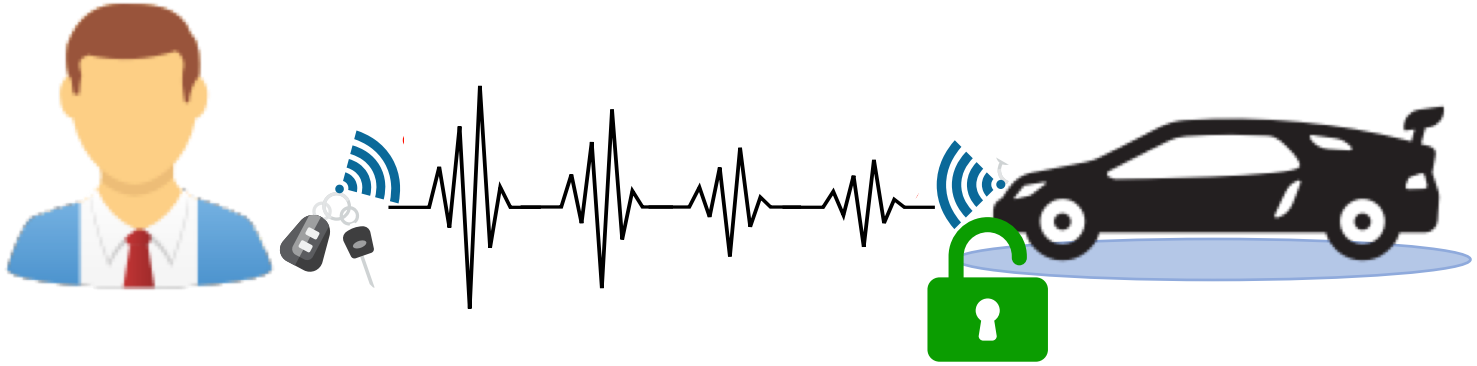
UWB with Pulse Reordering:
Securing Ranging against Relay and Physical-Layer Attacks

Mridula Singh, Patrick Leu, Srdjan Čapkun

ETH Zurich

Applications of Distance Measurement

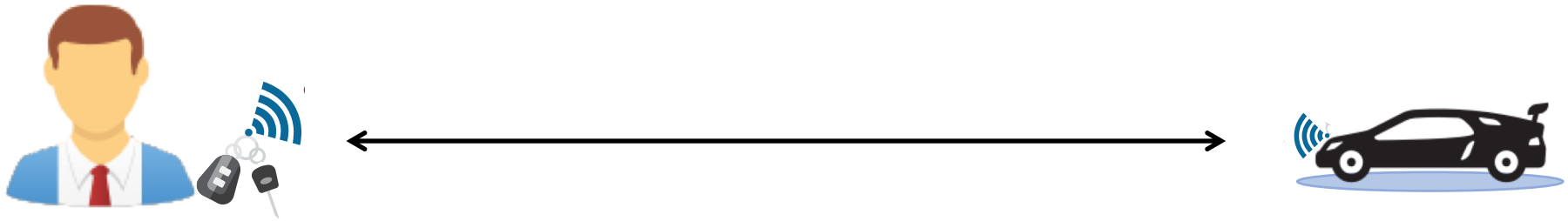
Passive Keyless Entry and Start System



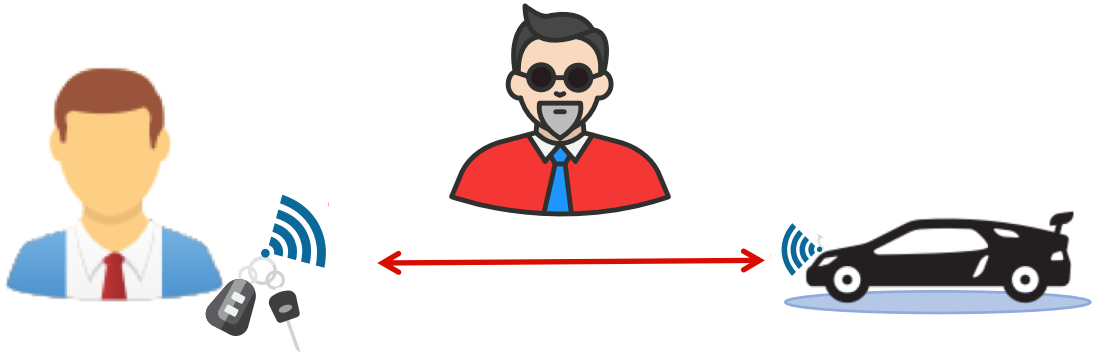
Contactless Payment

Attacker Model

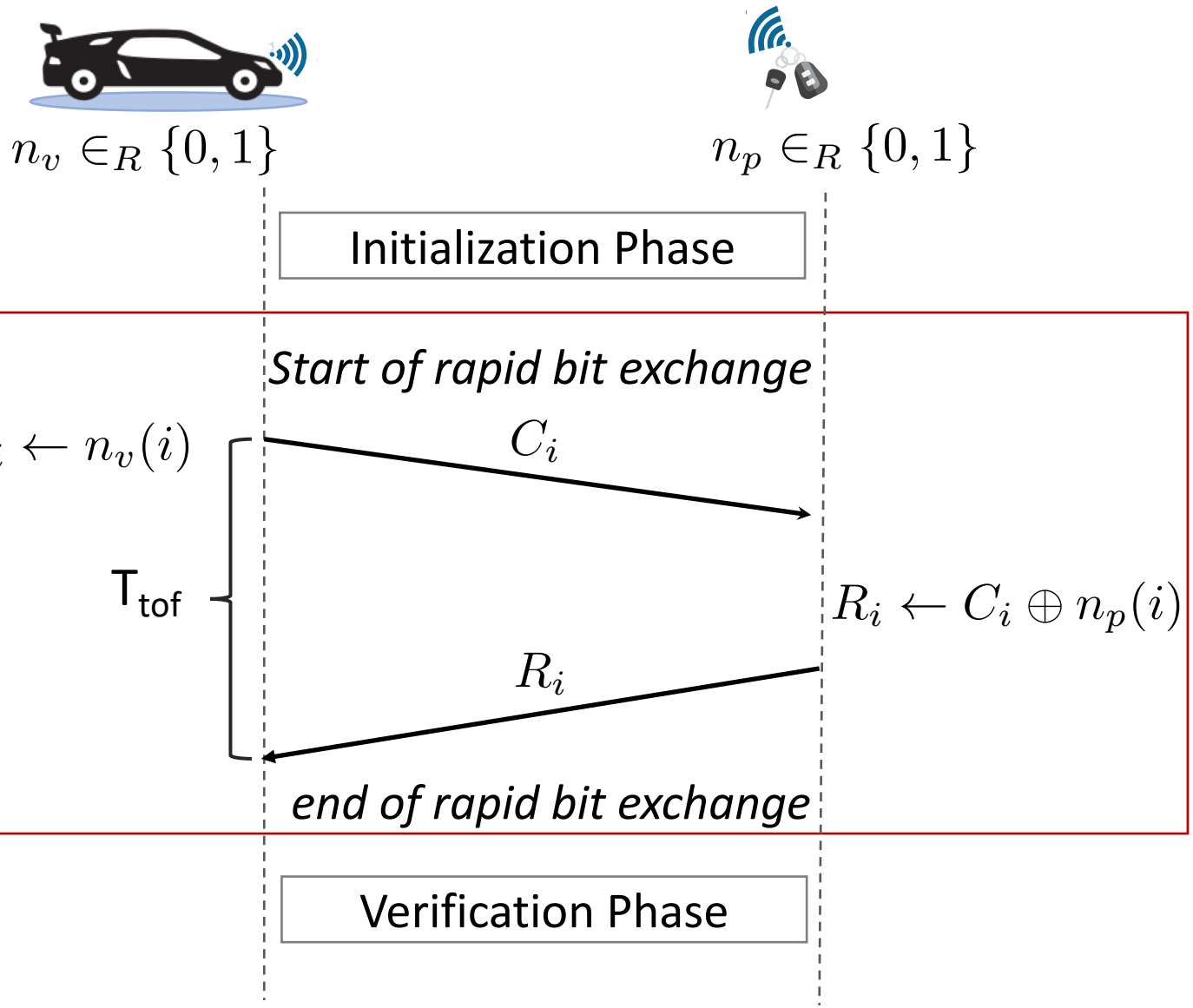
Actual Distance



Distance perceived in presence of an external attacker



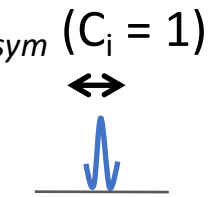
Distance Bounding: Logical Layer Solution

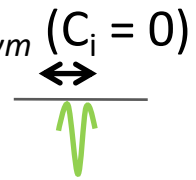


- Distance Bounding protocols do not protect against physical-layer attacks
- An attacker can manipulate the time of arrival of each bit at the physical layer using early-detect/late-commit (ED/LC) attack

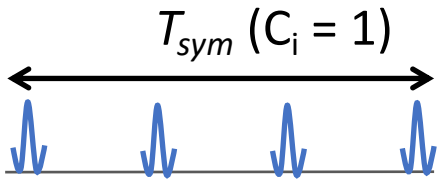
UWB: Physical Layer for Distance Measurement

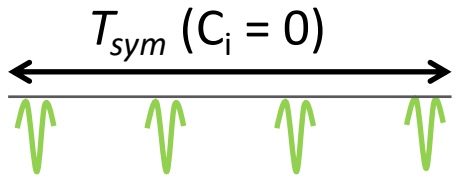
Base Mode
(single pulses per symbol)
$T_{sys} \approx 2ns$





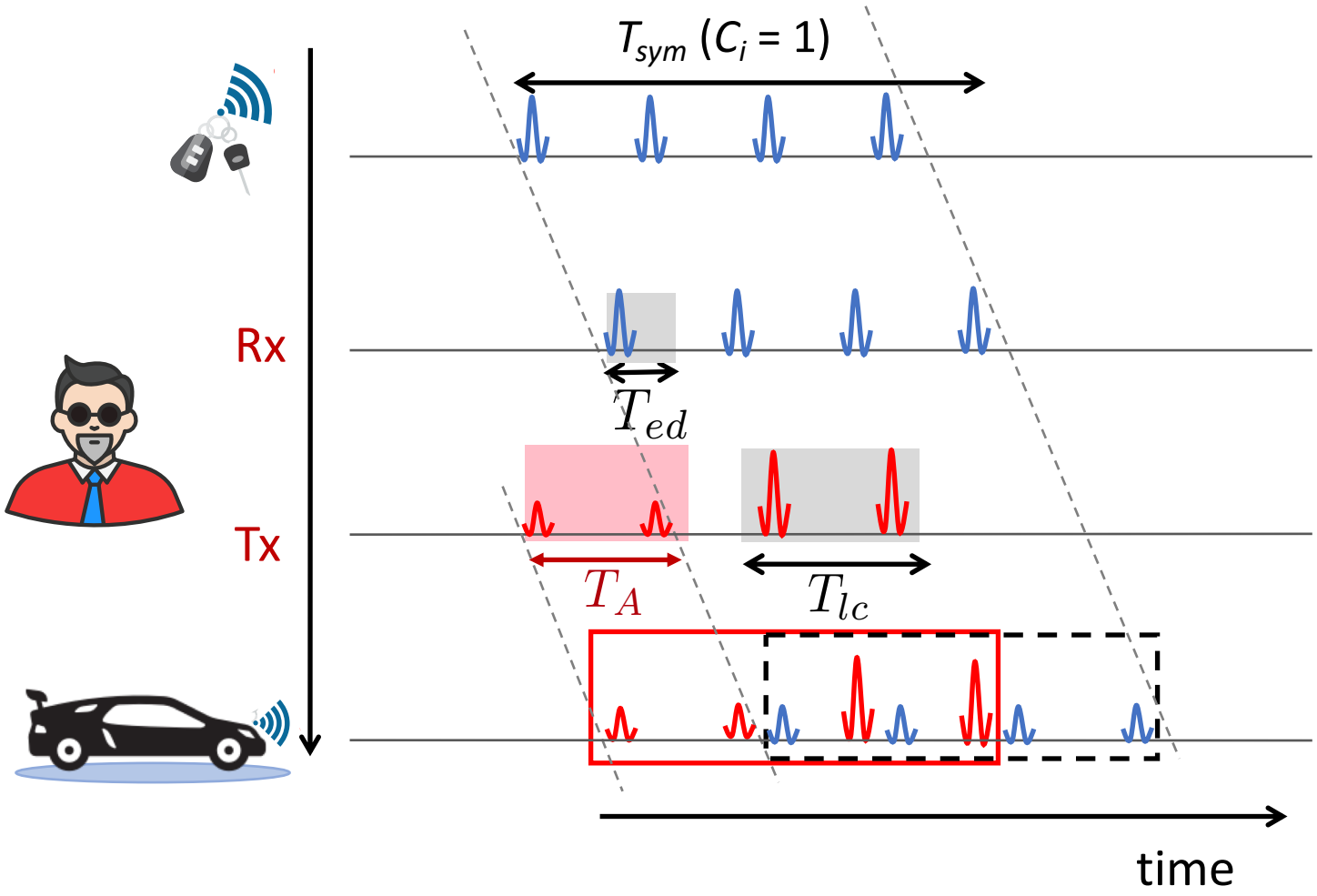
Extended Mode
(Multi-pulse per symbol)
$T_{sys} \approx 2\mu s$





- Power per pulse is limited by FCC and ETSI regulations
- Power of multiple pulses is aggregated to support longer distance

Example Physical Layer Attack



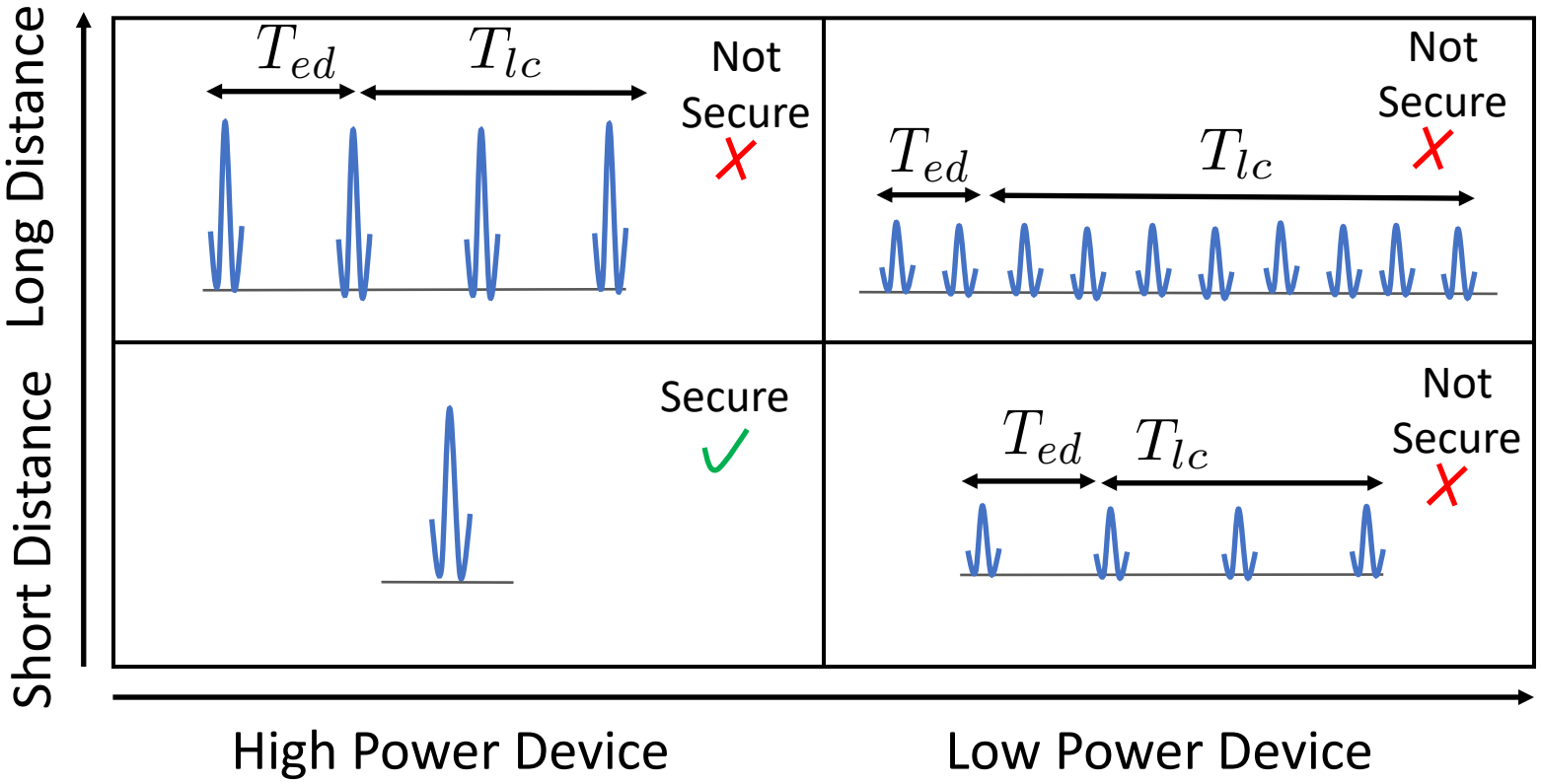
Early-detect/late-commit (ED/LC) Attack

- The attacker advances the symbol by time T_A
- T_A = 200 ns translates to a 60m distance reduction

- To prevent an ED/LC attack, use shorter symbols (single pulse)

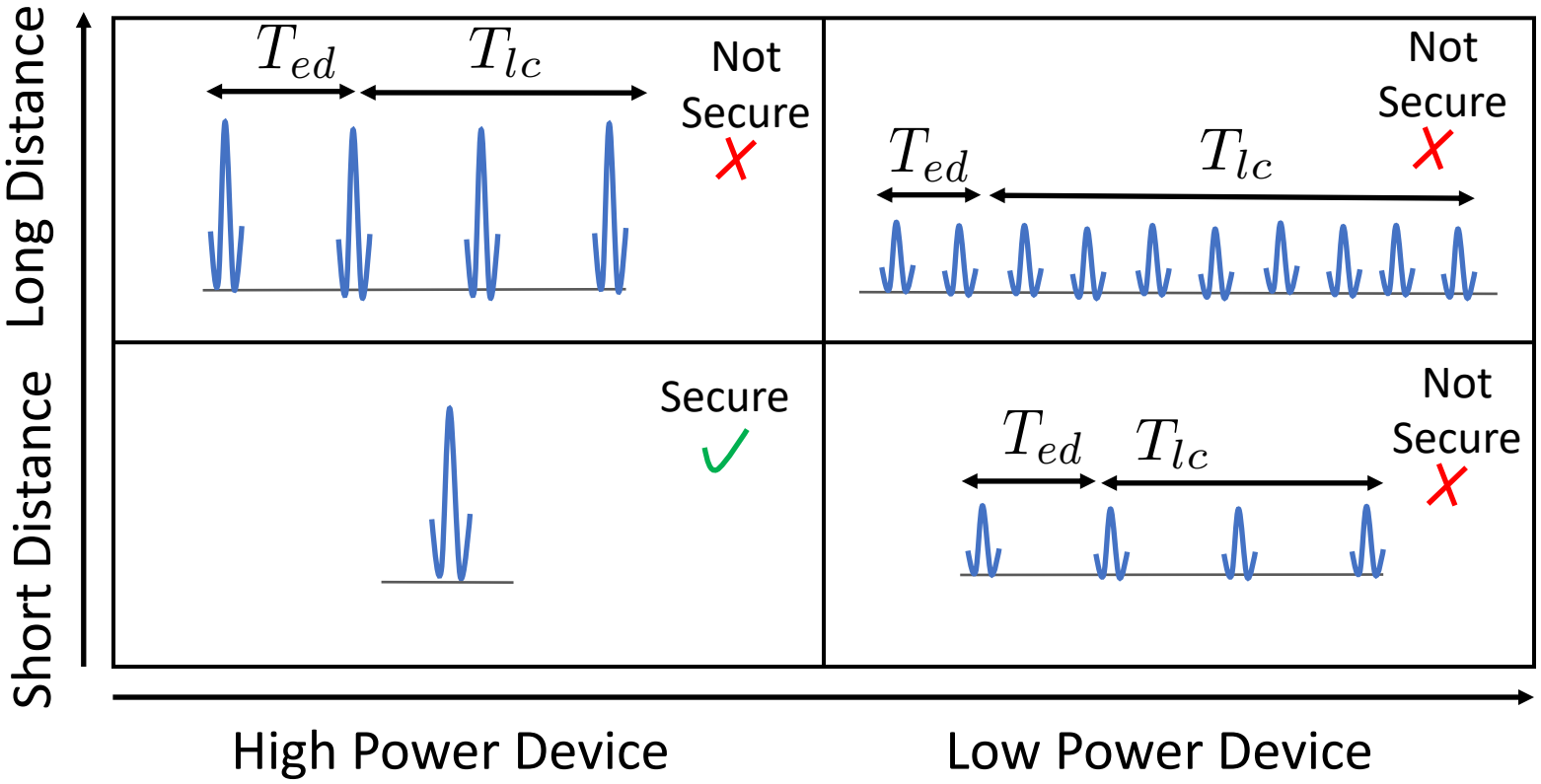
- IEEE 802.15.4z UWB is now being developed to address physical-layer attacks.

Motivation - Trade performance for Security



- We need longer symbols (multi-pulse) for performance (range and robustness)
- Longer symbols are vulnerable to ED/LC attack

Motivation - Trade performance for Security



Does this mean we can only secure short-range systems?

Contribution

UWB with Pulse Reordering

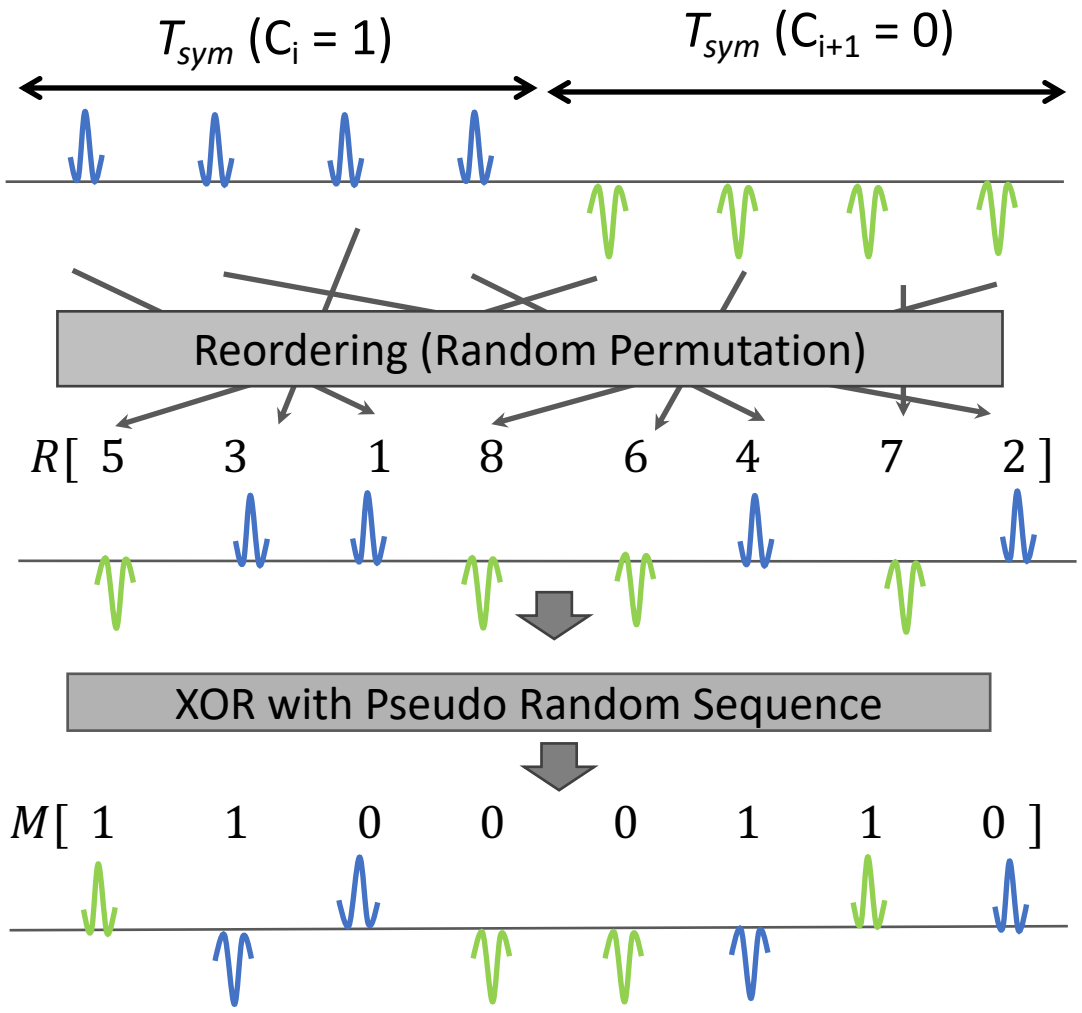
Allows for both Security
and Range

UWB with Pulse Reordering uses two techniques:

1. UWB-PR modulation - Randomized symbol interleaving through pulse reordering
2. Distance commitment [1]

[1] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, “Uwb rapid-bit-exchange system for distance bounding,” in WiSec 2015

UWB-PR Modulation



#pulses per symbol (N_P) = 4
#bits reordered (N_B) = 2

Perform Cryptographic operations on pulses

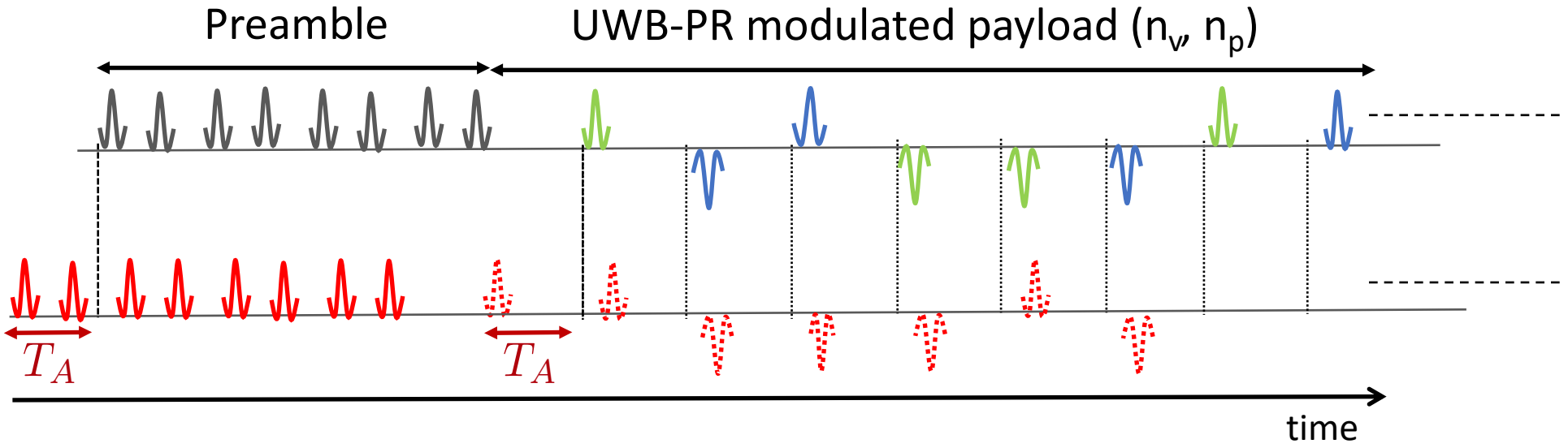
1. Symbol interleaving through pulse reordering
2. Masking polarity through XOR

Information needed for the ED/LC attack is lost

1. Shape of the symbols is hidden
2. Start and end time of symbols is unpredictable

Attacker can only guess!

Distance Commitment

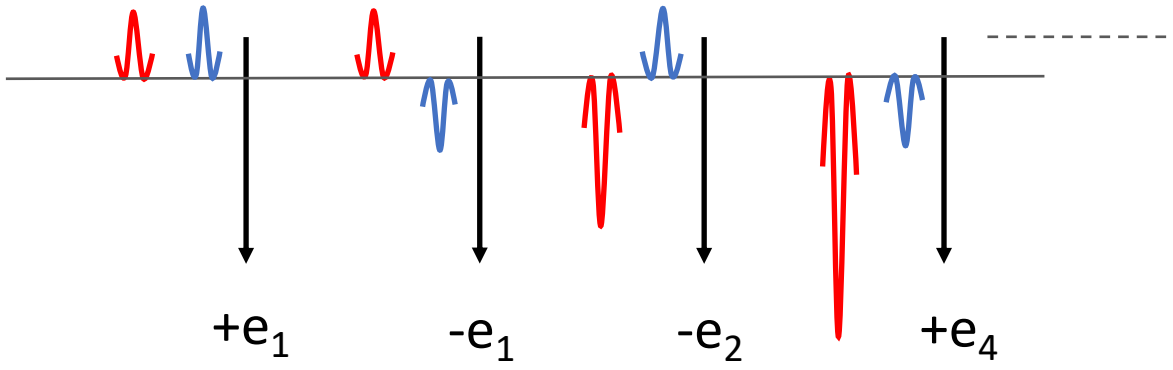


- Distance Commitment = distance computed on a fixed preamble (known to the attacker) & then 'verified' using payload pulses generated using UWB-PR
- The timing of the preamble is binding. An attacker needs to advance payload if he advance preamble

An attack strategy

The attacker does not need to guess polarity of each pulse correctly.

However, the attacker needs positive net contributions in all bits to get the correct nonce (n_V,n_P) at the receiver

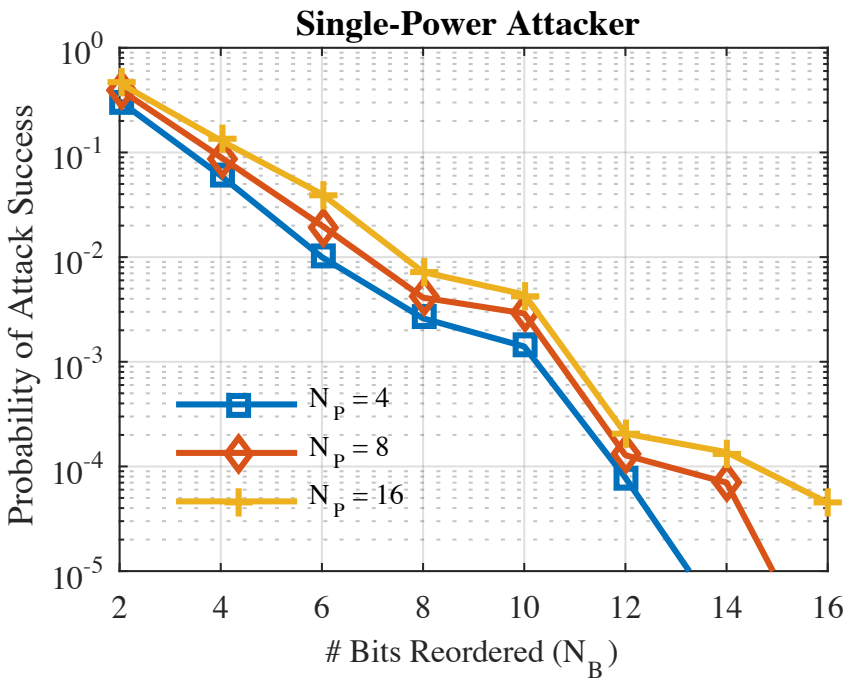


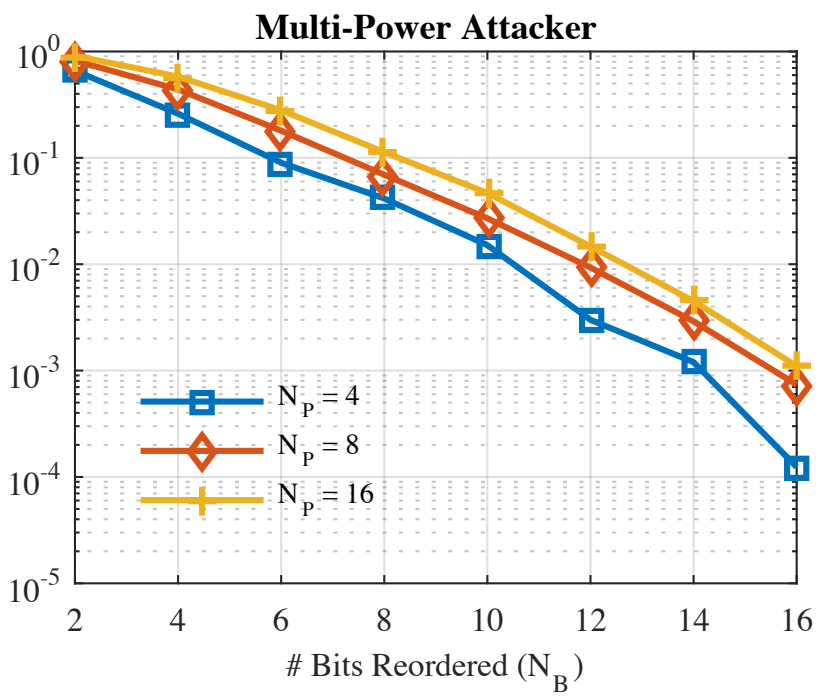
How can an attacker influence the outcome?
By choosing –

- **Power per pulse (e_1, e_2, …)**
- **When to stop**

Reordering is secret!
It is hard to asses progress of the attack

Attack Analysis





- The probability of attack success decreases on increasing the number of bits reordered (N_B)
- Longer symbols (higher N_P) achieve increased security by interleaving more bits – representing a longer nonce (n_v,n_p)

So far, the community has believed that only short symbols with rapid bit exchange are secure [2].

It has lead to complicated system designs.

With UWB-PR we show that Distance Bounding protocols can be much simpler

[2] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, “So near and yet so far: Distance-bounding attacks in wireless networks,” in ESAS’06

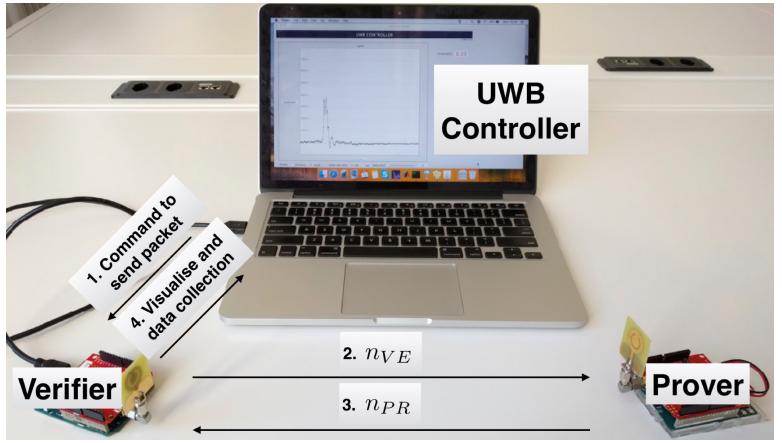
Revisiting principles for secure distance measurement

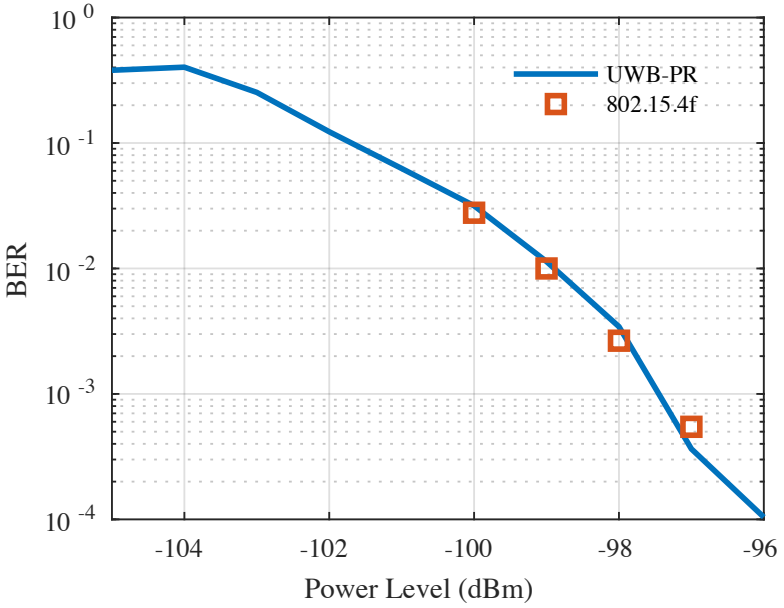
- Short symbols (preferably one pulse per symbol) are necessary for secure ranging.
  - Cryptographic operations at the physical layer prevent ED/LC attacks.
- Rapid bit/pulse exchange is necessary for secure ranging.
  - Multiple bits can be part of the same frame using a distance commitment.
- Special bit-error tolerant protocols are required at the logical layer.
  - Multi-pulse system can be designed to prevent bit errors by increasing the symbol length.

Proof-of-concept Implementation

- Based on the IEEE 802.15.4f – OOK modulation
  - System bandwidth of 500 MHz
  - Pulses are separated by 250ns
- In LoS condition, single pulse system can operate up to distance 32m, and 16 pulse system can operate up to 93m.
- BER is the same as legacy IEEE 802.15.4f
- The ranging precision 10cm (LoS)

- Compliant with the upcoming IEEE 802.15.4z standard





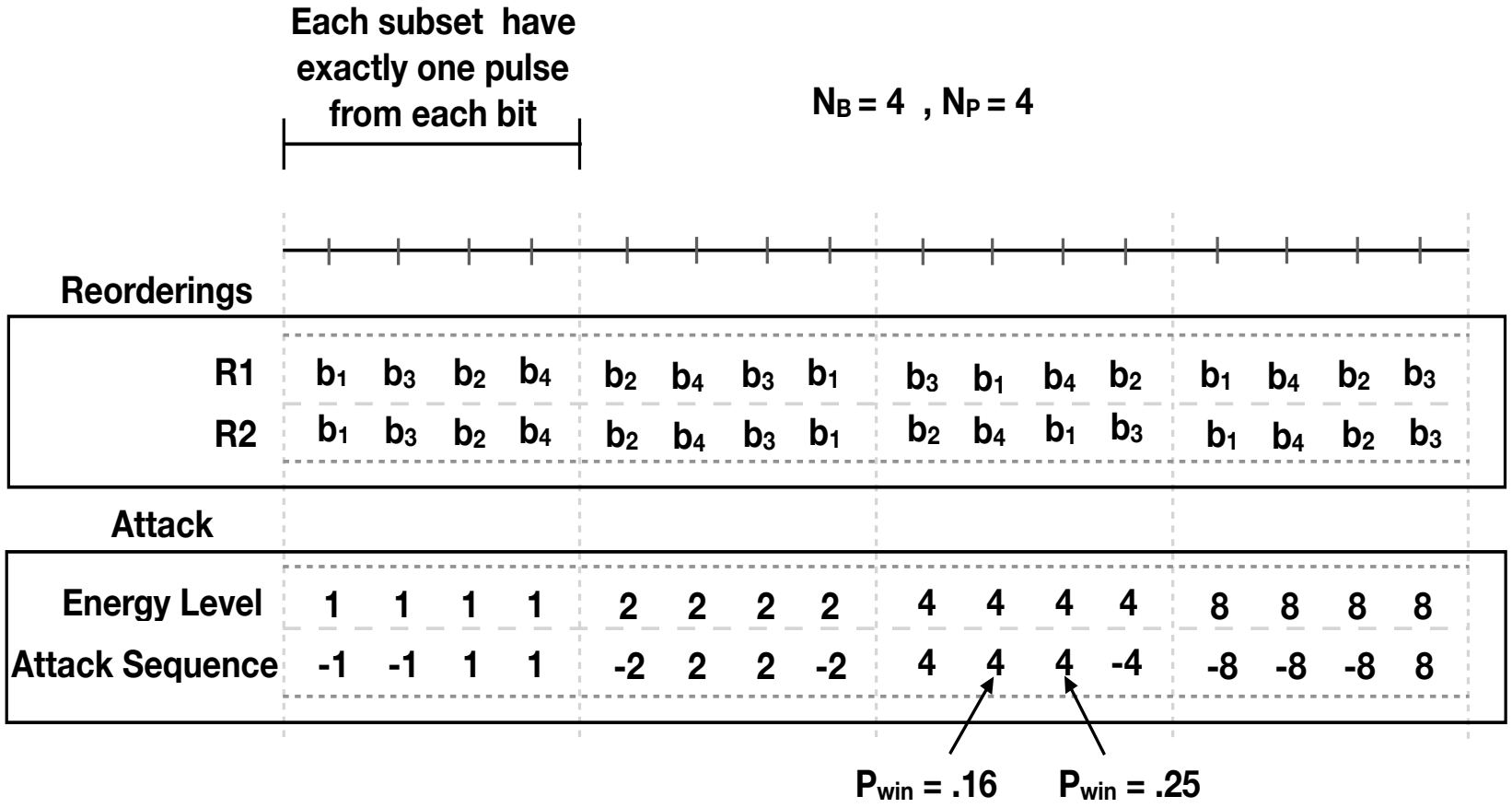
Summary

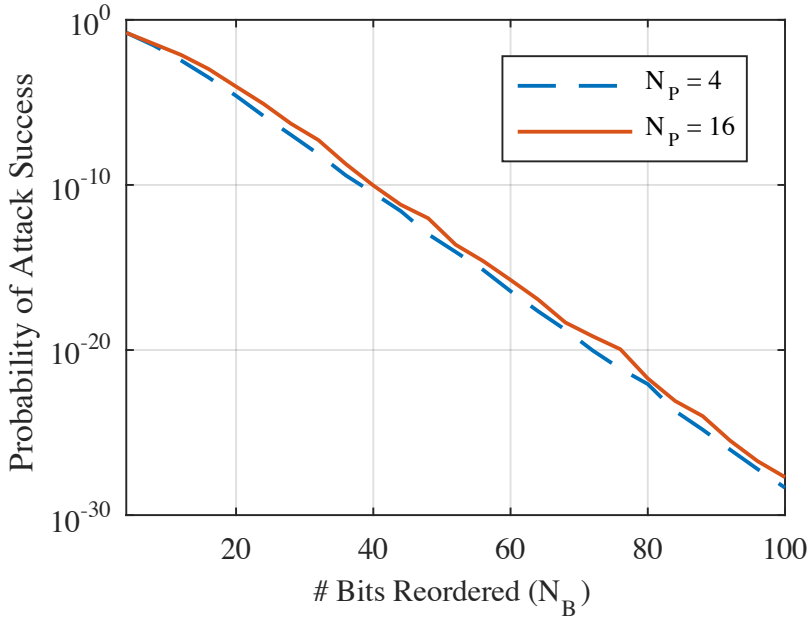
- UWB-PR achieve secure, performant and precise ranging system
- UWB-PR modulation with distance commitment simplifies the design of UWB ranging systems

Thank you!

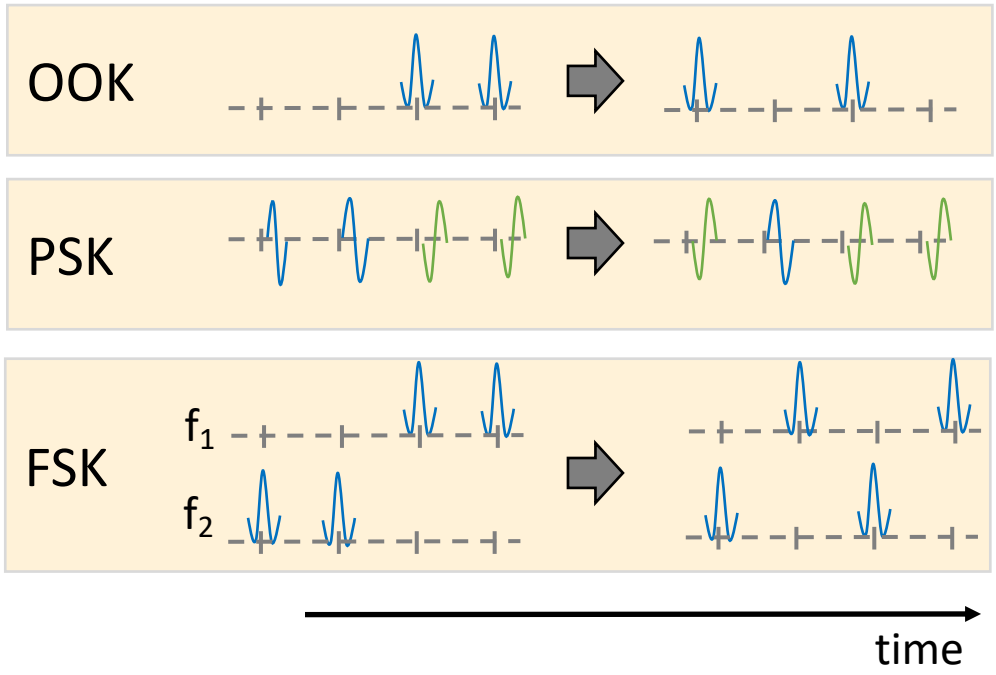
Questions?

Structured Reordering





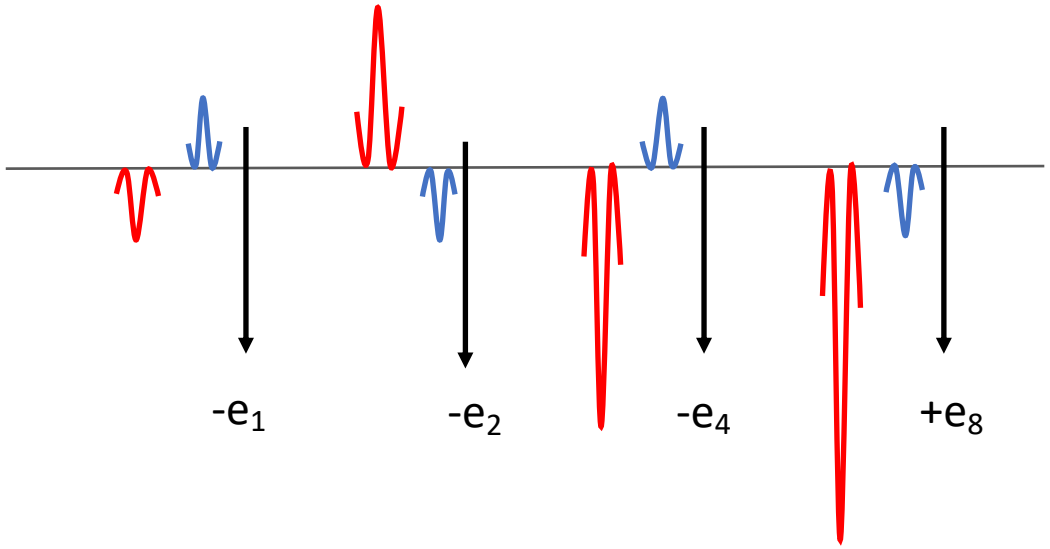
Physical-Layer Cryptographic Operations



- The cryptographic operations at the logical layer are not sufficient to prevent physical layer attacks
- Logical layer data should not change due to cryptographic operations at the physical layer
- Physical layer cryptographic operations add an additional layer of security

we can model each pulse as having two polarities.

Using only XOR for Secure Distance Measurement

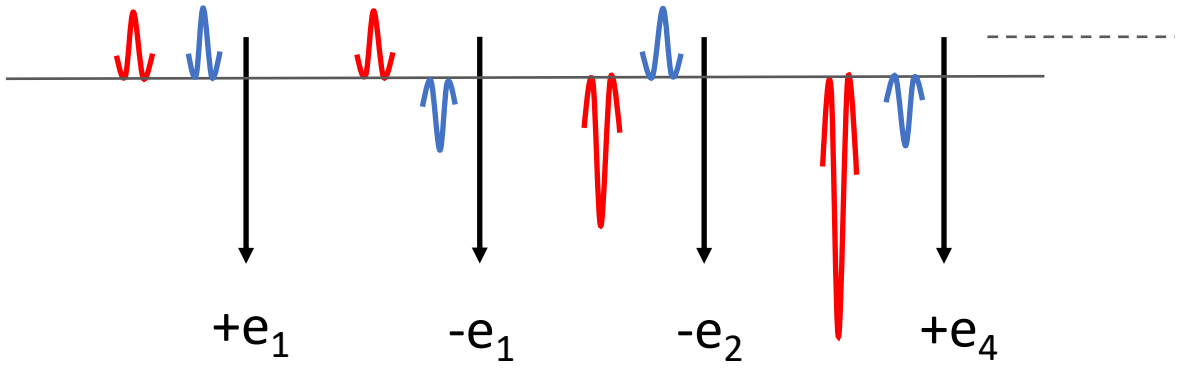


- Attacker can adapt power levels
- Attacker can evaluate progress of the attack

An attack strategy

The attacker does not need to guess polarity of each pulse correctly.

However, the attacker needs positive net contributions in all bits to get the correct nonce (n_V,n_P) at the receiver



How can an attacker influence the outcome?

By choosing –

- **Power per pulse (e_1, e_2, …)**
- **When to stop**

Reordering is secret!

$R1[$	2	1	1	2	… …] ✗
$R2[$	2	1	1	1	… …] ✓

R1 (b_i → -1, b_{i+1} → +5)

R2 (b_i → +1, b_{i+1} → +1)

Distance Reduction Attack