

WiFi security and physical layer stuff

CSE 468 Fall 2024
jedimaestro@asu.edu

Name: _____

CSE 468 Fall 2024 Midterm

Instructions

Don't forget to write your name at the top. You have an hour and 15 minutes (a regular class period) to complete this exam (unless you are taking it in another location with different arrangements). Mark on these sheets of paper with a pen or pencil, and then turn it in at the front of the room to the TA or I. You may not use scratch paper or notes of any kind, so there should be no other pieces of paper on your desk during the exam and you should not write on anything other than the exam itself. This exam is closed book (note that there is no textbook for the course) and closed note. You may use a calculator, even a scientific calculator if you like, but you may not use any other electronic device (and especially not a cell phone). You may not communicate in any way with any individuals other than the instructor of the course, the TA, or another official proctor during the exam. Any violation of these policies will result in a 0 on the exam and will be treated as an act of academic dishonesty as per the syllabus. For multiple choice questions, circle the one best answer. The exam is worth 100 points total. Students can ignore this number: 0.

Who cares about the local physical layer?

- Example 1: Poor transport-layer security
- Example 2: ARP cache poisoning

WiFi security

- WEP, WPA, WPA2, WPA3

Other applications of radio signals

- 3G, 4G, 5G, 900 Mhz, Bluetooth, ...

Who cares?

meituan.pcap

- Check out frame 36878
- Almost 700 million Annual Transacting Users

Who cares? (continued)

arpspoof.pcap

-Downloaded from

<https://github.com/researcher111/ARP-pcap-files/blob/master/arpspoof.pcap>

-Real gateway is 08:00:27:5e:01:7c

-Fake gateway is 08:00:27:2d:f8:5a

-This is called ARP cache poisoning or ARP spoofing

-(Used to be a lot more complicated, these days switches and ARP caches mostly all act the same)

Free US shipping for orders over \$250

PRODUCTS ▾ PAYLOADS ▾ SHOWS



COMMUNITY SUPPORT ▾

HOME / ALL / WIFI PINEAPPLE



WIFI PINEAPPLE

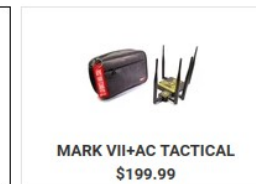
\$119.99

The industry standard WiFi pentest platform has evolved. Equip your red team with the WiFi Pineapple® Mark VII. Newly refined. Enterprise ready.

Basic edition includes antennas and USB-C power/ethernet cable.



MARK VII BASIC
\$119.99



MARK VII+AC TACTICAL
\$199.99

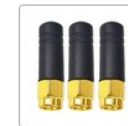
Accessories



WiFi Pineapple E-Book



MK7AC WiFi Adapter



Stubby Antenna 3 Pack

WiFi security

Basically three use cases

- Open
- Personal (e.g., a passphrase)
- Enterprise

<https://securityuncorked.com/2022/07/wifi-security-the-3-types-of-wifi-networks/>

WiFi security in a nutshell

WEP is very, very bad (see stream cipher slides)

WPA was only a stop gap

WPA2 is maybe okay for now if you do it right?

WPA3 is better, maybe?

WEP: the dawn of wireless

Open just meant unencrypted

Personal meant pre-shared key

No such thing as Enterprise

Top song in 1997: “Candle in the Wind 1997”

WEP encryption

“Wired Equivalent Privacy”

-Have to be physically in a building to plug in, have to know the passphrase to join WiFi (or do you?)

RC4, 40-bit key, 24-bit IV

WiFi Protected Access

- Stop gap because of WEP's failures
- Encrypt like it's 1999

Temporal Key Integrity Protocol (TKIP)

- Key mixing with IV and counter instead of concatenation
- Out of order packets rejected by access point
- 64-bit Message Integrity Check (MIC)
 - Same thing as a Message Authentication Code (MAC)

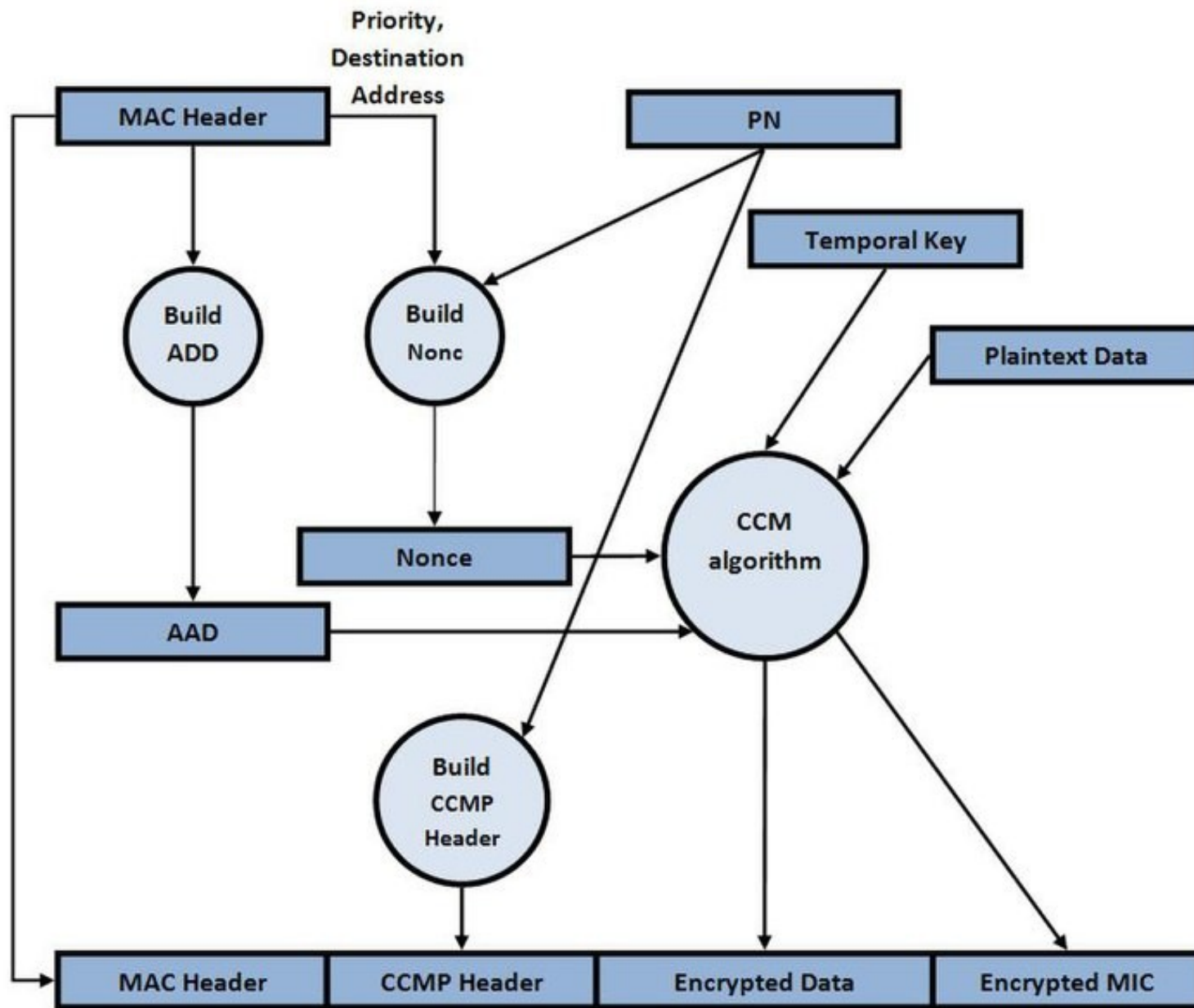
WPA2

Personal vs. Enterprise

Actual solution, not just new WPA version

-Top 2004 pop song: Yeah! (feat. Lil Jon & Ludacris)Usher, Lil Jon, Ludacris

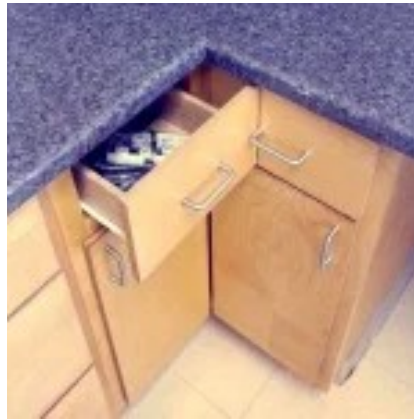
AES and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)



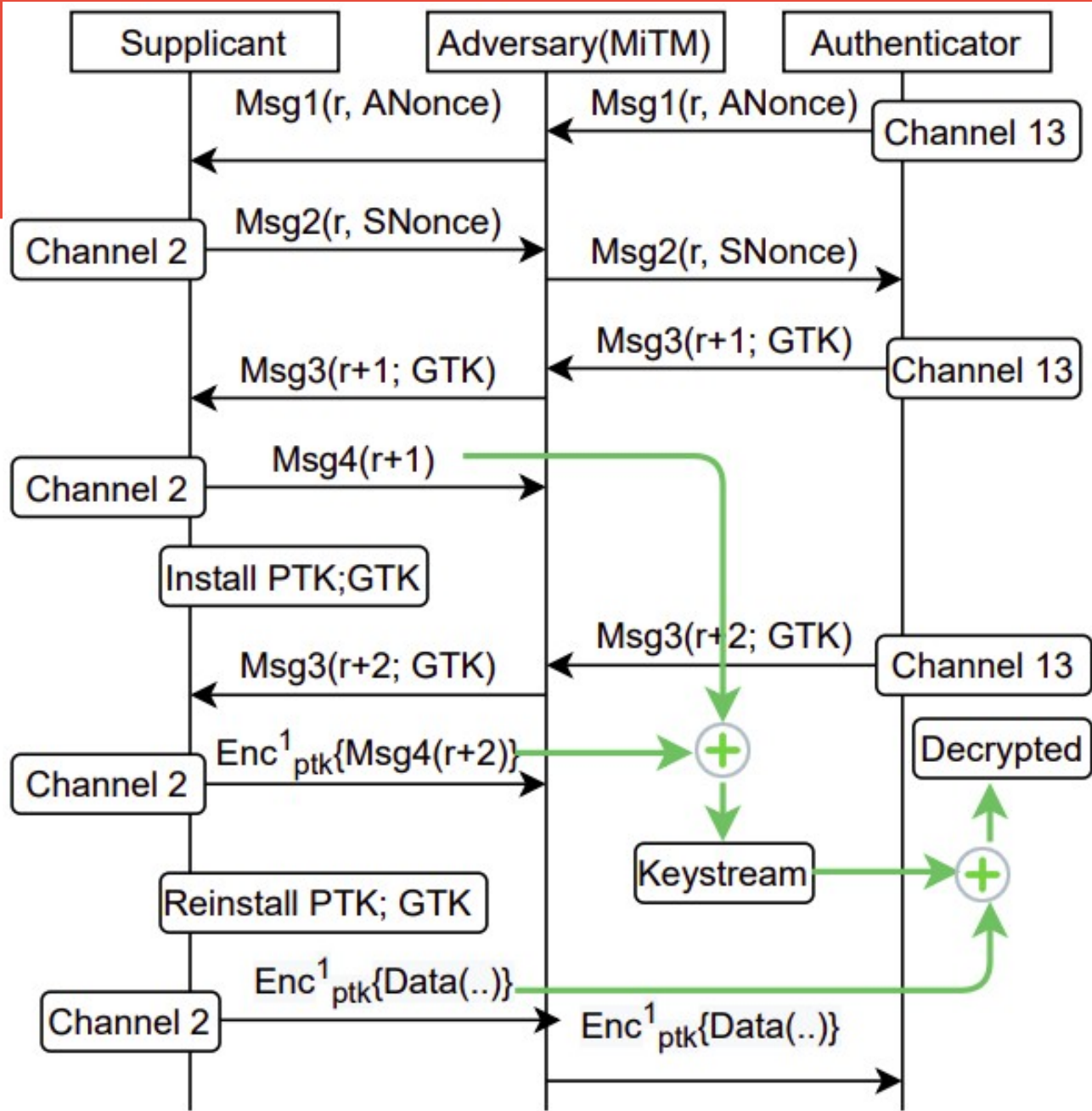
KRACK attacks

-<https://www.krackattacks.com/>

-<https://blog.cryptographyengineering.com/2017/10/16/falling-through-the-cracks/>



Crypto protocol and handshake



A. Agrawal, U. Chatterjee and R. Maiti, "CheckShake: Passively Detecting Anomaly in Wi-Fi Security Handshake Using Gradient Boosting Based Ensemble Learning" in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 06, pp. 4868-4880, 2023.

WPA2 Enterprise

RADIUS server, Extensible Authentication Protocol (EAP)

- First step of 4-way handshake is, e.g., username and password instead of pre-shared password
- Still vulnerable to KRACK

WPA3

Lots of improvements over WPA2

- Top pop song in 2018: "God's Plan" by Drake
- Bigger keys possible: 192-bit equivalent AES-256 GCM and SHA-384 HMAC
- Simultaneous Authentication of Equals (SAE), Diffie-Hellman and forward secrecy
- Open network improvements a.k.a. Enhanced Open (<https://securityuncorked.com/2022/08/wifi-security-wpa2-vs-wpa3/>)

Dragonblood attacks (2019)

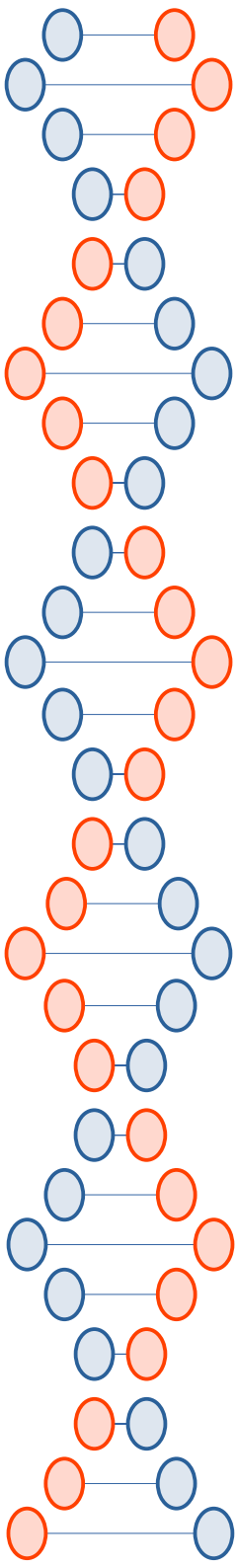
- Side channels and downgrade attacks
- <https://wpa3.mathyvanhoef.com/>



Dragonblood attacks on WPA3

- Downgrade attacks (enterprise)
- Side channel (personal)
- Slides plagiarized from...


<https://papers.mathyvanhoef.com/wac2019-slides.pdf>

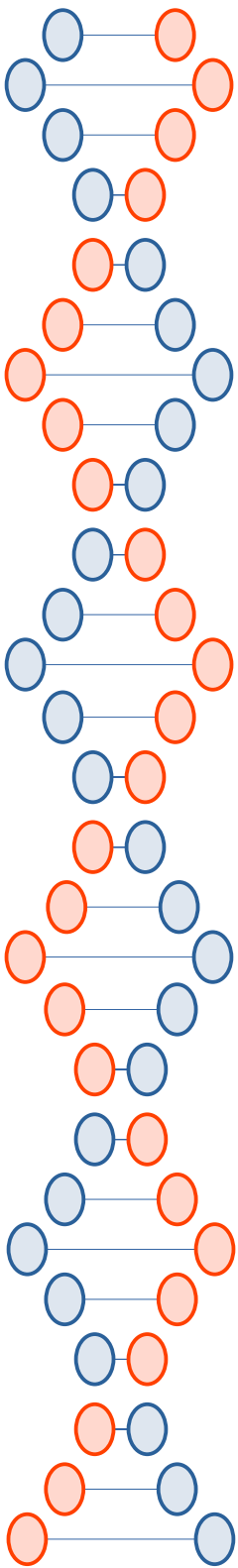


Convert password to MODP element

```
for (counter = 1; counter < 256; counter++)  
    value = hash(pw, counter, addr1, addr2)  
    if value >= p: continue  
    P = value(p-1)/q  
    return P
```

Leaked information: #iterations needed

Client address	addrA	addrB	addrC
Measured			
Password 1			
Password 2			
Password 3			



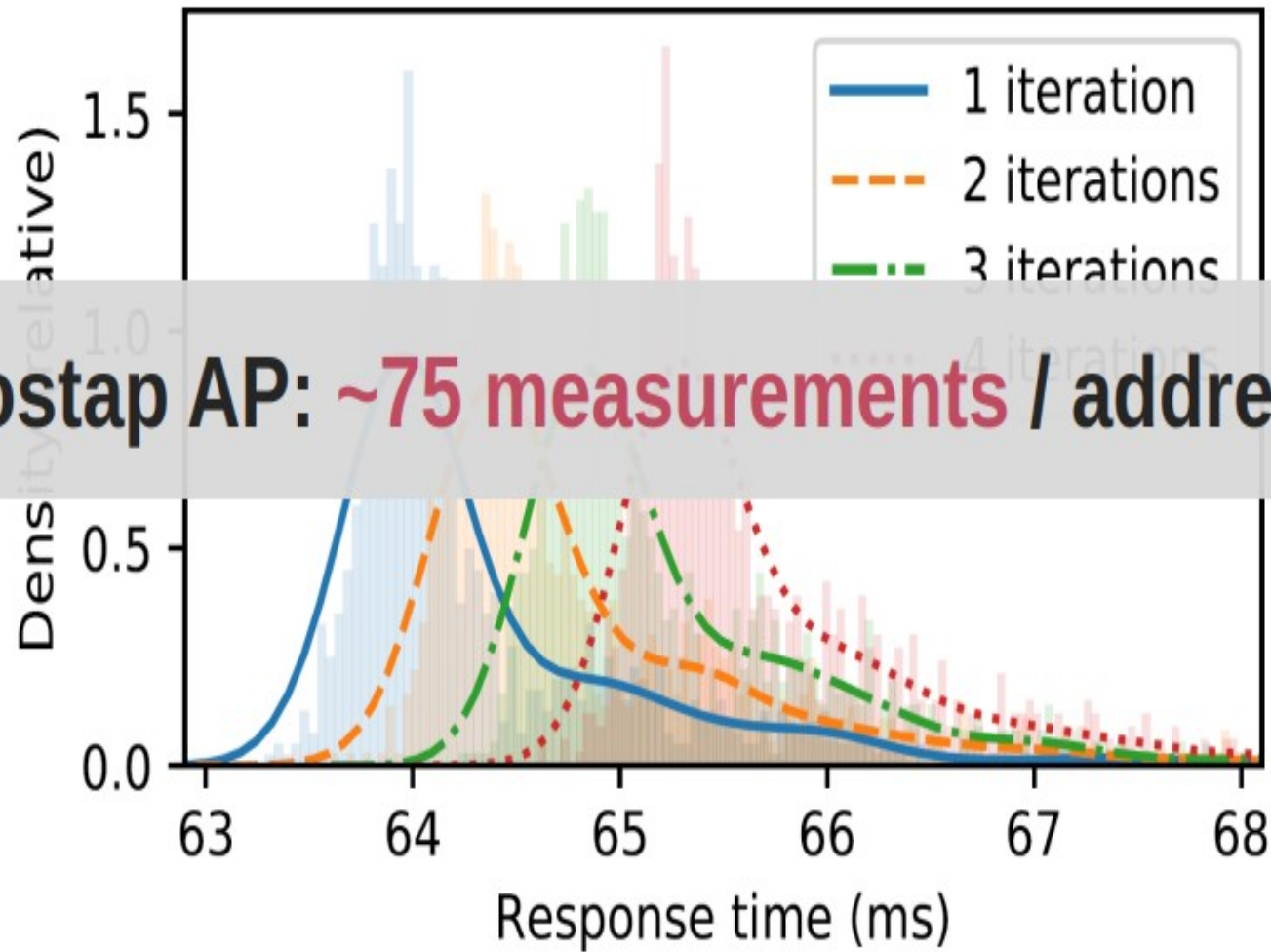
Leaked information: #iterations needed

Client address	addrA	addrB	addrC
Measured			

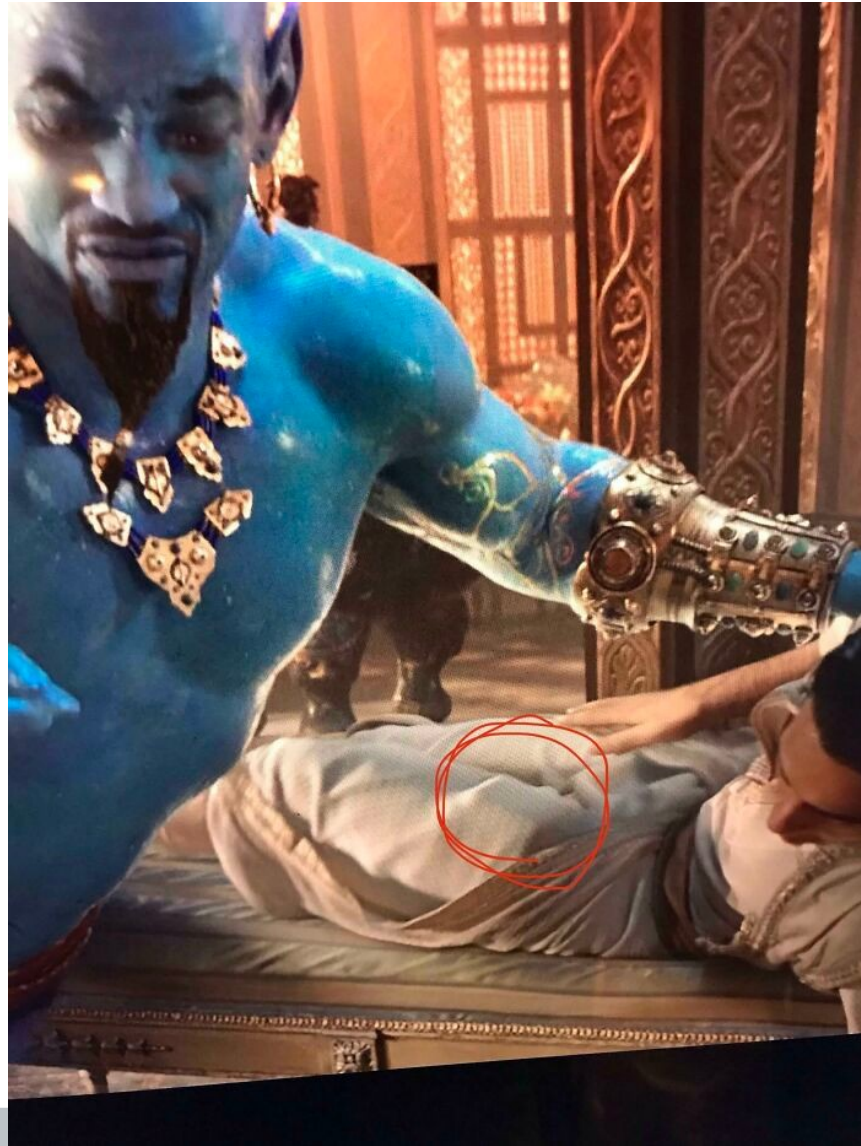
Forms a signature of the password

Need ~17 addresses to determine password in RockYou ($\sim 10^7$) dump

Raspberry Pi 1 B+: differences are measurable



Other applications of radio



3G (cracked?)

A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony

Orr Dunkelman, Nathan Keller, and Adi Shamir

Faculty of Mathematics and Computer Science

Weizmann Institute of Science

P.O. Box 26, Rehovot 76100, Israel

`{orr.dunkelman,nathan.keller,adi.shamir}@weizmann.ac.il`

4G LTE

Authentication in the clear

- User's identity and location are vulnerable, IMSI catchers
- Calls and messages, etc., after are not

Purely symmetric crypto

- No perfect forward secrecy

Not end-to-end

- Only protects between user and base station
- If you've ever visited a network, they have the key

Curve25519 (asymmetric), end-to-end, and other improvements

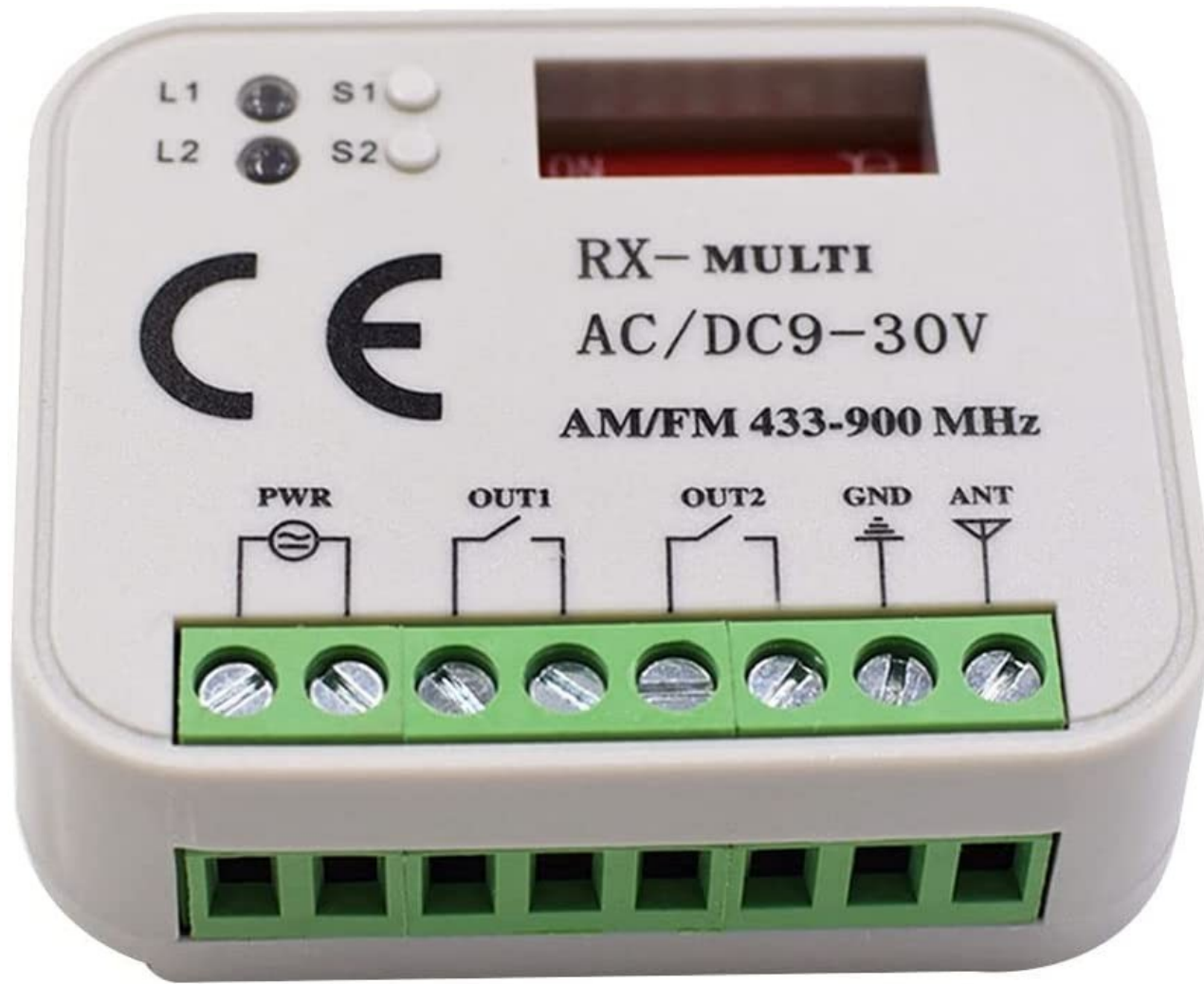
-<https://datatracker.ietf.org/meeting/113/materials/slides-113-hrpc-5g-security-privacy-and-surveillance-2022-update-00>

No perfect forward secrecy

IMSI catchers still an issue because of downgrade attacks and implementation issues?

-<https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-5G-IMSI-Catchers-Mirage.pdf>

UHF



Others

Bluetooth

Zigbee

- Physical frame injection

https://www.usenix.org/legacy/event/woot11/tech/final_files/Goodspeed.pdf

ANT+

- Garmin products

Zwave

- Smart homes

- Replay attacks, etc. (<https://github.com/CNK2100/VFuzz-public>)

<https://wigle.net/>

SDR fun

FM radio

GPS

L1: 1575.42 MHz

L2: 1227.6 MHz

L5: 1176.45 MHz

L6: 1278.75 MHz

WiFi, etc.

2.4 GHz, 5.18 GHz., etc.

IVAO

122.8 MHz

ADS-B

978 MHz and 1090 MHz

NOAA Weather

162.40 to 162.55 MHz

Wired networks

Ethernet

CAN bus

FPD-Link

SONET

ATM

PPP, tunnels, etc.