IUT WEBINARS

Quantum Information Technology

Episode #5: Joint Symposium on Quantum Photonic Integrated Circuits

A Photonic Integrated Quantum Secure Communication System

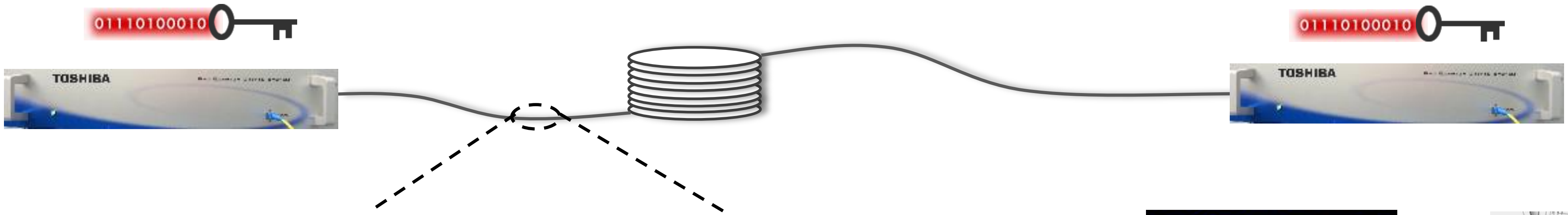
T.K. Paraiso, T. Roger, D.G. Marangon, I. de Marco, M. Sanzaro, R.I. Woodward, J.F. Dynes, Z. Yuan, A.J. Shields

TOSHIBA

Toshiba Europe Limited
Cambridge Research Laboratory
Quantum Information group

2021.11.02

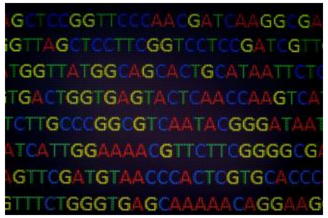
Quantum Cryptography



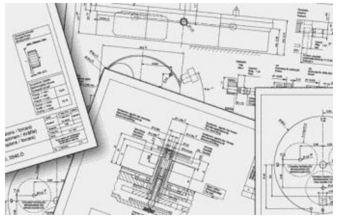
Quantum Key Distribution
- each bit encoded on a single photon

Conventional public-key cryptography (RSA, ECDH)

- Long-term confidentiality threatened by *harvest and decrypt* attacks
- Encrypted data are easily collected and stored
- Decrypt later when more powerful computers are available



Bio-Medical



Corporate

Financial

Critical Infrastructure

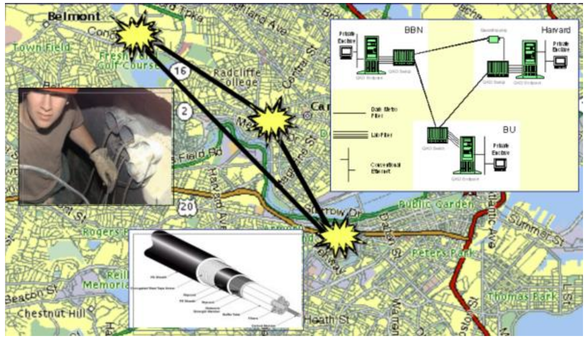
Quantum key distribution

- Detect eavesdropping on fibre as <u>measurable noise</u> in the quantum channel

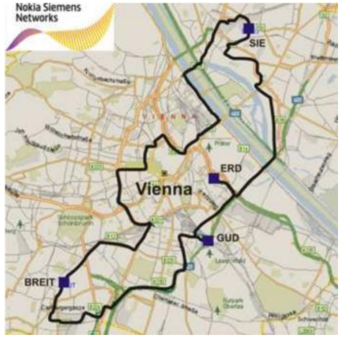
- Distribute secret digital keys that are secure from future advances in cryptanalysis and computing

Enabling the wide-scale deployment of quantum cryptography

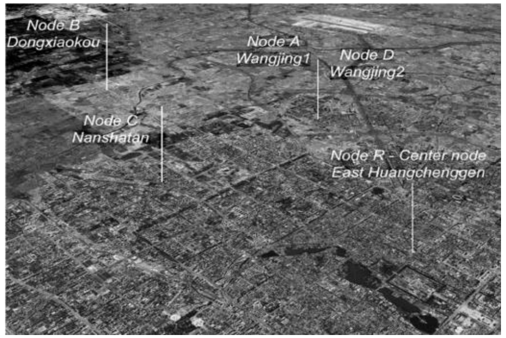
Boston 2002



Vienna 2003



Beijing 2009

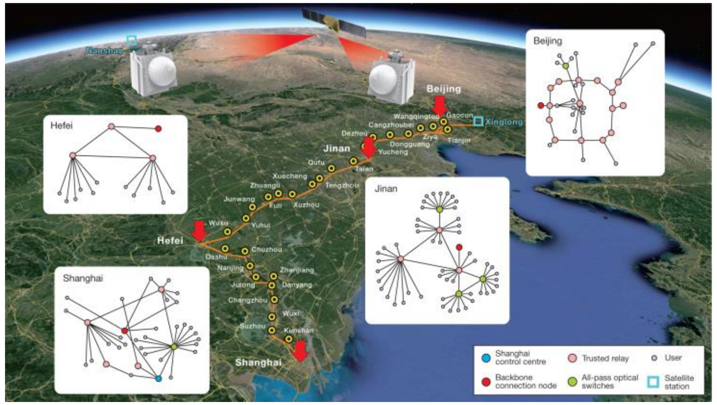


Geneva 2009

Tokyo 2010

UK 2015

China 2017, 2021



Enabling the wide-scale deployment of quantum cryptography

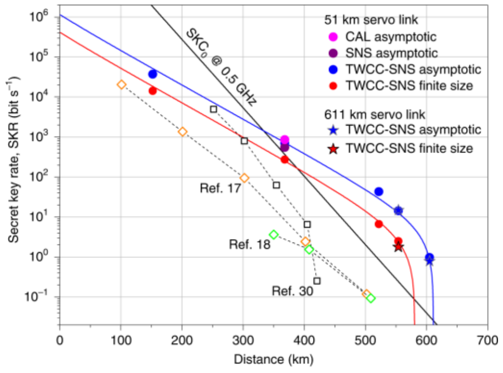
Distance

Secret key capacity bound

Photon loss vs distance

Limit on key rate

- Satellite-QKD
- TF-QKD



Pittaluga et al.,
Nat. Photon. **15,** 530–535 (2021)

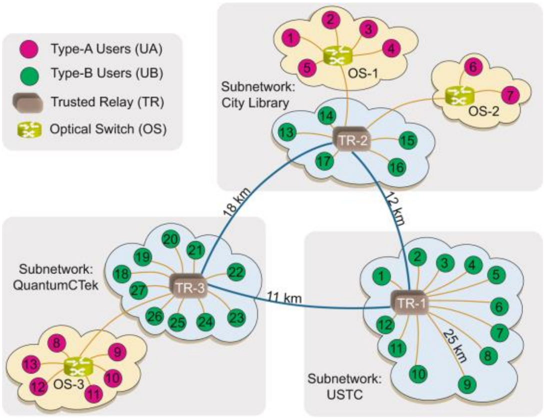
Scalability &cost

Coherent optical comms networks:

High density

High connectivity

- Multi-node QKD networks
- Trusted-node architectures



Chen et al.,
npj Quantum Information 7:134 (2021)

QKD Deployment – Main challenges

Enabling the wide-scale deployment of quantum cryptography

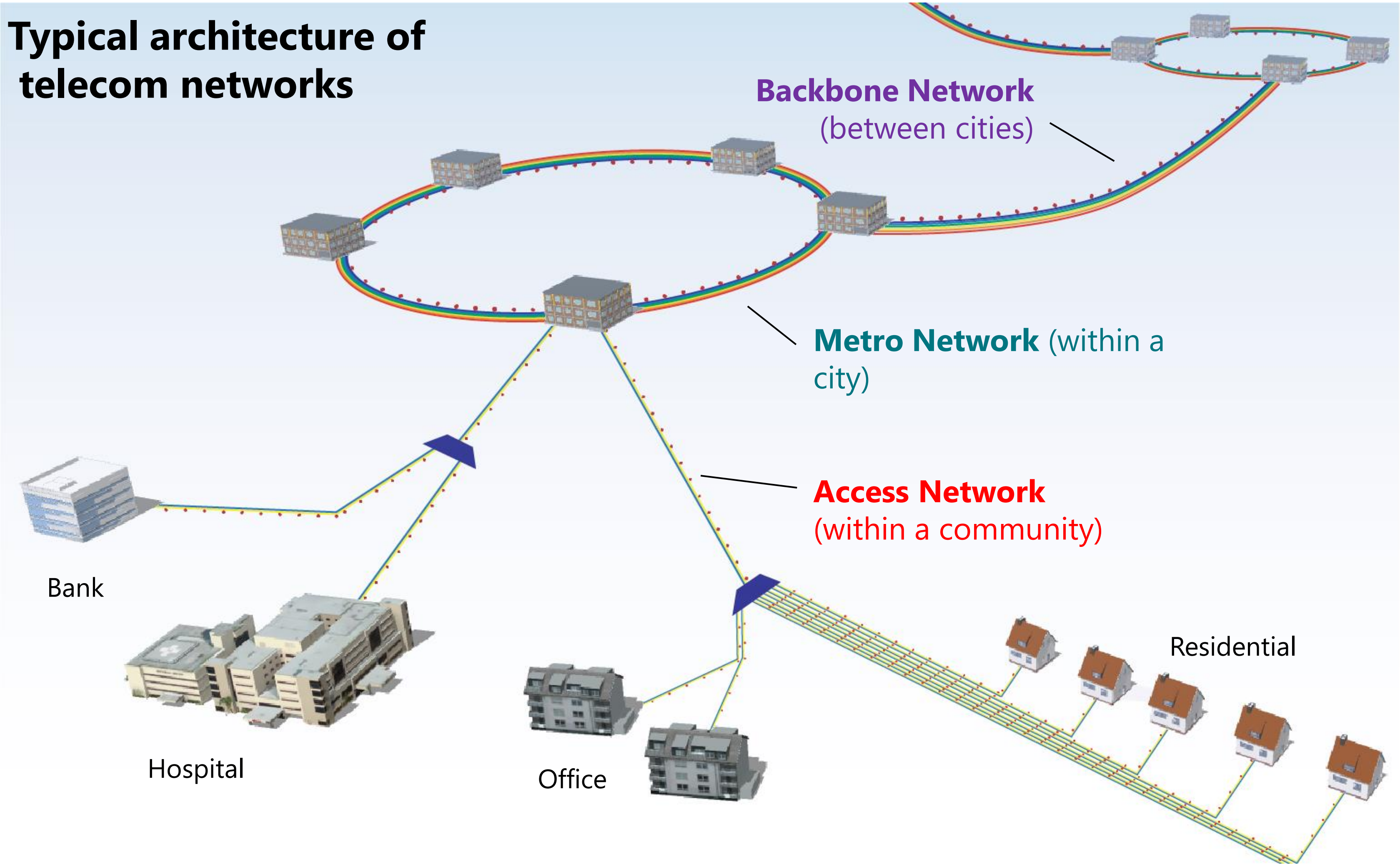
- More than 50% of the global population within metro & access areas
- High density and connectivity
- Route to practical deployment of QKD in these networks

- **Bandwidth**
- **Loss/Distance**
- **Production, operation and deployment costs**

- Multiplexing, higher clock rates
- Trusted relay nodes
- Power efficient information encoding

➔ Volume production and scalability

➔ Compatibility with coherent optical comm. infrastructure



Integrated Quantum Photonics

CORE QKD FUNCTIONS ON CHIP

QKD Transmitters (QTx) chips

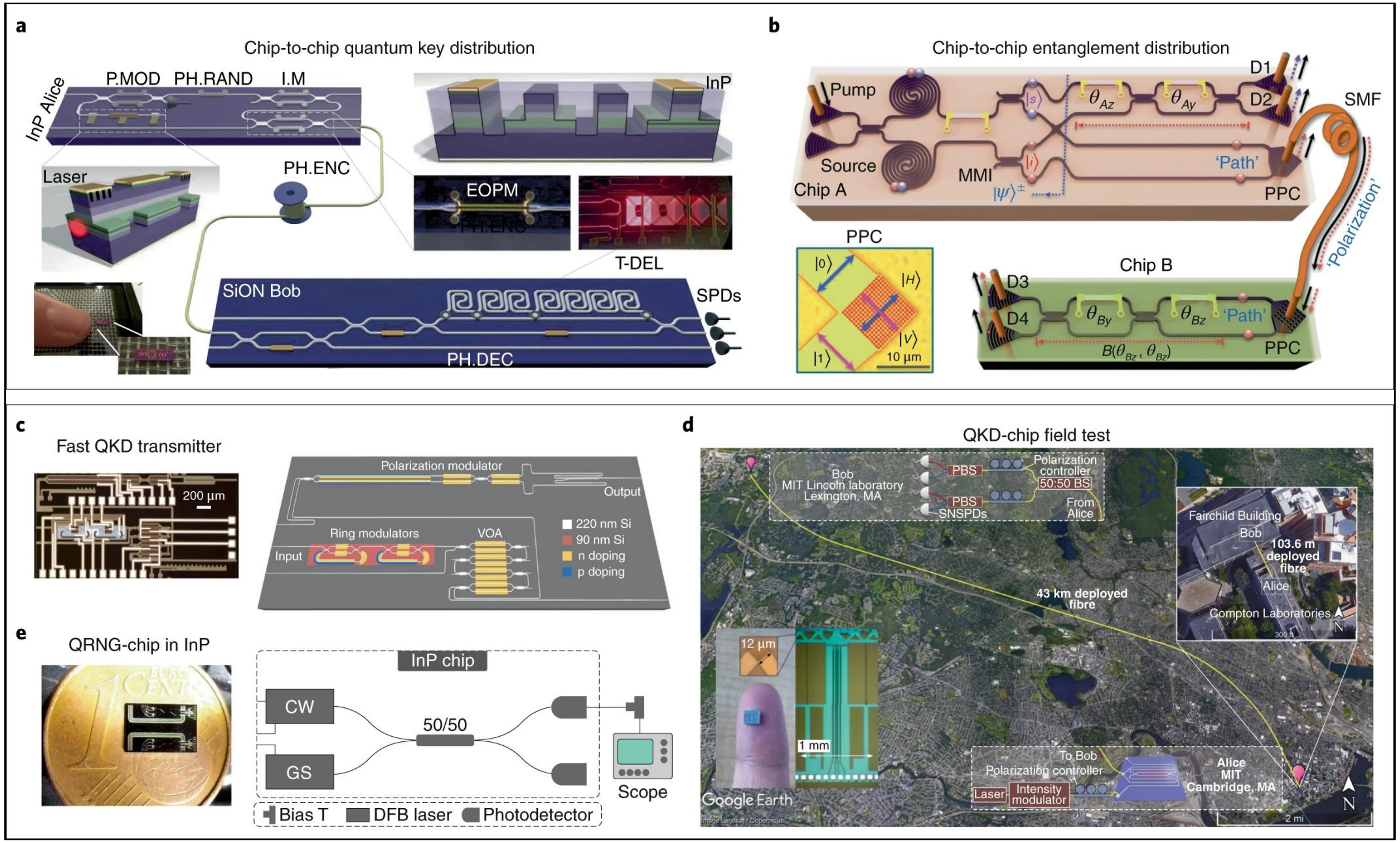
- Polarization/Phase encoding
- Fully integrated
- External light sources, intensity modulation

QKD Receiver (QRx) chips

- Low loss interferometers
- Path demodulators

Quantum Random number Generator (QRNG) chips

- Balance homodyne QRNGs
- Interferometric QRNGs



Wang, J., Sciarrino, F., Laing, A. *et al.* Integrated photonic quantum technologies. *Nat. Photonics* **14,** 273–284 (2020)
The rise of integrated quantum photonics. *Nat. Photonics* **14,** 265 (2020)

QKD transmitter chip demonstrations: a survey

	Si/InP	Protocol	Encoding	Laser source	Receiver	Phase Modulation	Quantum Random	Real-time	Clock rate	Bit rate @ channel loss
Ma et al. *Optica* **3**, 11 (2016)	Si	BB84	Polarization	Discrete optics	Fibre	Carrier depletion (CDM)	No	No	10 MHz	1 kbps [@1dB, **APD**]
Sibson et al. *Nat Commun* **8**, 13984 (2017)	*InP*	BB84, DPS, COW	Time-bin	**On-chip**	Si chip	Traveling wave EOPM	**Yes**	No	0.56 GHz [BBB84] 1.76 GHz [DPS]	345 kbps [4 dB, SNSPD] 565 kbps [4dB, SNSPD]
Sibson et al. *Optica* **4**, 172 (2017)	Si	BB84, COW	Time-bin Polarization	Discrete optics	Si chip	CIM	No	No	1 GHz 0.86 GHz	329 kbps [4 dB, SNSPD] 916 kbps [4 dB, SNSPD]
Ding et al. *npj Quantum Inf* **3**, 25 (2017)	Si	High-Dim. QKD	Path entanglement	Discrete optics	Si chip	TOPM	No	**Yes**	5 kHz / 10 kHz	[0.65 bit / photon]
Bunandar et al. *Phys Rev X* **8**, 021009 (2018)	Si	3-state BB84	Polarization	Discrete optics	Si chip	CDM	No	**Yes**	625 MHz	864 kbps [SNSPD] 157 kbps [16 dB, field trial]
❖ Paraiso et al. *npj Quantum Inf* **5**, 42 (2019)	*InP*	BB84, DPS	Time-bin	**On-chip**	Si chip	**Phase-seeding**	**Yes**	No	1 GHz	840 kbps [10 dB, **APDs**]
Zhang et al. *Nat. Photonics* **13**, 839 (2019)	Si	CV-QKD	Gaussian-modulated	Discrete optics	Si chip	CDM	No	**Yes**	1-10 MHz	0.14 kbps [16 dB, BHD]
Avesani et al. arXiv:1907.10039v1 (2019)	Si	3-state BB84, free space	Polarization	Discrete optics	Fibre	CDM	No	No	50 MHz	30 kbps [free space]
Geng et al. *Opt Express* **27**, 29045 (2019)	Si	BB84	Time-bin	Discrete optics	Si chip	CDM	No	No	100 MHz	85 kbps [4dB, SNSPD]
Cao et al. *Phys Rev Applied* **14**, 011001 (2020)	Si	*MDI-QKD*	Polarization	Discrete optics	Si chip	CDM	NA	No	0.5 MHz	[2.9 x 10-6 / pulse, SNSPD]
Semenenko et al. *Optica* **7**, No. 3 (2020)	*InP*	*MDI-QKD*	Time-bin	**On-chip**	Si chip	Traveling wave EOPM	**Yes**	No	250 MHz	1 kbps [20 dB, SNSPD]
Wei et al. *Phys Rev X* **10**, 031030 (2020)	Si	*MDI-QKD*	Polarization	Discrete optics	Fibre	CDM	**Gl. phase**	**Yes**	1.25 GHz	0.5 kbps [27 dB, SNSPD]

System integration challenges

✓ Pioneering proof-of-concept demonstrations: → capability confirmed

⇒ **Complete standalone chip-based system still missing ?**

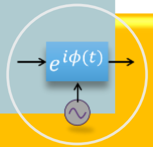
Numerous challenges to tackle at once

- **Bit, basis choices**
- Global phase randomization
- Decoy intensities
- Biased intensities
- **High bit rate QRNG**

Quantum random number generator

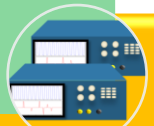
- **Time-bin and polarization encoding**
- Intensity modulation MZM
- Number of RF channels
- EOPM footprint on chip
- Low V_π for CMOS level compatibility

Phase modulation technique



- **Compact driving & processing electronics**
- Power consumption
- Thermal management
- Co-design optical chips and control electronics

Remove lab equipment for driving/processing



- Photonic **packaging**
- Optoelectronic assembly
- Clock distribution and **synchronization**
- **Stability** – feedback control
- Long term operation

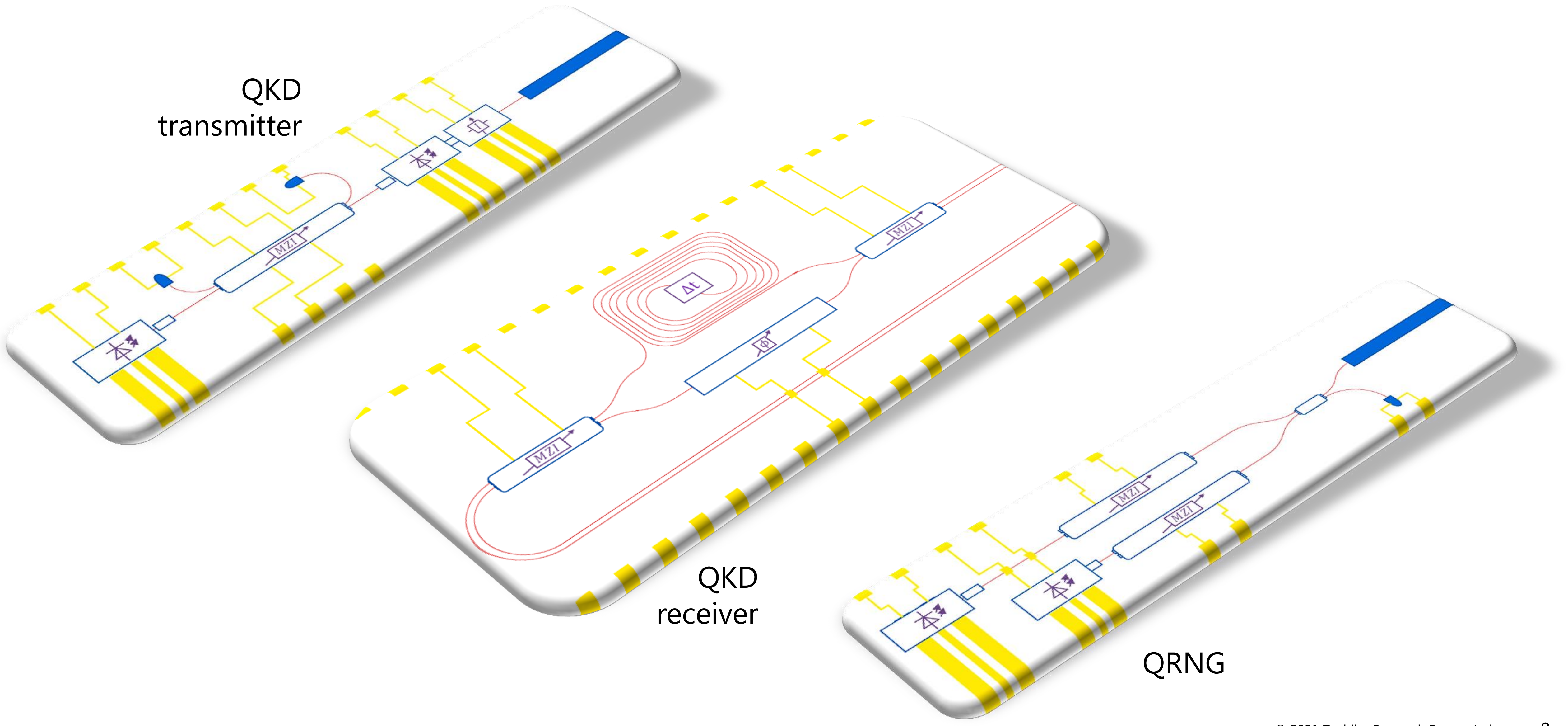
System integration

- **Real-time random choice variables**
- Real time public communication
- Error-correction, Privacy amplification
- **Data-encryption**

Real-time operation

quantum secure → power efficient → deployable units

Core Function QKD Chips

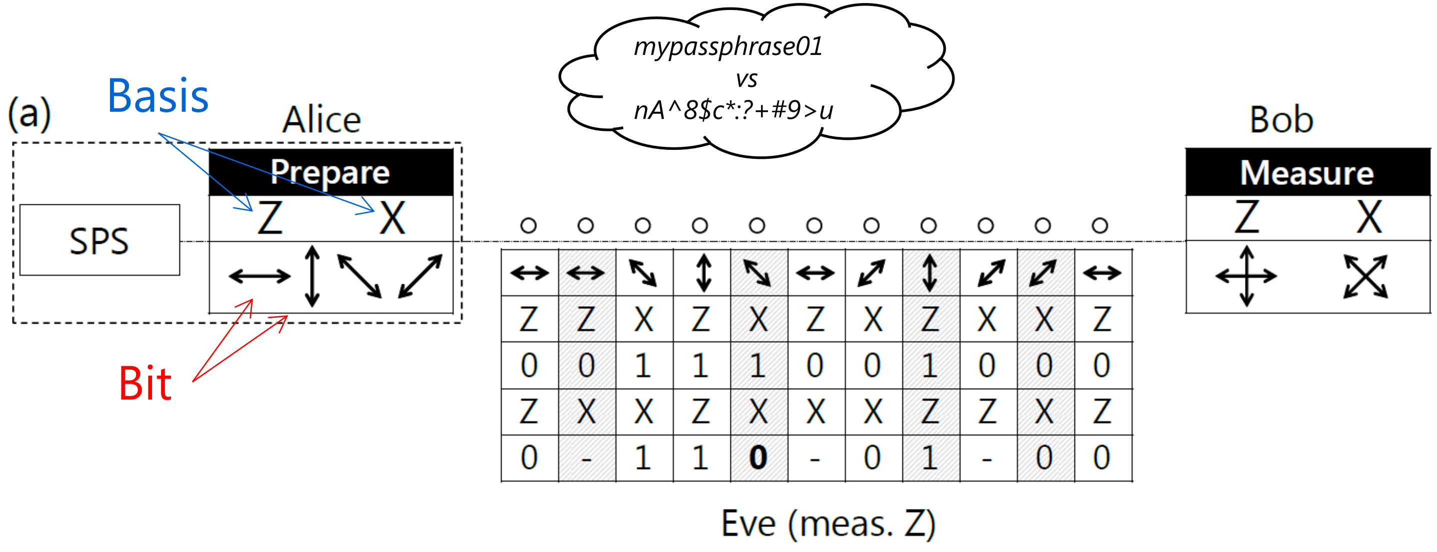


QUANTUM RANDOM NUMBERS ON CHIP

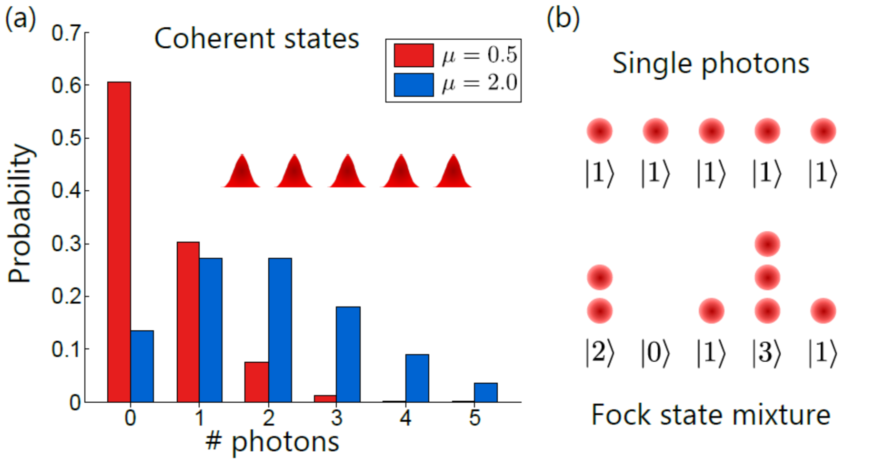
Photonic ICs for QKD: Quantum Random Number Generator

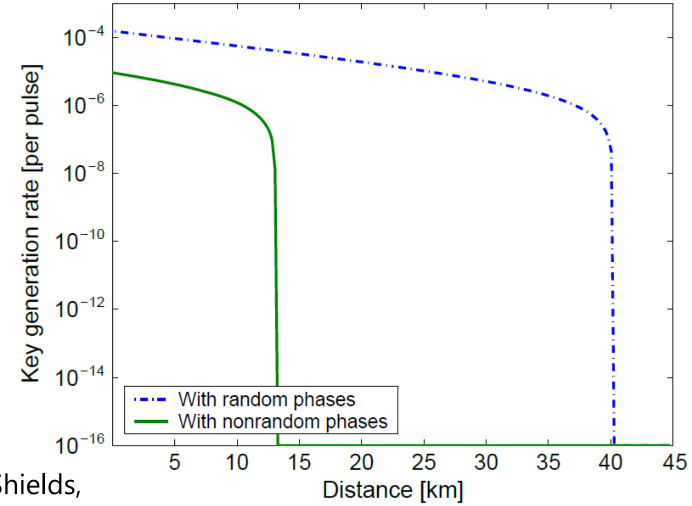
- Information theoretic security
  - Random choices of bit, bases
  - Decoy state: random intensity choice
- Global phase randomisation
  - Weak coherent pulses

  ⇒ Retrieve physics of single photons
- Pseudo-random numbers:
  - Not suitable for QKD



BB84 QKD protocol





T.K. Paraiso, R.I. Woodward, D. G. Marangon, V. Lovic, Z.-L. Yuan and A.J. Shields, *Advanced Laser Technology for Quantum Communications (Tutorial Review)* Advanced Quantum Technologies 4, 2100062 (2021)

H. K. Lo and J. Preskill, Quant. Inf. Comput. 8, 431–458 (2007)

quantum secure

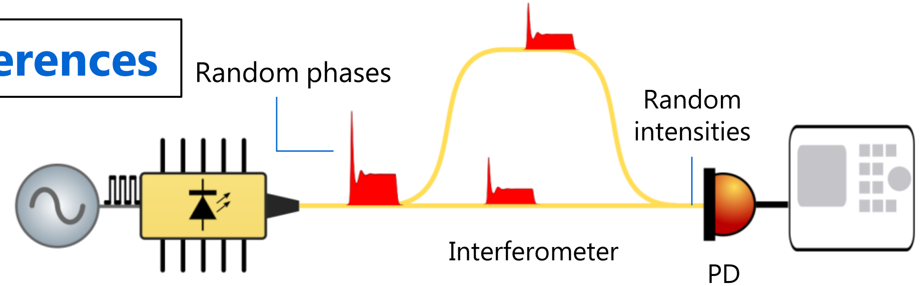
Photonic ICs for QKD: Quantum Random Number Generator

- Information theoretic security
  - Random choices of bit, bases
  - Decoy state: random intensity choice
- Global phase randomisation
  - Weak coherent pulses

  ⇒ Retrieve physics of single photons
- Gain switching in laser diodes
  - Spontaneous emission noise
    - Quantum phase fluctuations
  - Quantum source of entropy

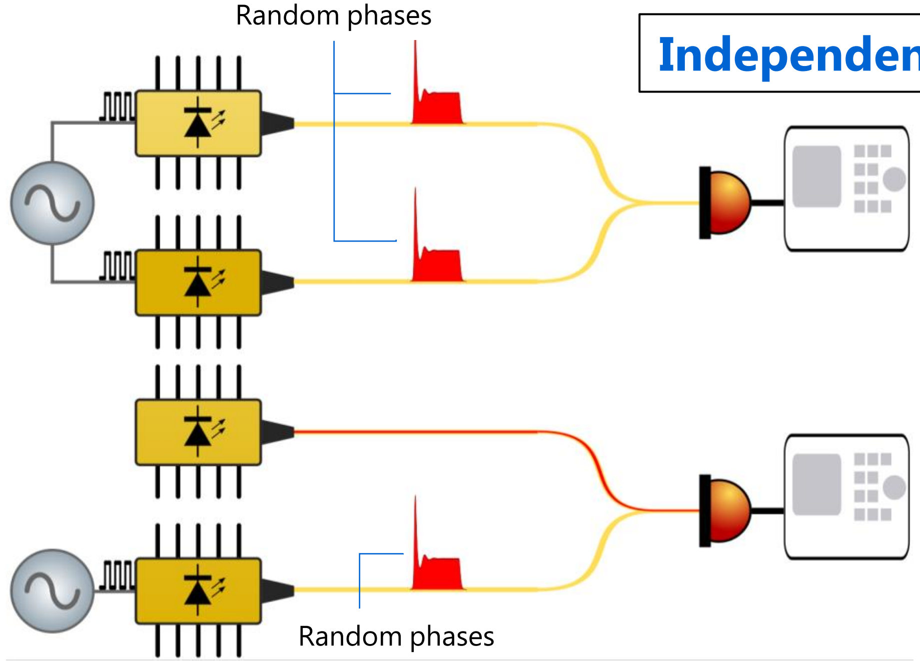
quantum secure

Self interferences



- F. Xu et al. Ultrafast quantum random number generation based on quantum phase fluctuations, *Opt. Express* **20**, 12366–12377 (2012)
- Z. L. Yuan et al. Robust random number generation using steady-state emission of gain-switched laser diodes, *Appl. Phys. Lett.* **104**, 261112 (2014)

Independent lasers



- S.-H. Sun and F. Xu, Experimental study of a quantum-number generator based on two independent lasers, Phys. Rev. A 96, 062314 (2017)

Photonic ICs for QKD: Quantum Random Number Generator

QRNG CHIPS

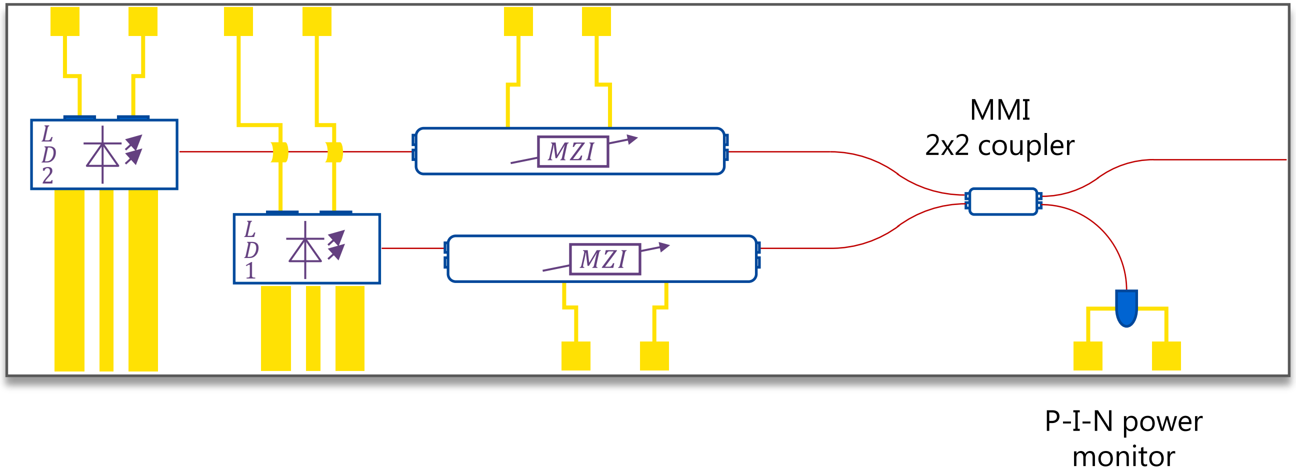
Active: InP

Entropy source:
Spontaneous emission

Measurement:
Dual-DFB interference

Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm



T Roger et al. Real-time interferometric quantum random number generation on chip
J. Opt. Soc. Am. B **36**(3), B137–B142 (2019)

Photonic ICs for QKD: Quantum Random Number Generator

QRNG CHIPS

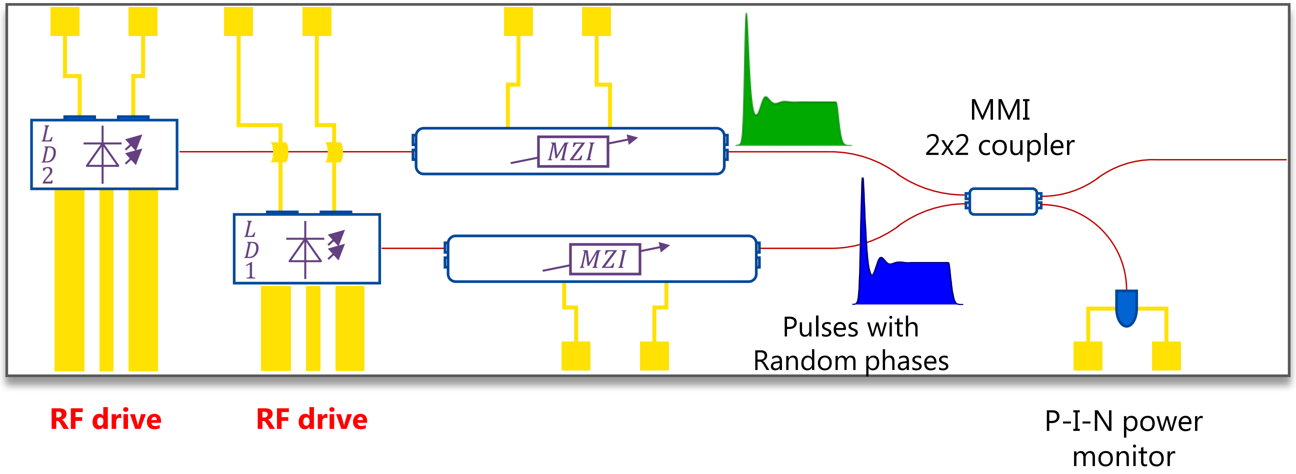
Active: InP

Entropy source:
Spontaneous emission

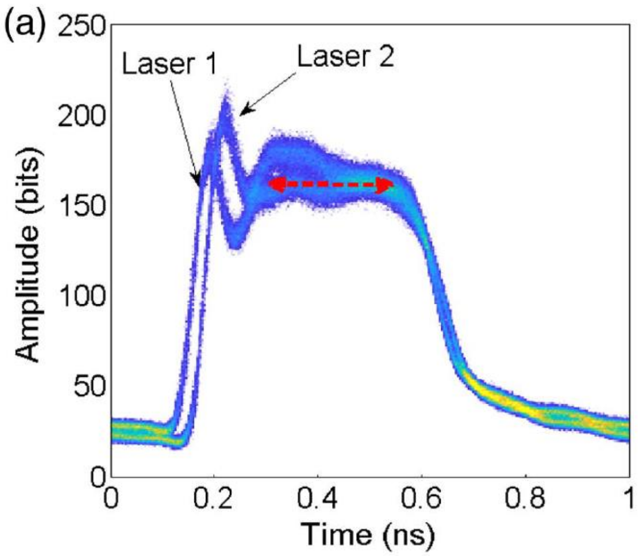
Measurement:
Dual-DFB interference

Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm



Adjust temporal delay



T Roger et al. Real-time interferometric quantum random number generation on chip
J. Opt. Soc. Am. B **36**(3), B137–B142 (2019)

Photonic ICs for QKD: Quantum Random Number Generator

QRNG CHIPS

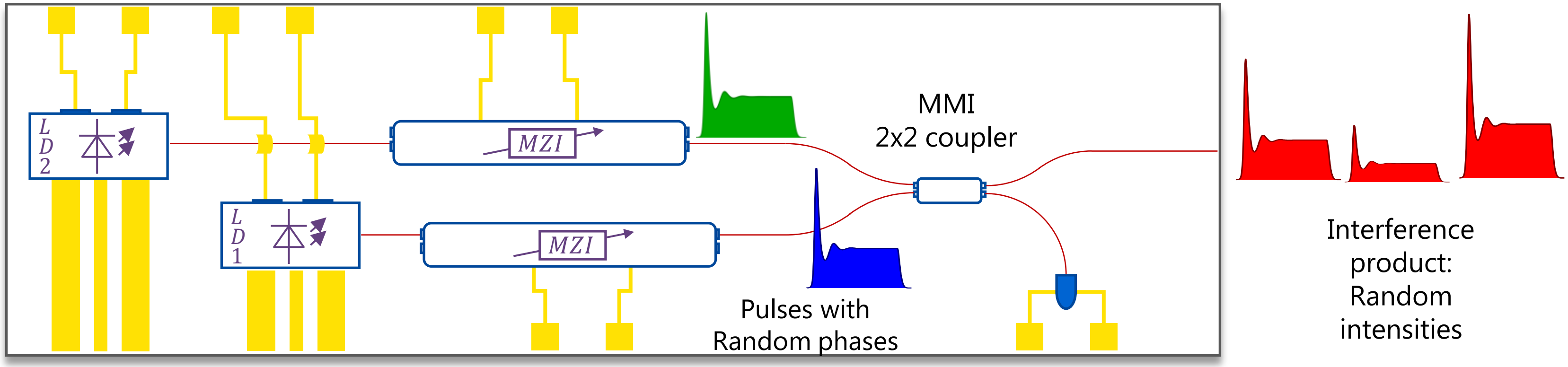
Active: InP

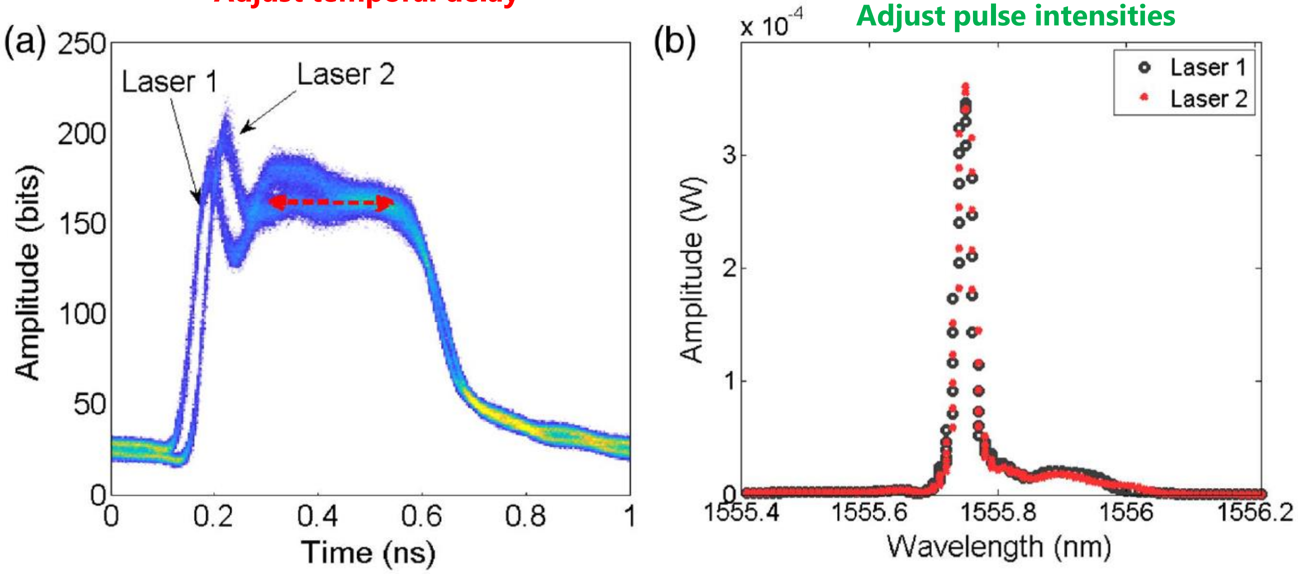
Entropy source:
Spontaneous emission

Measurement:
Dual-DFB interference

Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm





T Roger et al. Real-time interferometric quantum random number generation on chip
J. Opt. Soc. Am. B **36**(3), B137–B142 (2019)

Photonic ICs for QKD: Quantum Random Number Generator

QRNG CHIPS

Active: InP

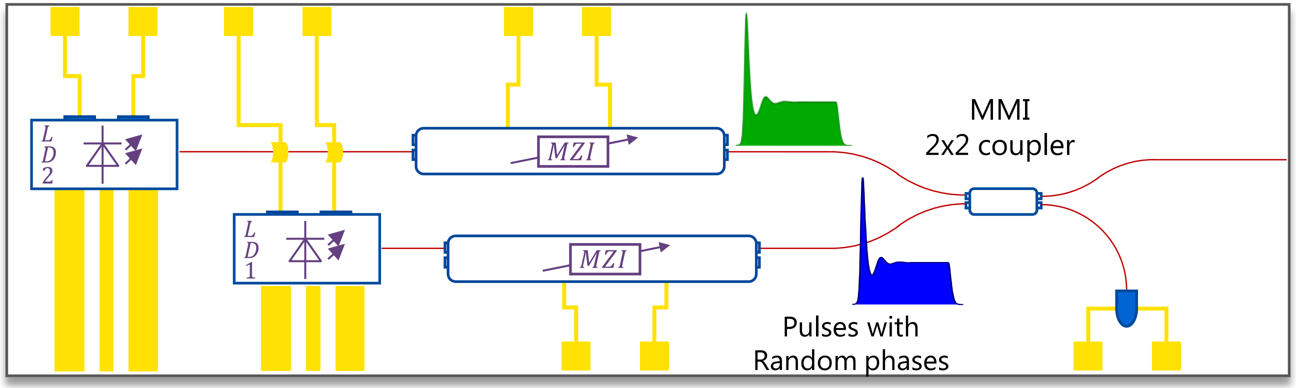
Entropy source:
Spontaneous emission

Measurement:
Dual-DFB interference

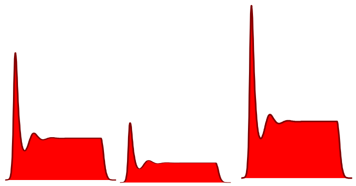
Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm

Adjust spectral detuning **VOA**

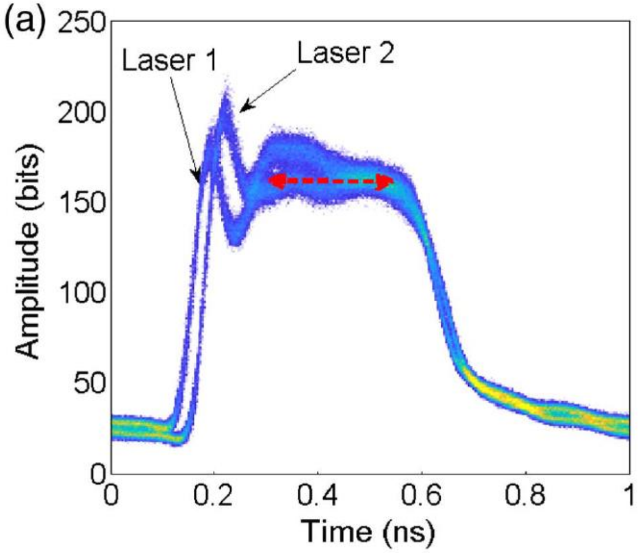


RF drive **RF drive** **VOA** P-I-N power monitor

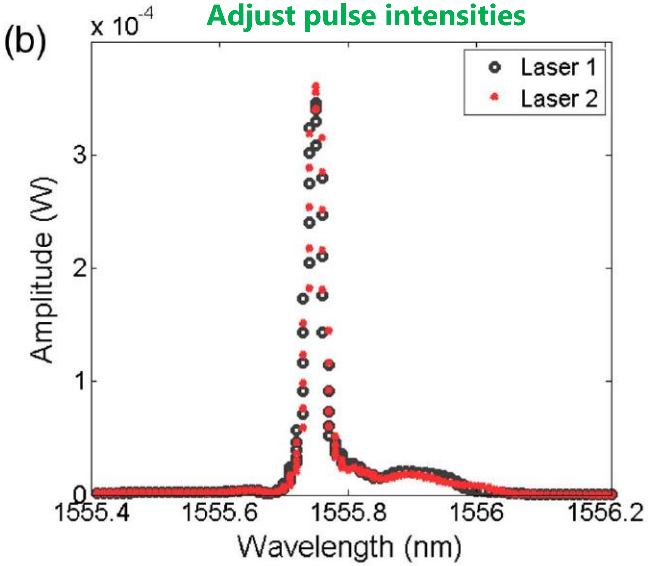


Interference product: Random intensities

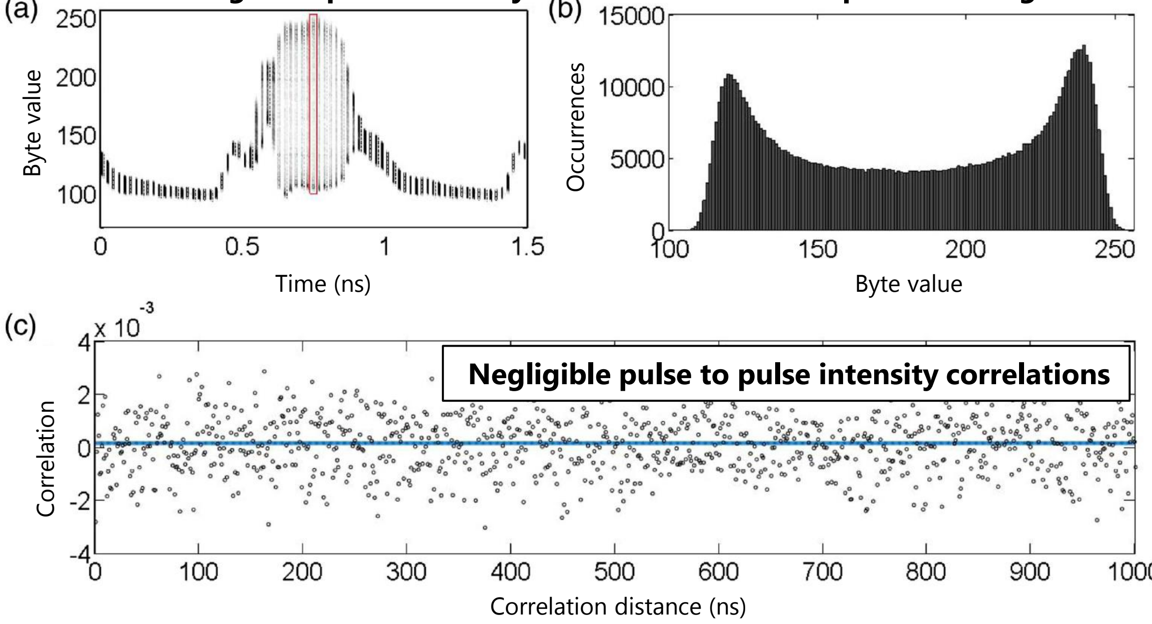
Adjust temporal delay



Adjust spectral detuning
Adjust pulse intensities



Time integrated pulse intensity **Double-peaked histogram**



T Roger et al. Real-time interferometric quantum random number generation on chip
J. Opt. Soc. Am. B **36**(3), B137–B142 (2019)

Photonic ICs for QKD: Quantum Random Number Generator

QRNG CHIPS

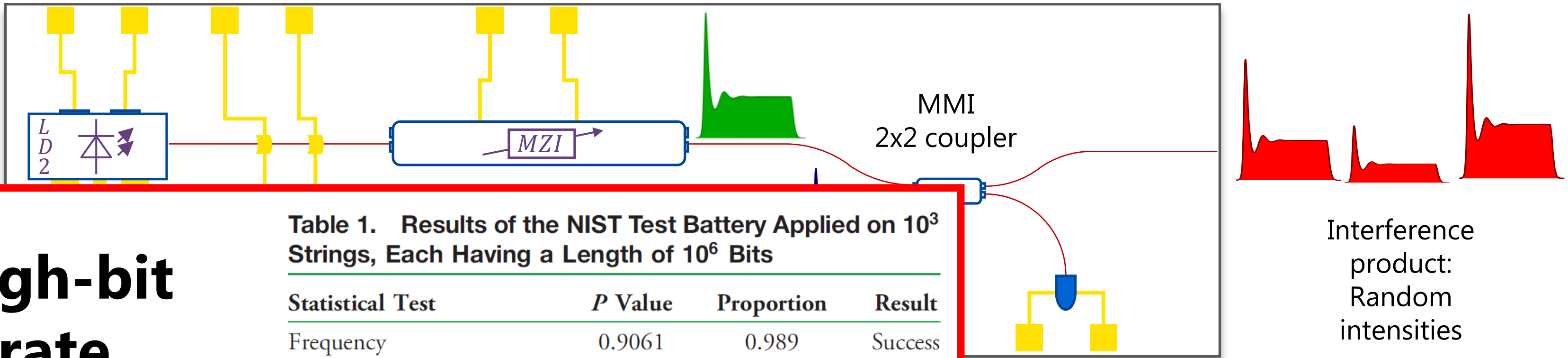
Active: InP

Entropy source:
Spontaneous emission

Measurement:
Dual-DFB interference

Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm



High-bit rate
4 Gbit/s

BB84@1GHz clock

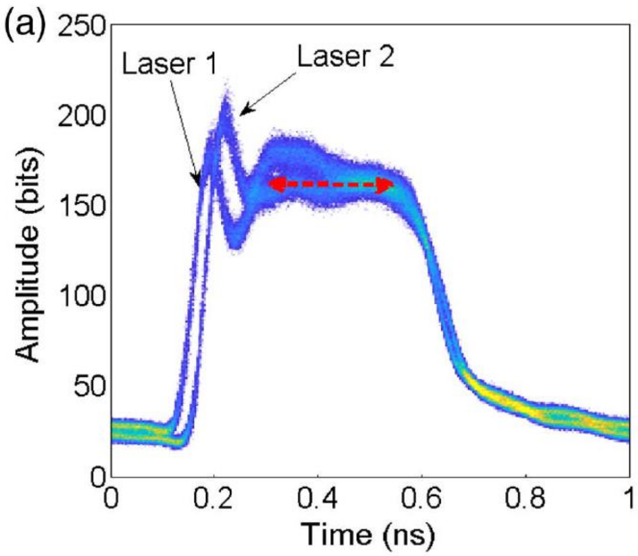
1 bit -> state {0,1}
1 bit -> basis $\{X, Y\}$
2 bits -> int $\{S, D, V\}$

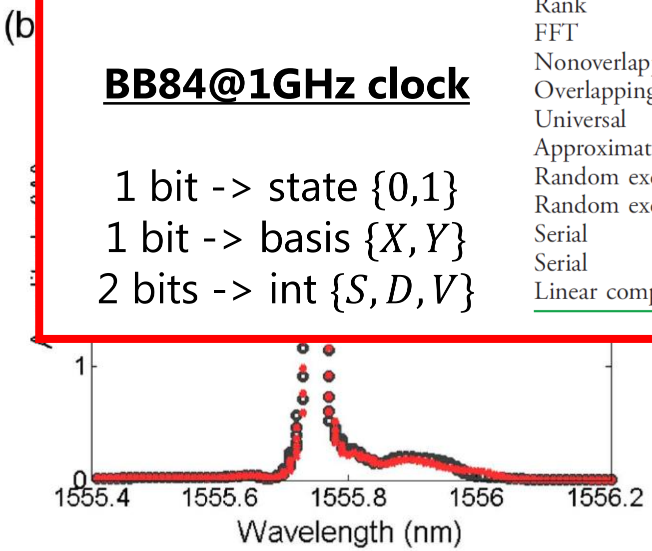
Table 1. Results of the NIST Test Battery Applied on 10^3 Strings, Each Having a Length of 10^6 Bits

Statistical Test	*P* Value	Proportion	Result
Frequency	0.9061	0.989	Success
Block frequency	0.0835	0.992	Success
Cumulative sums	0.8817	0.986	Success
Cumulative sums	[illegible]	0.989	Success
Runs	[illegible]	0.986	Success
Longest run	[illegible]	0.992	Success
Rank	[illegible]	0.986	Success
FFT	[illegible]	0.993	Success
Nonoverlapping tem[illegible]	0.5045	0.990	Success
Overlapping template	0.8343	0.983	Success
Universal	0.1238	0.987	Success
Approximate entropy	0.3330	0.990	Success
Random excursions	0.4151	0.989	Success
Random excursions variant	0.4882	0.992	Success
Serial	0.2012	0.990	Success
Serial	0.4101	0.995	Success
Linear complexity	0.3361	0.992	Success

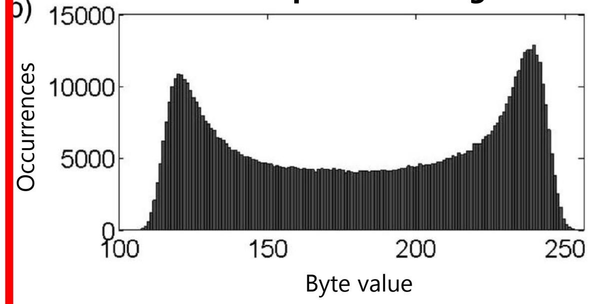
PASSED

Adjust temporal delay

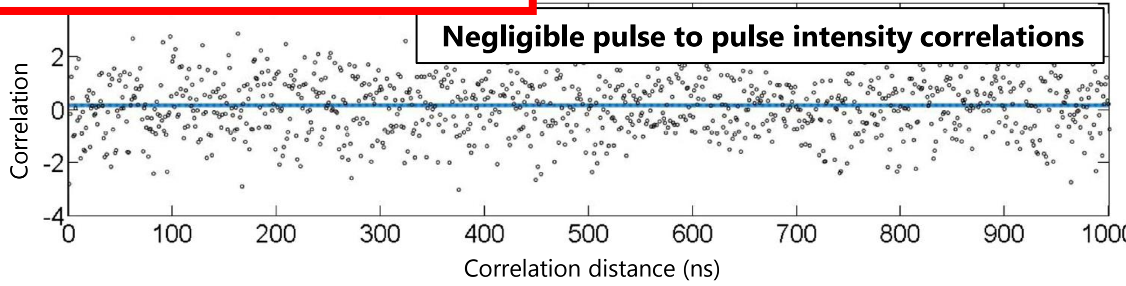




Double-peaked histogram



Negligible pulse to pulse intensity correlations



T Roger et al. Real-time interferometric quantum random number generation on chip
J. Opt. Soc. Am. B **36**(3), B137–B142 (2019)

QKD TRANSMITTER CHIP

Photonic ICs for QKD: Quantum Transmitter

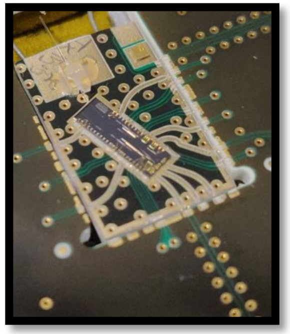
QTx CHIP

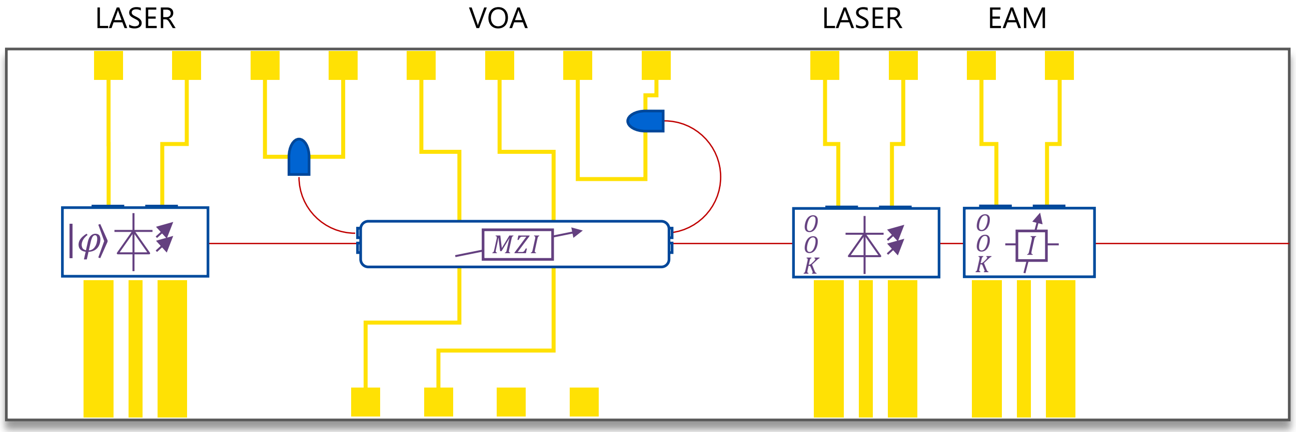
Active: InP
Protocol:
Time-bin decoy BB84

Modulation:
Phase-seeding
Multi-level, OOK

Clock-rate: 1 GHz

Chip footprint
2 mm x 6 mm





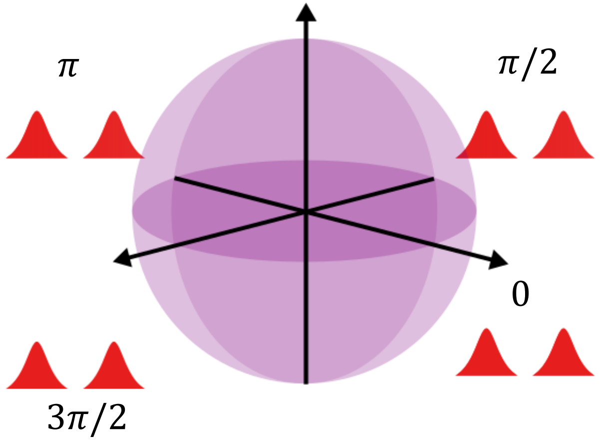
Phase-seeding = optical injection locking with phase preparation

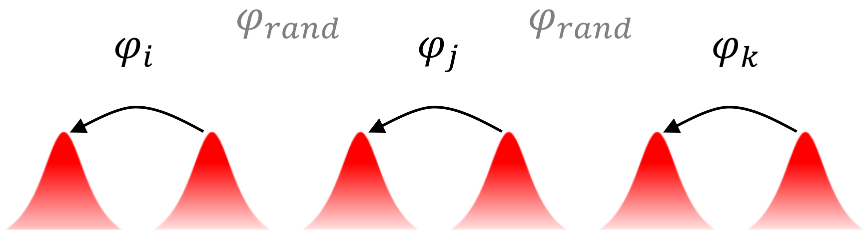
T Paraiso, R Woodward, D. Marangon et al. Advanced Laser Technology for Quantum Communications
Adv Quant Comm, in press (2021)

Time-bin BB84 protocol: 2 bases, 2 states

4 differential phase states: $\{0, \pi\}$, $\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$

Global phase randomisation





Z.L. Yuan et al. Directly Phase-Modulated Light Source
Phys Rev X **6**, 031044 (2016)

TK Paraiso et al. A modulator-free quantum key distribution chip
npj Quantum Inf **5**, 42 (2019)

Photonic ICs for QKD: Quantum Transmitter

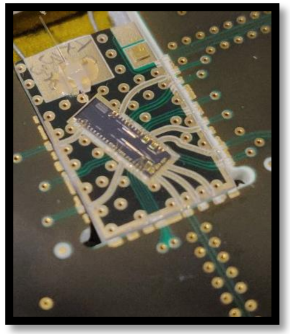
QTx CHIP

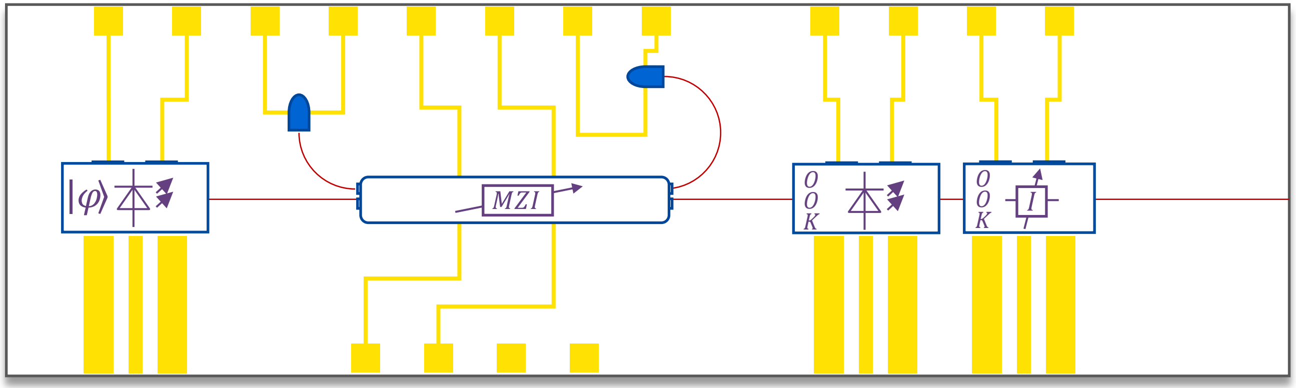
Active: InP
Protocol:
Time-bin decoy BB84

Modulation:
Phase-seeding
Multi-level, OOK

Clock-rate: 1 GHz

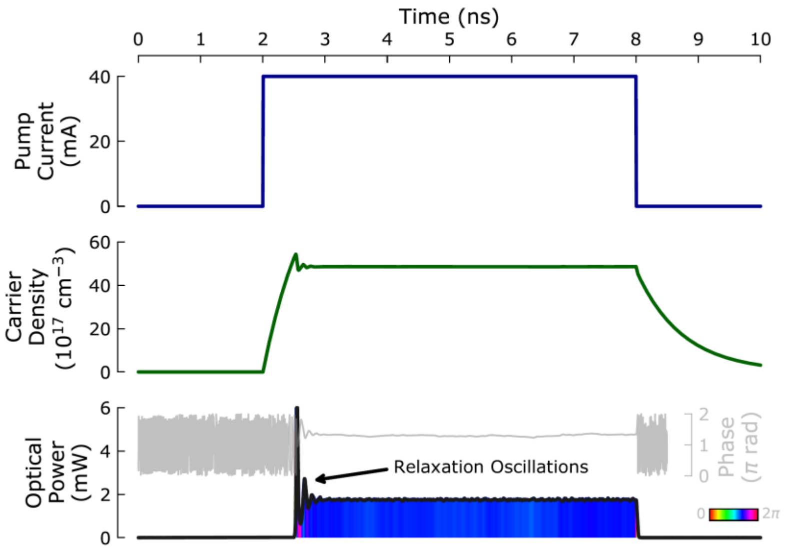
Chip footprint
2 mm x 6 mm





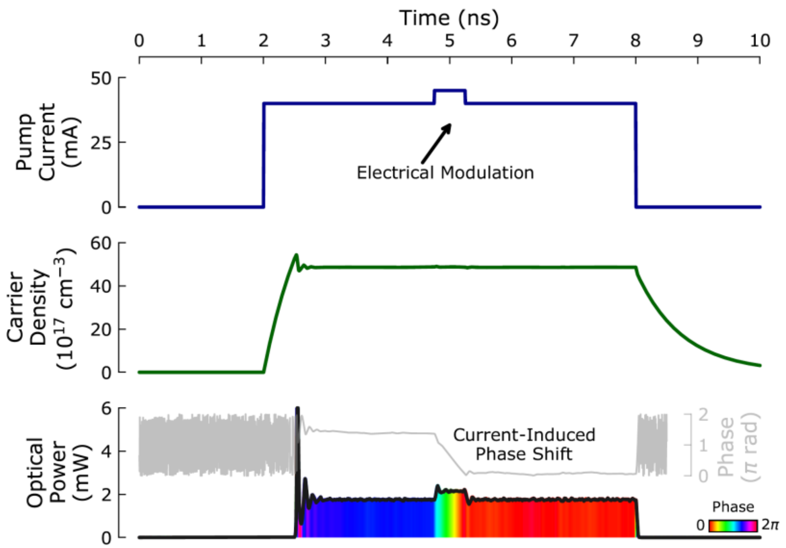
LD1: Phase preparation

(1) Long coherent GS pulse



Phase preparation
via
Direct modulation

(2) Phase preparation



TK Paraiso et al. A modulator-free quantum key distribution chip
npj Quantum Inf **5**, 42 (2019)

T Paraiso, R Woodward, D. Marangon et al. Advanced Laser Technology for Quantum Communications
Adv Quant Comm, in press (2021)

Photonic ICs for QKD: Quantum Transmitter

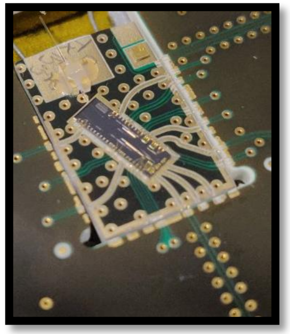
QTx CHIP

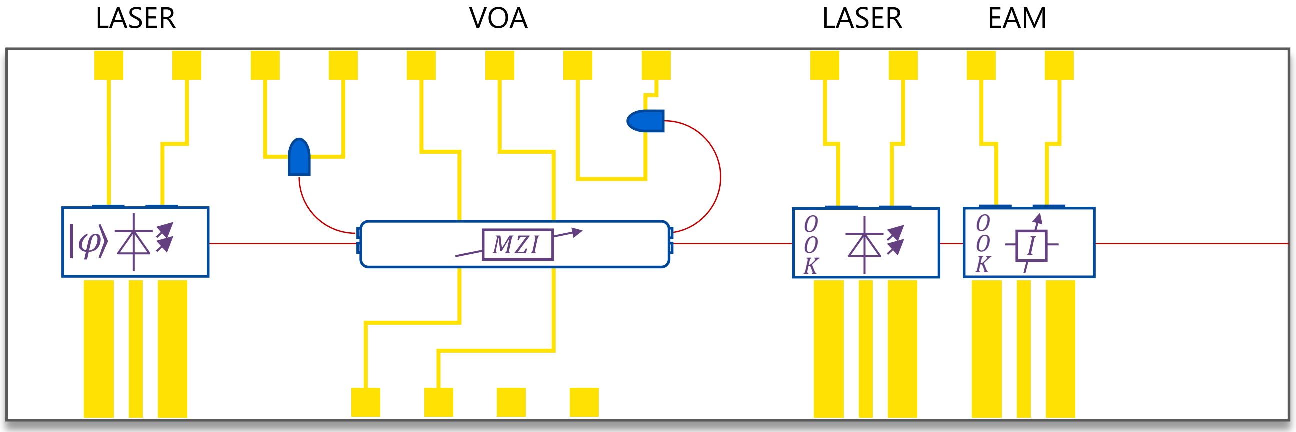
Active: InP
Protocol:
Time-bin decoy BB84

Modulation:
Phase-seeding
Multi-level, OOK

Clock-rate: 1 GHz

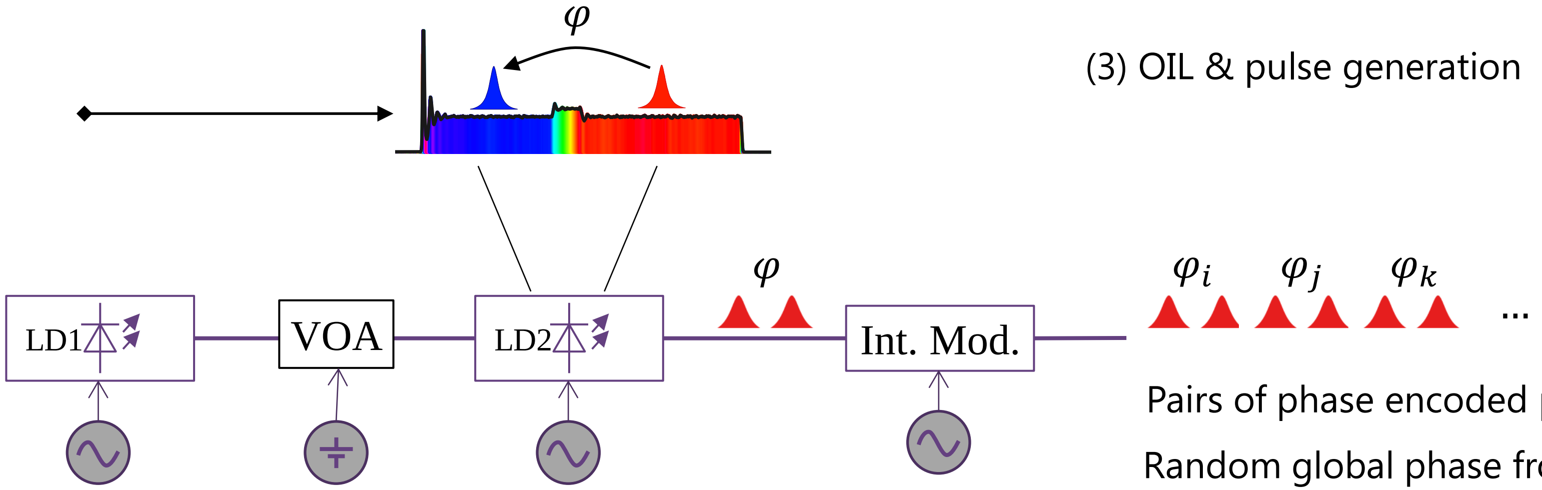
Chip footprint
2 mm x 6 mm





LD1: Phase preparation

LD2: Short GS pulses



(3) OIL & pulse generation

Pairs of phase encoded pulses

Random global phase from GS LD1 pulse

TK Paraiso et al. A modulator-free quantum key distribution chip
npj Quantum Inf **5**, 42 (2019)

T Paraiso, R Woodward, D. Marangon et al. Advanced Laser Technology for Quantum Communications
Adv Quant Comm, in press (2021)

Photonic ICs for QKD: Quantum Transmitter

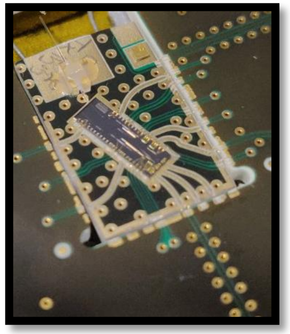
QTx CHIP

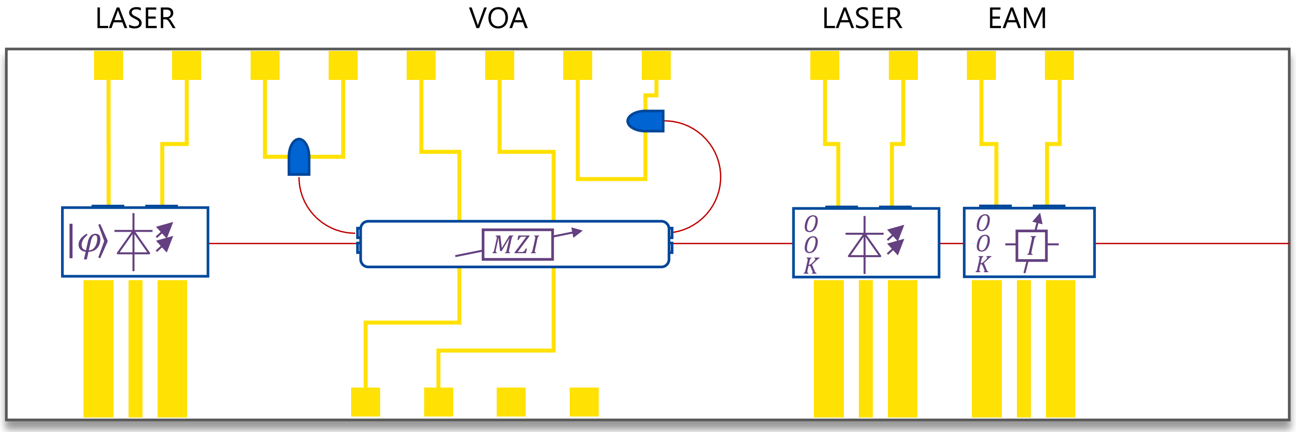
Active: InP
Protocol:
Time-bin decoy BB84

Modulation:
Phase-seeding
Multi-level, OOK

Clock-rate: 1 GHz

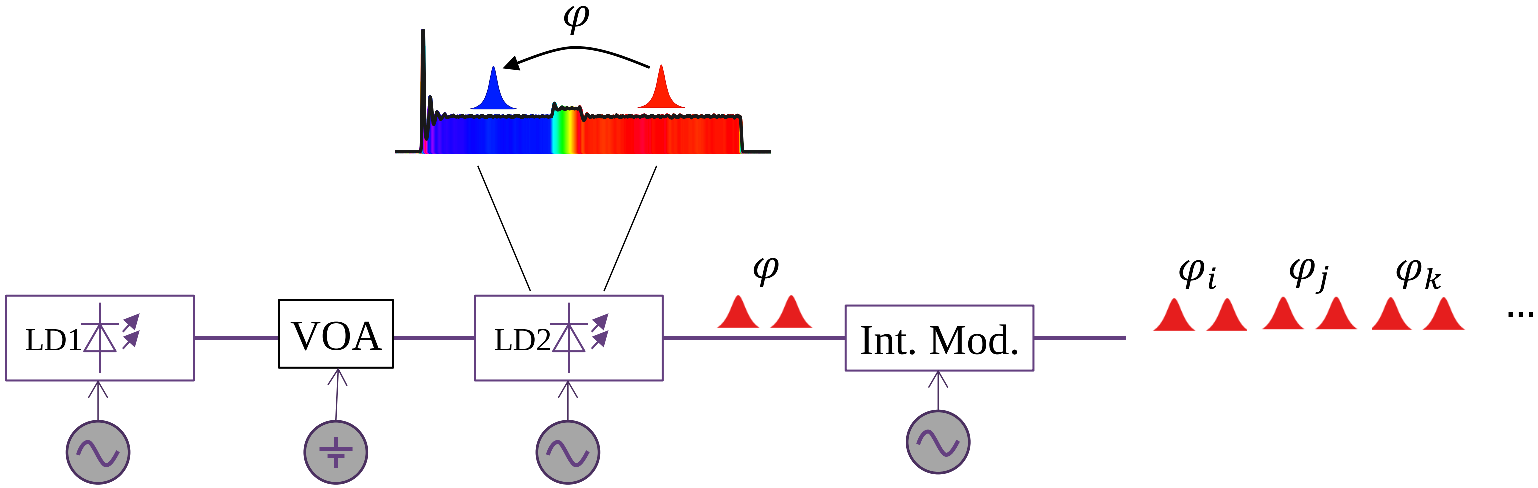
Chip footprint
2 mm x 6 mm





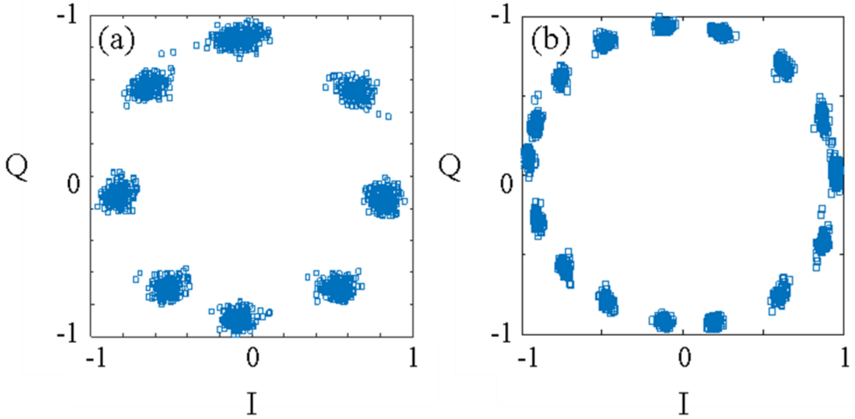
LD1: Phase preparation

LD2: Short GS pulses



Power efficient phase encoding:

8-RZ-DPSK **16-RZ-DPSK**



3 bits per state
2 GHz clock rate ⇒ 6 Gb/s

16 bits per state
2 GHz clock rate ⇒ 6 Gb/s

power efficient

TK Paraiso et al. A modulator-free quantum key distribution chip
npj Quantum Inf **5**, 42 (2019)

Photonic ICs for QKD: Quantum Transmitter

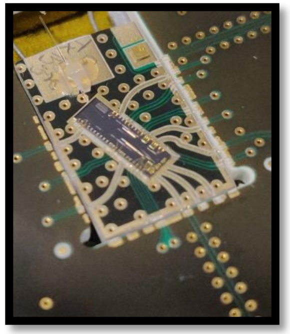
QTx CHIP

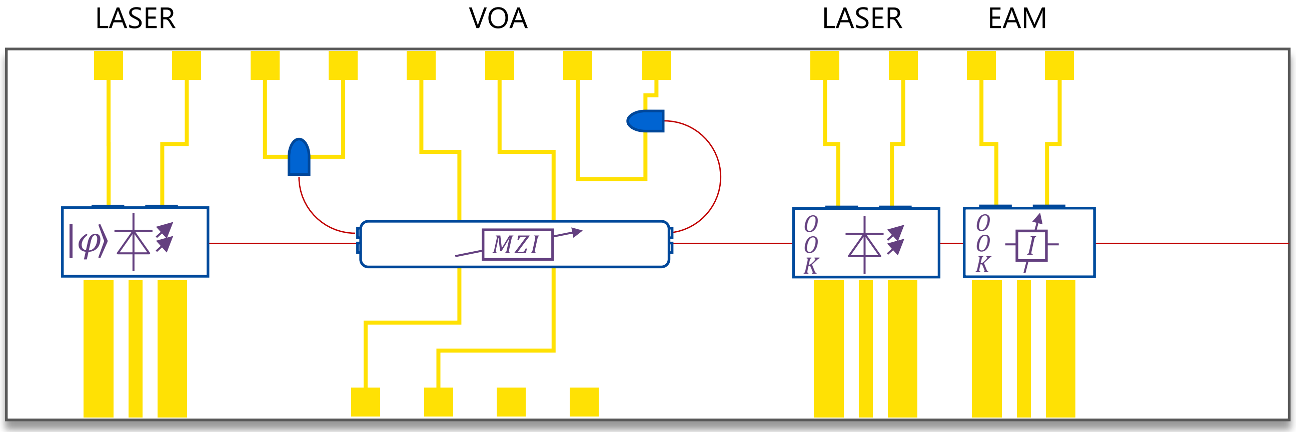
Active: InP
Protocol:
Time-bin decoy BB84

Modulation:
Phase-seeding
Multi-level, OOK

Clock-rate: 2 GHz

Chip footprint
2 mm x 6 mm

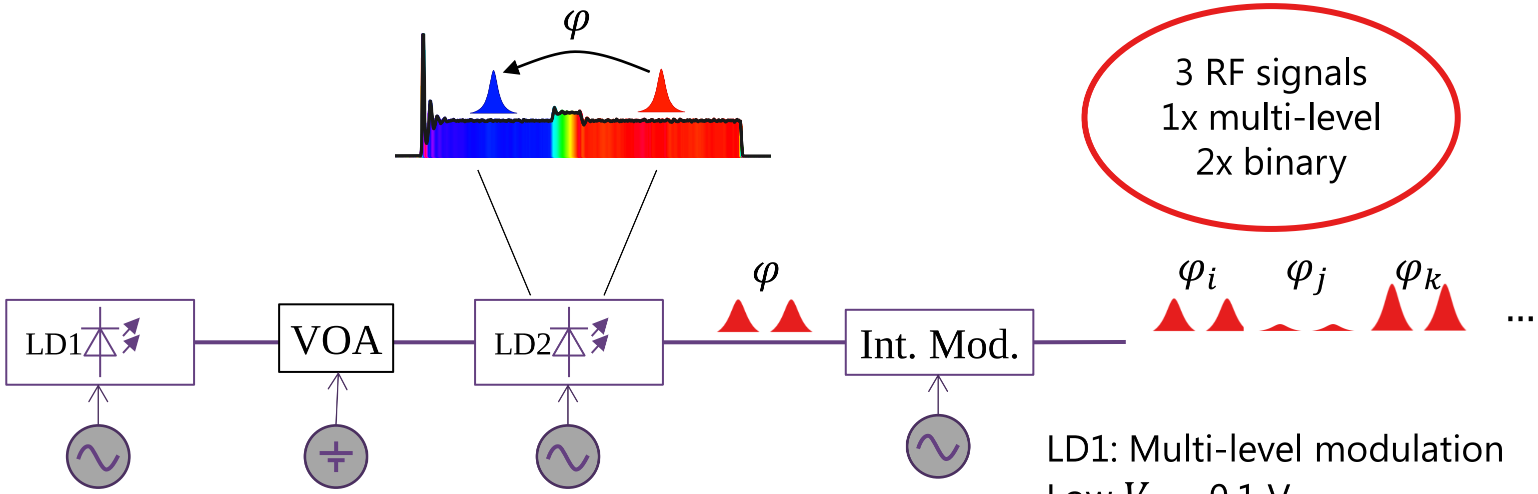




LD1: Phase preparation

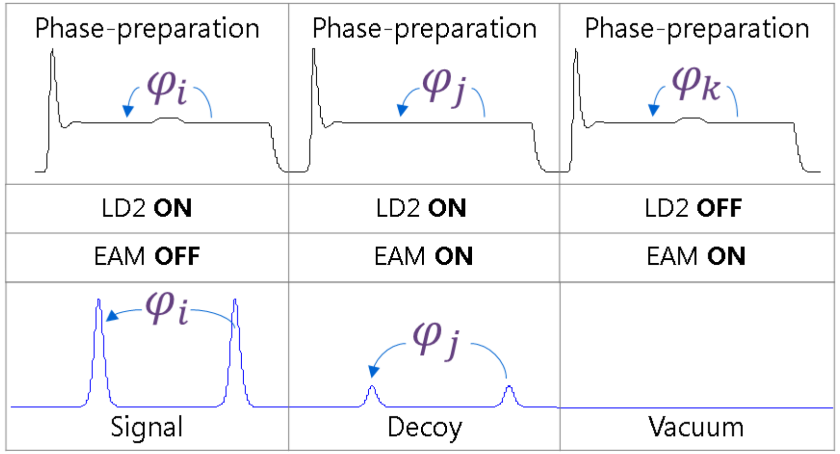
LD2: Short GS pulses

EAM Int. Mod.



LD1: Multi-level modulation
Low V_π ~ 0.1 V
EOPM/CDM V_π >4 V (typ.)
LD2: binary modulation
EAM: binary modulation

Power-efficient intensity encoding



LD2/EAM: interleaved binary modulation

power efficient

QKD RECEIVER CHIP

Photonic ICs for QKD: Quantum Receiver

QRx CHIP

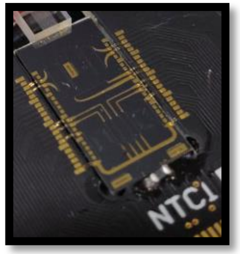
Passive: SiN/SiO2

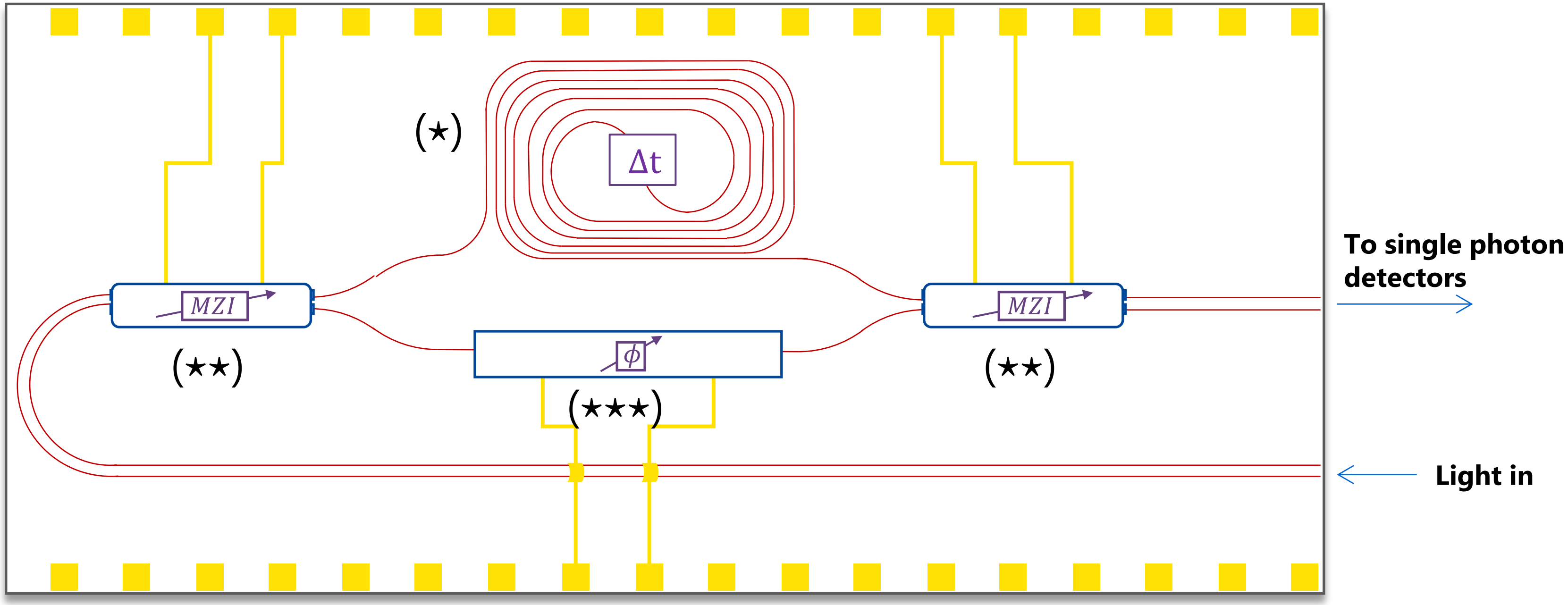
Decoding:
Delay-line MZI

Propagation losses:
~0.5 dB/cm

AMZI FSR: 2 GHz

Circuit footprint
4 mm x 8 mm





(⋆)

On-chip delay line 500 ps

(⋆⋆)

Loss compensation
Tunable MZI (thermo-optic)
Input beam-splitter loss compensation
Output beam-splitter fine tuning

(⋆⋆⋆)

Measurement basis
Phase tuning (thermo-optic)
Fast-modulation: external LiNb PM

Photonic ICs for QKD: Quantum Receiver

QRx CHIP

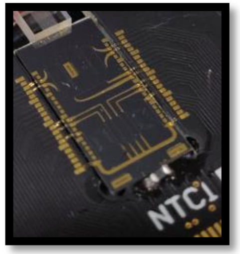
Passive: SiN/SiO2

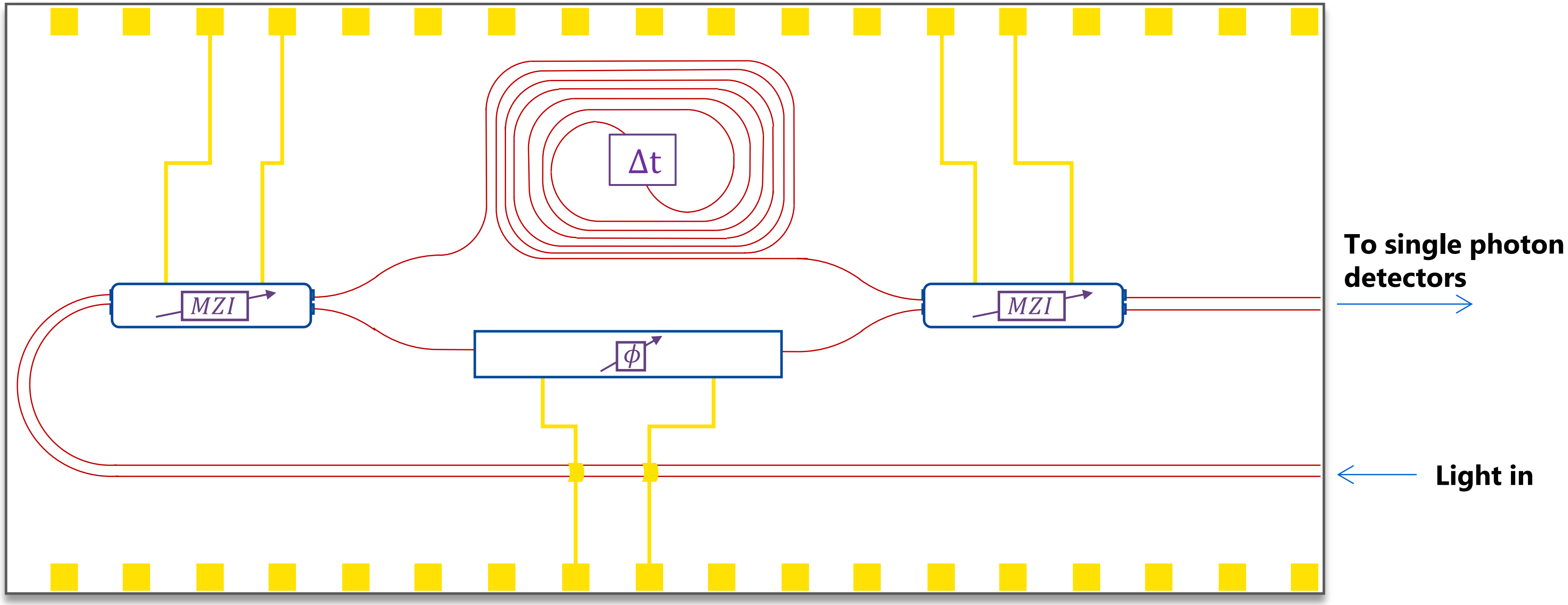
Decoding:
Delay-line MZI

Propagation losses:
~0.5 dB/cm

AMZI FSR: 2 GHz

Circuit footprint
4 mm x 8 mm





Insertion losses at receiver → penalty in QKD reach
Main contribution: on-chip delay line

- Propagation losses
- Bending losses

Material	SiO_2 / Si_3N_4	GaAs	InP	Silica
Group index	1.71	3.29	3.49	1.55
Refr. Ind. contrast [%]	15	25	25	<5
Bending radius [mm]	**0.5**	**0.2**	**0.25**	**10**
Propagation loss [db/cm]	**<0.5**	**<5**	**<4**	**< 0.05**
Transparency	VIS/NIR	VIS	NIR	VIS/NIR

Photonic ICs for QKD: Quantum Receiver

QRx CHIP

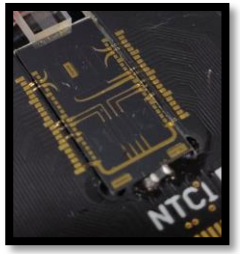
Passive: SiN/SiO2

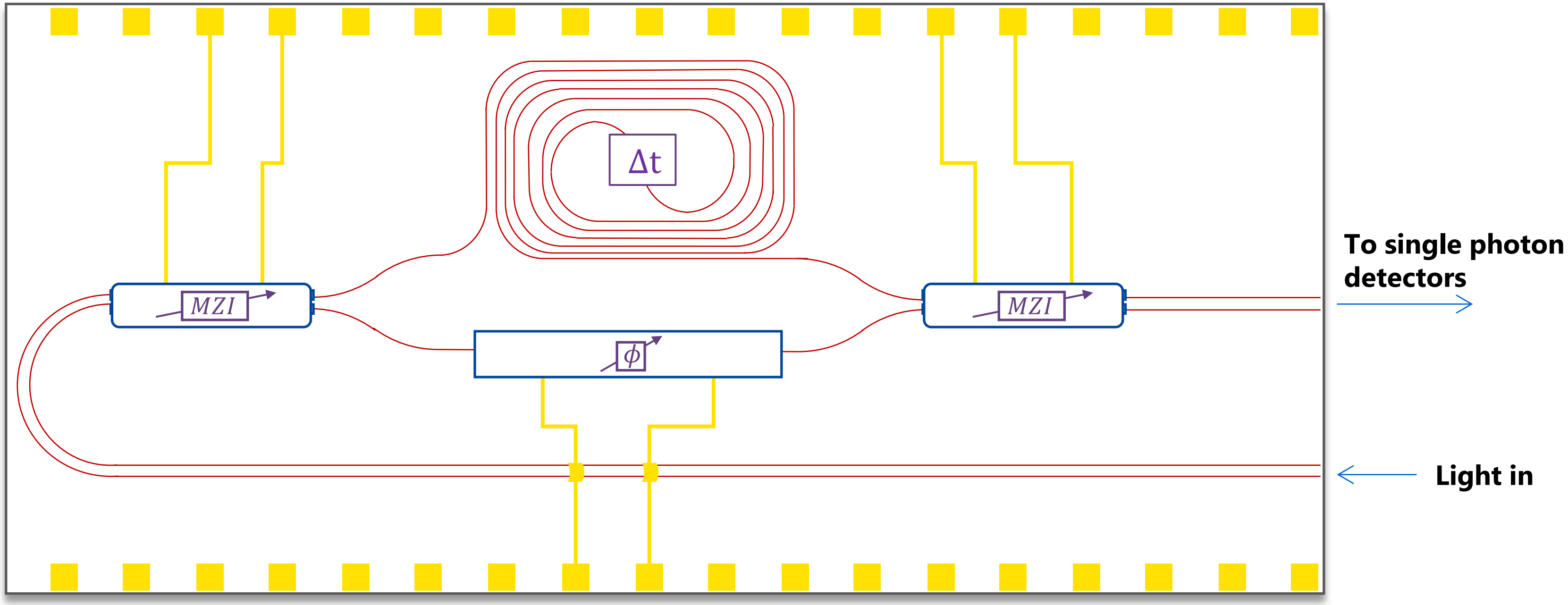
Decoding:
Delay-line MZI

Propagation losses:
~0.5 dB/cm

AMZI FSR: 2 GHz

Circuit footprint
4 mm x 8 mm





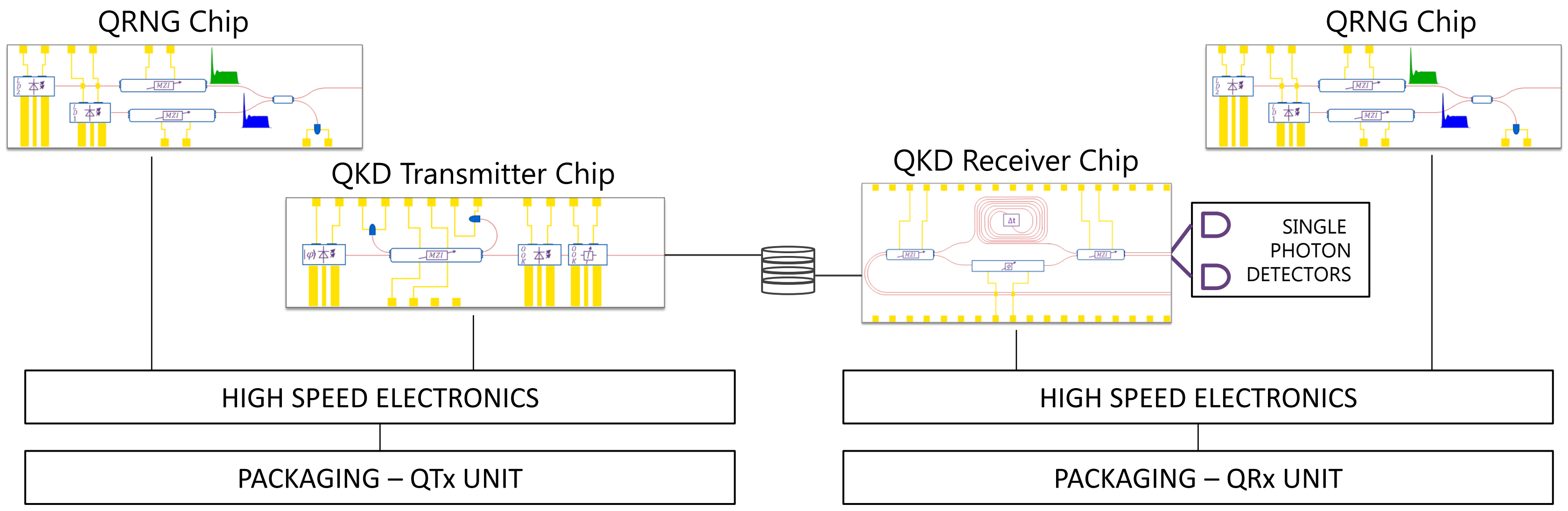
Insertion losses at receiver → penalty in QKD reach
Main contribution: on-chip delay line

- Propagation losses
- Bending losses

Loss vs footprint trade-off

Material	SiO_2 / Si_3N_4	GaAs	InP	Silica
Total loss (dB)	**4.5**	**22.80**	**17.19**	0.48
Delay line footprint (approx.)	**<5 mm^2**	~1 mm^2	~1 mm^2	**~ cm^2**

System integration challenges



- Global phase randomization
- Bit, basis choices
- Optimally biased choices
- High bit rate QRNG

Quantum random numbers generator

- Large number of RF channels
- Increased footprint
- High V_π -x-> CMOS level compatibility
- Complex electronics

Phase modulation technique

Si: CDM, InP: EOPM

- **Compact RF drive & processing electronics**
- Power consumption
- **Thermal management**
- Co-design optical chips and control electronics

Remove lab equipment for driving/processing

- **Photonic packaging**
- Optoelectronic assembly
- Clock distribution and synchronization
- **Stability – feedback control**
- Long term operation

System integration

- **Real-time random choice variables**
- Real time public communication
- Error-correction, Privacy amplification
- **Data-encryption**

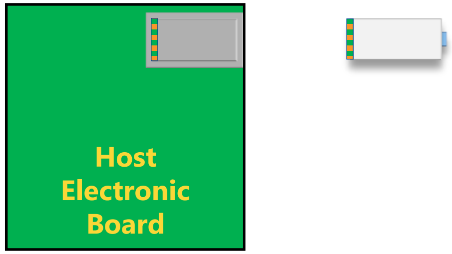
Real-time operation

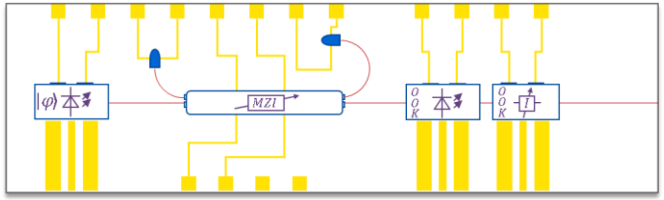
quantum secure — power efficient — deployable units

Photonic Packaging

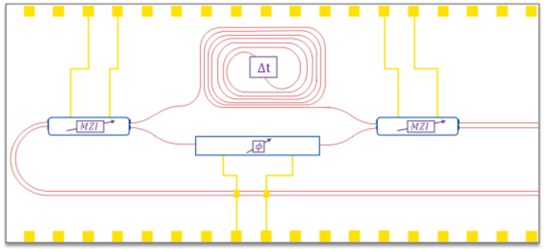
- Interface QKD chip and driving electronics
- Optical interface with outside world
- Thermal control and management (dT<0.005°C)
- Provide protection for photonic circuit

- QTx, QRx package
  - Pluggable compact form factor modules (CFP2)
  - Same approach as coherent optical comms.
  - Off-the shelf parts
  - Optics upgrade



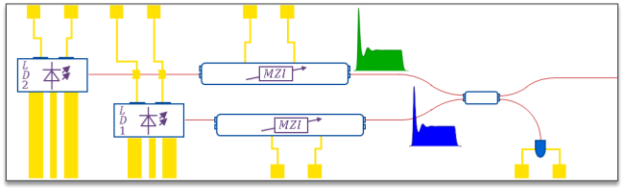


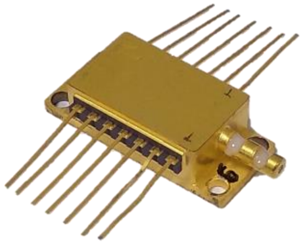
QKD Transmitter module (QTx)

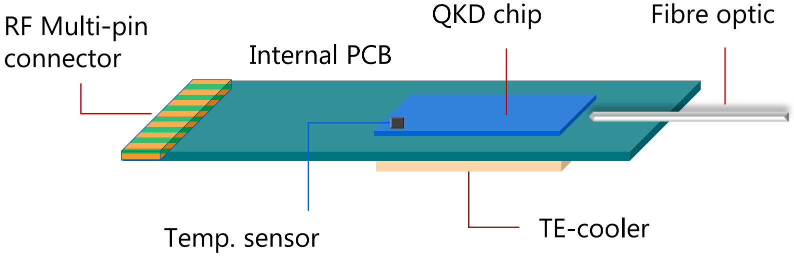


QKD Receiver module (QRx) Plugged in cage, with heat sink

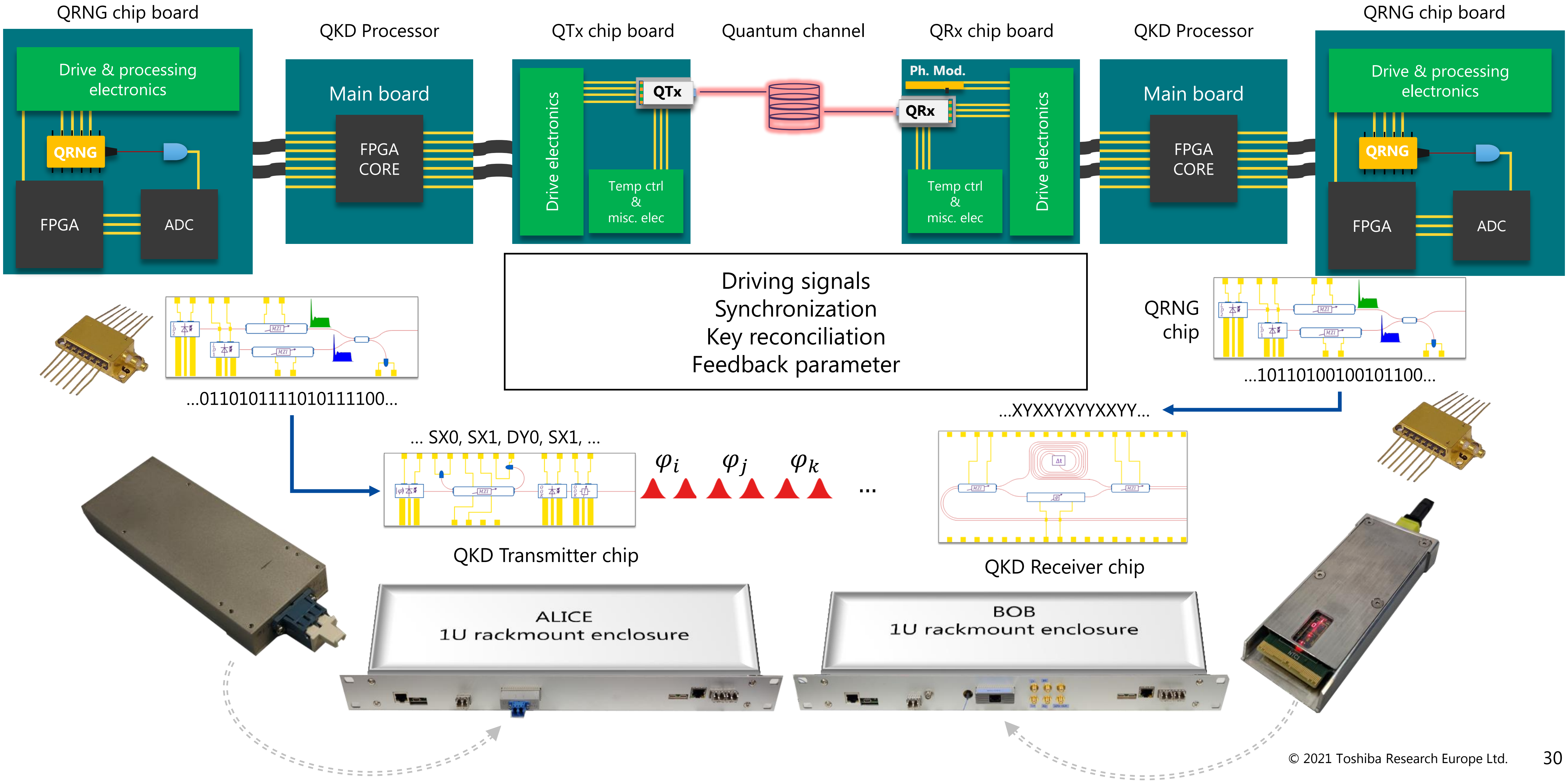
- QRNG package
  - 14-pin butterfly
  - Compatibility with pre-existing electronics



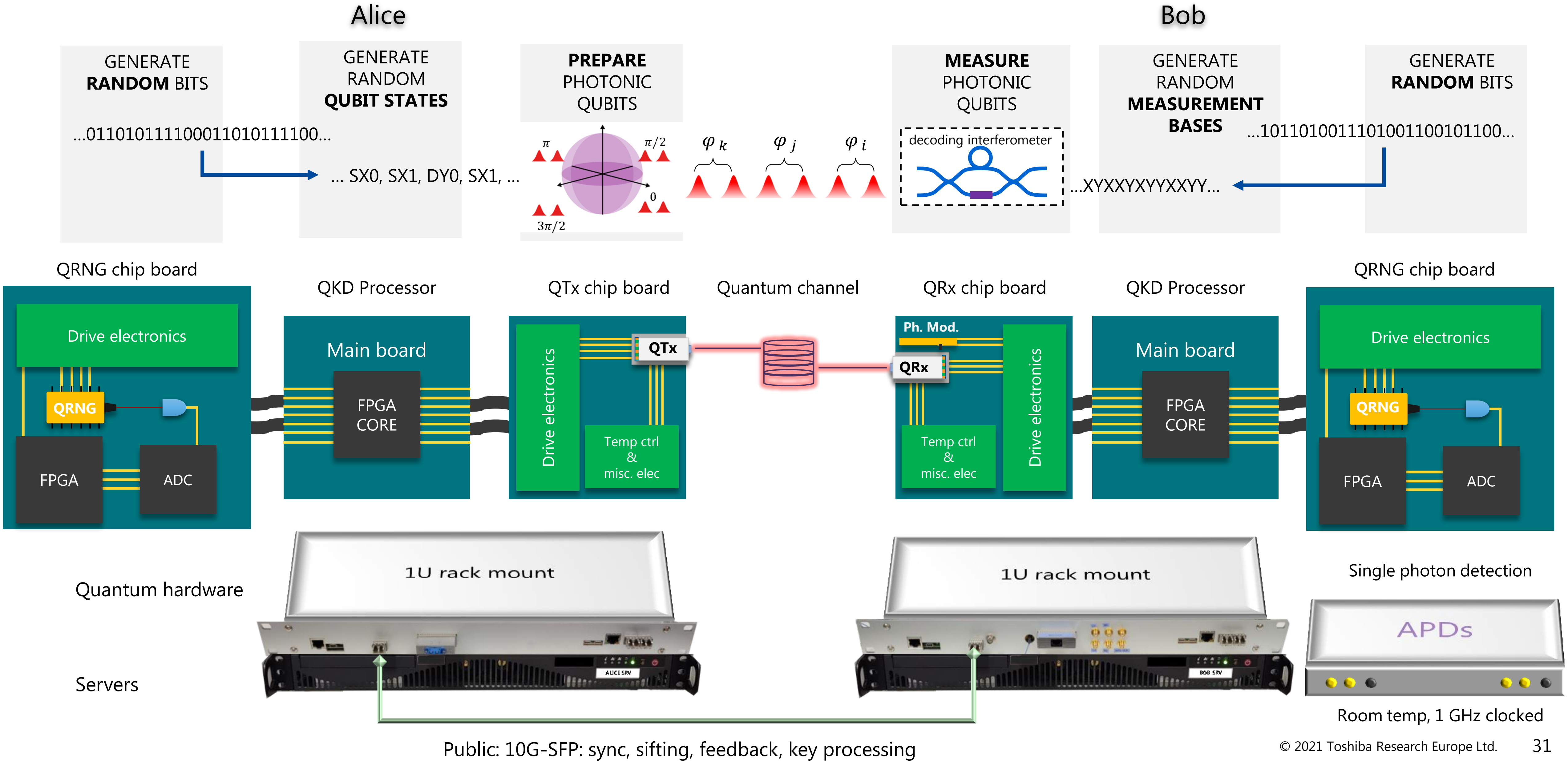




Real-time, High-speed Control Electronics



Real-time, High-speed Control Electronics



Stability and performance over long fibres

Fibre spools– metro distances

T12 Protocol:

- $P(Basis = X) = 15/16$
- $P(Decoy) = P(Vacuum) = 1/16$

Long term stability:

- >12h no interruption, no user intervention
- 0 dB sift rate: 4.6 Mb/s, QBER < 3.8%

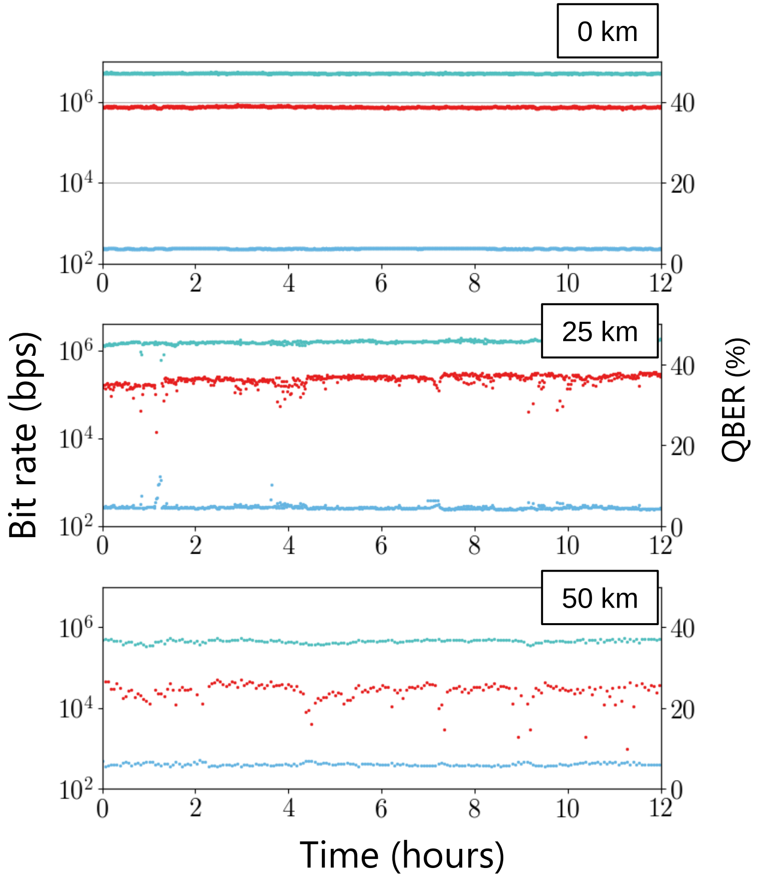
Feedback:

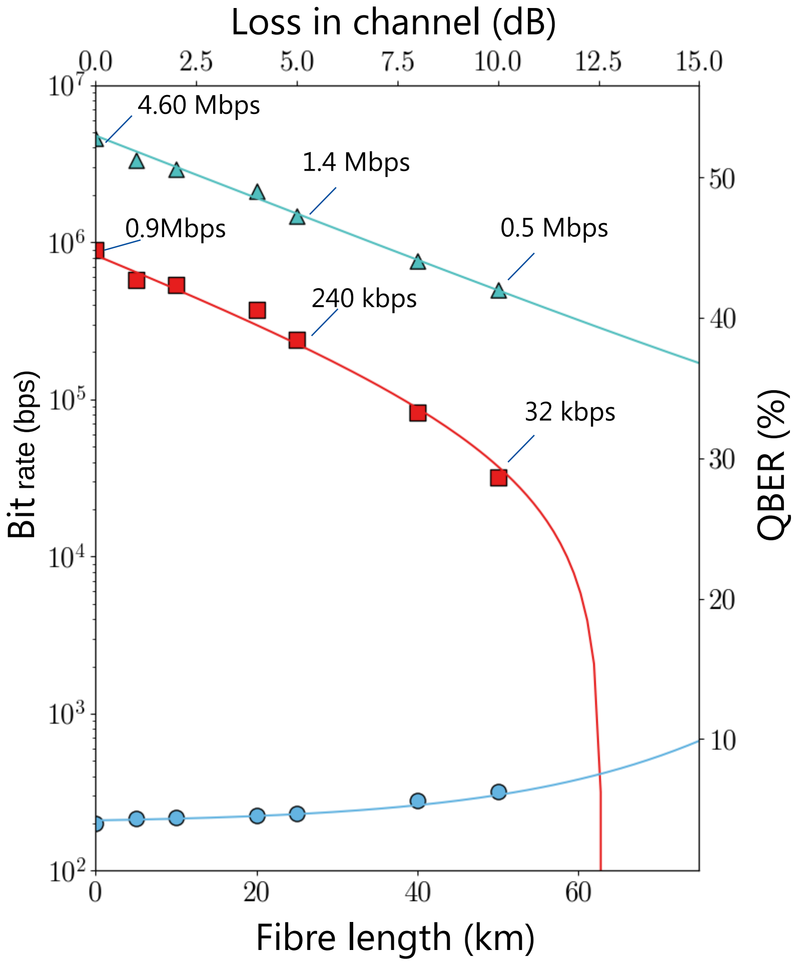
Phase drift compensation

Timing compensation in long fibres

Total receiver loss: ~8 dB

- QRx chip IL: 4.5 dB
- APD efficiency: 10%





deployable units

T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan and A. J. Shields, "A Photonic Integrated Quantum Communication System," Nature Photonics (2021).

Fully Deployable Autonomous System

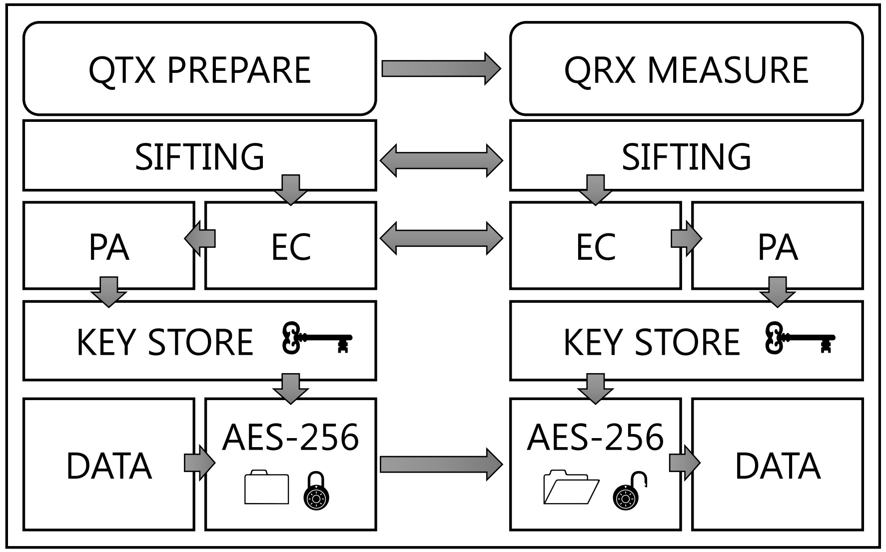
Real conditions

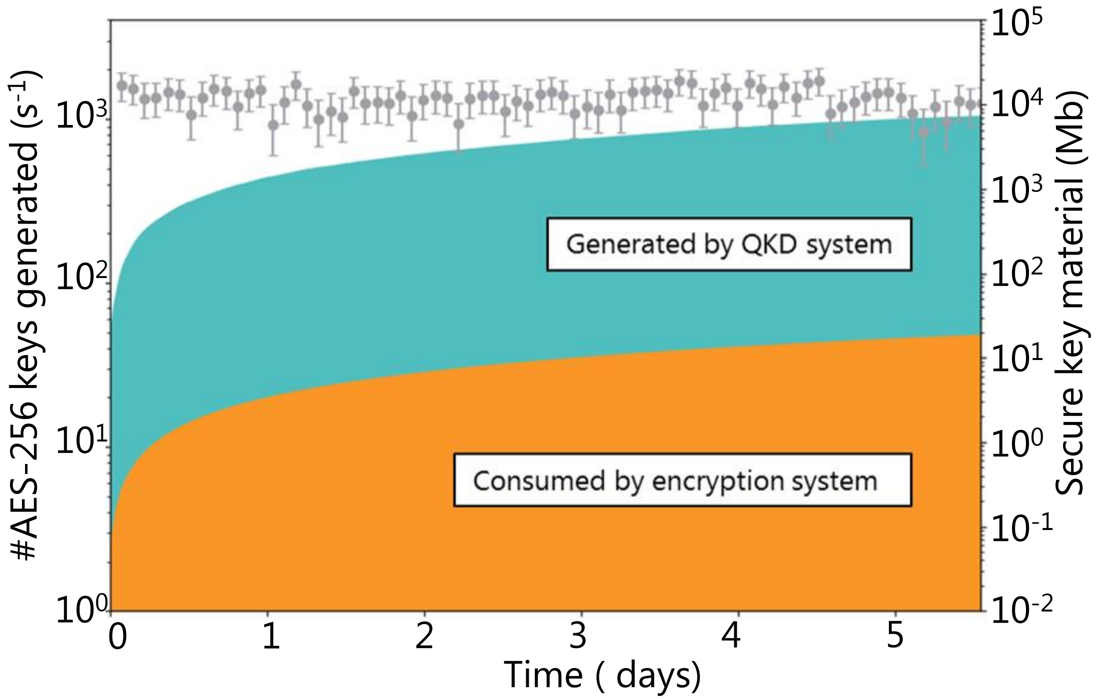
100G data encryption rate

AES 256 (256+96 init.) bits

Key management API compliant with ETSI GS QKD 014 standard

Channel loss	10 km
Secure key rate (SKR)	470 kbps
Standard deviation SKR	110 kbps
QBER	4.50 %
Sift rate	3.1 Mbps
QKD key block size	98.5 Mb
AES key size	256 + 96 bits (init.)
Number of AES keys per second	1335

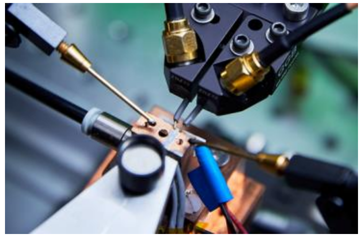


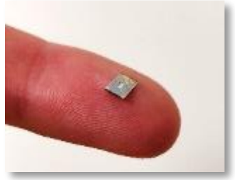


deployable units

T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan and A. J. Shields, "A Photonic Integrated Quantum Communication System," Nature Photonics (2021).

From Single Chips to Standalone System: a timeline



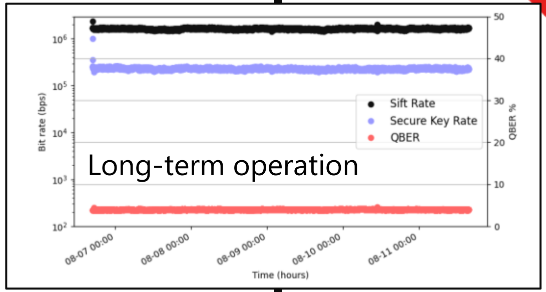


Single Photonic Chips

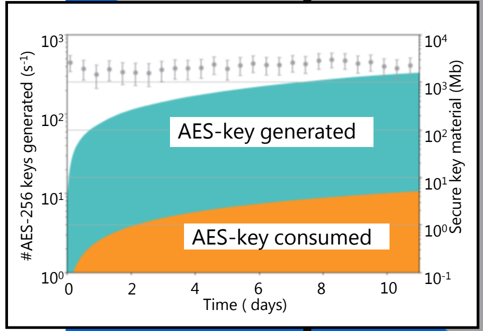
Individual chips

QKD Transmitter
Pluggable module
QRNG module

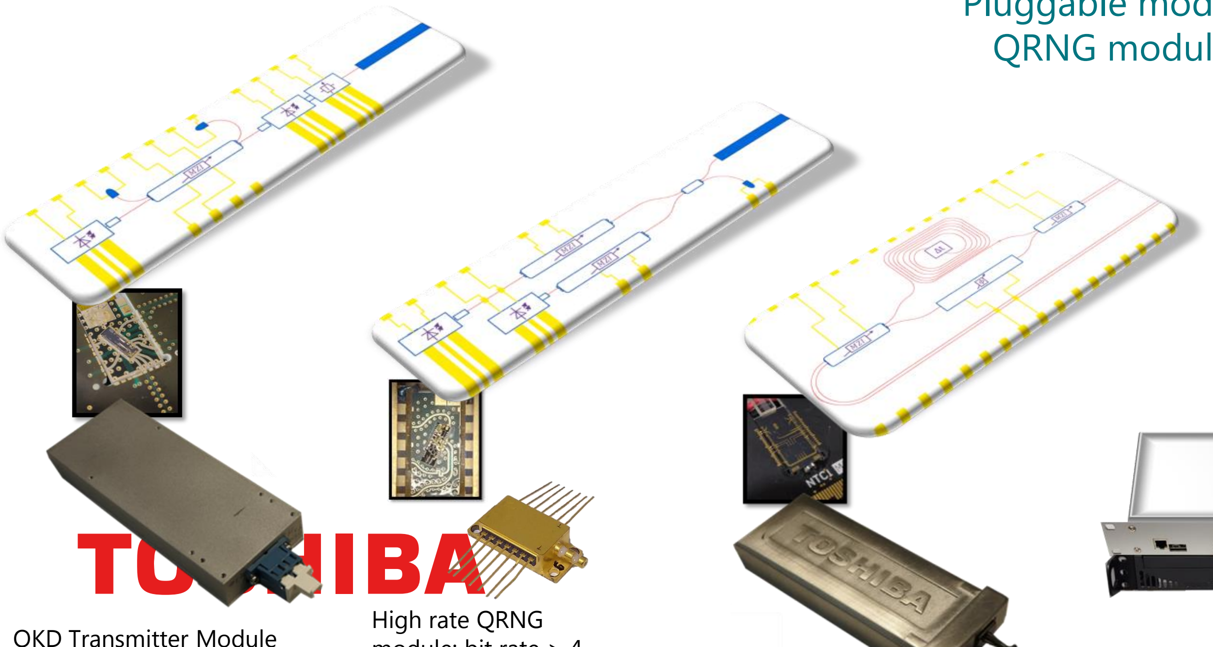
QKD Receiver
Pluggable module



Photonic integrated
QKD system



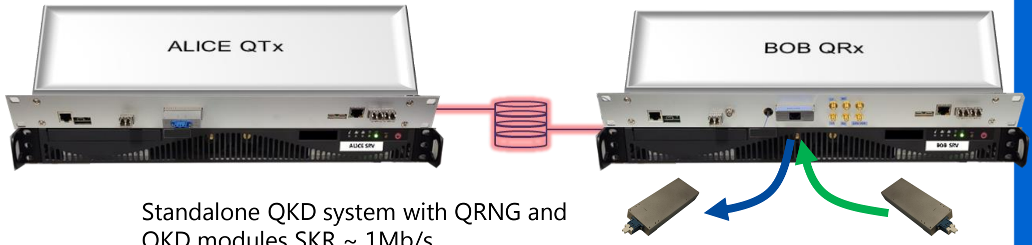
Interface with
100 G encryptors
via standard KMS



QKD Transmitter Module
Half-wave voltage < 1 V

High rate QRNG module: bit rate > 4 Gb/s

QKD receiver module:
Interference stability > 24h

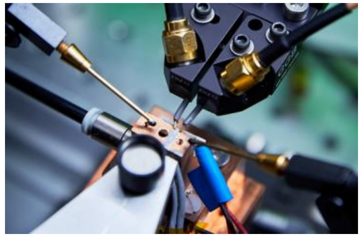


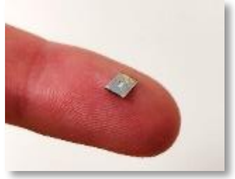
Standalone QKD system with QRNG and
QKD modules SKR ~ 1Mb/s

quantum secure | power efficient | deployable units

From Single Chips to Standalone System: a timeline

Thank you for your attention.
Questions?



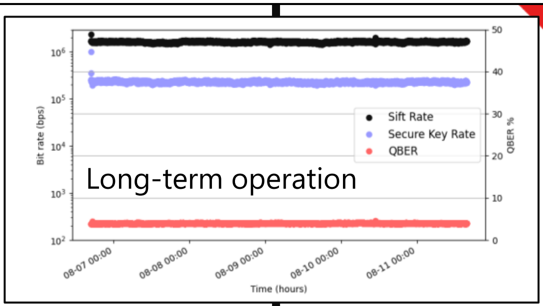


Single Photonic Chips

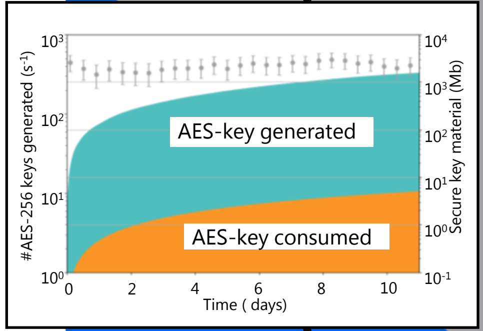
Individual chips

QKD Transmitter
Pluggable module
QRNG module

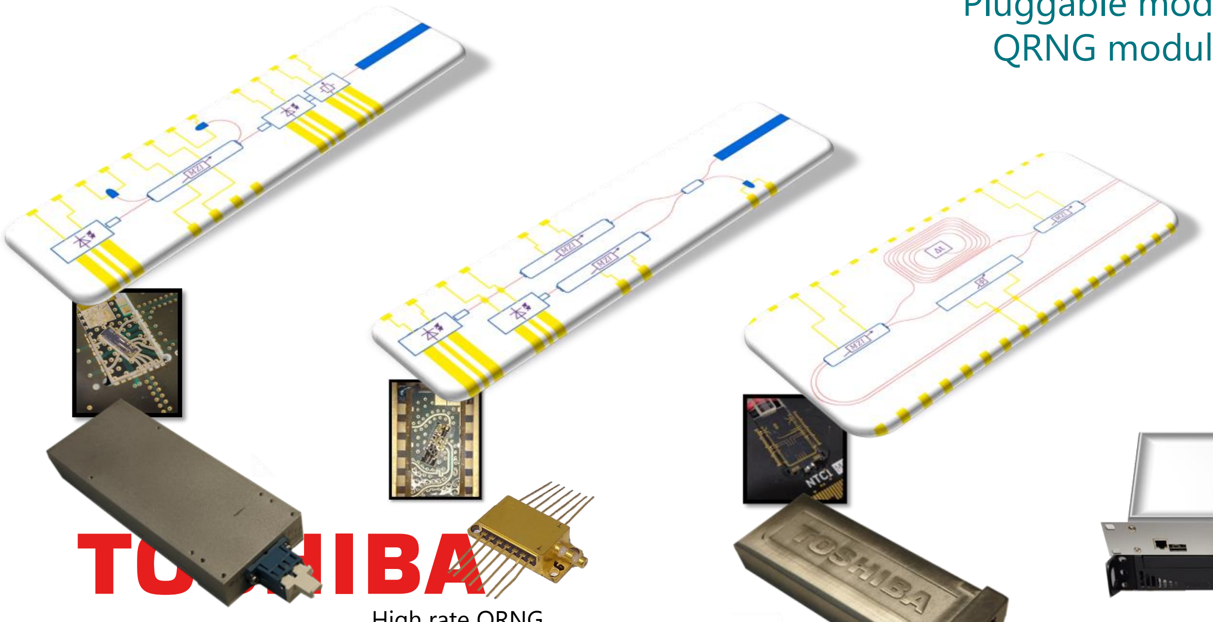
QKD Receiver
Pluggable module



Photonic integrated
QKD system



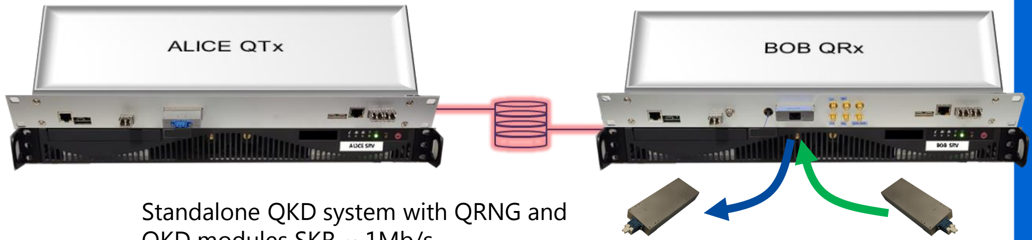
Interface with
100 G encryptors
via standard KMS



QKD Transmitter Module
Half-wave voltage < 1 V

High rate QRNG module: bit rate > 4 Gb/s

QKD receiver module:
Interference stability > 24h



Standalone QKD system with QRNG and QKD modules SKR ~ 1Mb/s

quantum secure — power efficient — deployable units