Cryptography with the space-time constraints

Kaushik Chakraborty, QuTech, Netherlands

International Crypto-Webinar

28th August, 2020

PRINCIPLES OF CRYPTOGRAPHY

1. Definitions.
2. Assumptions.
3. Security Proofs.

Assumptions

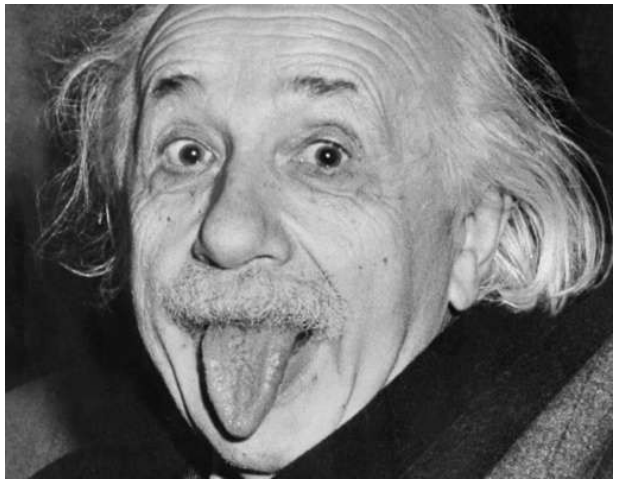
Example:

1. Computational Assumptions.
    a. Probabilistic polynomial time adversary.

2. Assumptions, inspired from the physical laws.

    a. No cloning principle in quantum information theory.
    b. No superluminal signalling(NSS) principle from the special theory of relativity.

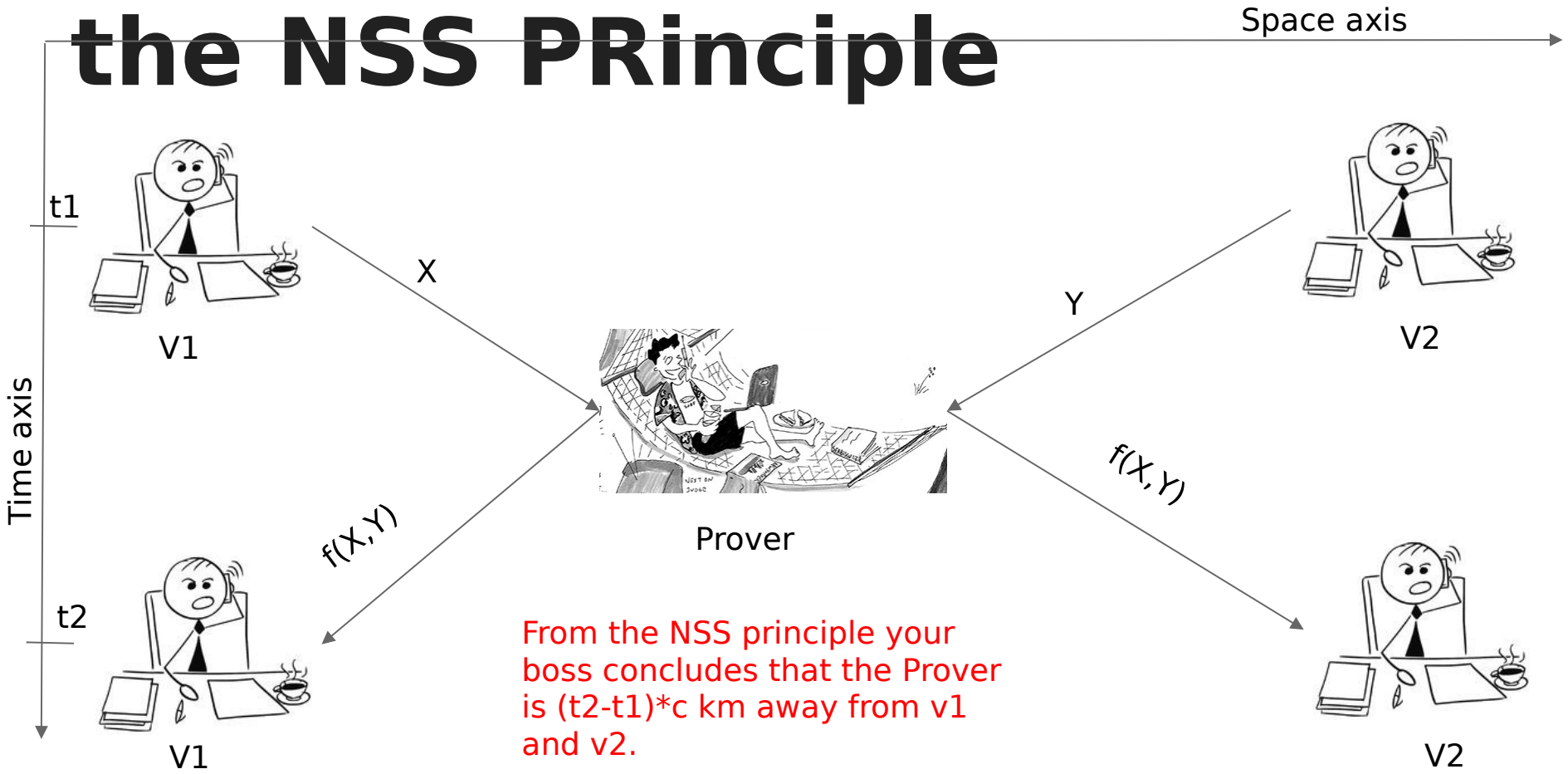
NSS PRINCIPLE



No physical carrier of information can travel faster than the speed of light.

Location verification using the NSS PRinciple

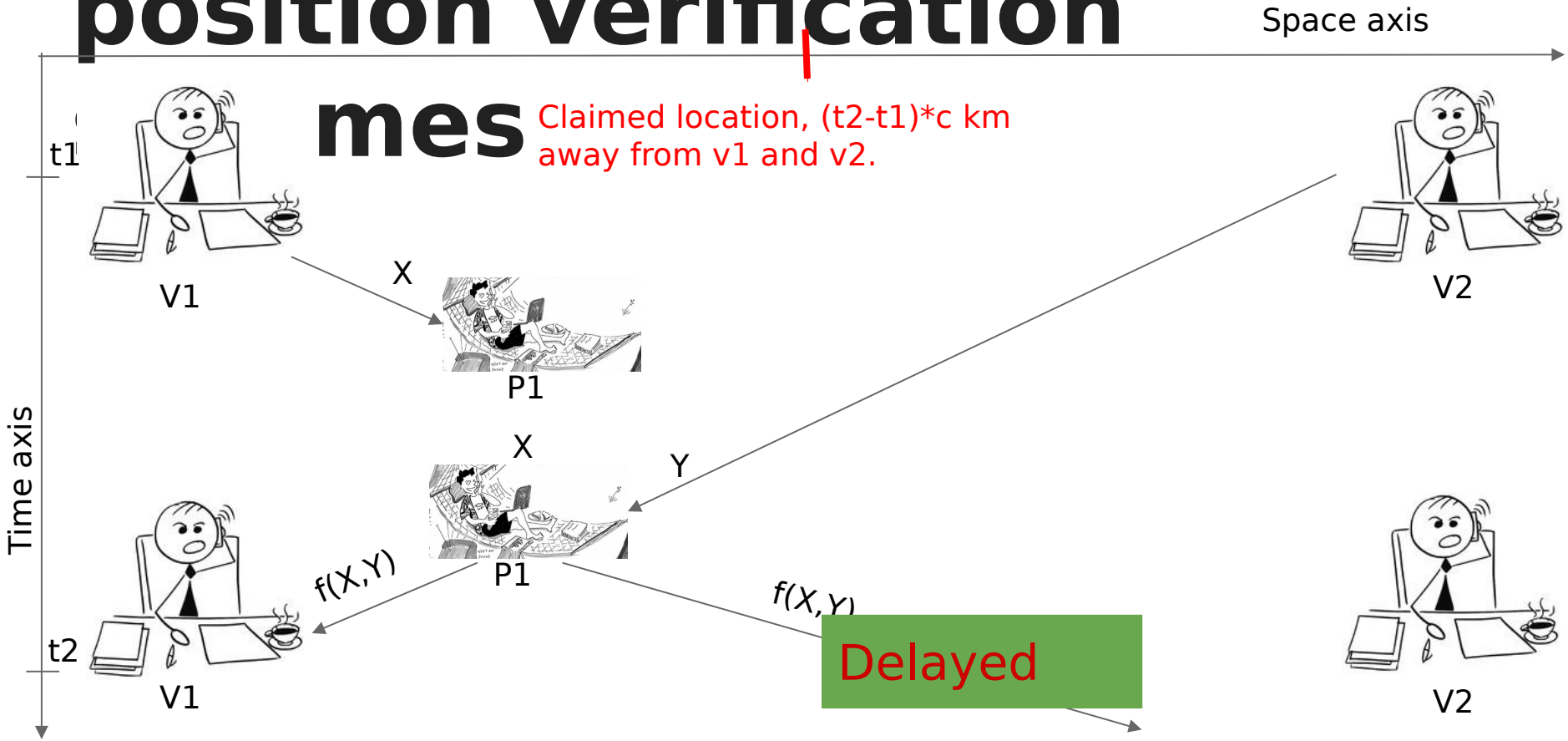
Location verification using the NSS PRinciple



APPLICATIONS

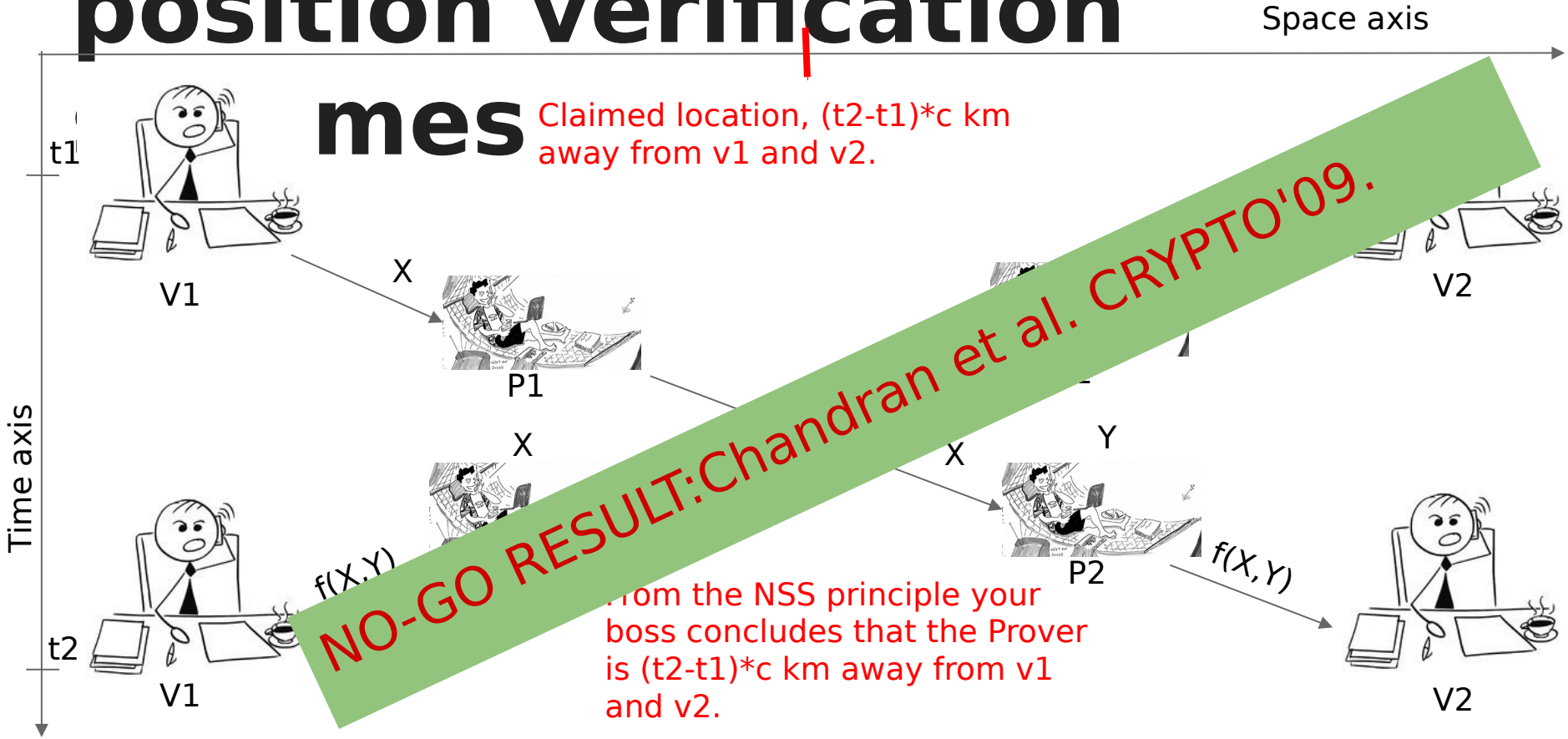
1. **Position verification :** a player Alice wants to convince the (honest) verifiers that she is located at a particular point.
2. **Position based encryption :** Alice wants to send a message to Bob at a specified position with the guarantee that it can only be read if BOB is located at that particular position.
3. **Position based authentication :** guarantee that a received message originated from a

Attack on the classical position verification

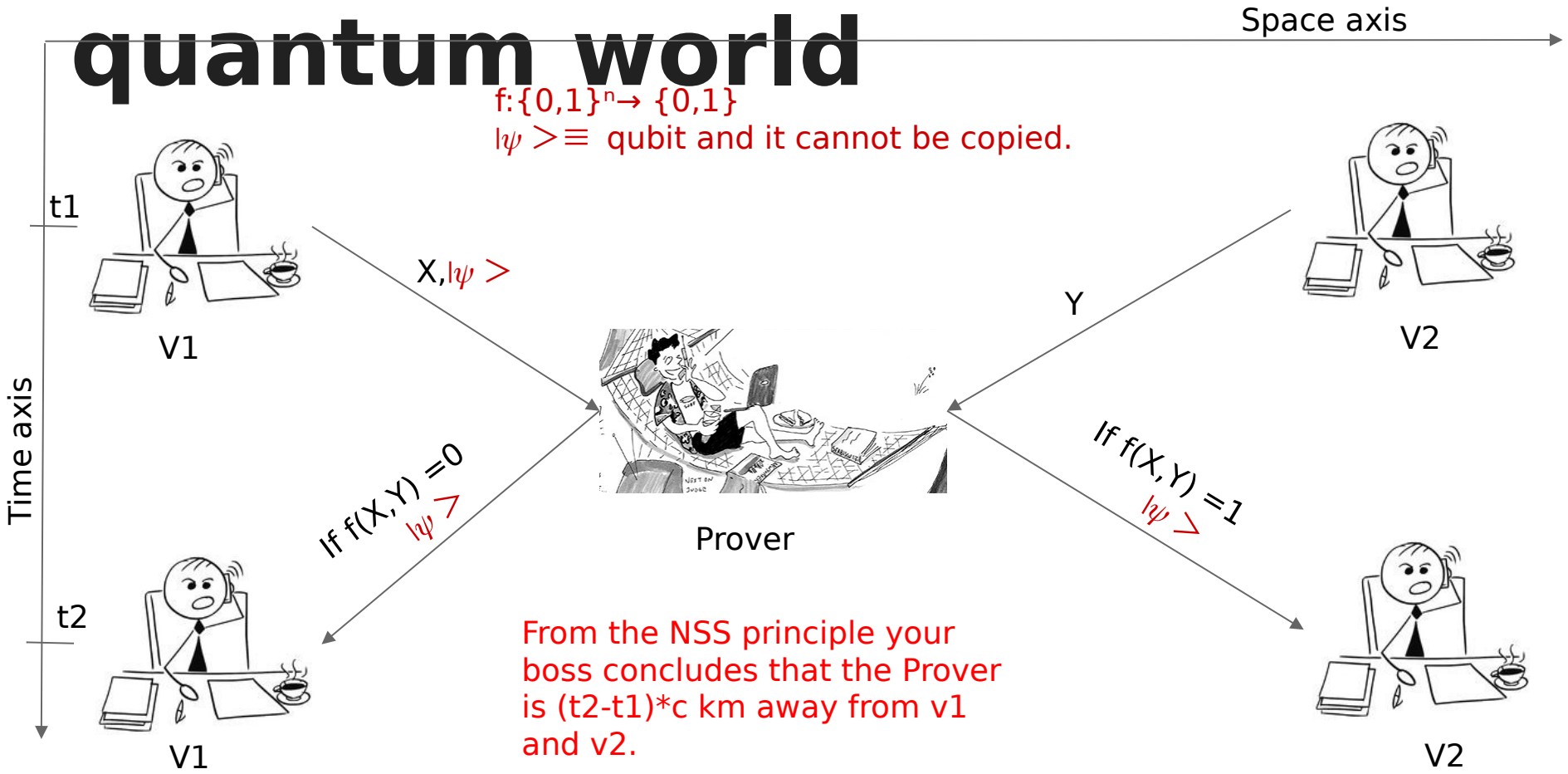


Claimed location, (t2-t1)*c km away from v1 and v2.

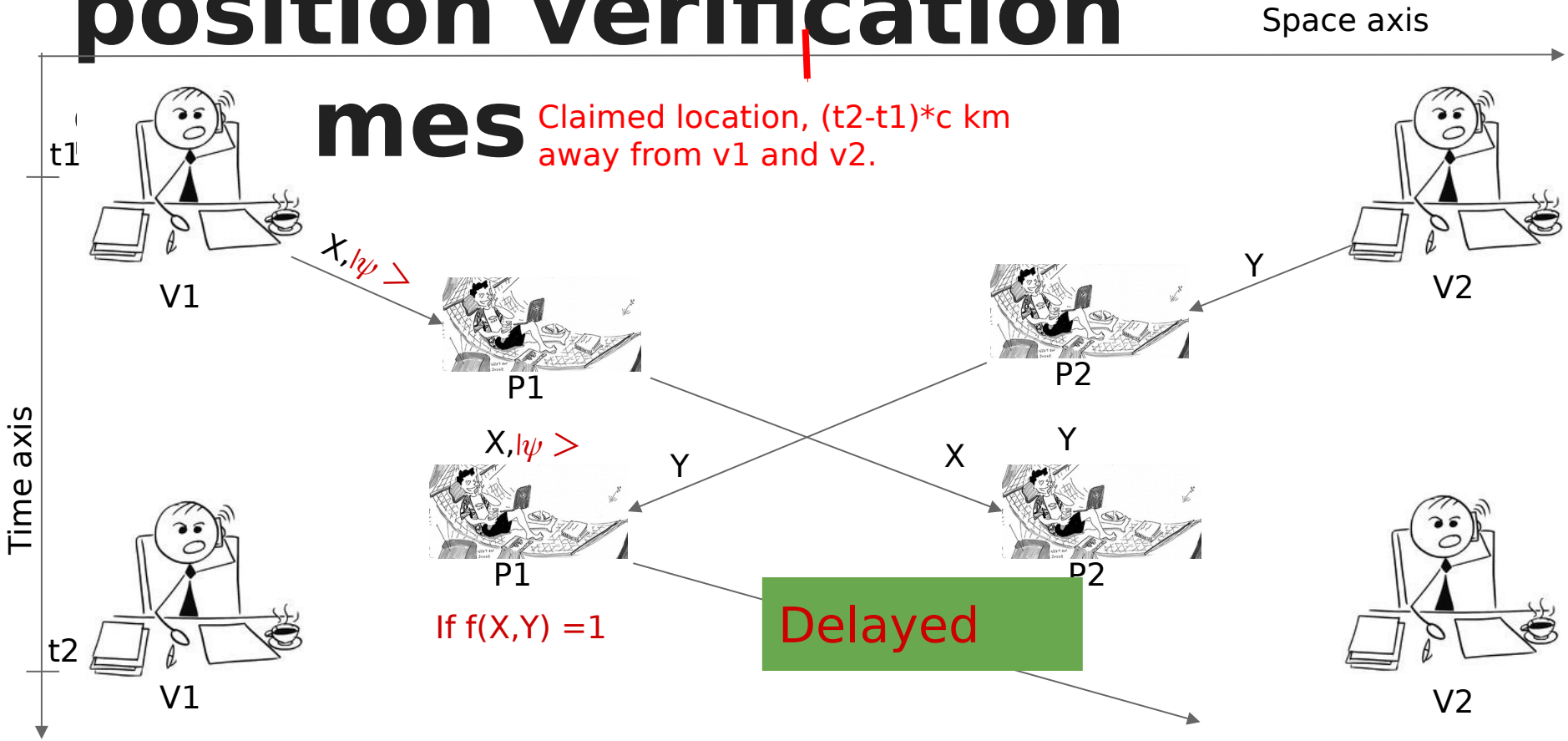
Attack on the classical position verification mes



Location verification in the quantum world



Attack on the classical position verification mes



Existing results on the location verification in the quantum world

1. If the adversaries do not have access to entanglement then it is possible to have a secure location verification scheme. (Buhrman et al. Crypto 2011.)

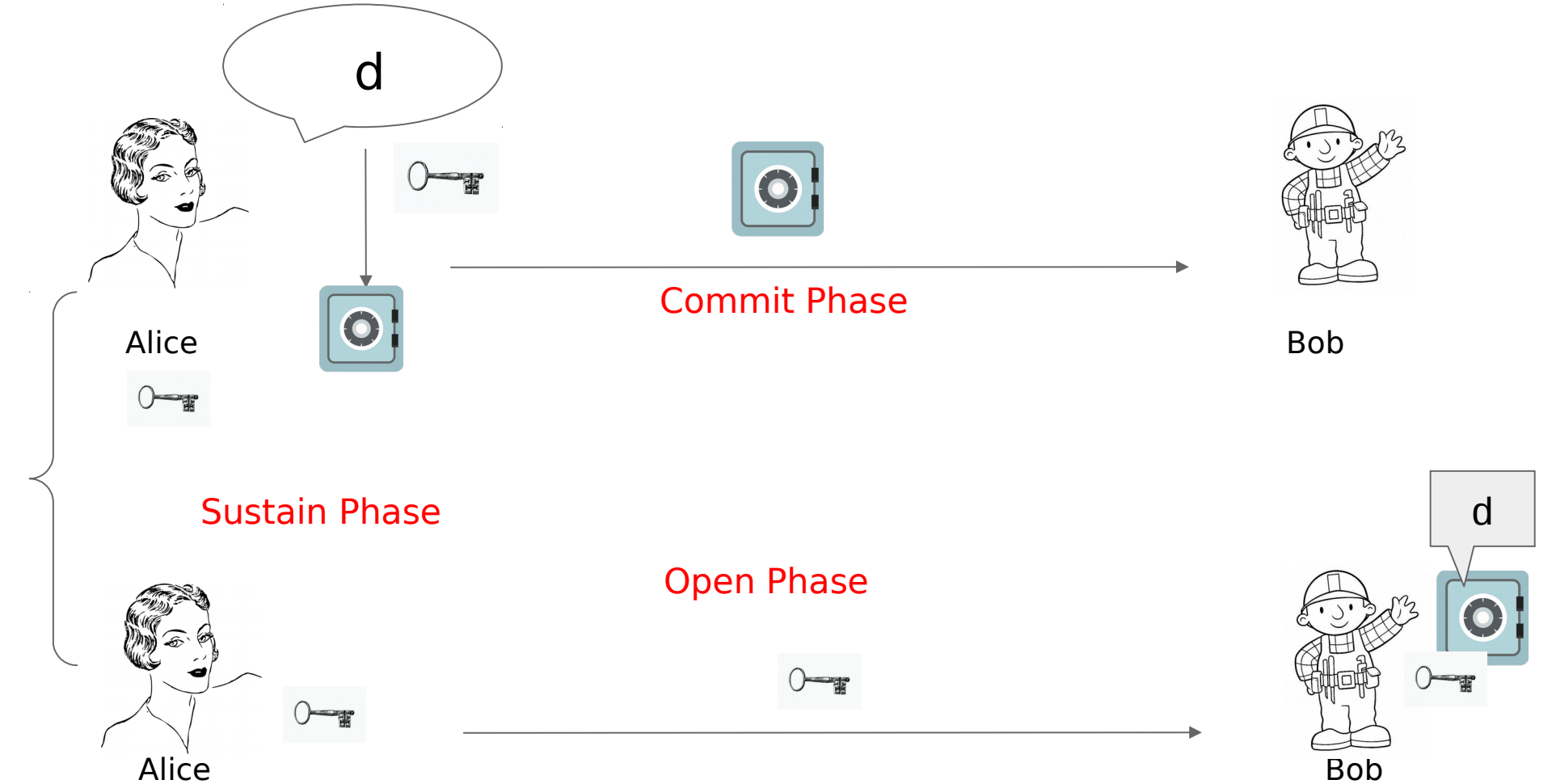
2. If the adversaries can pre-share exponential (in n) number of EPR-pairs then no secure location verification scheme is possible. (Buhrman et al. Crypto 2011.)

3. In the quantum random oracle model it is possible to design a secure location verification scheme. (Unruh, Crypto 2014.)

What about the other primitives?

Bit Commitment

Bit Commitment



Security Requirement for the Bit Commitment

- Security for Alice (Hiding Property):Bob shouldn't have any information about the commitment before reveal phase.

$$\Pr[\text{Bob guesses d}] \leqslant \frac{1}{2} + \epsilon$$

- Security for Bob (Binding Property):Alice can't change the commitment after the commit phase.

$\Pr[\text{Alice successfully reveals 0}|Y] + \Pr[\text{Alice successfully reveals 1}|Y] \leqslant 1 + \epsilon$. (Sum Binding)

EXISTING RESULTS ON THE BIT COMMITMENT

- In the classical setting information theoretically secure bit commitment protocol is impossible.
  - Ben-Or et al., STOC 1988.

- In the quantum setting information theoretically secure bit commitment protocol is also impossible.
  - Mayers, D., Physical Review Letters, 1997.
  - Lo, H.,K., Chau, H.,F., Physical Review Letters, 1997.

A brief overview o… e classical no-go…

Alice

Perfect hidi…

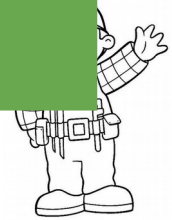
Per… …g.

Can relativistic assumptions help here?

Alice

…,r_A

Reveal Phase



Bob

Bindi… …ect hiding implies, Alice can reveal d ≠ d' and Bob can not… …em.

BIT COMMITMENT WITH MULTIPLE ALICE (Ben-OR et al., Stoc 1988)

q

x

y = dx+b

b is a shared random number between A1, A2

A1

Commit Phase

Bob

A2

d', b'

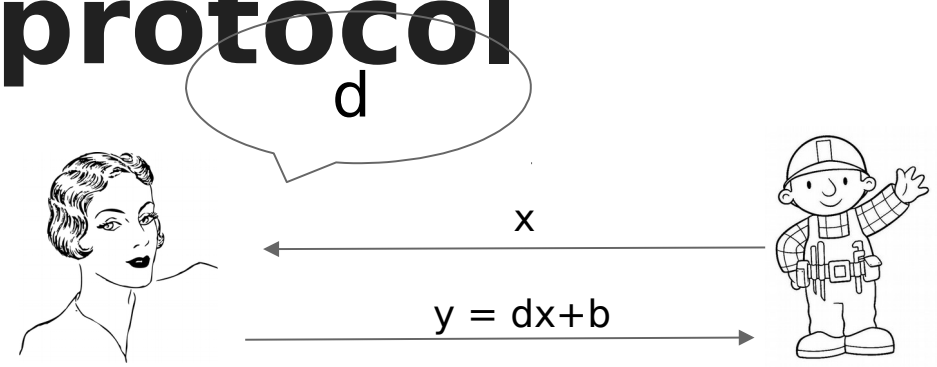
Bob computes,
y' = d'x+b'

Open Phase

Bob accepts if y = y'

Bob

Hiding property of the protocol



b is a shared random number between A1, A2

Bob has no information about b.

Hence, Bob will not have any information about d from y.

The protocol is hiding.

Binding property of [illegible] protocol

Pr[A2 successfully reveals 0|Y] + Pr[A2 successf[illegible]

This protocol i[illegible] A1, A2 are not[illegible]icate.

Ot[illegible]ding.

Is the non-communication assumption enough for a secure bit-commitment protocol?

A1

Com[illegible]

A2

For revea[illegible]

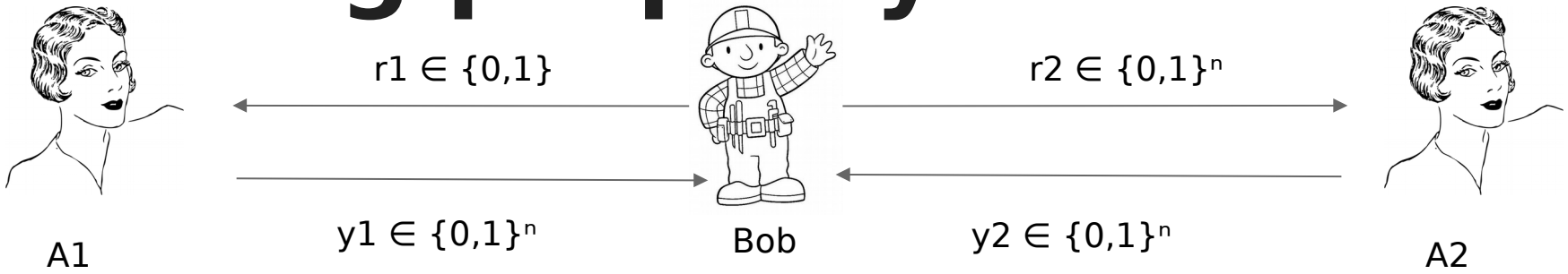
Can[illegible]

For re[illegible]eeds to send y = x + b'.

A2 can [illegible]he knows x.

Otherwise, A2 succeeds with probability 2/q.

Another look at the sum binding property



A1, A2 win iff y1 - y2 = r1.r2

CHSH Game

Lemma: If Win. Prob. of CHSH = ½ + δ then the bit commitment protocol is 2δ-binding.

Upper bound on The value of δ

- In the classical setting $\delta \leqslant 1/2^n$. It is a tight bound.

- In the quantum setting $\delta \leqslant 1/\sqrt{(2^n)}$. It is a tight bound.

Can we do better?

There are other physical theories where one can get $\delta = 1$. But we do not have any experimental evidence.

How to implement non-communication assumption

A1

A2

Put the D distance apart.

NSS Principle: It will take at least D/c seconds to send any information from A1 to A2.

BIT COMMITMENT WITH MU[illegible]PLE
ALICE (kEnt, a., prl 199[illegible]

A1

x

y = dx+b

Commit Phase

Bob

[illegible] number
[illegible]tween A1, A2

A2

d’ ,b’

Open Phase

[illegible]ates,
x+b’

B[illegible]
1. [illegible]ives d’,b’ befor D/c [illegible]onds.
2. y = y’.

Is it good for practical use?

Issues with the Kent, A., PRL 1999 protocol

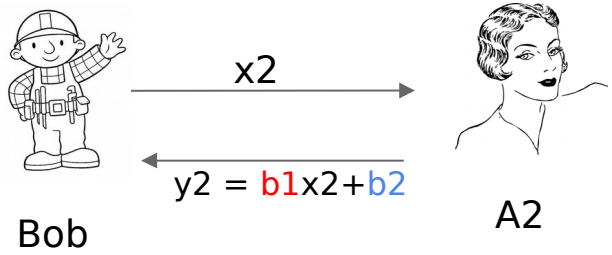
1. Needs multiple agents of Alice.

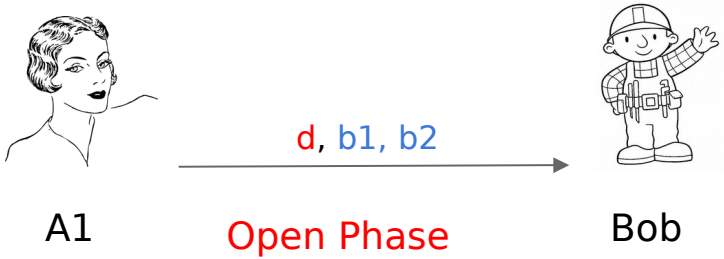
2. For practical purpose, needs two agents of Bob.

3. If the sustain phase is one year long, then A1, A2 should be separated by one light year.

INCREASING THE SUSTAIN TIME KEEPING D FIXED (LUNGHI ET AL., PRL 201

Time gap t < D/c.





Time gap t < D/c.

Total sustain time: 2t.

Security of k-round Lo-Chi et al.-protocol

Hiding Property: Perfectly hiding because, Bob doesn't
b2,...bk before the open phase.

Binding Property: Nontrivial.

- $\epsilon \leqslant \exp(-n/2^k)$ [Lung
  - Still impractical

- $\epsilon \leqslant 2k\sqrt{(2^{-}}$ akraborty et al. PRL, 2015, Fehr et
  ypt 2015.]

The problem is open against the quantum adversaries.

are true against the classical adversaries.

What about the other primitives?

EXISTING RESULTS

1. Oblivious transfer (OT) is not possible in the relativistic setting.

2. OT is possible under non-communication assumptions.

3. Single-round Zero-Knowledge proofs are possible in the relativistic setting.

Open problems

1. Security against quantum adversaries for the multi-round bit commitment protocols.

2. Increase the efficiency of the multi-round relativistic bit commitment protocols.

3. Design secure multi-round zero-knowledge proofs.

THANK YOU FOR YOUR ATTENTI ON