ETH zürich

System Security Group
Department of Computer Science

Time for Change: How Clocks Break UWB Secure Ranging

Claudio Anliker, Giovanni Camurati, and Srdjan Čapkun

Why Secure Ranging matters

Passive Keyless Entry And Start (PKES)

Contactless Payments

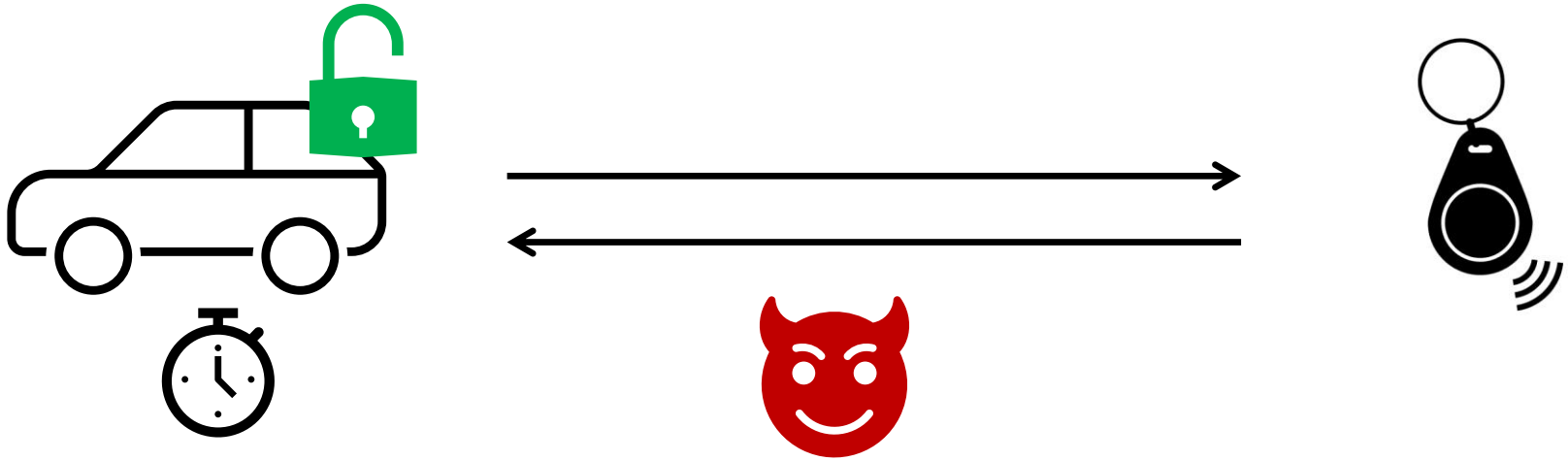
Generic Access Control

Attacks on the physical layer: distance reduction and distance enlargement

- Distance reductions to bypass authorization or access control
- Distance enlargements out of scope

Using UWB for Secure Ranging

UWB's bandwidth allows to measure the time of flight (ToF) of a signal precisely:



- High sensitivity to clock errors: $1\,ns \Rightarrow 30cm$
- Threat model: wireless channel under attacker control

Our Contribution

We identify device clocks as a new attack vector.

Mix-Down:

- Affects the current (and future?) UWB standard
- Targets the Single-Sided Two-Way Ranging (SS-TWR) mode

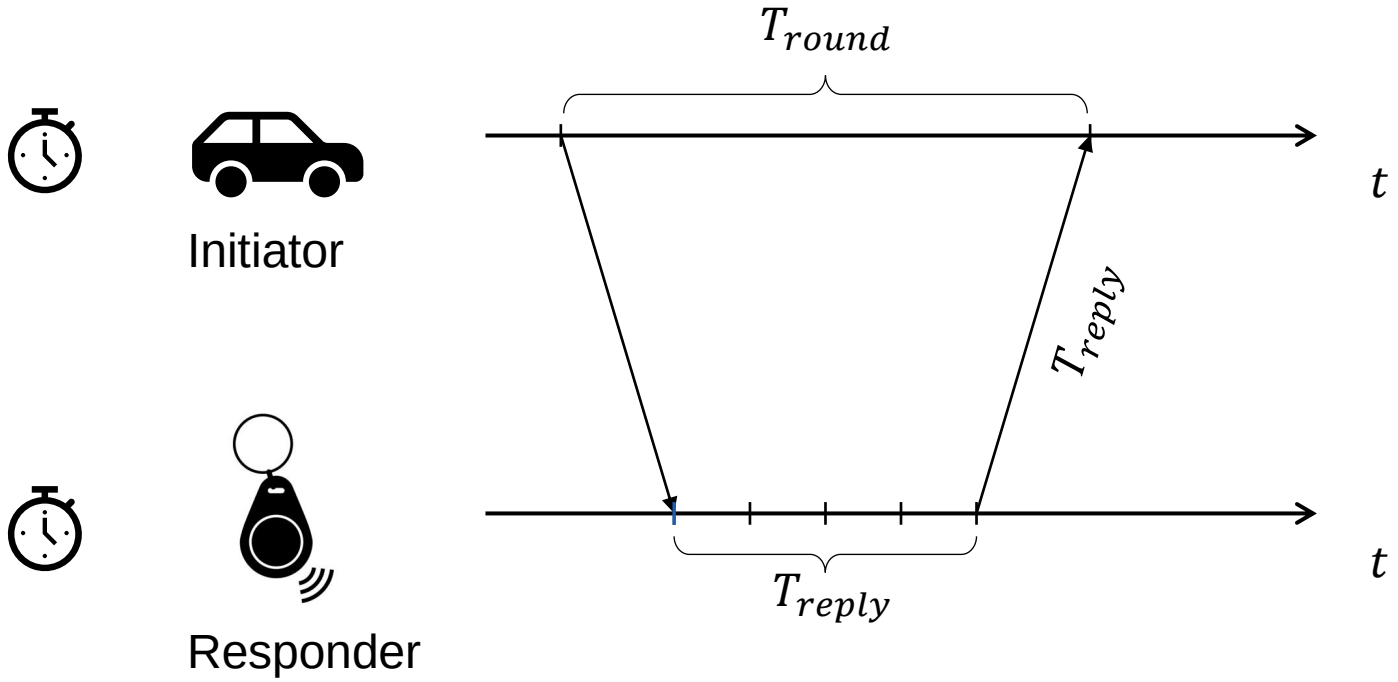
→ *We analyze and demonstrate the attack against off-the-shelf UWB chips*

Stretch-and-Advance:

- Affects the future UWB standard (IEEE 802.15.4ab)
- Attack is conceptual, vulnerable hardware does not exist (yet)

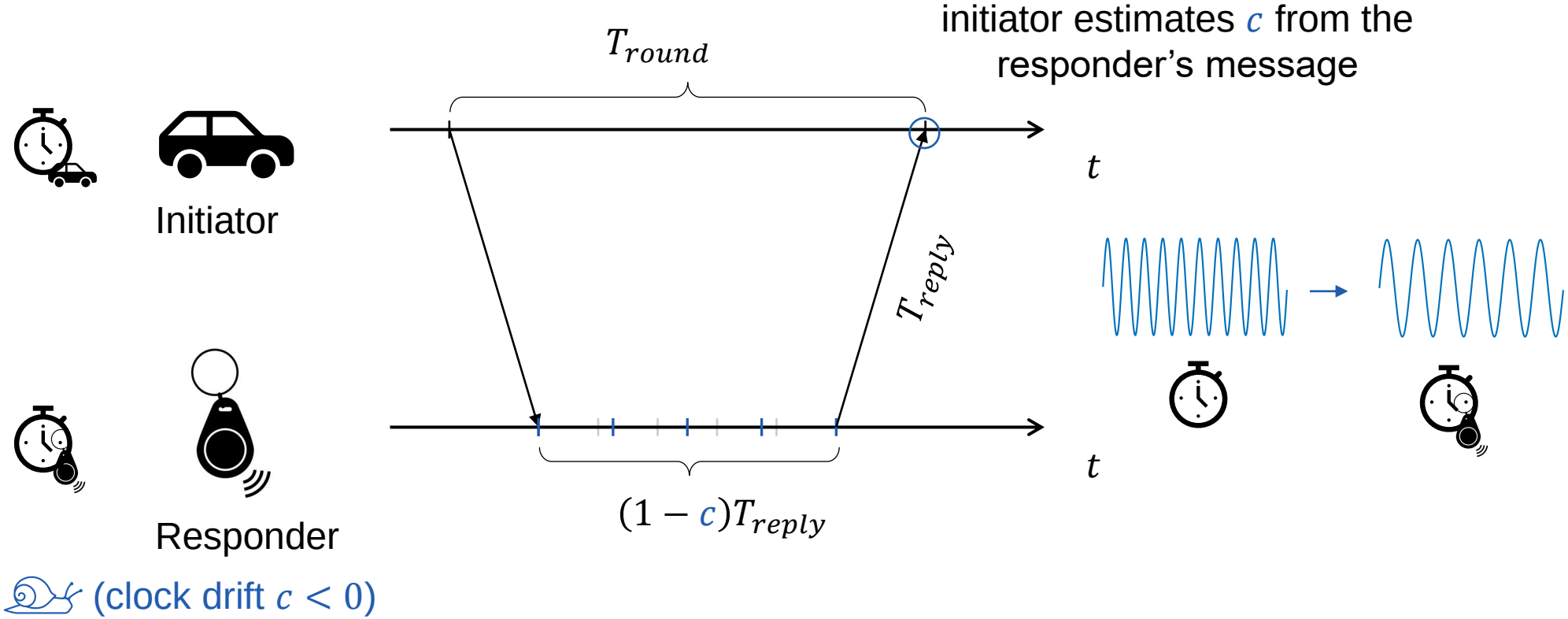
→ *We provide an extensive analysis of the attack and propose a countermeasure*

Single-Sided Two-Way Ranging in 802.15.4z



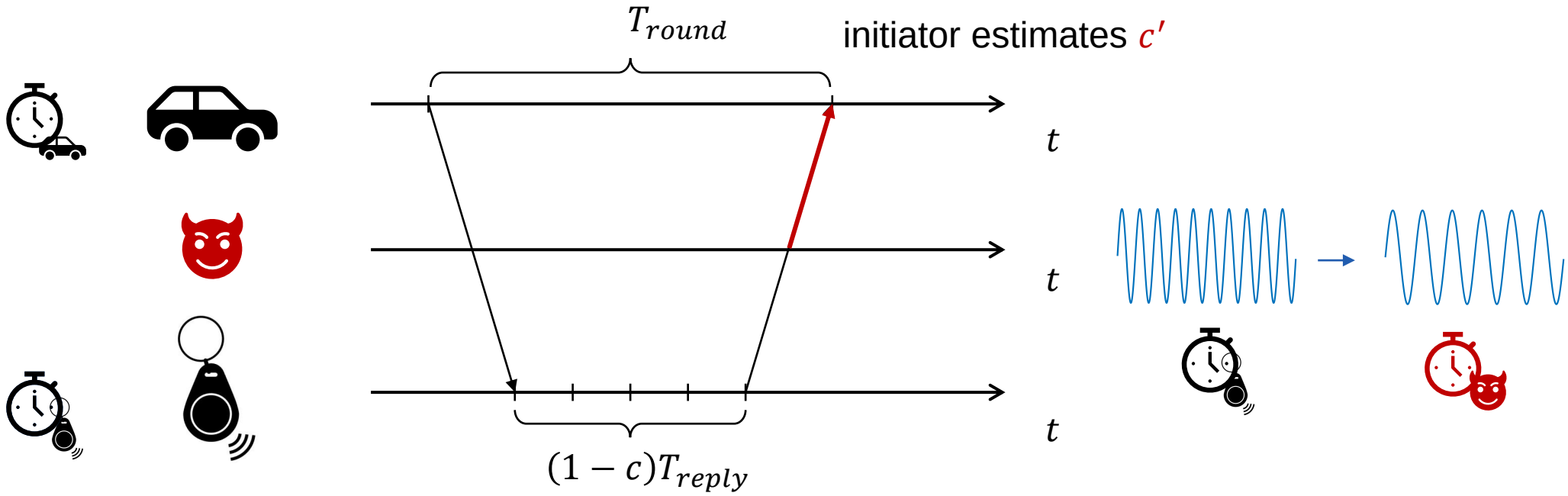
$$T_{ToF} = \frac{1}{2}\left(T_{round} - T_{reply}\right)$$

Single-Sided Two-Way Ranging in 802.15.4z



$$T_{ToF} = \frac{1}{2}\left(T_{round} - (1 - c)T_{reply}\right)$$

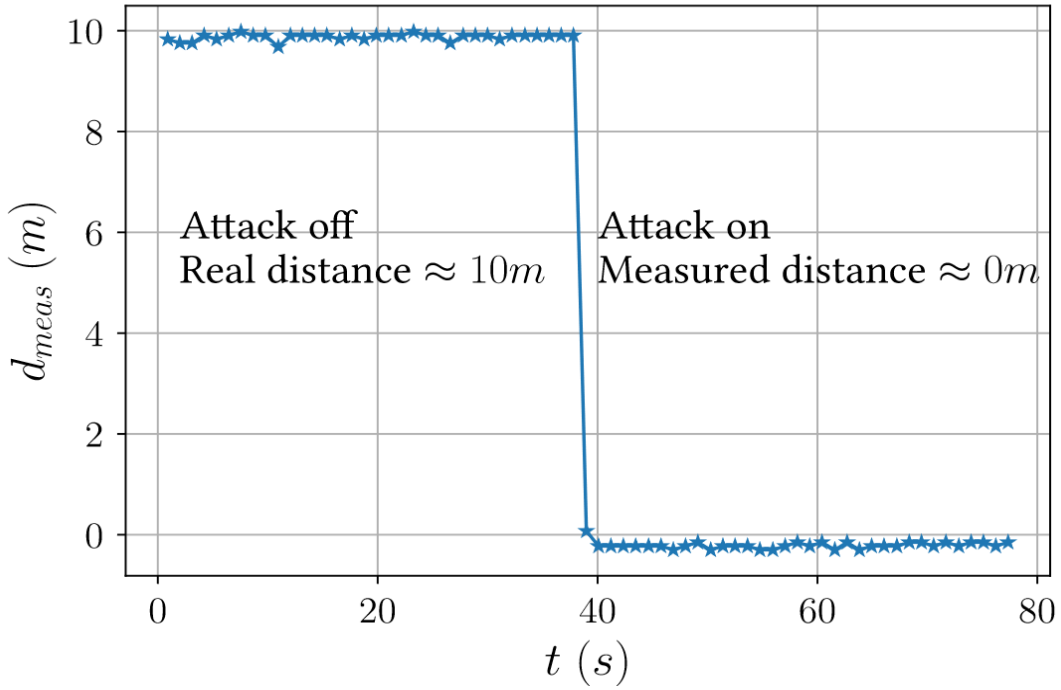
The Mix-Down Attack



$$T_{ToF} = \frac{1}{2}\left(T_{round} - (1-c)T_{reply}\right)$$

Results
(Figure 4)

We conducted the attack against two off-the-shelf UWB chips (Qorvo DWM3000EVB):



- Attack results in immediate, reliable distance reductions.
- Reductions can be controlled by gradually changing the clock drift.

Summary Mix-Down

Impact: Mix-Down only affects Single-Sided Two-Way Ranging (SS-TWR).

- Most (security-sensitive) applications use Double-Sided Two-Way Ranging.
- But: The upcoming standard IEEE 802.15.4ab seems to use SS-TWR as a default.

Countermeasures: No silver bullet in sight.

- The carrier frequency cannot be cryptographically protected
- Clocks drift naturally, e.g., due to changes in temperature
- Exchanging clock drift estimations? attacker can manipulate clock speeds in both directions

Alternative: Double-Sided Two-Way Ranging (but beware of Stretch-and-Advance!)

Takeaway

Mix-Down:

- Exploiting the clock drift compensation in SS-TWR
- Message content *not* changed
- Success rate: up to 100%
- Reductions depend on UWB chip's response time (e.g. $2ms \Rightarrow 12m$)
- No straightforward countermeasure

Stretch-and-Advance:

- Conceptual attack against the upcoming standard
- Affects SS-TWR and DS-TWR
- Reductions in the order of $100m$
- Analysis and countermeasure discussed in the paper

ETH zürich

Claudio Anliker
claudio.anliker@inf.ethz.ch

ETH Zurich
Department of Computer Science
Universitätsstrasse 6
8092 Zurich
Switzerland

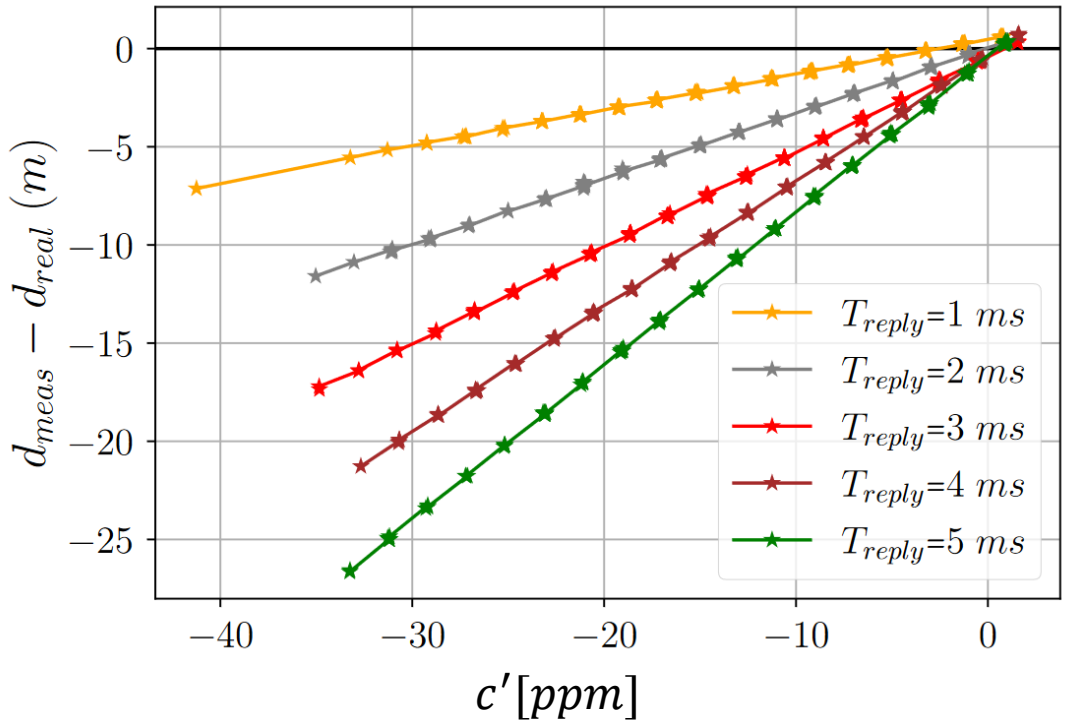
syssec.ethz.ch

APPENDIX

Image sources:

- BMW Keyfob: https://www.autox.com/quattroruote/bmw-ix-ev-road-test-110419/
- Keyfob icon: https://www.istockphoto.com/de/vektor/nfc-schl%C3%BCsselanh%C3%A4nger-silhouettensymbol-gm1352049152-427589349?phrase=key+fob+icon
- Contactless payments: https://n26.com/en-eu/contactless-card
- Access control: https://cie-group.com/how-to-av/videos-and-blogs/bluetooth-ble-access-control
- Chip icon: https://www.flaticon.com/free-icon/chip_2818291

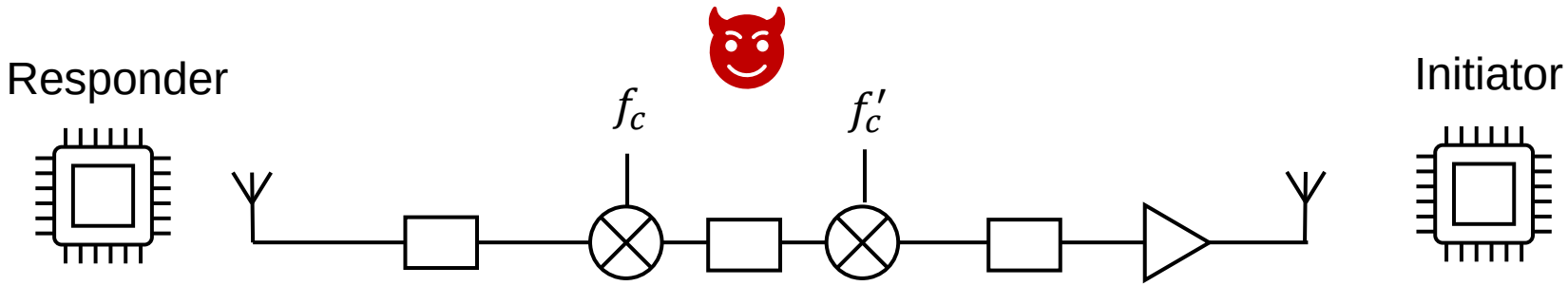
Results
(Figure 5, simplified)

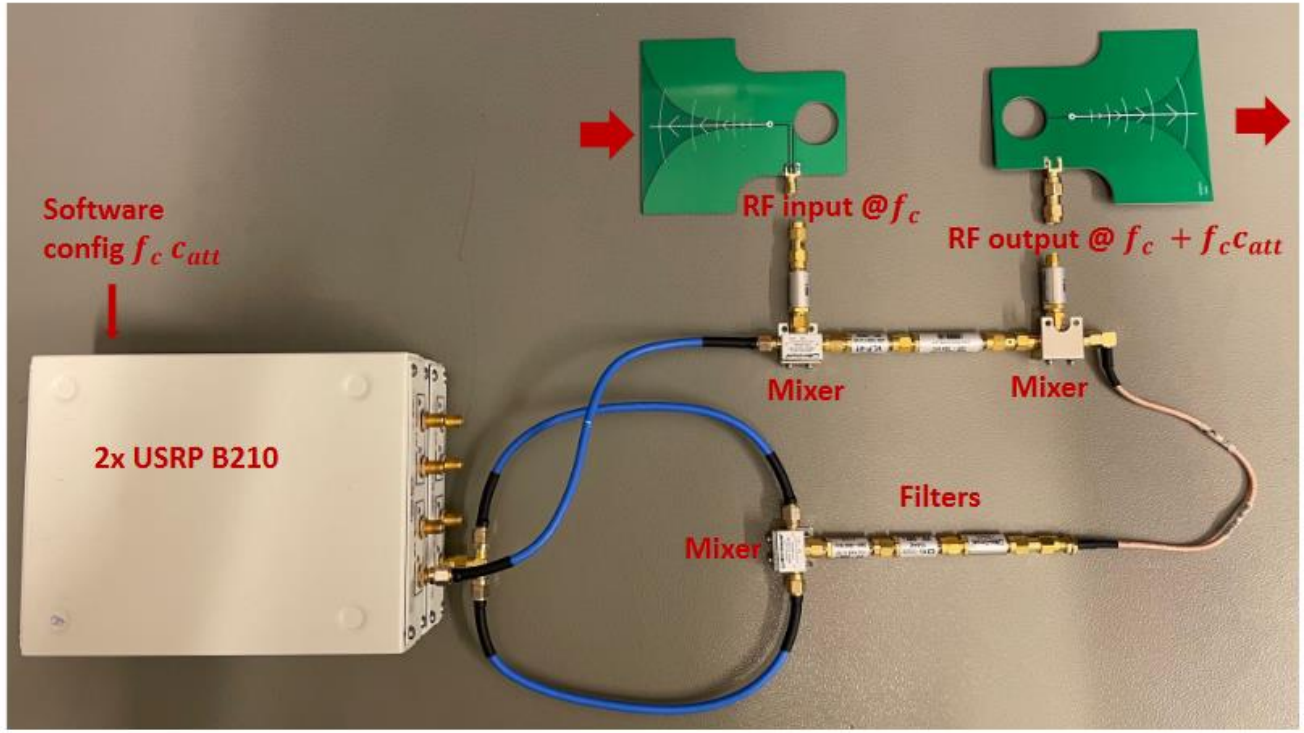


The distance reductions depend linearly on

- the clock drift c' caused by the attacker and
- the reply/processing time of the responder.

Setup


Responder
f_c
f_c'
Initiator


Software config f_c c_{att}
RF input @ f_c
RF output @ $f_c + f_c c_{att}$
Mixer
Mixer
2x USRP B210
Filters
Mixer

A Glimpse into Stretch-and-Advance

The upcoming UWB standard IEEE 802.15.4ab introduces Multi-Millisecond Ranging

- Length of ranging frames changes from $\approx 100\mu s$ to dozens of ms.
- Successful reception of such frames requires compensation of clock errors
- With specialized hardware, an attacker could
  - *stretch* the genuine ranging message in time and
  - *advance* parts of it (send it earlier)
- Exploitability and reduction limits depend on implementation
- These effects are negligible in 802.15.4z because the messages are too short.