Experimental bit commitment based on quantum communication and special relativity

T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, H. Zbinden

Group of Applied Physics, University of Geneva, Switzerland
Centre for Quantum Technologies, National University of Singapore, Singapore
Centre for Quantum Information and Foundations, University of Cambridge, UK
Perimeter Institute for Theoretical Physics, Waterloo, Canada

August 9, 2013
[arXiv:1306.4801]

Bit commitment – the primitive

Bit commitment – the primitive

Commit phase: Bob commits a bit to Alice.
Open phase: Bob opens his commitment and Alice accepts (or not).

Bit commitment – the primitive

Commit phase: Bob commits a bit to Alice.
Open phase: Bob opens his commitment and Alice accepts (or not).

The protocol should be:

- **correct**: If Alice and Bob are honest then Alice always accepts the opening.

Bit commitment – the primitive

Commit phase: Bob commits a bit to Alice.
Open phase: Bob opens his commitment and Alice accepts (or not).

The protocol should be:

- **correct**: If Alice and Bob are honest then Alice always accepts the opening.
- **binding**: If Alice is honest then there is at most one bit that Bob can successfully open.

Bit commitment – the primitive

Commit phase: Bob commits a bit to Alice.
Open phase: Bob opens his commitment and Alice accepts (or not).

The protocol should be:

- **correct**: If Alice and Bob are honest then Alice always accepts the opening.
- **binding**: If Alice is honest then there is at most one bit that Bob can successfully open.
- **hiding**: If Bob is honest then Alice learns nothing about his commitment until the open phase.

Bit commitment – the no-go

- Quantum mechanics does not allow for a bit commitment that gives perfect (or close to perfect) security to both parties [Lo,Chau'96; Mayers'96].
- There exist protocols that give partial security to both parties, the trade-offs are known [Spekkens,Rudolph'01; Chailloux,Kerenidis'11].

Bit commitment – the no-go

- Quantum mechanics does not allow for a bit commitment that gives perfect (or close to perfect) security to both parties [Lo,Chau'96; Mayers'96].
- There exist protocols that give partial security to both parties, the trade-offs are known [Spekkens,Rudolph'01; Chailloux,Kerenidis'11].

By imposing communication constraints
one can evade the no-go

Bit commitment – the no-go

- Quantum mechanics does not allow for a bit commitment that gives perfect (or close to perfect) security to both parties [Lo,Chau'96; Mayers'96].
- There exist protocols that give partial security to both parties, the trade-offs are known [Spekkens,Rudolph'01; Chailloux,Kerenidis'11].

By imposing communication constraints one can evade the no-go

Communication constraints can be enforced by special relativity

Bit commitment – the no-go

- Quantum mechanics does not allow for a bit commitment that gives perfect (or close to perfect) security to both parties [Lo,Chau'96; Mayers'96].
- There exist protocols that give partial security to both parties, the trade-offs are known [Spekkens,Rudolph'01; Chailloux,Kerenidis'11].

By imposing communication constraints one can evade the no-go

Communication constraints can be enforced by special relativity

RELATIVISTIC BIT COMMITMENT

Relativistic bit commitment protocols

1. Unconditionally Secure Bit Commitment
   A. Kent, Phys. Rev. Lett. 83, 1447 (1999)

Relativistic bit commitment protocols

1. Unconditionally Secure Bit Commitment
   A. Kent, Phys. Rev. Lett. 83, 1447 (1999)
2. Secure Classical Bit Commitment Using Fixed Capacity Communication Channels
   A. Kent, Journal of Cryptology 18, 313 (2005)

Relativistic bit commitment protocols

1. Unconditionally Secure Bit Commitment
   A. Kent, Phys. Rev. Lett. 83, 1447 (1999)
2. Secure Classical Bit Commitment Using Fixed Capacity Communication Channels
   A. Kent, Journal of Cryptology 18, 313 (2005)
3. Unconditionally Secure Bit Commitment with Flying Qudits
   A. Kent, New Journal of Physics 13, 113015 (2011)

Relativistic bit commitment protocols

1. Unconditionally Secure Bit Commitment
   A. Kent, Phys. Rev. Lett. 83, 1447 (1999)
2. Secure Classical Bit Commitment Using Fixed Capacity Communication Channels
   A. Kent, Journal of Cryptology 18, 313 (2005)
3. Unconditionally Secure Bit Commitment with Flying Qudits
   A. Kent, New Journal of Physics 13, 113015 (2011)
4. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes
   A. Kent, Phys. Rev. Lett. 109, 130501 (2012)

BC by Transmitting Measurement Outcomes

BC by Transmitting Measurement Outcomes

1. (commit) Alice generates n random BB84 states and (simultaneously) sends them to Bob.

BC by Transmitting Measurement Outcomes

1. (commit) Alice generates n random BB84 states and (simultaneously) sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations.

BC by Transmitting Measurement Outcomes

1. (commit) Alice generates n random BB84 states and (simultaneously) sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations.
3. (open) Bob's agents have to simultaneously unveil the commited bit and the measurement outcomes to Alice's agents.

BC by Transmitting Measurement Outcomes

1. (commit) Alice generates n random BB84 states and (simultaneously) sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations.
3. (open) Bob's agents have to simultaneously unveil the commited bit and the measurement outcomes to Alice's agents.
4. (verify) Alice's agents verify whether the outcomes provided by Bob are consistent with the BB84 states.

Security

Proven secure in
[S. Croke and A. Kent, Phys. Rev. A 86, 052309 (2012),
J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner,
Information Theory, IEEE Transactions on 59, 4687 (2013)]

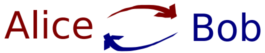
Secure you say, mhhmmmm, but what's the security model?

Security

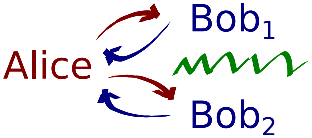
Proven secure in
[S. Croke and A. Kent, Phys. Rev. A 86, 052309 (2012),
J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner,
Information Theory, IEEE Transactions on 59, 4687 (2013)]

Secure you say, mhhmmmm, but what's the security model?

Commit phase



Open phase



Security

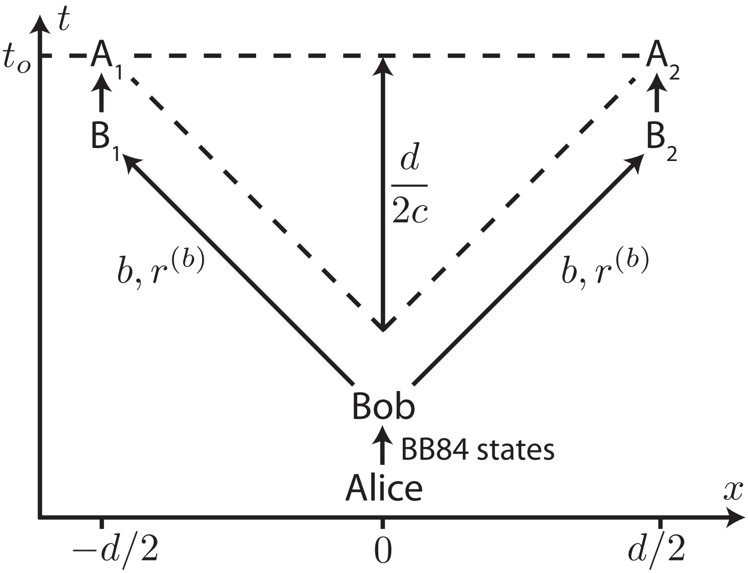
Proven secure in
[S. Croke and A. Kent, Phys. Rev. A 86, 052309 (2012),
J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner,
Information Theory, IEEE Transactions on 59, 4687 (2013)]

Secure you say, mhhmmmm, but what's the security model?

Commit phase | Open phase

not possible classically
[quantum advantage]

Relativistic realisation



Implementation issues

Source: We do not use a single photon source. We use a weak coherent source with phase randomisation:

$$\rho = \sum_{r=0}^{\infty} p_r |r\rangle\langle r|,$$

$$\text{where} \quad p_r = e^{-\mu} \cdot \frac{\mu^r}{r!},$$

μ is the average number of photons per pulse and $|r\rangle$ is the Fock state of r photons.

Implementation issues

Source: We do not use a single photon source. We use a weak coherent source with phase randomisation:

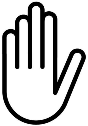
$$\rho = \sum_{r=0}^{\infty} p_r |r\rangle\langle r|,$$

$$\text{where} \quad p_r = e^{-\mu} \cdot \frac{\mu^r}{r!},$$

μ is the average number of photons per pulse and $|r\rangle$ is the Fock state of r photons.

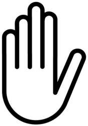
Channel and Bob's detectors: They are not perfect. They introduce bit-flip errors and losses.

Implementation issues and fixes...



on ONE hand
noise or losses make
honest Bob's life more
difficult

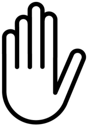
Implementation issues and fixes...



on ONE hand
noise or losses make
honest Bob's life more
difficult

(obvious) fix: make Alice "more
forgiving"
(undesired) result: cheating
becomes easier

Implementation issues and fixes...

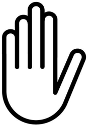


on ONE hand
noise or losses make
honest Bob's life more
difficult

on THE OTHER hand
multi-photon emissions
enable dishonest Bob to
cheat more easily

(obvious) fix: make Alice "more forgiving"
(undesired) result: cheating becomes easier

Implementation issues and fixes...



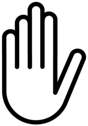
on ONE hand
noise or losses make honest Bob's life more difficult

(obvious) fix: make Alice "more forgiving"
(undesired) result: cheating becomes easier

on THE OTHER hand
multi-photon emissions enable dishonest Bob to cheat more easily

(obvious) fix: eliminate multi-photon emissions
(undesired) result: more vacuum rounds, honest Bob suffers

Implementation issues and fixes...



on ONE hand
noise or losses make honest Bob's life more difficult

(obvious) fix: make Alice "more forgiving"
(undesired) result: cheating becomes easier

on THE OTHER hand
multi-photon emissions enable dishonest Bob to cheat more easily

(obvious) fix: eliminate multi-photon emissions
(undesired) result: more vacuum rounds, honest Bob suffers

need to try a bit harder...

A fault-tolerant protocol

A fault-tolerant protocol

1. (commit) Alice generates n pulses of random BB84 states and sends them to Bob.

A fault-tolerant protocol

1. (commit) Alice generates n pulses of random BB84 states and sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations. Bob tells Alice which photons he received. Alice accepts if the losses are below a specific threshold. All the other rounds are discarded.

A fault-tolerant protocol

1. (commit) Alice generates n pulses of random BB84 states and sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations. Bob tells Alice which photons he received. Alice accepts if the losses are below a specific threshold. All the other rounds are discarded.
3. (open) Bob's agents have to simultaneously unveil the commited bit and the measurement outcomes to Alice's agents.

A fault-tolerant protocol

1. (commit) Alice generates n pulses of random BB84 states and sends them to Bob.
2. To commit to 0 (1) he measures all the incoming qubits in the computational (Hadamard) basis. Bob distributes the outcomes to agents occupying distant locations. Bob tells Alice which photons he received. Alice accepts if the losses are below a specific threshold. All the other rounds are discarded.
3. (open) Bob's agents have to simultaneously unveil the commited bit and the measurement outcomes to Alice's agents.
4. (verify) Alice's agents verify whether the outcomes provided by Bob are consistent with the BB84 states up to a certain number of errors.

A fault-tolerant protocol - Security

One-commitment steps (honest execution):

- Alice sends N pulses, Bob reports detecting n of them
- Let

$$p_{\mathrm{det}} = n/N$$

- After Bob revealed the commitment, Alice calculates the QBER:

$$\mathrm{QBER} = n_{\mathrm{err}}/n'$$

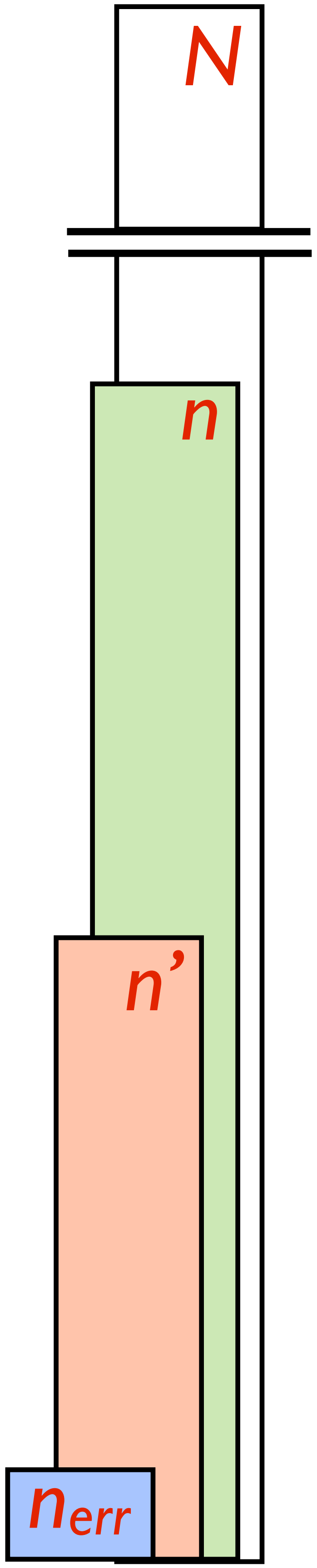
Number of errors within n'

Number of detections with same basis for preparation and measurement

- Security is possible only if

$$p_{\mathrm{det}} > \frac{1 - \mathrm{e}^{-\mu}(1+\mu)}{1 - \frac{\mathrm{QBER}}{\lambda}} \qquad \lambda \approx 14.6\%$$

- Calculate the security parameter from the finite stats



A fault-tolerant protocol - Security

One-commitment steps (honest execution):

- Alice sends N pulses, Bob reports detecting n of them
- Let

$$p_{\text{det}} = n/N$$

- After Bob revealed the commitment, Alice calculates the QBER:

$$\text{QBER} = n_{\text{err}}/n'$$

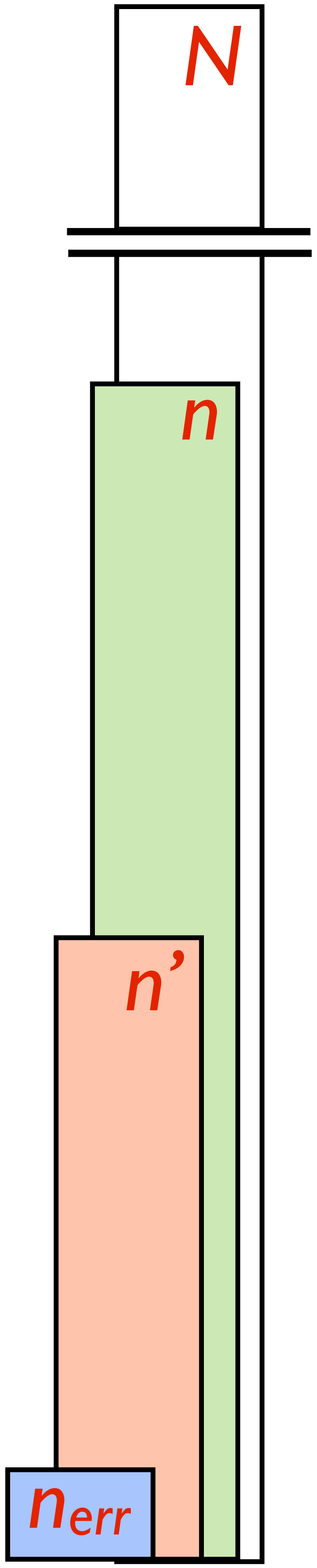
Number of errors within n'

Number of detections with same basis for preparation and measurement

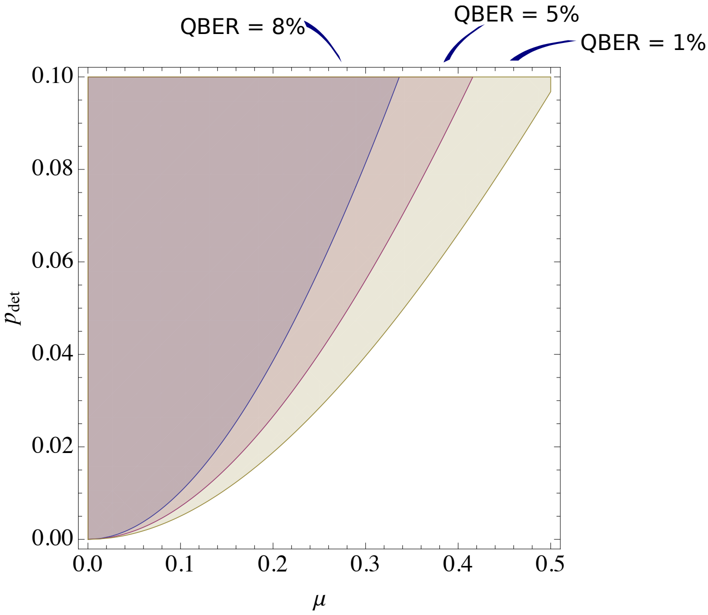
- Security is possible only if

$$p_{\text{det}} > \frac{1 - e^{-\mu}(1+\mu)}{1 - \frac{\text{QBER}}{\lambda}} \qquad \lambda \approx 14.6\%$$

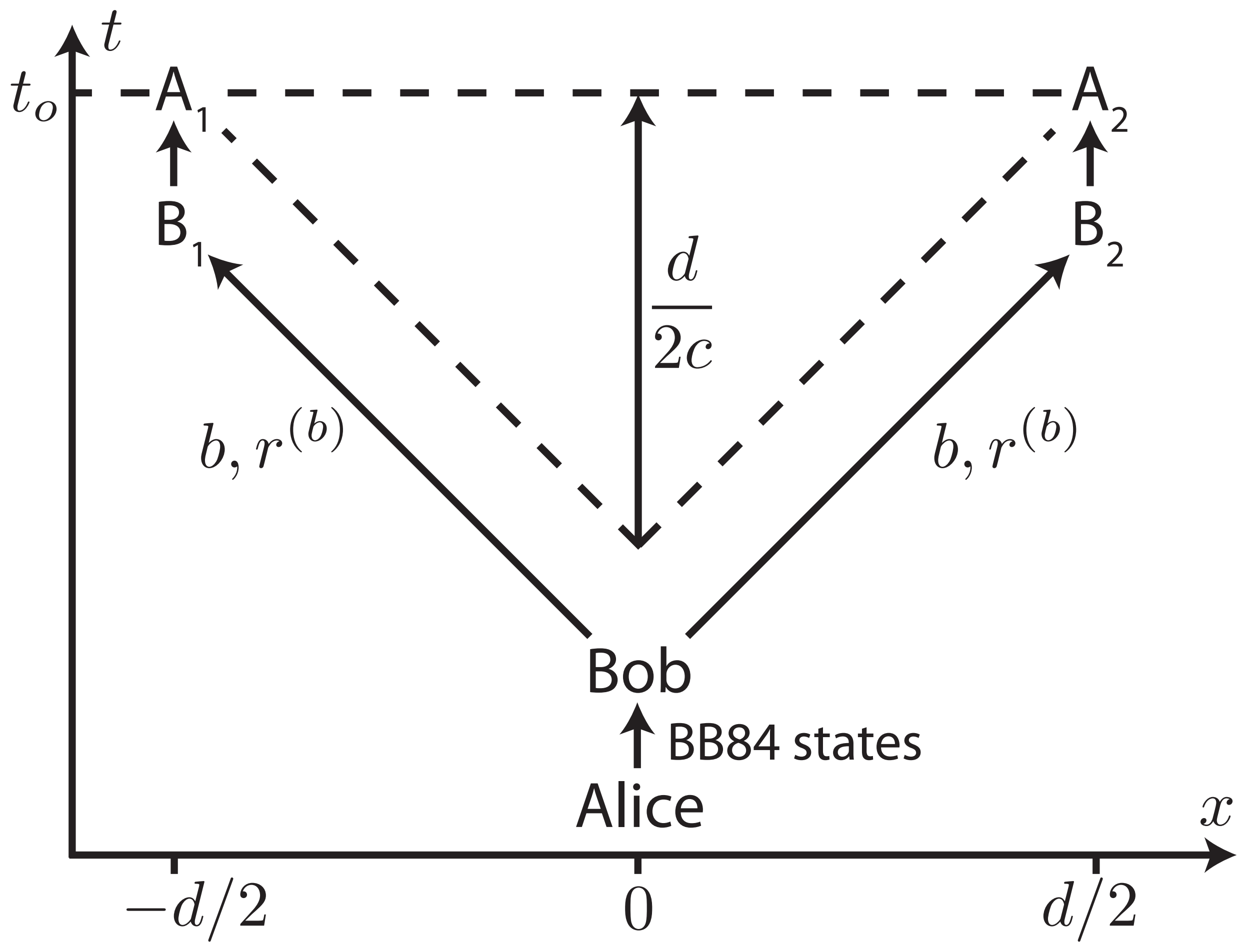
- Calculate the security parameter from the finite stats



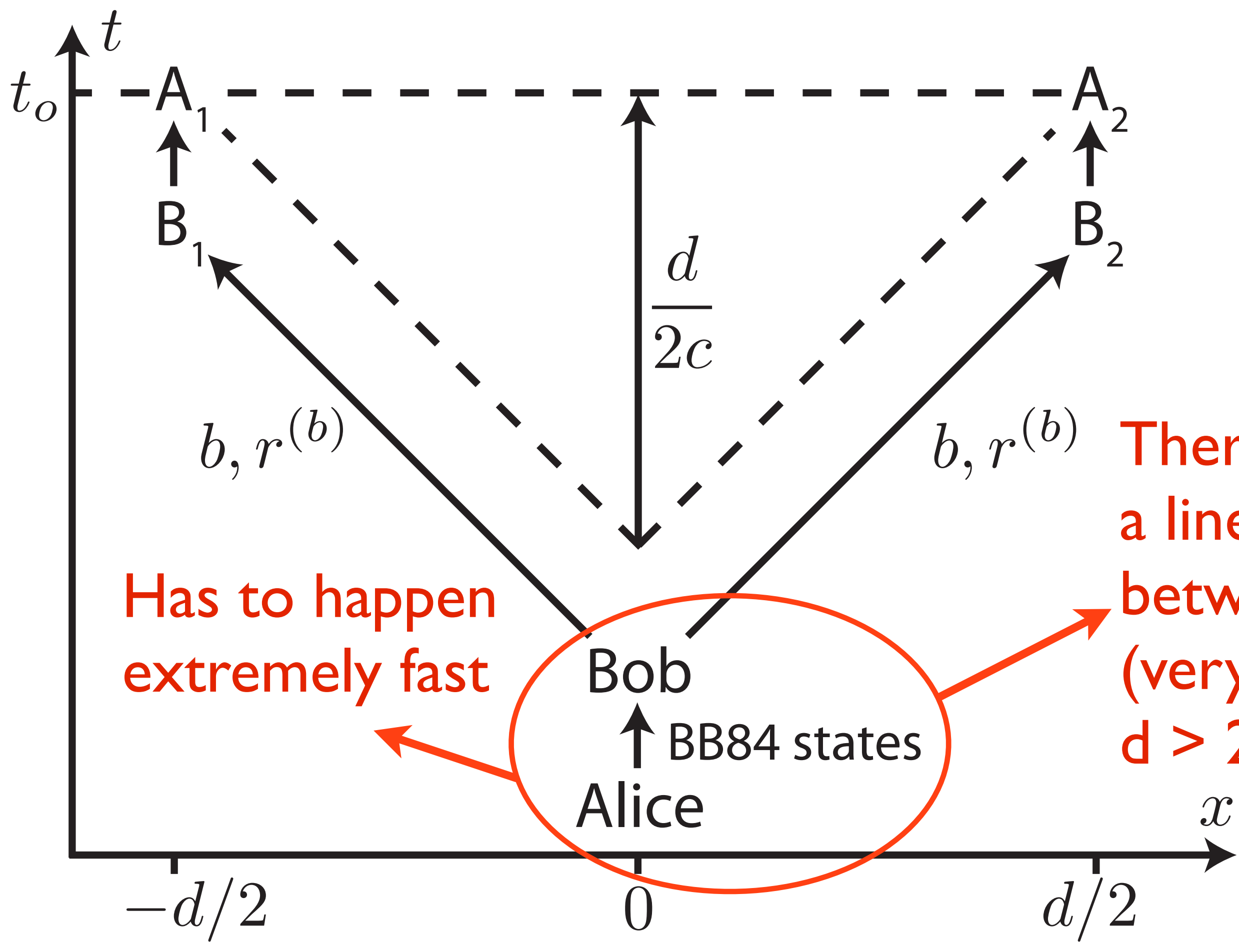
Feasibility plot



A more practical version of Kent'12 protocol

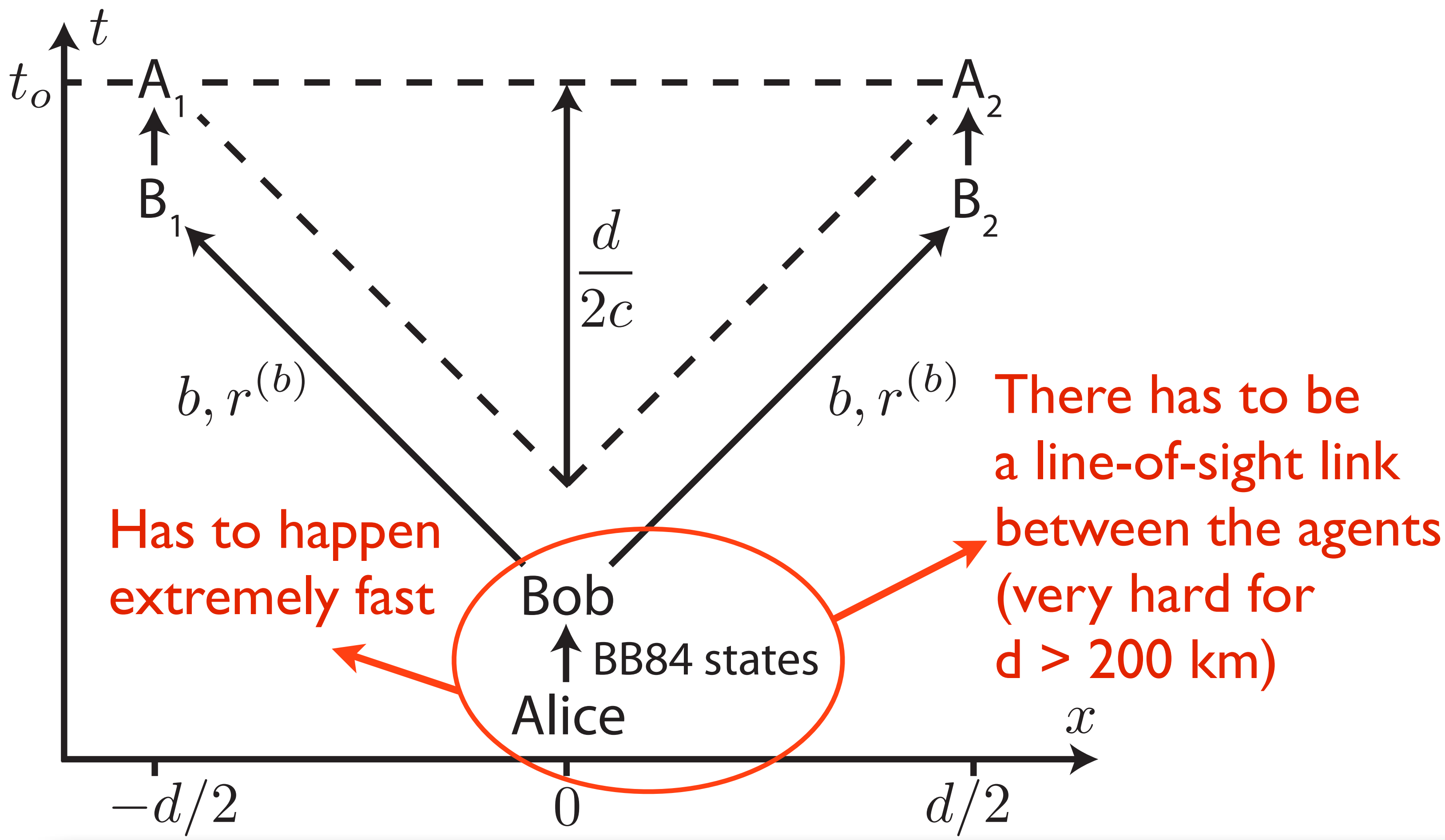


A more practical version of Kent'12 protocol



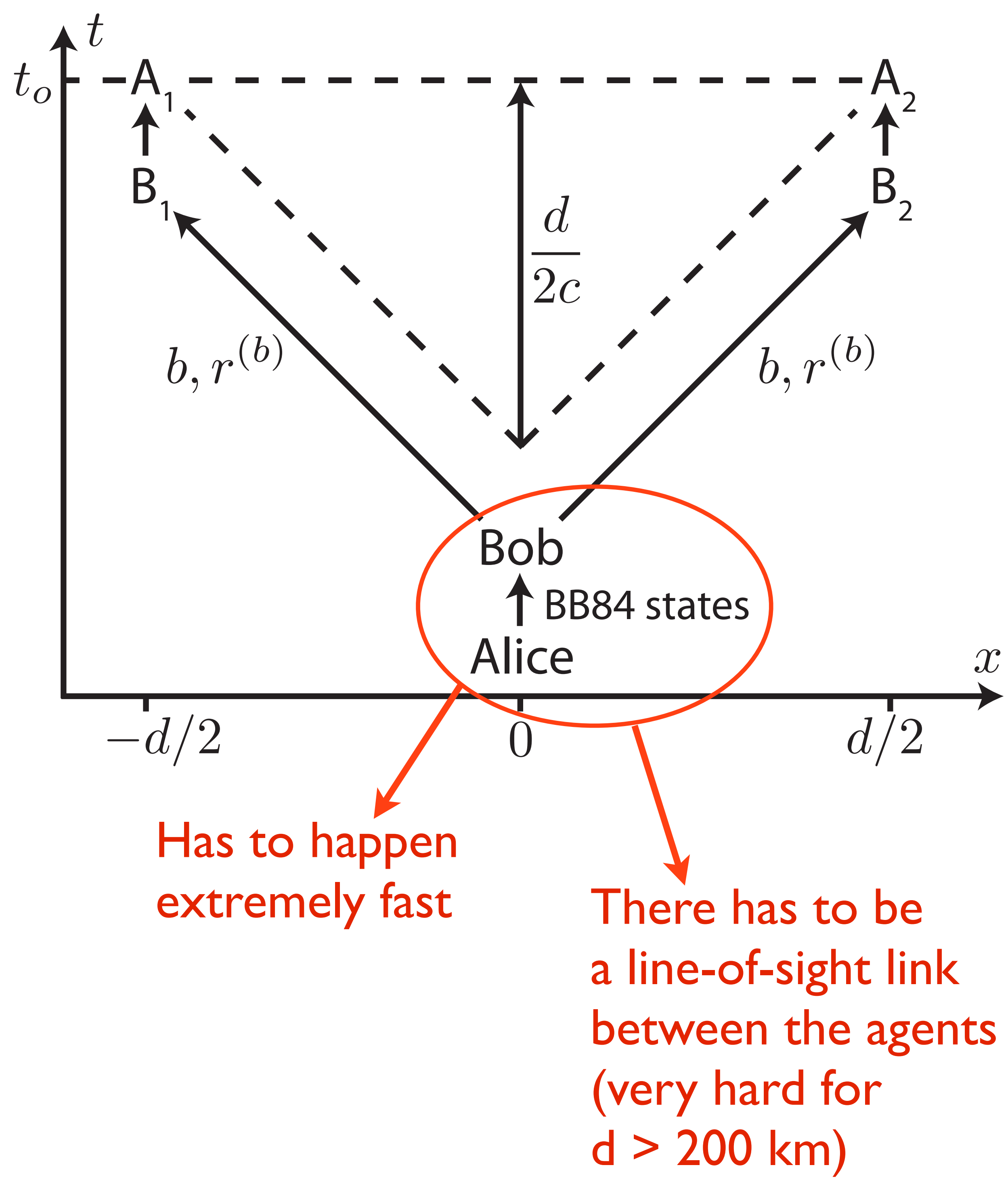
There has to be a line-of-sight link between the agents (very hard for d > 200 km)

A more practical version of Kent'12 protocol

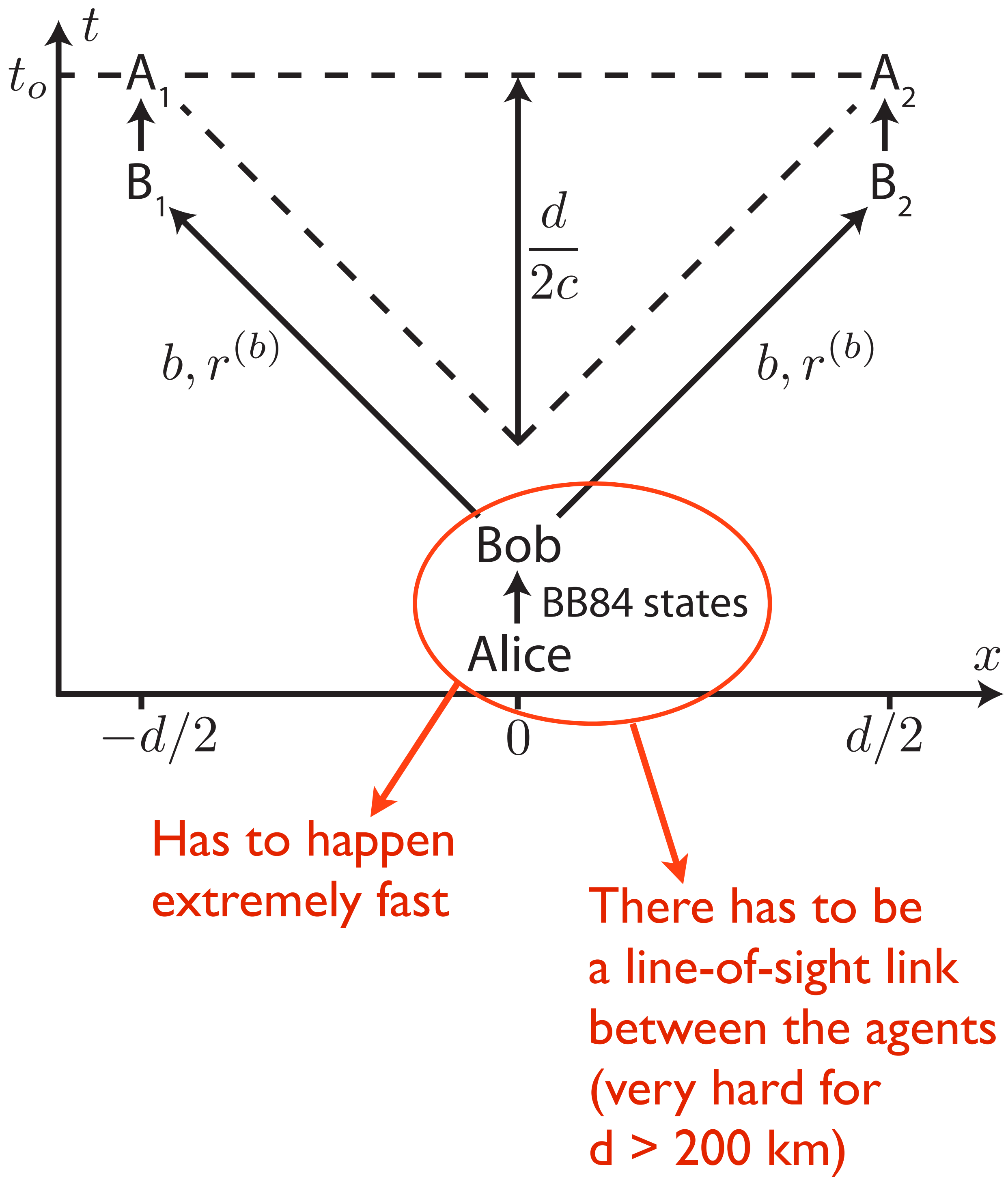


Y. Liu, Y. Cao, M. Curty *et al.* arXiv:1306.4413

A more practical version of Kent'12 protocol

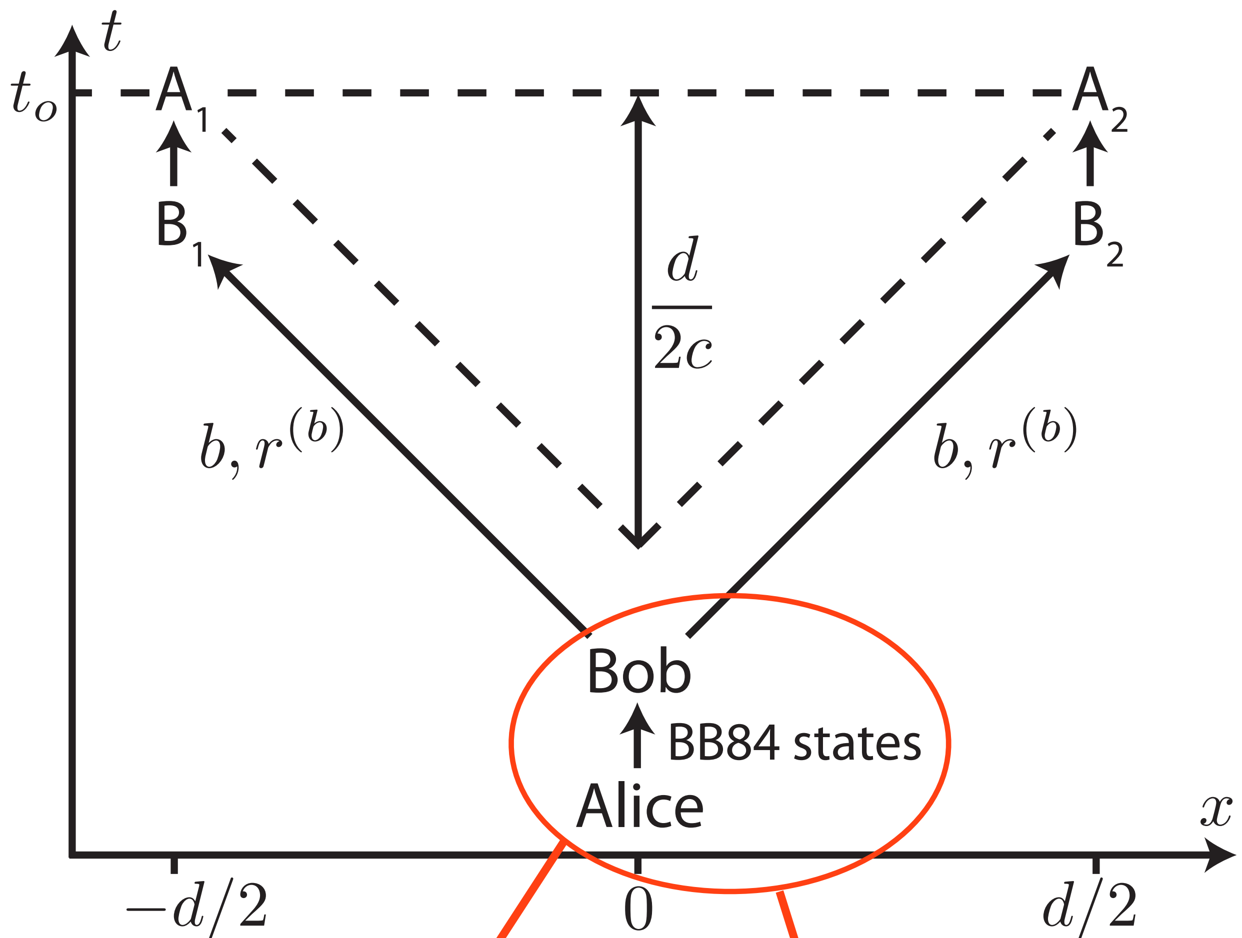


A more practical version of Kent'12 protocol



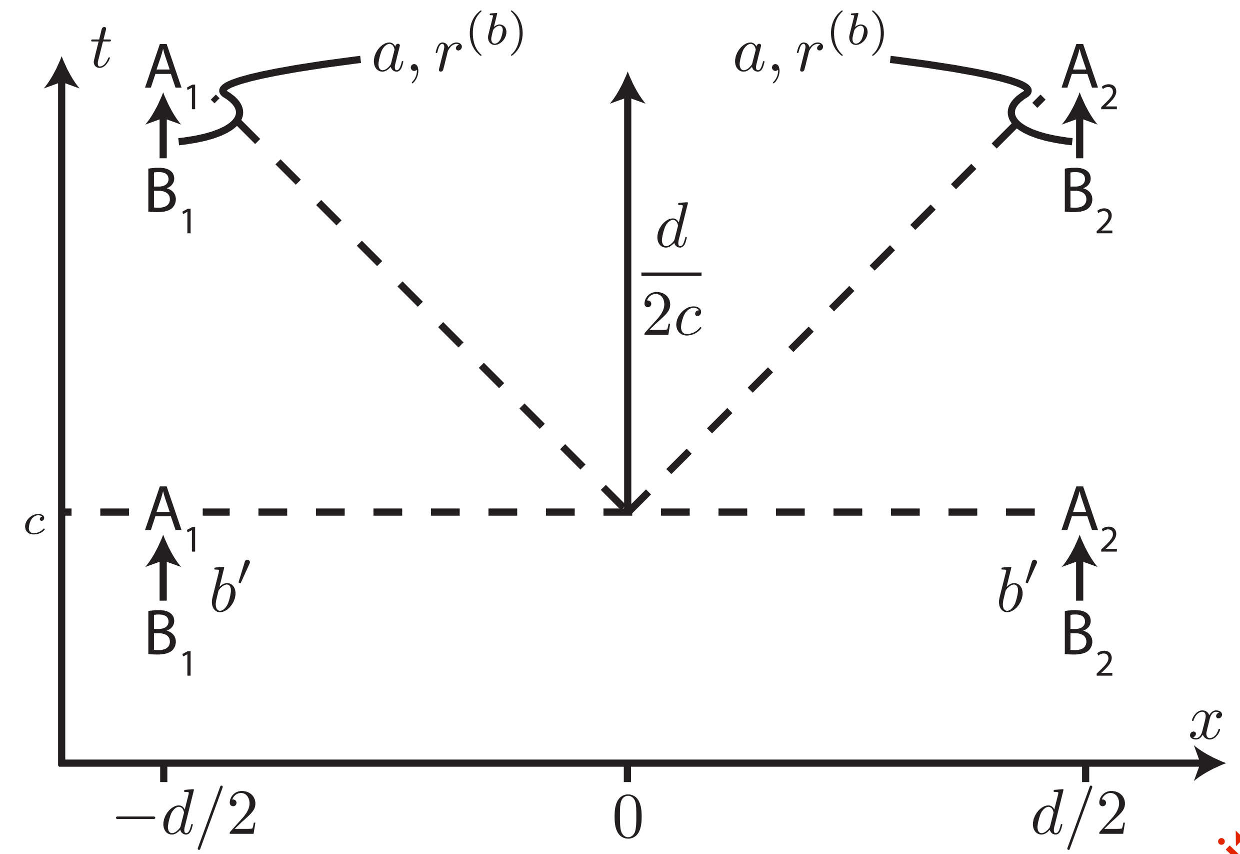
The quantum exchange happens in advance. Bob measures all qubits in a random basis b and informs B_1 and B_2 of the results $r^{(b)}$

A more practical version of Kent'12 protocol



Has to happen extremely fast

There has to be a line-of-sight link between the agents (very hard for d > 200 km)

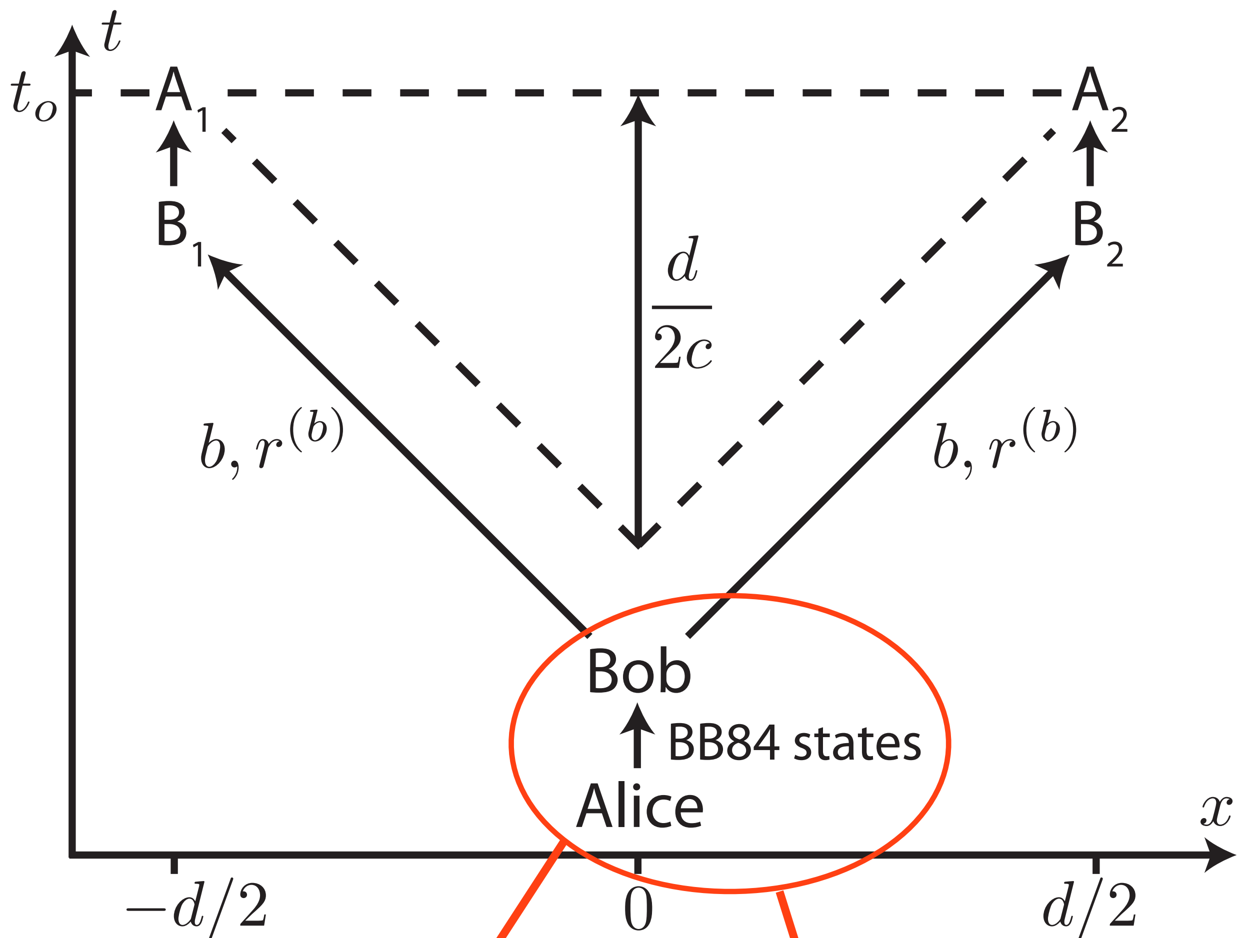


The quantum exchange happens in advance. Bob measures all qubits in a random basis b and informs B_1 and B_2 of the results $r^{(b)}$

Commitment!

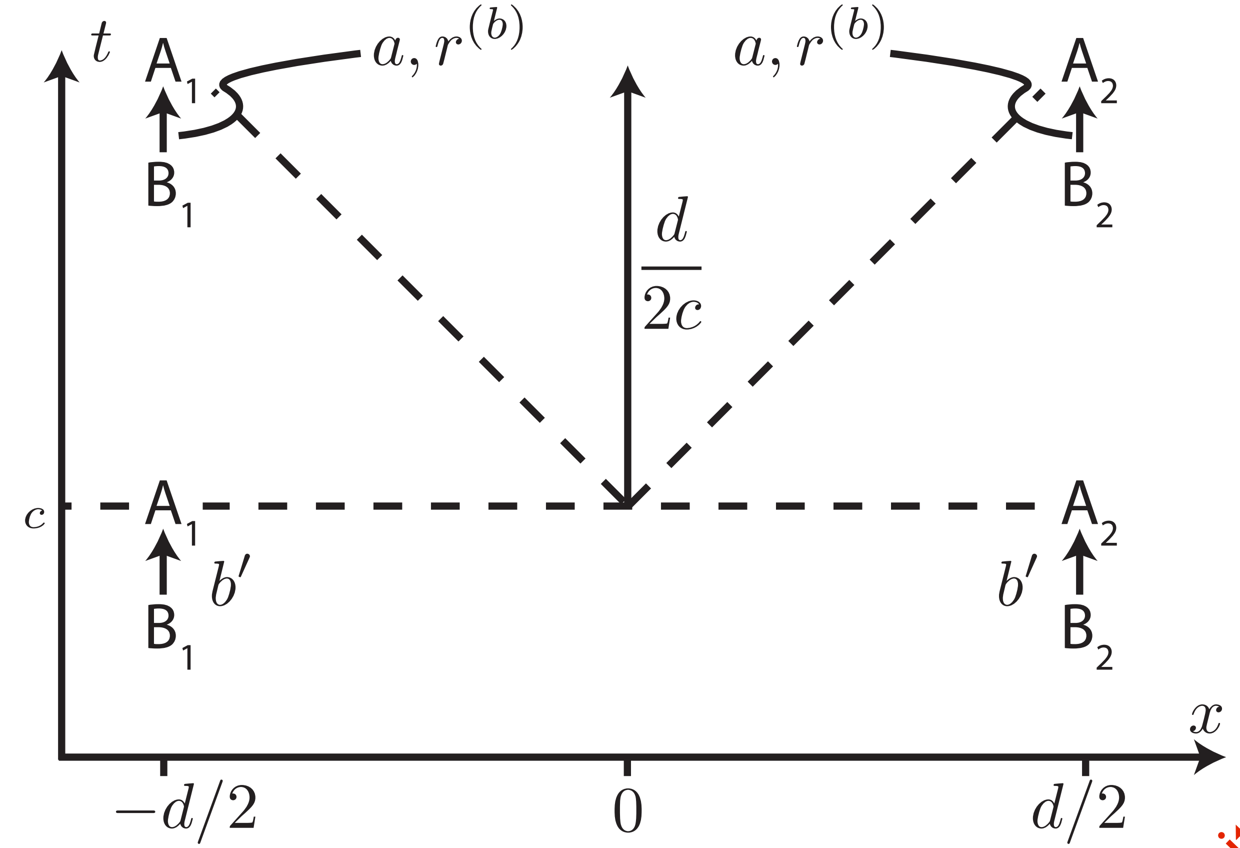
B_1 and B_2 simultaneously commit to $b' = b \oplus a$

A more practical version of Kent'12 protocol



Has to happen extremely fast

There has to be a line-of-sight link between the agents (very hard for d > 200 km)



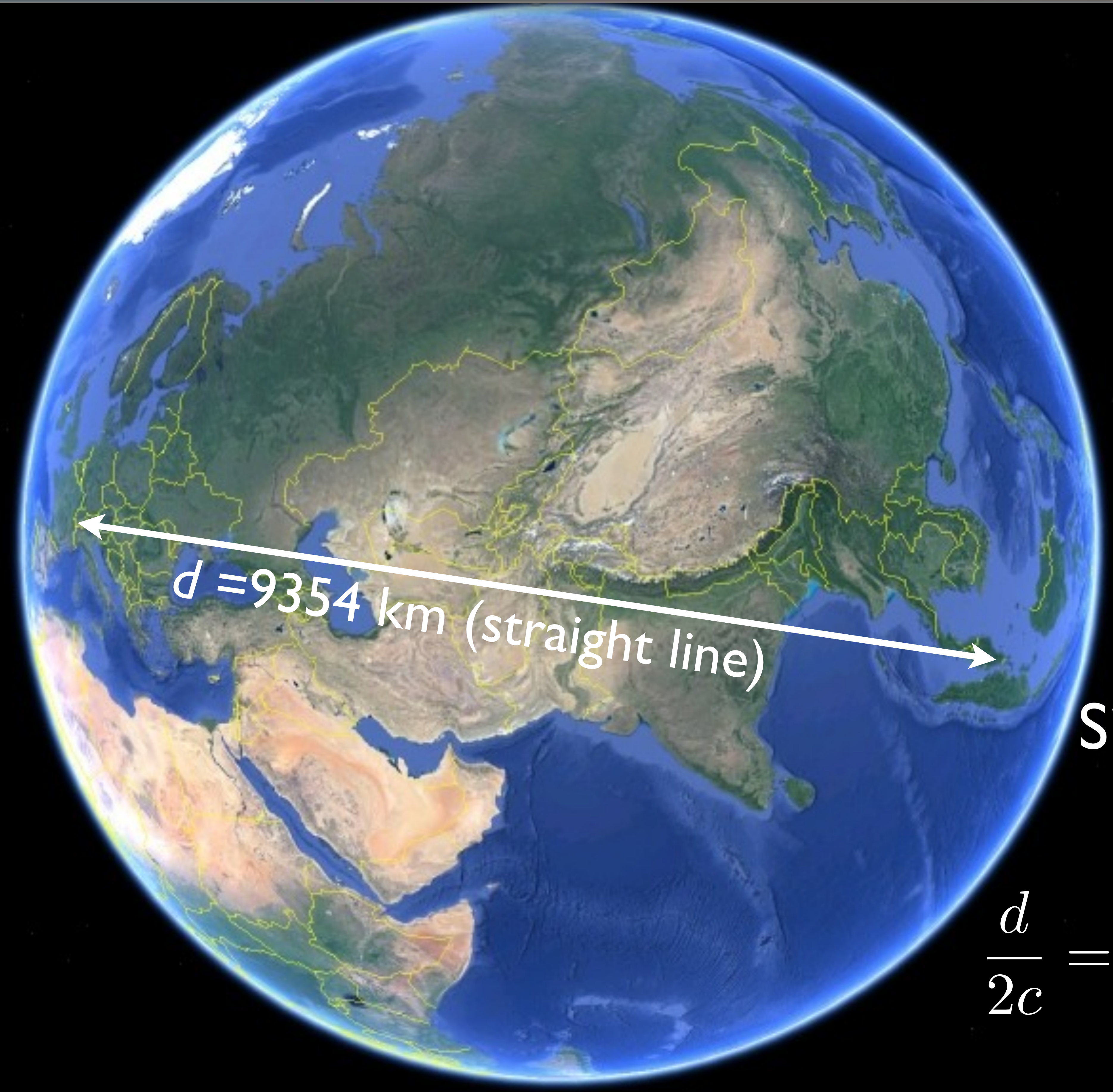
Commitment!

The quantum exchange happens in advance. Bob measures all qubits in a random basis b and informs B_1 and B_2 of the results $r^{(b)}$

B_1 and B_2 simultaneously commit to $b' = b \oplus a$

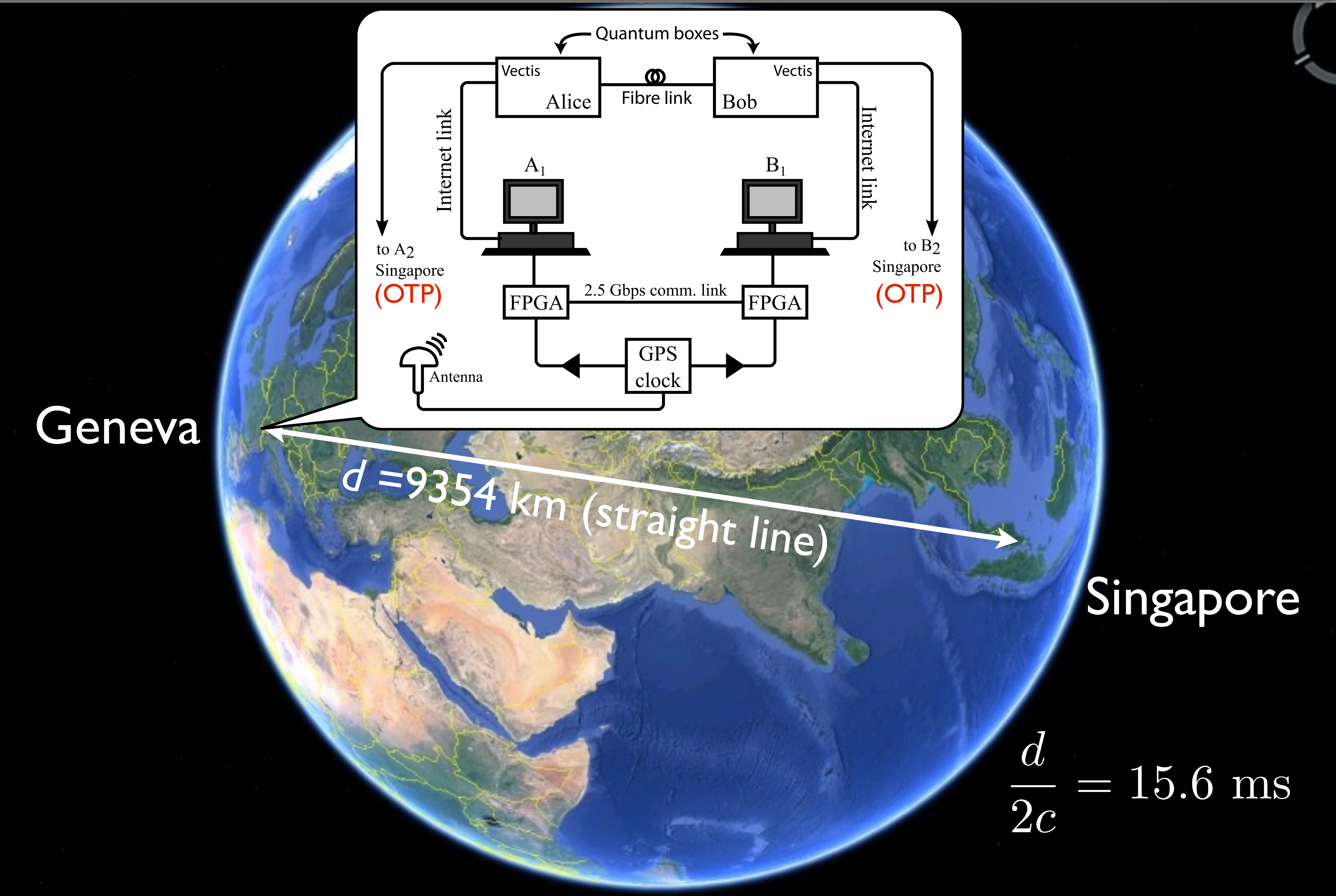
B_1 and B_2 simultaneously reveal a and $r^{(b)}$

Experimental setup - The global picture



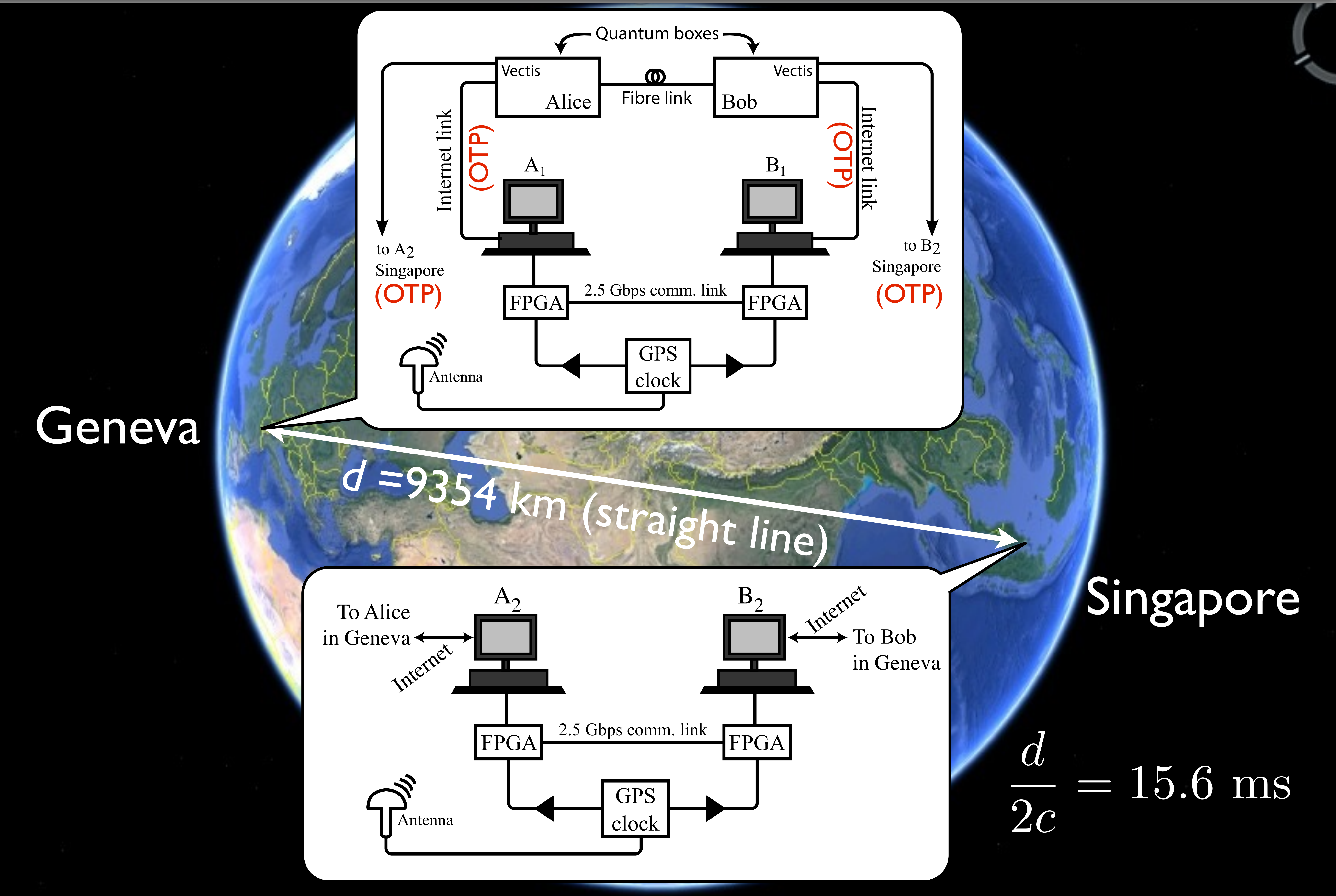
$$\frac{d}{2c} = 15.6 \text{ ms}$$

Experimental setup - The global picture



$$\frac{d}{2c} = 15.6 \text{ ms}$$

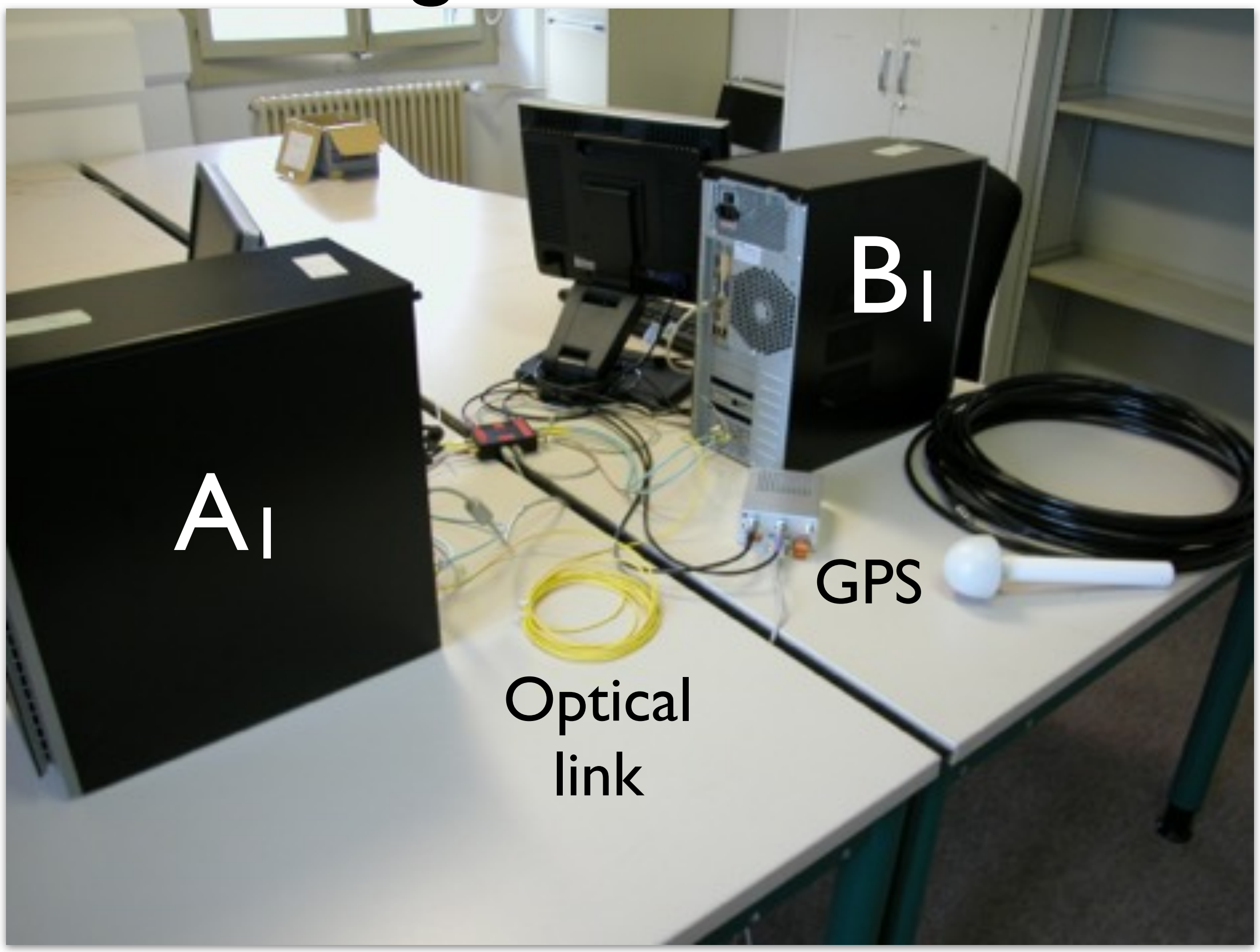
Experimental setup - The global picture



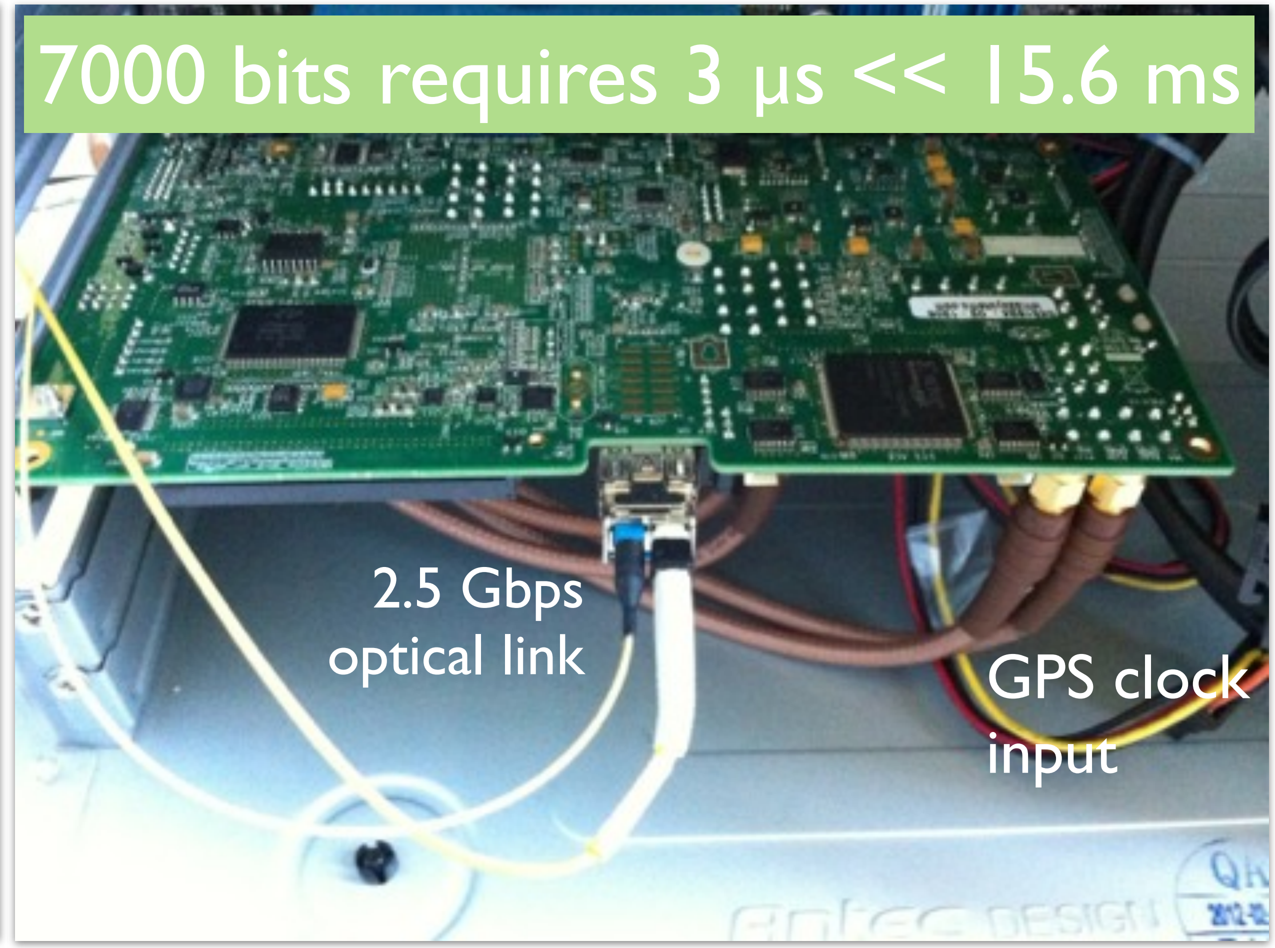
$$\frac{d}{2c} = 15.6 \text{ ms}$$

The classical agents : timing performances

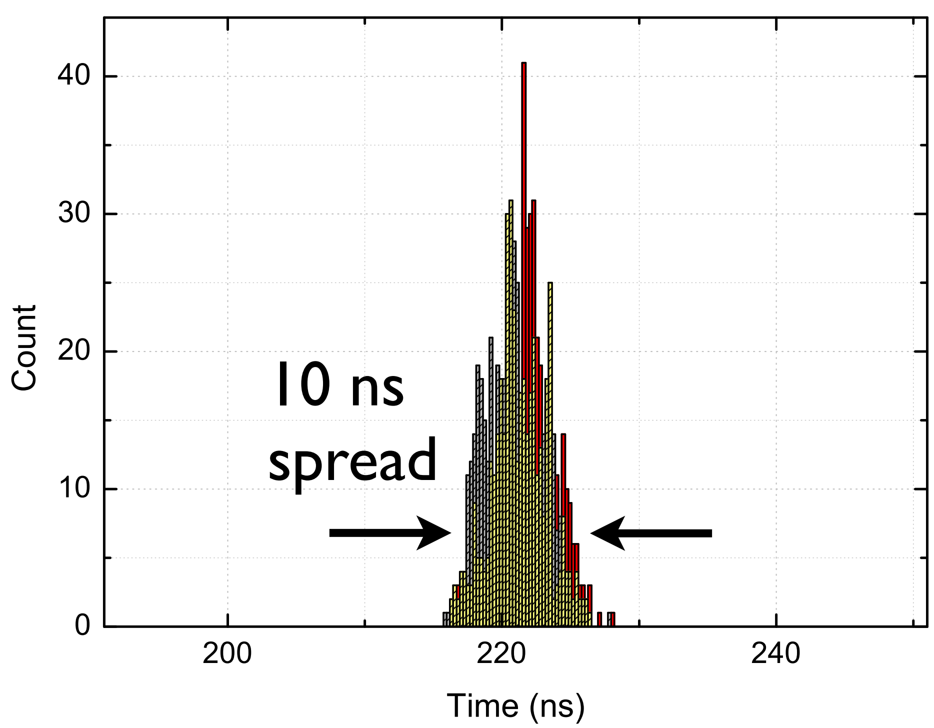
Classical agents in Geneva



FPGA boards



Timing accuracy of the FPGAs with a GPS for A_1 and another for B_1

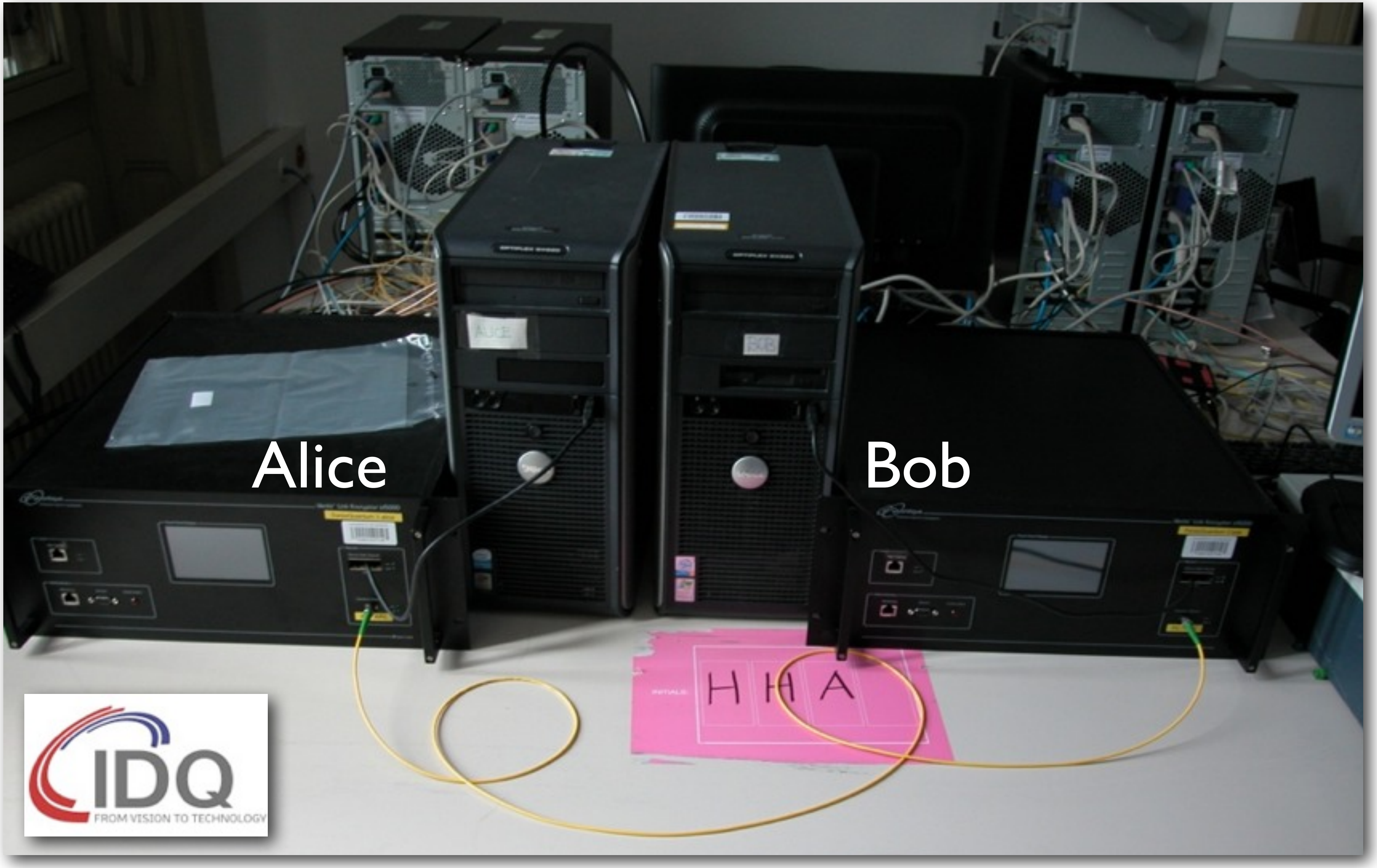


Other tests showed that

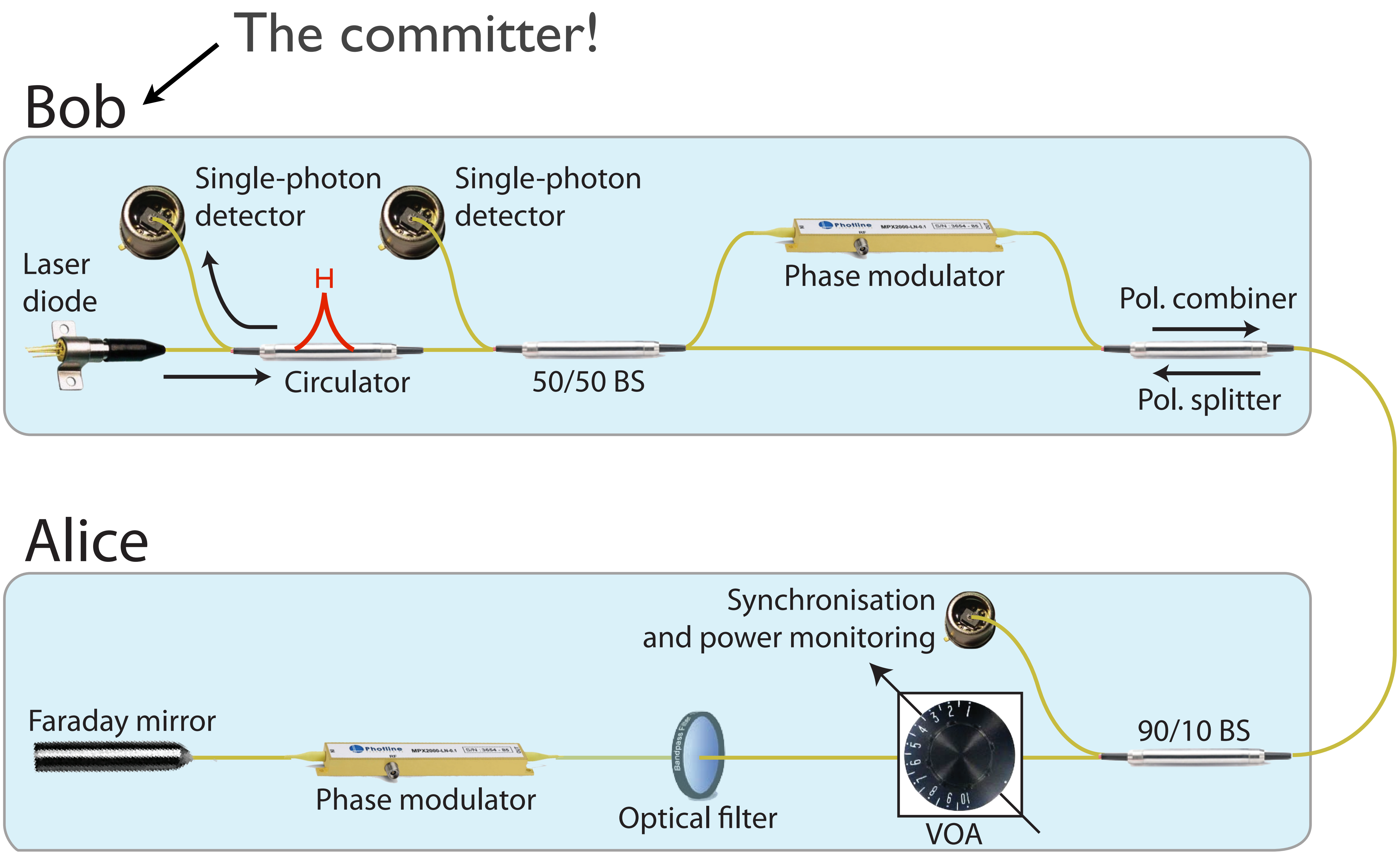
- B1 and B2 are in sync to within 100 ns
- Synchronization is maintained over the 15 ms of the protocol

The quantum boxes (Geneva)

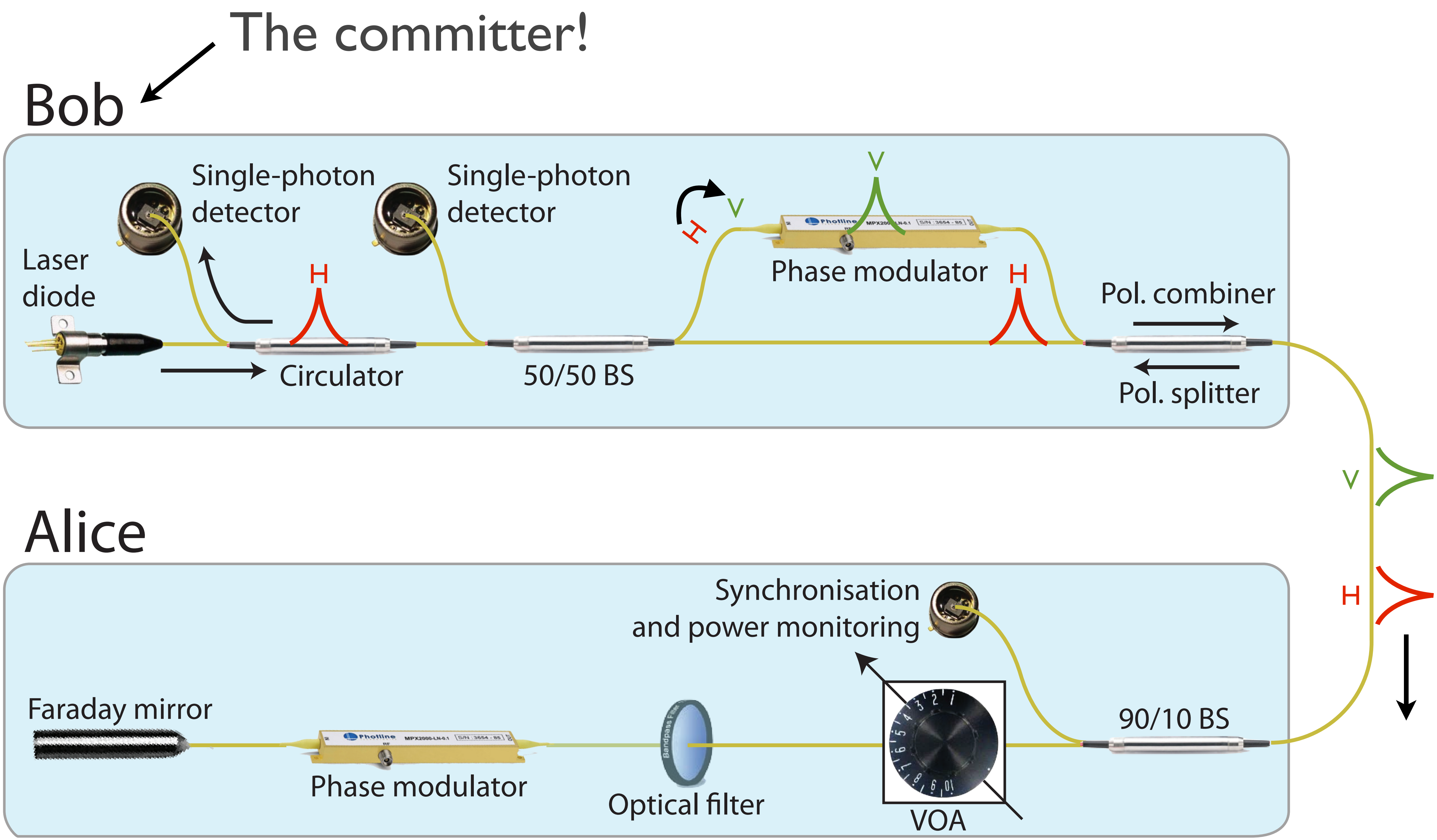
Commercial QKD system by IDQ "Vectis 5100"



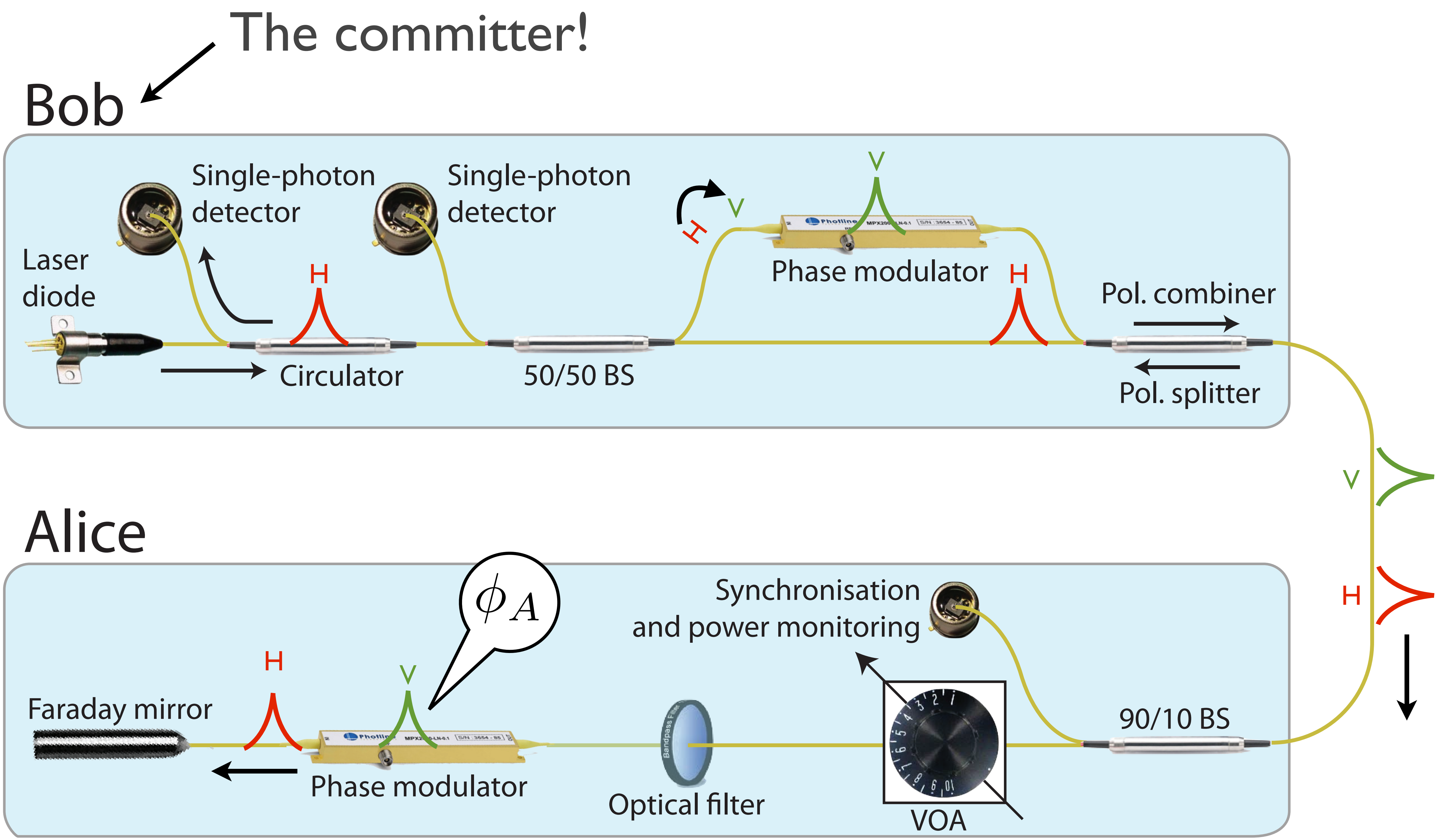
The quantum boxes (Geneva)



The quantum boxes (Geneva)

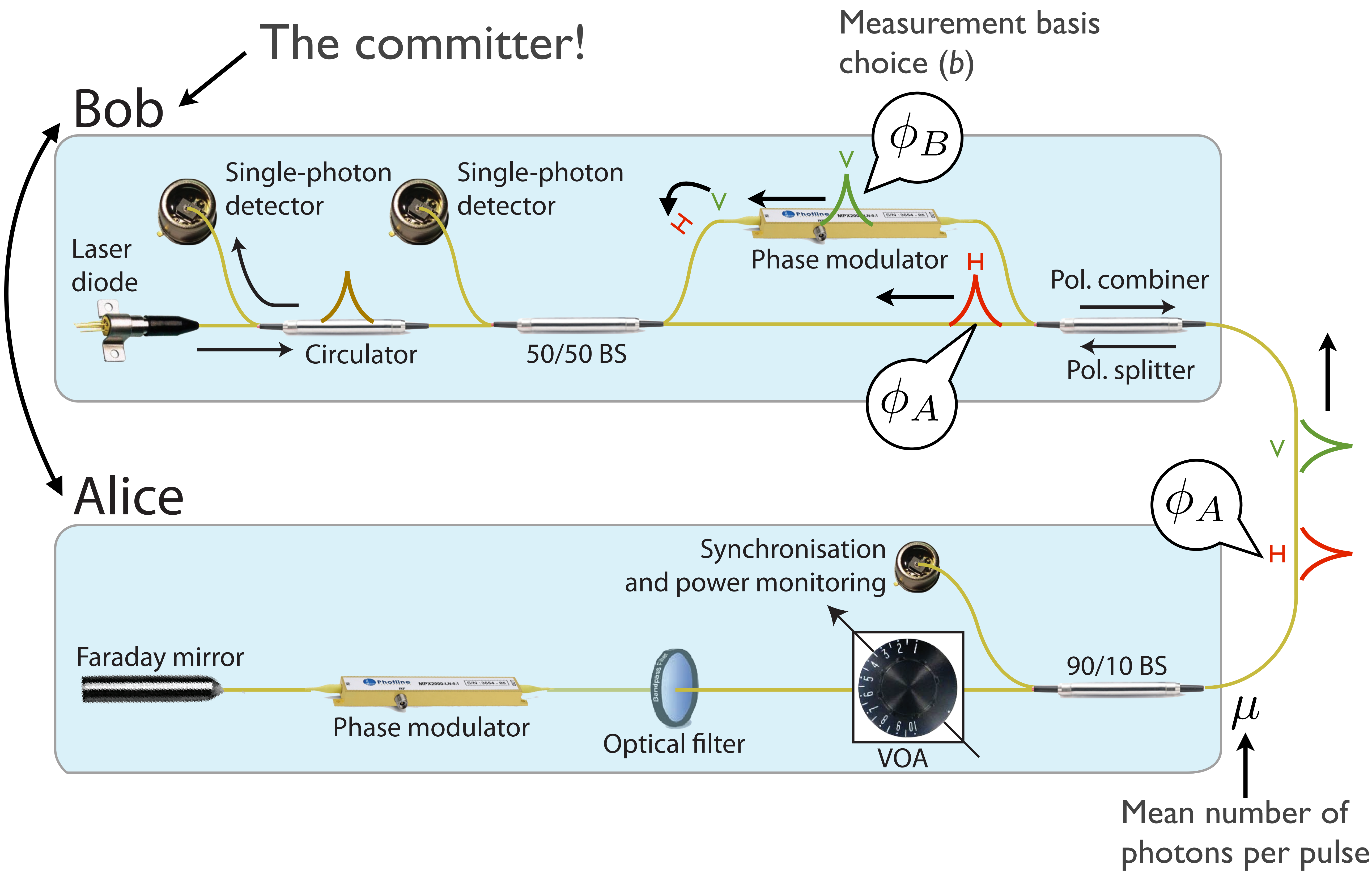


The quantum boxes (Geneva)

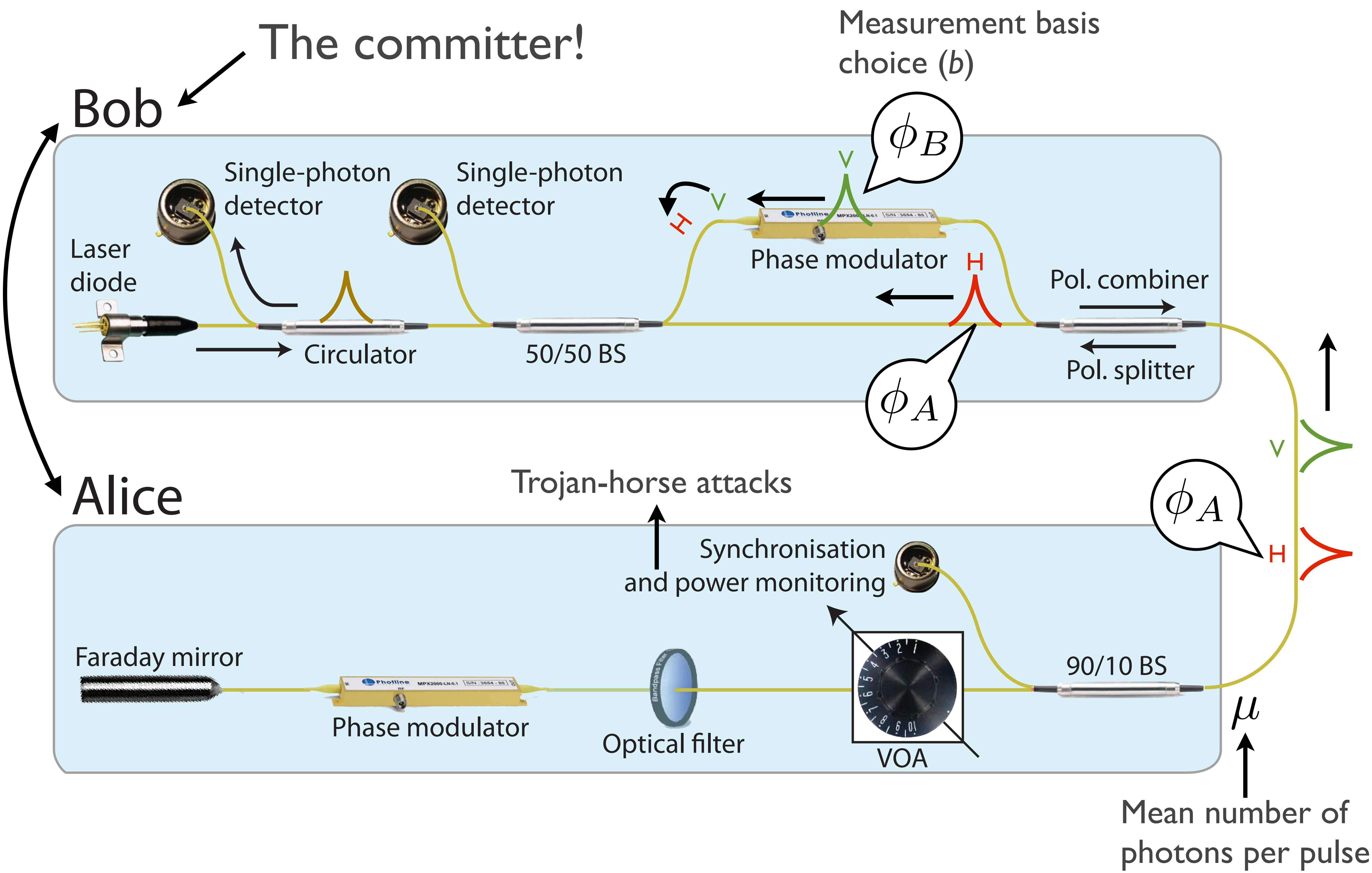


Qubit preparation
(phase encoding)

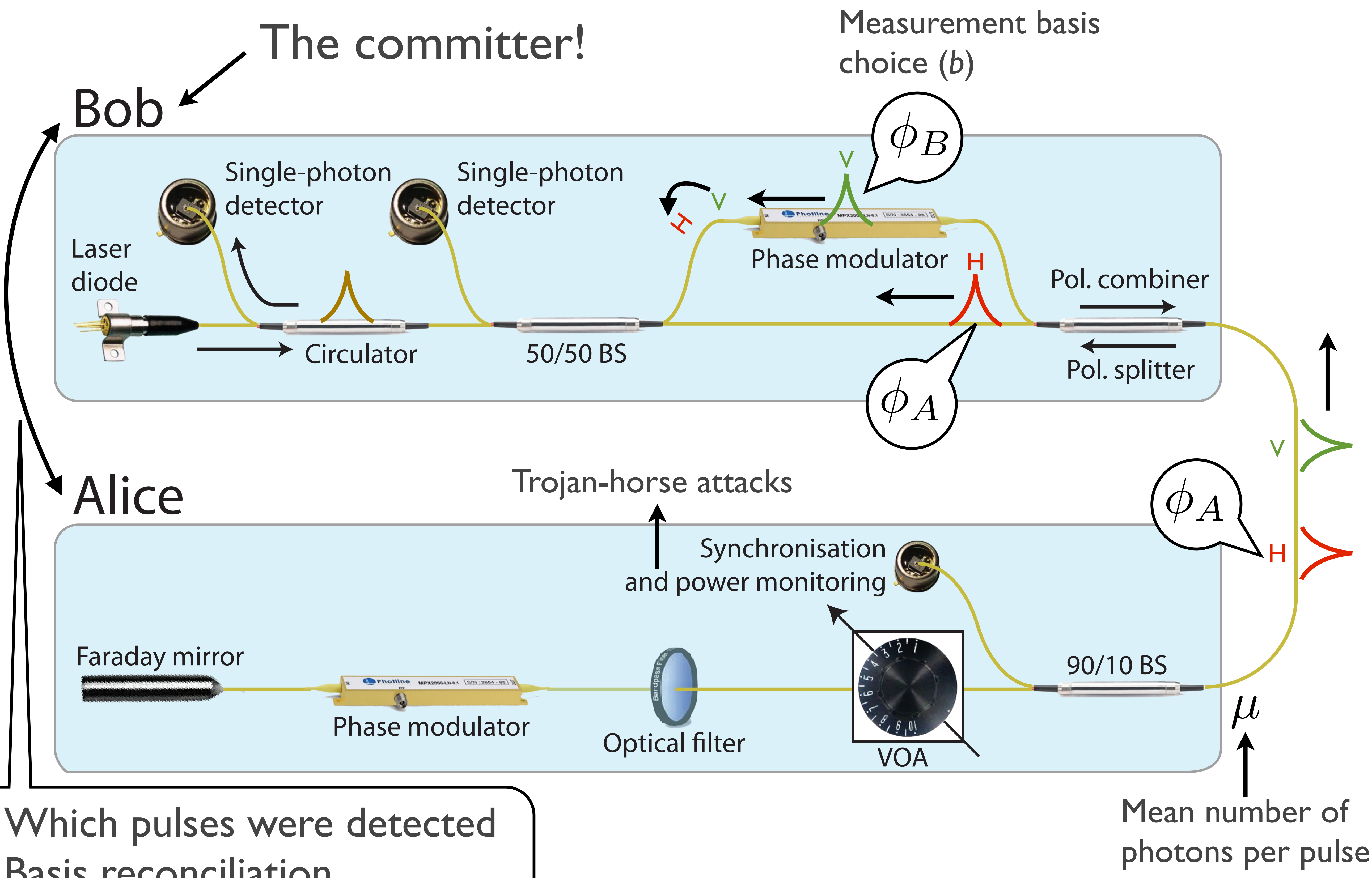
The quantum boxes (Geneva)



The quantum boxes (Geneva)

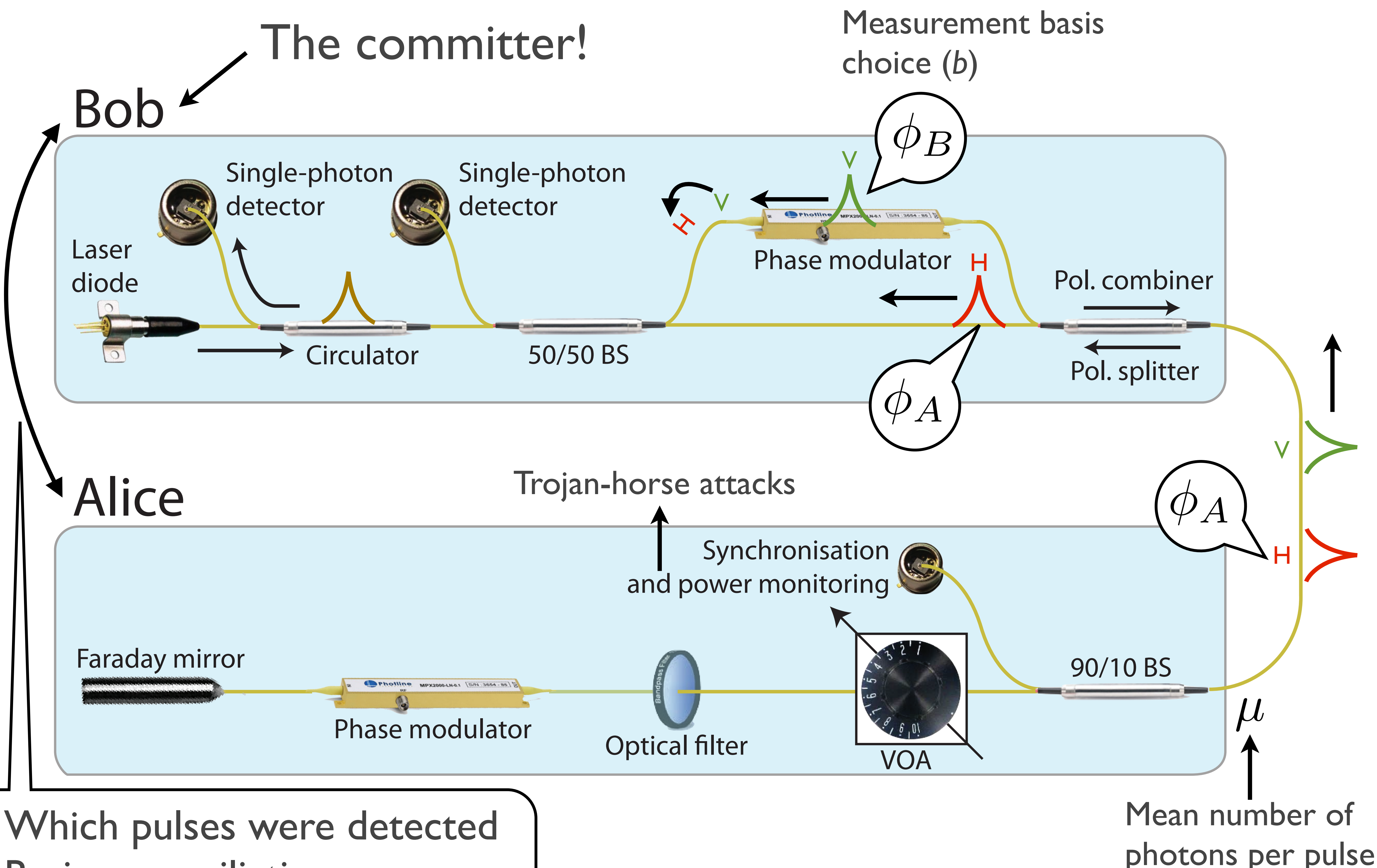


The quantum boxes (Geneva)



- Which pulses were detected
- Basis reconciliation

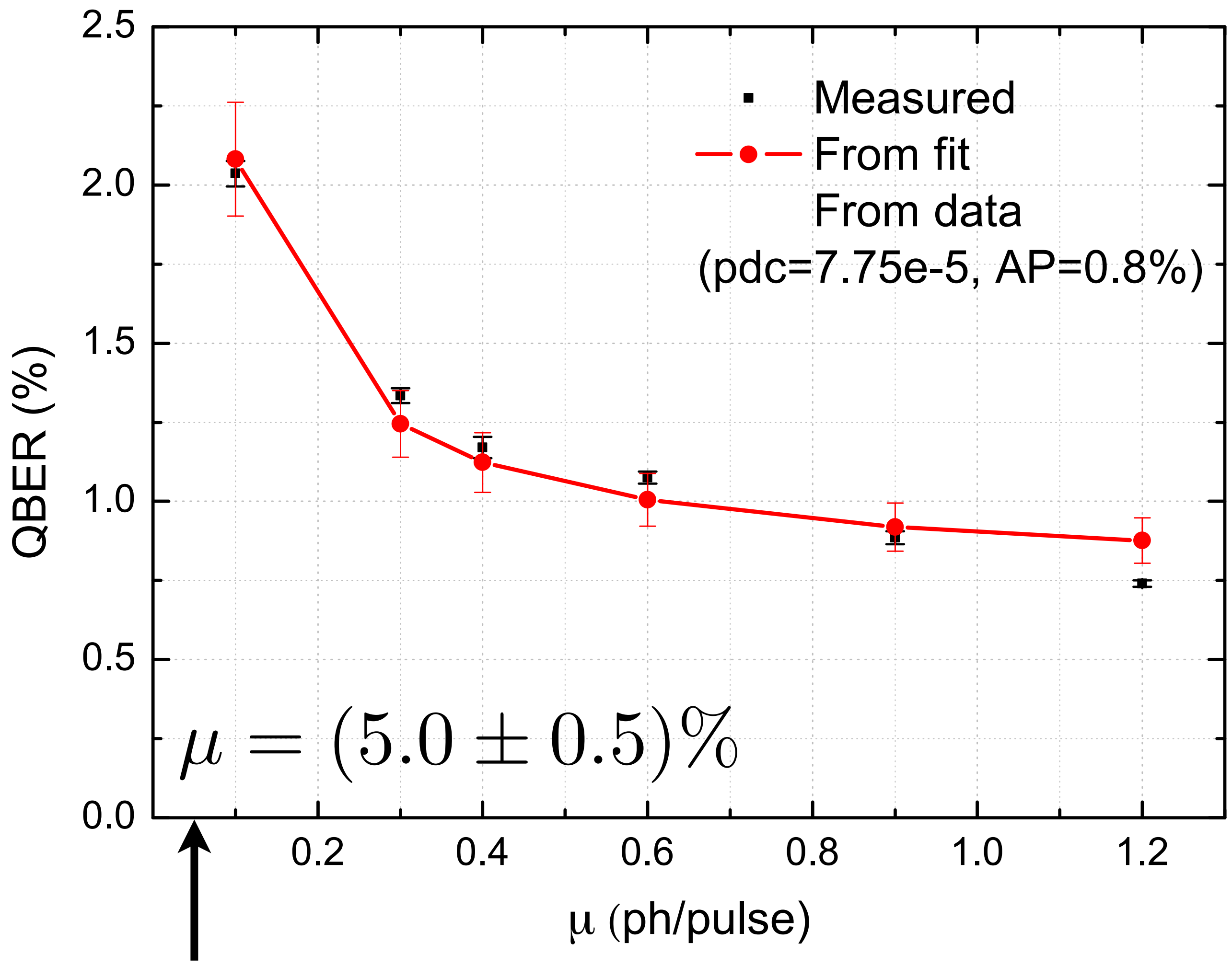
The quantum boxes (Geneva)



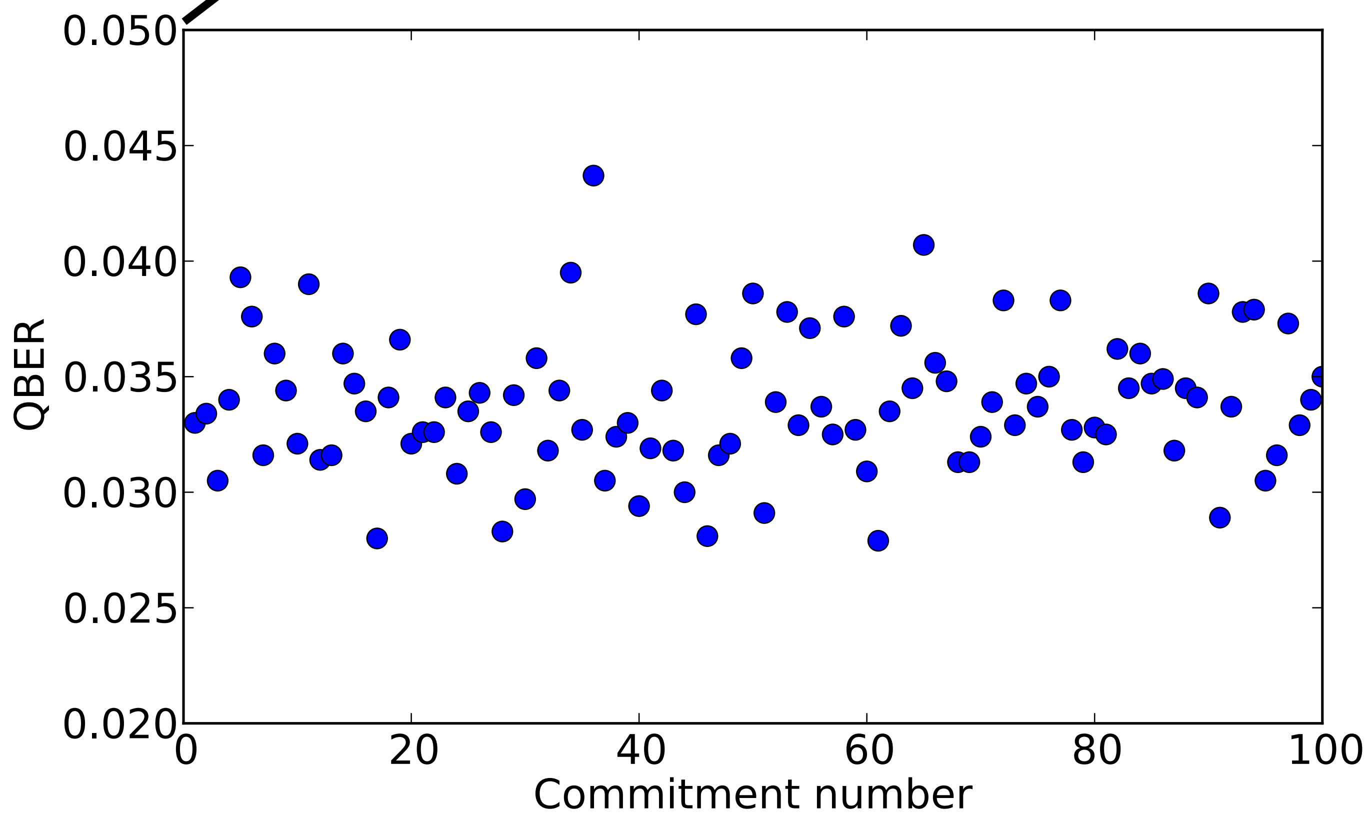
- Which pulses were detected
- ~~Basis reconciliation~~

The quantum boxes (Geneva) : performances

Choosing μ : security trade-off

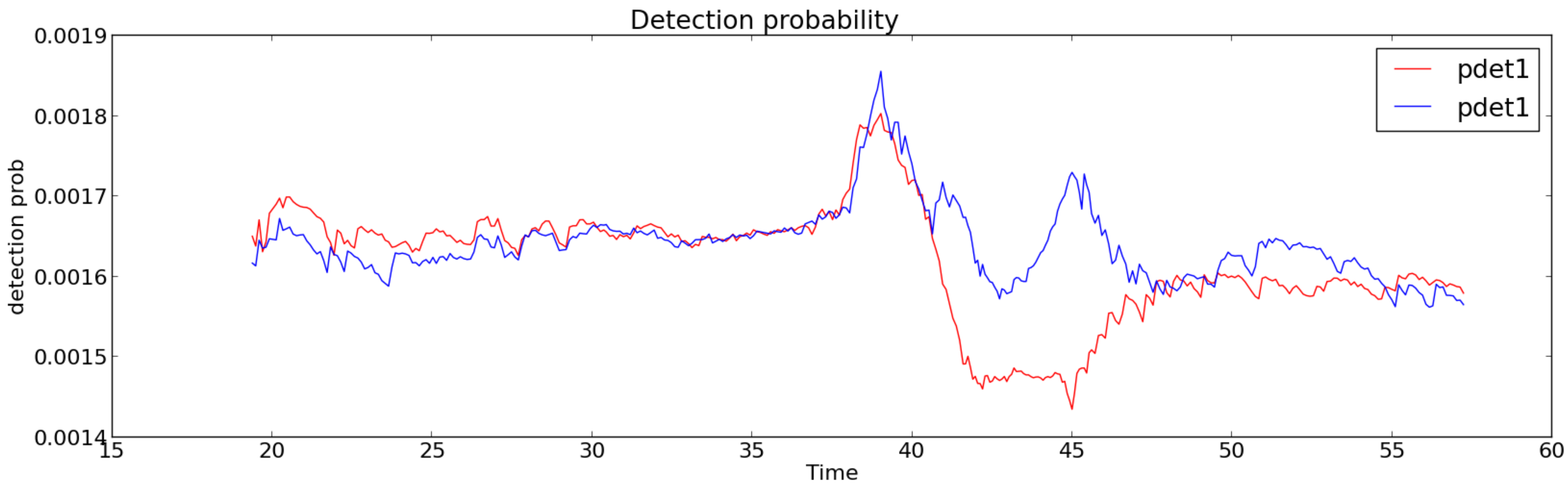


Took 5% as the maximum QBER for finite statistics analysis



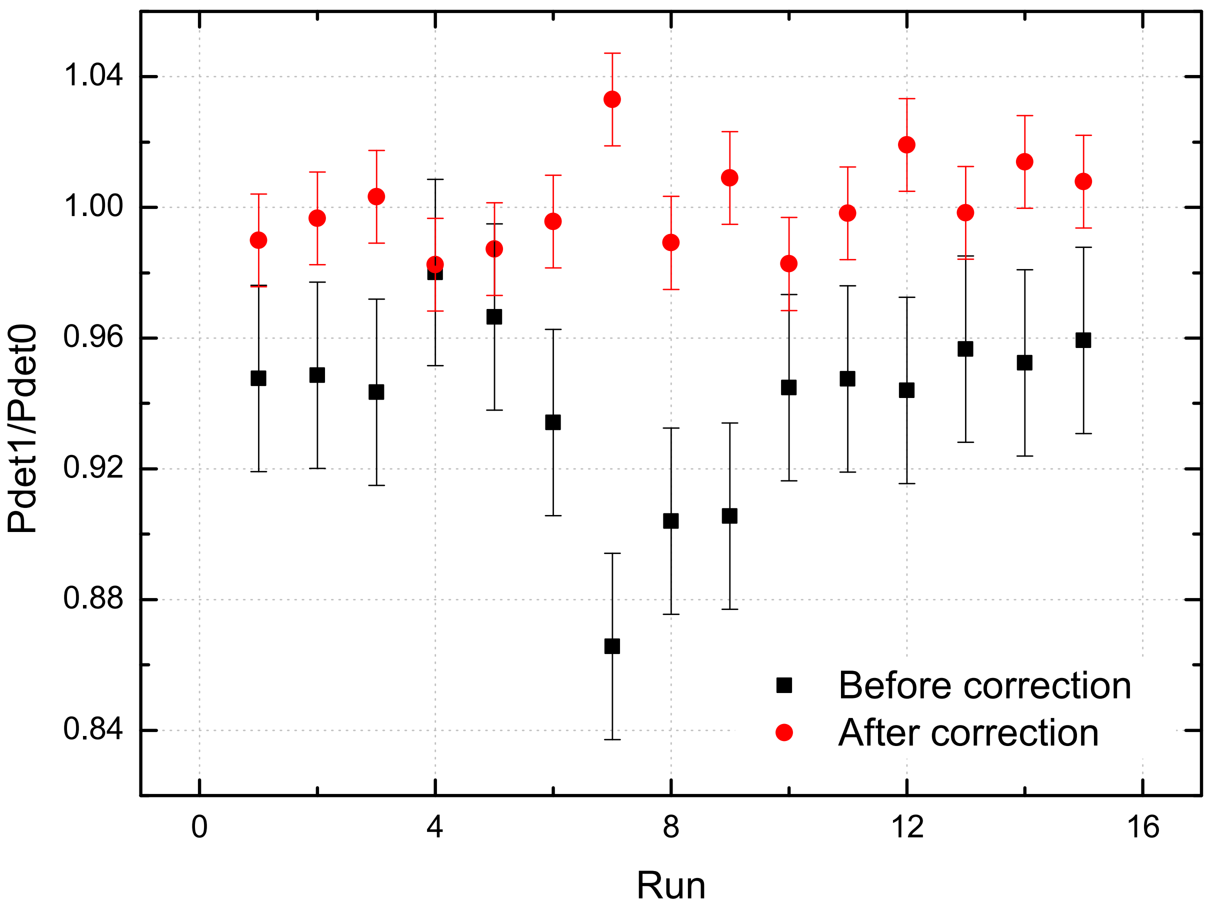
The quantum boxes (Geneva) : performances

Stability of the detection probability : Bob must monitor!



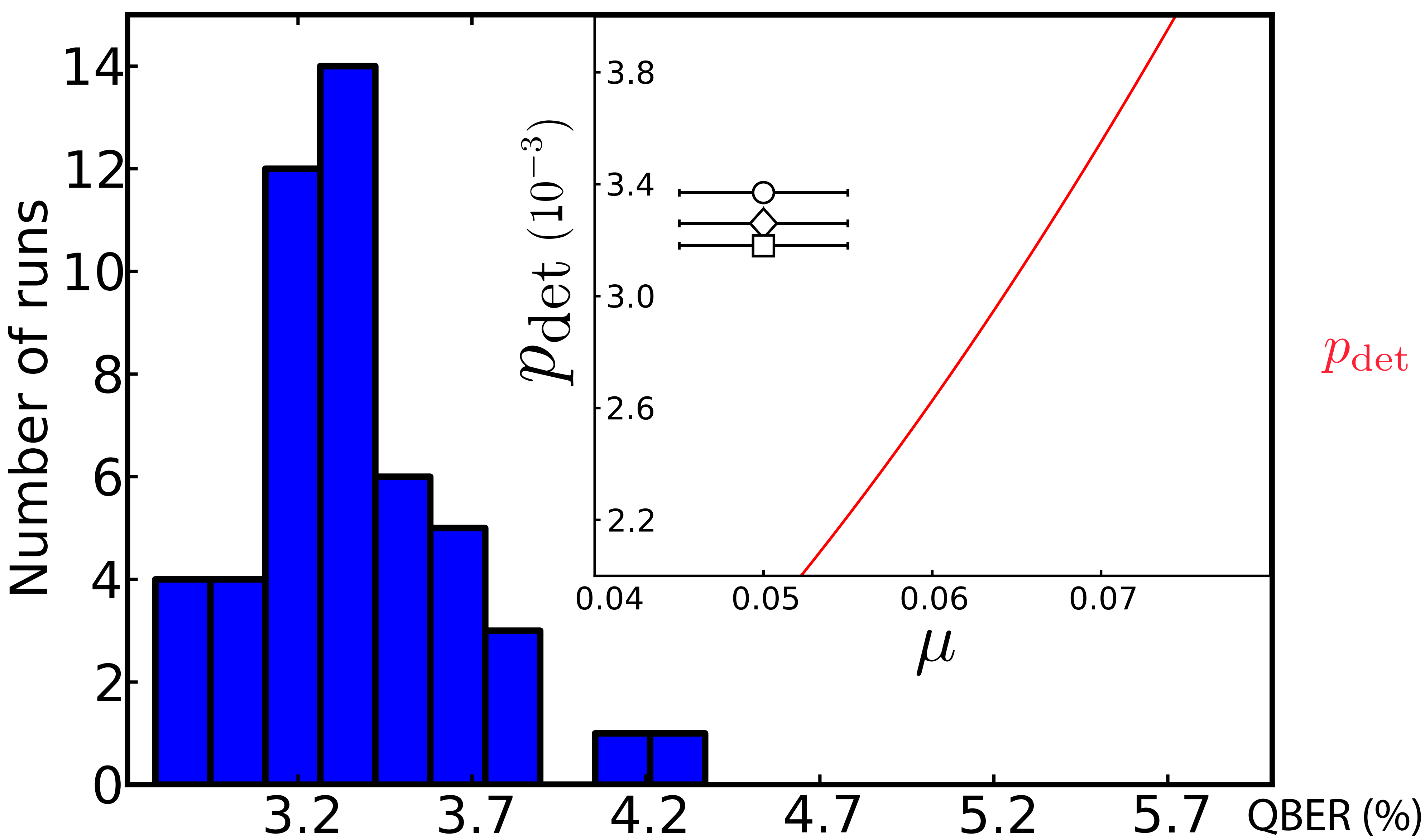
Basis detection probability mismatch: side-channel!

Software bias elimination.



The quantum boxes (Geneva) : performances

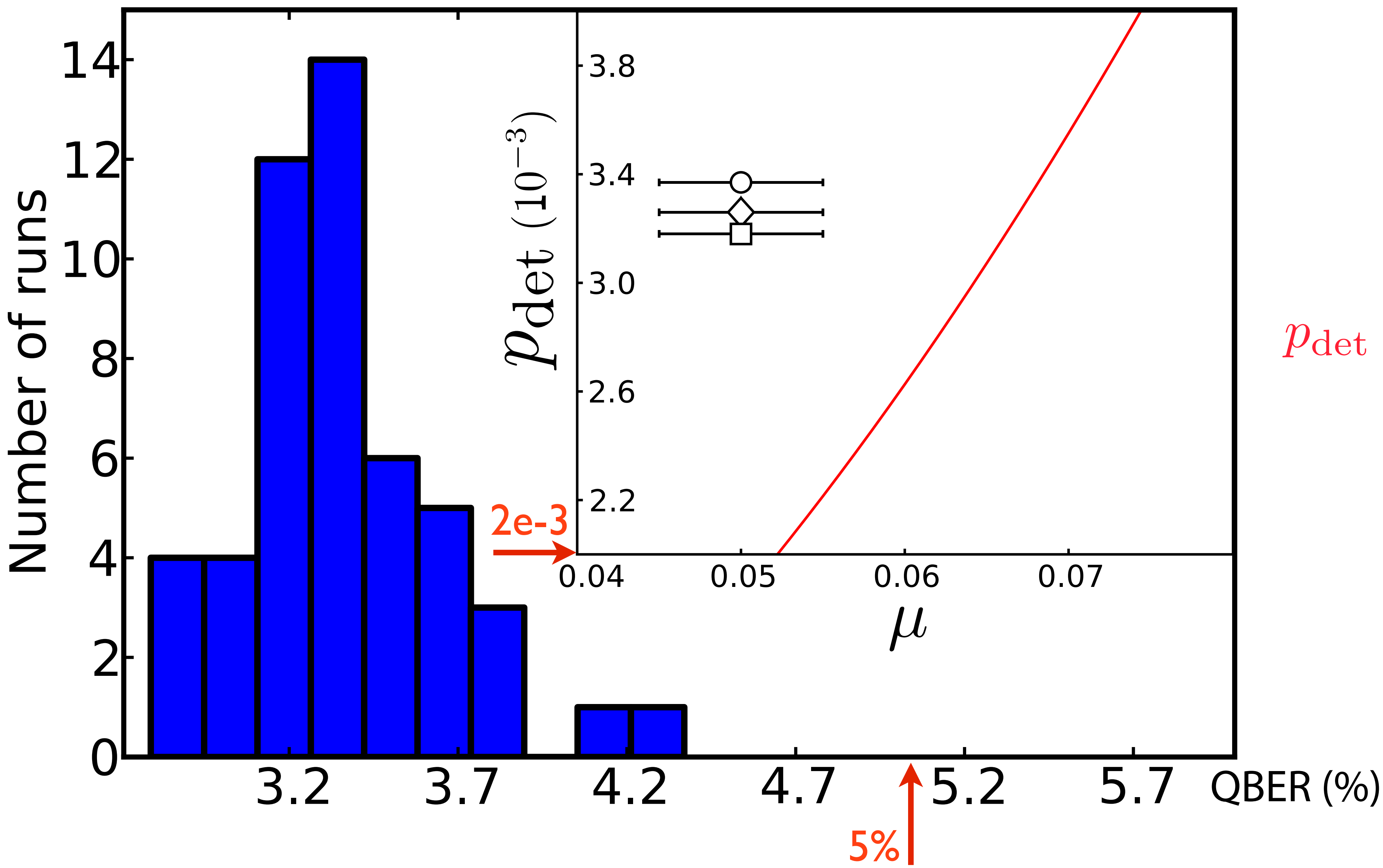
Results: 50 commitments of bit 1 from 7000 detections at Bob's



$$p_{\mathrm{det}} > \frac{1 - \mathrm{e}^{-\mu}(1+\mu)}{1 - \frac{\mathrm{QBER}}{\lambda}}$$

The quantum boxes (Geneva) : performances

Results: 50 commitments of bit 1 from
7000 detections at Bob's



$$p_{\rm det} > \frac{1 - {\rm e}^{-\mu}(1+\mu)}{1 - \frac{\rm QBER}{\lambda}}$$

Security parameter

$$\epsilon \leq 5.5 \times 10^{-8}$$

Summary and outlook

- First implementation of bit commitment using quantum communication and special relativity
- Closing on the maximum commitment time allowed on the surface of the Earth

- Possible extensions for sustained commitments with constant communication at each round? (Kent'05)

UNIVERSITÉ DE GENÈVE

NUS National University of Singapore

UNIVERSITY OF CAMBRIDGE

PI

QSIT Quantum Science and Technology
National Centre of Competence in Research

IDQ FROM VISION TO TECHNOLOGY

OSCILLOQUARTZ