Compact and Scalable Quantum Key Distribution Devices

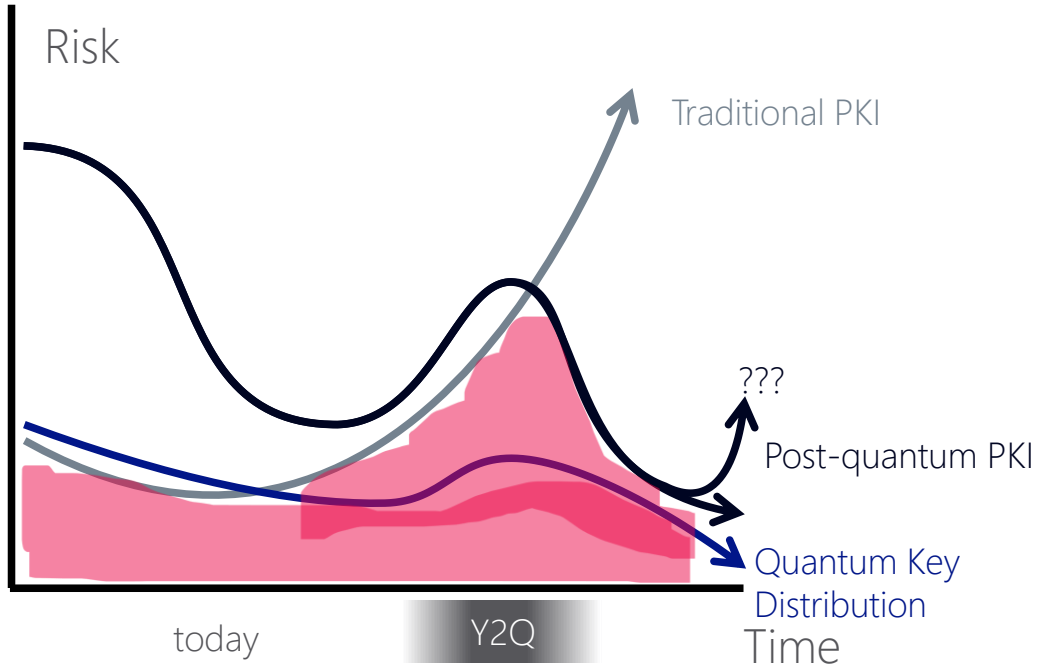
A Quantum Austria project

Daniel Spitzbart, Nutshell Quantum-Safe / IDQ

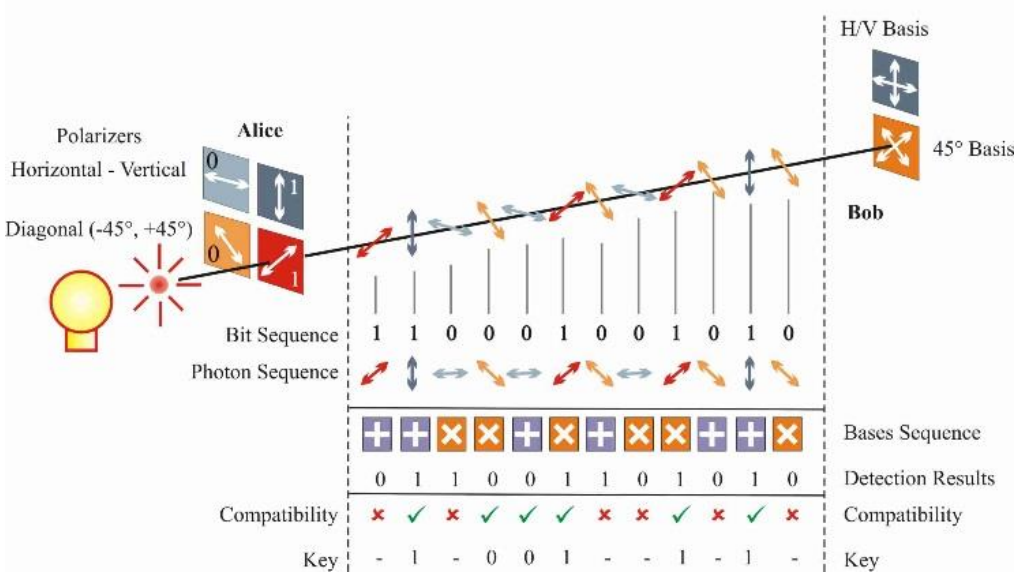
05-03-2025

Why Quantum Key Distribution?

- QKD is one way to provide quantum-safe communication
  - Upcoming quantum computers towards 2030 (?) will break traditional encryption
- Post-Quantum Cryptography still relatively new field with associated risks (e.g. SIKE algorithm)
- Well established (and provably secure) QKD protocols, e.g. BB84
  - Reliable, national security certified QKD systems available on the market
  - Threat of "Harvest now – decrypt later" is already present



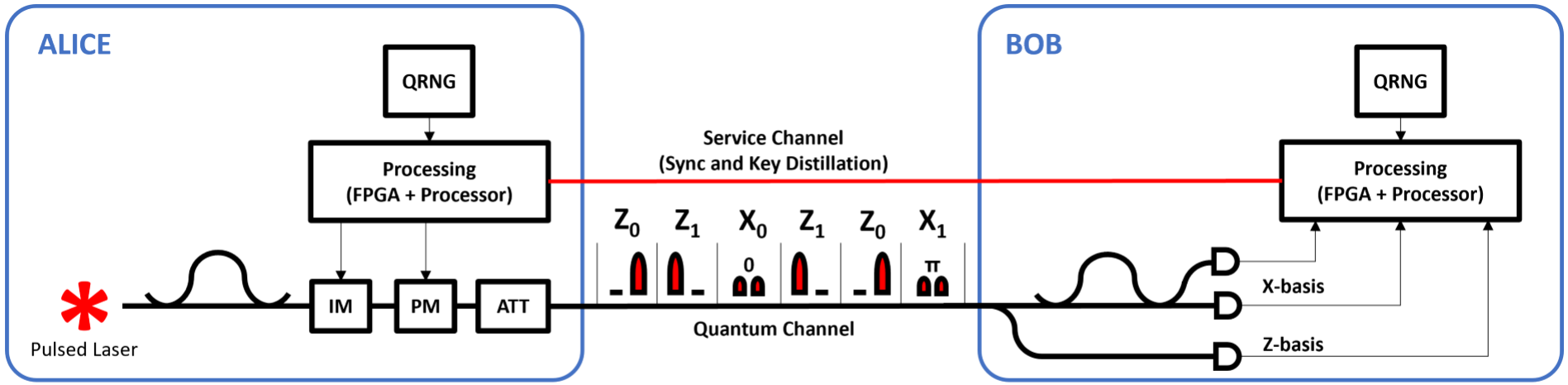
BB84 QKD with polarization states



Preparation: Alice creates a random bit (0 or 1) and then randomly selects one of two bases (+ or ×) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis

Measurement: Bob randomly chooses to measure either in the + basis or in the × basis

Time bin: two time slots, early/late



What is CompaQt?

- Consortium between NQS (IDQ), AIT, SAL and HHI; collaboration started 1/2023
- Develop “Compact and Scalable QKD Devices”: Miniaturize both optics and electronics
- Key innovations: integrated photonic and electric circuits for QKD receiver and transmitter

nutshell quantum-safe

AUSTRIAN INSTITUTE OF TECHNOLOGY

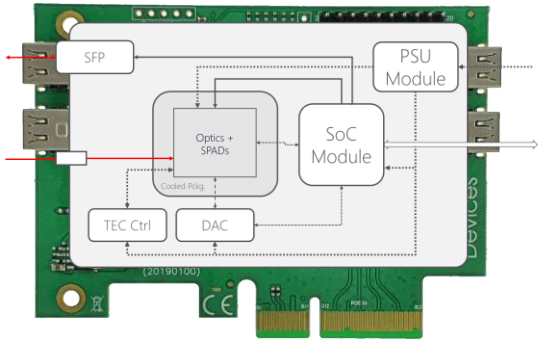
SAL SILICON AUSTRIA LABS

Fraunhofer HHI

19” rack system (state-of-the-art)

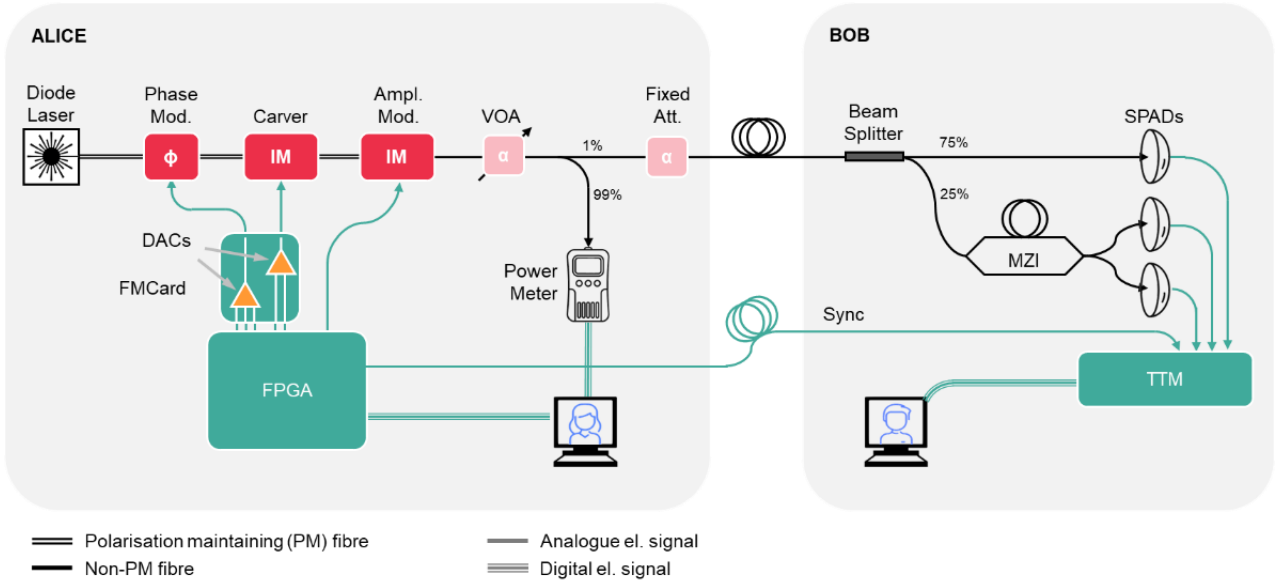
PCIe card

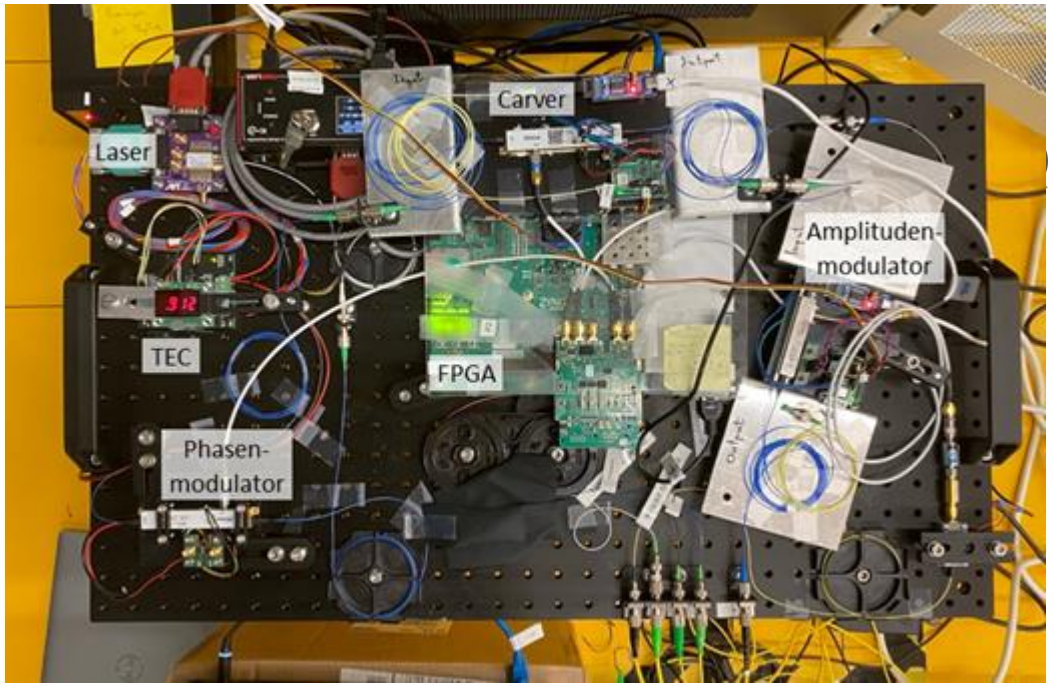
CFP/SFP

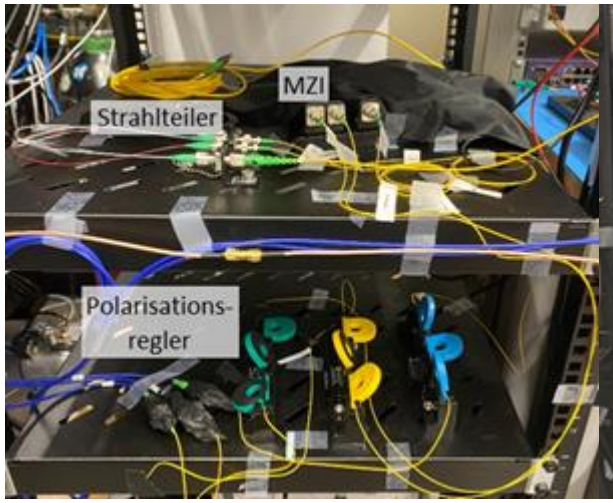


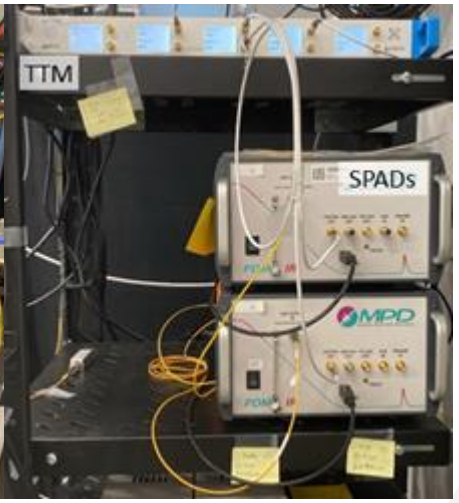
QKD Lab System

- Starting point of the project: QKD lab system at AIT
  - Time-bin BB84 decoy state system
  - Built from off-the-shelve bulk components, with custom drivers, hard- and software
  - Used as reference before replacement IC components become available
- Fiber test track from AIT to Uni Wien with 15dB → 1.4 kbps secure key rate



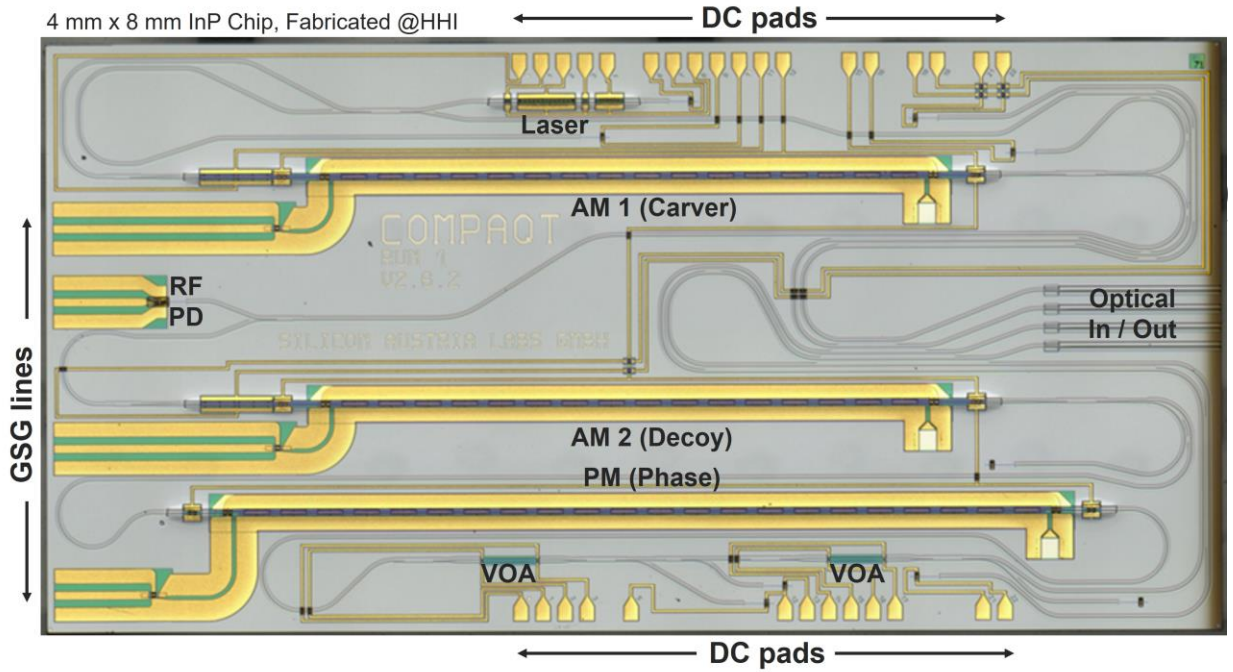


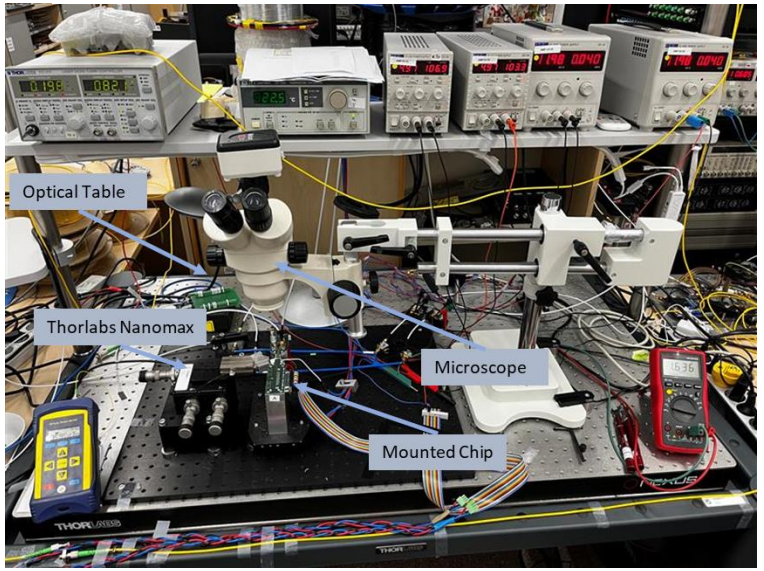


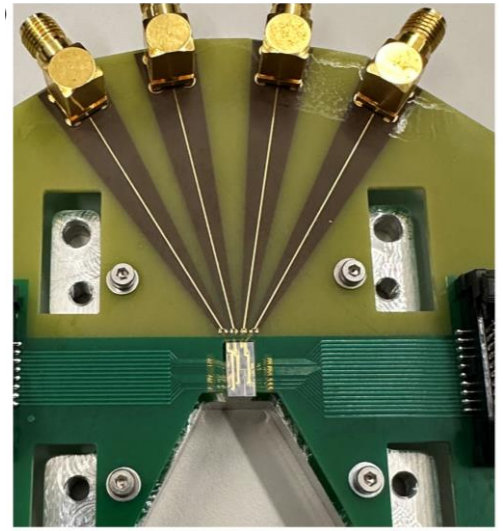


Alice: Transmitter Optics on a Chip

- Responsible for generating quantum level signals
  - Custom driver electronics developed by AIT
- Laser, modulators and attenuators on 4x8mm2 chip
- 1550nm (C-band) based on Indium Phosphide TX-RX platform
- Designed by SAL, fabricated at Fraunhofer HHI
- Characterization of first version of the chip ongoing at AIT
  - Laser, DC bias and HF signals, attenuators
- Lithium Niobate on Insulator (LNOI) platform under development

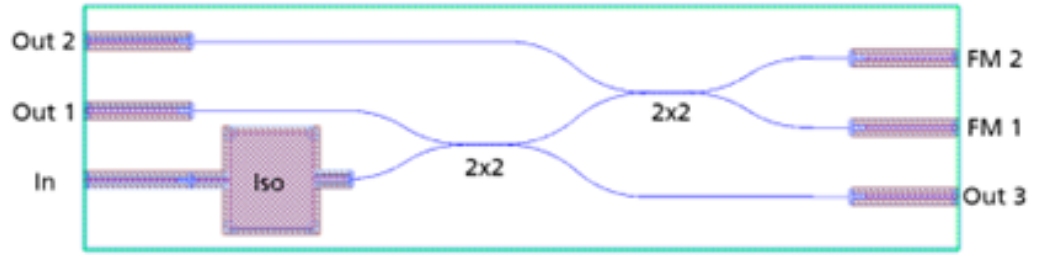


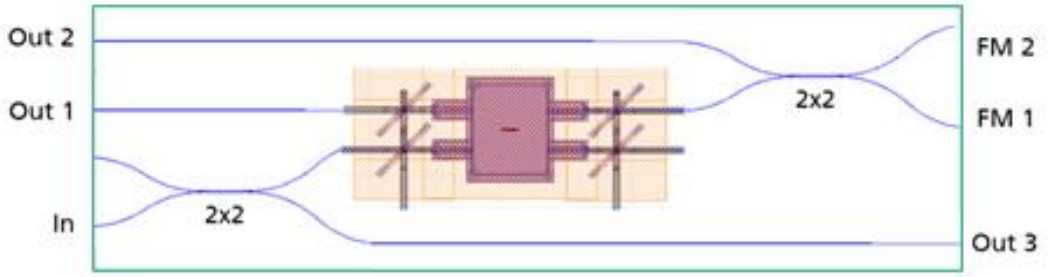


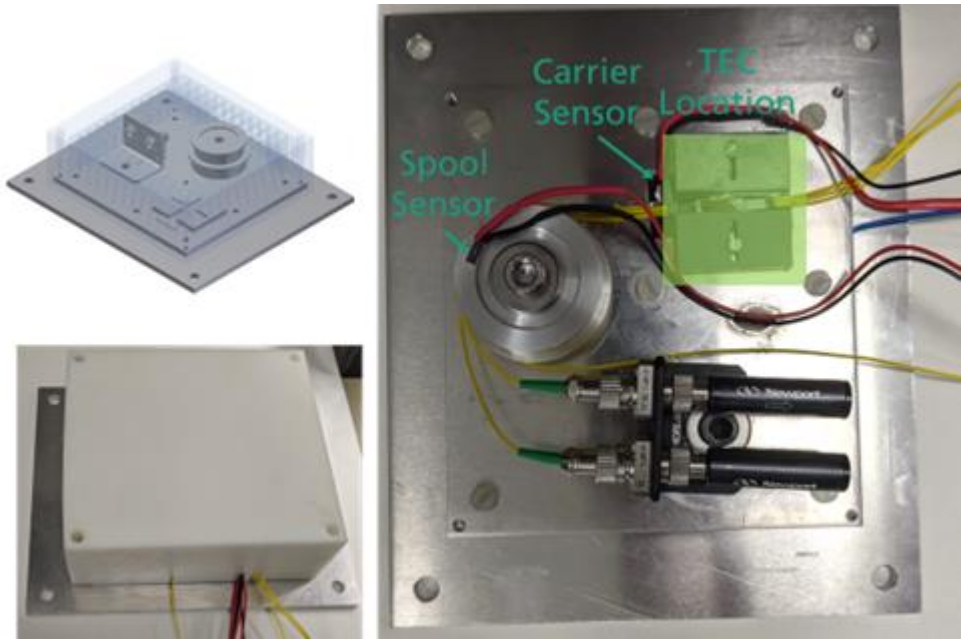


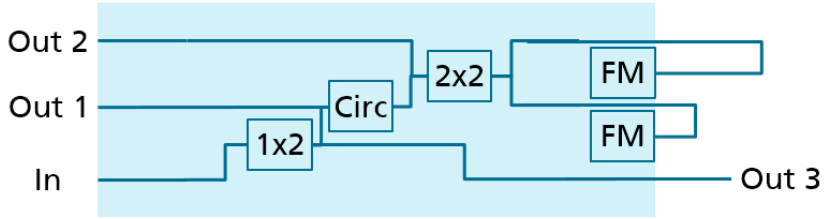
Bob: Receiver Optics on a Chip

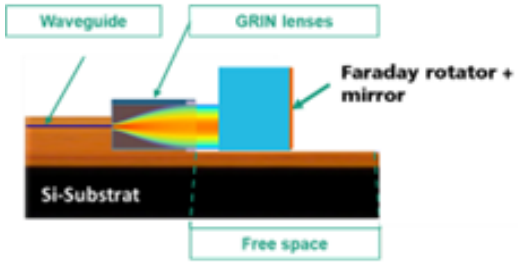
- Two generations of receiver chips have been developed
  - Delay-line interferometer uses Faraday mirrors (FM)
  - Reduced losses thanks to integrated optical circulator based on polarizing beam splitter and optical bench with Faraday rotator
- Inclusion of FM in interferometer arms on chip for full integration as last step
  - GRIN lenses made from graded fibers
  - Integration into HHI polyboard micro-optical bench





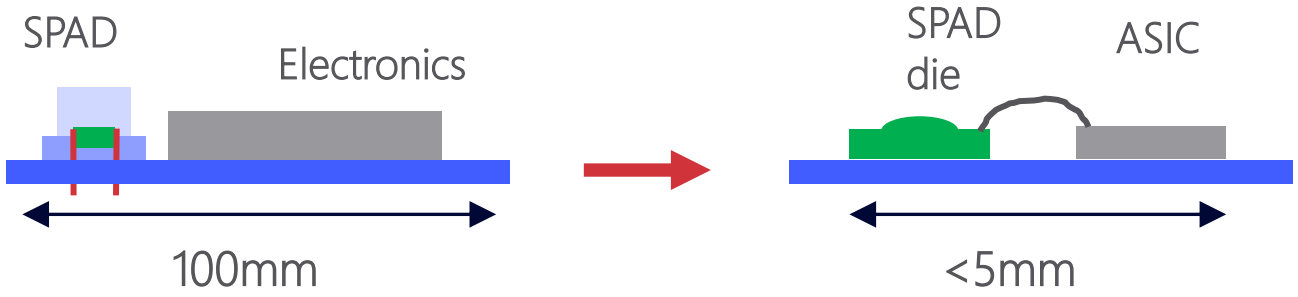


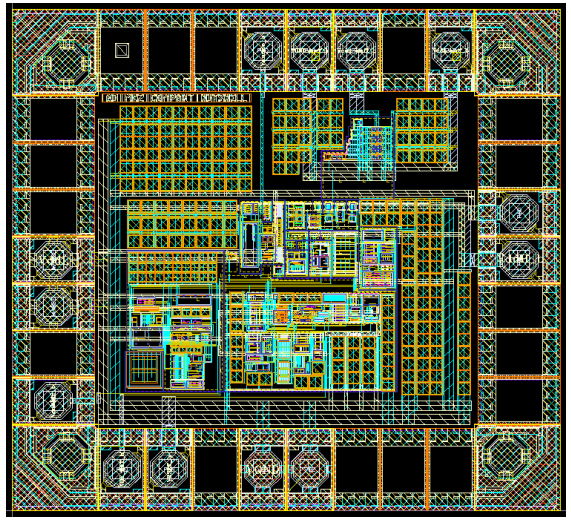




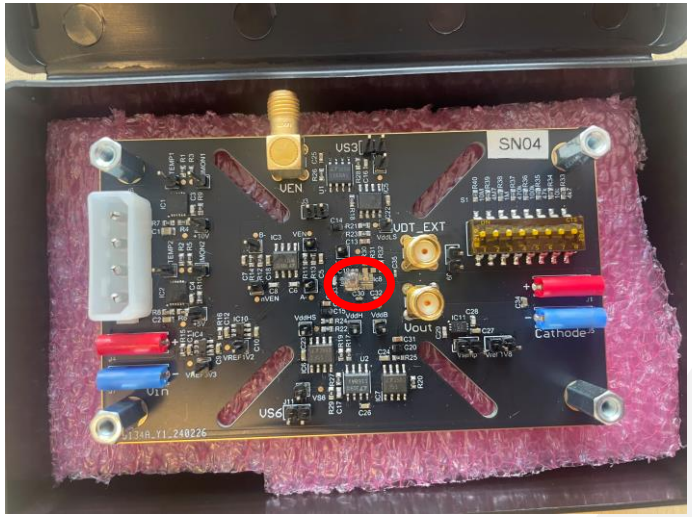
Bob: Single photon detector readout ASIC

- Single photon avalanche diodes need to get quenched after each signal
- Faster quenching requires smallest possible capacitance of system to detect avalanche early
- Goal: IC for active quenching in SPAD free running mode
- Integrated circuit with direct wire bond between SPAD and ASIC
- 1.4 x 1.28 mm2 footprint of ASIC, includes dead time adjustment for optimal performance
- Use established X-Fab XH035 (350nm) technology
- Quenching times below 1ns achieved (voltage swing of anode ~500ps for 6.6V)





ASIC layout



ASIC + SPAD test board

Status and Outlook

- First prototypes of integrated electronics and optics have been fabricated
  - Test results look very promising
  - Feedback is being incorporated in design of second (final) prototypes

- Consortium is confident in successfully completing a QKD lab system using developed components at TRL 4