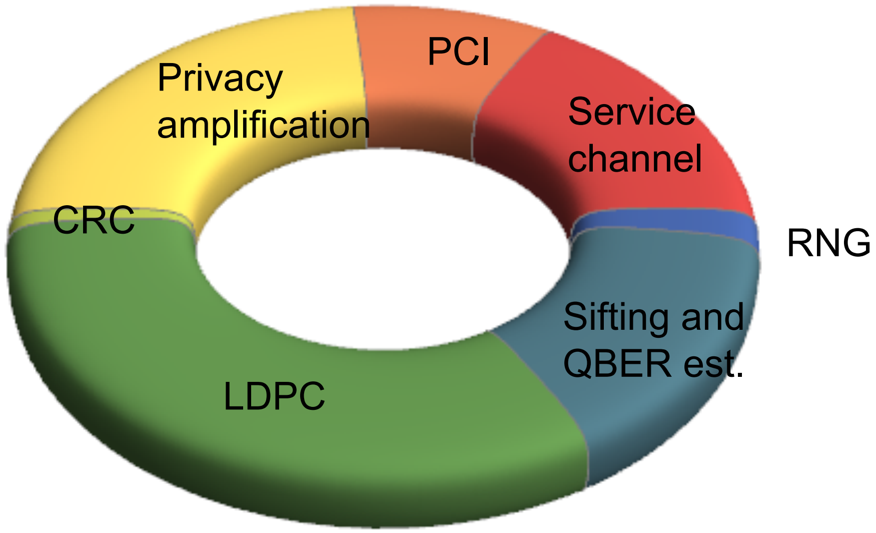
FPGA resource usage



Number of Flip Flops



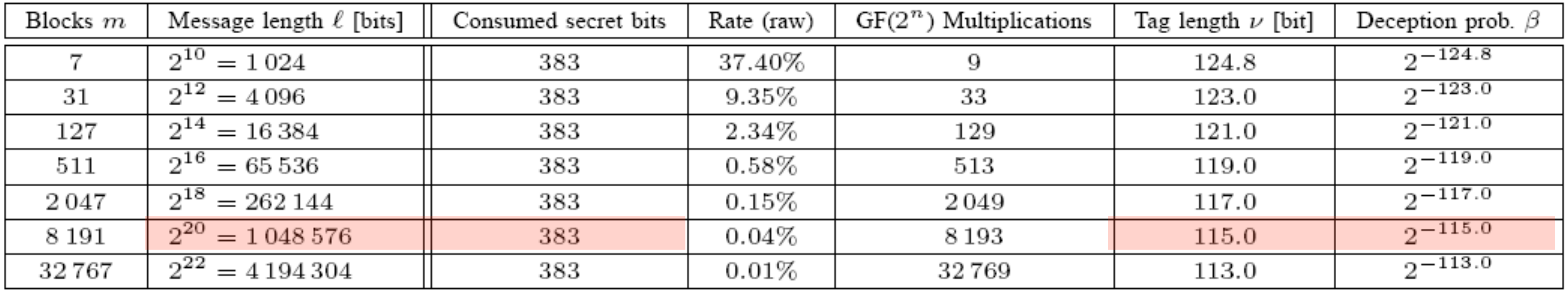
Memory



Information theoretic authentication

Polynomial hashing

- Construct almost universal family of hash functions and apply strongly universal hash function at the end
- Per 10^6 bit of classical communication 383 secret bits are required to generate a tag of length 115 bit



Blocks m	Message length ℓ [bits]	Consumed secret bits	Rate (raw)	GF(2^n) Multiplications	Tag length ν [bit]	Deception prob. β
7	$2^{10} = 1\,024$	383	37.40%	9	124.8	$2^{-124.8}$
31	$2^{12} = 4\,096$	383	9.35%	33	123.0	$2^{-123.0}$
127	$2^{14} = 16\,384$	383	2.34%	129	121.0	$2^{-121.0}$
511	$2^{16} = 65\,536$	383	0.58%	513	119.0	$2^{-119.0}$
2 047	$2^{18} = 262\,144$	383	0.15%	2 049	117.0	$2^{-117.0}$
8 191	$2^{20} = 1\,048\,576$	383	0.04%	8 193	115.0	$2^{-115.0}$
32 767	$2^{22} = 4\,194\,304$	383	0.01%	32 769	113.0	$2^{-113.0}$

One-time pad encryption of authentication tag

- Encrypt authentication tag per one-time pad
- Requires only 115 secret bits per 10^6 bit of classical communication
- Proven ε-universal composability in key recycling scenario: r QKD rounds involving r_{MAC} authentication rounds each, yields secret keys with

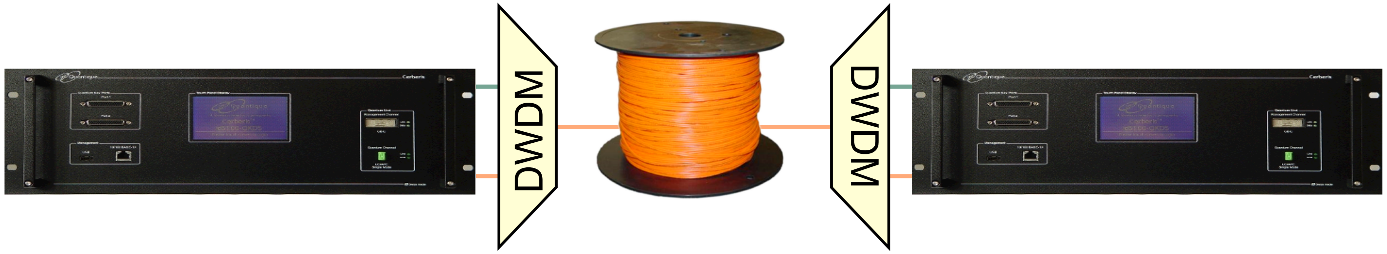
$$\varepsilon = r \cdot (\varepsilon_{\mathrm{QKD}} + r_{\mathrm{MAC}} \cdot \varepsilon_{\mathrm{MAC}})$$

D.R. Stinson. Universal hashing and authentication codes. Designs, Codes and Cryptography, 4 (1994).

C. Portmann. Key recycling in authentication. arXiv:1202.1229v2 [cs.IT] (2012).

Dense wavelength division multiplexing

Multiplexing classical channels (> -28 dBm) along with quantum channel (< -71 dBm) on 100 GHz DWDM grid



Impairment due to Channel crosstalk

- „Off-band noise“ due to finite channel isolation of the multiplexers
- Reduced below detector dark counts by MUX channel isolation (-82 dB)

Impairment due to Raman scatter

- Scattering off optical phonons, in forward and backward direction
- Dominating for fibre lengths > 10 km

Pros

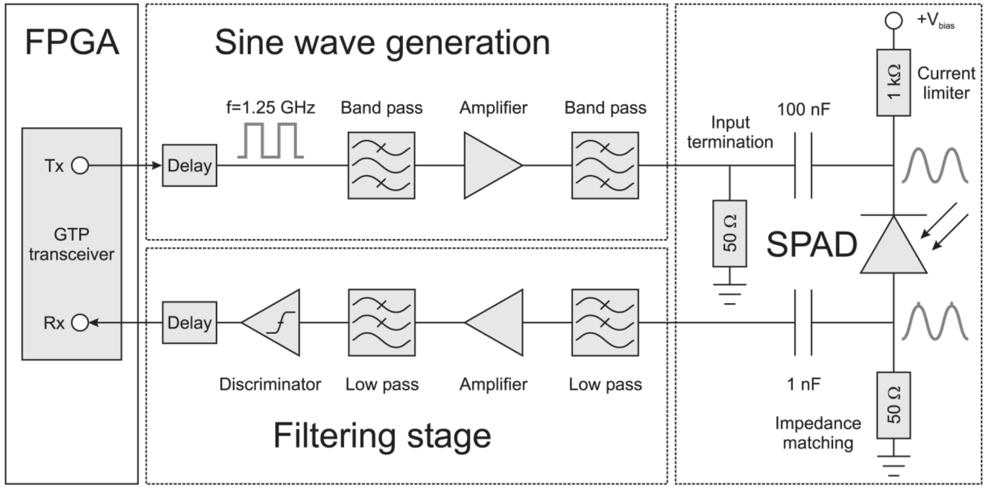
- 1 interconnecting fiber only
- Higher synchronization stability due to lower temperature fluctuation sensitivity

Cons

- 2.5 dB losses in DWDM and filter
- Raman scattering impairment

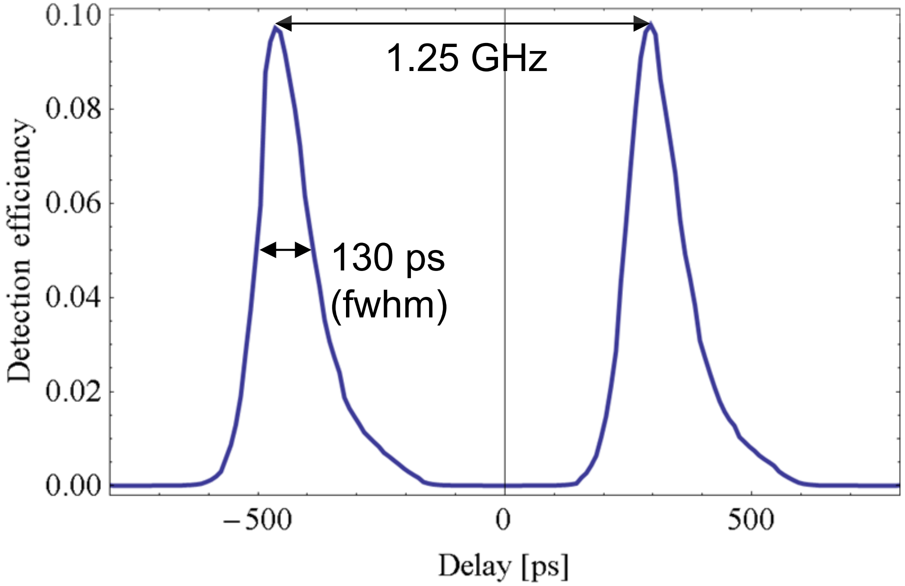
Sine gated single photon detectors

Robust low-pass filtering scheme

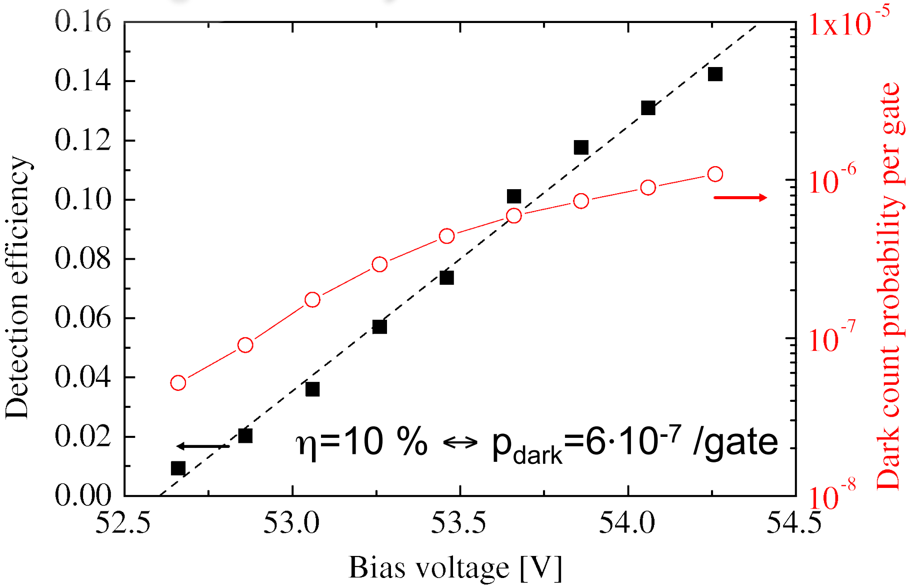


- 1.25 GHz gate frequency
- High detection rates > 33 MHz
- Low afterpulse probability < 1%
- Low dead time of 8 ns
- Low timing jitter of ~70 ps (fwhm)
- Room temperature operation
- Compact design, Peltier cooling

High gate frequency and short gate width



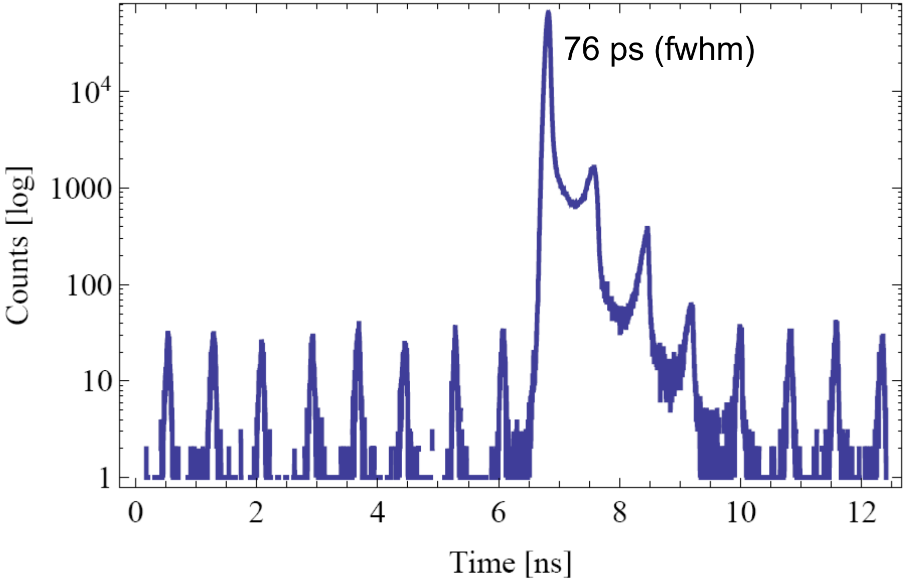
High efficiency and low dark counts



N. Walenta *et al*. To be published in J. of App. Phys.(2012), arXiv:1205.3084v1 [quant-ph].

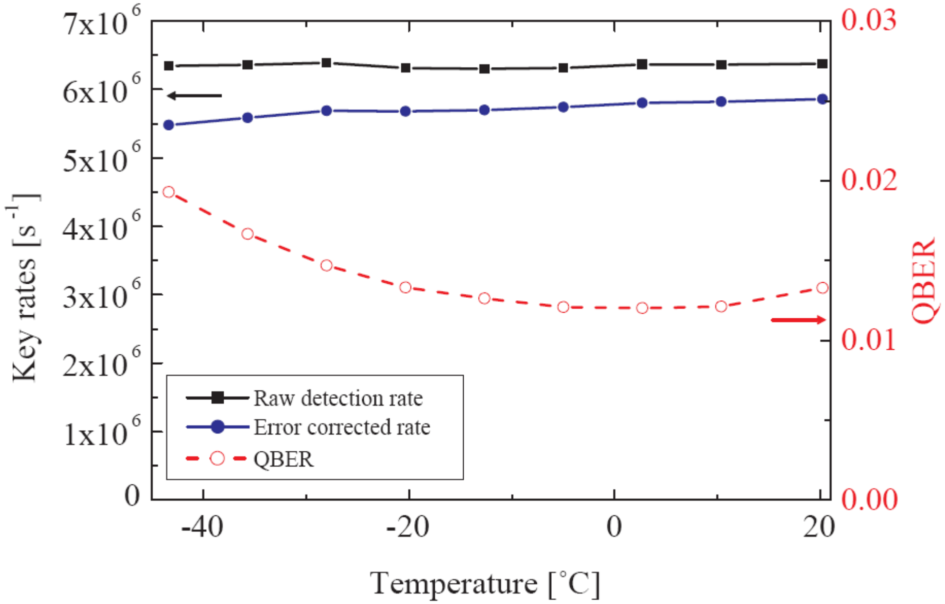
Sine gate QKD performance

High timing resolution

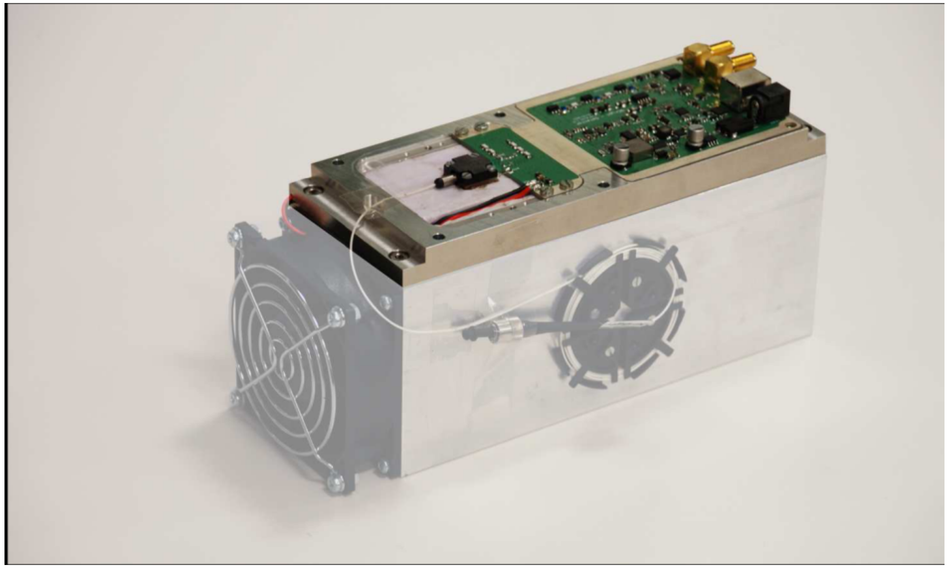


- 1.25 GHz gate frequency
- High detection rates > 33 MHz
- Low afterpulse probability < 1%
- Low dead time of 8 ns
- Low timing jitter of ~70 ps (fwhm)
- Room temperature operation
- Compact design, Peltier cooling

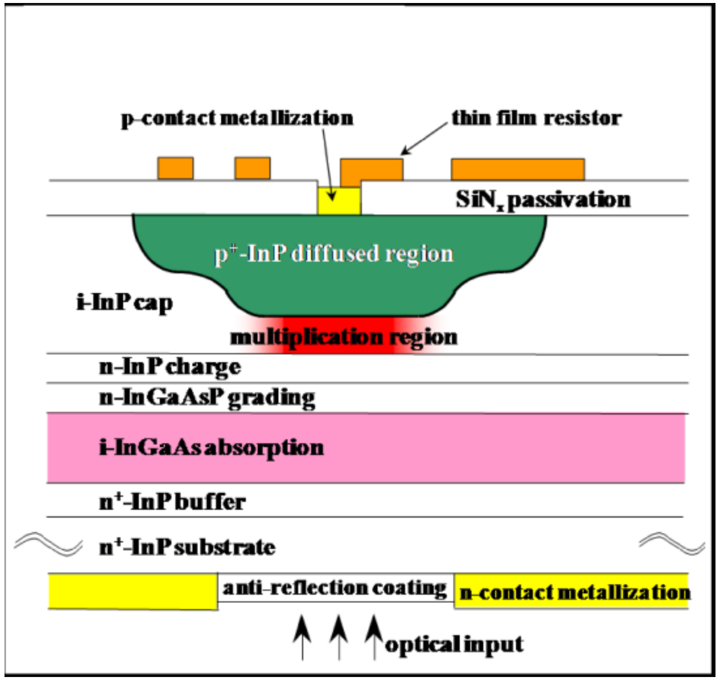
Room temperature operation



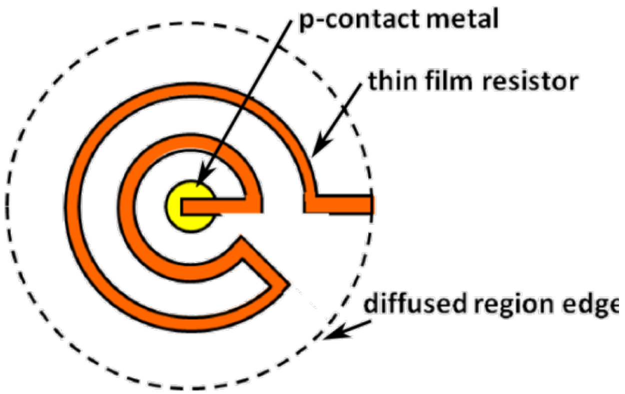
Compact design

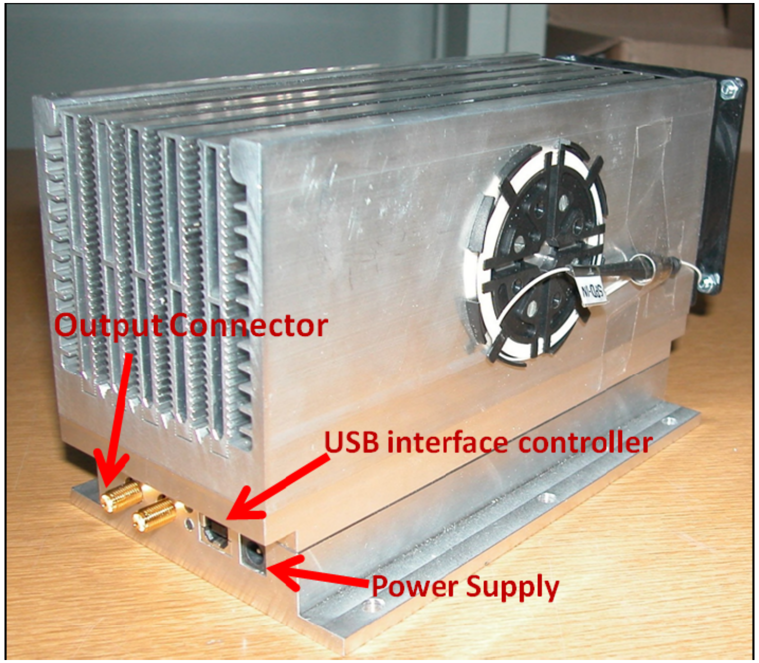


Free-running single photon detectors



Diode with monolithically integrated resistor



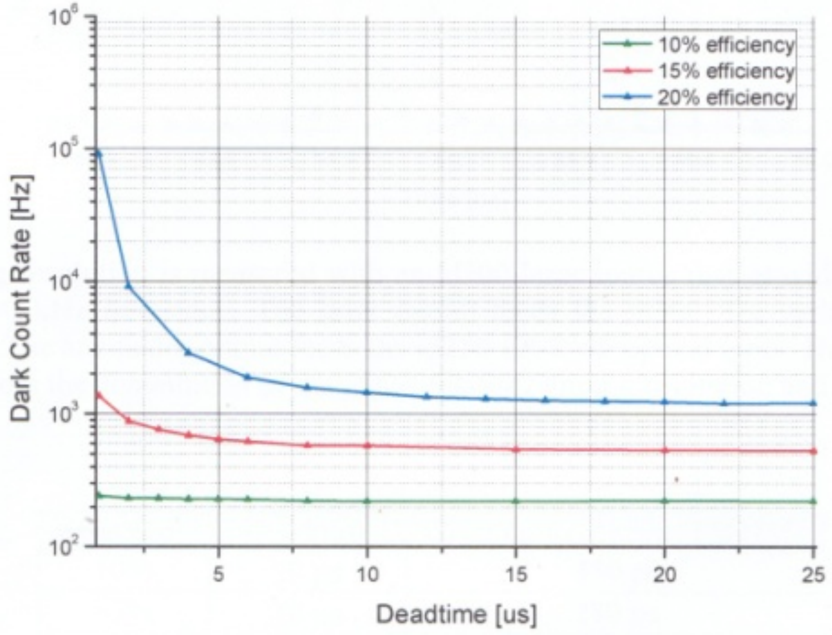


- Effective quench due to monolithically integrated resistor
- Passive-quench active-reset circuit with variable hold-off time
- Performances in free-running mode comparable with gated single-photon diode

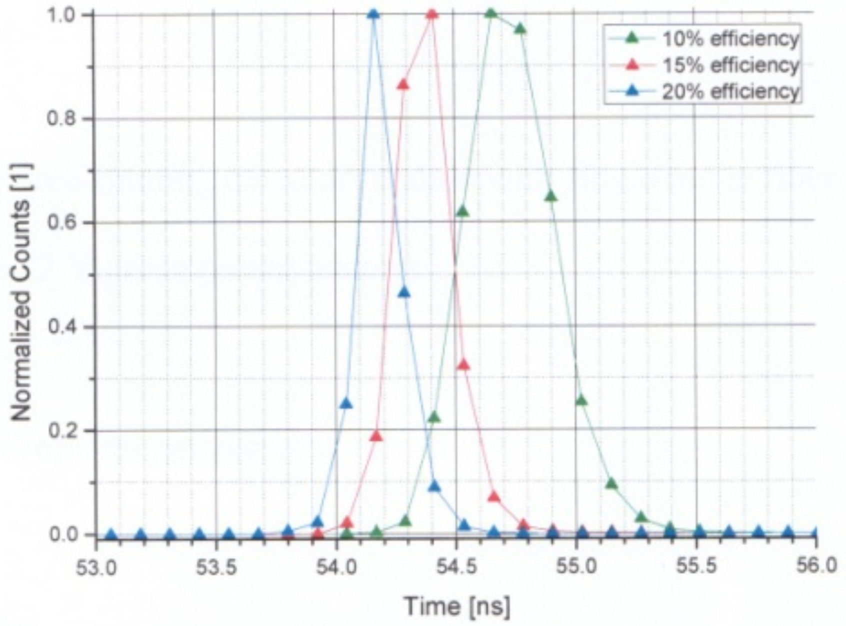
T. Lunghi *et al.*, to appear in J. Mod. Opt., arXiv:1204.4594v1 [physics.ins-det].

Free-running SPD performance

Low noise impairment



Low timing jitter

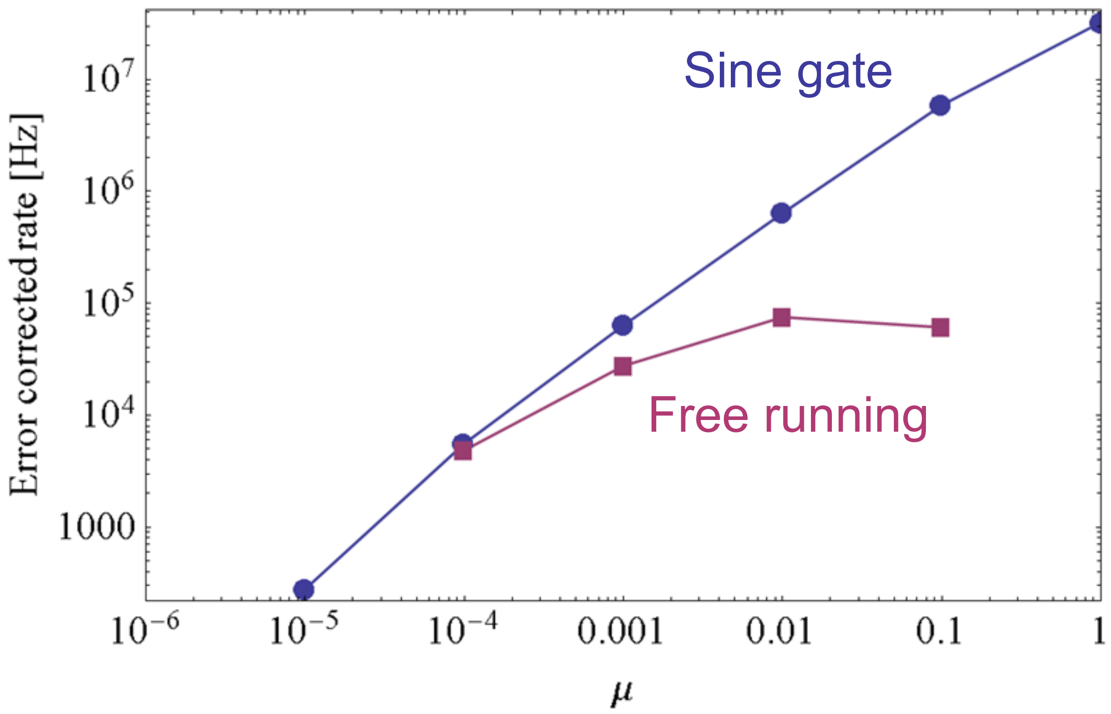


Efficiency at 1550 nm	Deadtime	Dark count rate
10 %	10 μs	222 Hz
15 %	10 μs	580 Hz
20 %	10 μs	1454 Hz

Efficiency at 1550 nm	Deadtime	Timing resolution (fwhm)
10 %	20 μs	450 ps
15 %	20 μs	280 ps
20 %	20 μs	200 ps

📖 T. Lunghi *et al.*, to appear in J. Mod. Opt., arXiv:1204.4594v1 [physics.ins-det].

Comparison between sine gated and free-running detector



Finite key

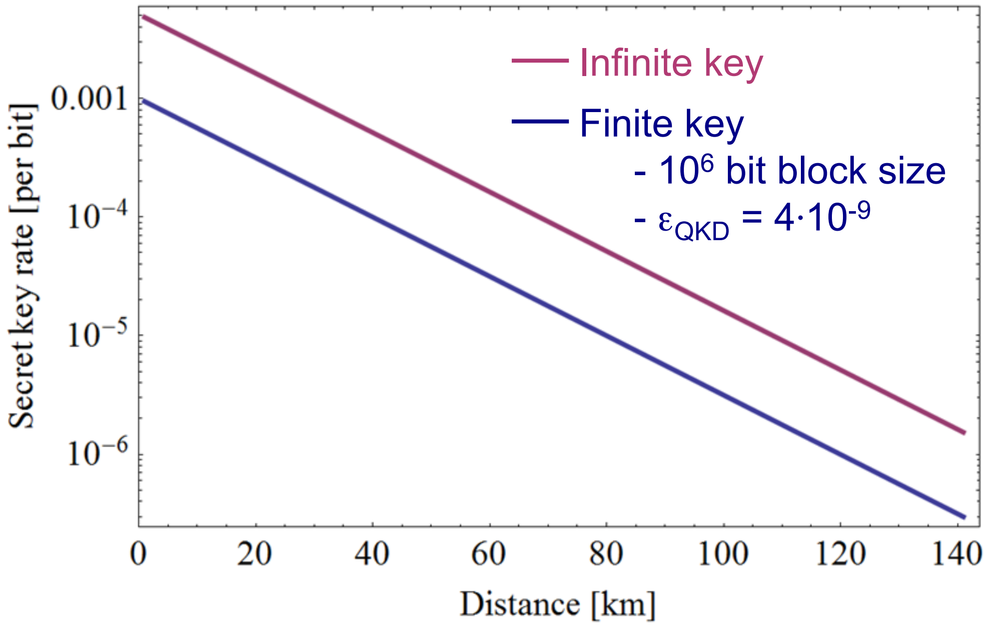
$$r_{\sec} = \left(1 - e^{-\mu \cdot t_{fib} \cdot t_B \cdot \eta_{\det}}\right)\left(1 - p_{decoy}\right) \cdot \left(1 - \eta_{PE}\right) \cdot \left(1 - \chi(A:E)\right)$$

$$\chi(A:E) = Q^* + h\left[Q^*\right] + \left(1 - Q^*\right) h\left[\frac{1 + \Delta\left(V^*\right)}{2}\right] + f_{smooth} + f_{EC} + f_{PA} + f_{MAC}$$

$$Q^* = Q + \delta Q, \; V^* = V - \delta V$$

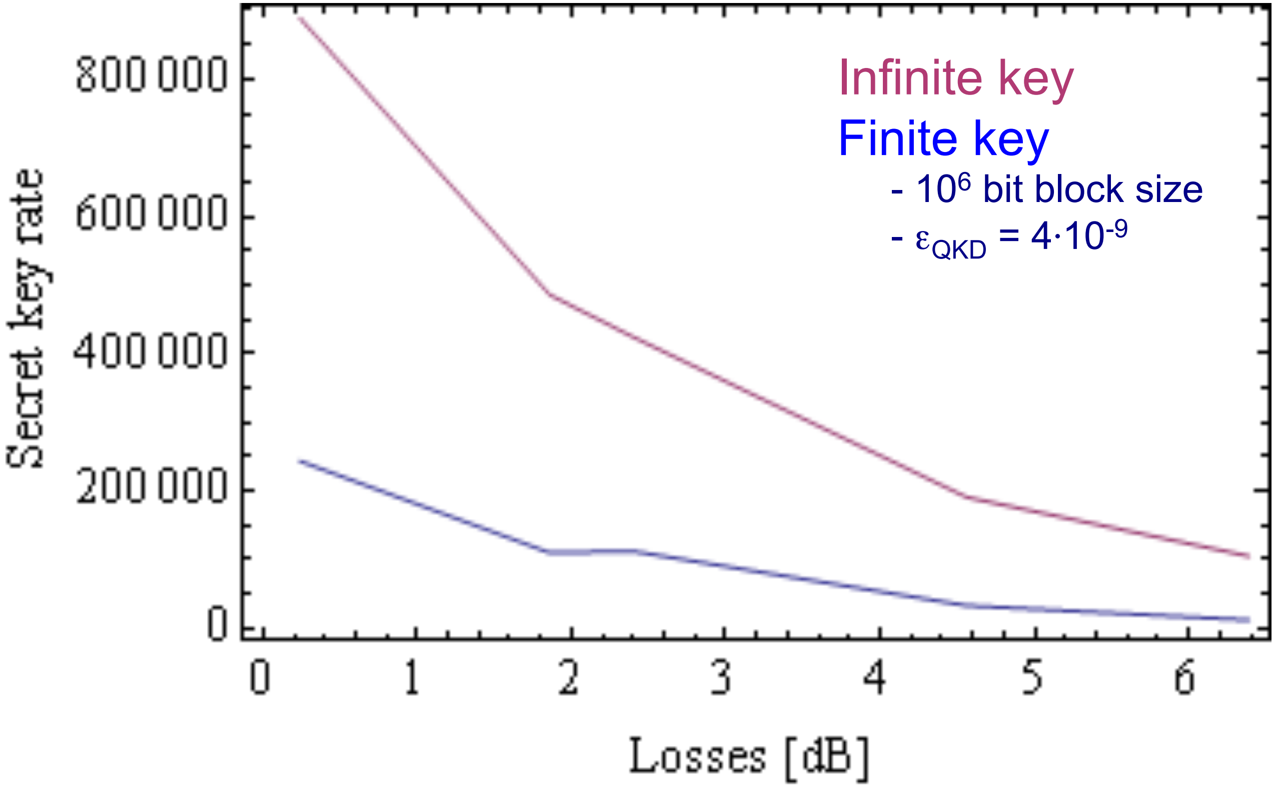
$$\varepsilon_{QKD} = \varepsilon_{PE} + \varepsilon_{EC} + \varepsilon_{smooth} + \varepsilon_{PA} + \varepsilon_{MAC}$$

- 80 % secret key reduction due to finite effects for 10^6 bit post-processing block size
- coherent state amplitude μ independent of fiber transmission
- photon number μ and other parameters depend on QBER and visibility



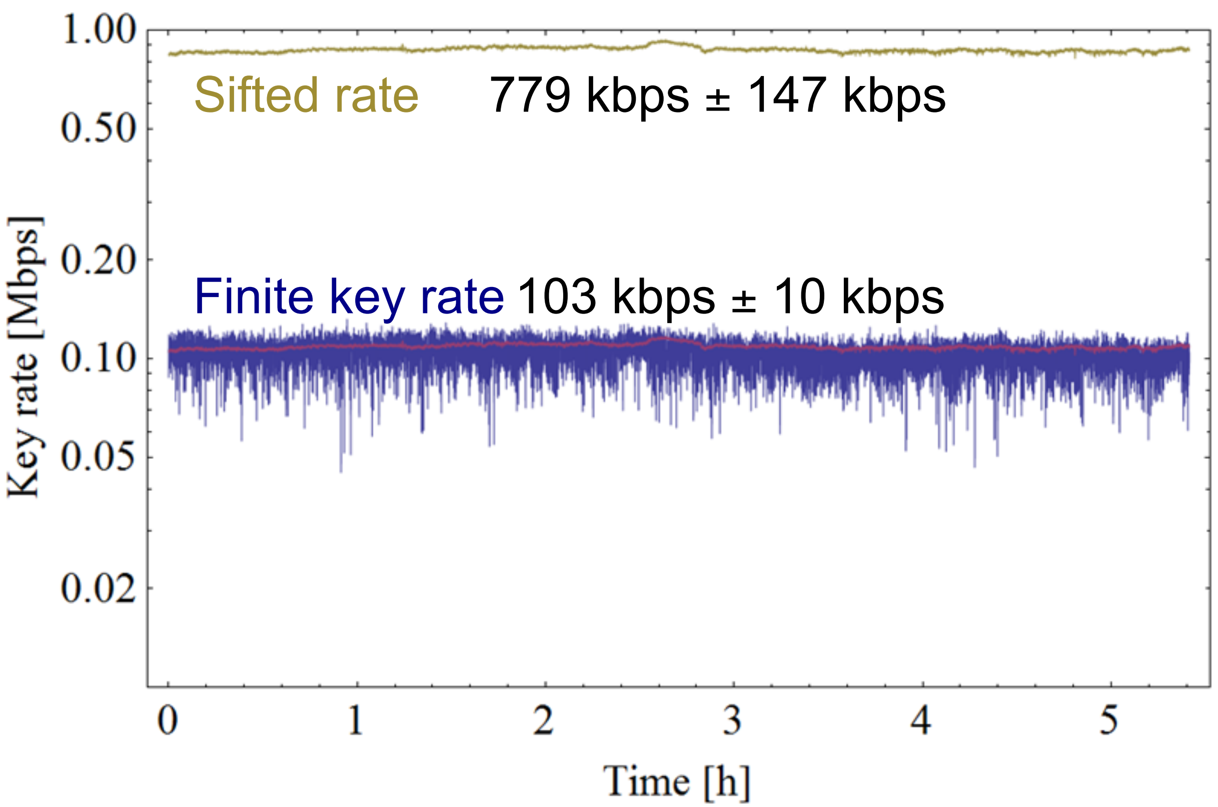
Finite key results

- Sine gating data detector and free-running monitor detector
- Complete DWDM and filtering setup
- Hardware distillation engine:
  - 10^6 bit post-processing block size
  - $\varepsilon_{QKD} = 4 \cdot 10^{-9}$



Finite key overnight run

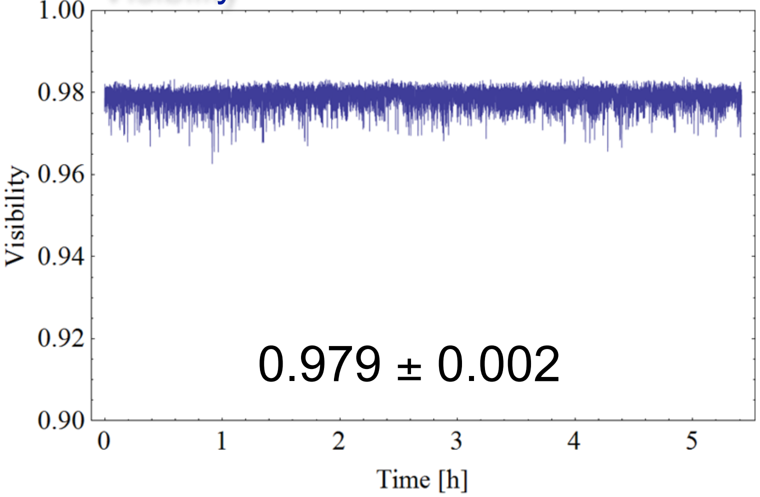
12 km Fiber length



Sifted rate 779 kbps ± 147 kbps

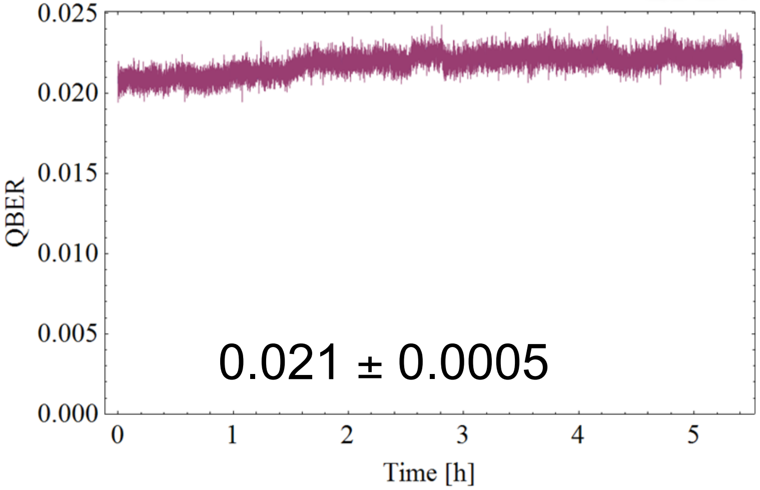
Finite key rate 103 kbps ± 10 kbps

Visibility



0.979 ± 0.002

QBER



0.021 ± 0.0005

Outlook

- > 1 Mbps secret key rate
- New FPGA Virtex 6
- Activating authentication and key manager
- Integration in final housing
- Real network compatibility and integration
- Resistance against detector blinding attack