Proof-of-principle demonstration of QKD immune to detector attacks

A. Rubenok, J.A. Slater, P. Chan, I. Lucio Martinez, and W. Tittel

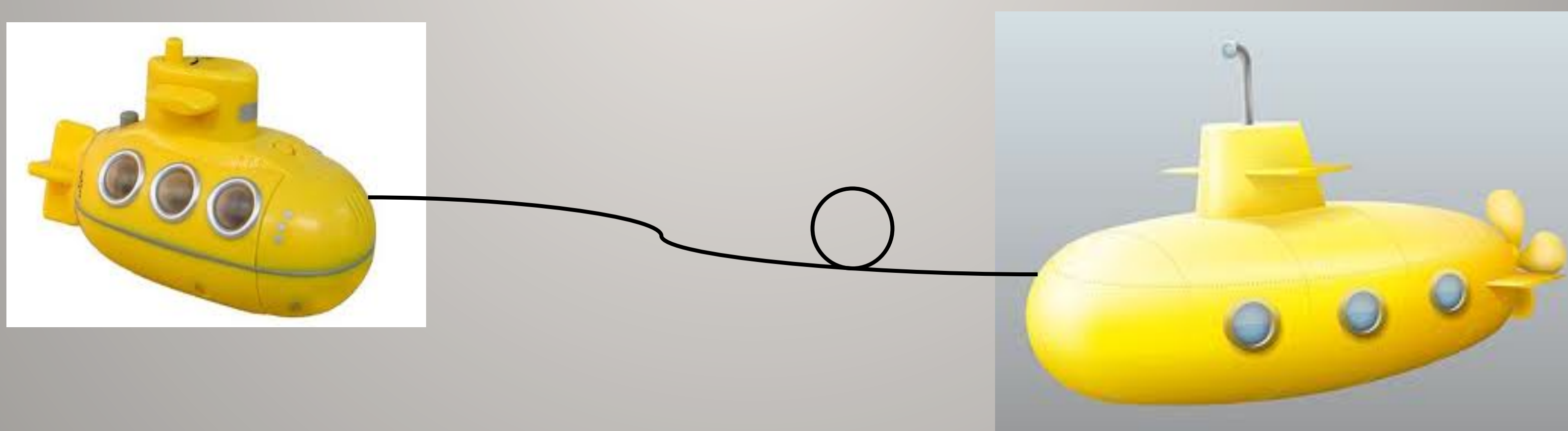
Institute for Quantum Information Science, University of Calgary, Canada

Proof-of-principle demonstration of QKD immune to detector attacks

in the maritime environment

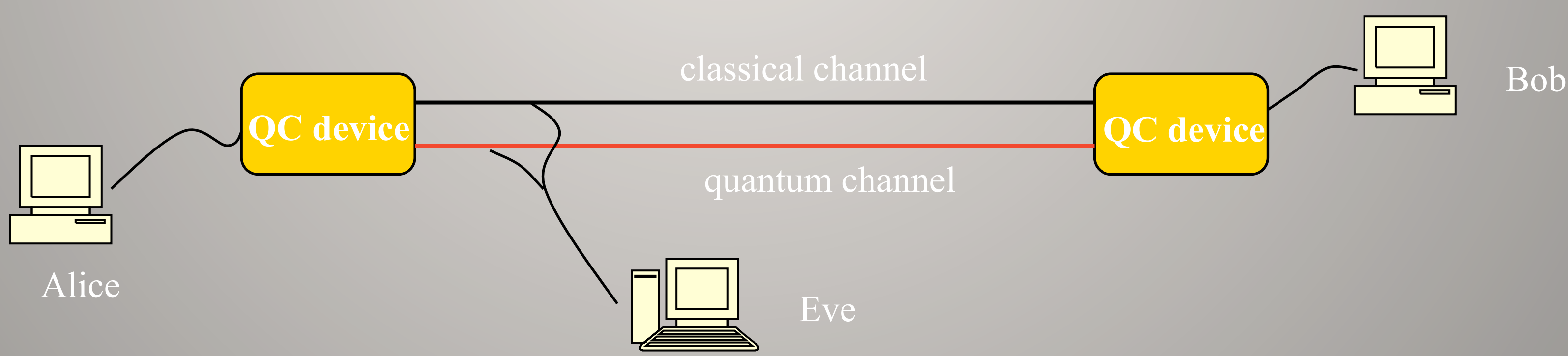
A. Rubenok, J.A. Slater, P. Chan, I. Lucio Martinez, and W. Tittel

Institute for Quantum Information Science, University of Calgary, Canada



Quantum key distribution

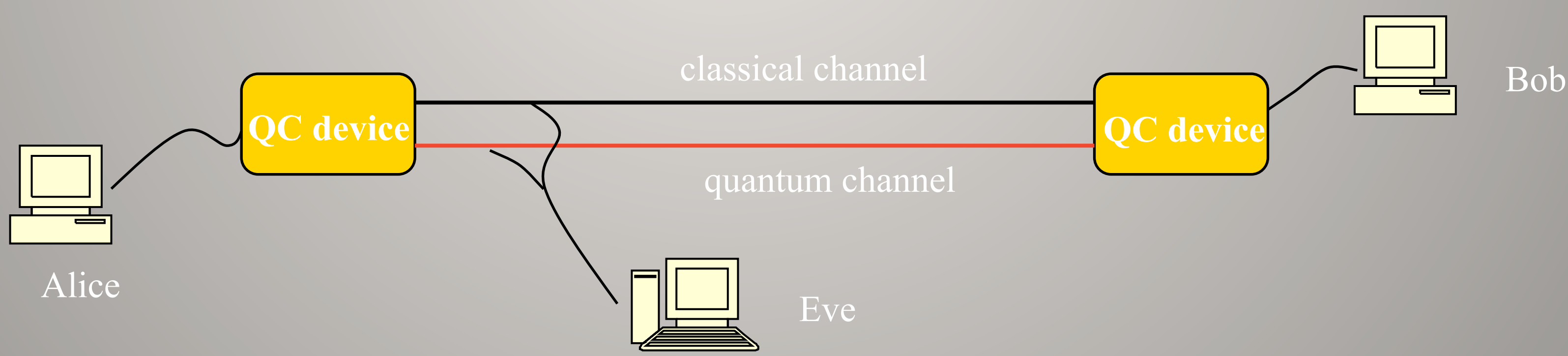
- Information-theoretic security proven (even assuming imperfect devices)
- Impressive experimental progress since 1989
    - more than 100 km distance (fiber and free-space)
    - trusted-node networks (BBN-DARPA, SECOQC, Tokio, Swiss)
    - commercial devices (idQuantique, MagiQ)



Quantum key distribution

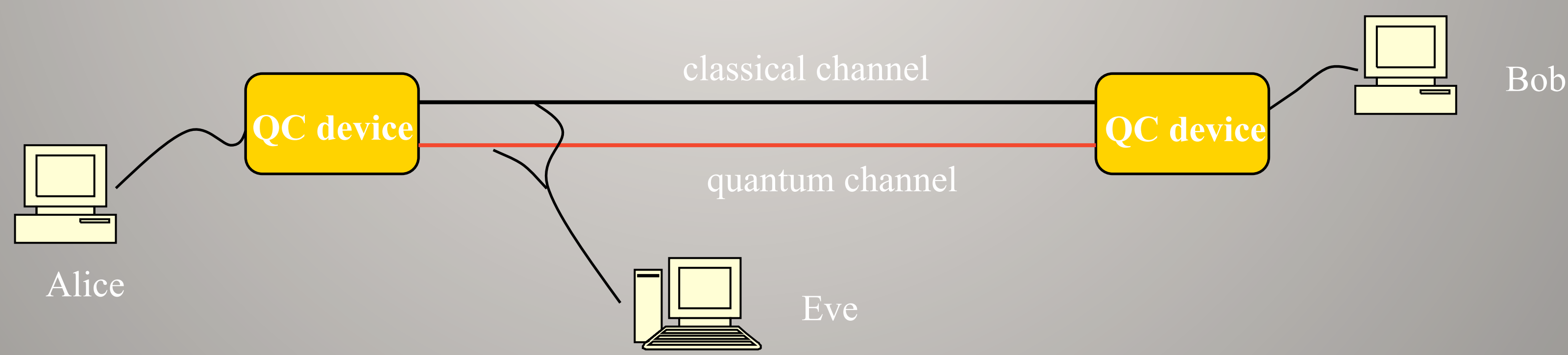
- Information-theoretic security proven (even assuming imperfect devices)
- Impressive experimental progress since 1989
    - more than 100 km distance (fiber and free-space)
    - trusted-node networks (BBN-DARPA, SECOQC, Tokio, …)
    - commercial devices (idQuantique, MagiQ)

BUT



Outline

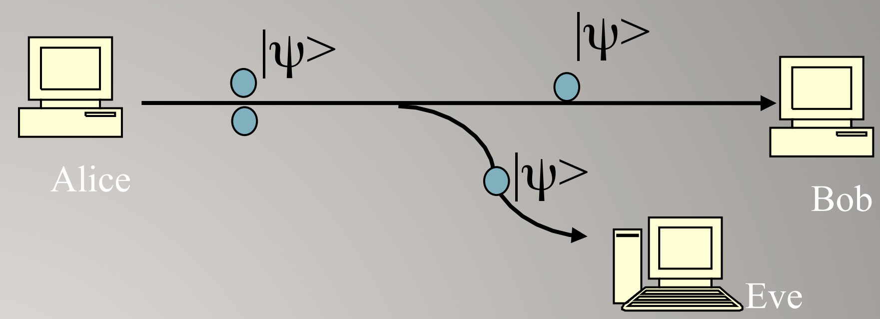
- Side-channel attacks
- Measurement-device independent (MDI) QKD
    - the protocol
    - proof-of-principle demonstration
- Conclusion



Side-channel attacks

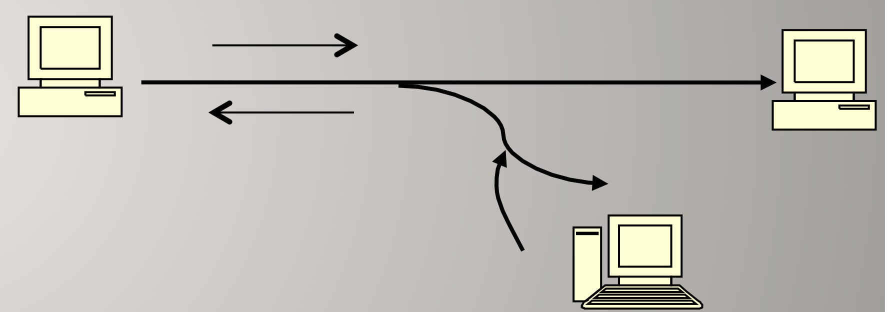
- **Photon number splitting**

  Counter measure: decoy state protocol



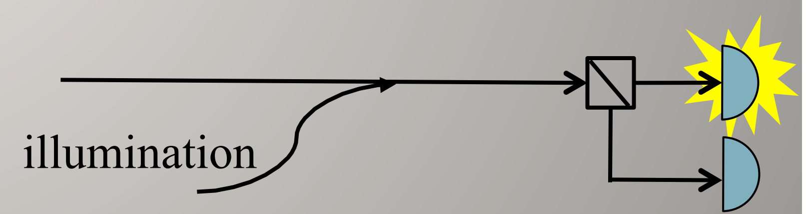
- **Trojan Horse attacks**

  Counter measure: optical isolator



- **Remote controlling detectors**

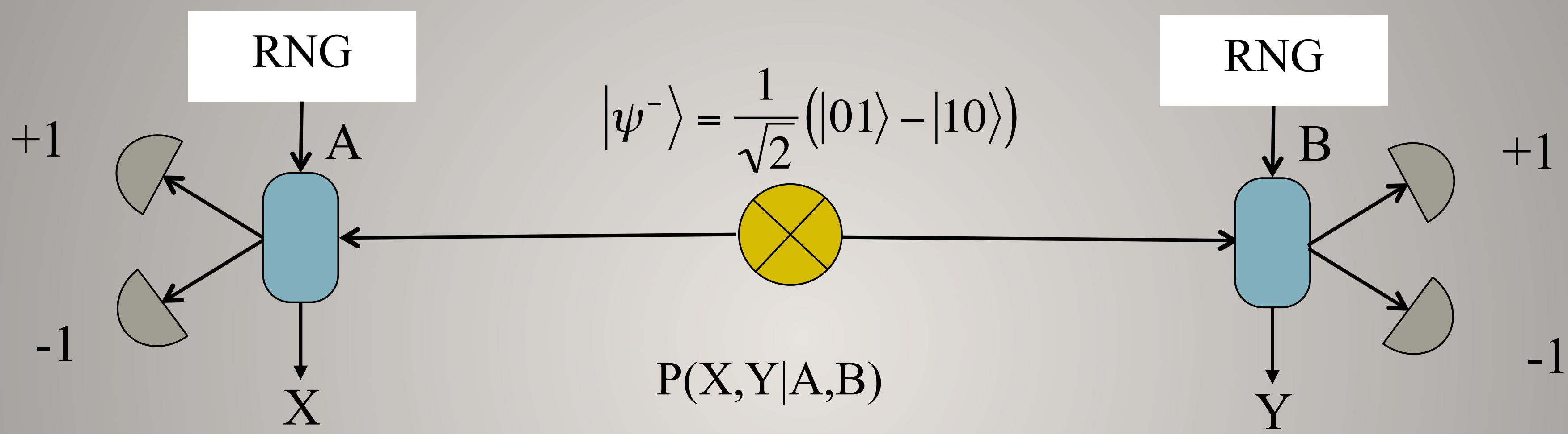
  Counter measure: robust detectors



Can we devise (& implement) a protocol that is robust wrt to <u>any side-channel attack</u> (known or yet-to-be discovered)??

Brassard *et al*, PRL 85, 1330 (2002); Gisin et al, PRA 73, 022320 (2006), Lydersen, Nature Phot. **4**, 686 (2010)

Device independent QKD



- requires generation of entangled photons, and projections onto qubit states

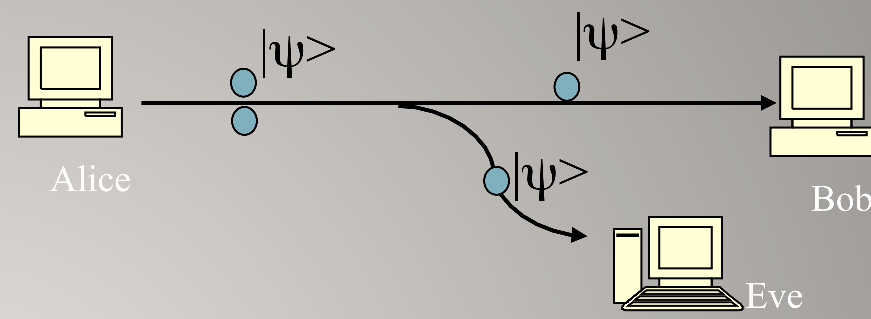
- sifting, error correction and privacy amplification allows distributing secret keys

- currently infeasible (detection loophole needs to be closed)

Side-channel attacks

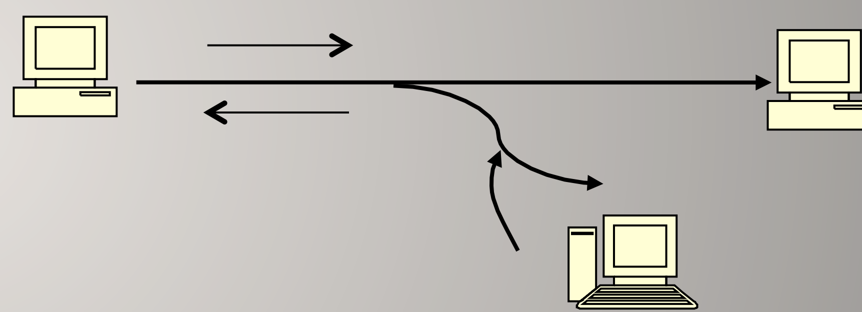
- Photon number splitting

Counter measure: decoy state protocol



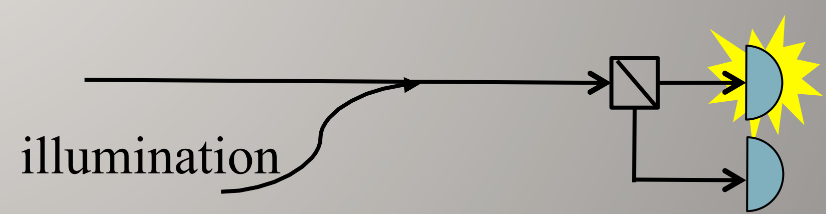
- Trojan Horse attacks

Counter measure: optical isolator



- remote controlling detectors

Counter measure: robust detectors



Can we devise (& implement) a protocol that is robust wrt to <u>any detector attacks</u>?

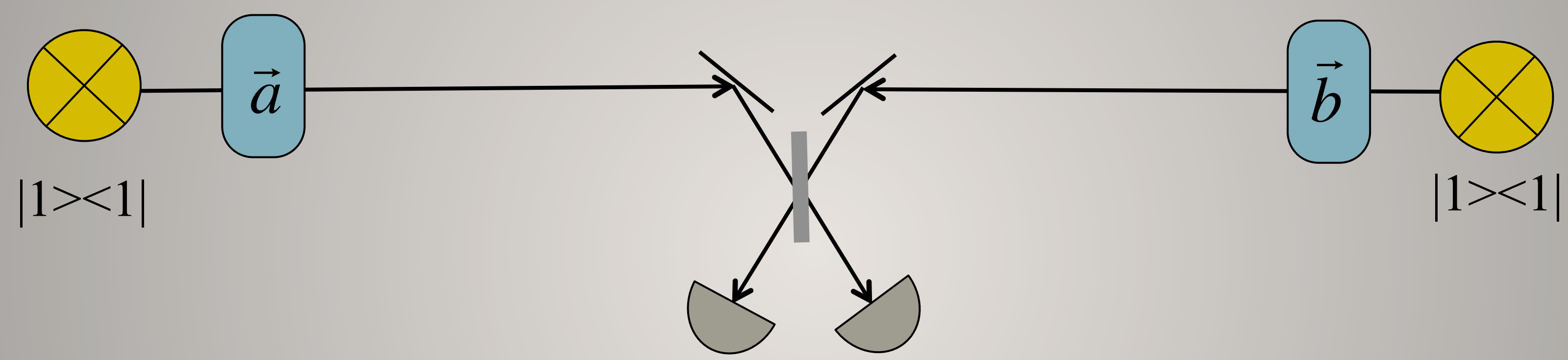
(known or yet-to-be discovered)??

Brassard *et al*, PRL 85, 1330 (2002); Gisin et al, PRA 73, 022320 (2006), Lydersen, Nature Phot. **4**, 686 (2010)

QKD using time-reversed entanglement

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right)$$

$\vec{\alpha}, \vec{\beta} \in [|0>, |1>, |+>, |->]$



- requires generation of qubit states, and projection onto entangled states

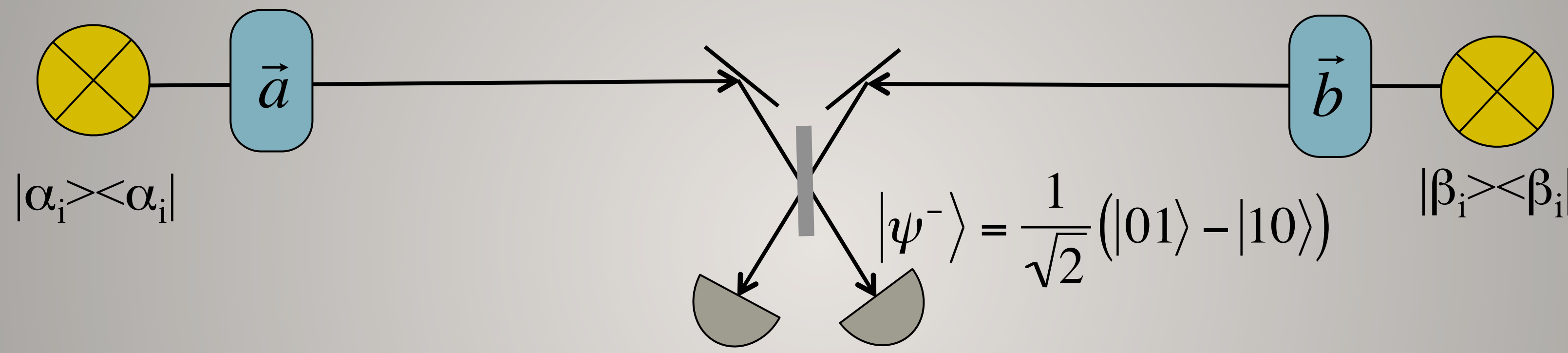
- sifting (*x-key*, *z-key*), bit flip at Bob's, EC and PA allows distributing secret keys

- de-correlates detection pattern from key bit -> immune to any detector attack

- currently difficult to implement (single photon sources)

Measurement Device Independent - QKD

$\vec{\alpha}, \vec{\beta} \in [|0\rangle, |1\rangle, |+\rangle, |-\rangle]$



- requires generation of qubit (signal&decoy) states and proj. onto entangled states

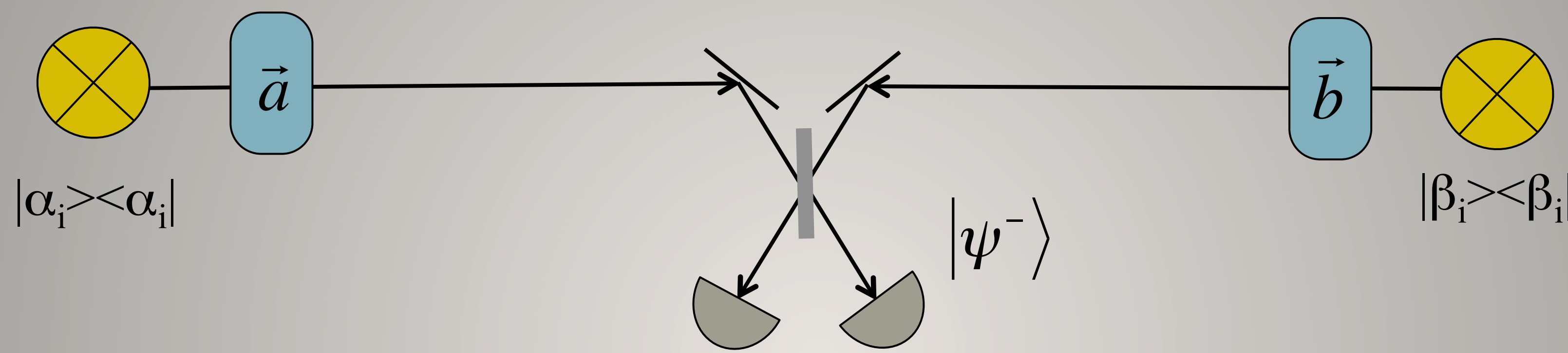
- sifting (*x-key, z-key*), bit flip at Bob's, EC and PA allows distributing secret keys

- de-correlates detection pattern from key bit -> immune to any detector attack

- should be feasible with existing technology

Lo et al. PRL **108**, 130503 (2012) (see also Braunstein et al, PRL 108, 130502 (2012)).

Decoy states in MDI-QKD



- allows overcoming threat of PNS attacks

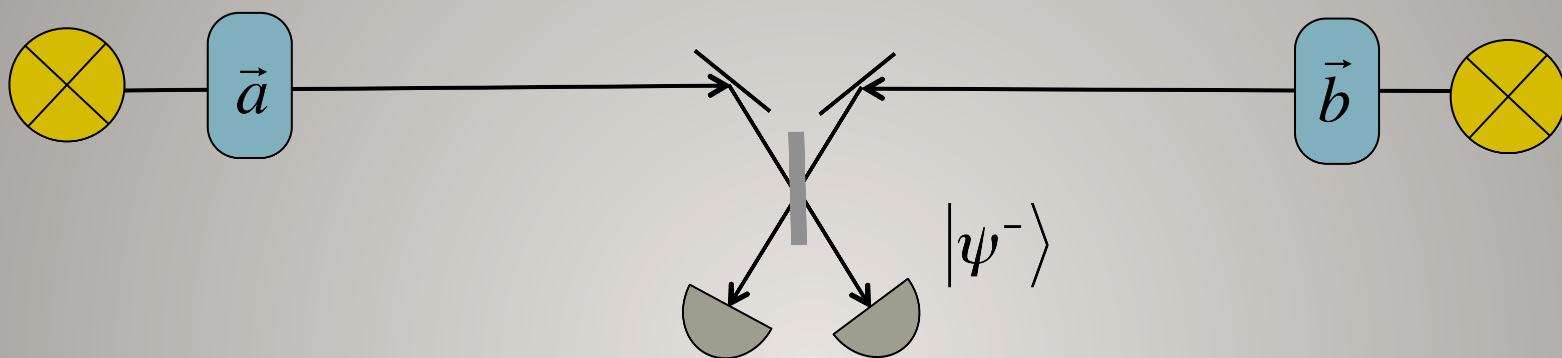
- random variation between 3 different mean numbers of photons per qubit carrier allows assessing Q^x_{11}, Q^z_{11}, e^x_{11}, and e^z_{11} ($\rho=\Sigma P(n)|n\rangle\langle n|$)

- secret key is distilled from *z-key* (using *x-key to* assess I(A;E))

$Q^z_\mu := Q^z_{\mu_A \mu_B}$

$$R = Q^z_{11} \{1 - h_2(e^x_{11})\} - Q^z_\mu \, f \, h_2(e^z_\mu)$$

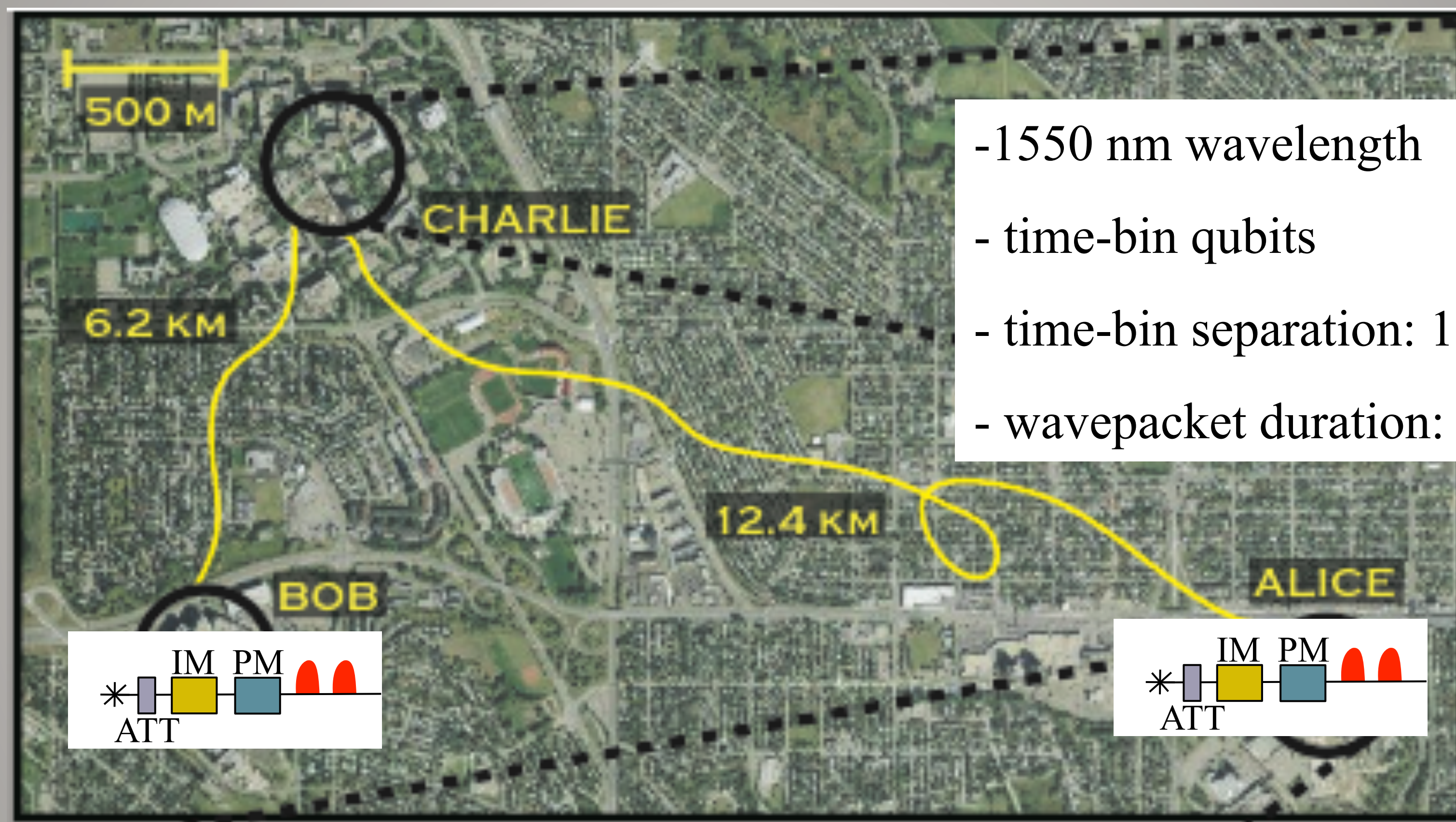
Bell-state measurement



- requires indistinguishable photons
    - spatial mode
    - temporal mode
    - spectrum
    - polarization
- needed for MDI-QKD, quantum repeater, quantum networks, LOQC

note: as difficult for attenuated laser pulses as for photons from photon pairs

Generic setup



-1550 nm wavelength

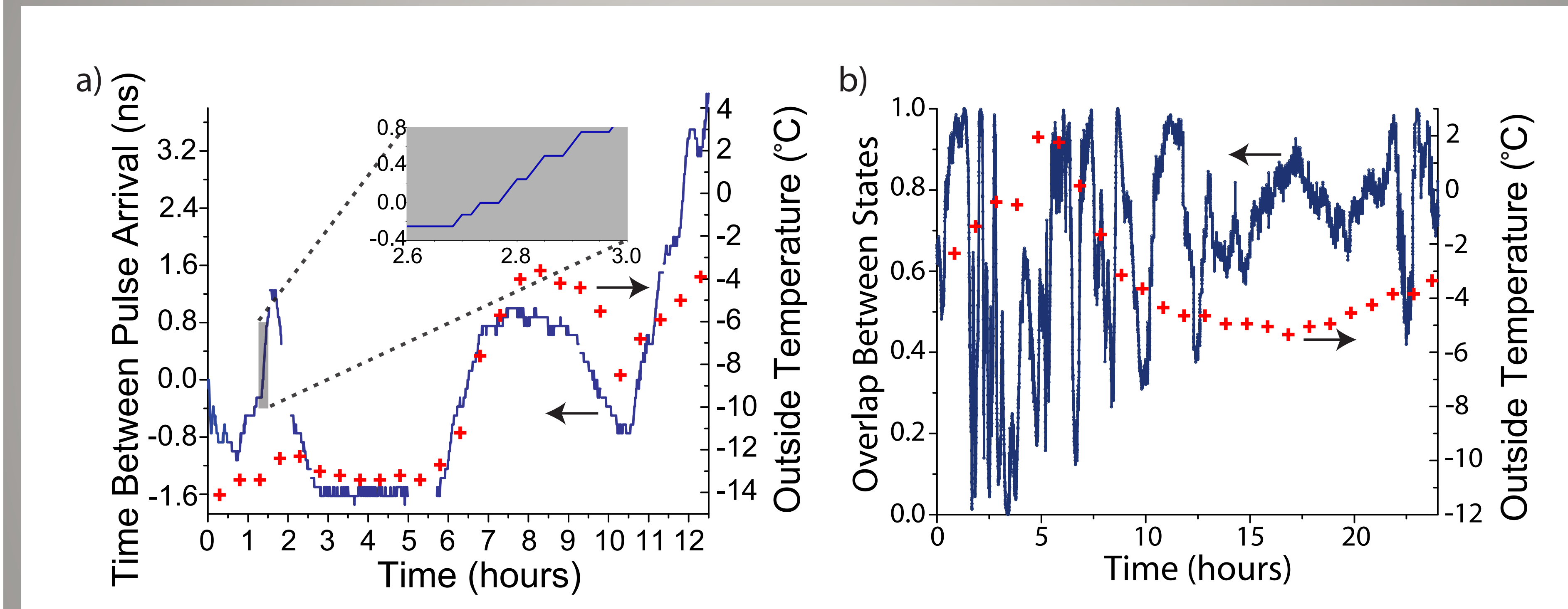
- time-bin qubits

- time-bin separation: 1.4 ns

- wavepacket duration: 500 ps

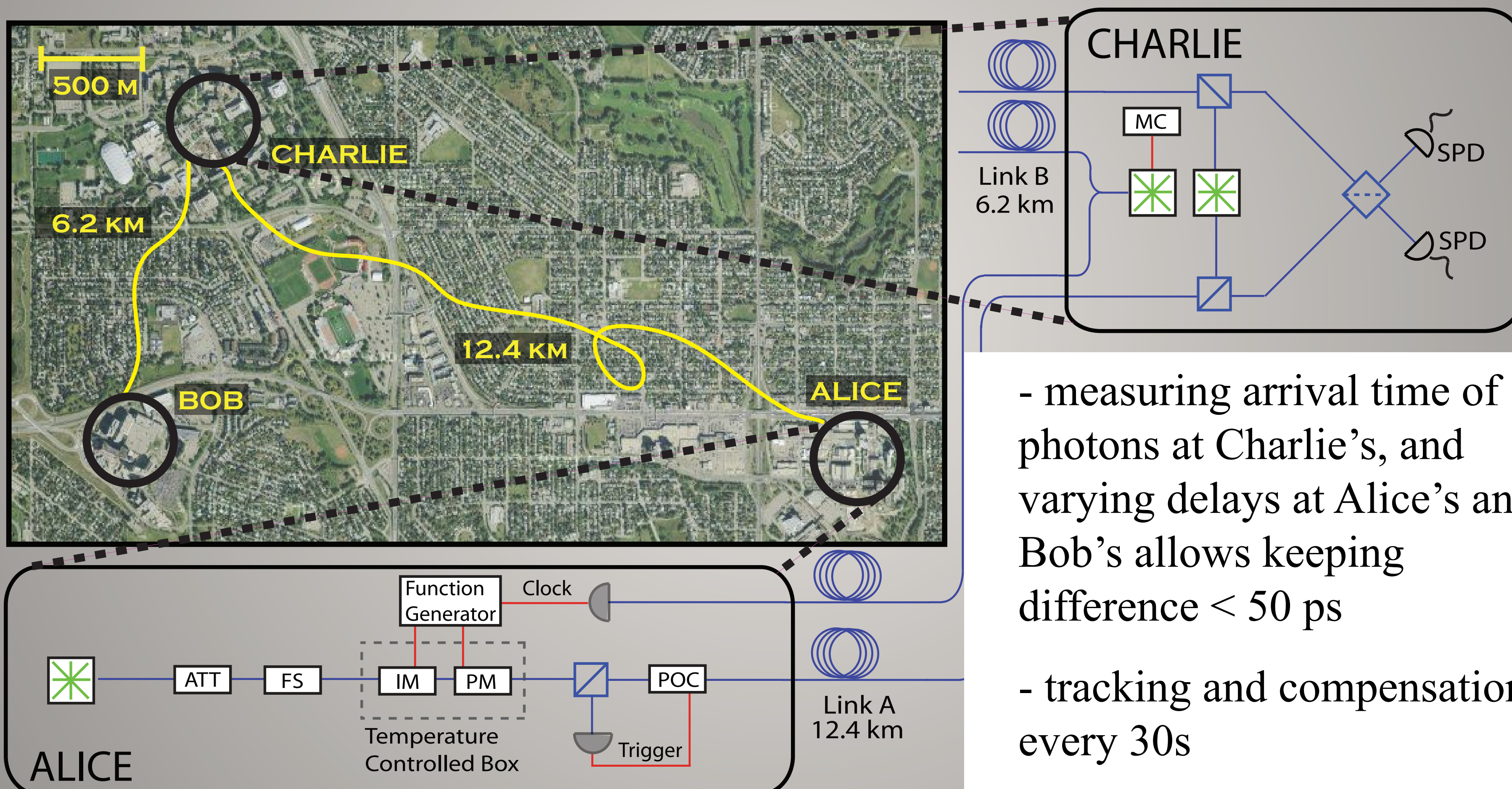
and measurements in the lab with fibre on spools

Environment-induced fluctuations



plus frequency drift of Alice's with respect to Bob's laser of up to 20 MHz/hour

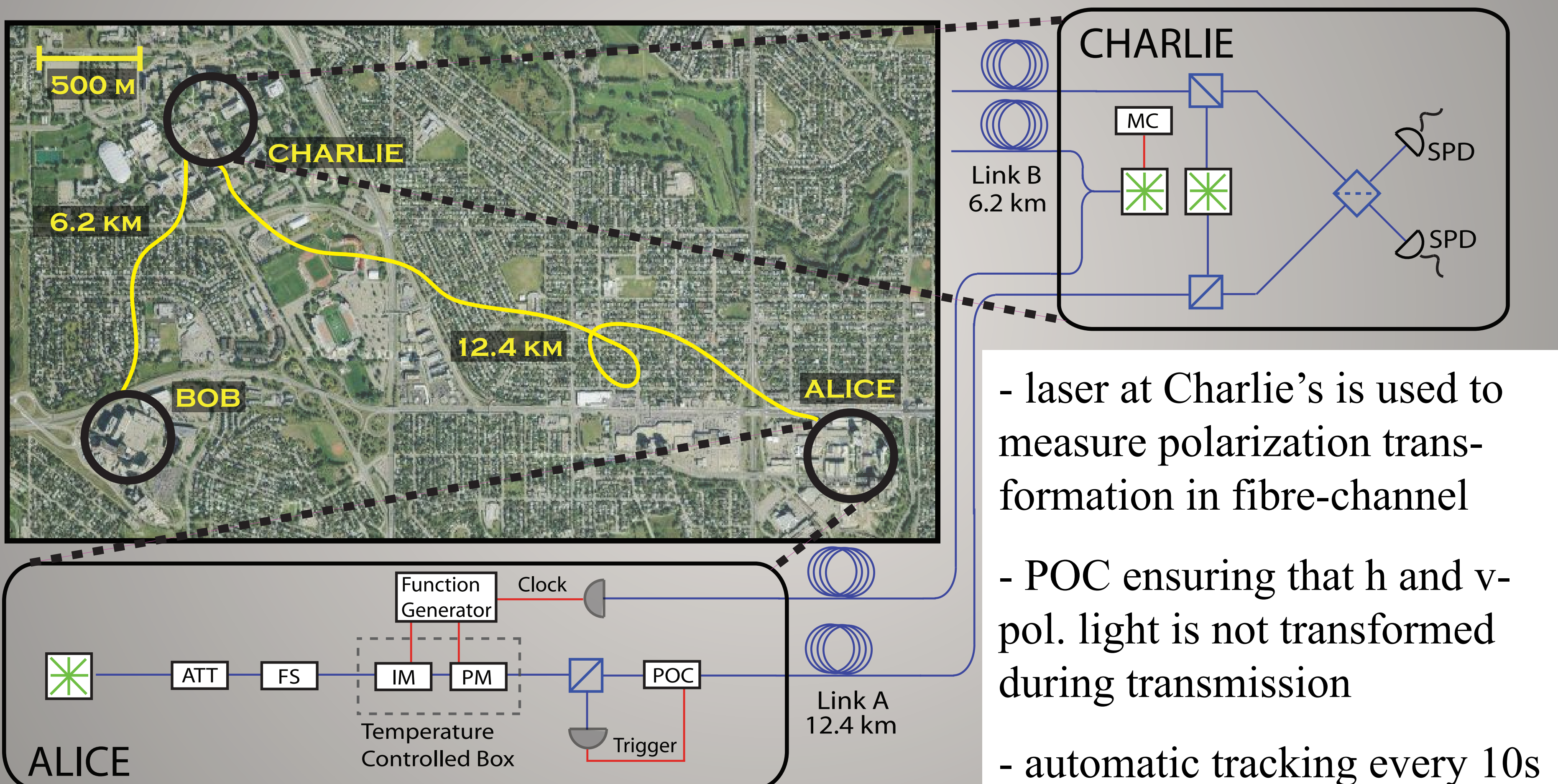
Feedback systems – arrival time



- measuring arrival time of photons at Charlie's, and varying delays at Alice's and Bob's allows keeping difference < 50 ps

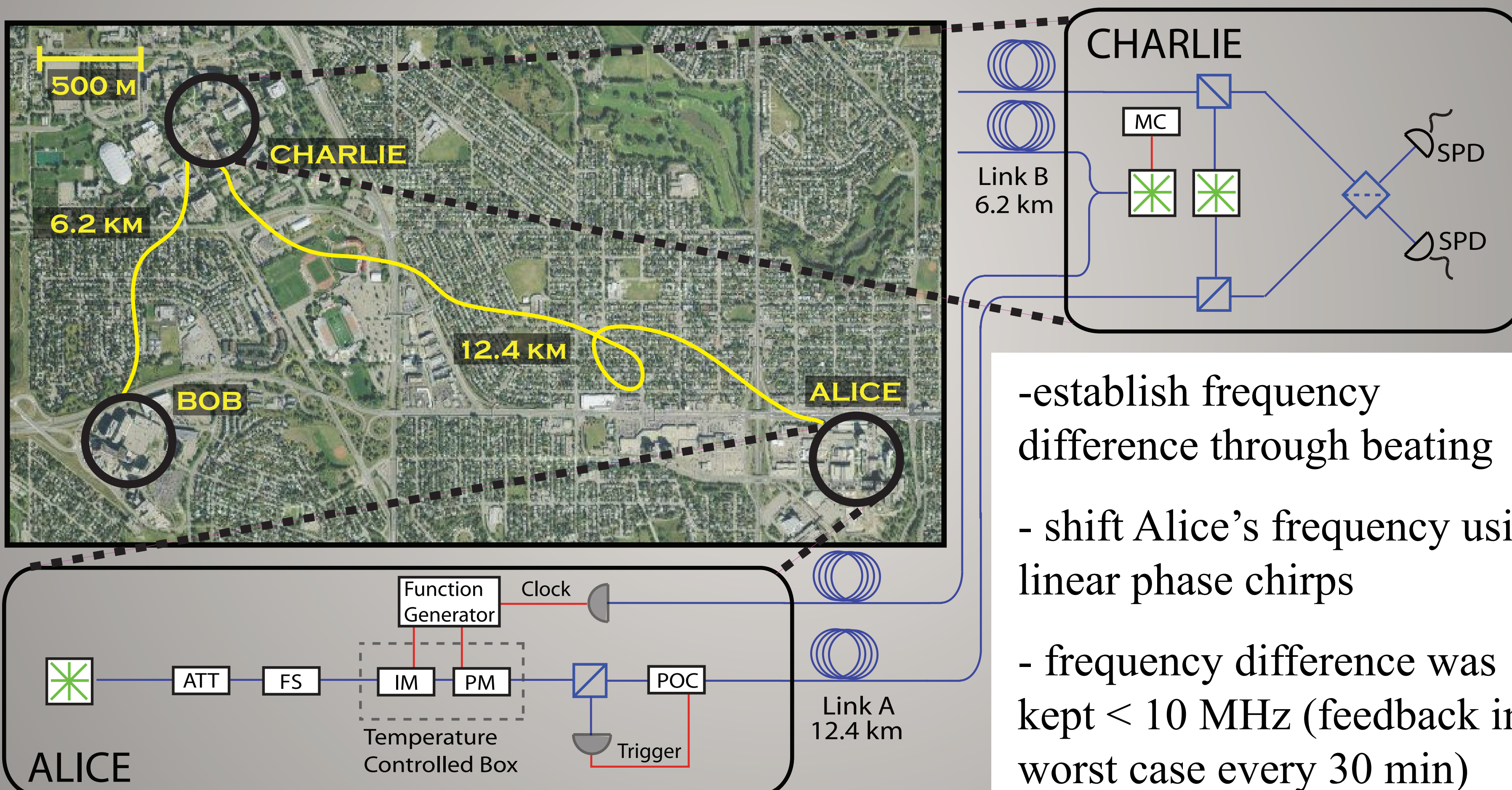
- tracking and compensation every 30s

Feedback systems – polarization



- laser at Charlie's is used to measure polarization transformation in fibre-channel
- POC ensuring that h and v-pol. light is not transformed during transmission
- automatic tracking every 10s

Feedback systems – frequency (spectrum)

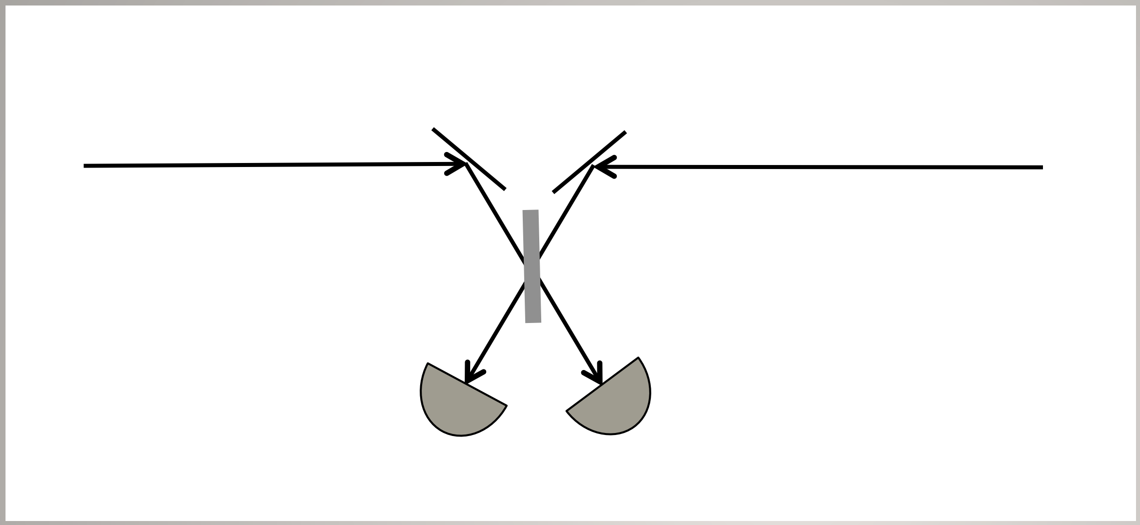


-establish frequency difference through beating

- shift Alice's frequency using linear phase chirps

- frequency difference was kept < 10 MHz (feedback in worst case every 30 min)

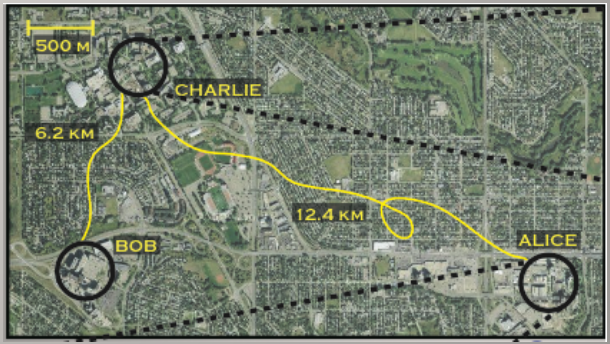
Feedback systems - performance



Indistinguishability assessed via HOM dip:

V_{HOM}=47±1% (V_{max}=50%)

(measurement with classical light is sufficient!)



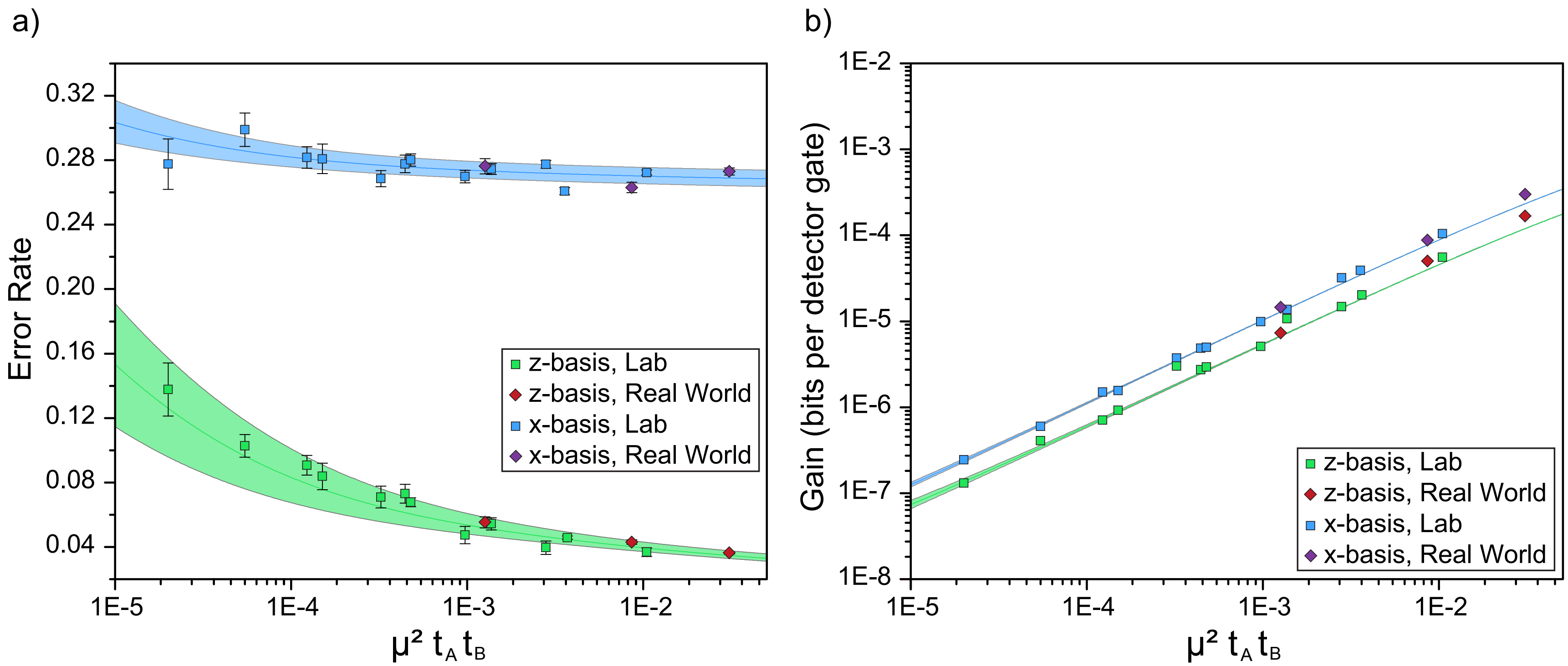
Measurements

- Generate all 8 combinations of states with Alice and Bob using the same basis (x or z)
- $\mu \in [0.1, 0.25, 0.5]$; $\mu_A = \mu_B$
- various distances (loss), inside and outside lab; $l_A = l_B$
- measure error rates and gains

ℓ_A [km]	l_A [dB]	ℓ_B [km]	l_B [dB]	total loss l [dB]
30.98	6.8	11.75	6.8	13.6
40.80	9.1	40.77	9.1	18.2
51.43	11.3	32.19	11.3	22.7
61.15	13.7	42.80	13.6	27.2
12.4	4.5	6.2	4.5	9.0

Real-world measurements

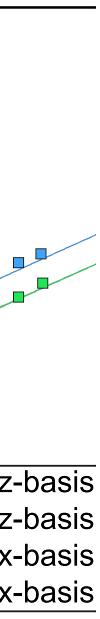
Results

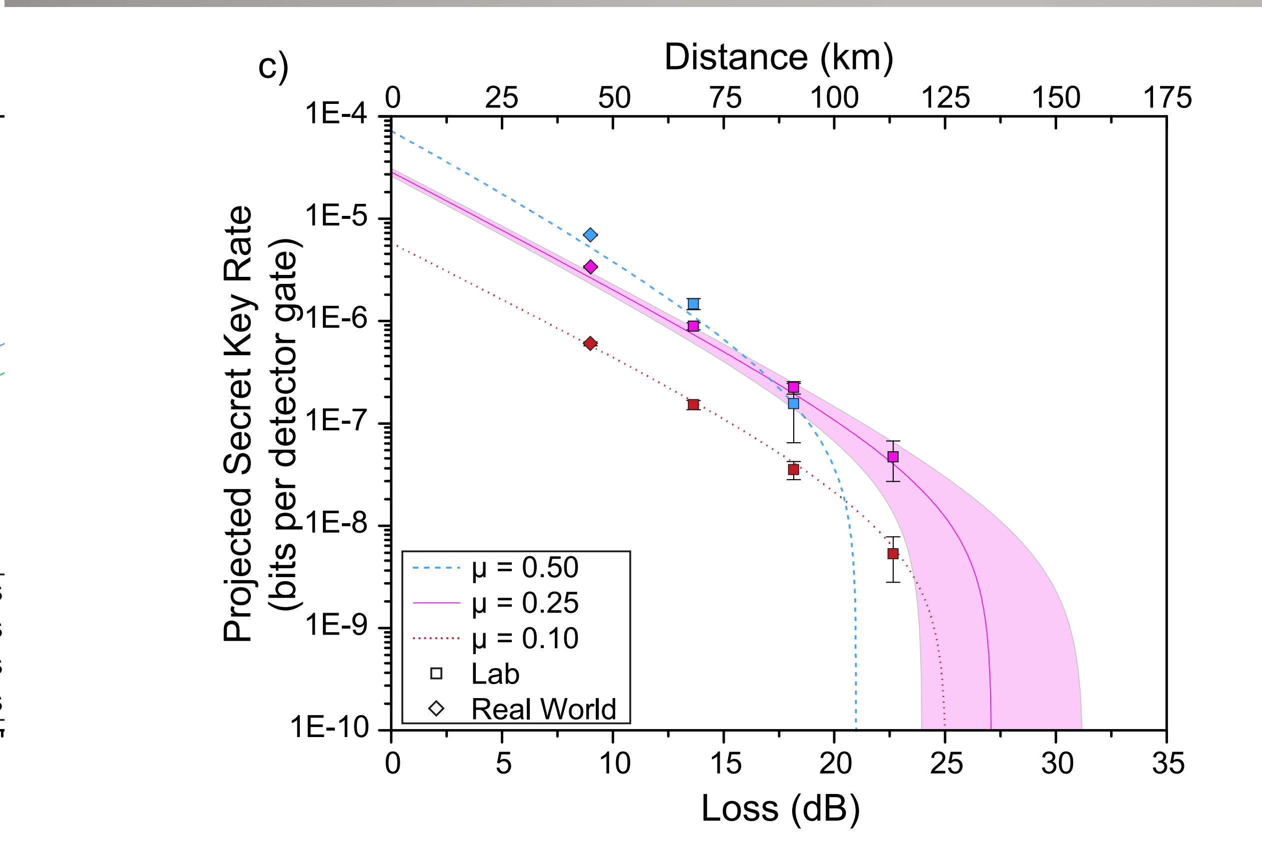


Simulations using independently established parameters and assuming ≤ 2 photons behind BS describe observed error rates and gains over >3 orders of magnitude, and in and out-of lab

-> we understand the imperfections (state preparation, detector noise) that affect the measurable quantities

Results





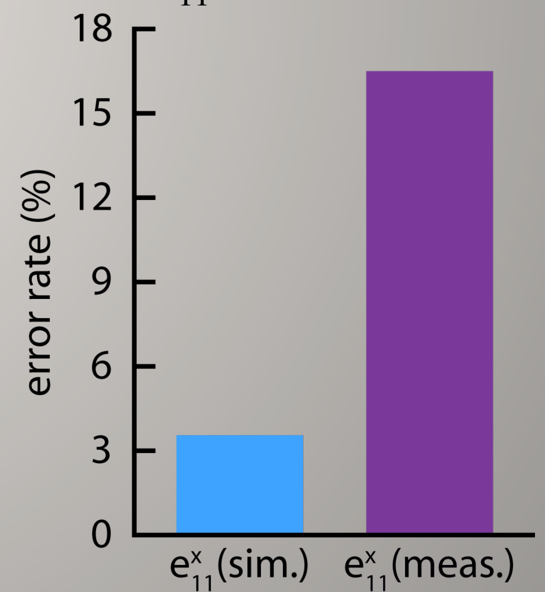
Measured: Q^x_μ, Q^z_μ, e^x_μ, e^z_μ

Estimated: Q^z_{11}, e^x_{11}

- model allows estimating $R= Q^z_{11}\,\{1-h_2(e^x_{11})\} - Q^z_\mu\, h_2(e^z_\mu)$
- but decoy state method needed for actual key distribution
- QKD up to ~125 km assuming efficient decoy state method

More recent results

- 3-value decoy state method has recently been proposed
- requires measuring 7 combinations of different mean photon numbers
- tests over 2x30 km fibre spools yield first results
- discrepancy between simulated and measured e^x_{11} currently large
    - μ_d, μ_s not yet optimized to yield good (upper) bound on e^x_{11}
    - state generation currently not perfect
- work in progress

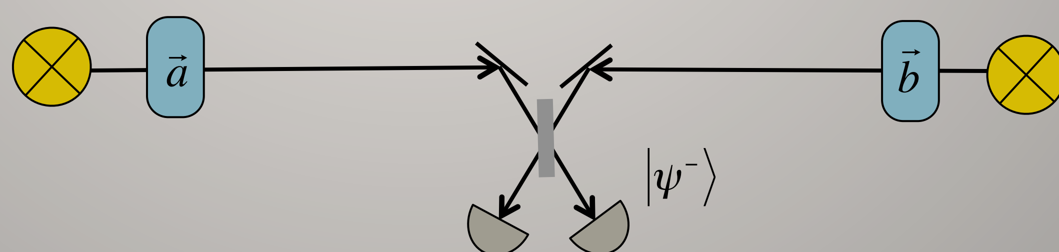


X.-B. Wang, arXiv:1207.0392, similar work by T. Ferreira da Silva et al., arXiv:1207.6345

QC2 Lab

Conclusion

- MDI-QKD protocol removes detector side-channels
- technology is sufficiently mature to implement protocol
- more (straightforward) work require to build complete system
- efficiency of decoy-state protocol can probably be improved
- two-photon interference over real-world optical fibers also removes obstacle for quantum repeaters



PhD and PDF positions available (email to wtittel@ucalgary.ca)

Thank you

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

NSERC
CRSNG

Les Fiducies
Killam
Trusts

Alberta Advanced Education and Technology

GENERAL DYNAMICS
Canada

iCORE

Carlsberg Group