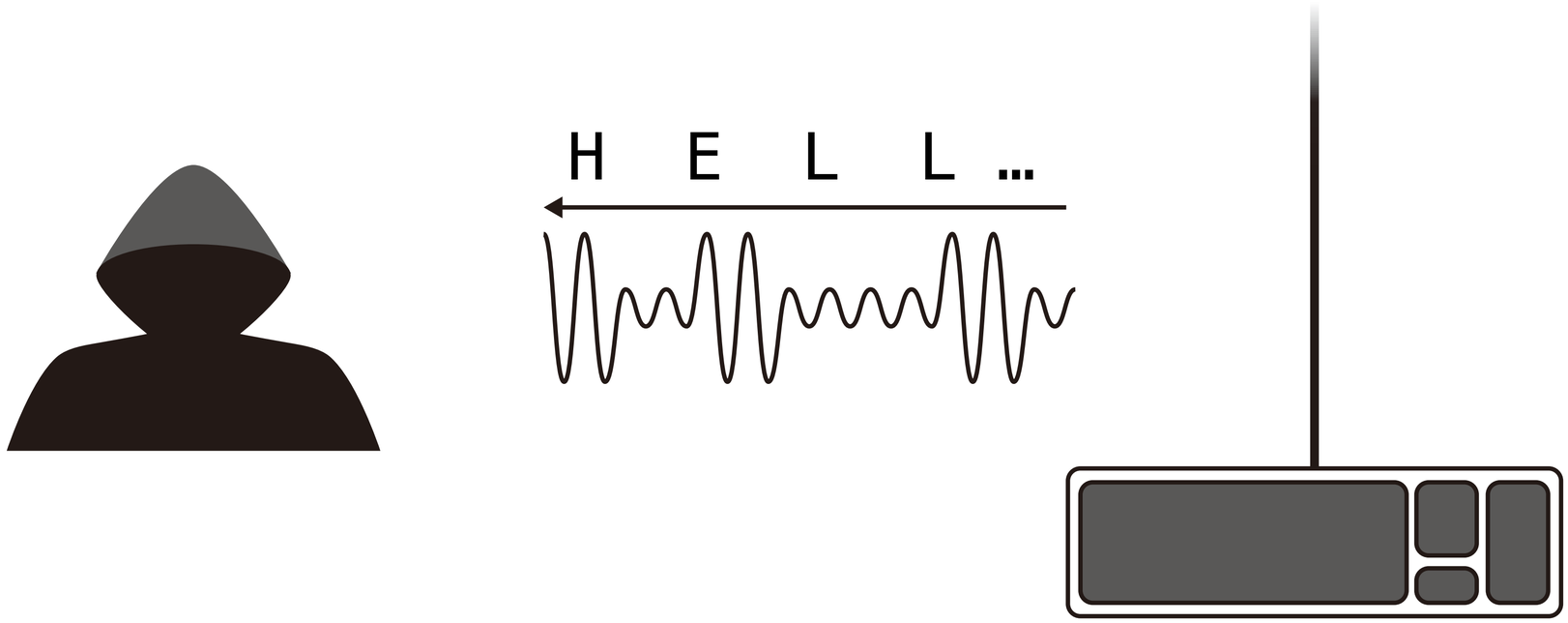
A Feasibility Study of Radio-frequency Retroreflector Attack

Satohiro Wakabayashi, Seita Maruyama, Tatsuya Mori, Shigeki Goto, Masahiro Kinugawa, Yu-ichi Hayashi

Waseda University, National Institute of Technology
Sendai College, Nara Institute of Science and Technology

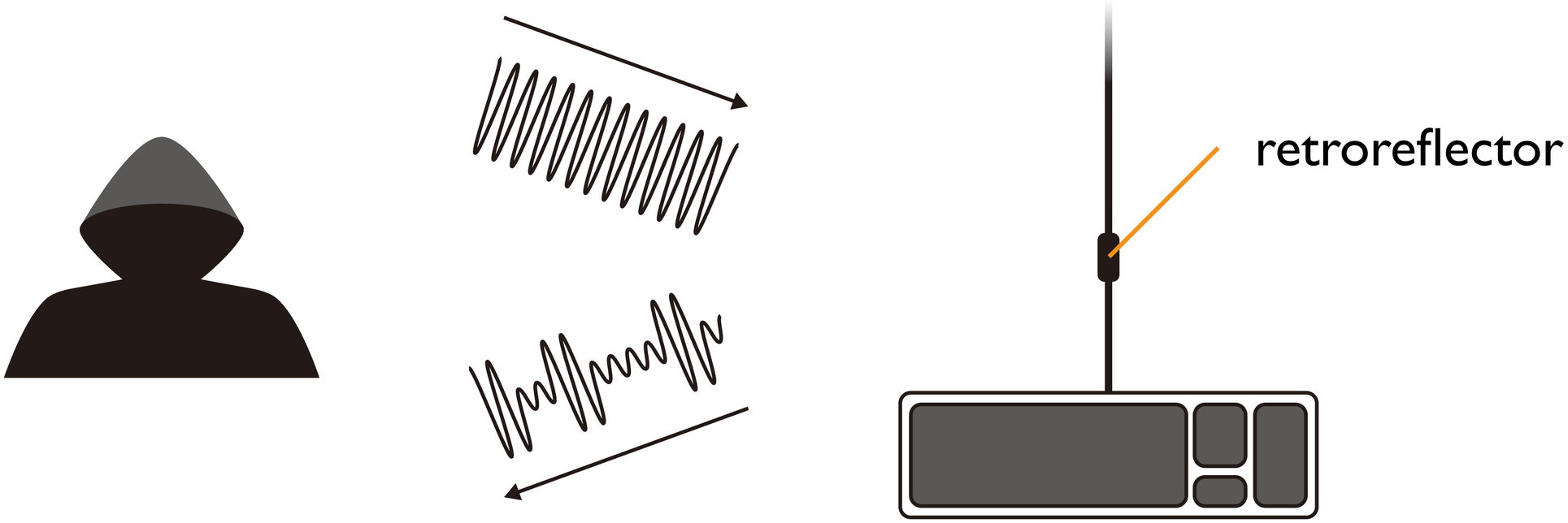
Background: (passive) EM side-channel attack



Typing “Hello”

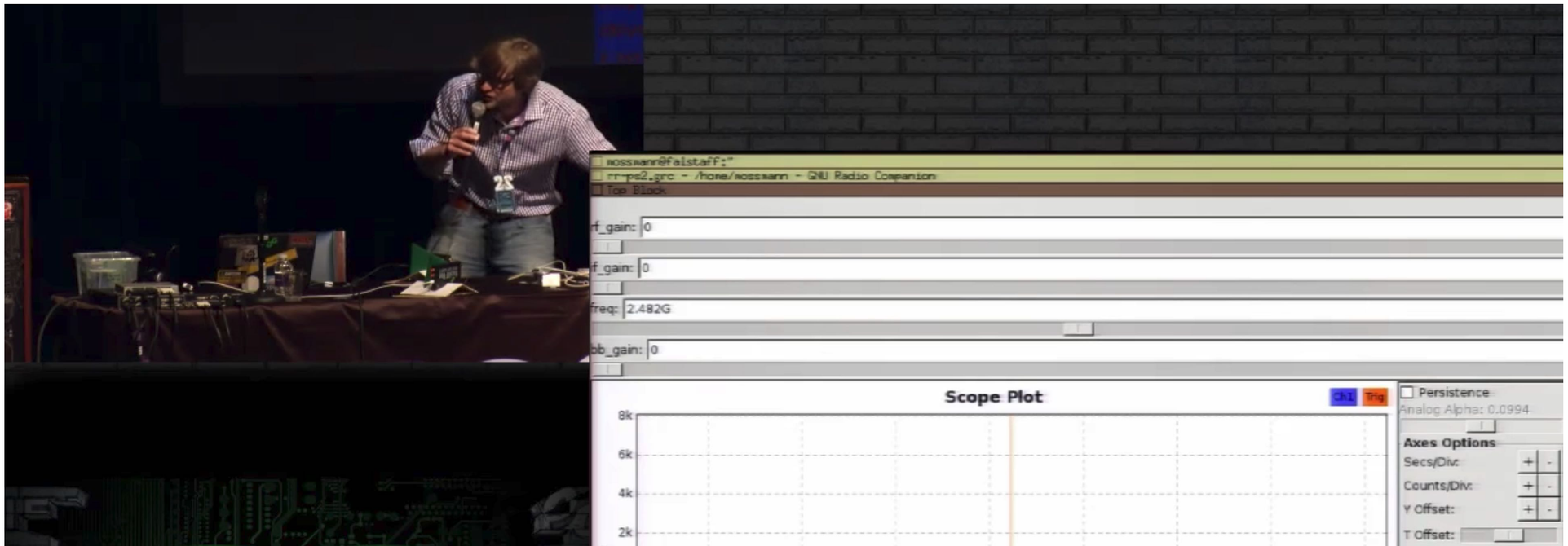
Radio-Frequency Retroreflector Attack (RFRA)

- is an **active** electromagnetic side-channel attack
- aims to steal **the target's signals** by actively irradiating the targeted device with a radio wave
- A **malicious circuit (retroreflector)** is embedded in the target device in advance

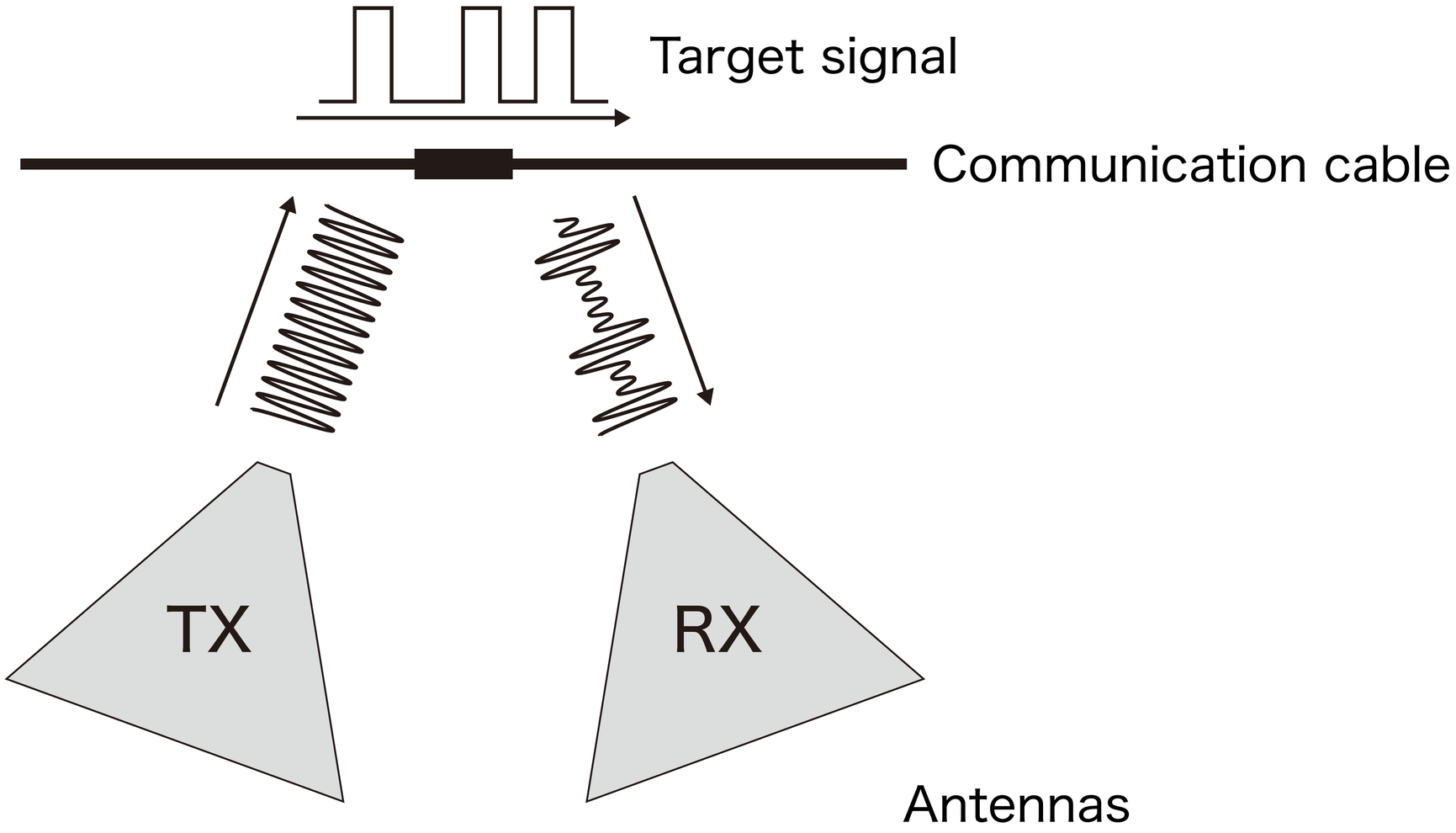


Background of RFRA

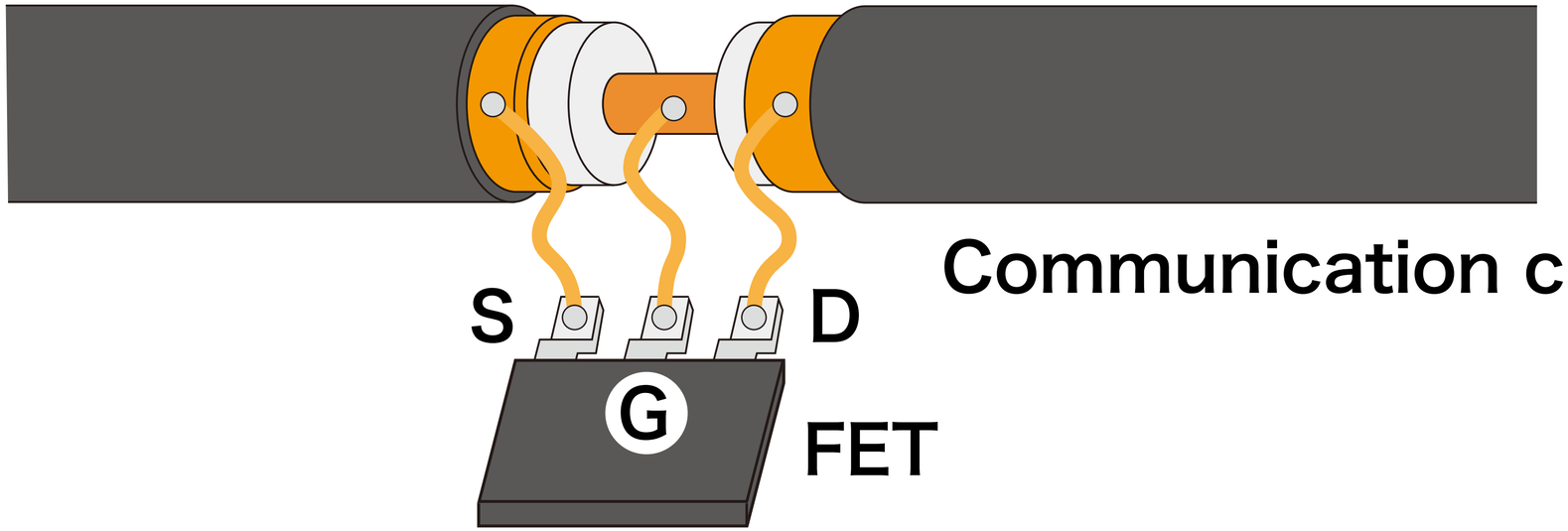
- "The Thing": a predecessor of RFID and RFRA (mid 20th century)
- Possible use of RFRA in the intelligence community (R. J. Anderson 2008)
- NSA ANT catalog: ANGRYNEIGHBOR (2014)
- RFRA demo/talk: DEF CON 22, USENIX WOOT2015 (M. Ossmann)

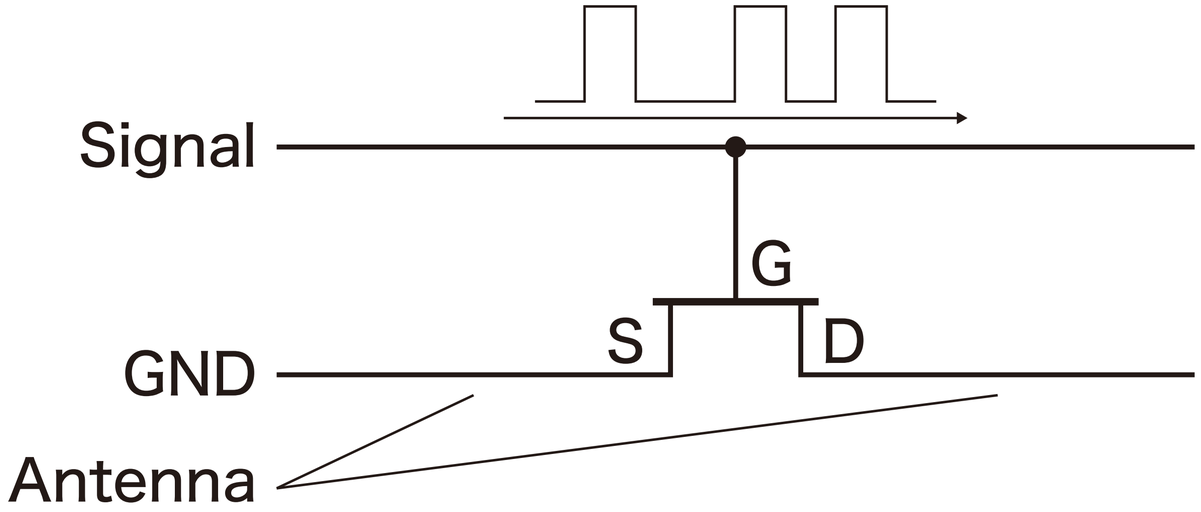


Attack overview



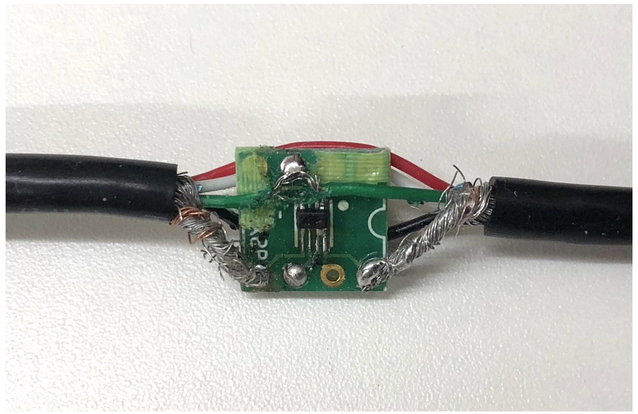
Retroreflector

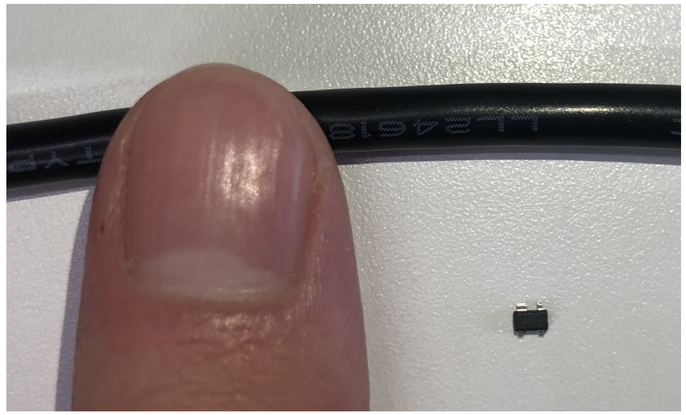




Retroreflector

- Retroreflector consists of
  - field-effect transistor (FET) chip
  - wire that can work as a dipole antenna
- FET is very small
  - It is easy to implement anywhere
- An attacker needs to transmit radio waves that is resonant frequency of dipole antenna



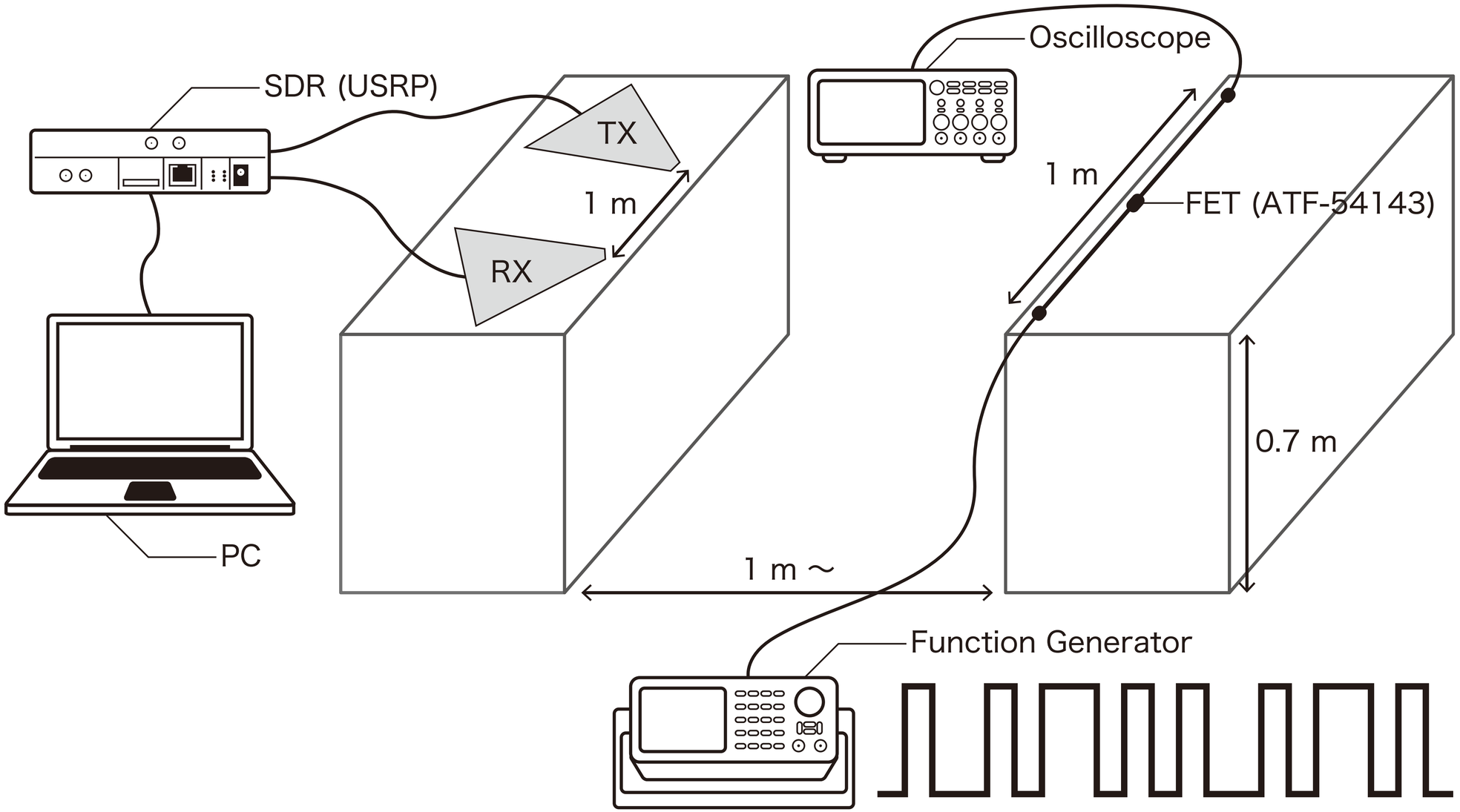


Research Questions

- It is known that the RFRA works in practice
- Our research question is: Is the RFRA a feasible attack?
  - The attackable distance between target and attacker
  - The limit of the speed of the target signal
  - Real-world applications

1. Evaluation of RFRA

Attack setup



Equipment

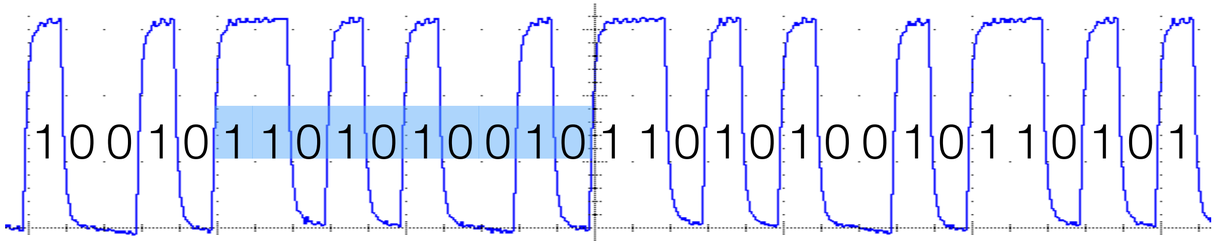
Instruments used in the experiments

Insturument	Model
Antenna	Ettus Research LP0410
SDR	USRP N210（Up to 50 MS/s）
Attacker PC	ASUS ROG G752VS
FET	ATF-54143

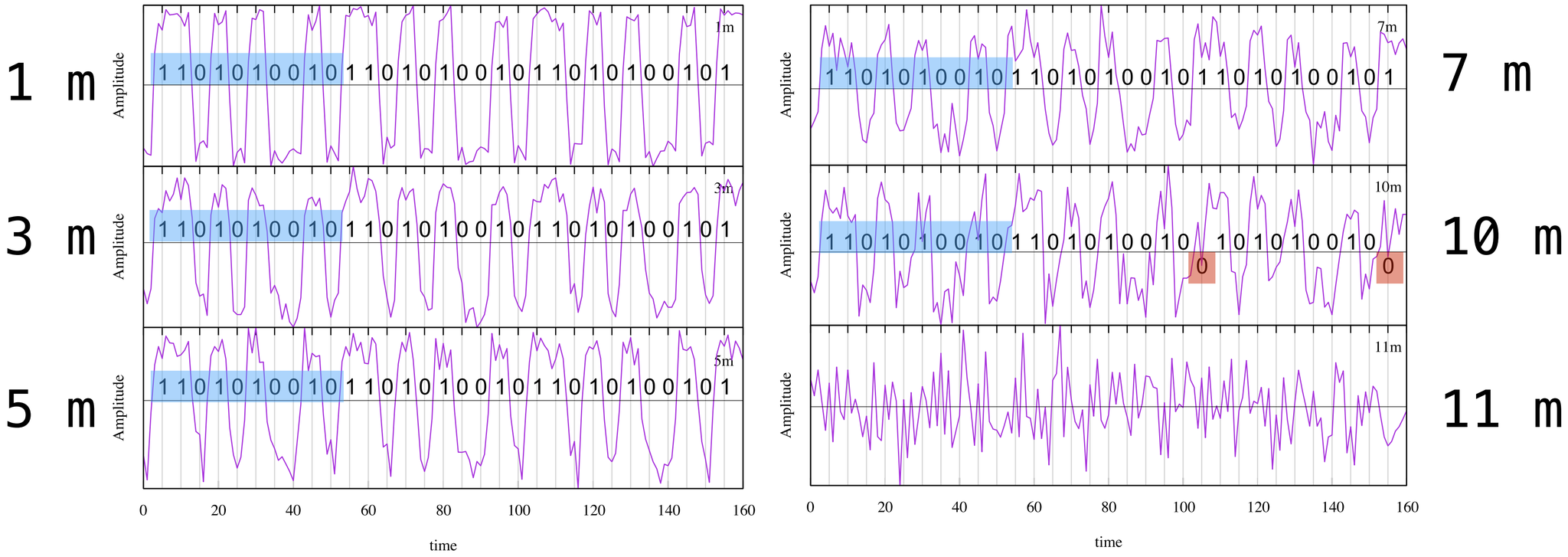
List of software and PC used for SDR

OS	Windows 10
SDR software toolkit	GNU Radio 3.7.11
CPU	Core i7 7700HQ 2.8 GHz/4 Core
RAM	32 GB

Results on distance

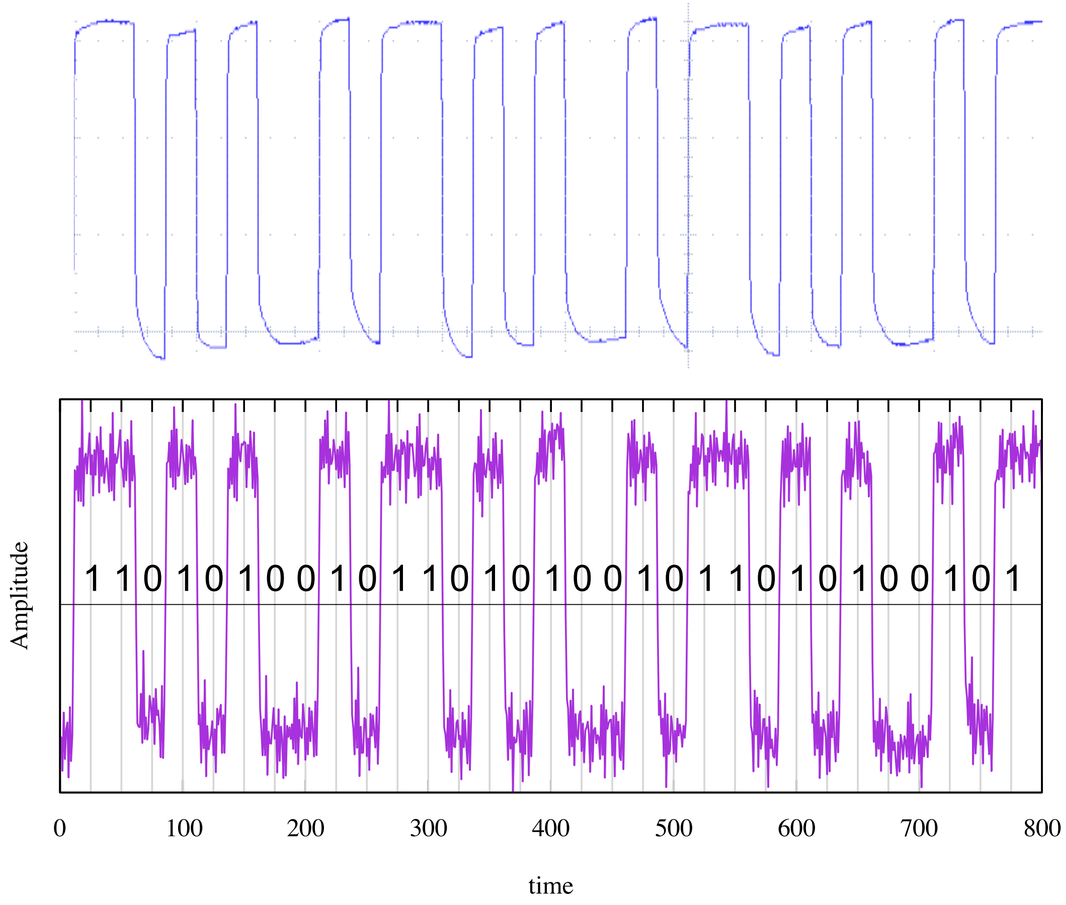


Target signal
2 Mbps



SDR sampling rate is 10 MS/s

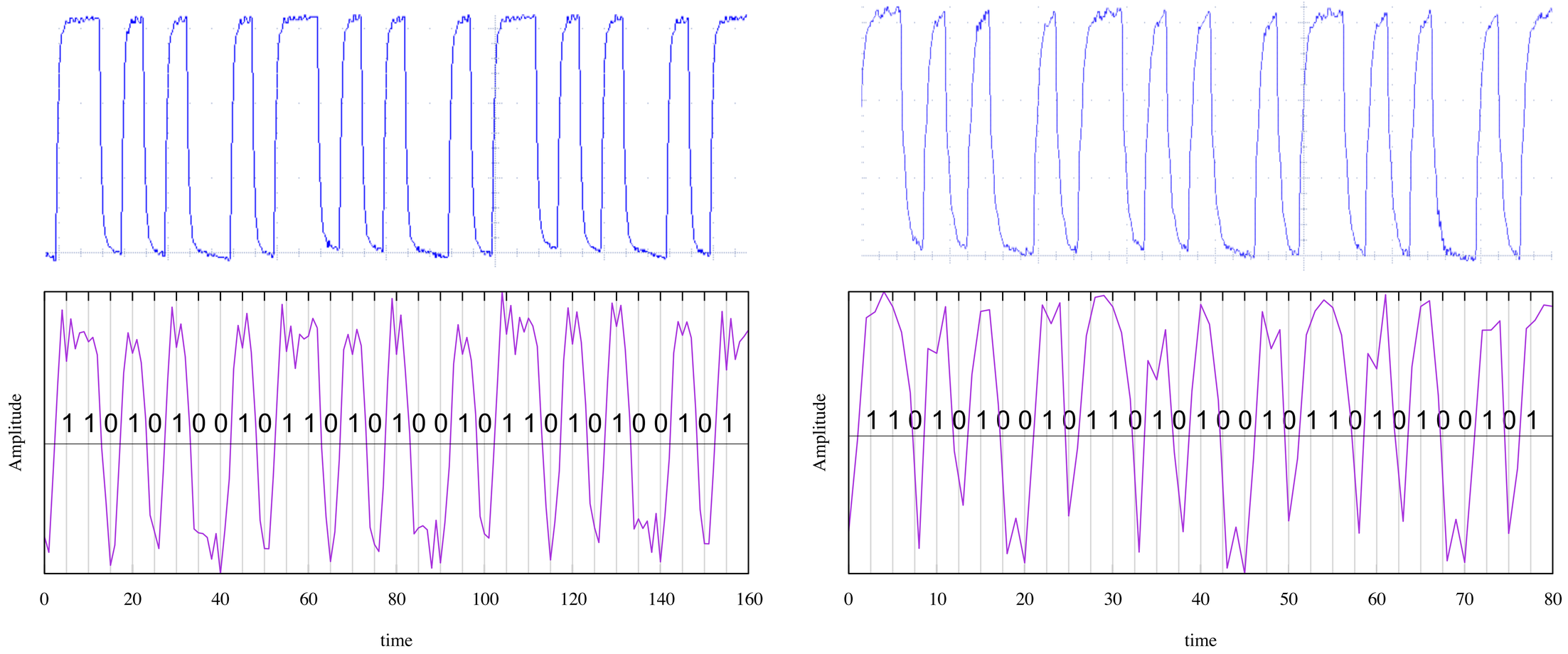
Results on rate of target signal



1 Mbps

Attacked from 1 m, SDR sampling rate is 25 MS/s

Results on rate of target signal



5 Mbps

10 Mbps

Attacked from 1 m, SDR sampling rate is 25 MS/s

Summary of the experiment

- The total cost of setup is approximately 5000 US dollars.
- The attack succeeded from 10m distance
  - 10 m is enough flexibility in setting up the attack equipment
- The attack succeeded to the target signal of 10 Mbps
  - USB keyboard may be attackable

2. Application

Application

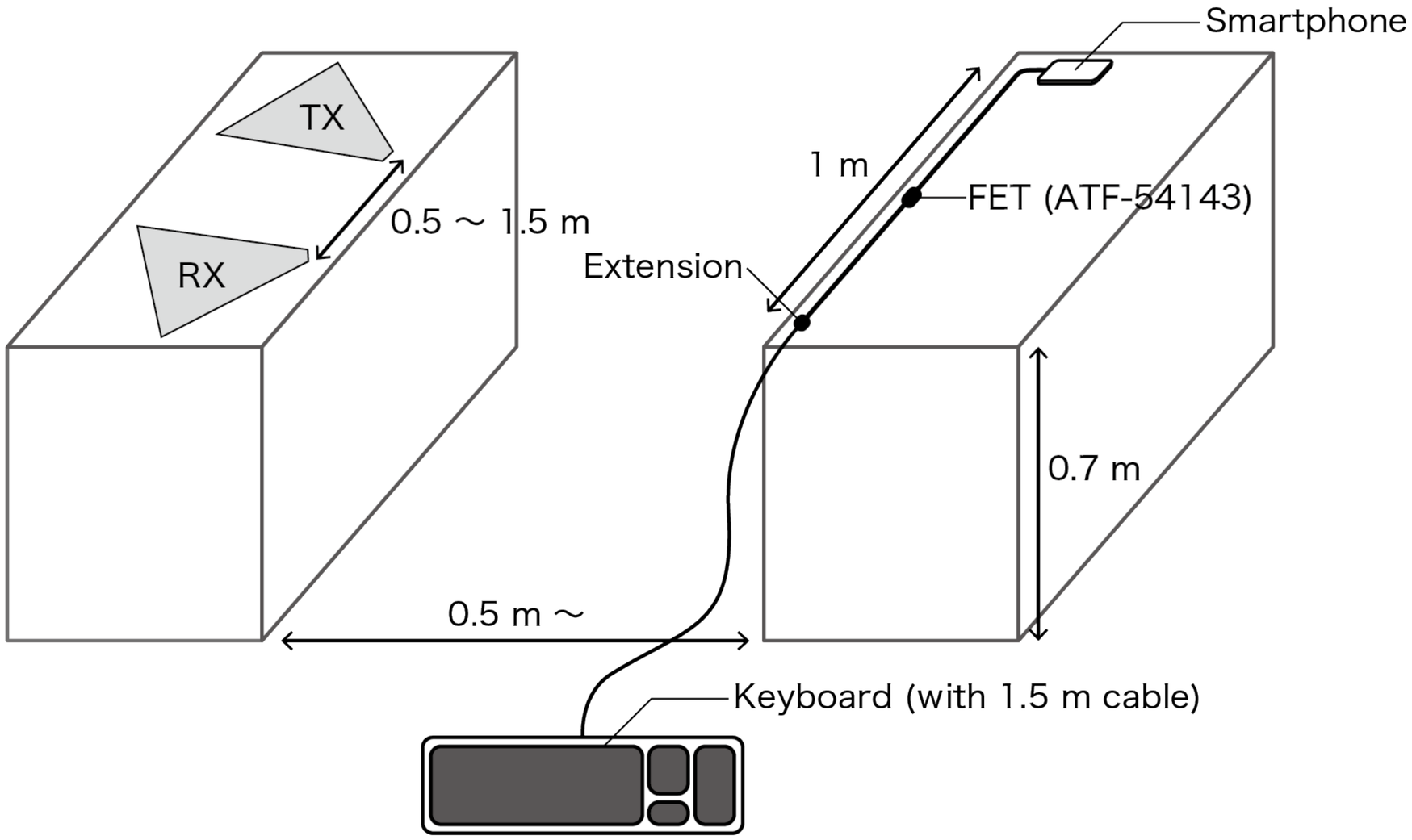
- 10 Mbps communication is attackable (previous experiment)
- USB transfer rates are …
  - **USB low-speed mode: 1.5 Mbps**
  - USB full-speed mode: 12 Mbps
  - USB high-speed mode: 480 Mbps
- USB low-speed mode is attackable!

Application

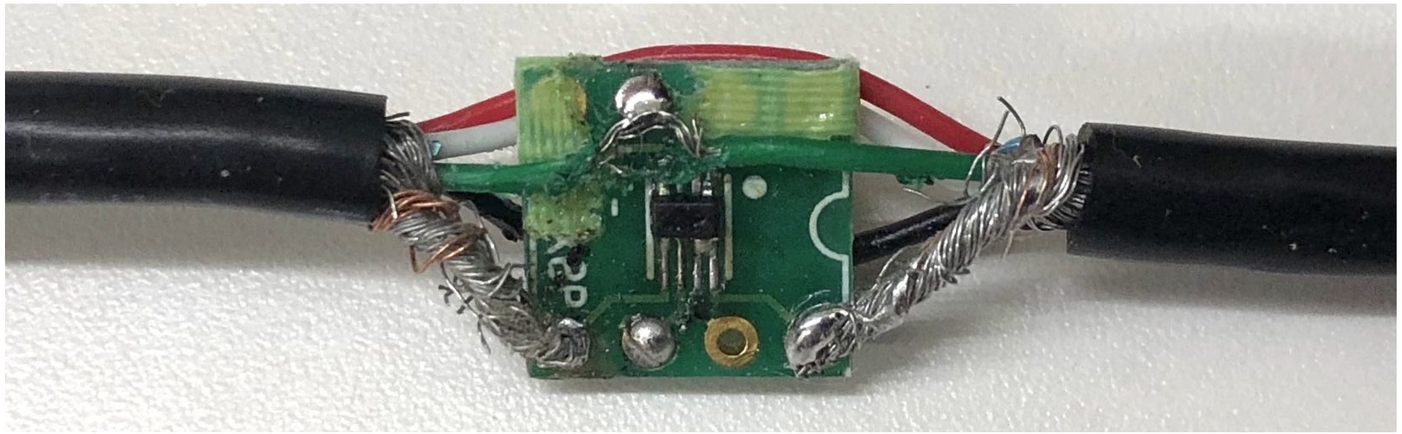
- Most of USB keyboards use USB low-speed mode
- Is RFRA effective for real-world applications?

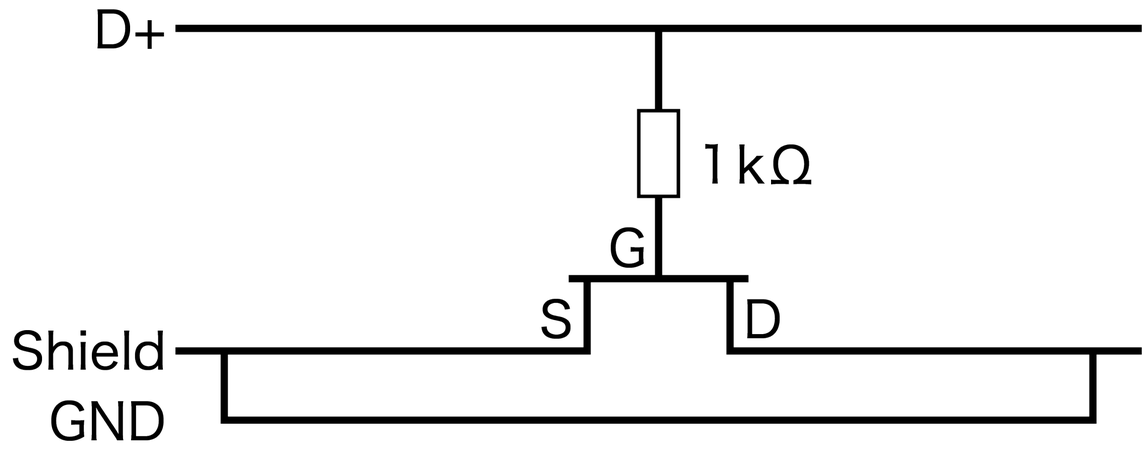
- Eavesdrop typing of USB keyboard and evaluate the accuracy
  - We typed pangram
    ex) “My faxed joke won a pager in the cable TV quiz show.”
- We developed program to detect typed keys from an eavesdropped waveform

Experiment


Smartphone
TX
RX
0.5 ～ 1.5 m
1 m
FET (ATF-54143)
Extension
0.7 m
0.5 m ～
Keyboard (with 1.5 m cable)

Implementation





It works as folded dipole antenna

Result

Error rate

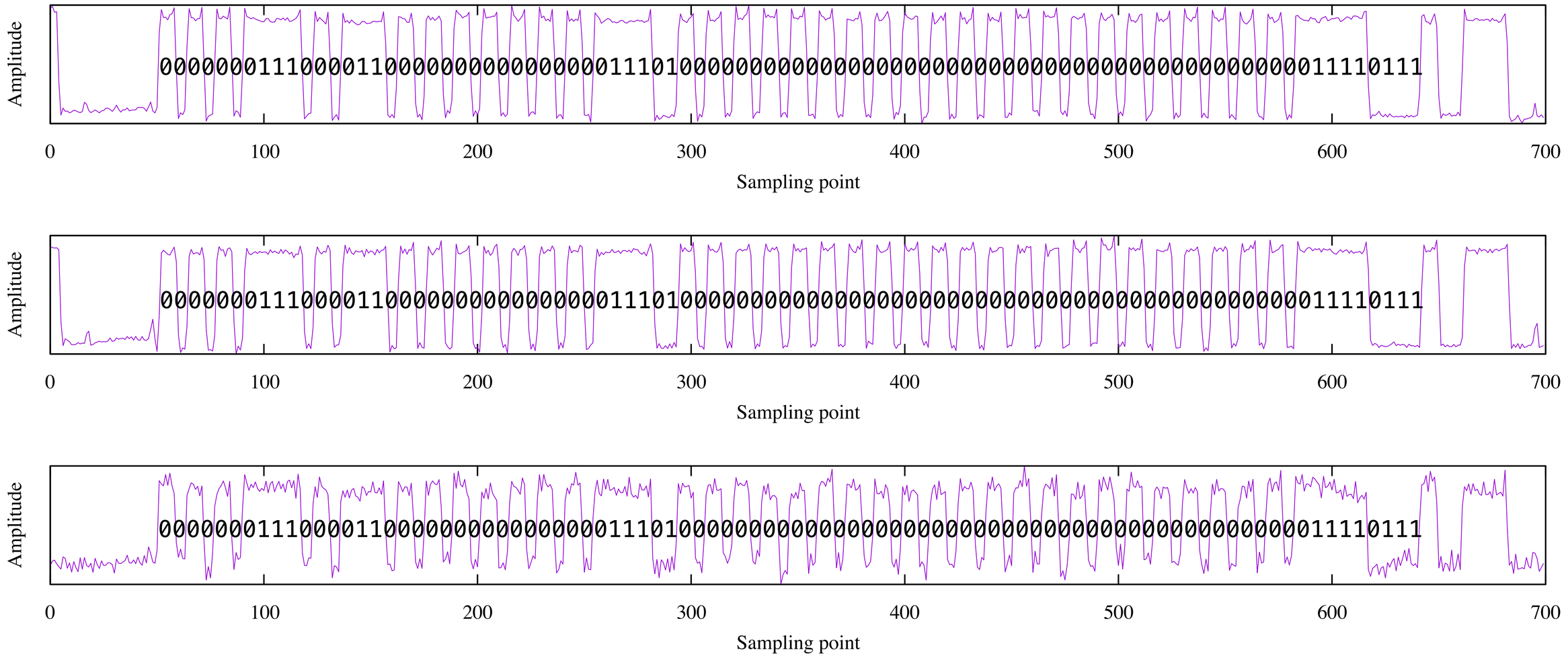
Distance [m]	Error rate [%]
0.5	0.0
1.0	0.0
1.5	1.0
2.0	100.0

Error point (1.5 m)

… paper in the cable tv …
… paper in th cable tv …

Result

Waveforms we eavesdropped (0.5, 1.0, 1.5 m)



Limitation

- Attackable target communication speed depends on the sampling rate of SDR
  - high-performance hardware can extend the limitation
- The resonant frequency is changed by the shape of target cable.
  - Attack becomes difficult if victim wears a cable because the shape of cable changes frequently

Countermeasures

- The best solution is “encryption.”
- Detecting malicious circuit in the physical layer
  - There was a previous study on detecting hardware key loggers
  - If a FET is embedded at the time of manufacturing, this approach may not be directly applicable
- Monitoring malicious/reflected radio waves
  - Quite difficult…
- Further research is needed

Future work

- Some conditions are not clear
  - Frequency of irradiation radio waves
  - Antenna position
- Attacking analog signals
  - Audio cable (less than 20 kHz)
  - VGA cable (25 MHz)

Conclusion

- Using 5000 dollars setup
  - Attackable from 10 m
  - Attackable 10 Mbps signal
- We showed that RFRA is applicable for USB devices