Practical relativistic bit commitment

T. Lunghi[1], J. Kaniewski[2], F. Bussières[1], R. Houlmann[1], M. Tomamichel[2], S. Wehner[2], H. Zbinden[1]

[1]Group of Applied Physics, University of Geneva, Switzerland
[2]Centre for Quantum Technologies, National University of Singapore, Singapore

QCrypt'14, Paris, France
1 September 2014

UNIVERSITÉ DE GENÈVE

Centre for Quantum Technologies
National University of Singapore

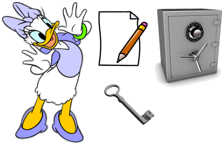
Outline

Outline

- What is a **commitment scheme**?
- Why **relativistic**?
- **Short story** of relativistic bit commitment
- **Two-round** protocol by Simard (limited commitment time)
- A new **multi-round** protocol (arbitrarily long commitment)
- Two and more rounds **in practice**

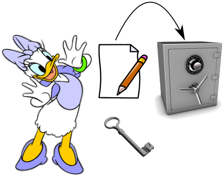
Commitment scheme – ideal functionality

Commit phase



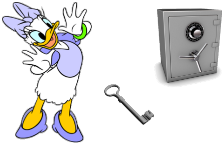
Commitment scheme – ideal functionality

Commit phase



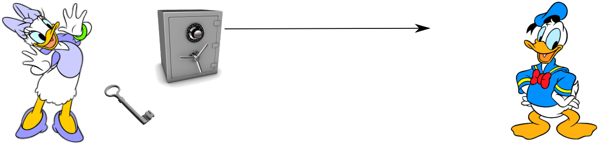
Commitment scheme – ideal functionality

Commit phase



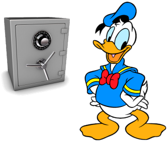
Commitment scheme – ideal functionality

Commit phase



Commitment scheme – ideal functionality

Commit phase



Commitment scheme – ideal functionality

Commit phase

Open phase

Commitment scheme – ideal functionality

Commit phase

Open phase

Commitment scheme – ideal functionality

Commit phase

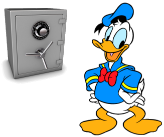
Open phase

Commitment scheme – ideal functionality

Commit phase

Open phase

Commitment scheme – cheating objectives

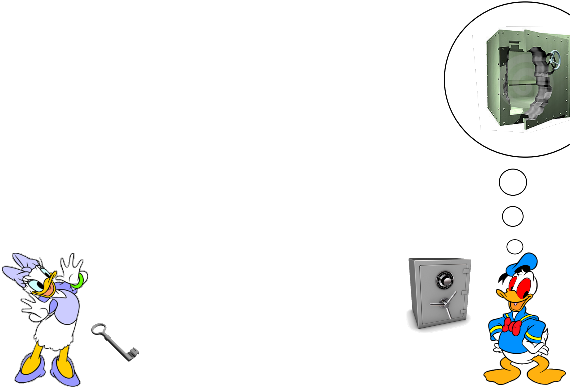


The commit phase is over...

Commitment scheme – cheating objectives

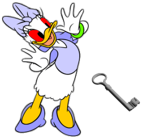
Bob goes mad!

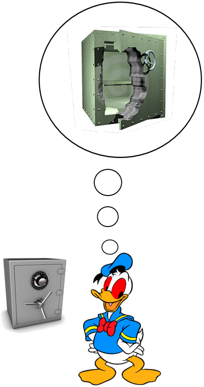
Commitment scheme – cheating objectives



He wants to break the safe and read the message!

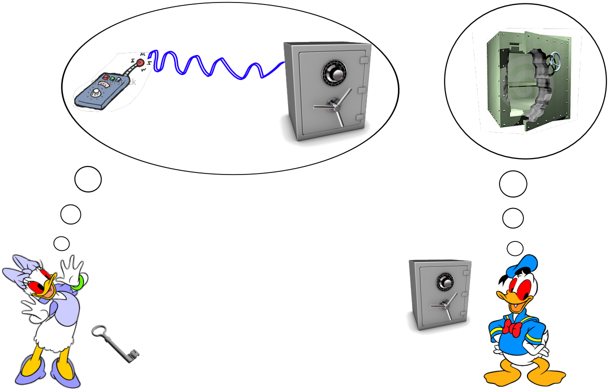
Commitment scheme – cheating objectives





Alice goes mad!

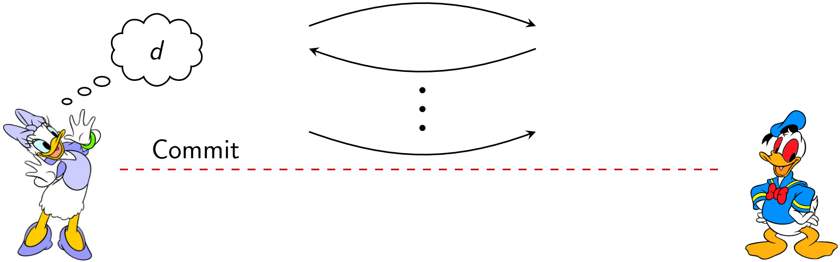
Commitment scheme – cheating objectives



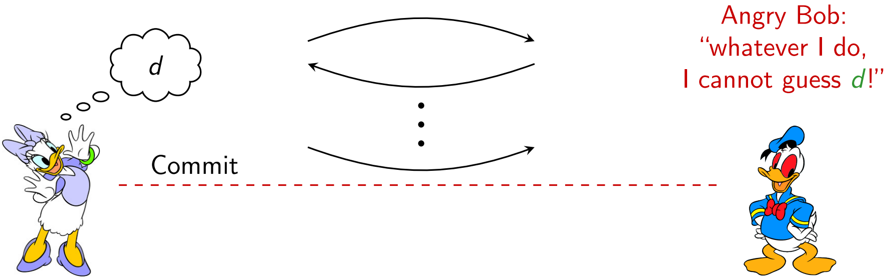
She wants to influence the message and change her commitment!

Bit commitment – security models

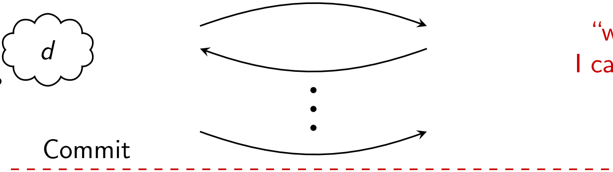
Bit commitment – security models



Bit commitment – security models



Bit commitment – security models

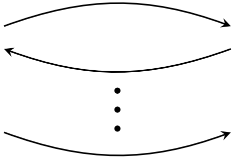


Angry Bob:
"whatever I do,
I cannot guess d!"

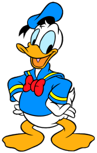
Goal:
transcripts for
$d = 0$ and $d = 1$
should be
indistinguishable

Bit commitment – security models

Angry Alice:
"don't want
to commit!"



Commit



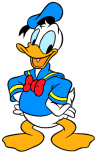
Bit commitment – security models

Angry Alice:
"don't want
to commit!"

Commit

Open

$d, \ldots$



Cheating:
$\exists$ "generic" commit
strategy s.t. Alice can later
open both $d = 0$ and $d = 1$
with (reasonably)
high probabilities

Bit commitment – security models

Security for honest Bob as a game

1. Alice performs a **generic commit strategy**
2. Alice is **challenged** to open one of the bits with equal probabilities
3. Alice wins iff Bob **accepts** the commitment

Bit commitment – security models

Security for honest Bob as a game

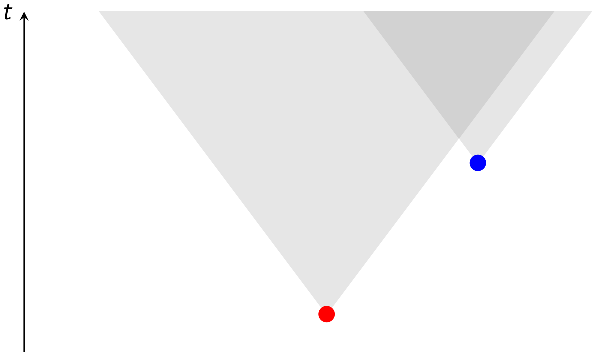
1. Alice performs a generic commit strategy
2. Alice is challenged to open one of the bits with equal probabilities
3. Alice wins iff Bob accepts the commitment

Want: $\mathrm{p_{win}} \leq \frac{1}{2} + \varepsilon$ for all strategies of dishonest Alice
Ideally, ε should be exponentially small in number of bits exchanged

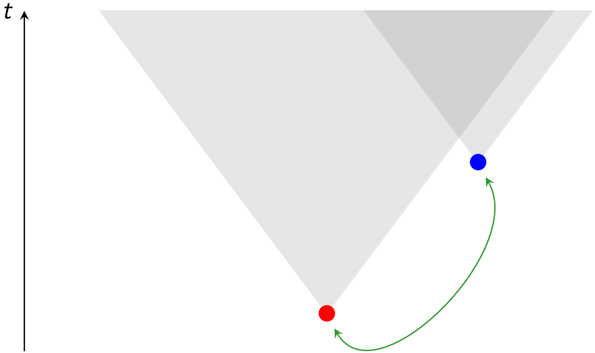
[Note that $2\,\mathrm{p_{win}} = p_0 + p_1$ for p_d = "probability that Alice successfully unveils d"

$\implies$ equivalent to the usual requirement $p_0 + p_1 \leq 1 + 2\varepsilon$]

Why relativistic?

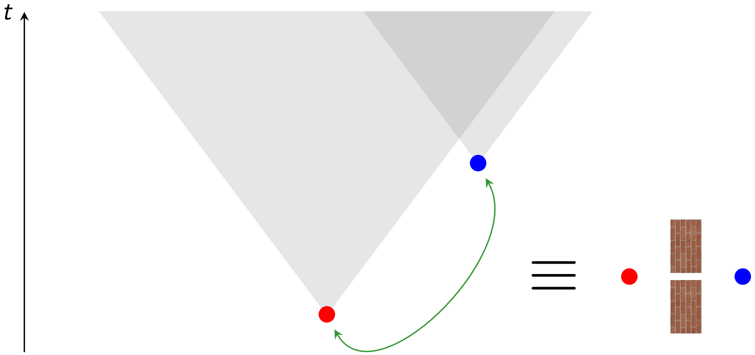


Why relativistic?



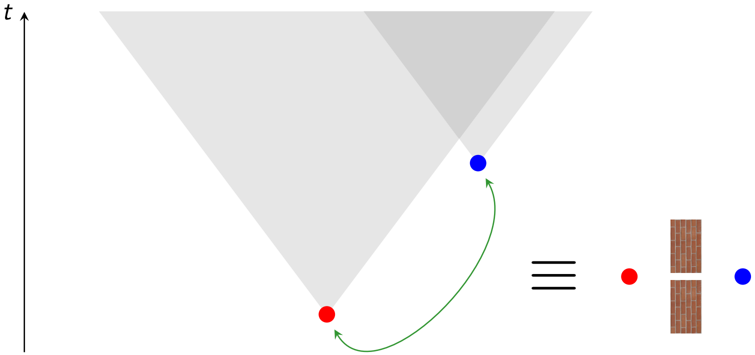
space-like separated $\implies$ no communication

Why relativistic?



space-like separated $\implies$ no communication

Why relativistic?

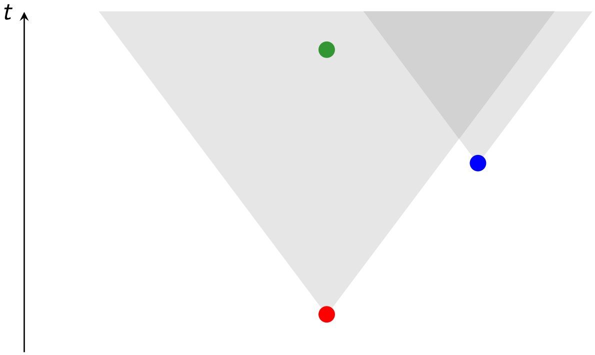


space-like separated $\implies$ no communication

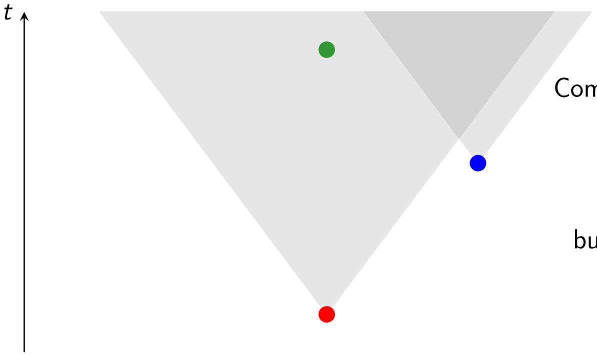
For two rounds (classical or quantum)
Relativistic $\equiv$ Two isolated provers

$\implies$ compact, tractable description

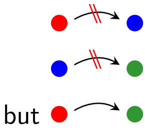
More rounds?



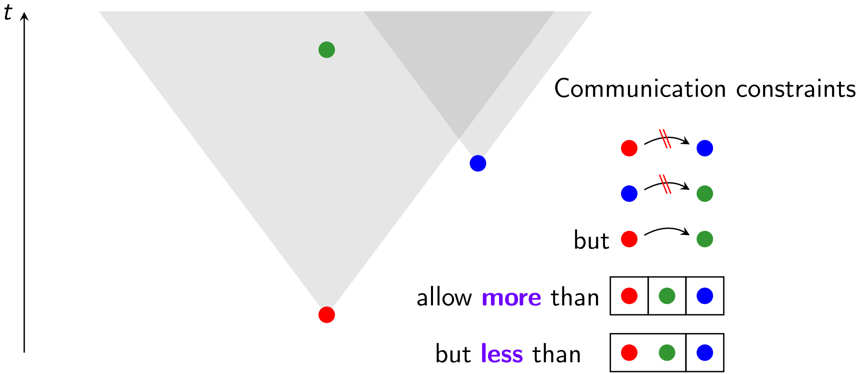
More rounds?



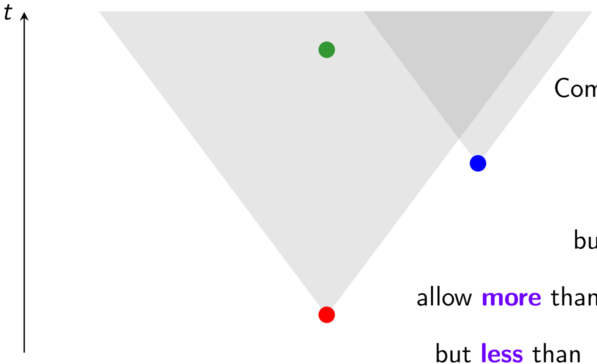
Communication constraints



More rounds?


t
Communication constraints
but
allow **more** than
but **less** than

More rounds?

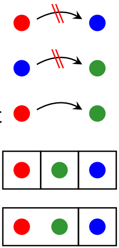


Communication constraints

but

allow **more** than

but **less** than



No **simple** description in terms of non-communication models...

Short story of relativistic bit commitment

Short story of relativistic bit commitment

- First **two-round** protocol proposed by Ben-Or et al. in 1988; established security against classical adversaries
- First **multi-round** protocol proposed by Kent in 1999 arbitrary length but exponential blow-up in communication
- Further combined with a compression scheme to achieve constant communication rate [Kent'05]
- Simard in 2007 simplified the protocol by Ben-Or et al. and proved security against a restricted class of quantum attacks
- Two (two-round) quantum protocols by Kent in 2011 and 2012 rely on inherently **quantum** features (no-cloning/monogamy of correlations)

How did it all start?

How did it all start?

Goal: a multi-round protocol which

- has a **rigorous** security proof
- can be **implemented** using currently available technology
- can achieve commitment time **longer than 42ms**

How did it all start?

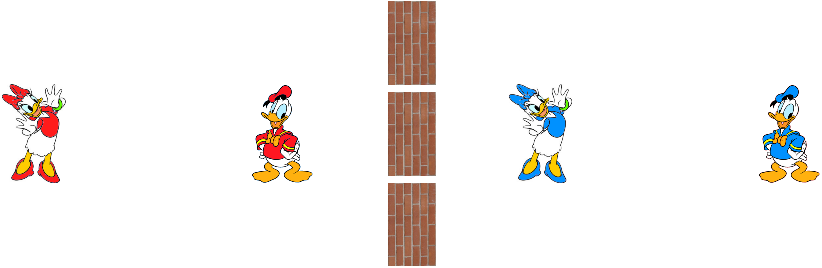
Goal: a multi-round protocol which

- has a **rigorous** security proof
- can be **implemented** using currently available technology
- can achieve commitment time **longer than 42ms**

Our contributions:

- Security of Simard's protocol against the **most general quantum attack**
- New multi-round protocol and a **security proof** against classical adversaries
- Experimental **implementation** of both schemes

Two-round protocol [Simard]



a – private randomness of Alice
b – private randomness of Bob
$a, b \in_R \{0,1\}^n$

Two-round protocol [Simard]

Commit

b

$y_1 = d \cdot b \oplus a$

bitwise AND

XOR

$0 \cdot b = 0$

$1 \cdot b = b$

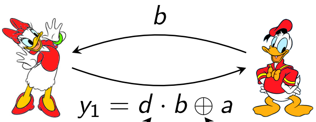
a – private randomness of Alice

b – private randomness of Bob

$a, b \in_R \{0,1\}^n$

Two-round protocol [Simard]

Commit



$y_1 = d \cdot b \oplus a$

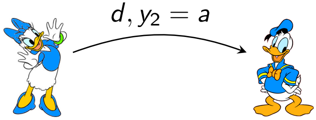
bitwise AND

XOR

$0 \cdot b = 0$
$1 \cdot b = b$

a – private randomness of Alice
b – private randomness of Bob
$a, b \in_R \{0,1\}^n$

Open



accept iff $y_1 \oplus y_2 = d \cdot b$

Two-round protocol [Simard]

Commit

b

$y_1 = d \cdot b \oplus a$

bitwise AND

XOR

$0 \cdot b = 0$

$1 \cdot b = b$

a – private randomness of Alice

b – private randomness of Bob

$a, b \in_R \{0,1\}^n$

Open

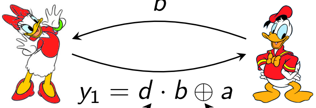
$d, y_2 = a$

accept iff $y_1 \oplus y_2 = d \cdot b$

Security for **honest Alice** guaranteed by the XOR

Two-round protocol [Simard]

Commit



b

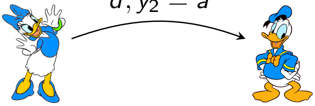
$y_1 = d \cdot b \oplus a$

bitwise AND XOR

$0 \cdot b = 0$
$1 \cdot b = b$

a – private randomness of Alice
b – private randomness of Bob
$a, b \in_R \{0,1\}^n$

Open



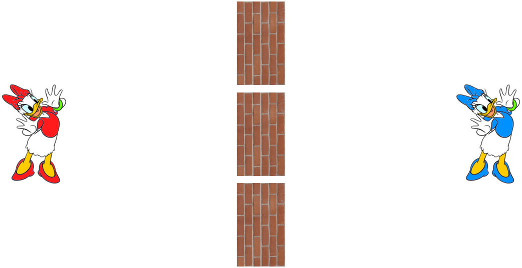
$d, y_2 = a$

accept iff $y_1 \oplus y_2 = d \cdot b$

Security for **honest Alice** guaranteed by the XOR

Security for **honest Bob** more complicated...

Two-round protocol – honest Bob

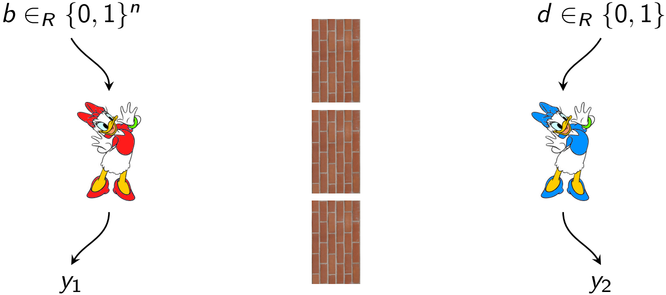


Two-round protocol – honest Bob

$b \in_R \{0,1\}^n$

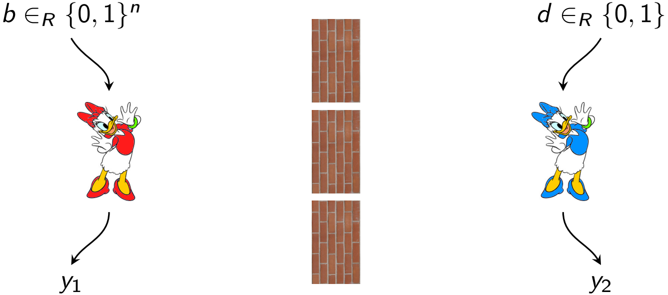
$d \in_R \{0,1\}$

Two-round protocol – honest Bob



win **iff** $y_1 \oplus y_2 = d \cdot b$

Two-round protocol – honest Bob

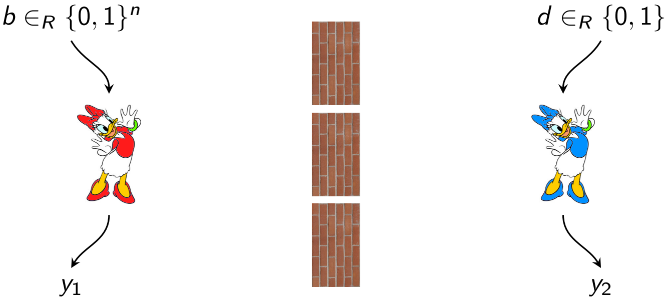


win **iff** $y_1 \oplus y_2 = d \cdot b$

Classically: $\mathrm{p_{win}} = \frac{1}{2} + \frac{1}{2^n}$

Quantumly: $\mathrm{p_{win}} \leq \frac{1}{2} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2^n}}$ [Sikora, Chailloux, Kerenidis'14]

Two-round protocol – honest Bob



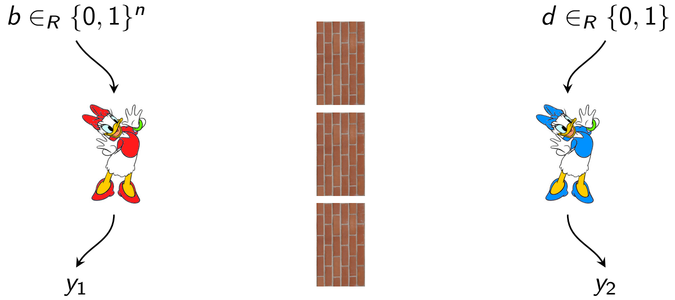
win **iff** $y_1 \oplus y_2 = d \cdot b$

Classically: $p_{\text{win}} \overset{\textbf{(tight)}}{=} \frac{1}{2} + \frac{1}{2^n}$

Quantumly: $p_{\text{win}} \leq \frac{1}{2} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2^n}}$ [Sikora, Chailloux, Kerenidis'14]

exponential decay conjectured to be (essentially) tight

Two-round protocol – honest Bob



win **iff** $y_1 \oplus y_2 = d \cdot b$

exponential decay conjectured to be (essentially) tight

Classically: $p_{\text{win}} \overset{(\textbf{tight})}{=} \frac{1}{2} + \frac{1}{2^n}$

Quantumly: $p_{\text{win}} \leq \frac{1}{2} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2^n}}$ [Sikora, Chailloux, Kerenidis'14]

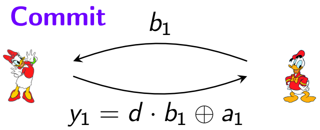
quantum-classical gap

quantum adversary **strictly more** powerful

A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must
be **space-like** separated

A new multi-round protocol

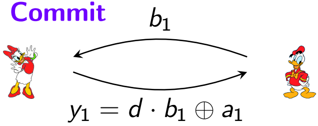


$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

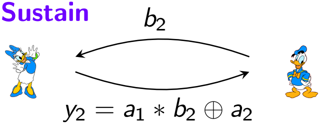
A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

Commit



Sustain



A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

Commit

$$\xleftarrow{b_1}$$
$$y_1 = d \cdot b_1 \oplus a_1$$

Sustain

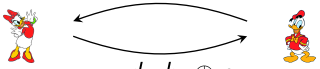
$$\xleftarrow{b_2}$$
$$y_2 = a_1 * b_2 \oplus a_2$$

finite field multiplication over $GF(2^n)$

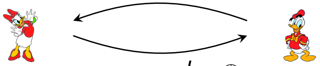
A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

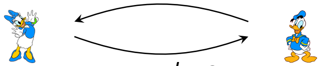
Commit



$\vdots$



Sustain

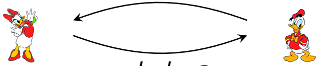


finite field multiplication over $GF(2^n)$

$\vdots$

A new multi-round protocol

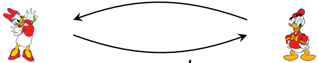
Commit b_1



$y_1 = d \cdot b_1 \oplus a_1$

$\vdots$

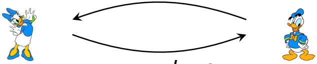
b_m



$y_m = a_{m-1} * b_m \oplus a_m$

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

Sustain b_2



$y_2 = a_1 * b_2 \oplus a_2$

finite field multiplication over $GF(2^n)$

$\vdots$

Open $d, y_{m+1} = a_m$

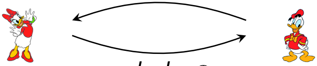
accept iff $V(d, b_1, y_1, \ldots, b_m, y_m, y_{m+1}) = 1$

A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must be **space-like** separated

Commit

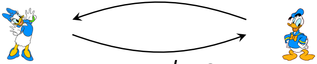
b_1



$y_1 = d \cdot b_1 \oplus a_1$

Sustain

b_2

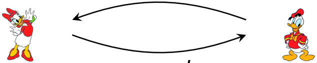


$y_2 = a_1 * b_2 \oplus a_2$

finite field multiplication over $GF(2^n)$

$\vdots$

b_m



$y_m = a_{m-1} * b_m \oplus a_m$

Open

$d, y_{m+1} = a_m$

Security for **honest Alice** guaranteed by the XOR

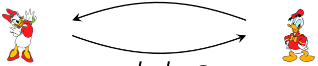
accept iff $V(d, b_1, y_1, \ldots, b_m, y_m, y_{m+1}) = 1$

A new multi-round protocol

$a_k, b_k \in_R \{0,1\}^n$
consecutive rounds must
be **space-like** separated

Commit

b_1



$y_1 = d \cdot b_1 \oplus a_1$

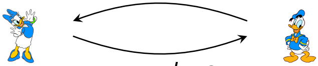
$\vdots$

b_m

$y_m = a_{m-1} * b_m \oplus a_m$

Sustain

b_2



$y_2 = a_1 * b_2 \oplus a_2$

finite field multiplication
over $GF(2^n)$

$\vdots$

Open

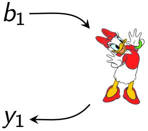
$d, y_{m+1} = a_m$

accept iff $V(d, b_1, y_1, \ldots, b_m, y_m, y_{m+1}) = 1$

Security for **honest Alice**
guaranteed by the XOR

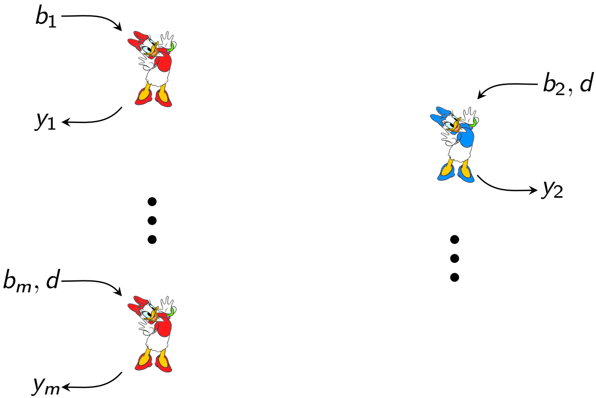
Security for **honest Bob**
more complicated...

A new multi-round protocol – honest Bob

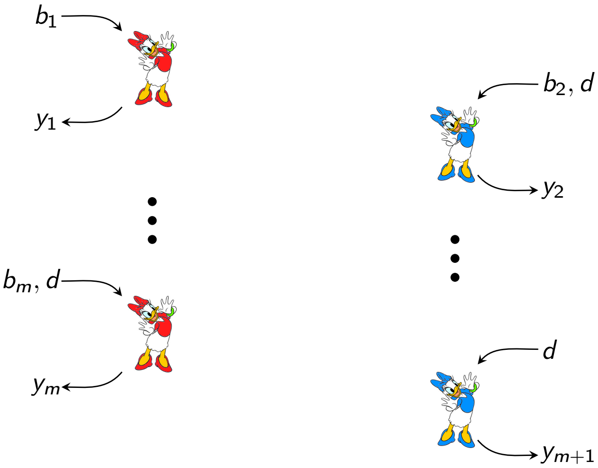


A new multi-round protocol – honest Bob

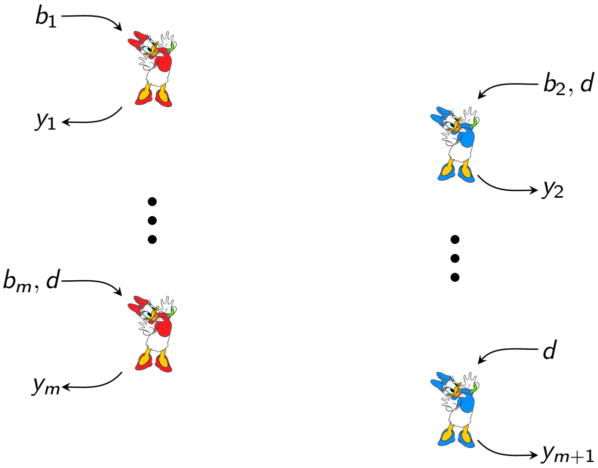
A new multi-round protocol – honest Bob



A new multi-round protocol – honest Bob

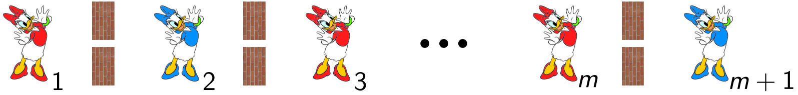


A new multi-round protocol – honest Bob

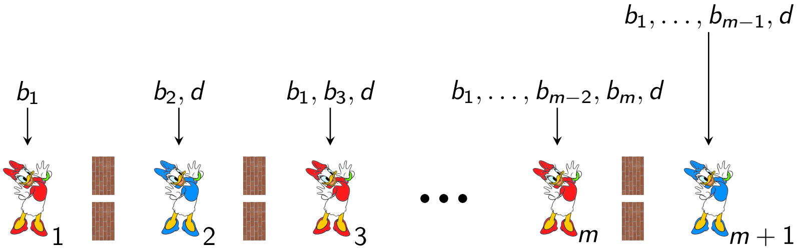


Quantumly: causal constraints make the analysis very hard...
Classically: **shared randomness** doesn't help; **deterministic** strategies "flatten" the causal structure to give a **multi-prover** model

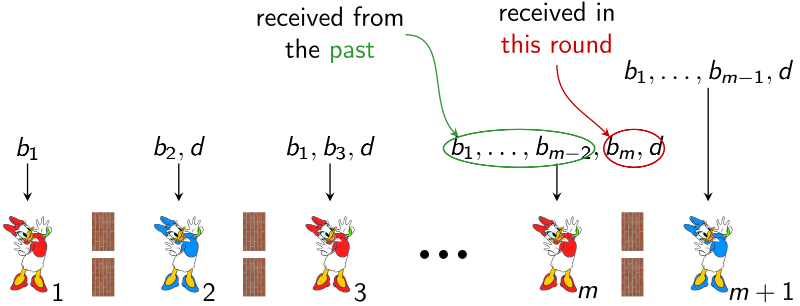
A new multi-round protocol – honest Bob



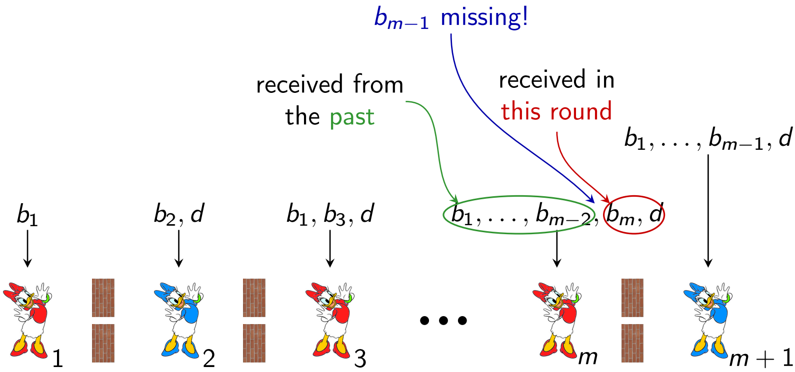
A new multi-round protocol – honest Bob



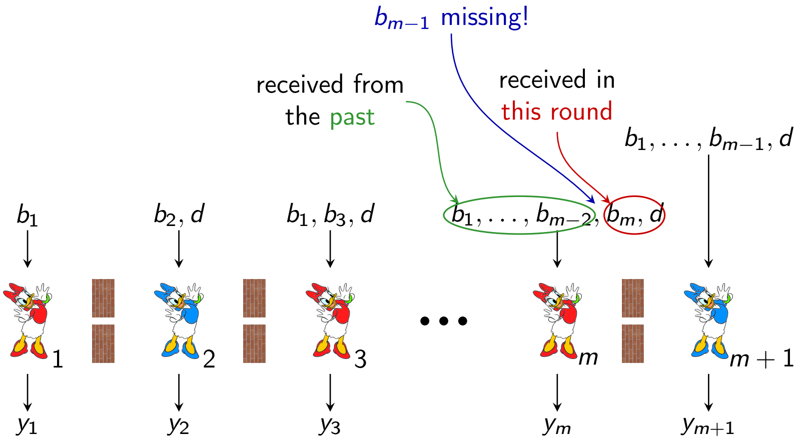
A new multi-round protocol – honest Bob



A new multi-round protocol – honest Bob

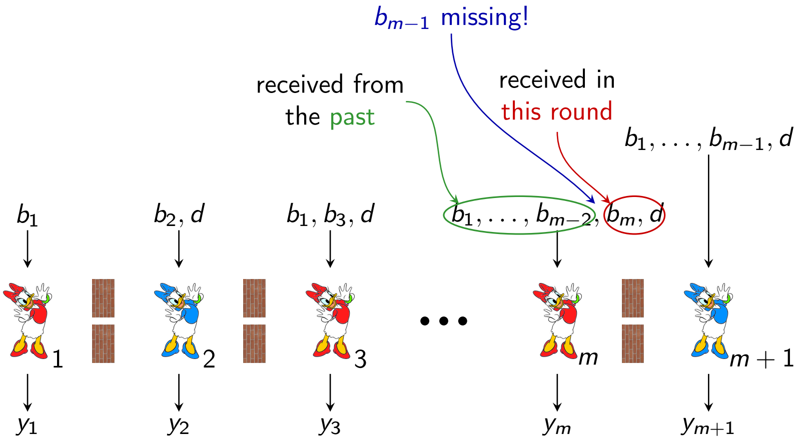


A new multi-round protocol – honest Bob



check whether $V(d, b_1, y_1, \dots, b_m, y_m, y_{m+1}) = 1$

A new multi-round protocol – honest Bob



check whether $V(d, b_1, y_1, \ldots, b_m, y_m, y_{m+1}) = 1$

this reduction is **exact** – same optimal winning probability

A new multi-round protocol – honest Bob

Conclusions:

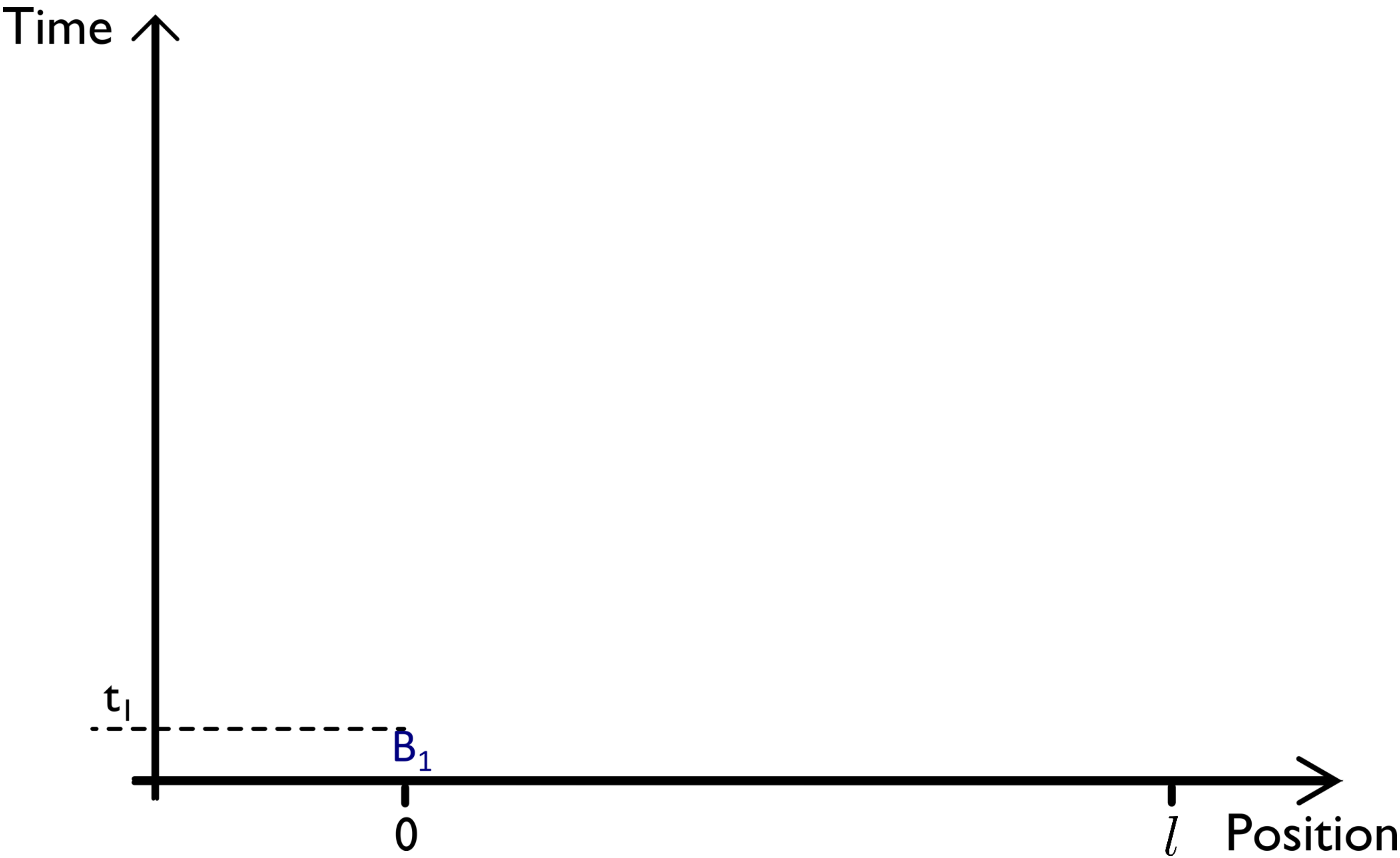
- End up with a **complicated** game of $m + 1$ **non-communicating** players; exact cheating probability is hard to calculate.
- Can be relaxed to the problem of computing a certain function in the **"Number on the Forehead"** model.
- This class of problems is well-studied in computer science and has profound implications. It is believed to be **hard** (which would imply that cheating is **difficult**) but only **weak** bounds are known.
- Equivalent to counting the **number of zeroes** of a certain family of **multivariate polynomial** over finite field $GF(2^n)$.

A new multi-round protocol – honest Bob

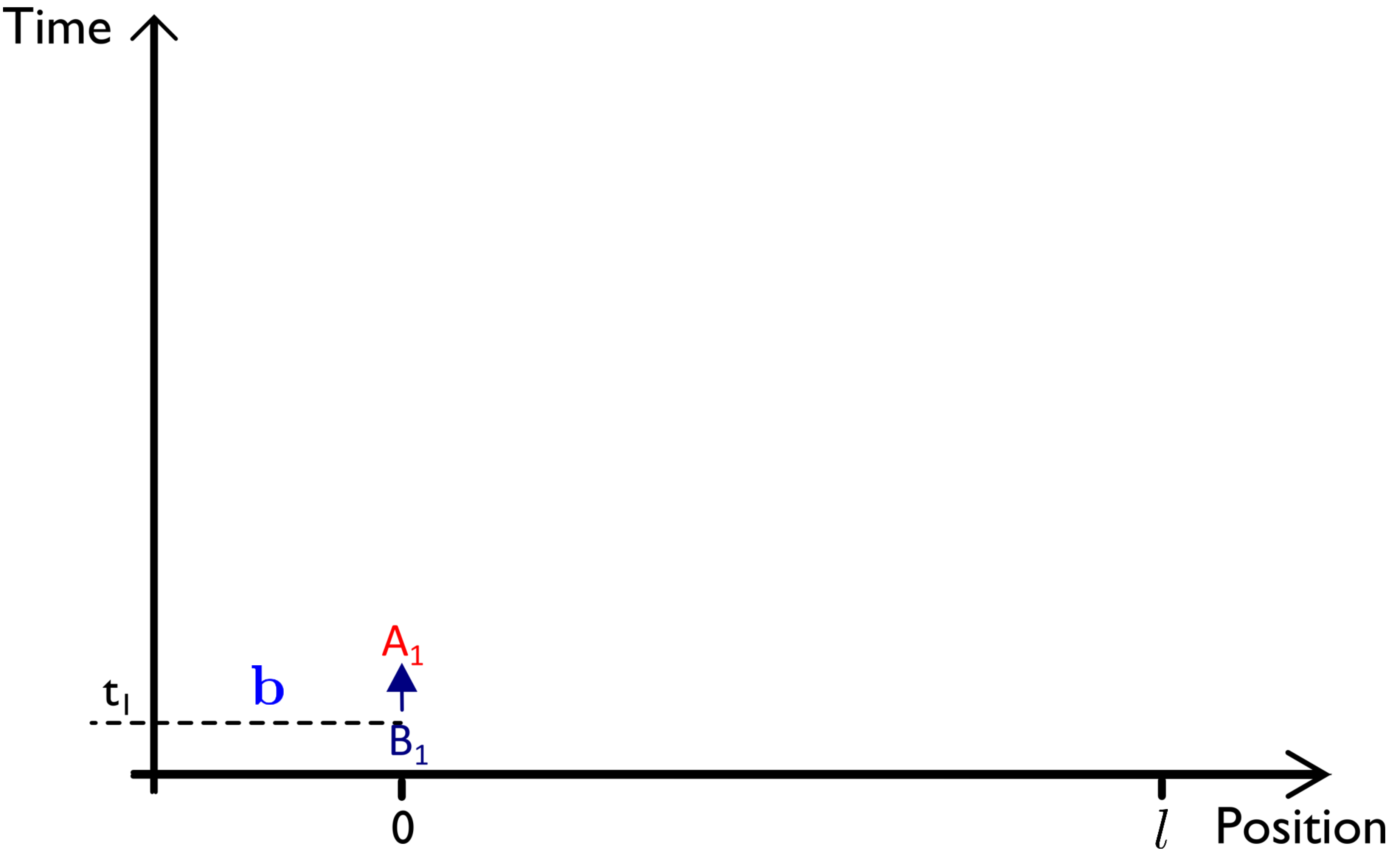
Final result: Security for honest Bob with $\varepsilon \approx 2^{-n/2^m}$.

- Security **deteriorates drastically** as m increases.
- Looks very similar to **communication complexity lower bounds** for this model: $\Omega(\frac{n}{2^m})$.
- In **principle**, an arbitrary long commitment is possible (at the price of very large n).
- In **practice**, technology puts a limit on n so the commitment time is limited.

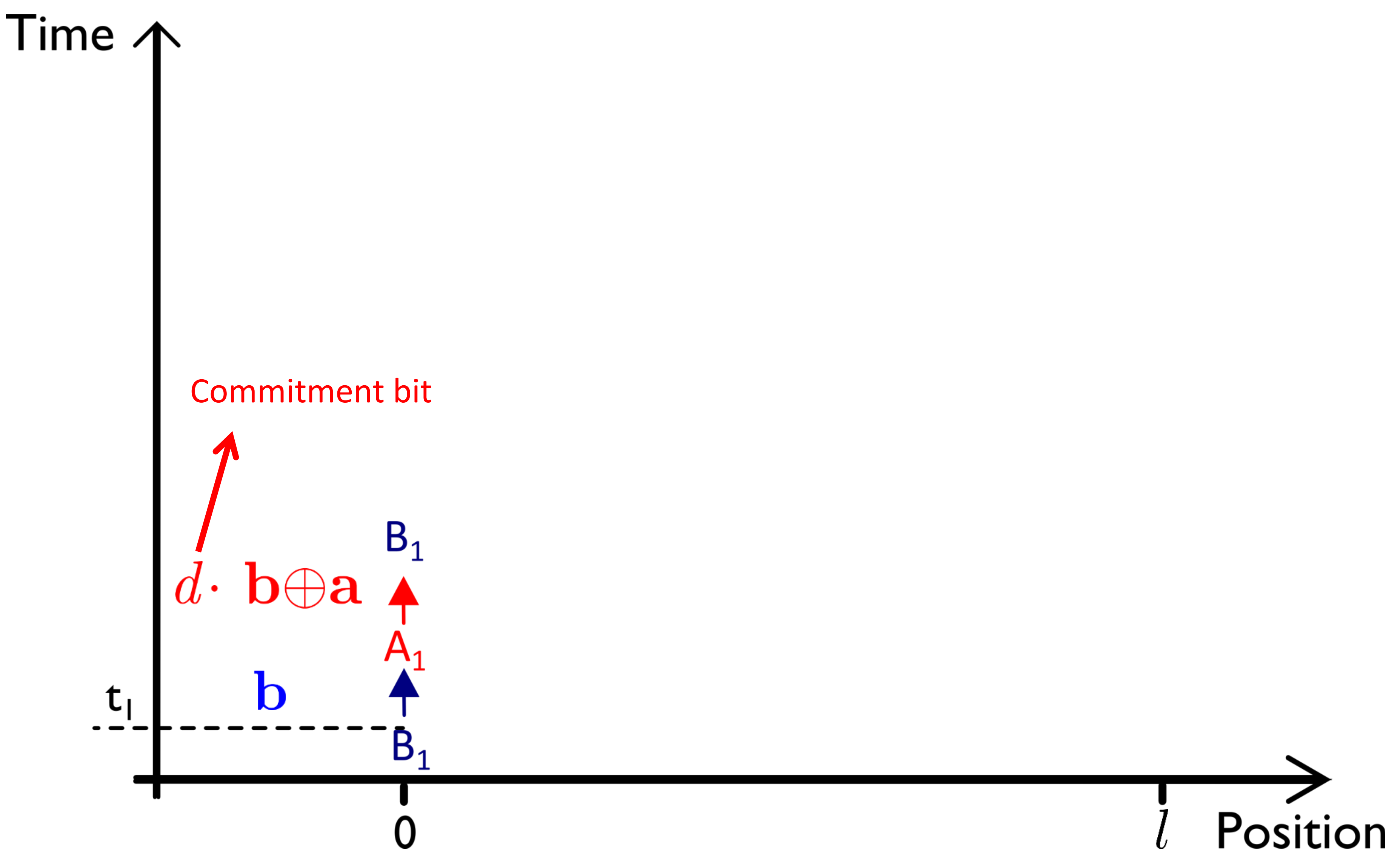
Two-round experiment



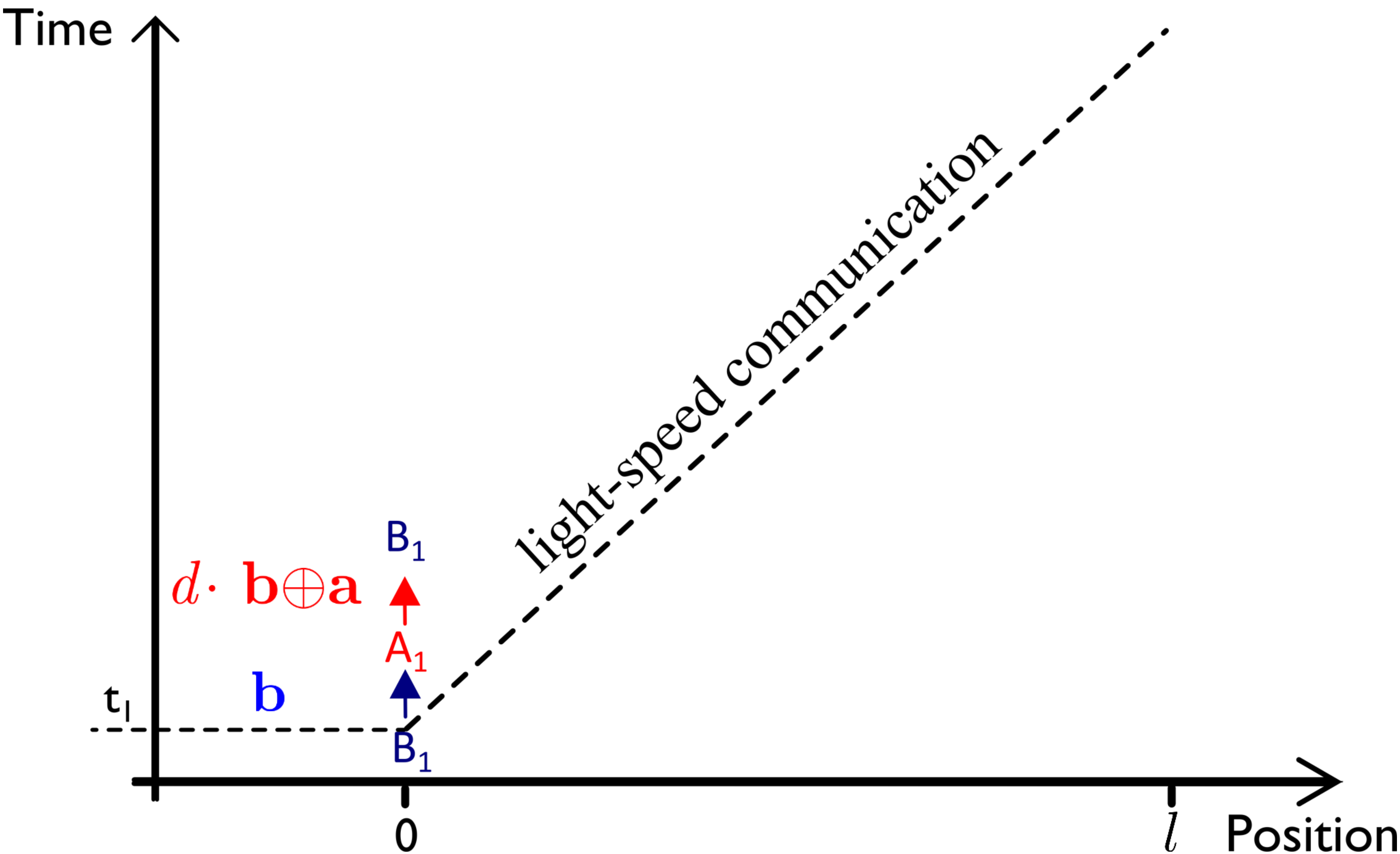
Two-round experiment



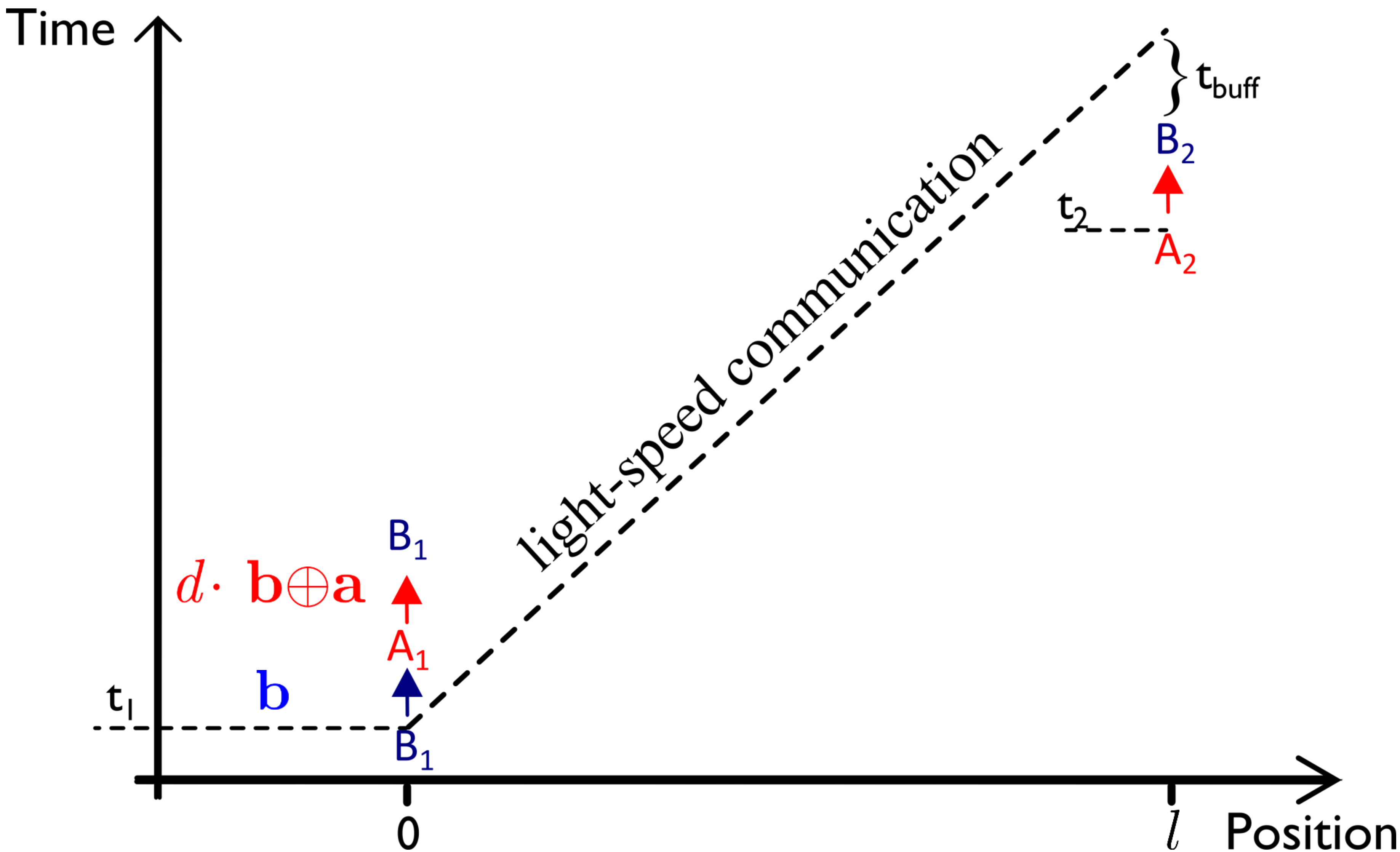
Two-round experiment



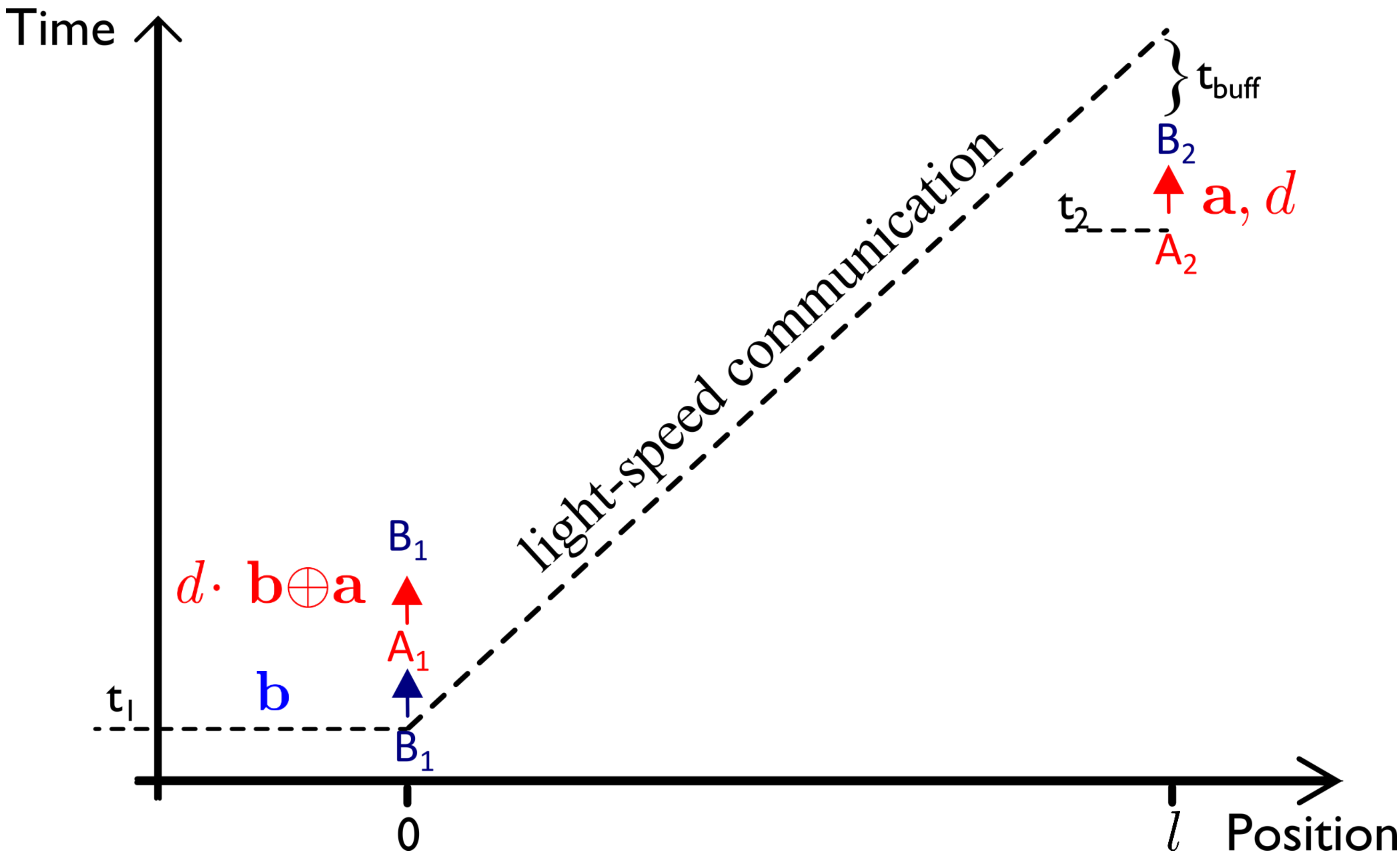
Two-round experiment



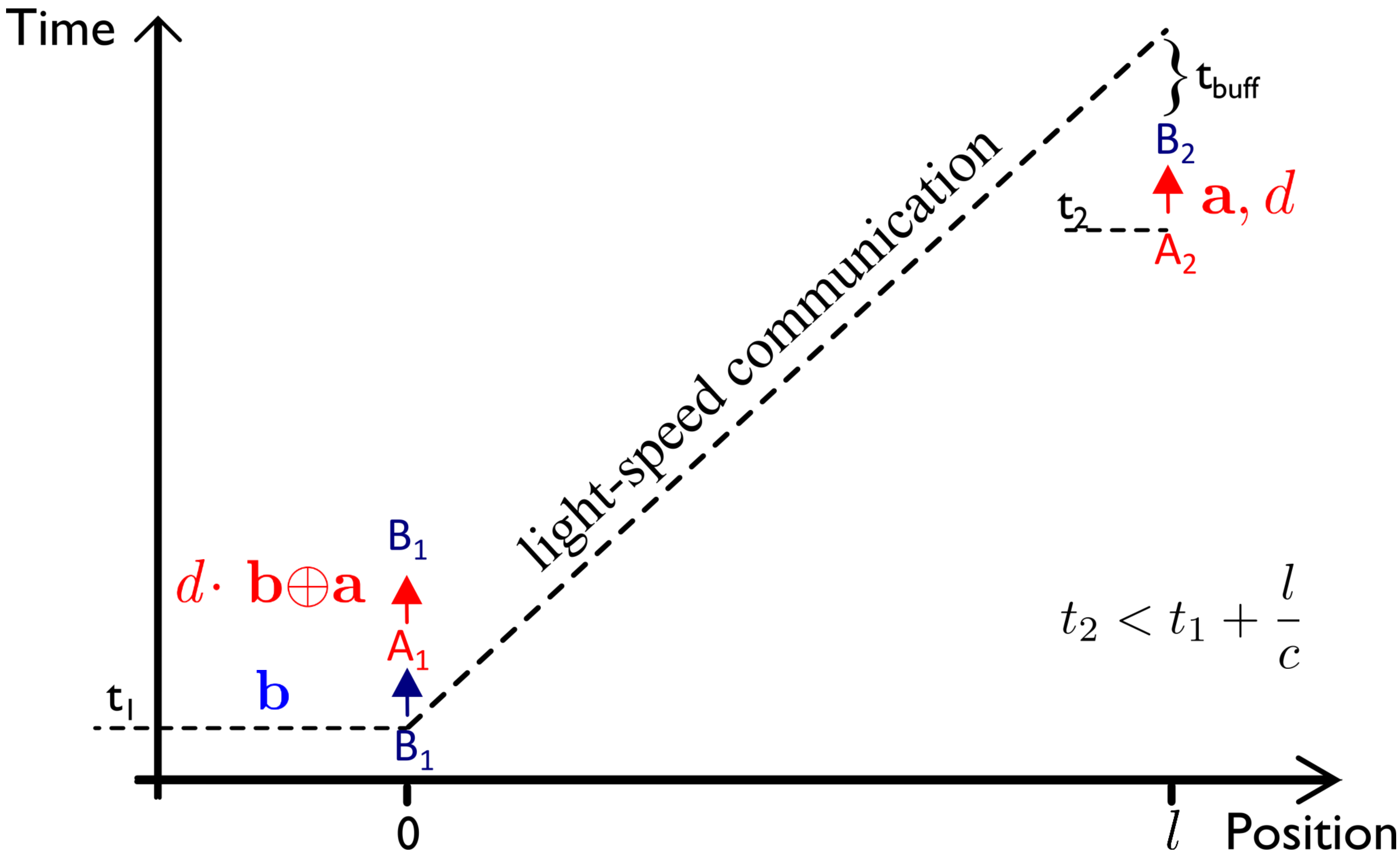
Two-round experiment



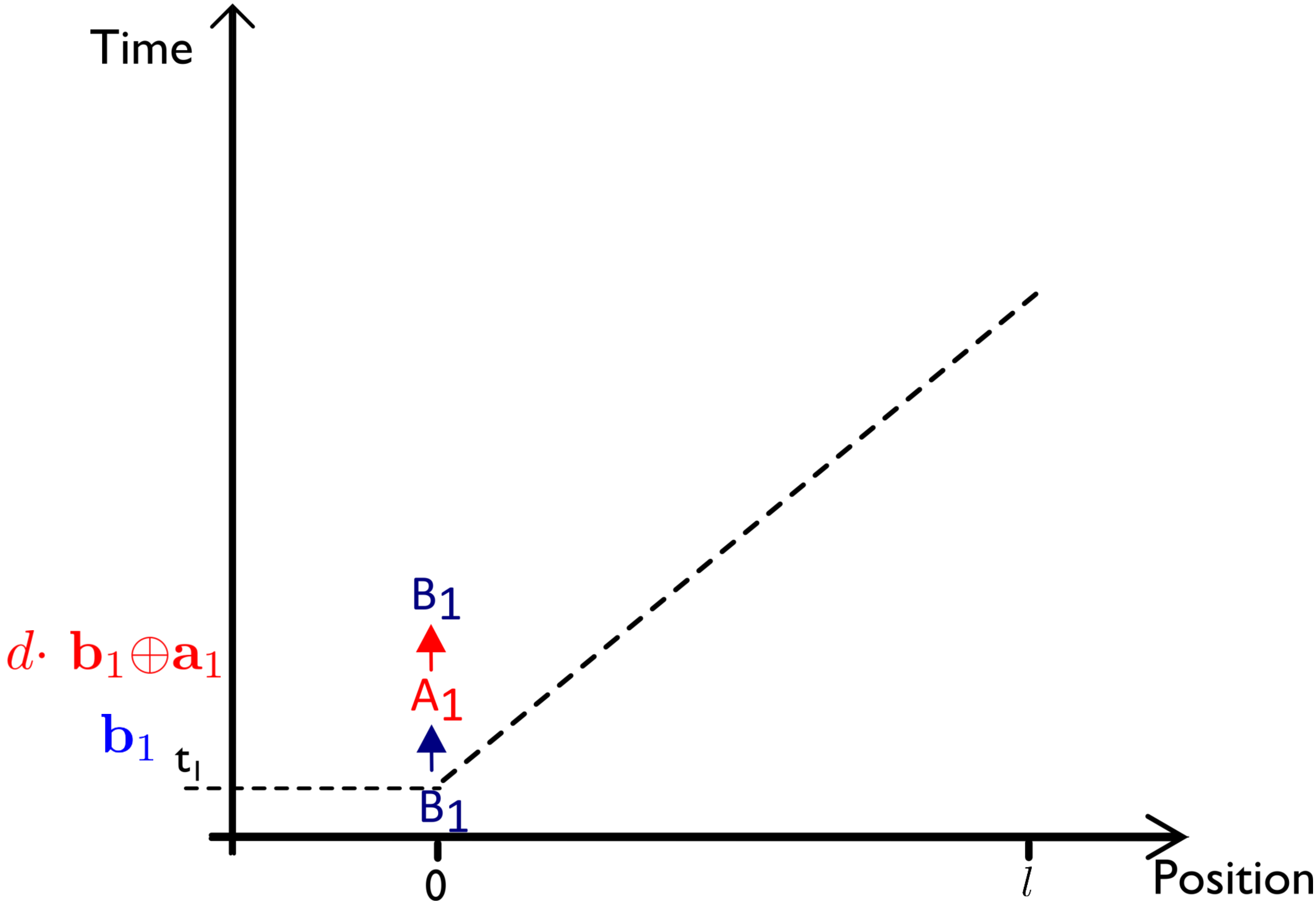
Two-round experiment



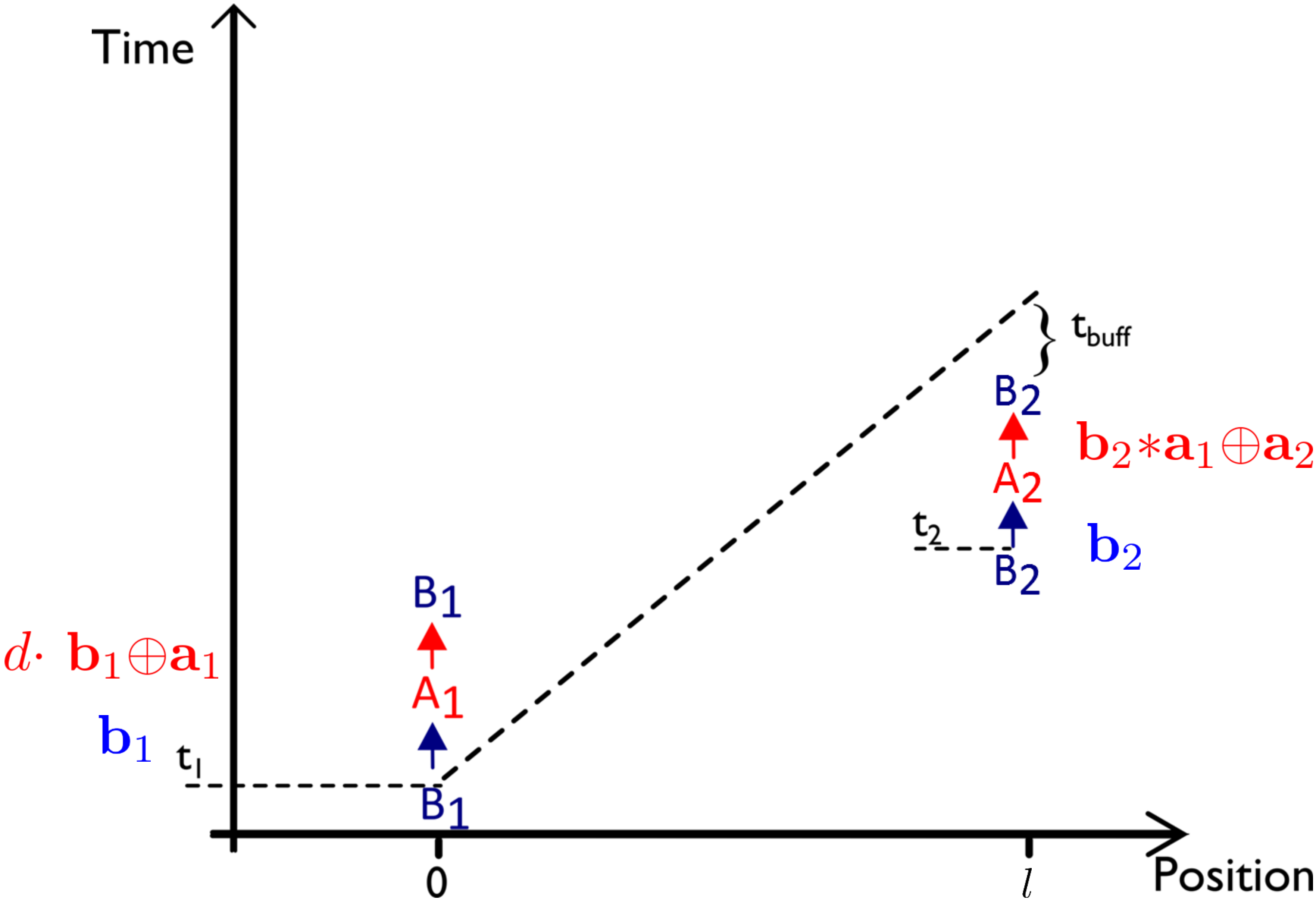
Two-round experiment



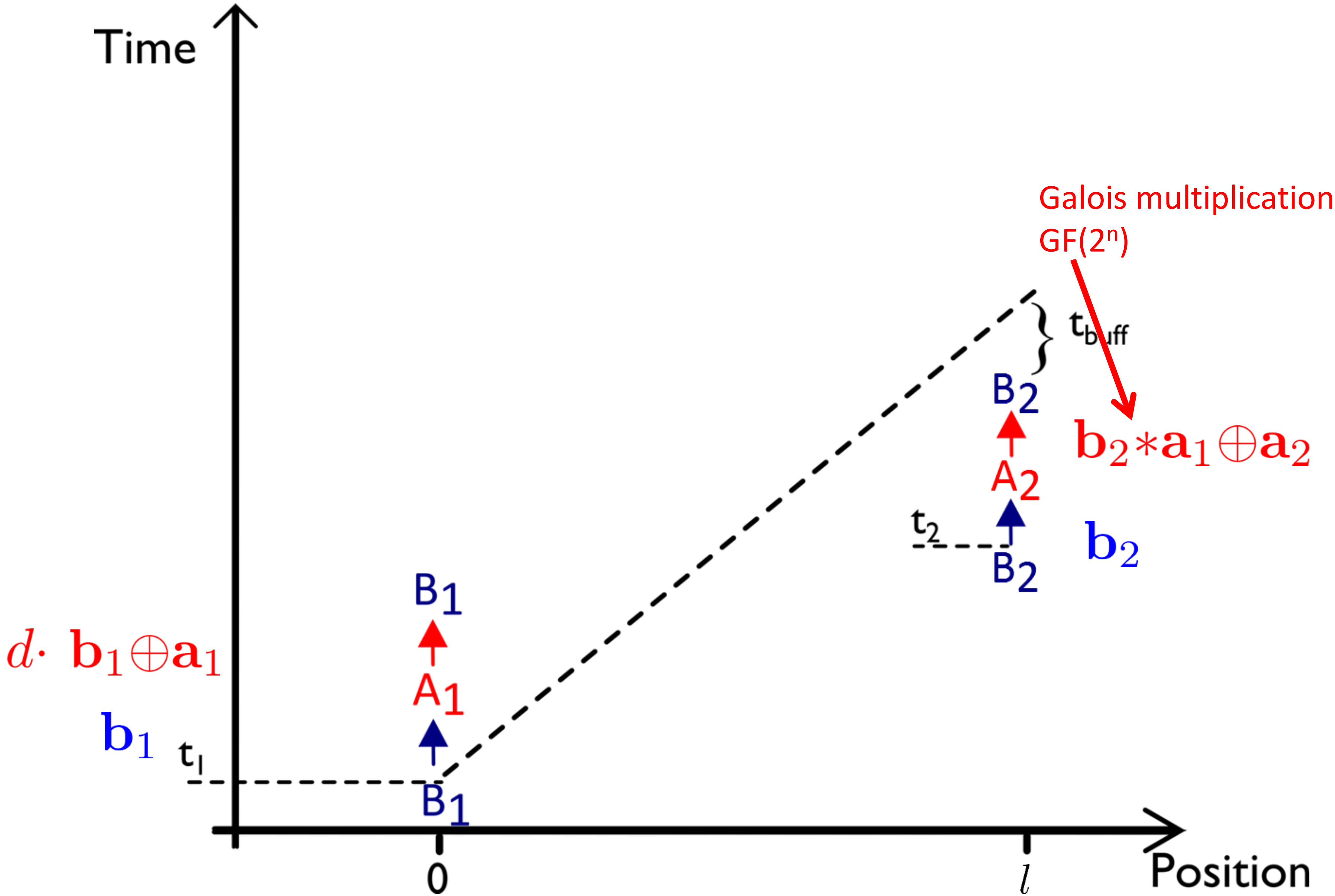
Multi-round experiment



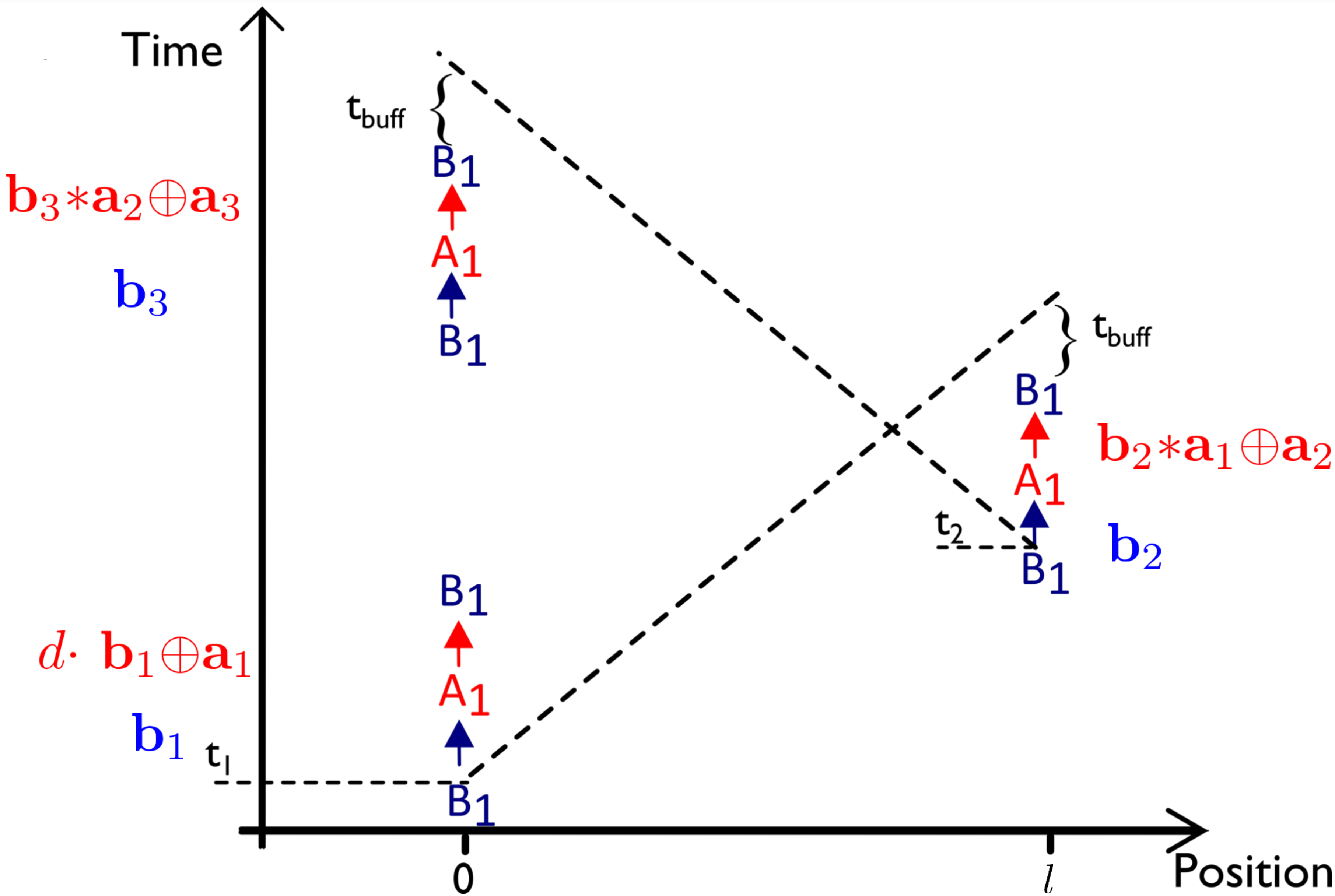
Multi-round experiment



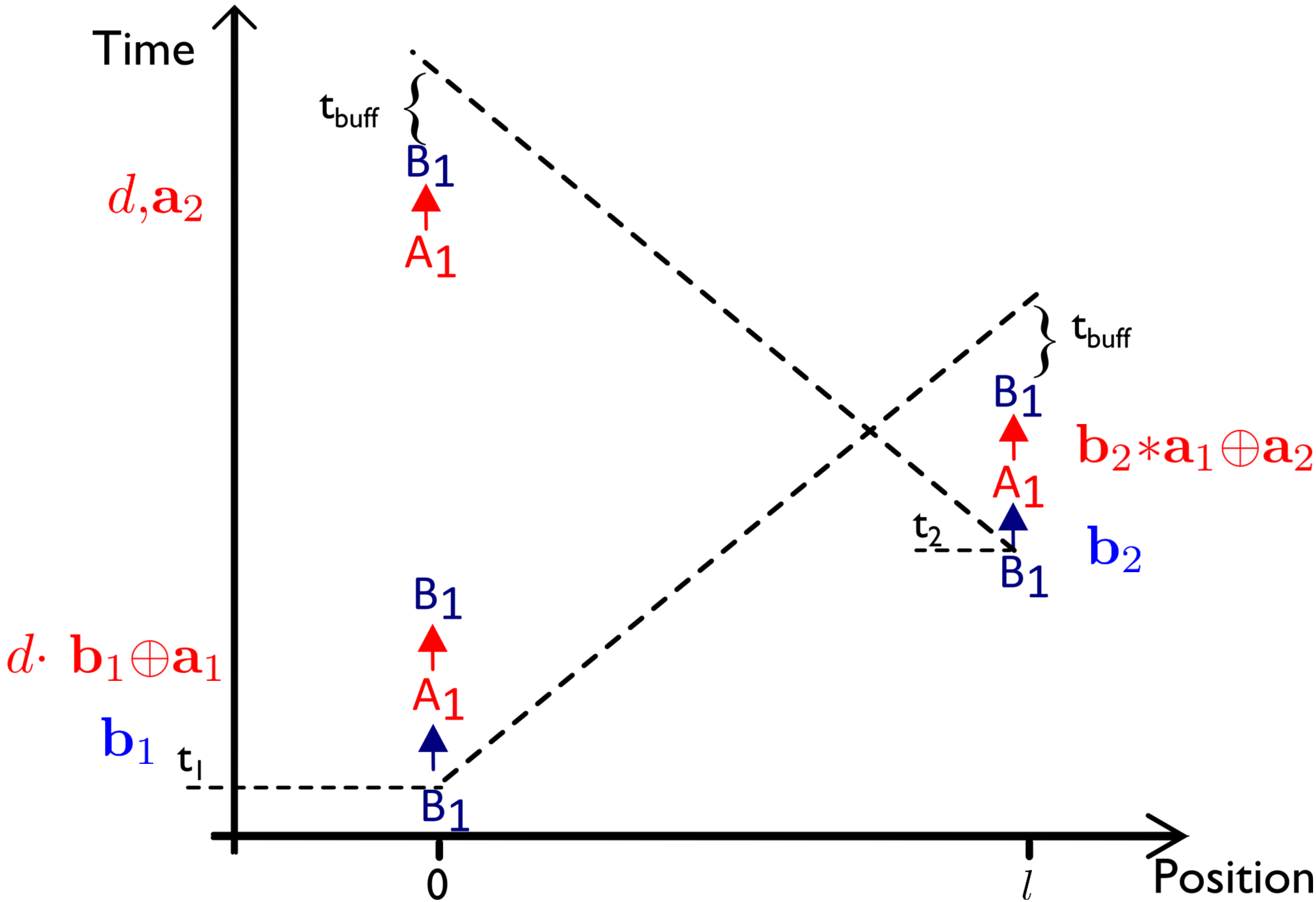
Multi-round experiment



Multi-round experiment



Multi-round experiment



Security parameter

Two-rounds RBC

Provably secure against quantum adversary

Multi-rounds RBC

Provably secure against classical adversary

Security parameter

Two-rounds RBC

[Quantum adversary]

$$\varepsilon_n = \frac{1}{\sqrt{2}} 2^{-n/2}$$

Multi-rounds RBC

[Classical adversary]

$$\varepsilon_{n,m} = \frac{1 + \sqrt{1 + 2^{n+2}(2^n - 1)\varepsilon_{n,m-1}}}{2^{n+1}}$$

$$\varepsilon_{n,1} = 2^{-n}$$

n = number of bits

m = number of rounds

Security parameter

Two-rounds RBC

[Quantum adversary]

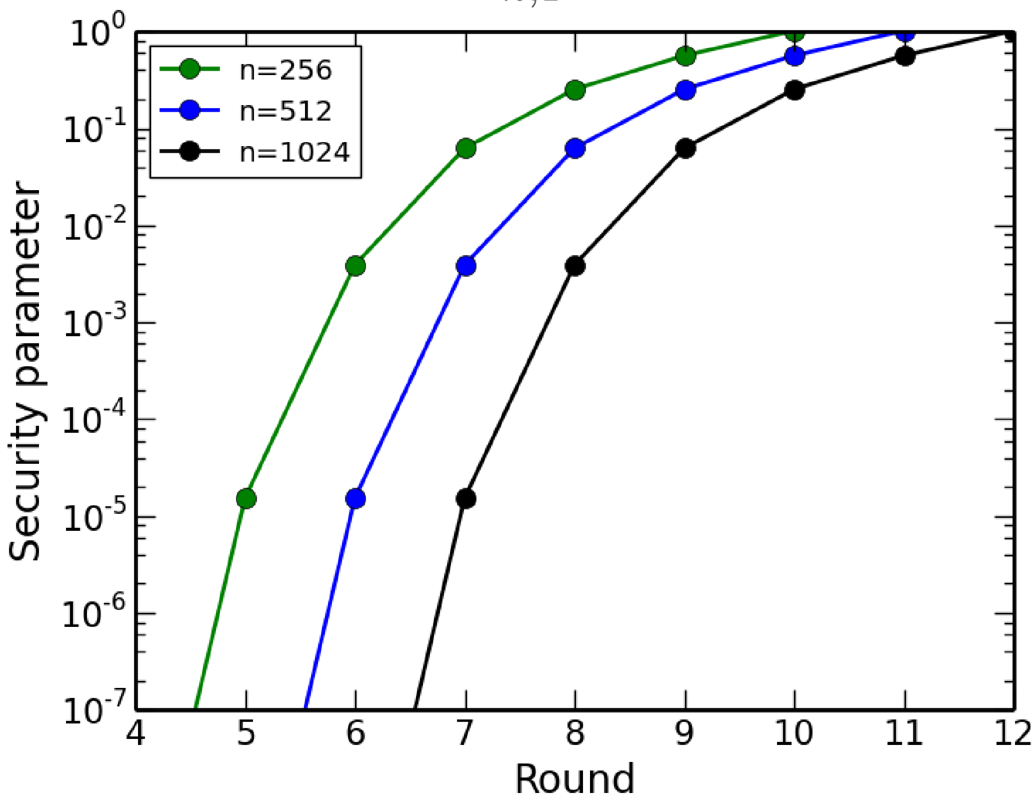
$$\varepsilon_n = \frac{1}{\sqrt{2}} 2^{-n/2}$$

Multi-rounds RBC

[Classical adversary]

$$\varepsilon_{n,m} = \frac{1 + \sqrt{1 + 2^{n+2}(2^n - 1)\varepsilon_{n,m-1}}}{2^{n+1}}$$

$$\varepsilon_{n,1} = 2^{-n}$$



n = number of bits

m = number of rounds

Security parameter

Two-rounds RBC

[Quantum adversary]

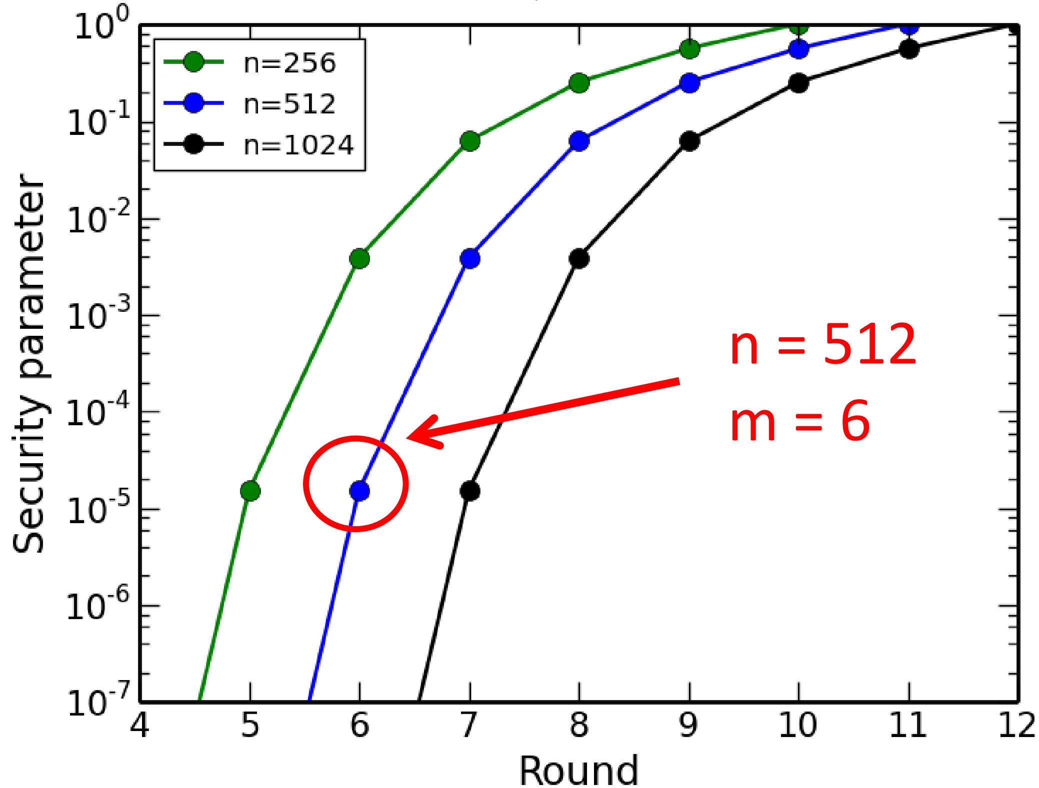
$$\varepsilon_n = \frac{1}{\sqrt{2}} 2^{-n/2}$$

Multi-rounds RBC

[Classical adversary]

$$\varepsilon_{n,m} = \frac{1 + \sqrt{1 + 2^{n+2}(2^n - 1)\varepsilon_{n,m-1}}}{2^{n+1}}$$

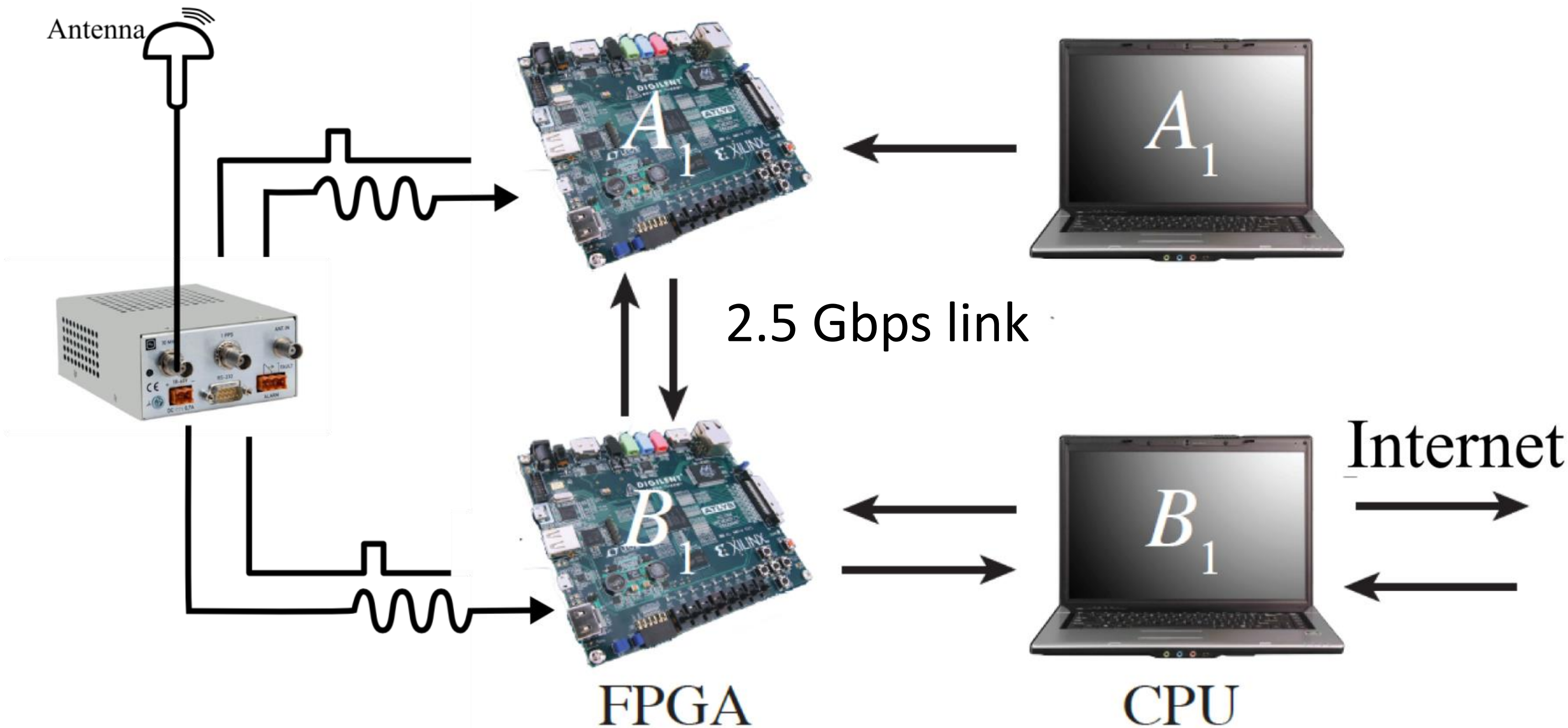
$$\varepsilon_{n,1} = 2^{-n}$$



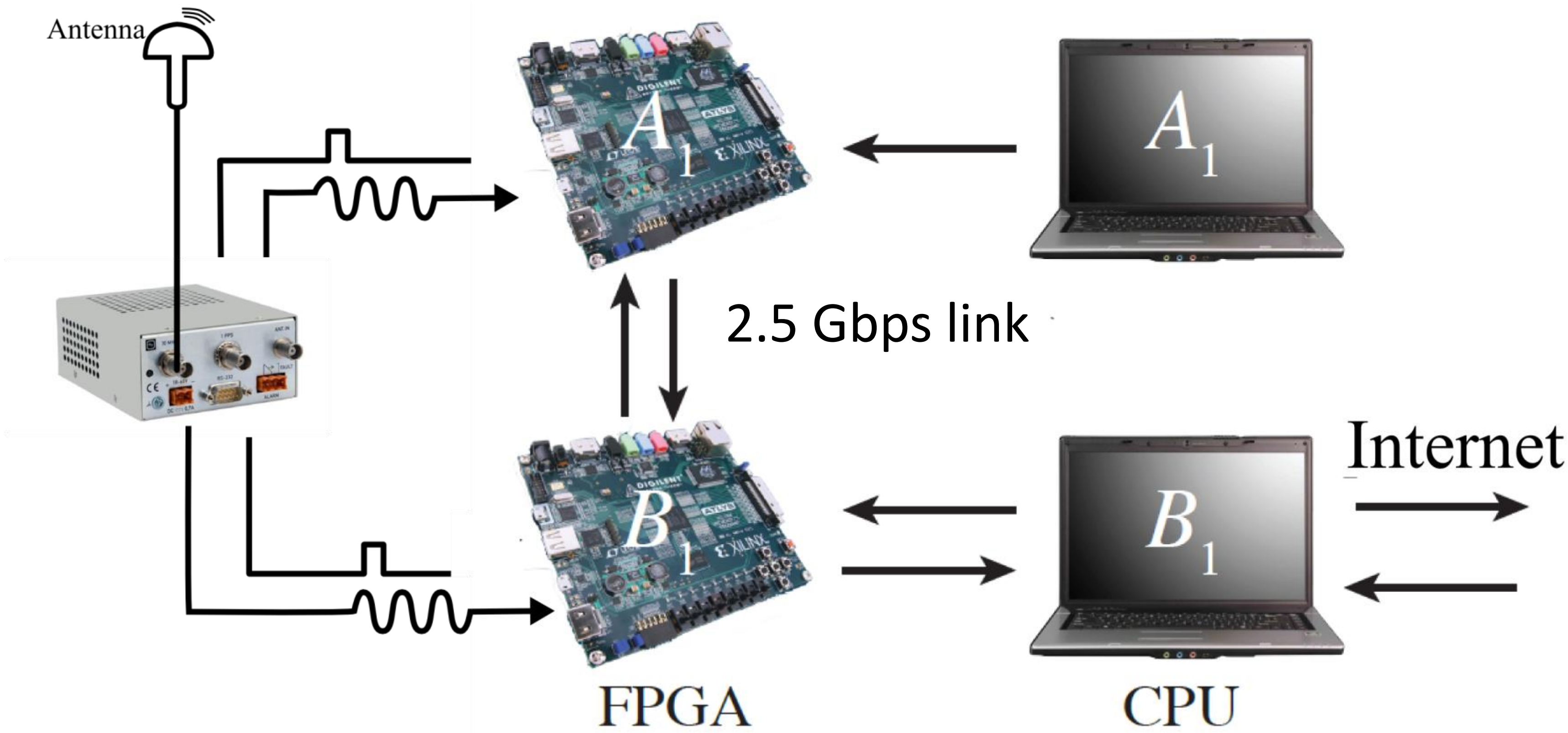
n = number of bits

m = number of rounds

Node

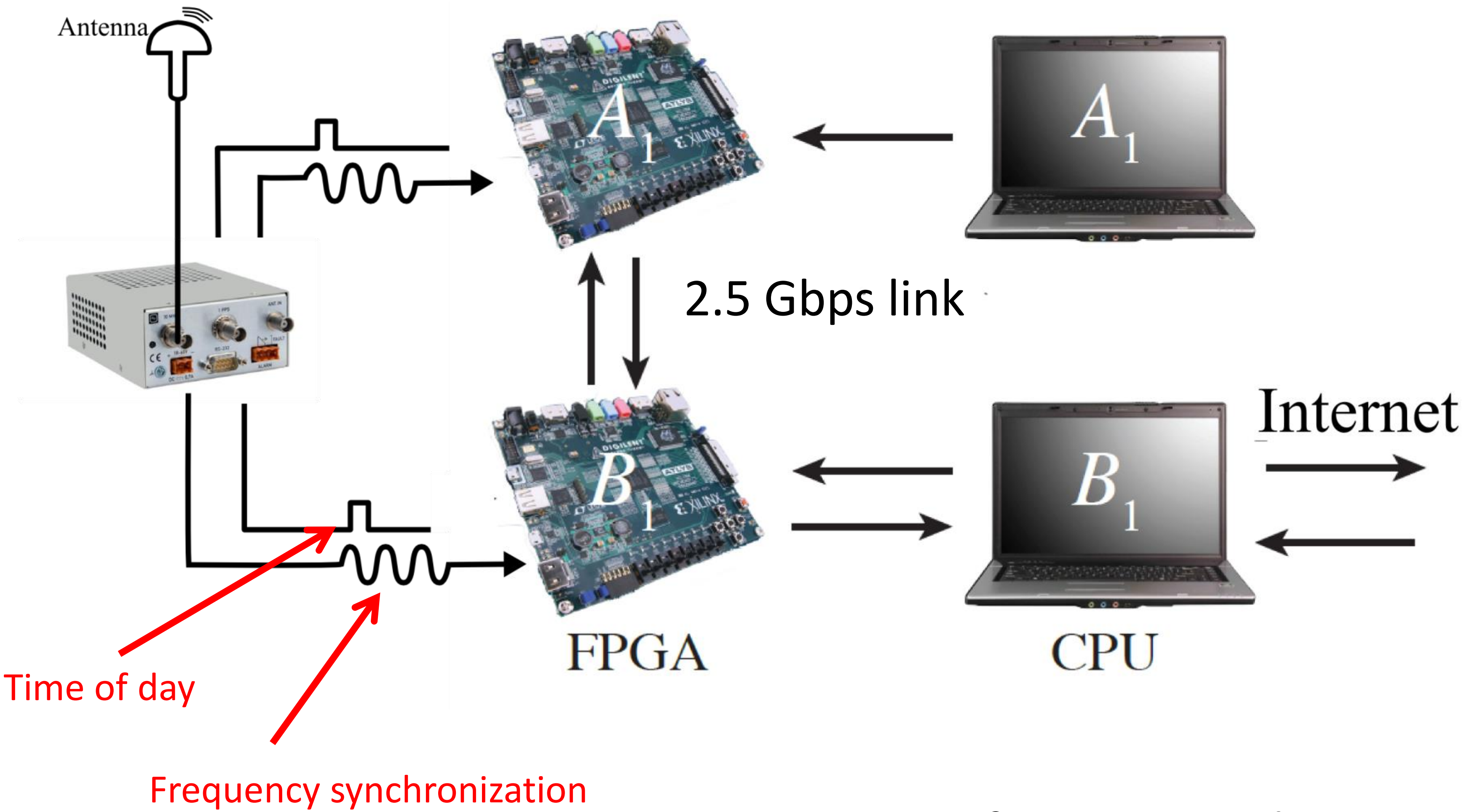


Node



Time for one round: ~ 6.1 µs

Node

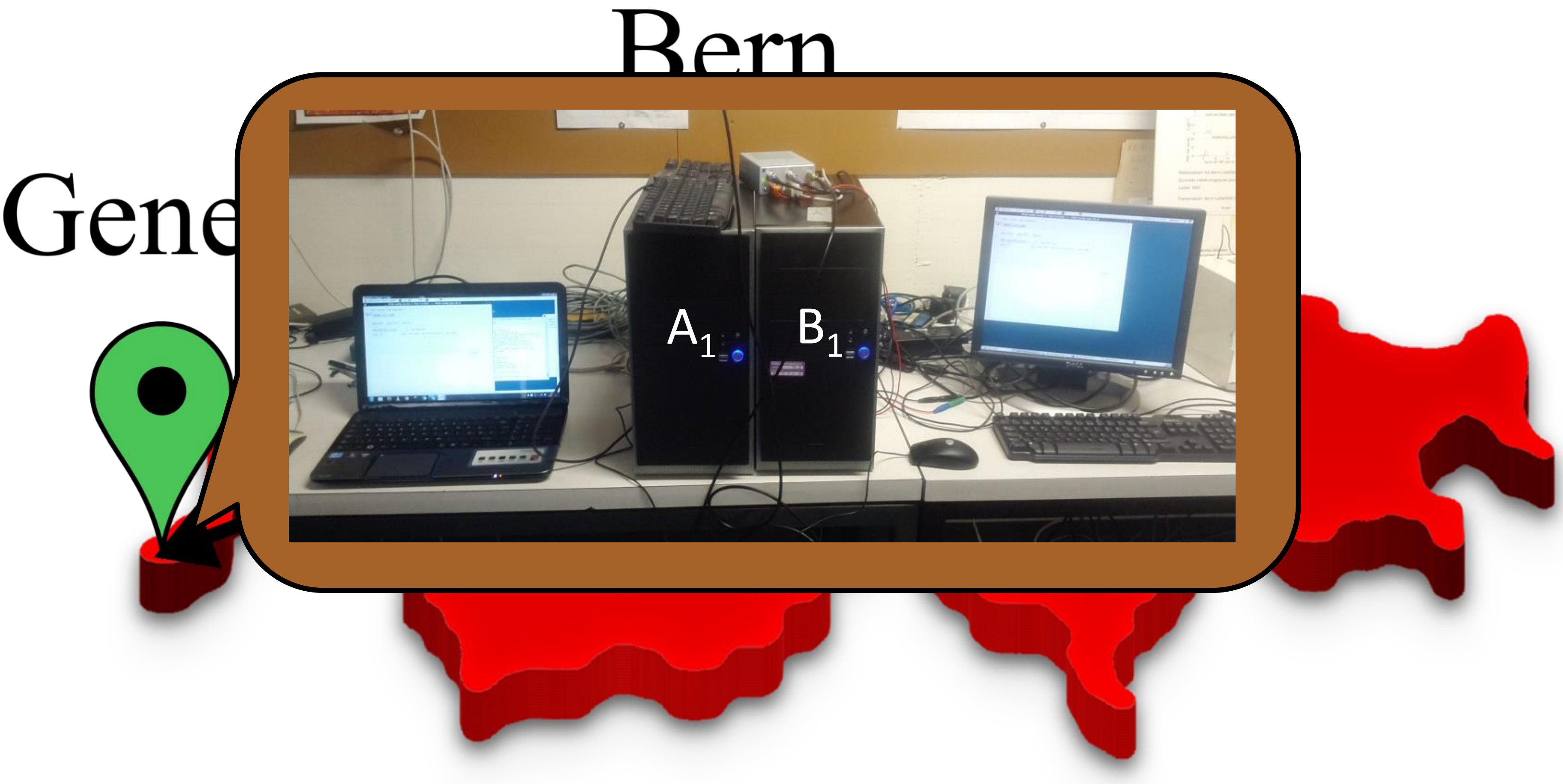


Time for one round: ~ 6.1 μs

Experimental realization

$$\frac{l}{c} = 437\mu s$$

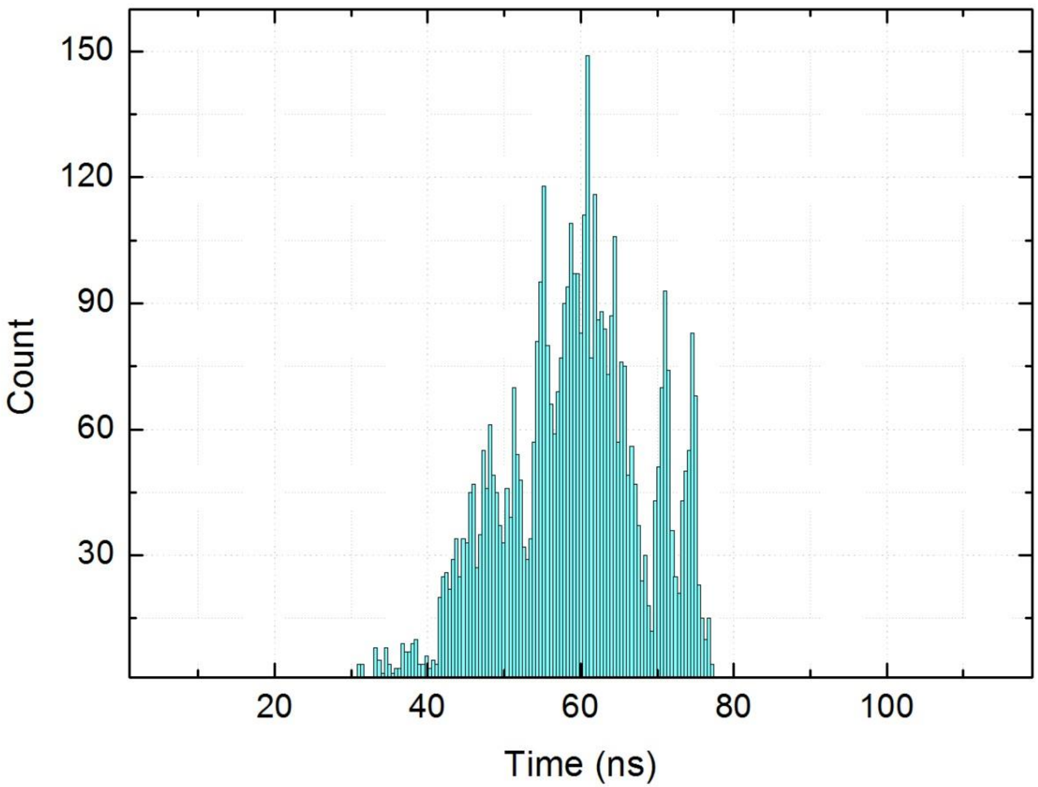
Experimental realization



$$\frac{l}{c} = 437\mu s$$

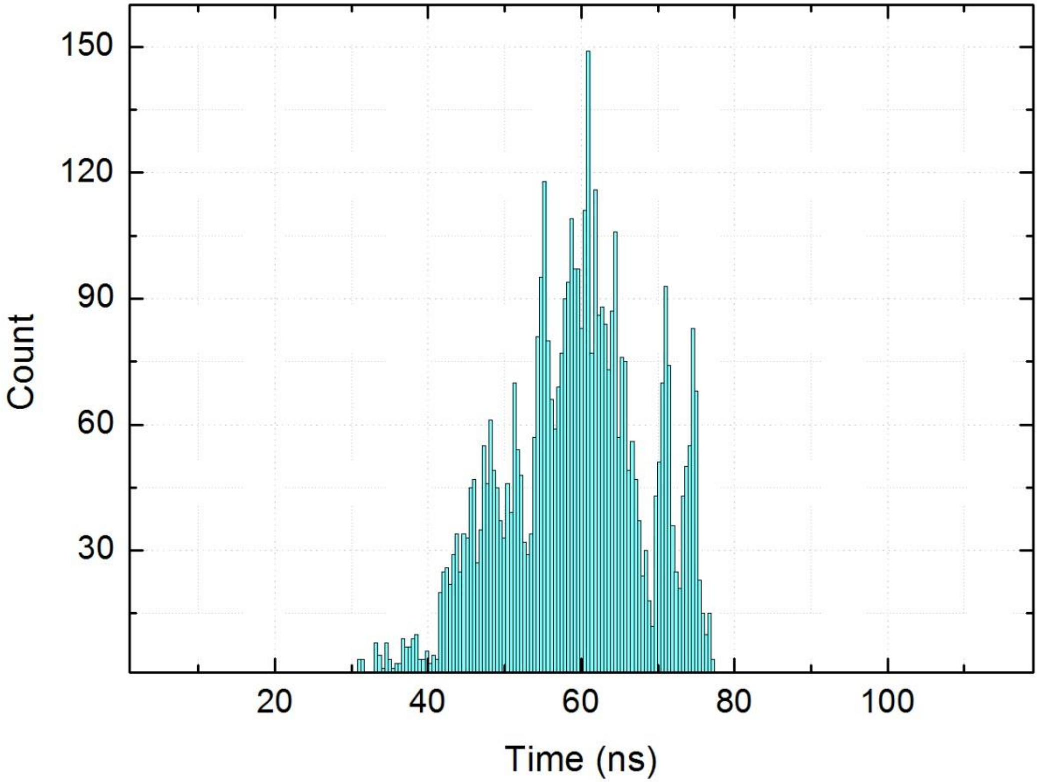
Timing matters: clock uncertainty

Synchronization between two GPS-clocks



Timing matters: clock uncertainty

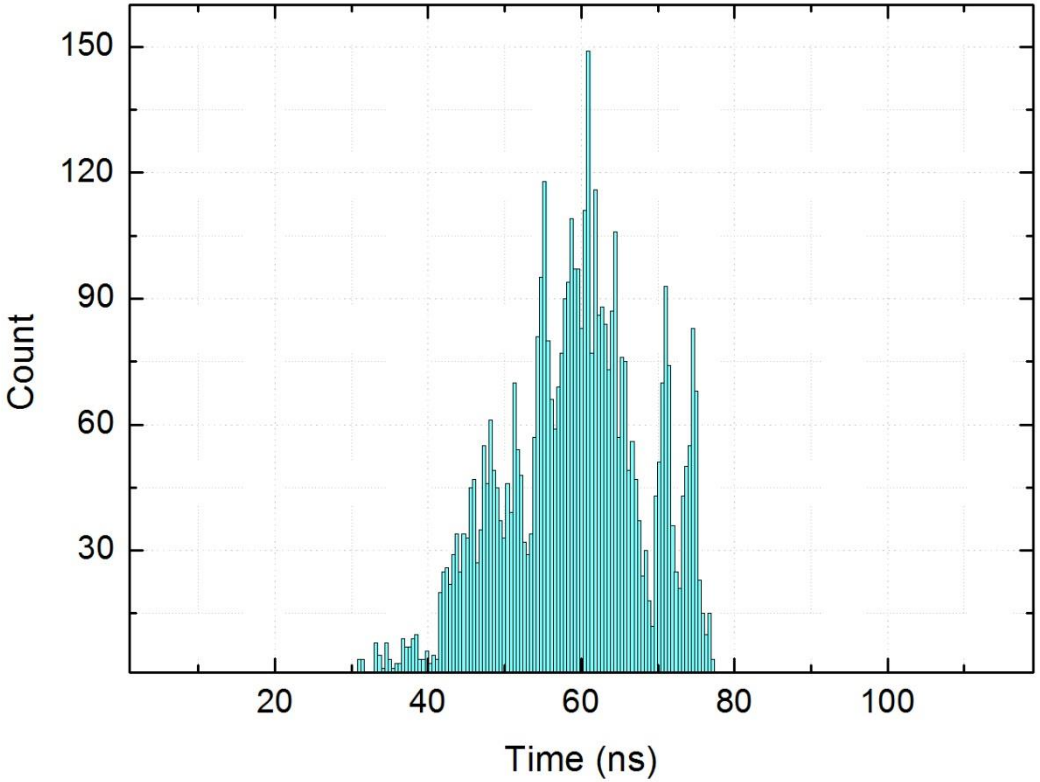
Synchronization between two GPS-clocks



Clock uncertainty: 150 ns

Timing matters: clock uncertainty

Synchronization between two GPS-clocks

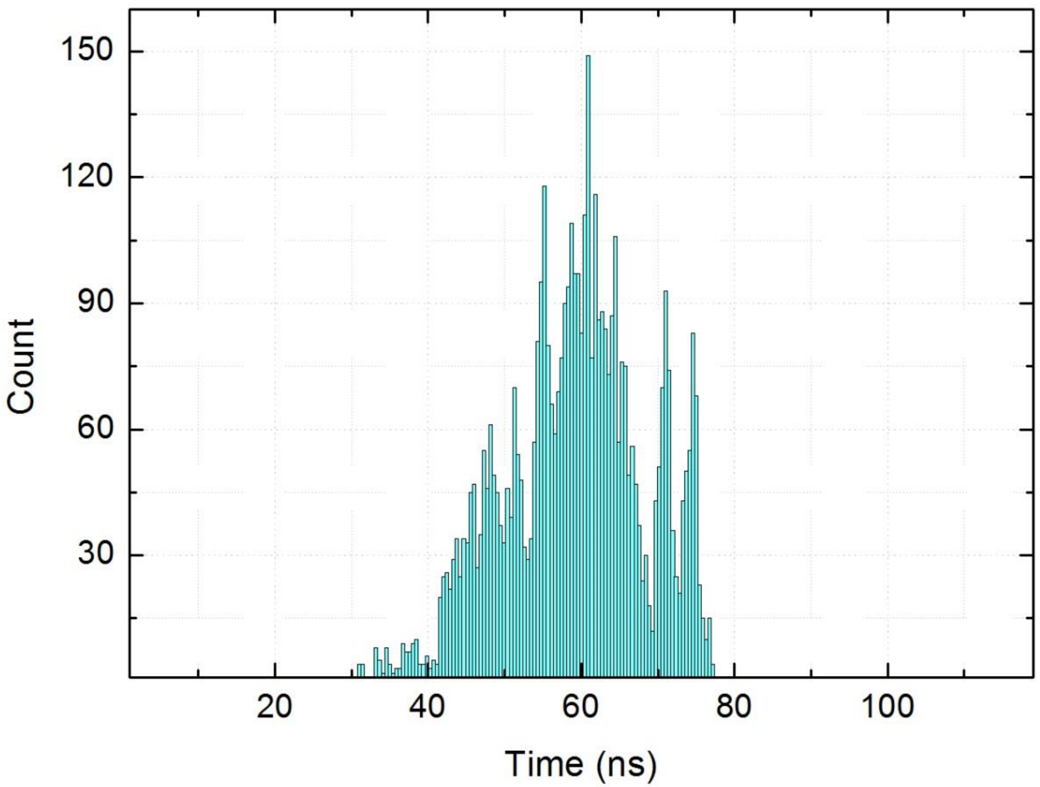


Clock uncertainty: 150 ns

Commitment time between two rounds

Timing matters: clock uncertainty

Synchronization between two GPS-clocks

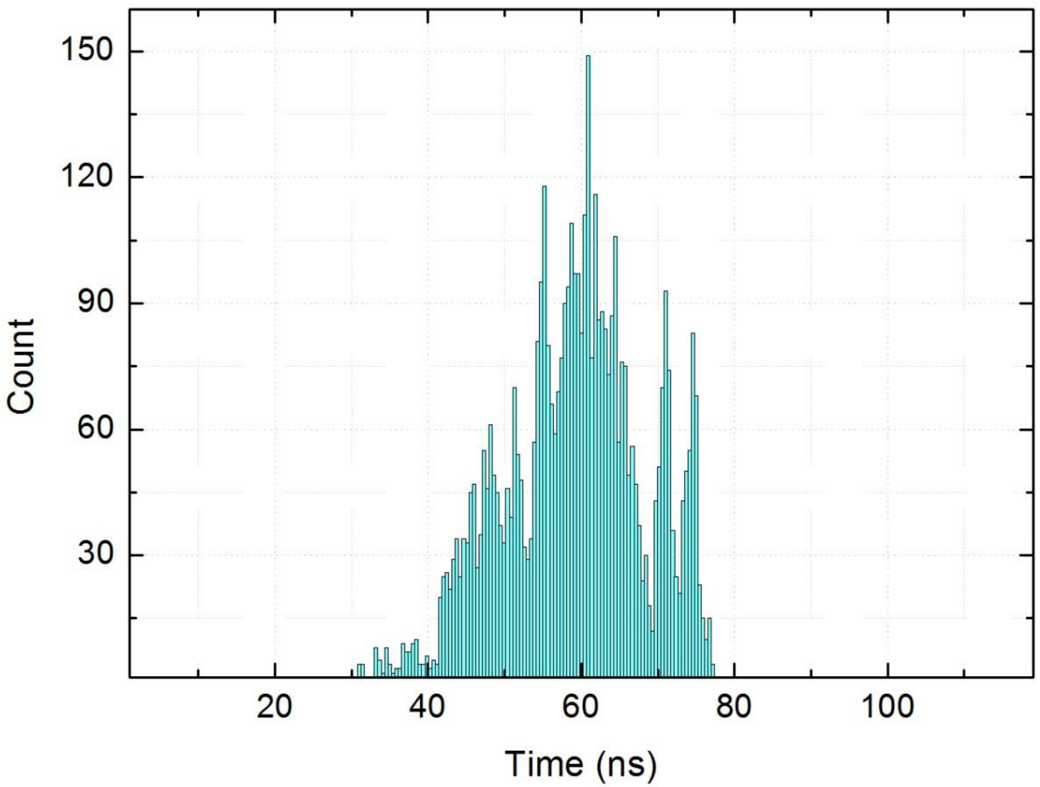


Clock uncertainty: 150 ns

Commitment time between two rounds

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



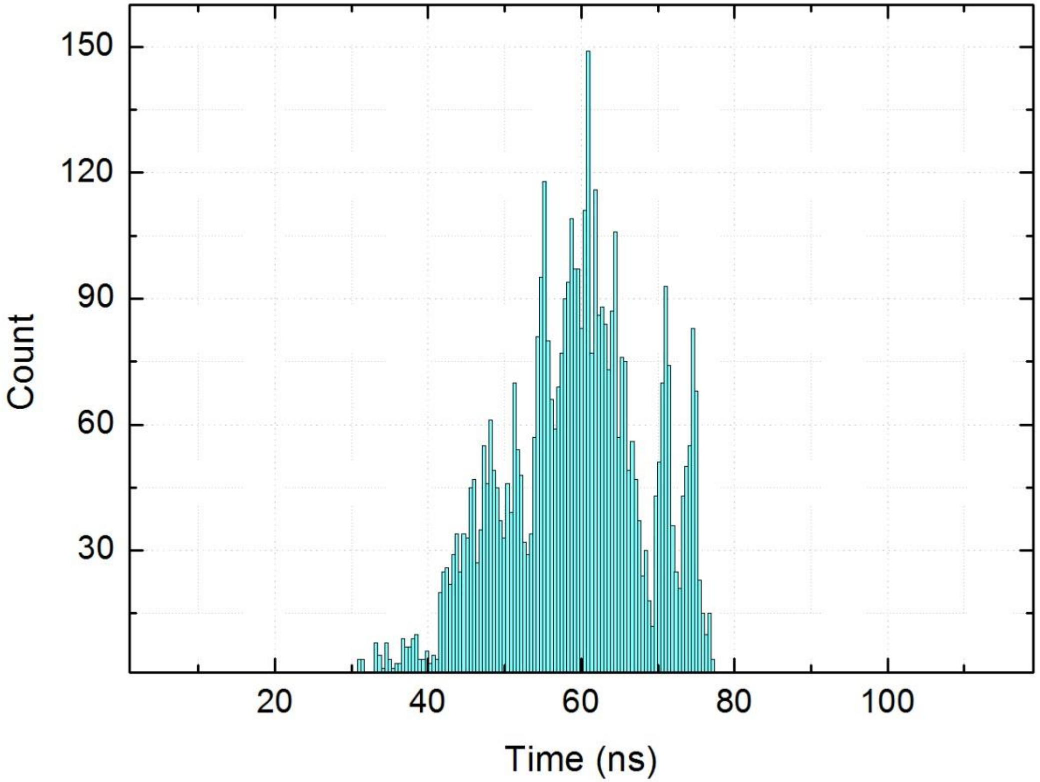
Clock uncertainty: 150 ns

Commitment time between two rounds

437 – 6.1

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



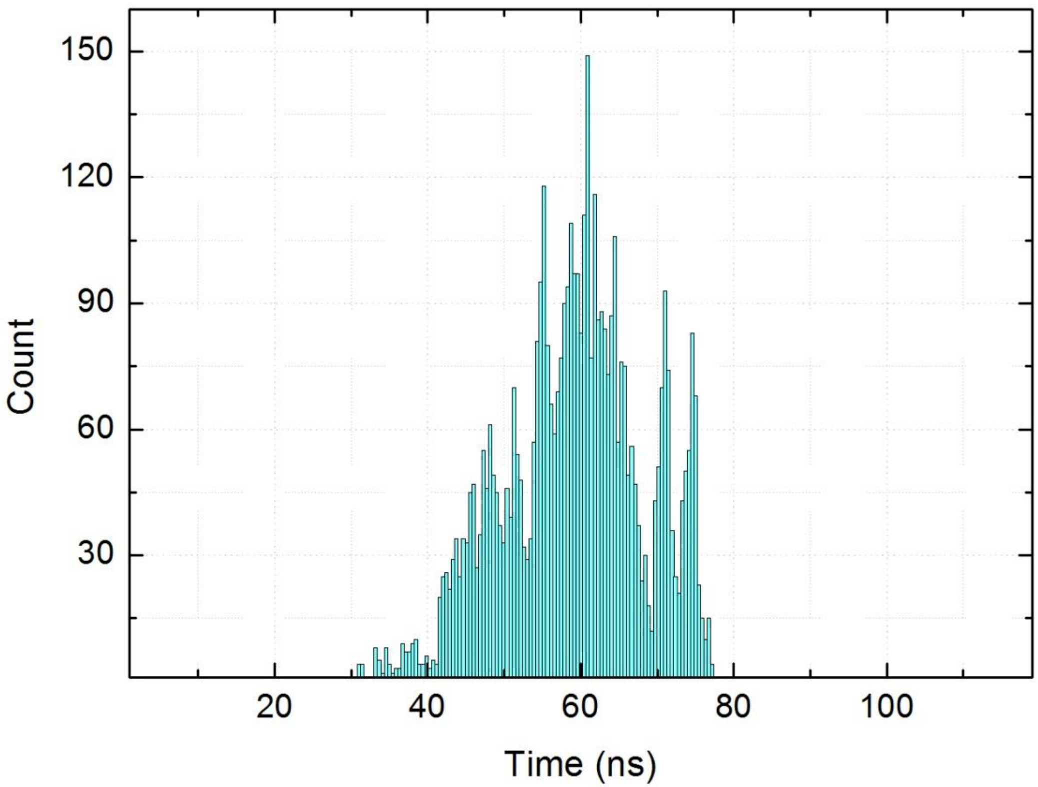
Clock uncertainty: 150 ns

Commitment time between two rounds

437 – 6.1 – 0.15

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



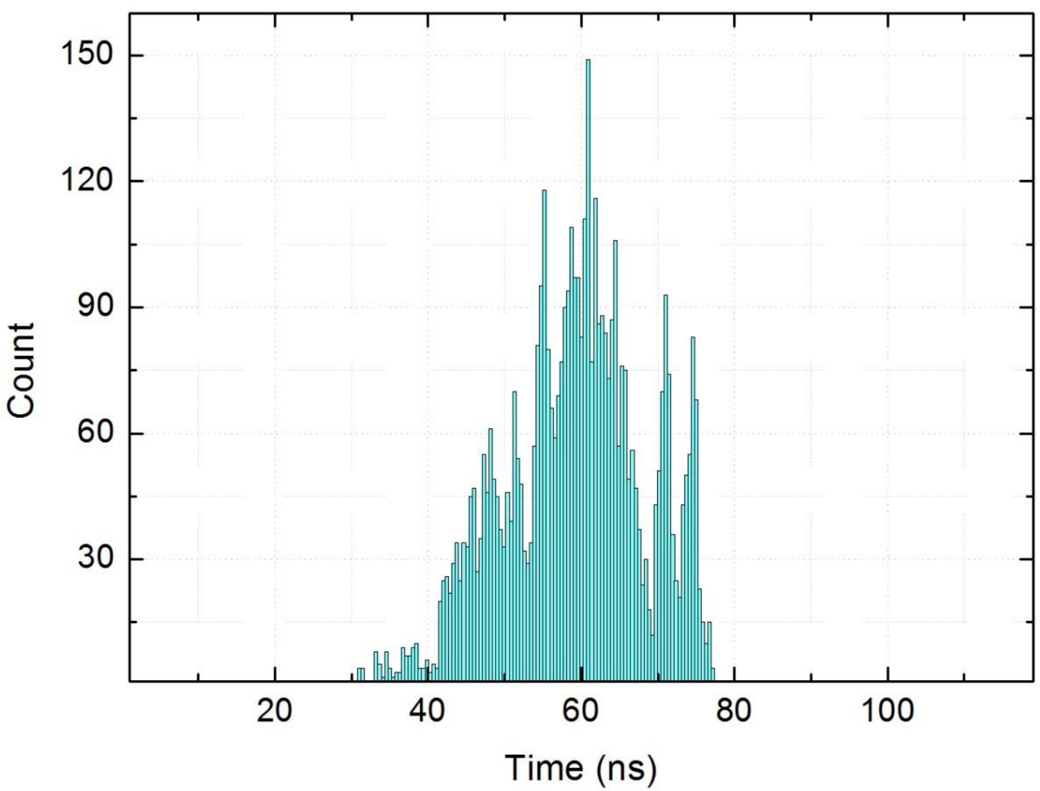
Clock uncertainty: 150 ns

Commitment time between two rounds

$437 - 6.1 - 0.15 - t_{buff} =$

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



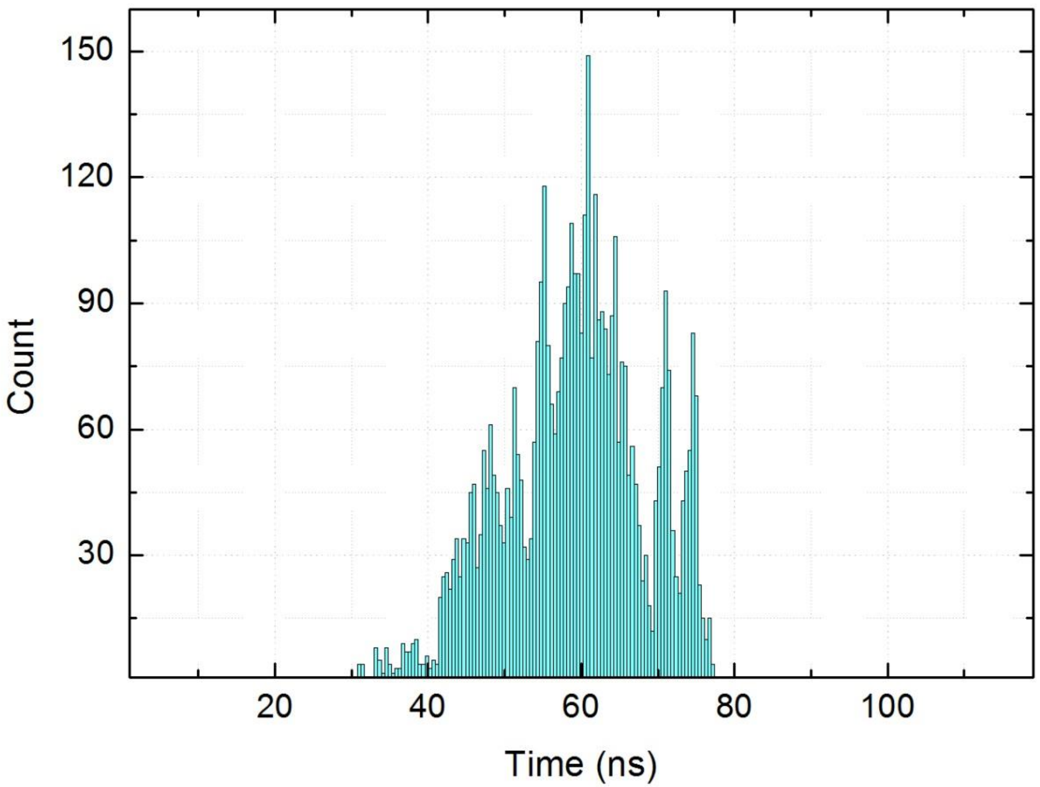
Clock uncertainty: 150 ns

Commitment time between two rounds

$437 – 6.1 – 0.15 - t_{buff} = 400\ \mu s$

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



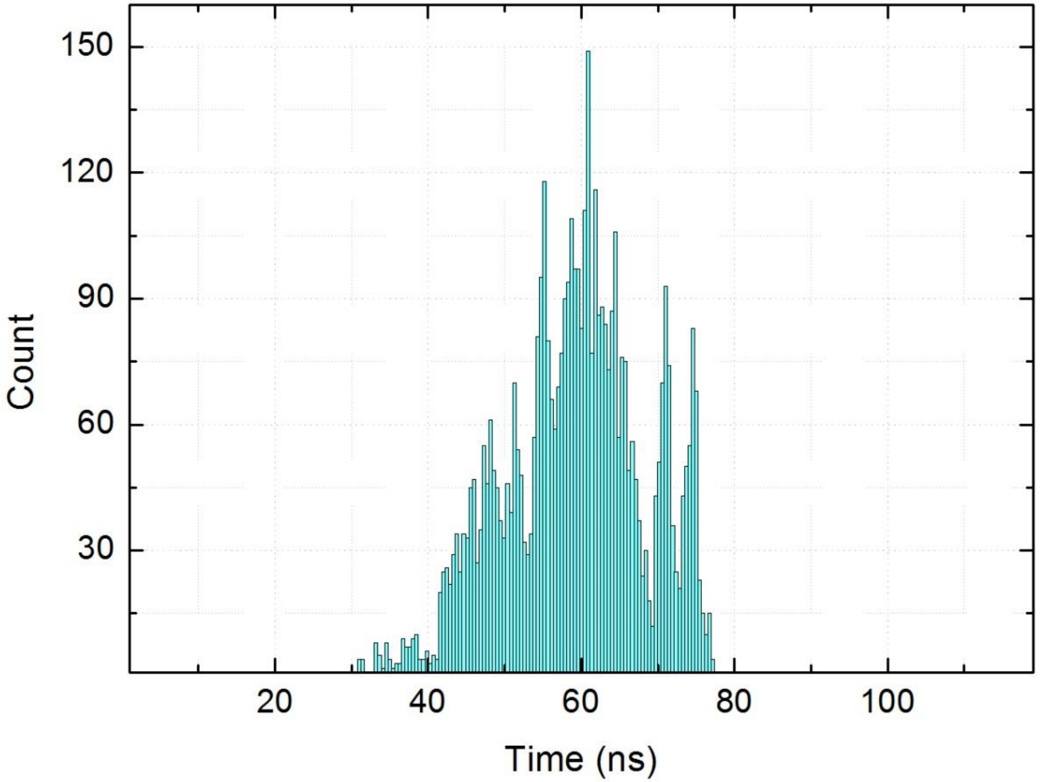
Clock uncertainty: 150 ns

Commitment time between two rounds

$437 - 6.1 - 0.15 - t_{buff} = 400\ \mu s \quad x\ 5$

Timing matters: clock uncertainty

Synchronization between two GPS-clocks



Clock uncertainty: 150 ns

Commitment time between two rounds

$437 – 6.1 – 0.15 - t_{buff} = 400\ \mu s \quad x\ 5$

2 ms of commitment

Relativistic Bit commitment: how far we can go?

Lunghi et al. PRL 111, 180504
Commitment time 16 ms

Relativistic Bit commitment: how far we can go?

Lunghi et al. PRL 111, 180504
Commitment time 16 ms

$$\text{2-Rounds} \quad = 31 \text{ ms}$$
$$\text{6-Rounds} \quad = 155 \text{ ms}$$

Conclusions

- Bit commitment provably secure using only relativistic constraints against quantum and classical adversary.
- Commitment time is not limited by the distance between the two locations (against a classical adversary)
- Even if the multi-round bound allows to sustain only few rounds the commitment, we can perform long commitment with a simple setup.

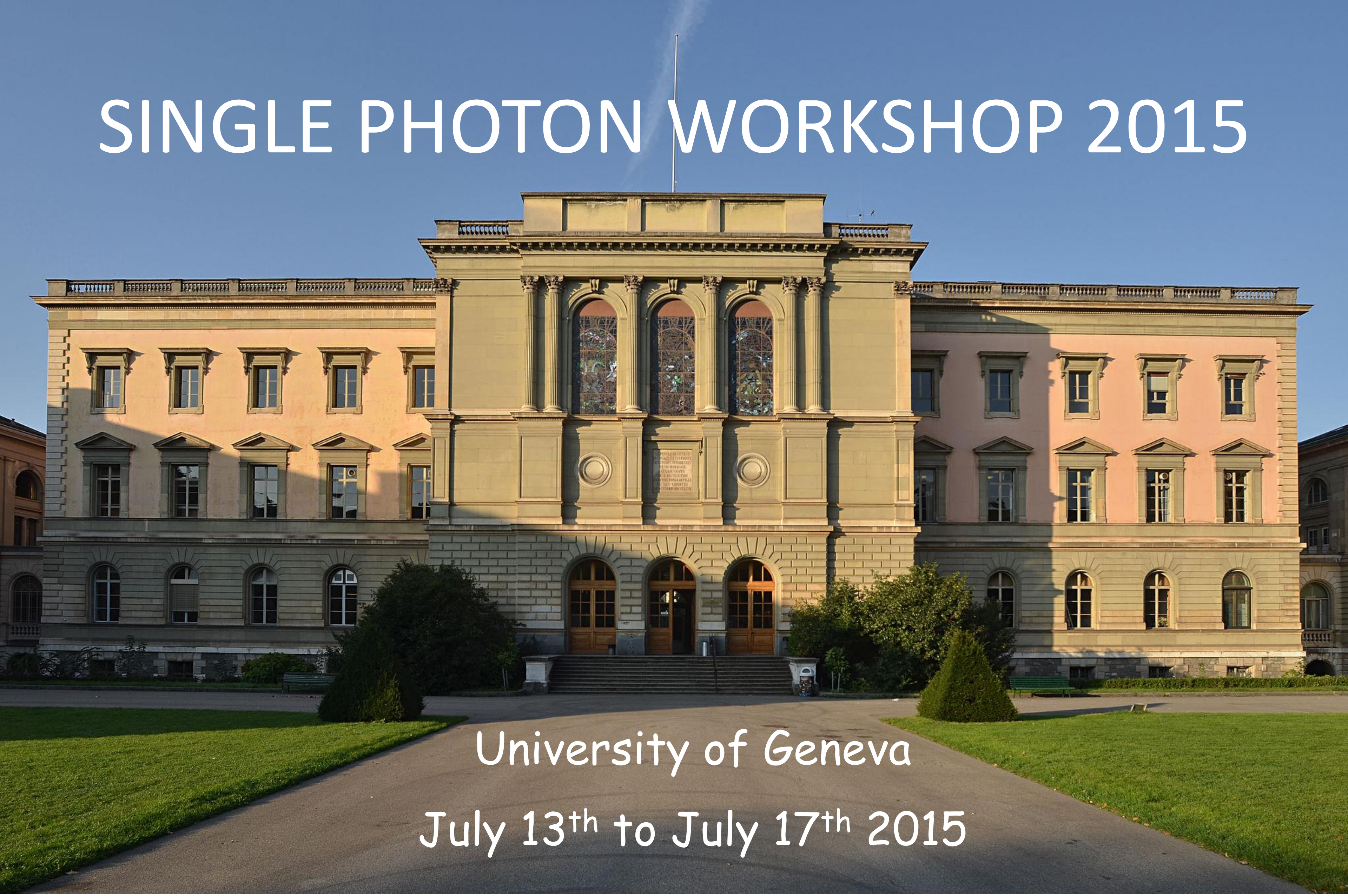
UNIVERSITÉ DE GENÈVE

Centre for Quantum Technologies
National University of Singapore

UNIVERSITÄT BERN

Funding

QSIT-Quantum Science and Technology
Ministry of Education and National Research Foundation Singapore



Save the date!

Wednesday 11:30
Device-independent uncertainty for binary observables
Jedrzej Kaniewski, *et al.*

54) [Area 3] **Practical QKD over 307 Km**,
Boris Korzh, *et al.*

71) [area 4] **A Convenient Countermeasure against Detector Blinding Attacks for Practical QKD**,
Charles Ci Wen Lim, *et al.*

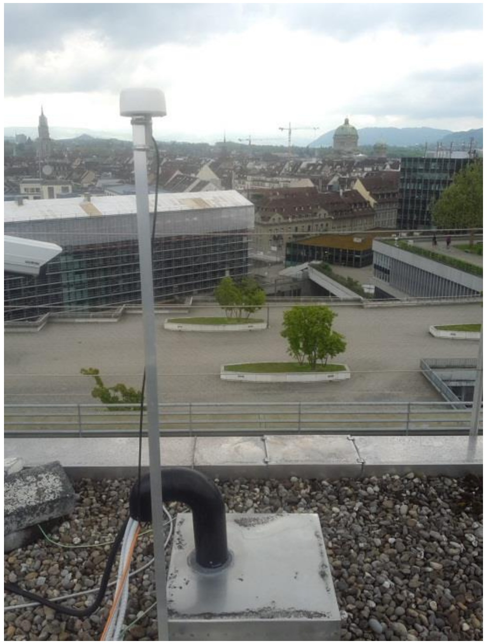
Wednesday 11:30
Device-independent uncertainty for binary observables
Jedrzej Kaniewski*, et al.*

71) [area 4] **A Convenient Countermeasure against Detector Blinding Attacks for Practical QKD**, Charles Ci Wen Lim*, et al.*

54 [Area 3] **Practical QKD over 307 Km**, Boris Korzh*, et al.*

Experimental realization

Bern



Geneva