CRYPTOGRAPHIC APPLICATIONS OF QUANTUM MECHANICS

Thomas Attema – Thomas.Attema@tno.nl

TNO innovation for life


QUANTUM TECHNOLOGY
OPPORTUNITY FOR CRYPTOGRAPHY
THREAT TO CRYPTOGRAPHY

CONTENT

- *Observer effect*
  - Quantum key distribution
  - Quantum authentication

- *No-cloning theorem*
  - Position verification

- *Entanglement*
  - Device independent cryptography

OBSERVER EFFECT

THE OBSERVER EFFECT

- The observation of a physical state changes that state
  - This effect can often be made negligible

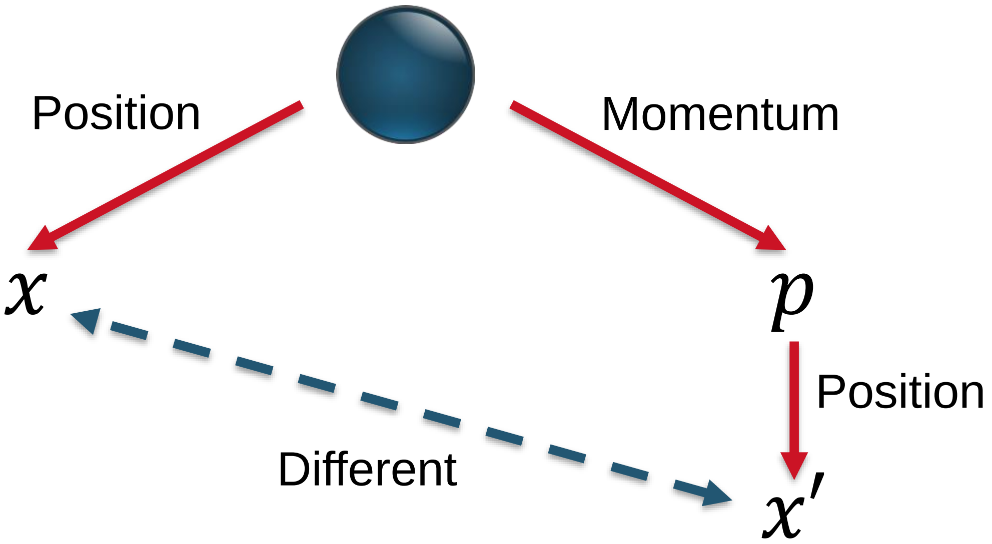
HEISENBERG’S UNCERTAINTY PRINCIPLE

- Heisenberg thought to have captured the observer effect in his uncertainty principle

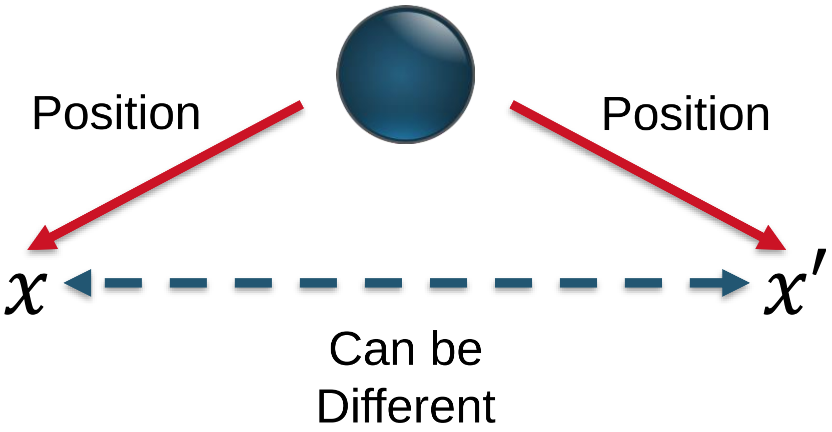
- **Position** versus **momentum** of particles

- This uncertainty is ***not*** caused by the measurement
  - Inherent property of quantum mechanics

HEISENBERG'S UNCERTAINTY PRINCIPLE

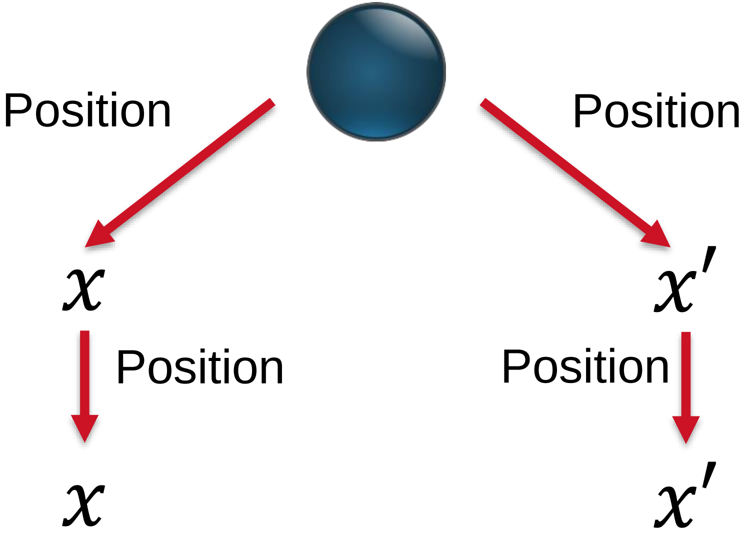


THE SAME ACTION CAN HAVE DIFFERENT CONSEQUENCES



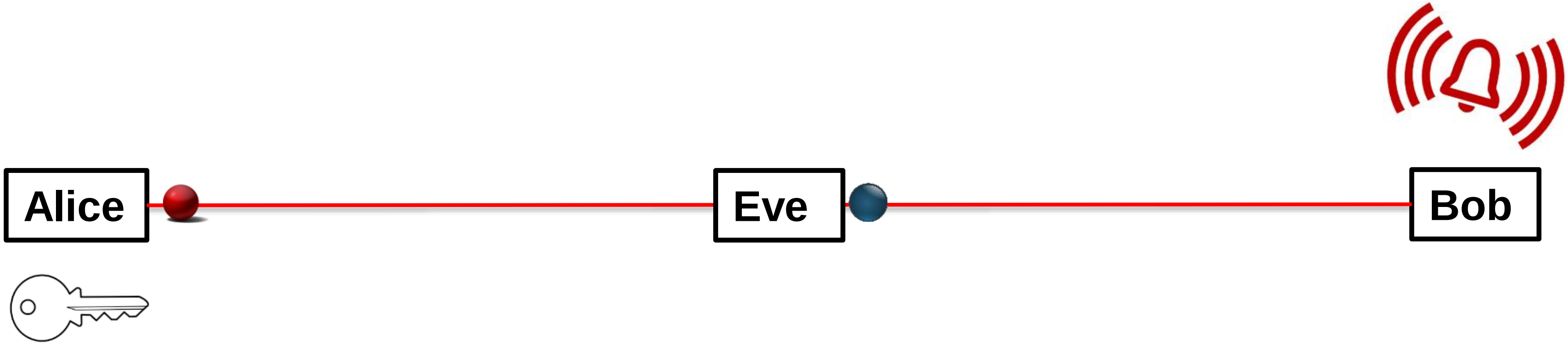
OBSERVER EFFECT IN QUANTUM MECHANICS

- Measurements cause states to ***collapse***
- Often the observer effect is used to describe this phenomenon
- Application:
  - Quantum key distribution



QUANTUM KEY DISTRIBUTION

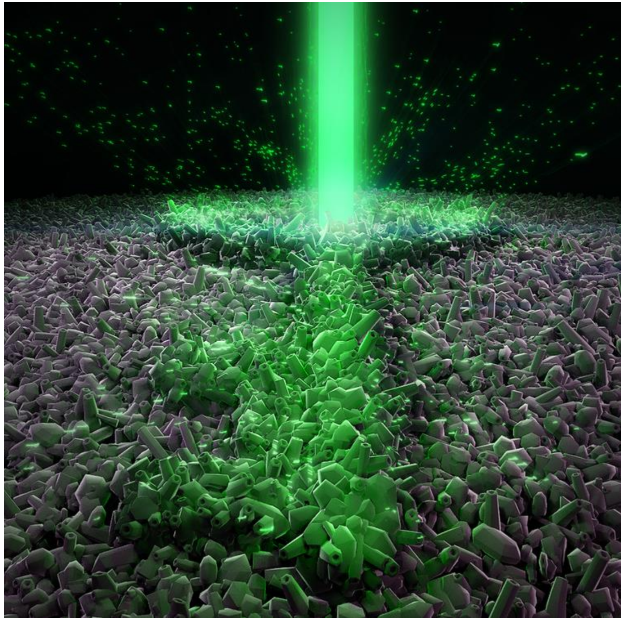
- Intuitively - Security based on the observer effect



QUANTUM AUTHENTICATION

- Physical Unclonable Functions (PUFs)
  - Digital fingerprint

- Risk
  - Digital emulation



PUF - CLASSICAL AUTHENTICATION

Challenge	Response
c_1	r_1
c_2	r_2
c_3	r_3
c_4	r_4

Alice' PUF

c

r

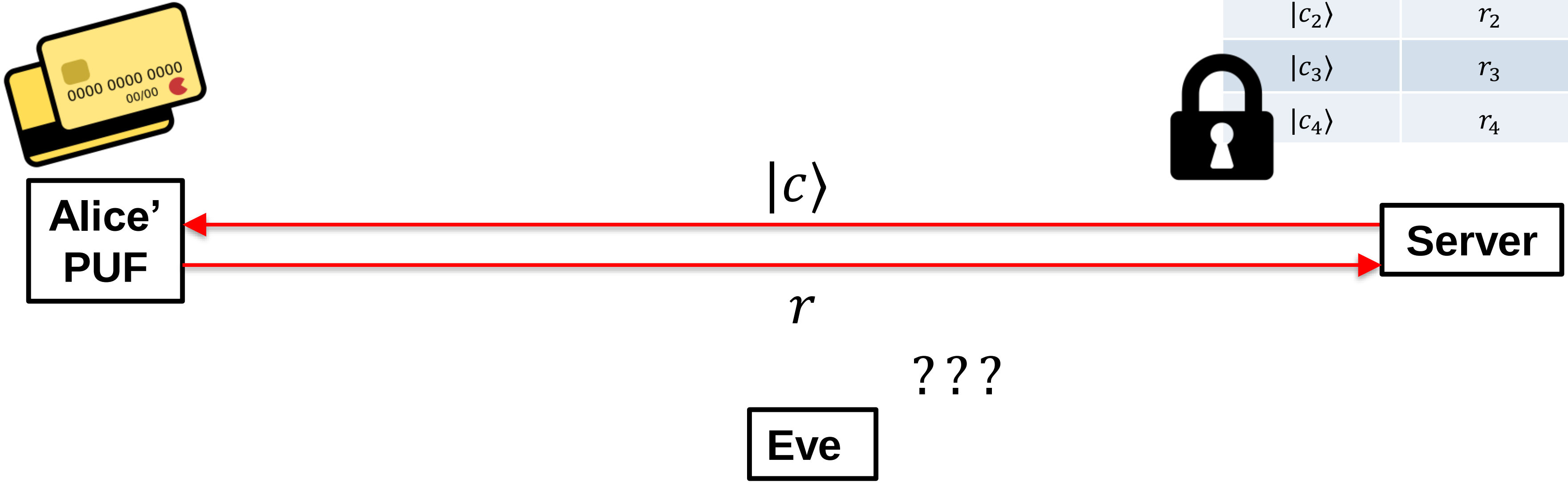
Server

Eve

Challenge	Response
c	r

QUANTUM AUTHENTICATION

Challenge	Response
$\vert c_1\rangle$	r_1
$\vert c_2\rangle$	r_2
$\vert c_3\rangle$	r_3
$\vert c_4\rangle$	r_4



NO-CLONING THEOREM

CLONING QUANTUM MECHANICAL STATES IS IMPOSSIBLE

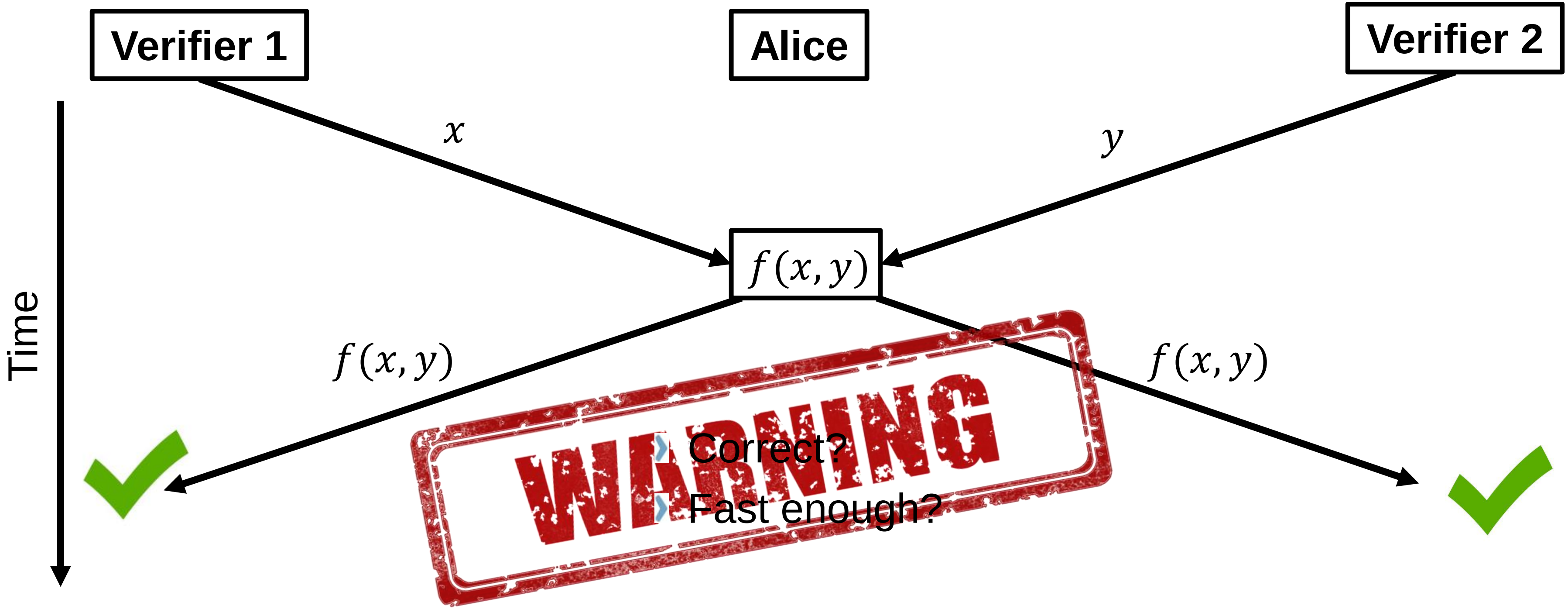
- By cloning one could measure quantum states without collapsing them
  - QKD would not be secure

POSITION BASED CRYPTOGRAPHY

- Authenticate solely based on geographical location
- Security assumption
  - Communication faster than the speed of light is impossible

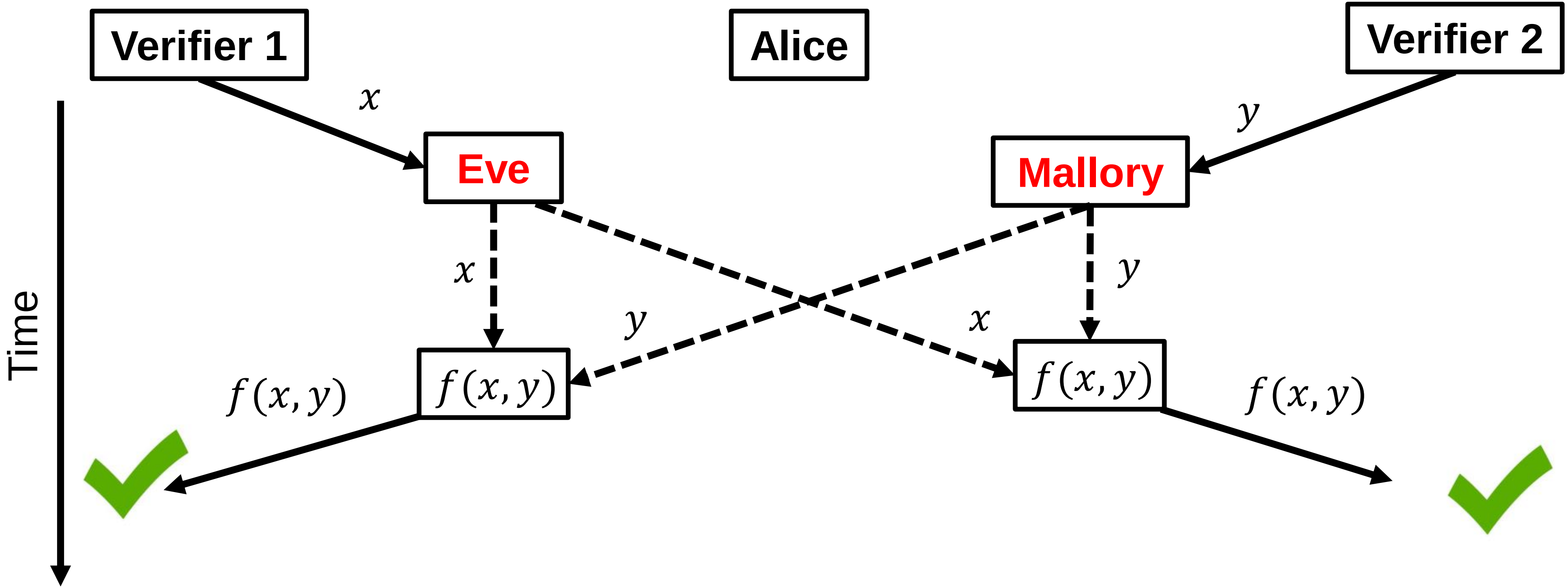
innovation for life

POSITION VERIFICATION – NAÏVE PROTOCOL

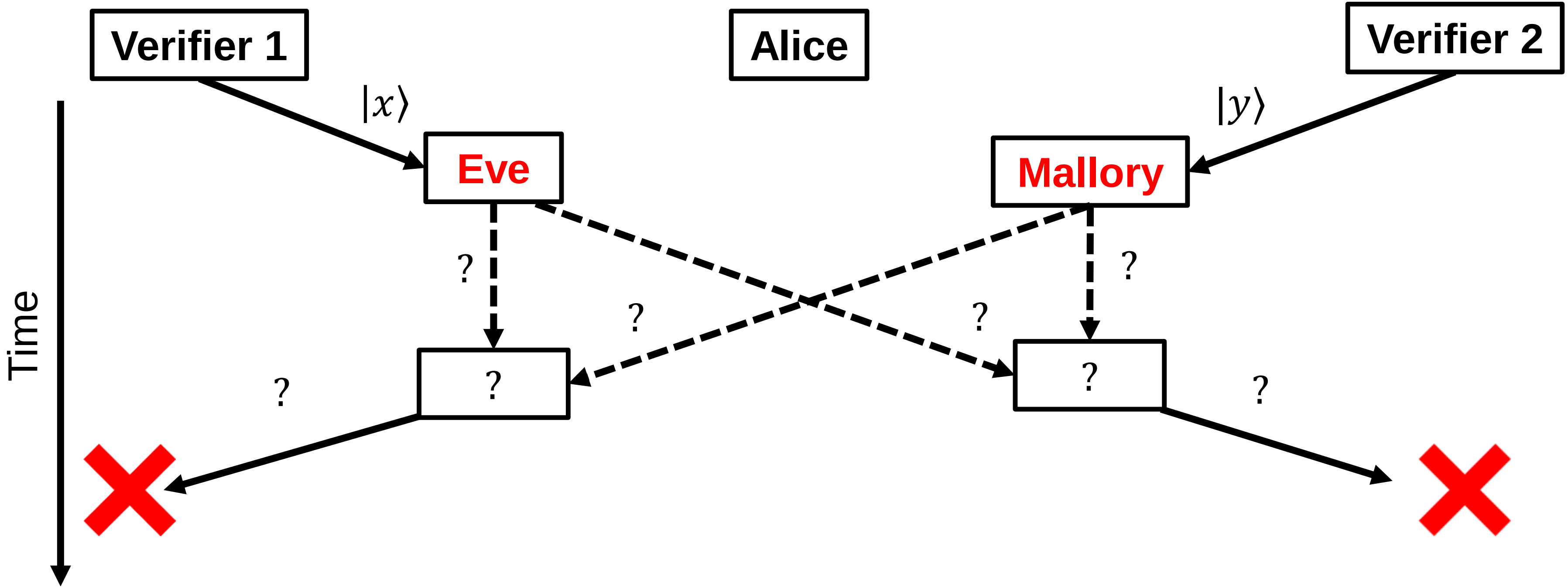


- Correct?
- Fast enough?

POSITION VERIFICATION – NAÏVE PROTOCOL



QUANTUM POSITION VERIFICATION



DISCLAIMER - QUANTUM POSITION VERIFICATION

- Quantum mechanics only gives a partial solution

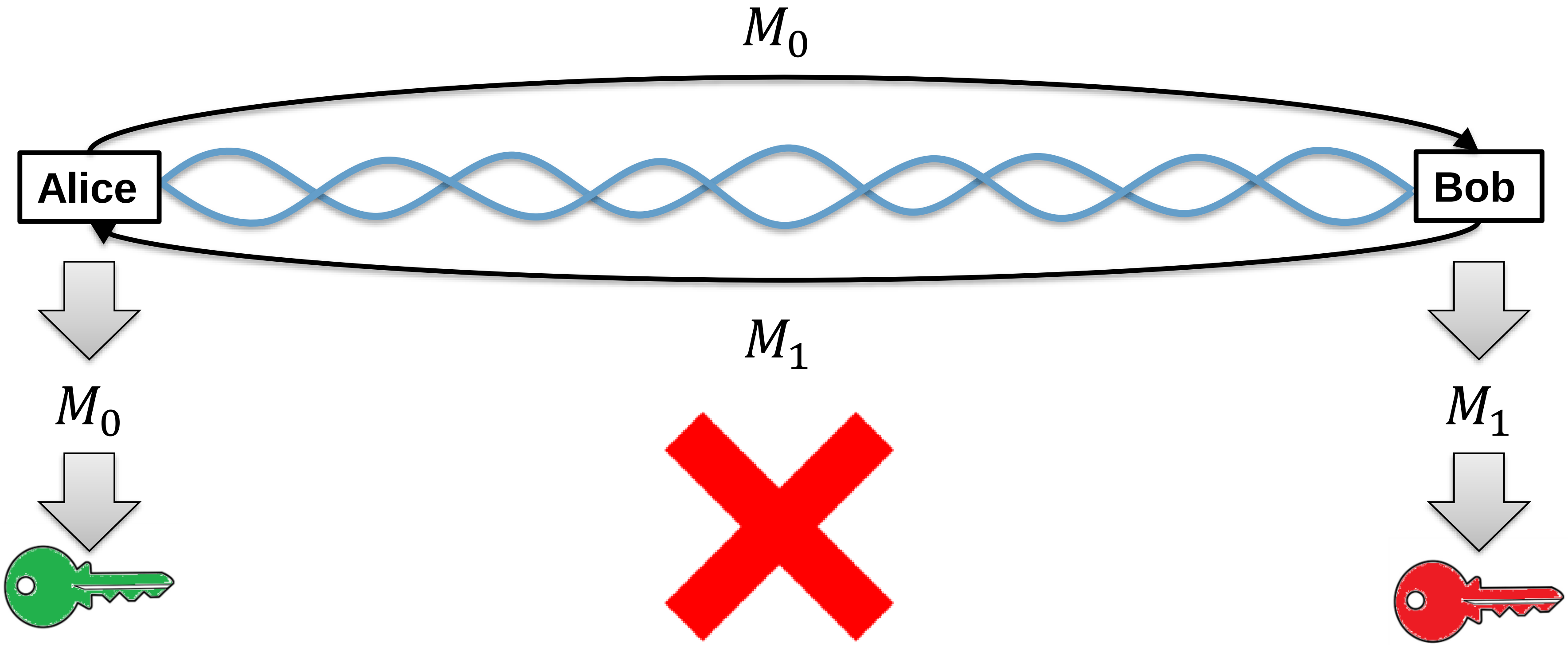
- More advanced quantum attacks exist to break the above scheme
  - New assumptions on the adversary are required

ENTANGLEMENT

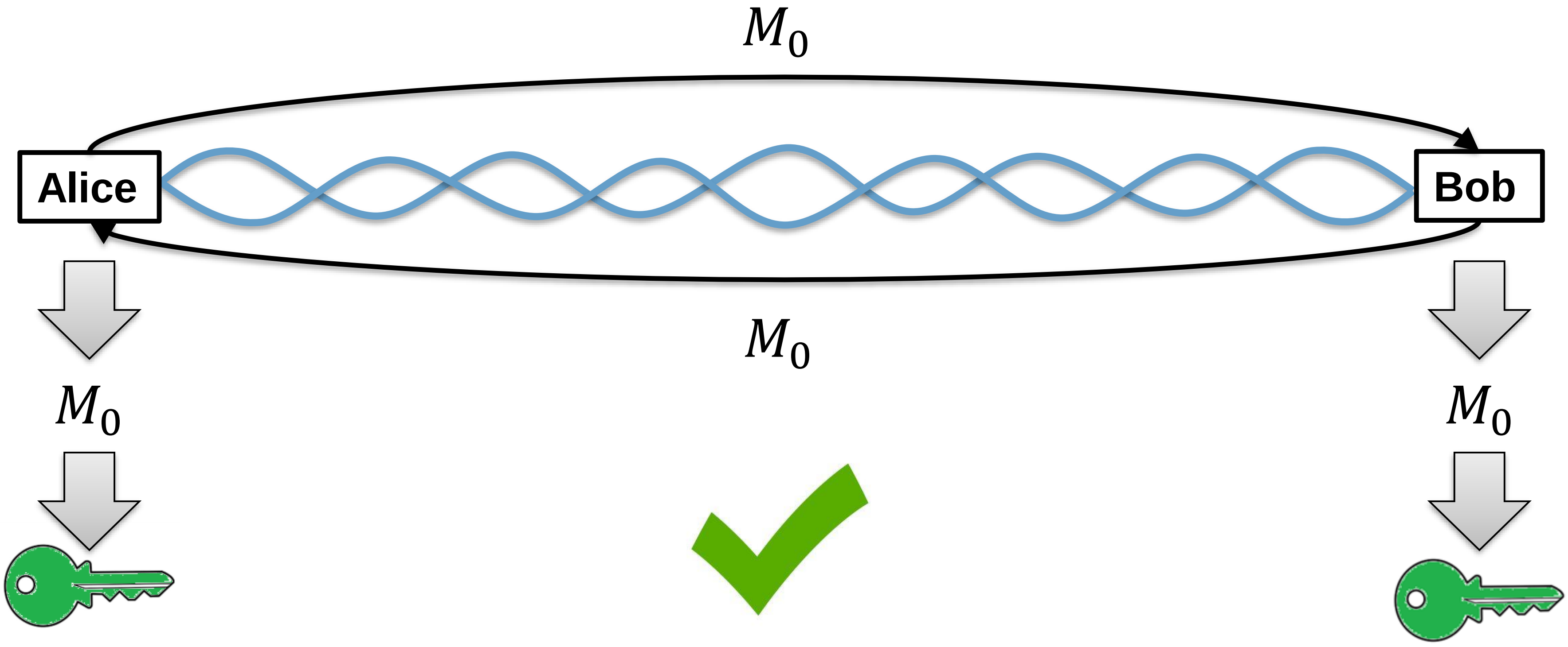
ENTANGLEMENT

- Entangled states can not be described without referring to each other
  - Even if they are separated
- This results in correlations that can not exist classically
- Quantum mechanics is a ***non-local*** theory
  - Does not violate relativity

ENTANGLEMENT BASED KEY DISTRIBUTION



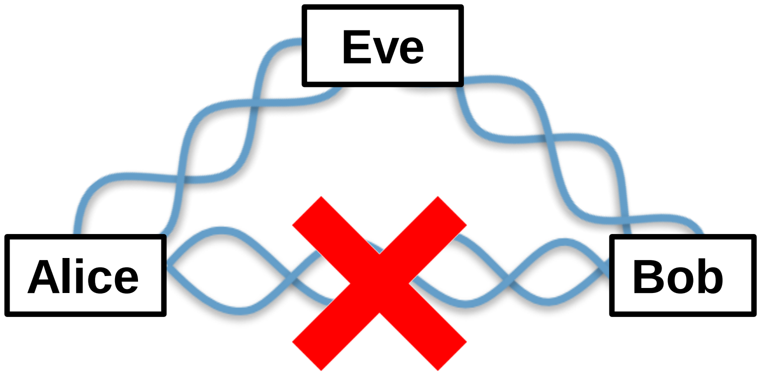
ENTANGLEMENT BASED KEY DISTRIBUTION



ENTANGLEMENT BASED KEY DISTRIBUTION

- Security follows from monogamy of entanglement
  - *Two maximally entanglement particles can not be entangled to a third particle*

- Device independent key distribution
  - QKD where we do not have to trust the devices or manufacturer



SUMMARY

- Quantum mechanics allows for cryptographic functionalities that are ***impossible*** classically

- But implementing these functionalities is challenging

THANK YOU FOR YOUR ATTENTION

Take a look:
TNO.NL/TNO-INSIGHTS

innovation
for life