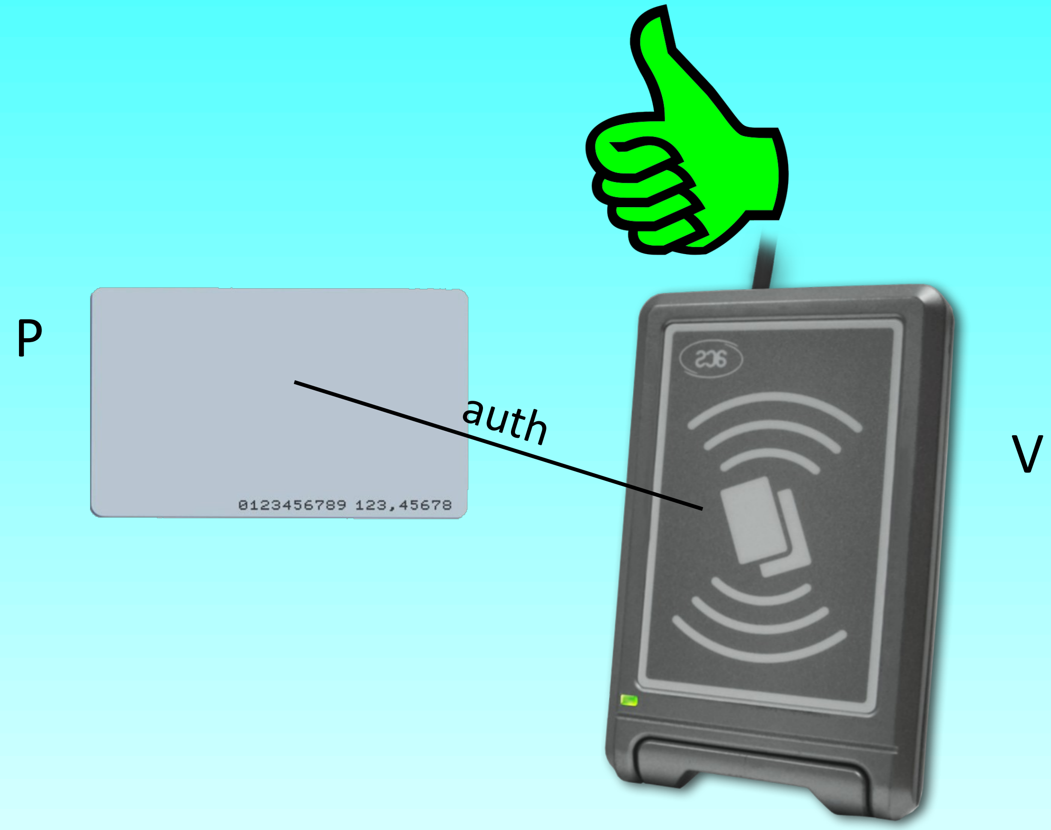
Security goes underground

PHY-layer attacks to secure localization

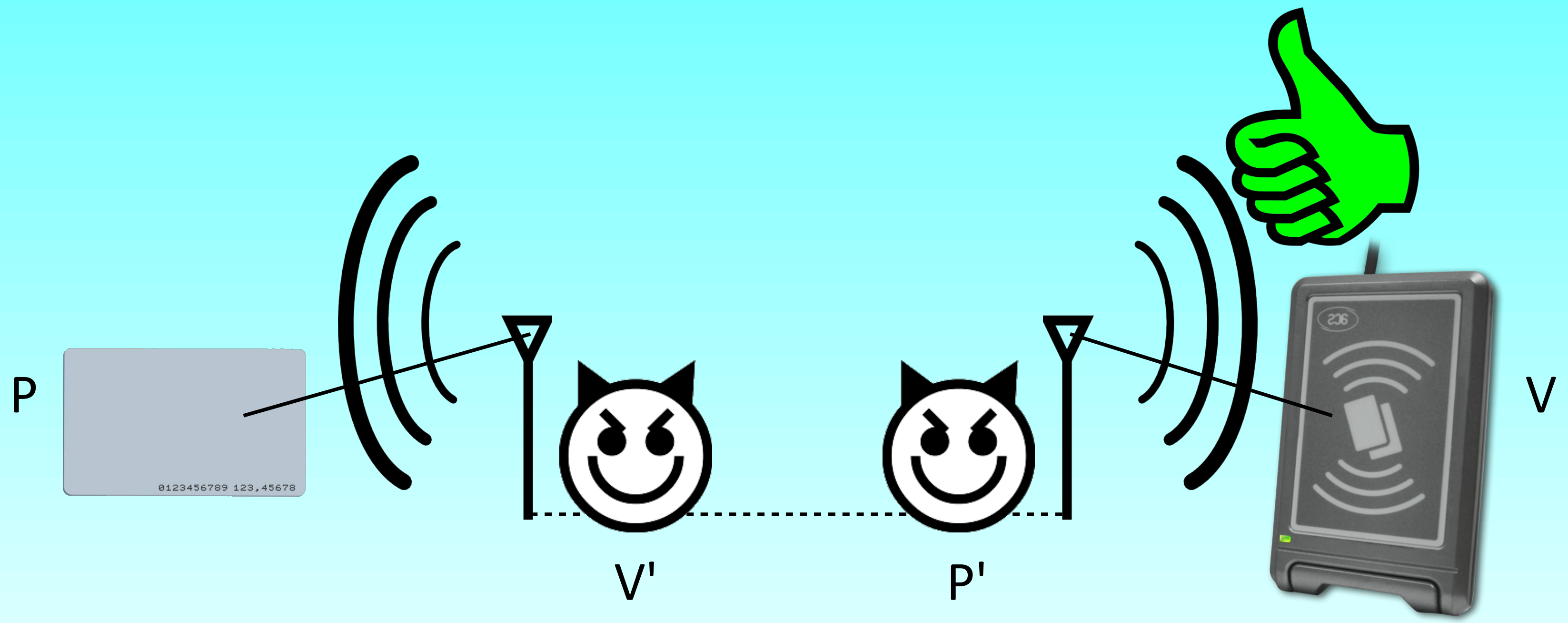
Secure localization

- Many systems rely explicitly or implicitly in location information (position, distance, proximity, etc.)

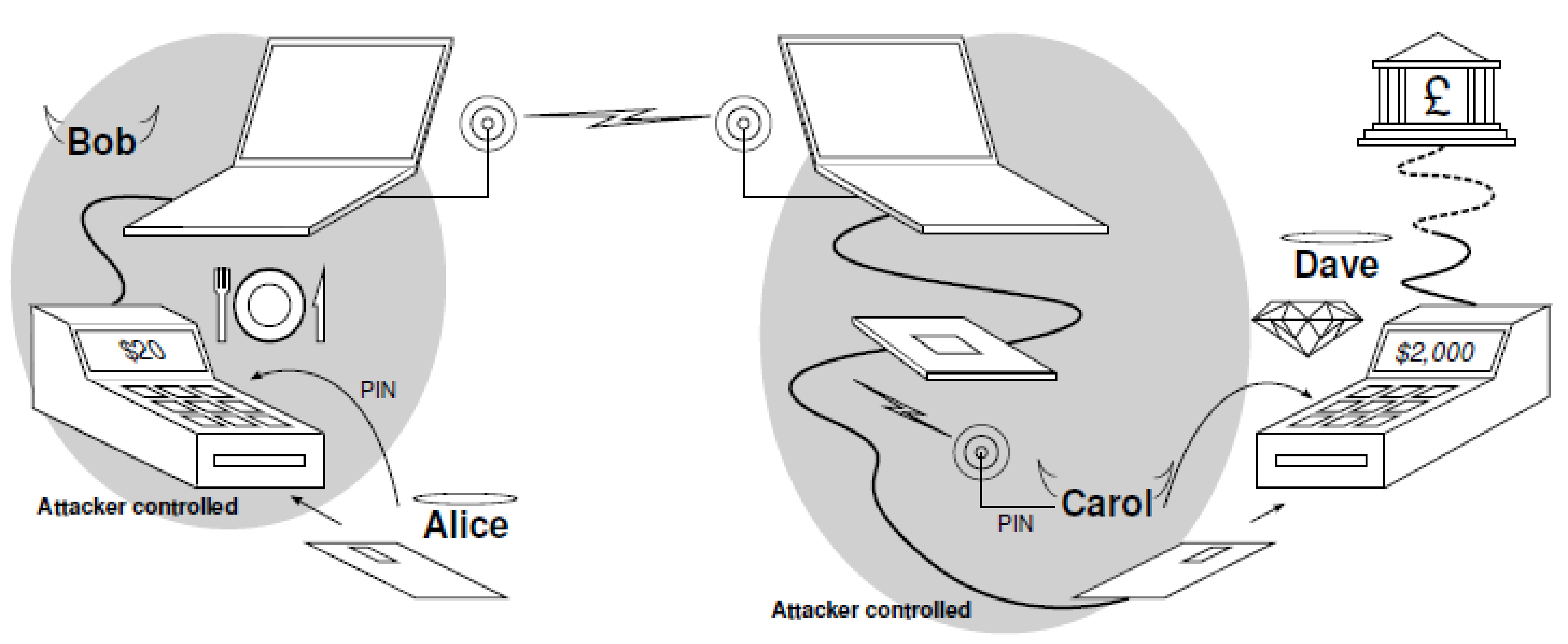
RFID access control



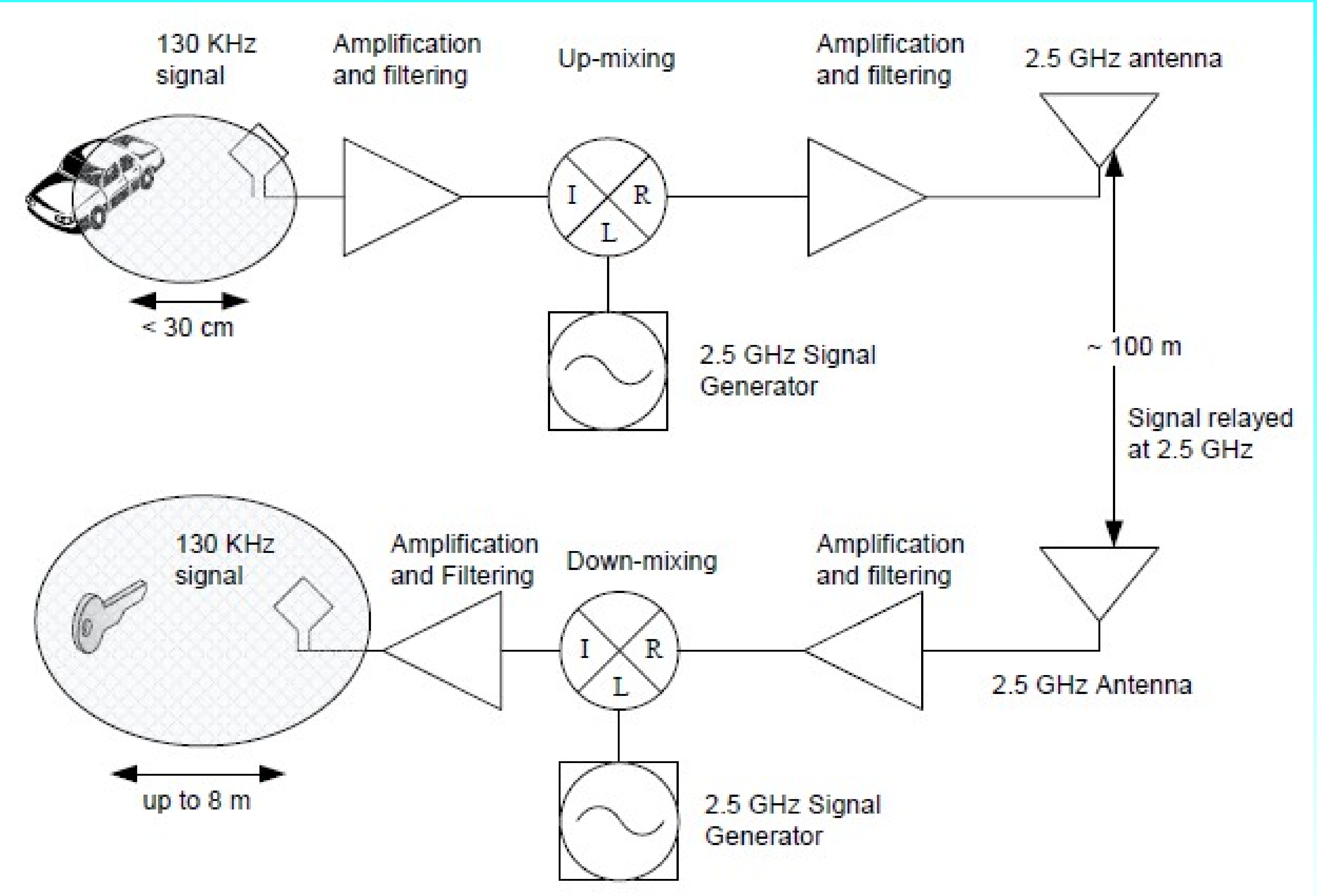
Relay attack



Mafia fraud

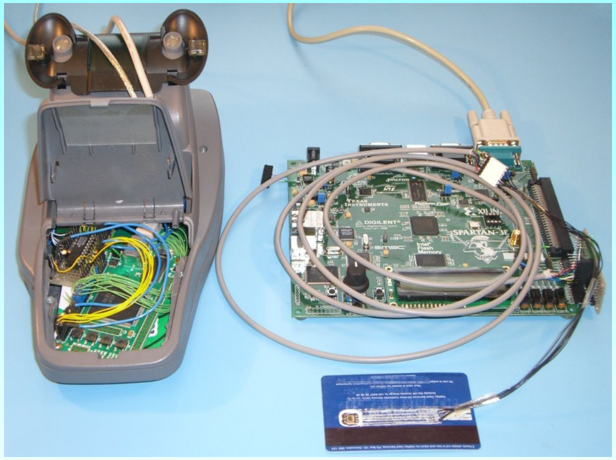

Bob
$20
PIN
Attacker controlled
Alice
£
Dave
$2,000
Carol
PIN
Attacker controlled

Relay attack



Other examples

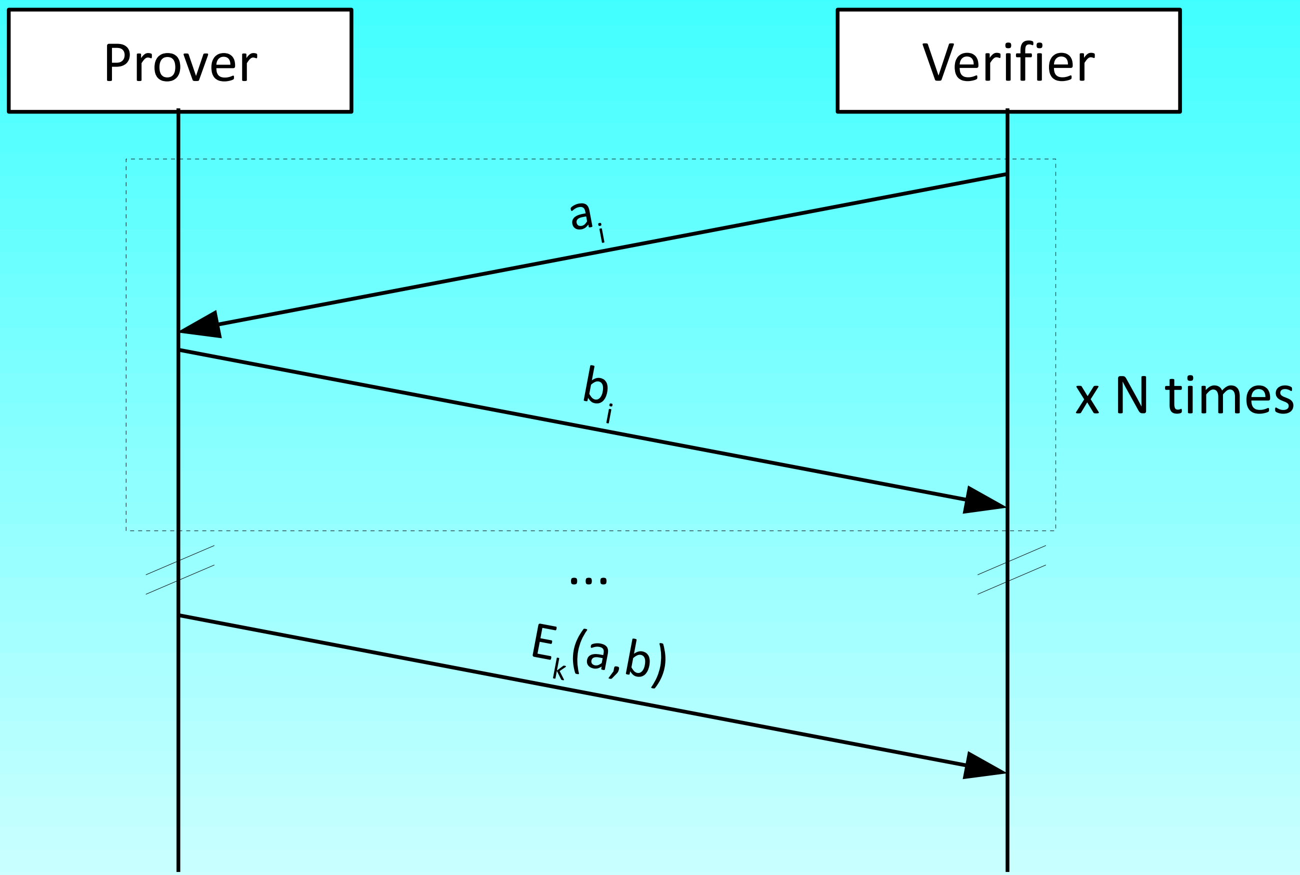
- Cargo tracking (GPS spoofing, performed in Russia, 1999)
- Electronic payments (mafia fraud, demonstrated in 2007)
- Passive keyless entry and start (relay attack, demonstrated in 2011)
- Wireless routing (wormhole attack)



Problem statement

- The verifier must be sure that:
  - he is talking with the prover (authentication),
  - the prover is actually in the proximity (proximity verification)

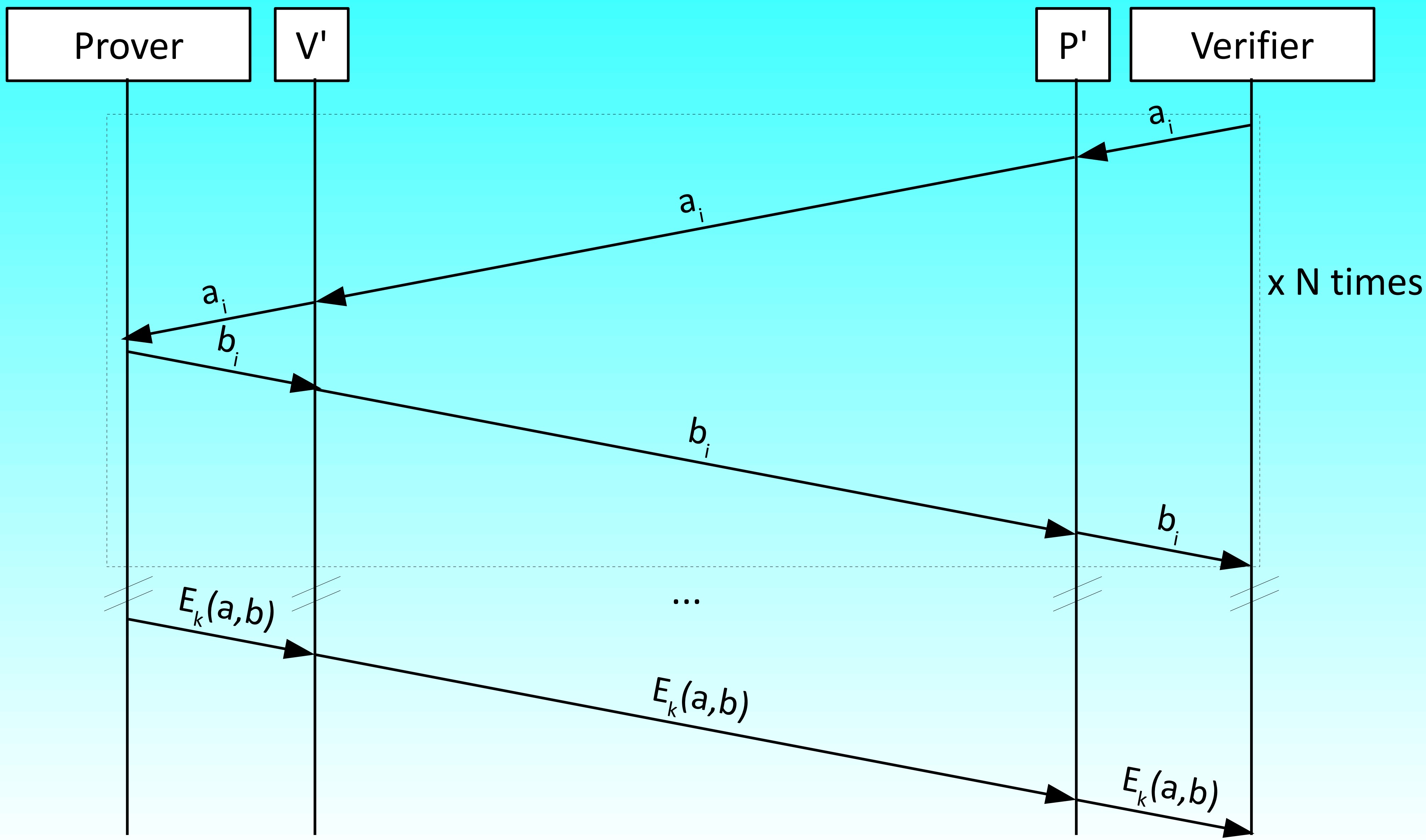
Distance bounding



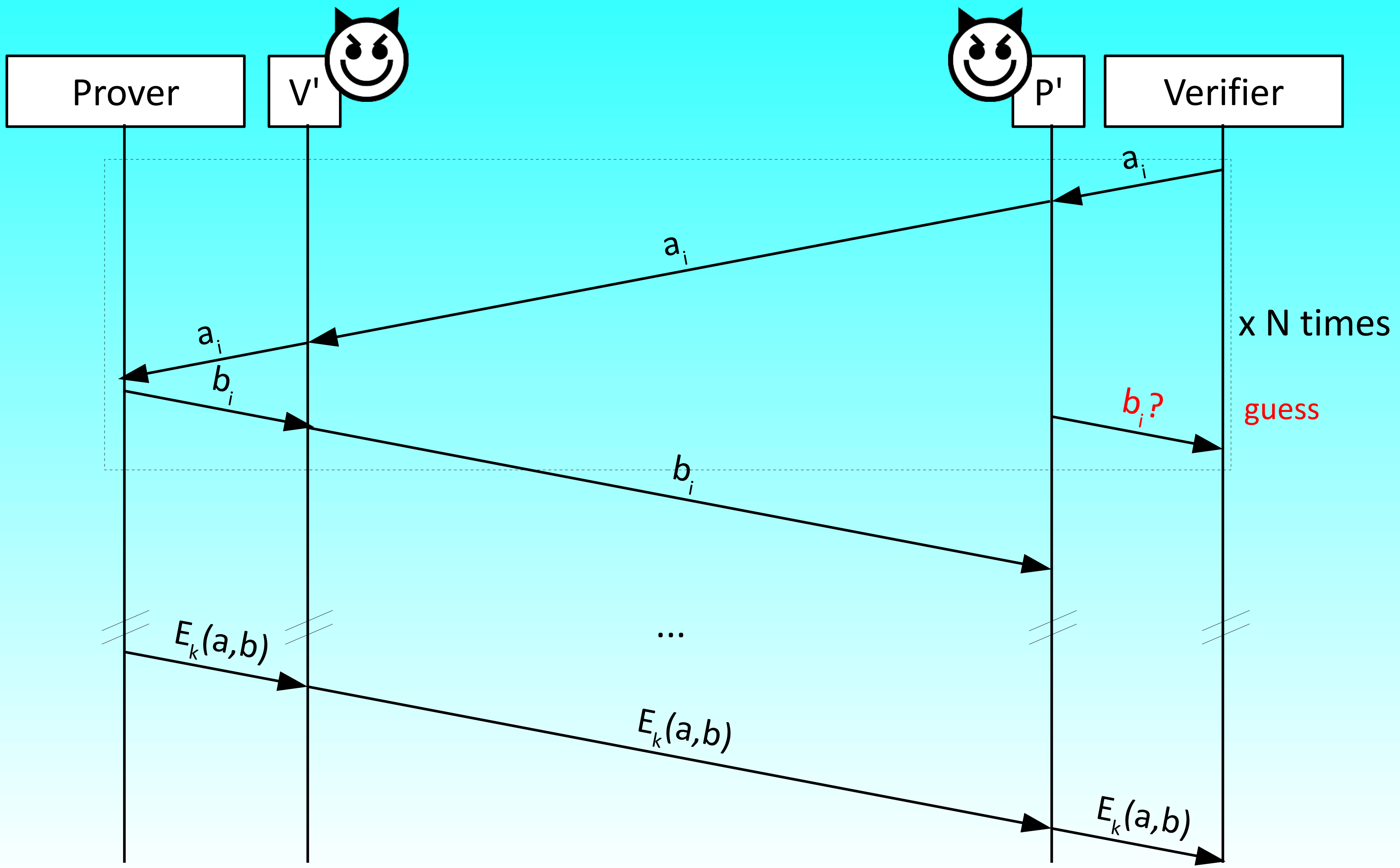
$d_{meas} = max_i\{RTT_i\}/2c$

$d <= d_{meas}$

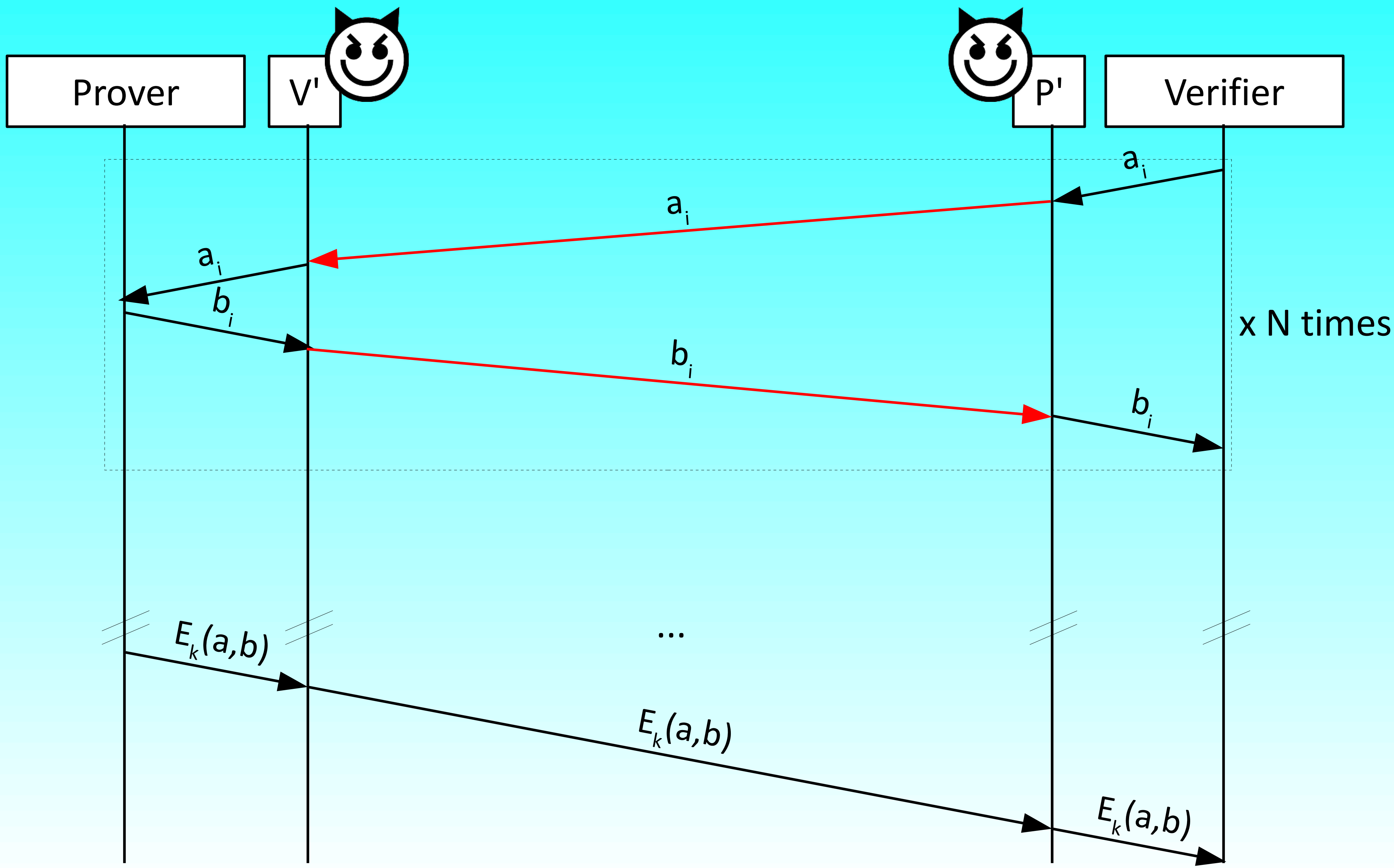
Distance bounding



Distance bounding



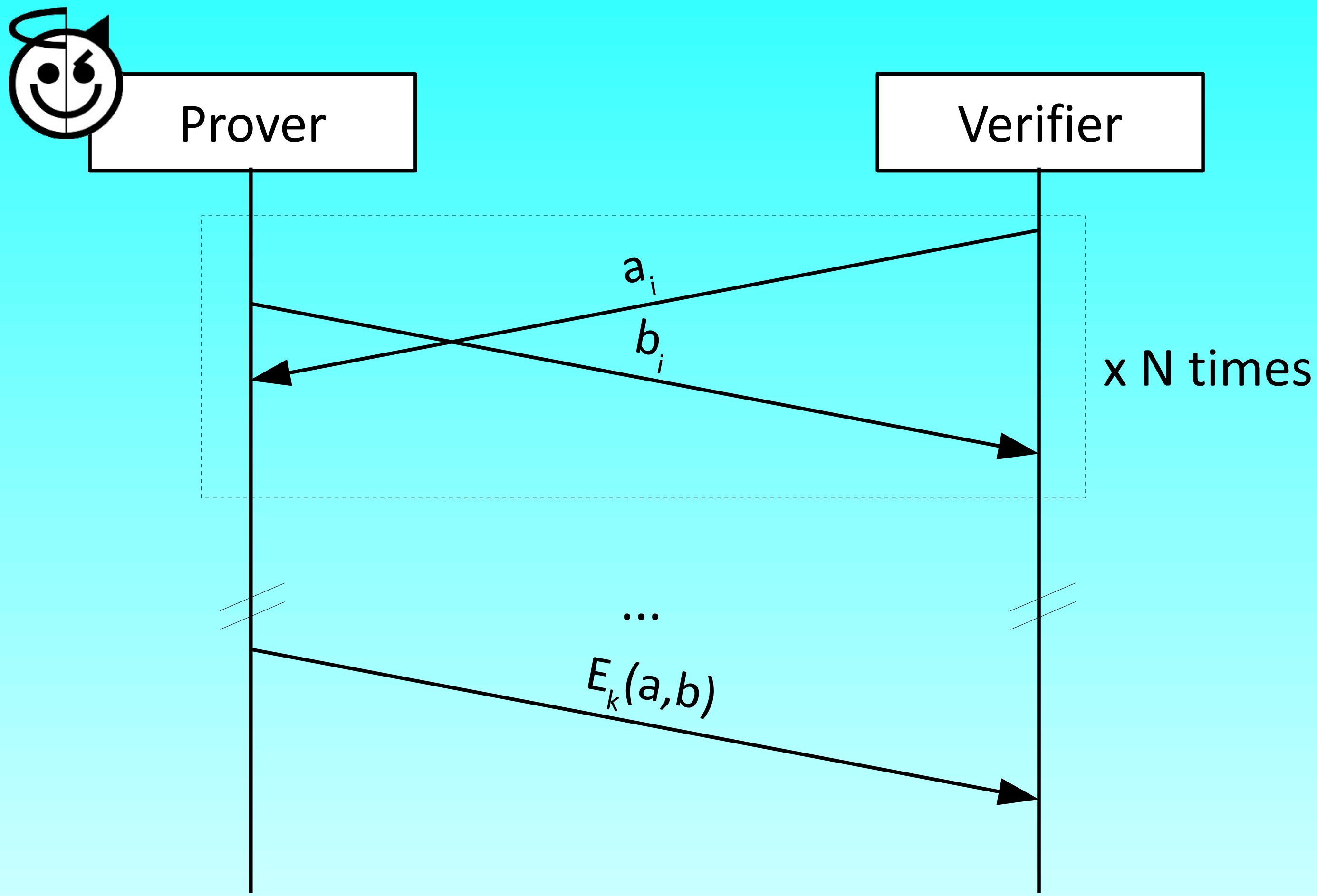
Distance bounding



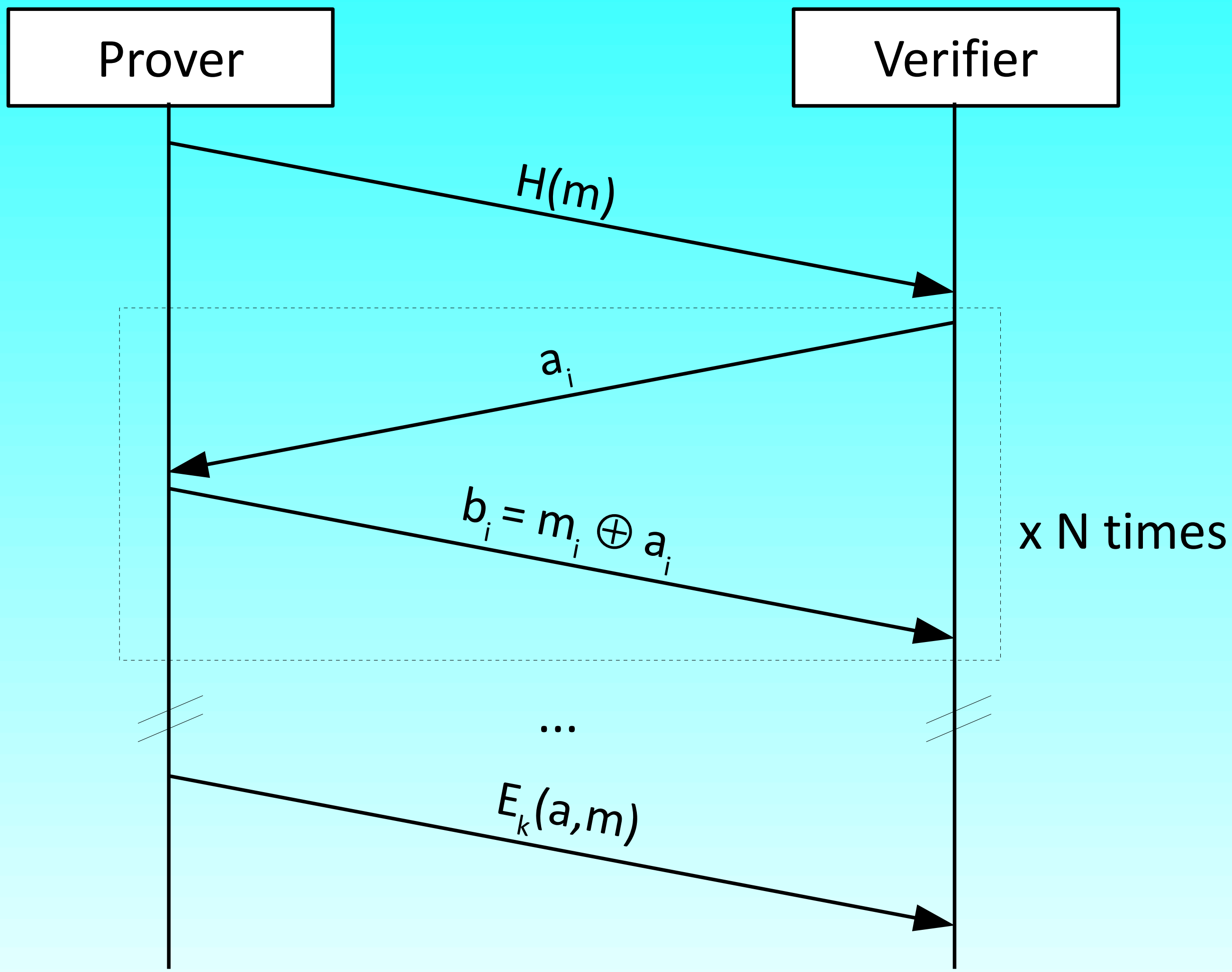
Distance fraud

- What happens if the prover has incentives to cheat?
- Employees can connect via Wi-Fi, but only from inside the office building, not from outside

Distance fraud



Distance bounding



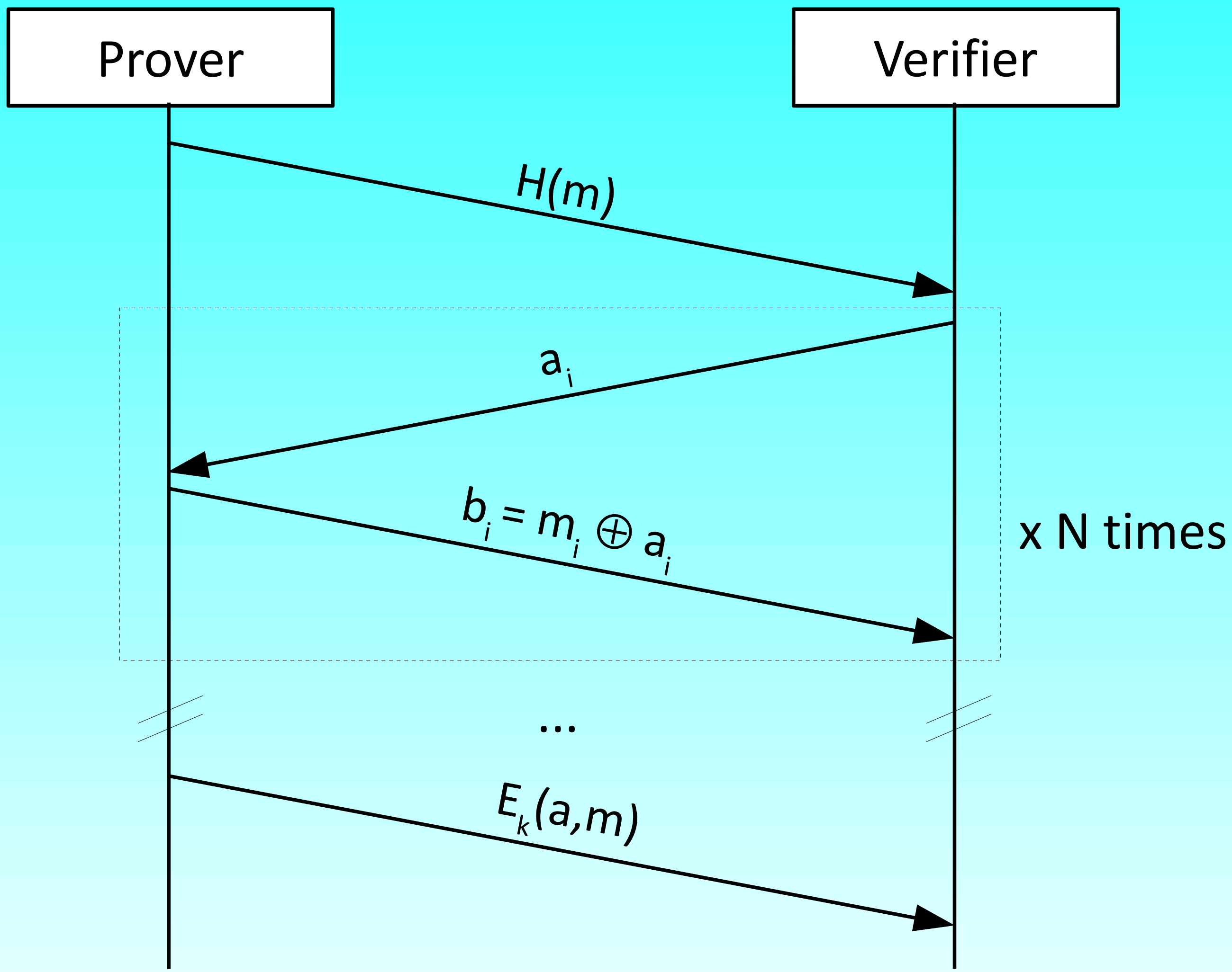
PHY-level attacks

- Outline:
  - PHY-level attacks on RFID
  - PHY-level attacks on sensors

Distance bounding on RFID

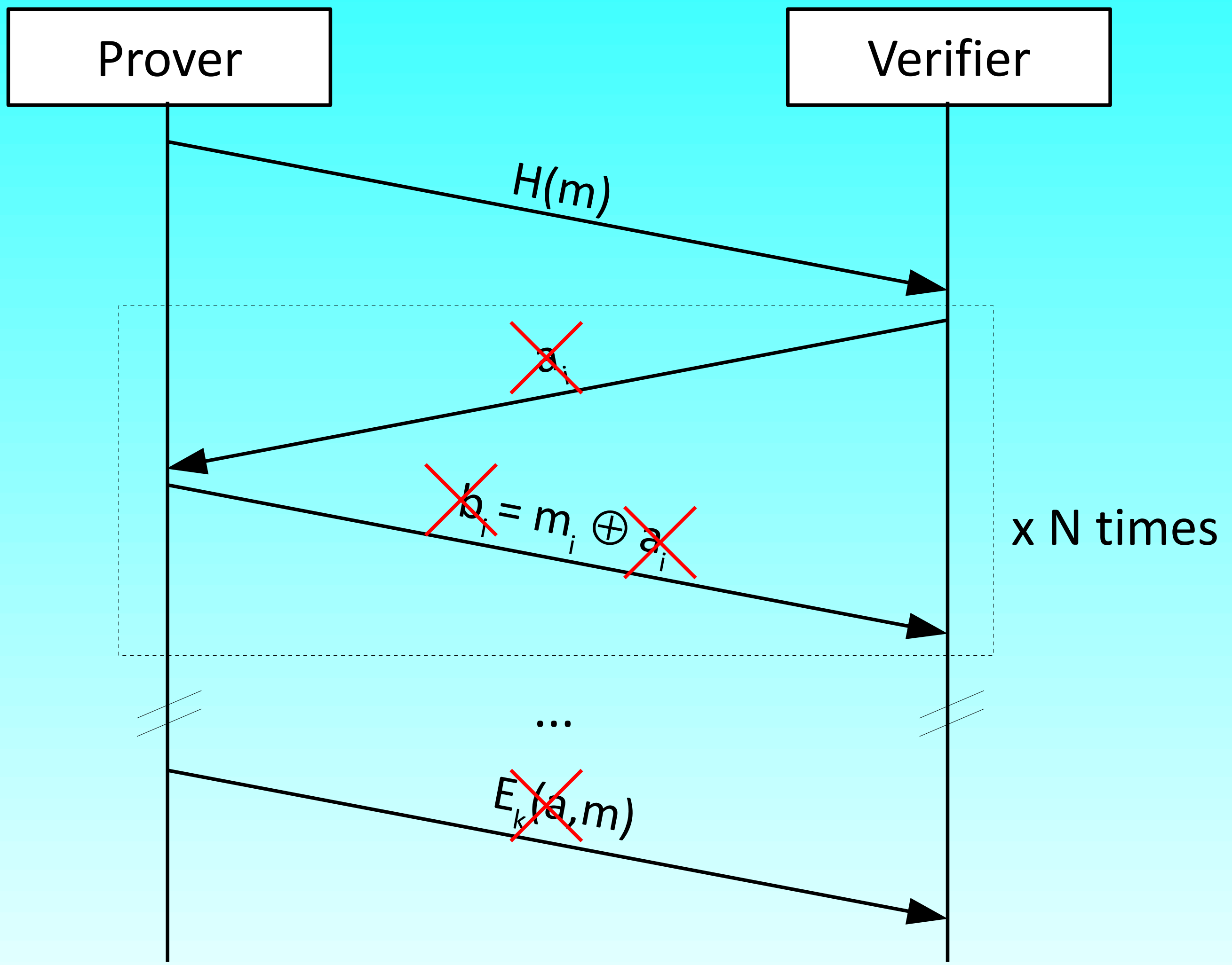
- Practical problems:
  - Resource-constrained devices
  - Passive tags
  - Noisy channels

Brands-Chaum protocol*

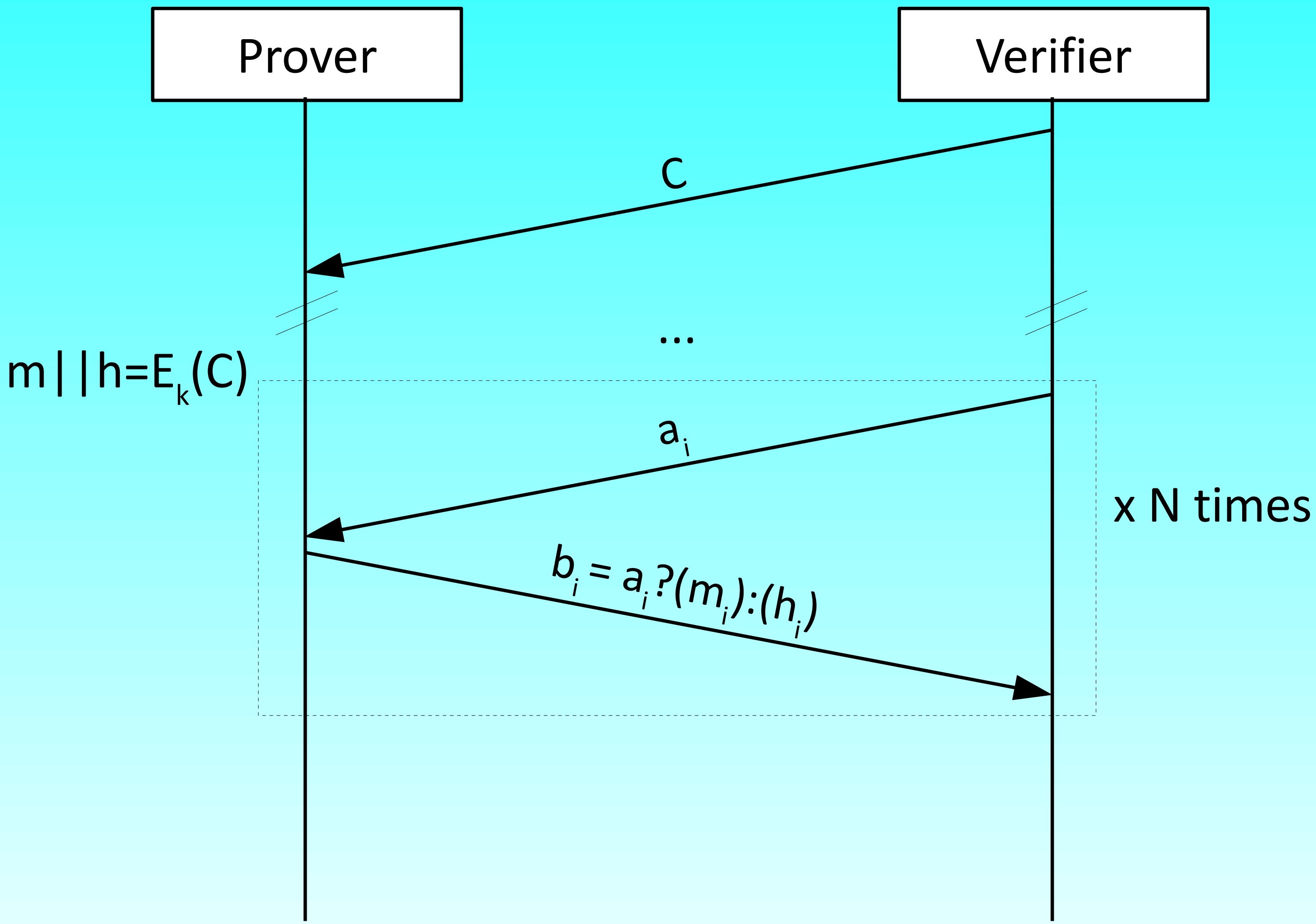


* 1994

Noise tolerance

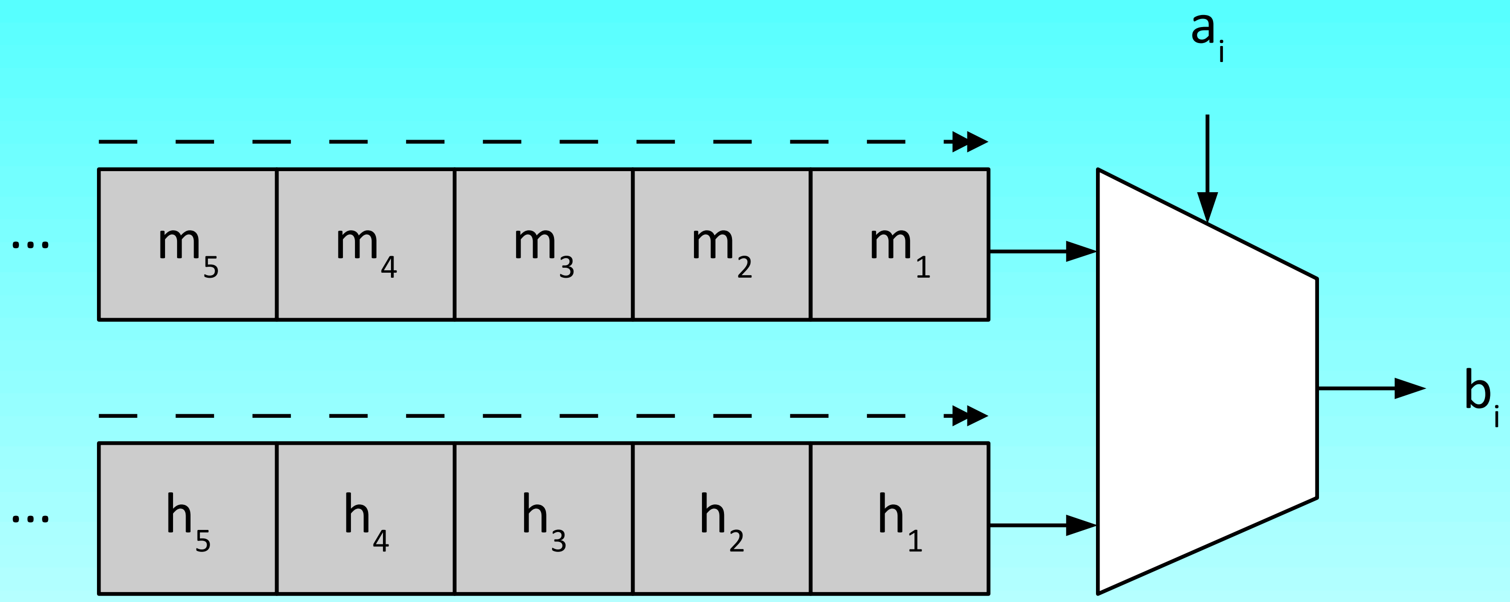


Hancke-Kuhn protocol*



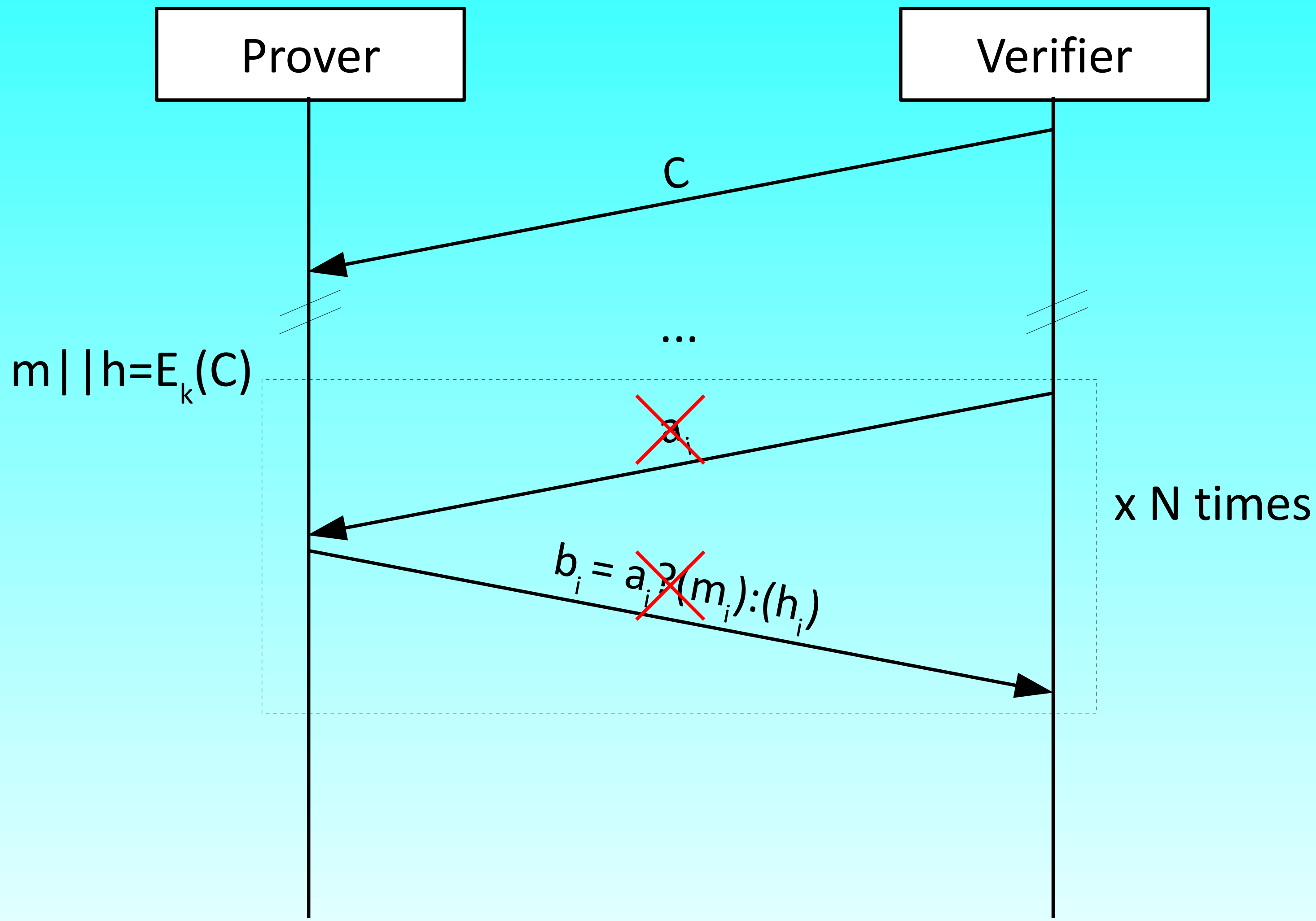
* 2005

Hancke-Kuhn protocol



Asynchronous realization

Noise tolerance



Noise tolerance

$$P(round\ success) = p$$

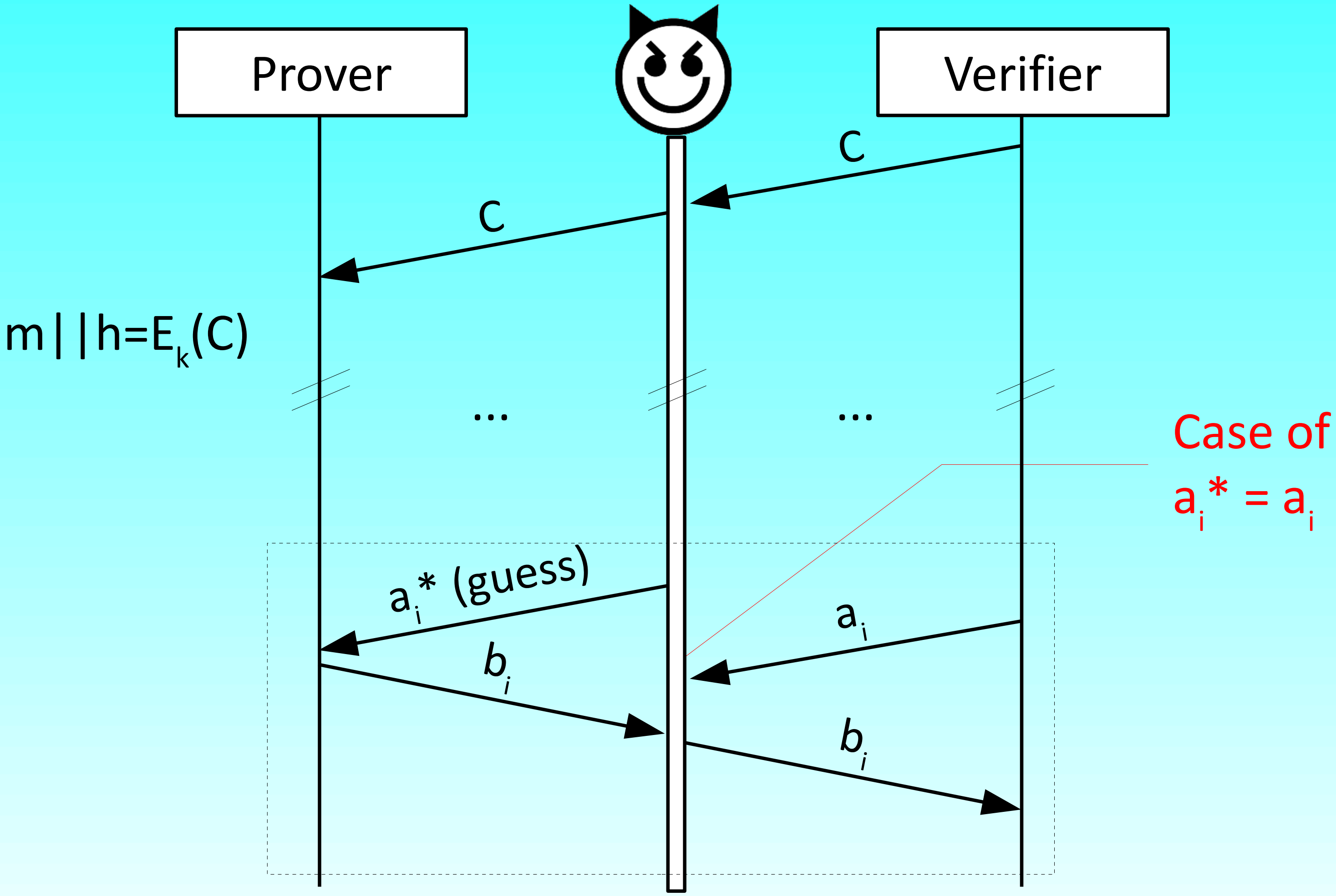
- Without error tolerance:

$$P(overall\ success) = (p)^N$$

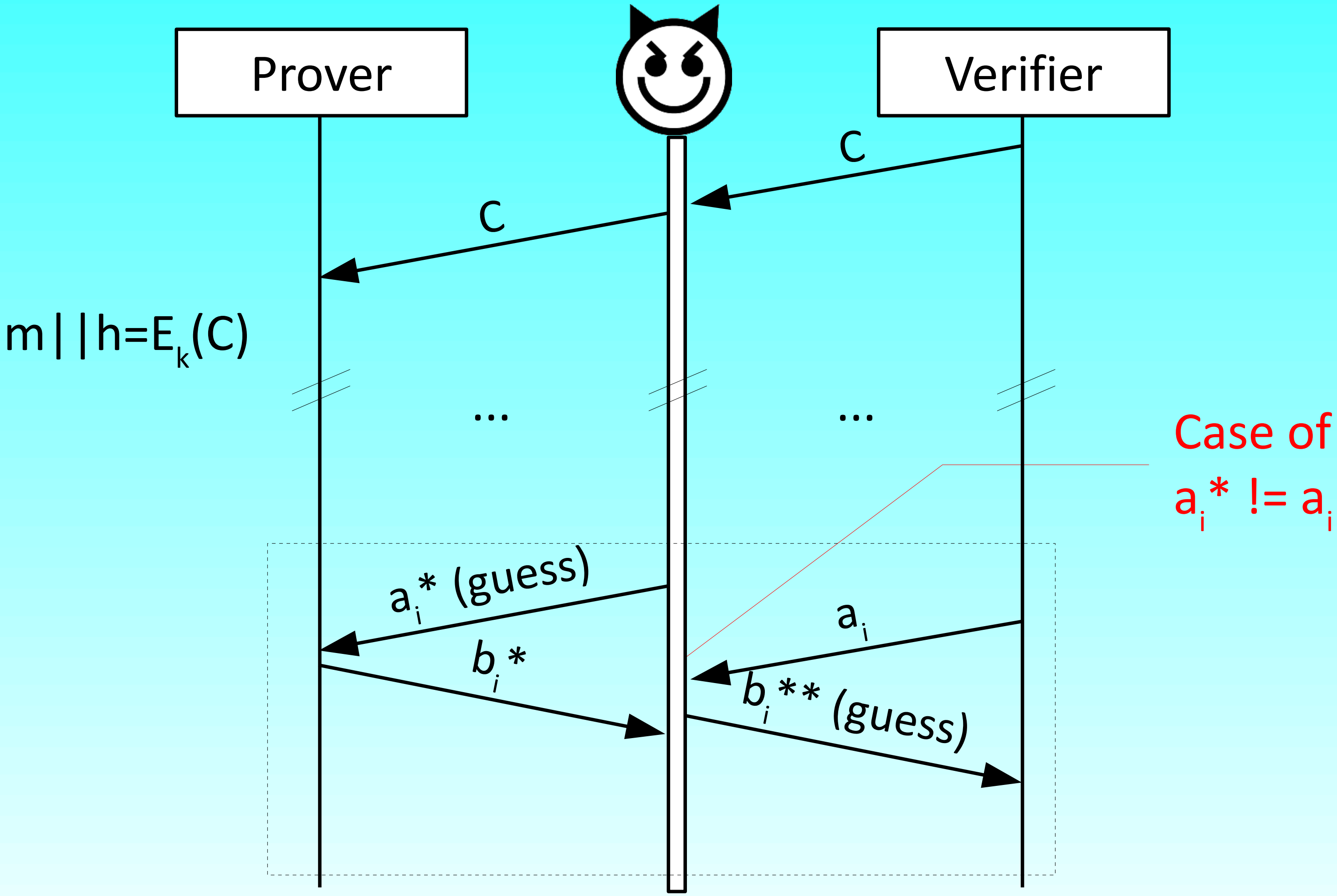
- With error tolerance (at least K bits must be correct):

$$P(overall\ success) = \sum_{i=K}^{N} \binom{N}{i} \cdot (p)^i \cdot (1-p)^{N-i}$$

Double-guess attack

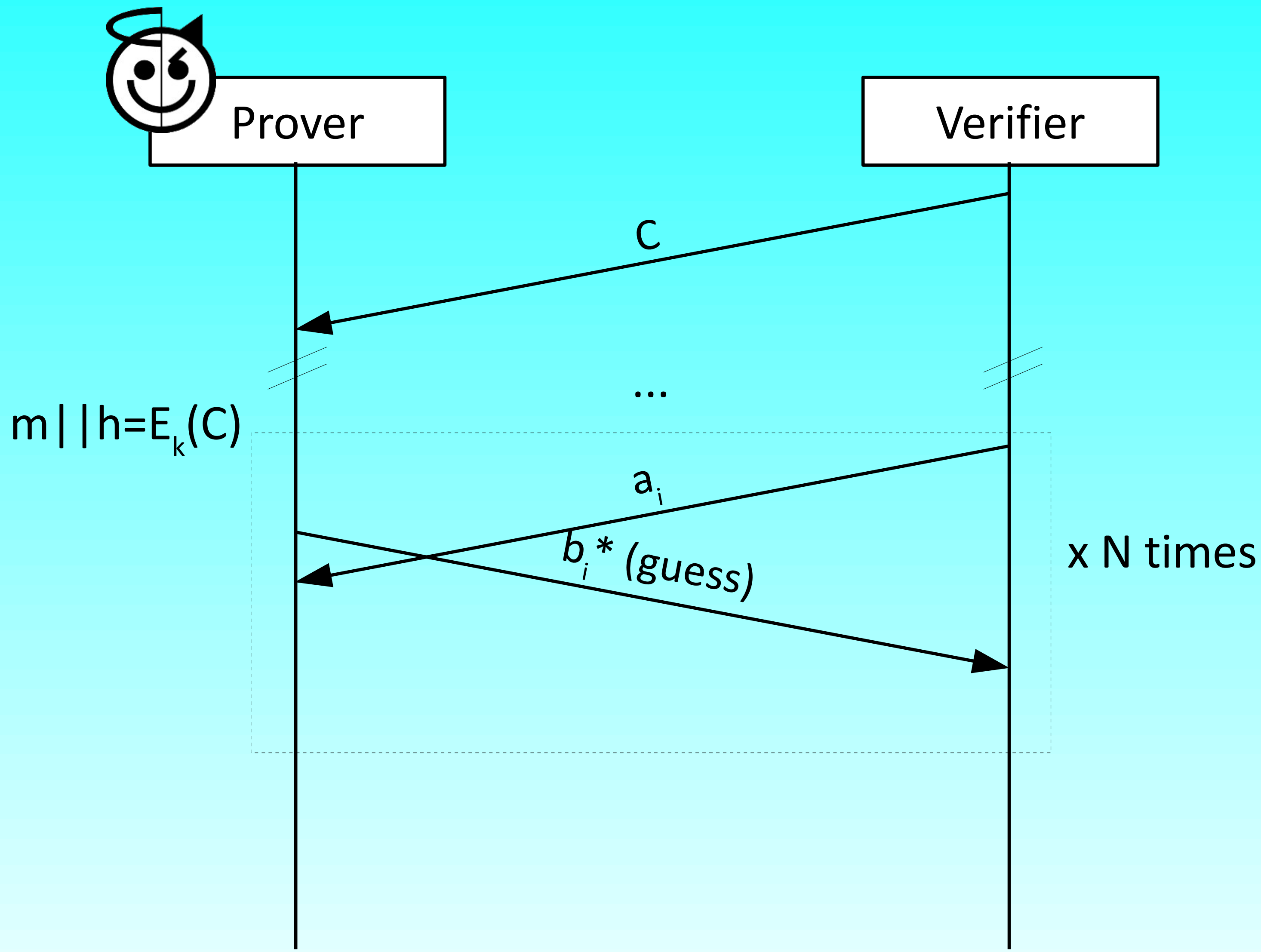


Double-guess attack

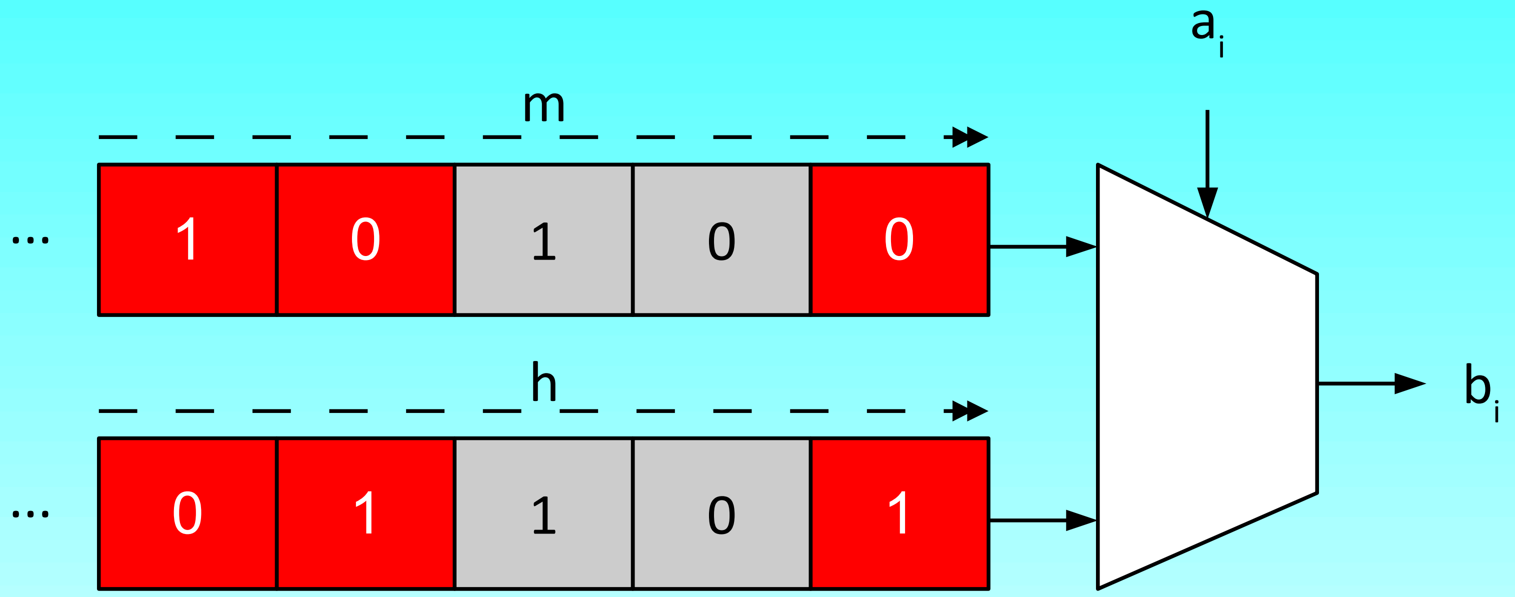


P(round success) = 3/4

Internal-guess attack



Internal-guess attack



P(round success) = 3/4

Overall security

- Brands-Chaum (N=128):

$$P(overall\ success) \approx 2.9 \cdot 10^{-39}$$

- Hancke-Kuhn (N=128, K=126):

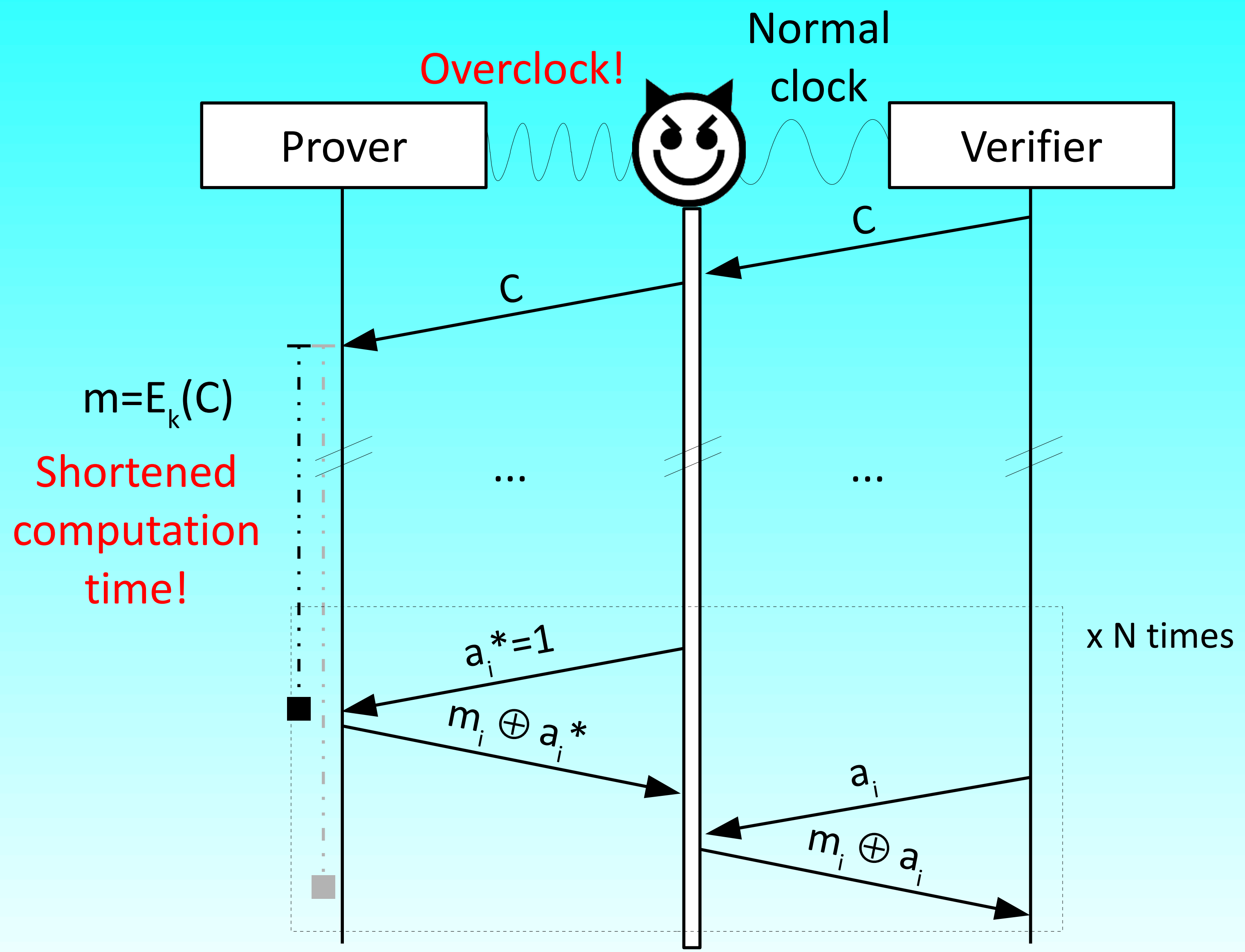
$$P(overall\ success) \approx 1.9 \cdot 10^{-13}$$

Efficiency improvement

- To offer the same security level of Brands-Chaum, the number of rounds (N) must be twice
- The RBE phase is less efficient, but:
  - resists to noise
  - does not need the final signature message
  - needs only one prover-side crypto function

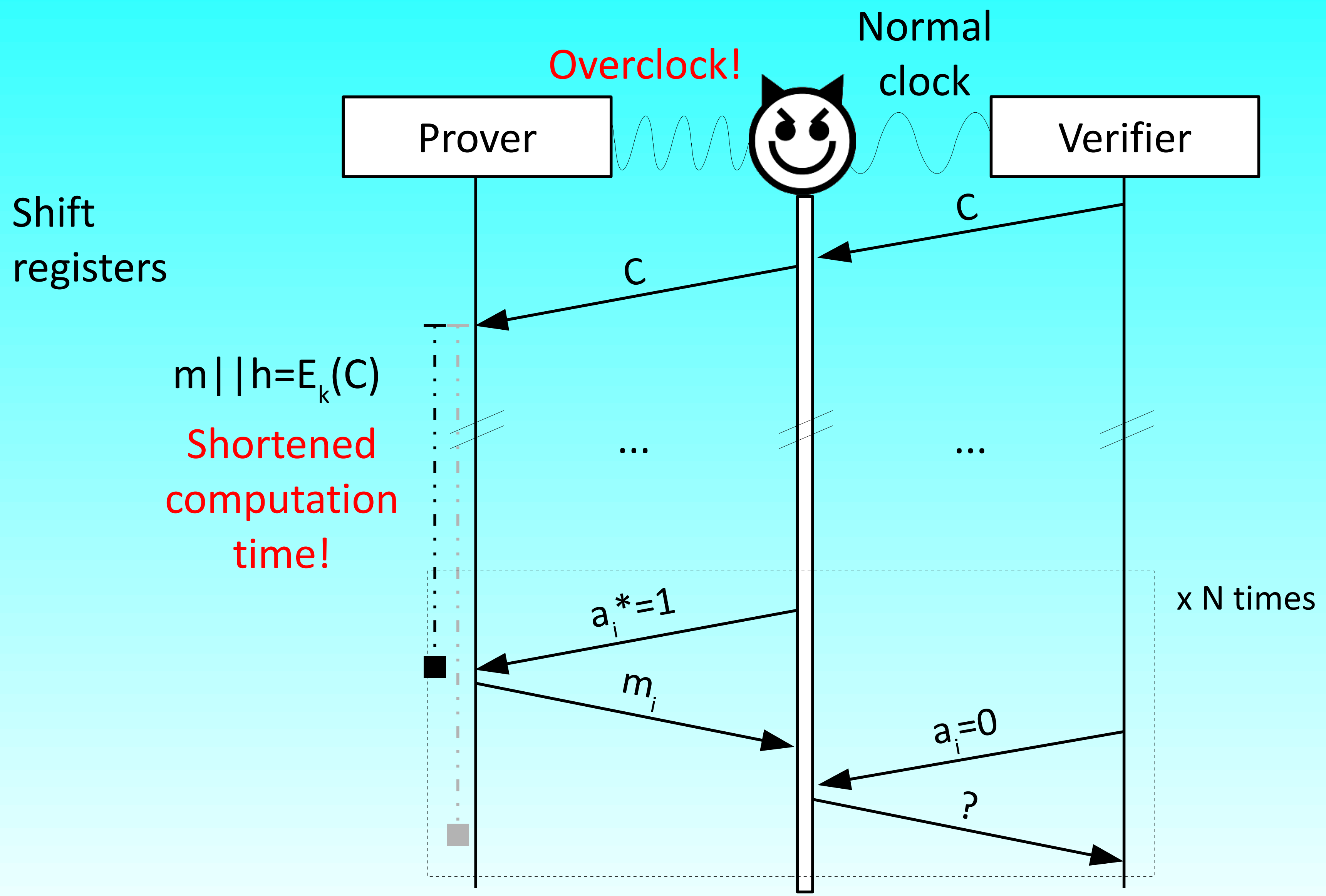
Overclock attacks

XOR



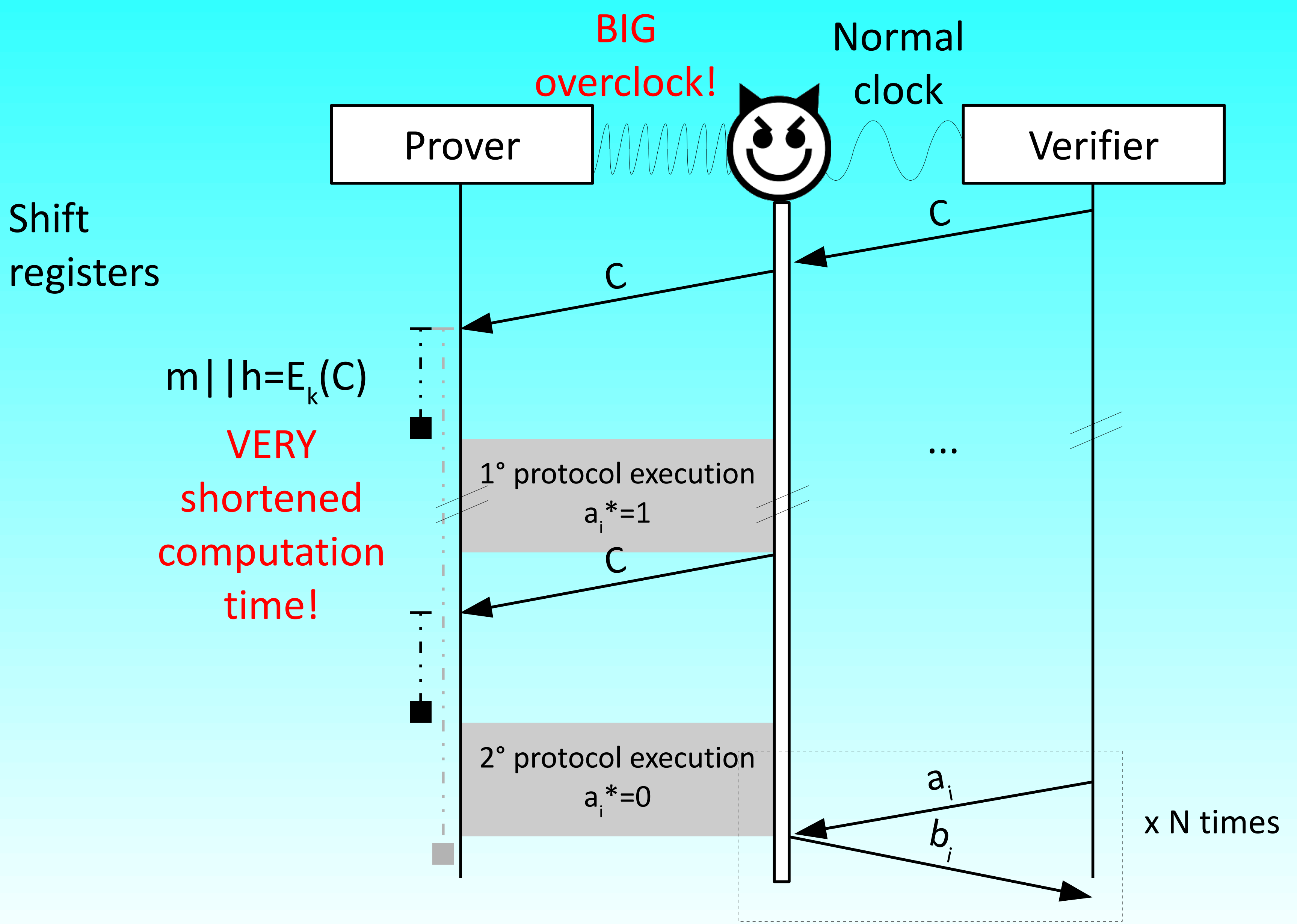
P(round success) = 1 !

Overclock attacks

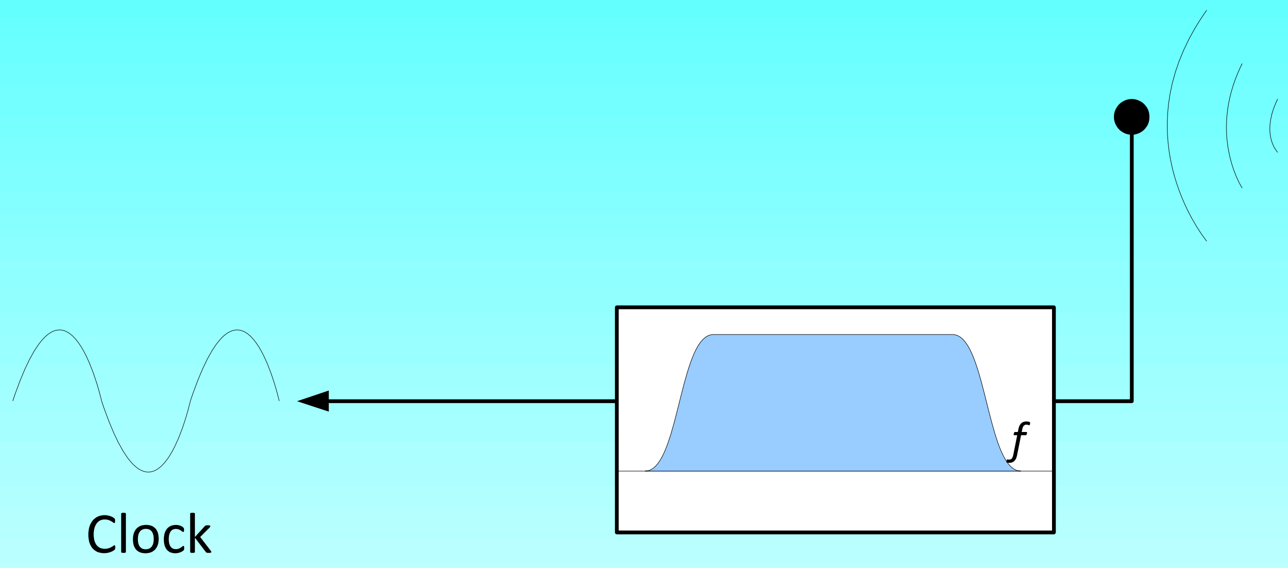


P(round success) = 3/4

Overclock attacks



Overclock attacks



Distance bounding on RFID

	Brands-Chaum	Hancke-Kuhn
Properties:		
Initial commitment:	Yes	No
a's to b's binding:	XOR	Shift registers
Final signature:	Yes	No
Performances:		
Relay attack success probability:	$\left(\frac{1}{2}\right)^N$	$\sum_{i=K}^{N} \binom{N}{i} \cdot \left(\frac{3}{4}\right)^i \cdot \left(\frac{1}{4}\right)^{N-i}$
Dishonest prover success probability:	$\left(\frac{1}{2}\right)^N$	$\sum_{i=K}^{N} \binom{N}{i} \cdot \left(\frac{3}{4}\right)^i \cdot \left(\frac{1}{4}\right)^{N-i}$
Noise tolerance:	No	Yes
Overclock attack:	Vulnerable	Resilient
Prover-side complexity:	Medium (2 crypto functions)	Low (1 crypto function)

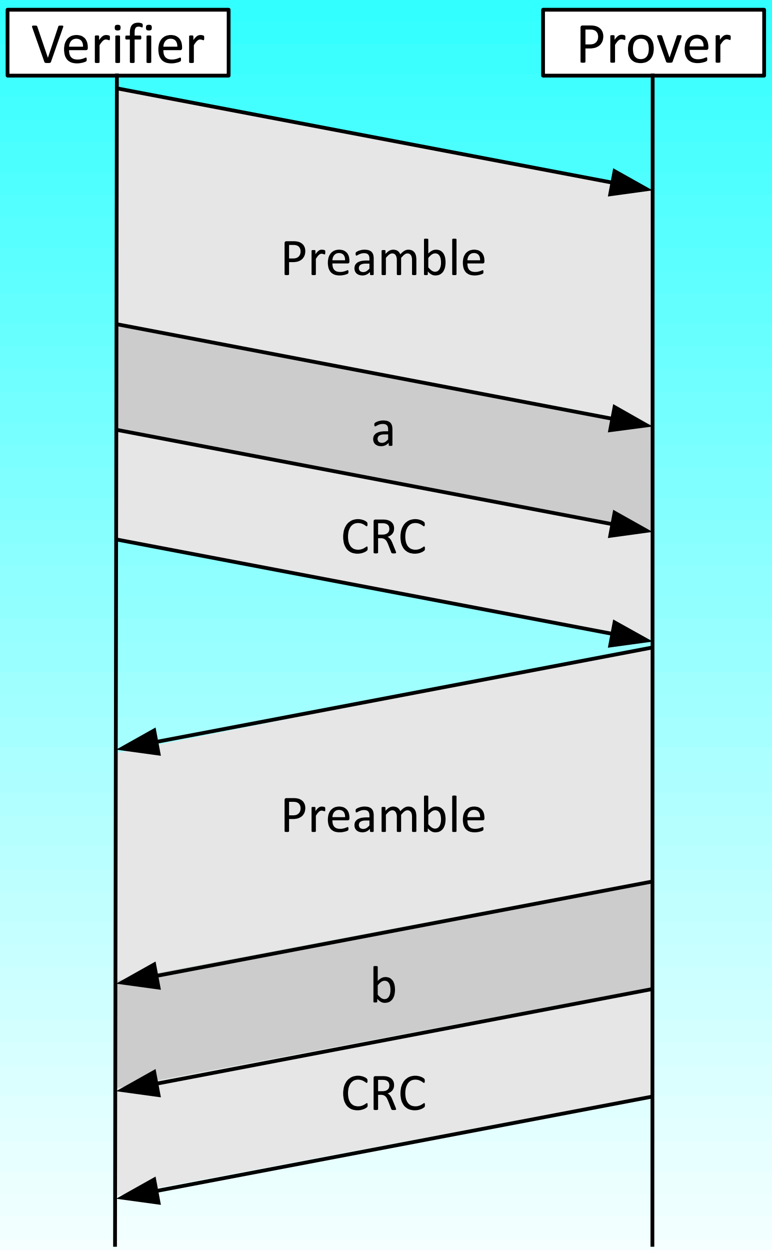
Distance bounding on sensors

- Ultra-wide band channels (IEEE 802.15.4a) reach sub-meter precision
- Problems:
  - We cannot send a single bit (ETS regulations)
  - Data must be preceded by (long) synchronization preambles
- Noise is corrected by FEC techniques

Naive solution #1

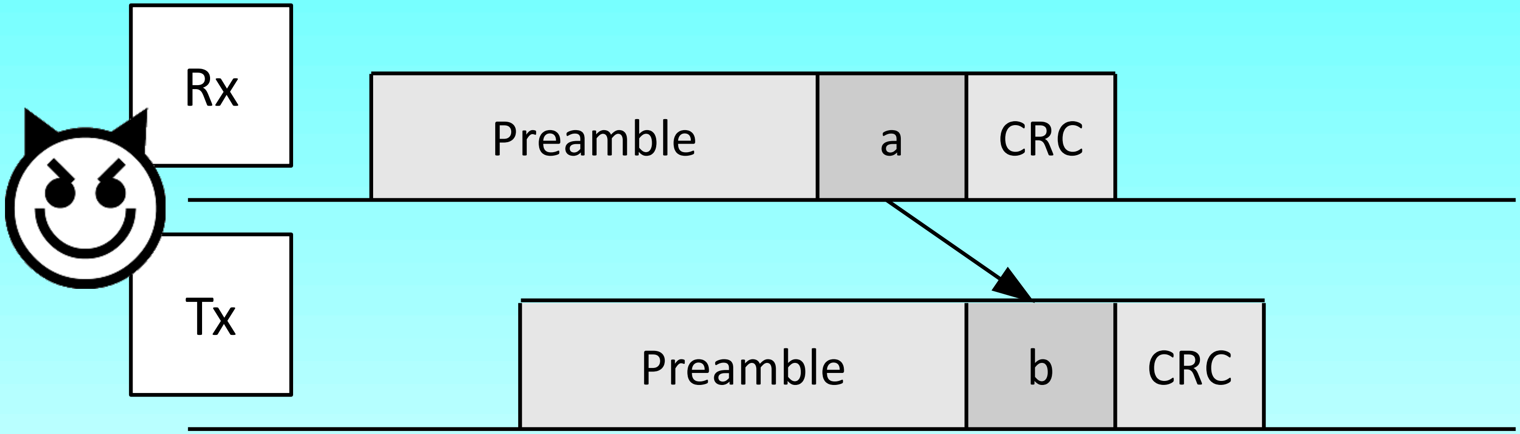
- Instead of performing N rounds of 1 bit each, we perform a single round carrying N bits

Packet latencies



Packet latencies

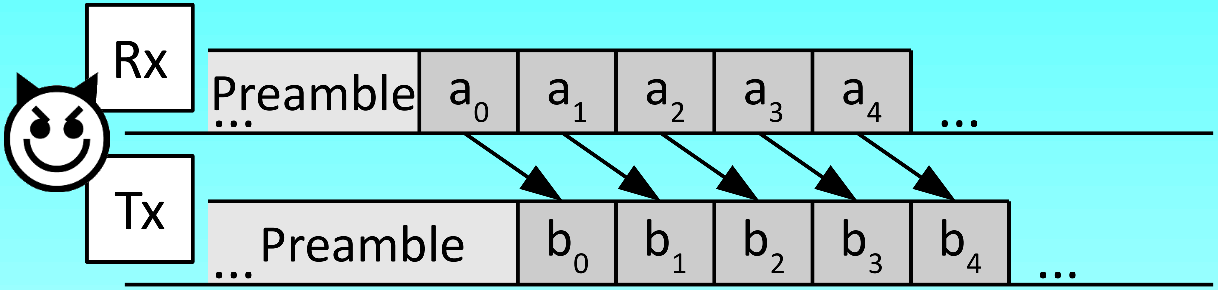
Dishonest prover



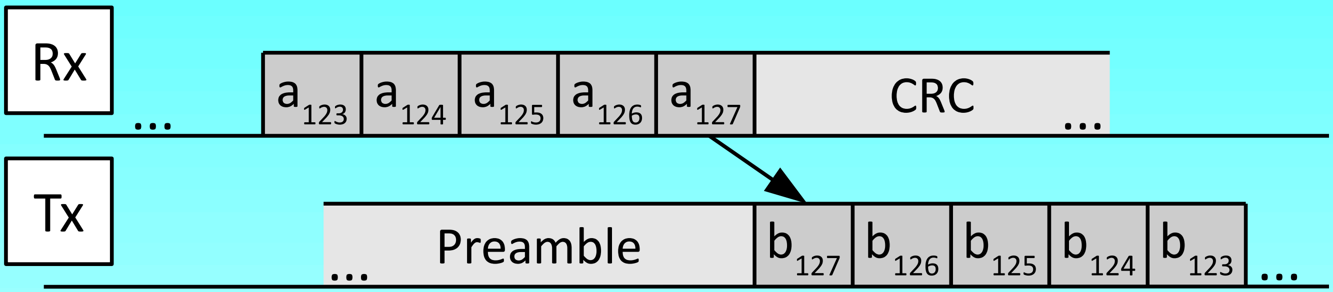
Packet latencies

- We cannot use complex, multi-bit elaboration functions (time constraints)
- The elaboration function must be simple and bit-a-bit

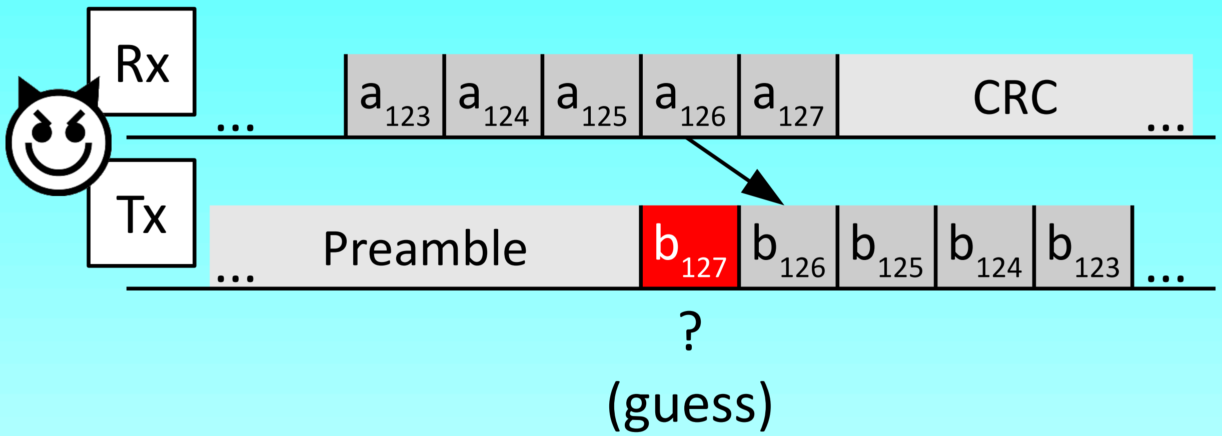
Packet latencies



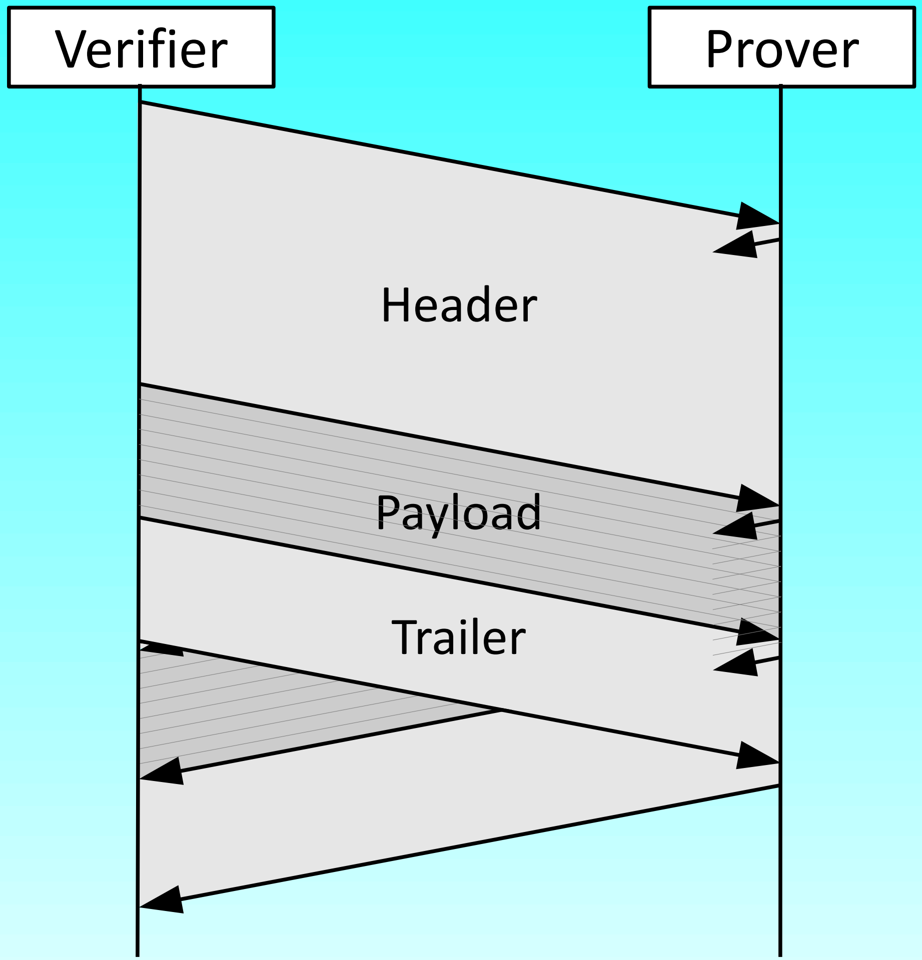
Naive solution #2



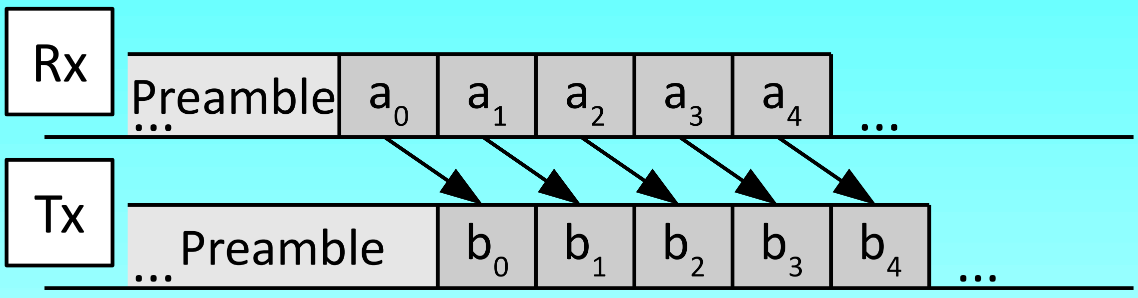
Packet latencies



Packet latencies

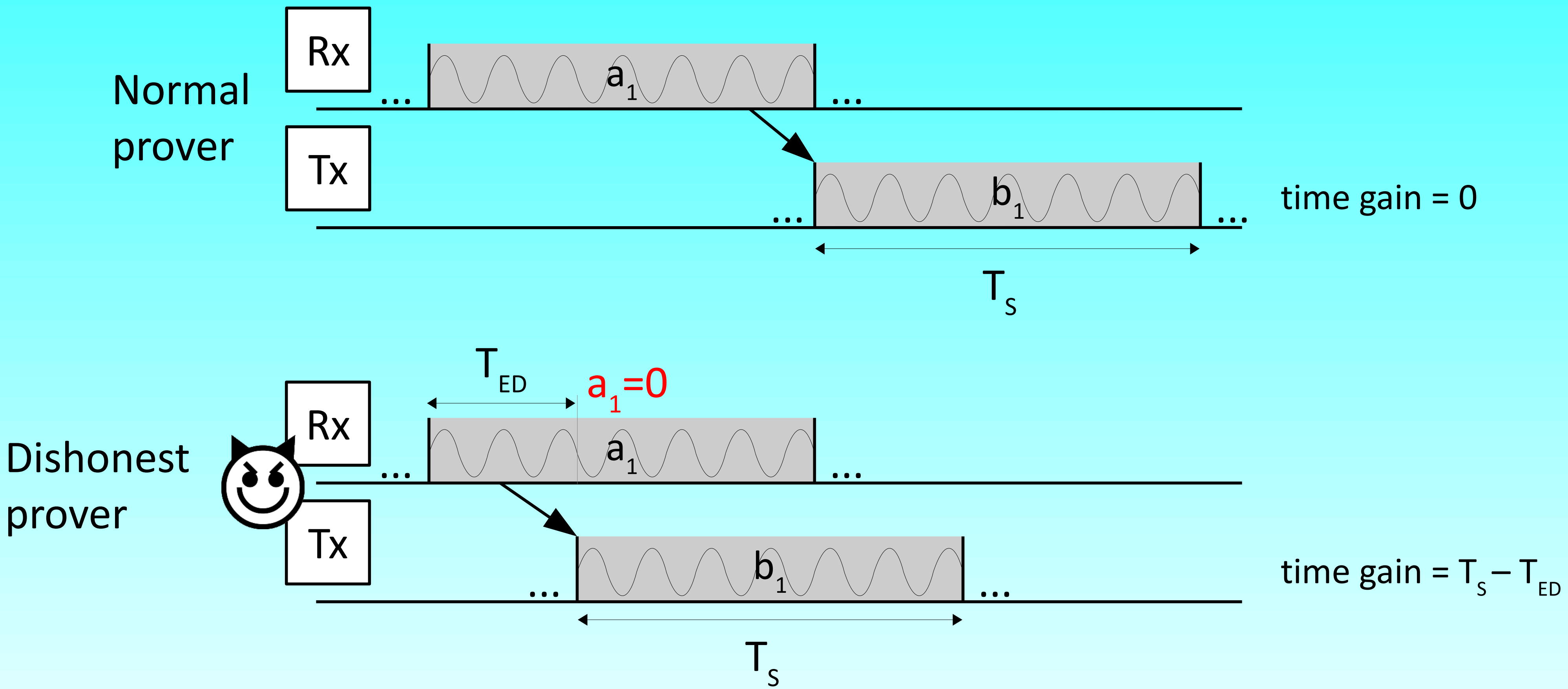


Packet latencies

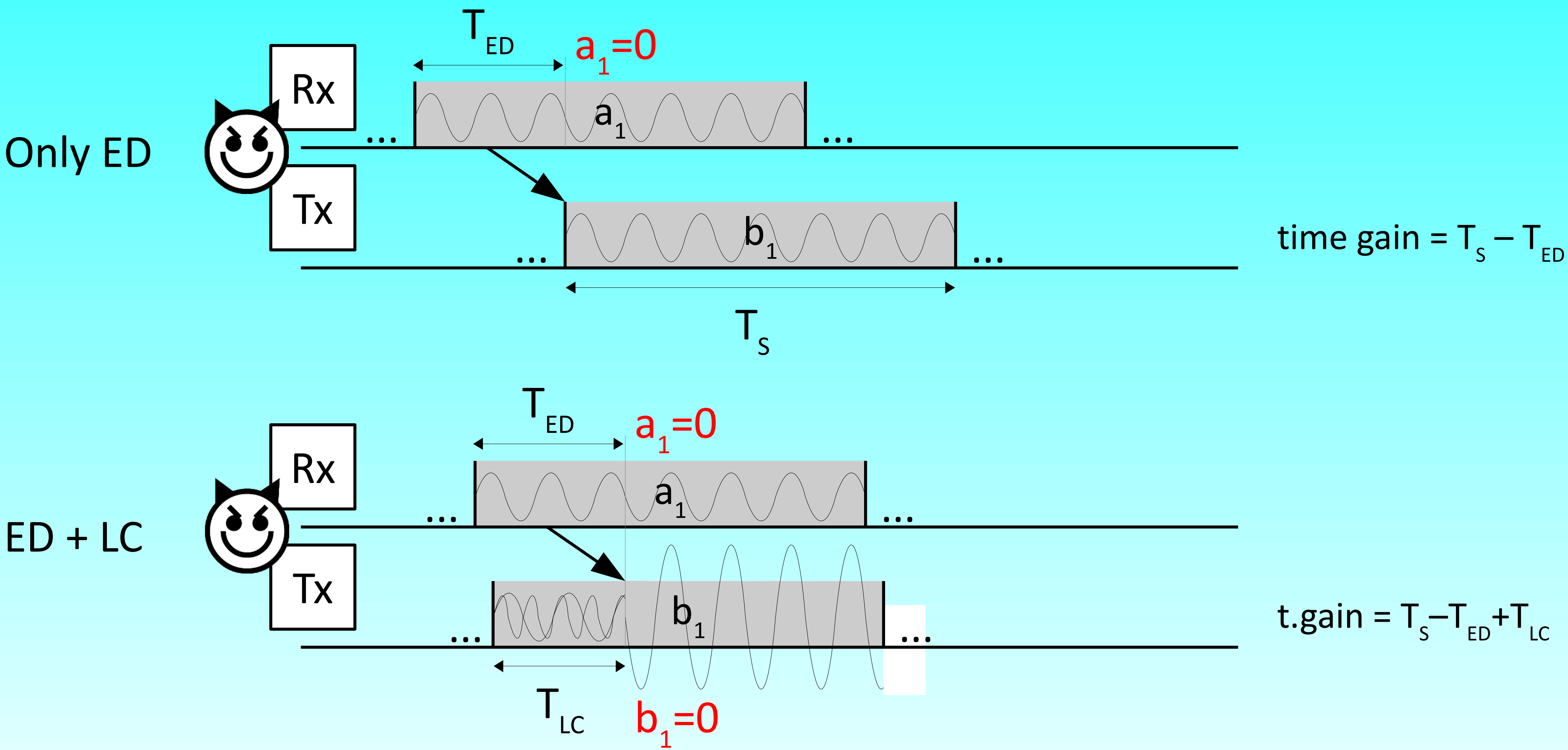


Going deeper...

Early detection

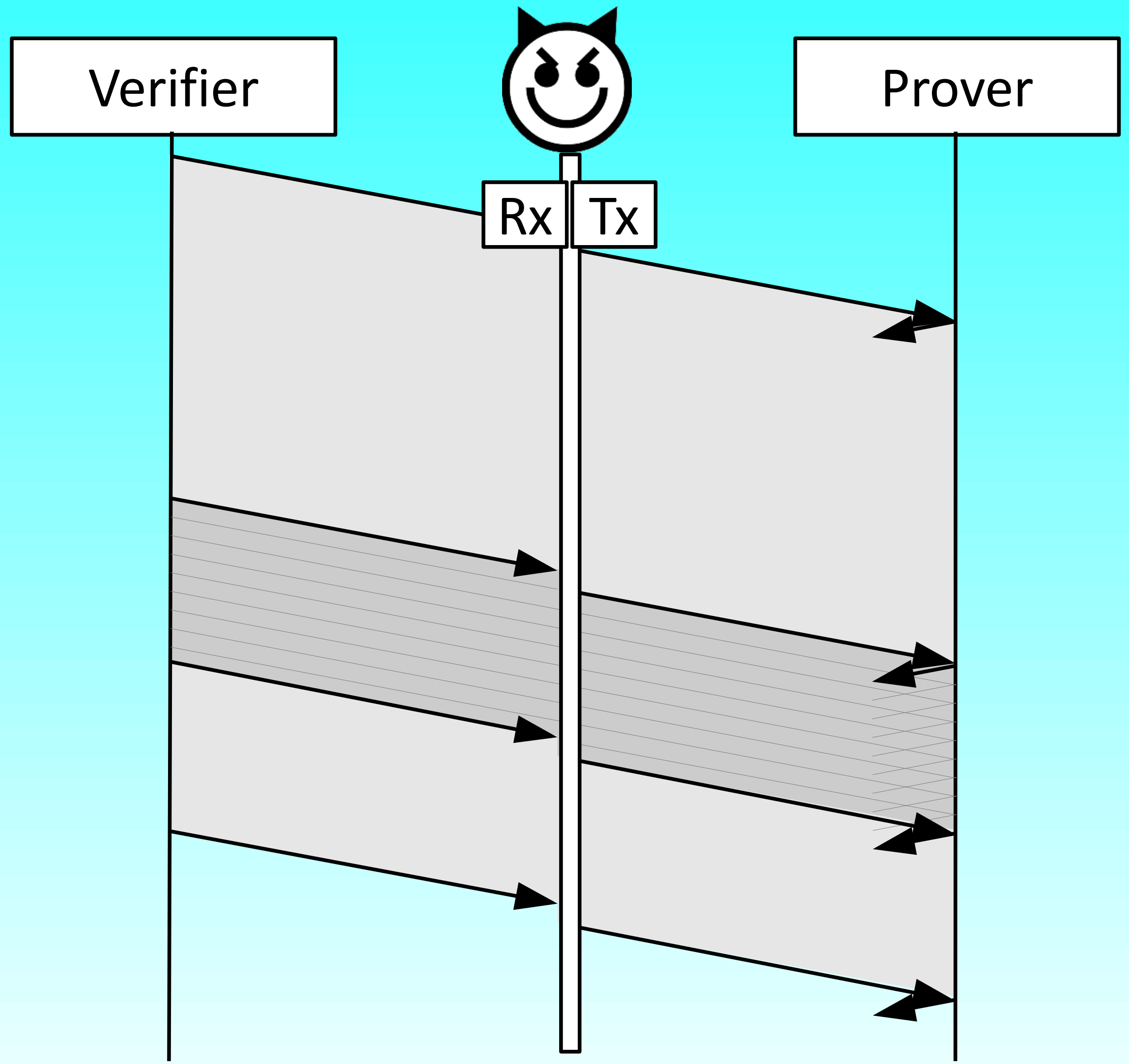


Late commit



T_{ED}
a_1=0
Rx
a_1
...
...
Only ED
Tx
b_1
...
...
time gain = $T_S - T_{ED}$
T_S
T_{ED}
a_1=0
Rx
a_1
...
...
ED + LC
Tx
b_1
...
...
t.gain = $T_S – T_{ED} + T_{LC}$
T_{LC}
b_1=0

ED and LC in relay attack

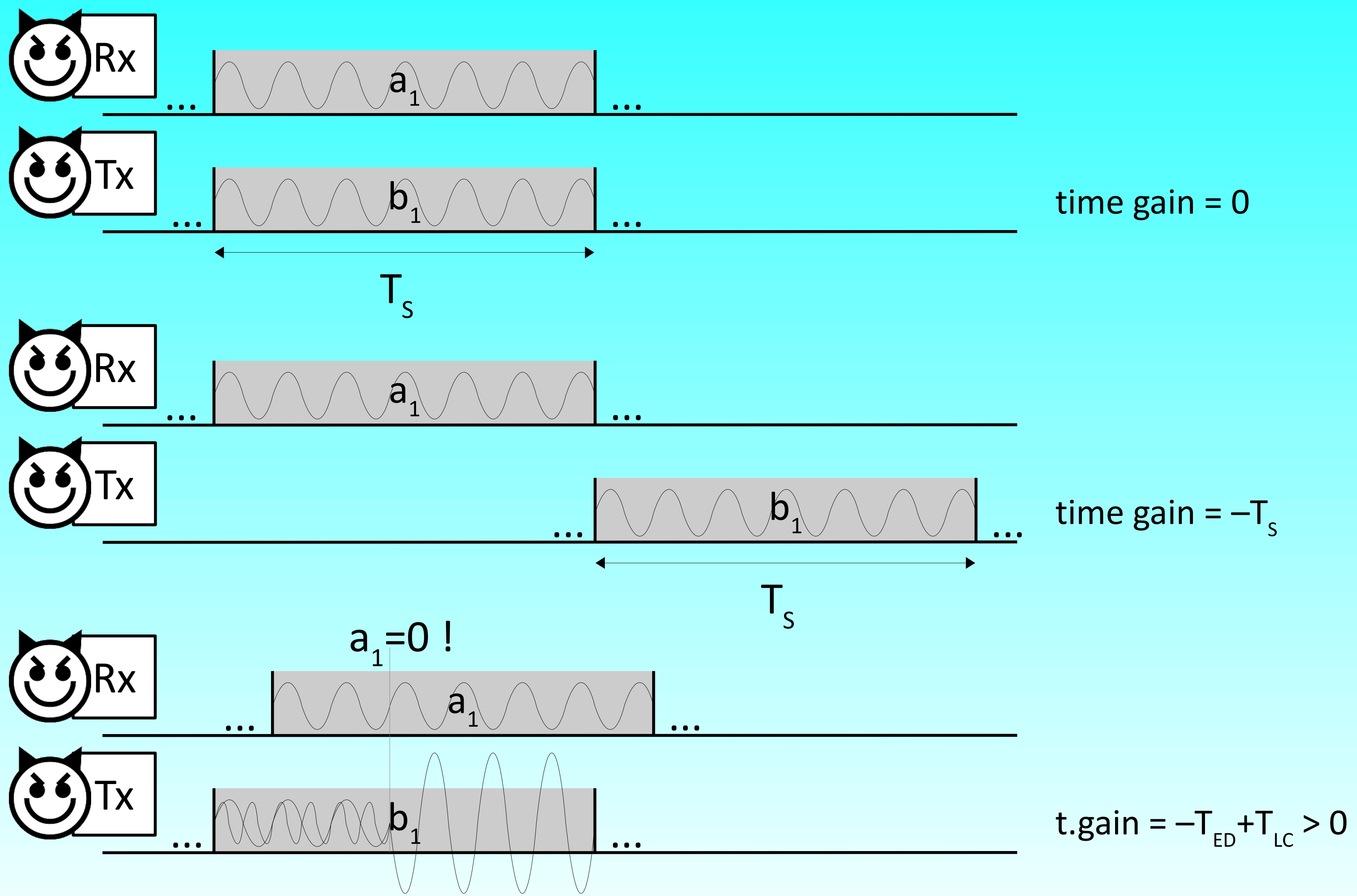


ED and LC in external adv.

„Analog“ relay

„Digital“ relay

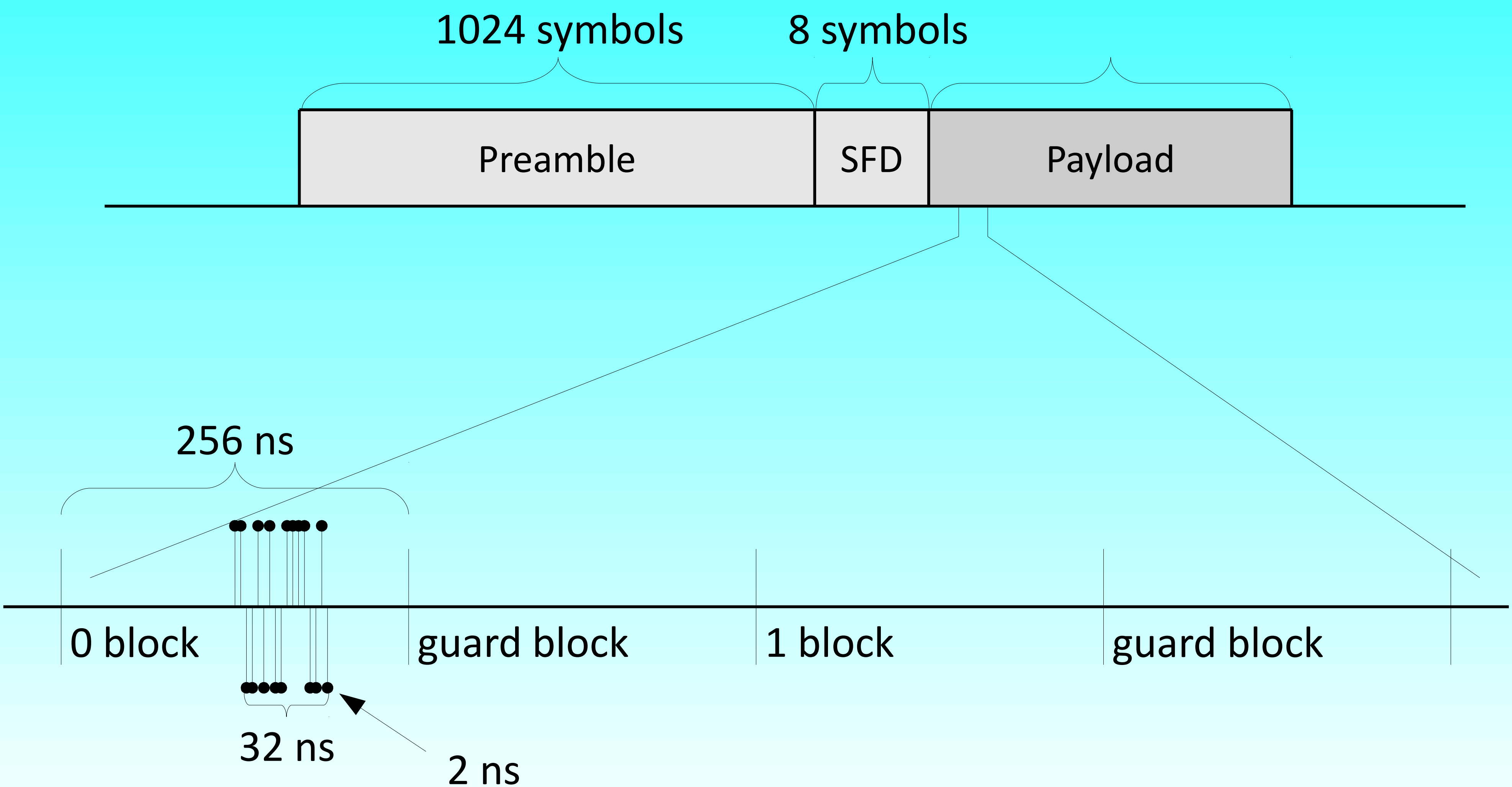
„Digital“ relay + ED/LC



802.15.4a resilience

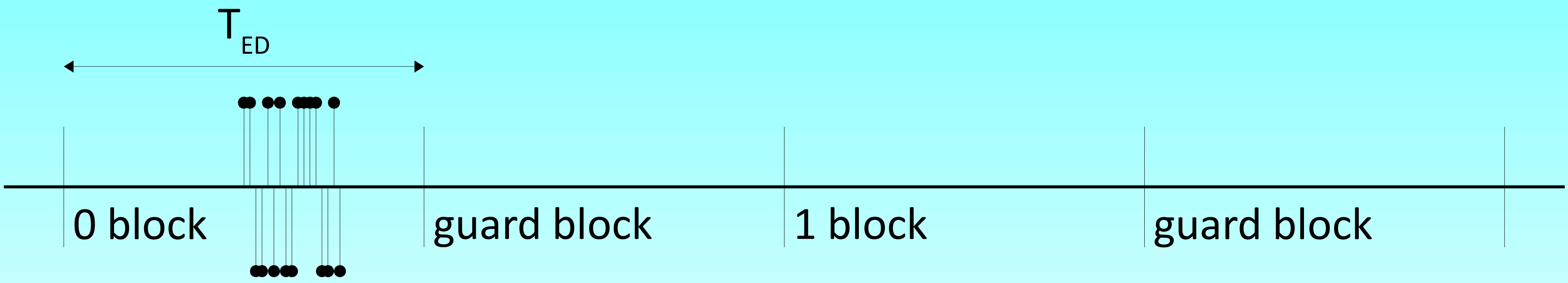
- IEEE 802.15.4a is a 2007 amendment of IEEE 802.15.4
- It adds PHY-layer specifications for UWB submeter-precision ranging

802.15.4a PHY format

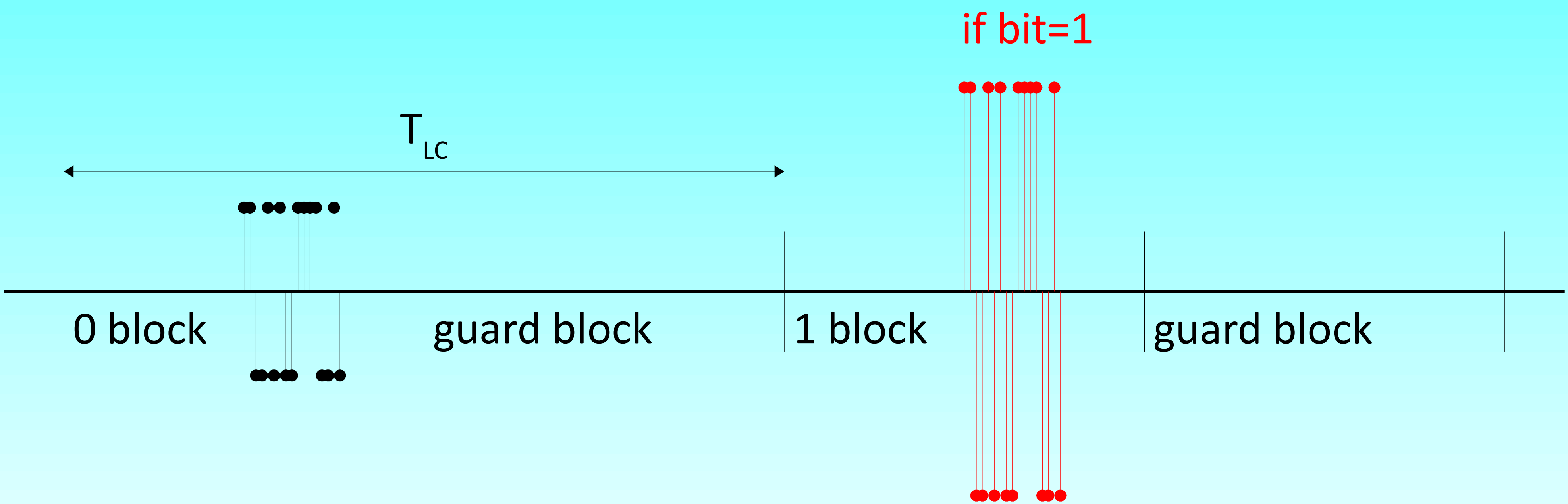


Pulse position modulation

Early detection in 802.15.4a

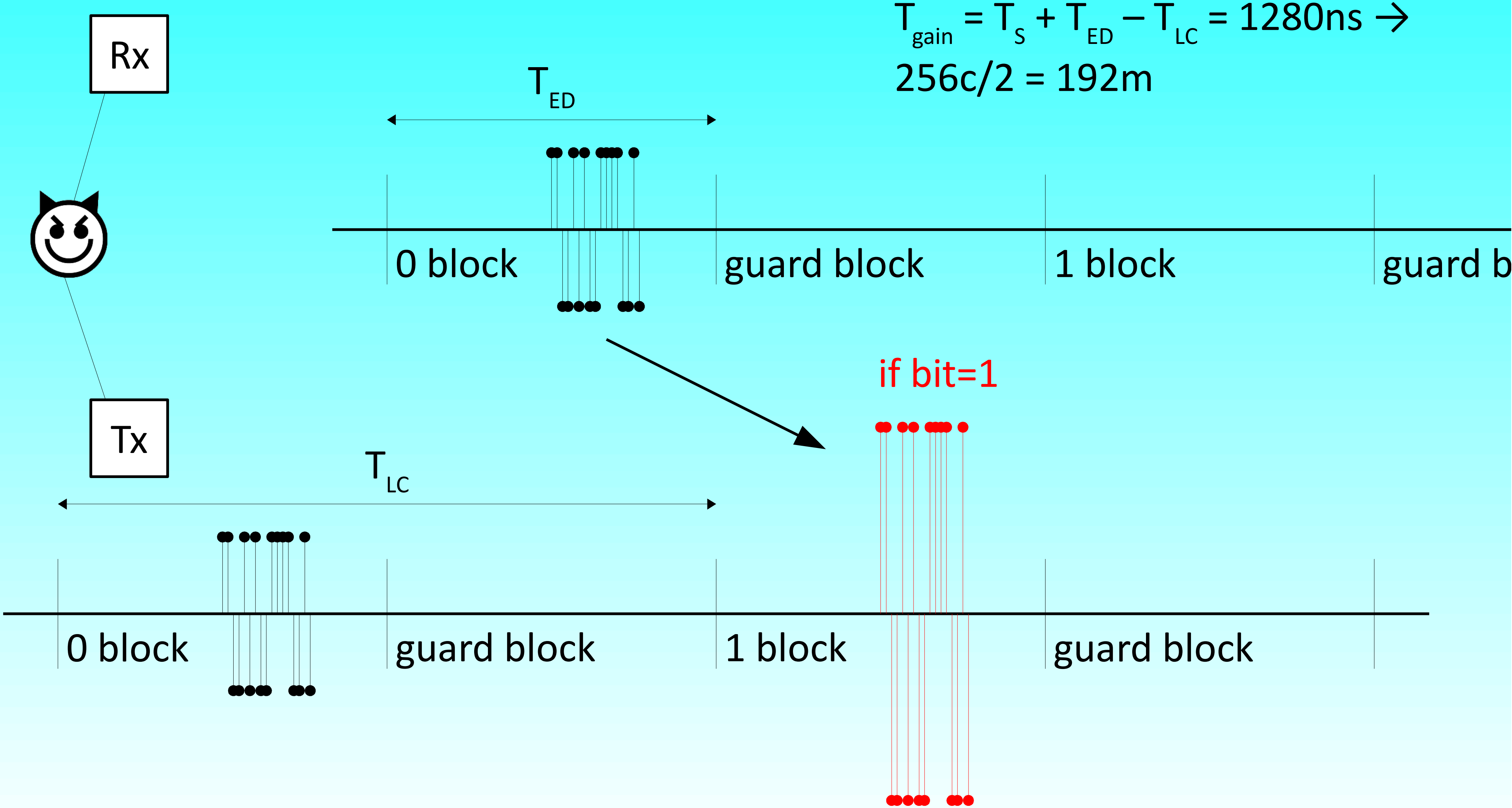


Late commit in 802.15.4a



ED+LC in 802.15.4a

$T_{gain} = T_S + T_{ED} - T_{LC} = 1280ns \rightarrow$
$256c/2 = 192m$



ED and LC

- We can only mitigate such attacks
- Make the symbol transmission time shorter
- Deal with bigger bit error rates

Four "Cambridge" principles

1 Use a communication medium with a propagation speed as close as possible to the physical limit

2 Use a communication format in which only a single bit is transmitted and the recipient can instantly react to its reception

3 Minimize the length of the symbols used to represents this single bit

4 As the previous criterion may limit the energy that can be spent on transmitting a single bit, the distance-bounding protocol must be designed to cope well with substantial bit error rates.

Pericle Perazzo

Department of Information Engineering
University of Pisa

pericle.perazzo@for.unipi.it

http://www.iet.unipi.it/p.perazzo/