WiFi security and physical layer stuff

CSE 468 Fall 2023
jedimaestro@asu.edu

To prepare for this lecture

https://www.youtube.com/watch?v=fZ1R9RIiM1w

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

-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)

PRODUCTS ⌄ PAYLOADS ⌄ SHOWS

HAK5

COMMUNITY SUPPORT ⌄

HOME / ALL / WIFI PINEAPPLE

WIFI PINEAPPLE

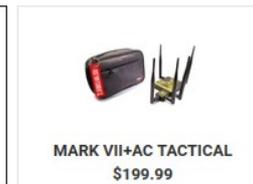### $119.99

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

WPA was only a stop gap

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

WPA3 is better?

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"
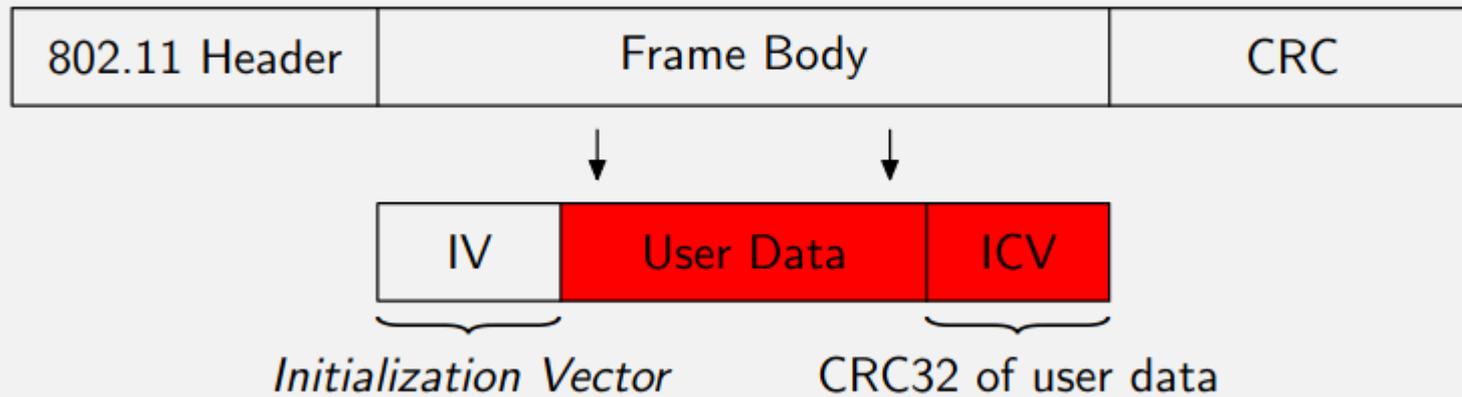
WEP encryption

"Wired Equivalent Privacy"

-Have to be physically in a building to plug in, have to know the passphrase to join WiFi (or do you?)
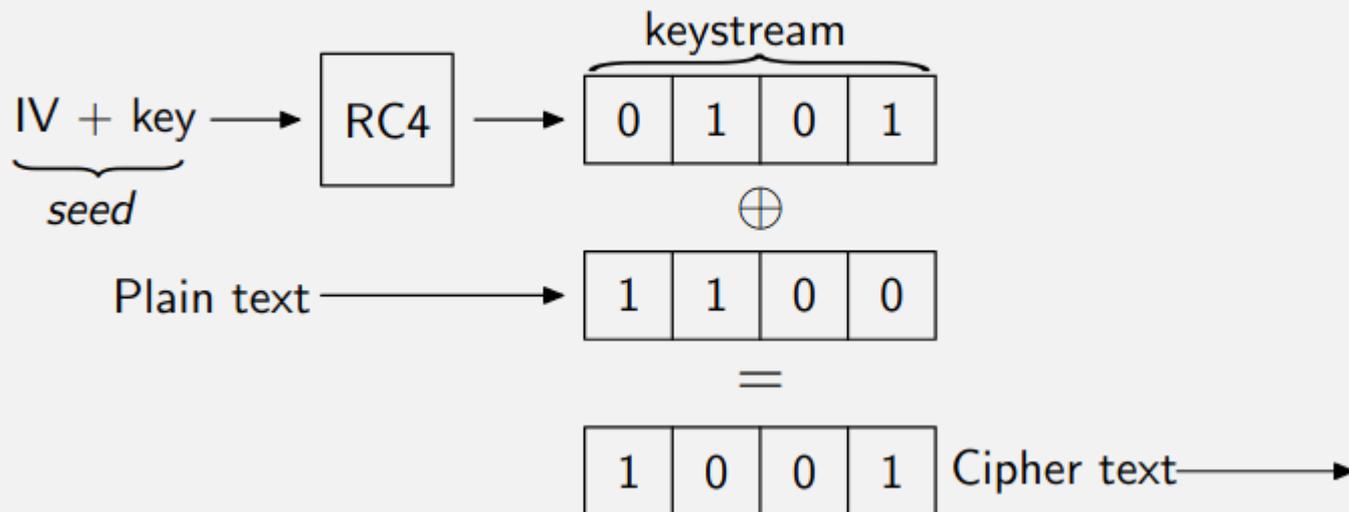
RC4, 40-bit key, 24-bit IV

Following are from:
https://jedcrandall.github.io/courses/cse468fall2022/wep/198fbe890b692e5296fcf7ad1b015e653ec9.pdf

Data frame format

802.11 Header	Frame Body	CRC

IV	User Data	ICV

Initialization Vector   CRC32 of user data

Encryption

keystream

$$IV + key \longrightarrow \boxed{RC4} \longrightarrow \boxed{0\ |\ 1\ |\ 0\ |\ 1}$$

seed

$\oplus$

Plain text $\longrightarrow$ | 1 | 1 | 0 | 0 |

$=$

| 1 | 0 | 0 | 1 | Cipher text $\longrightarrow$

If cipher-text & plain-text pair is known, their XOR is a keystream. Known plain-text (LLC/SNAP headers) in IP packets:

802.11 header	0xAA	0xAA	0x03	0x00	0x00	0x00	0x08	0x00

$\oplus$

802.11 header	Cipher-text

$=$

8 bytes of keystream

Can recover 8 bytes of keystream by eavesdropping a packet.

- Can encrypt (and transmit) 8 bytes of arbitrary data.

rc4-3.py

Possible to create statistical biases in the Key Scheduling Algorithm (KSA)

More info:

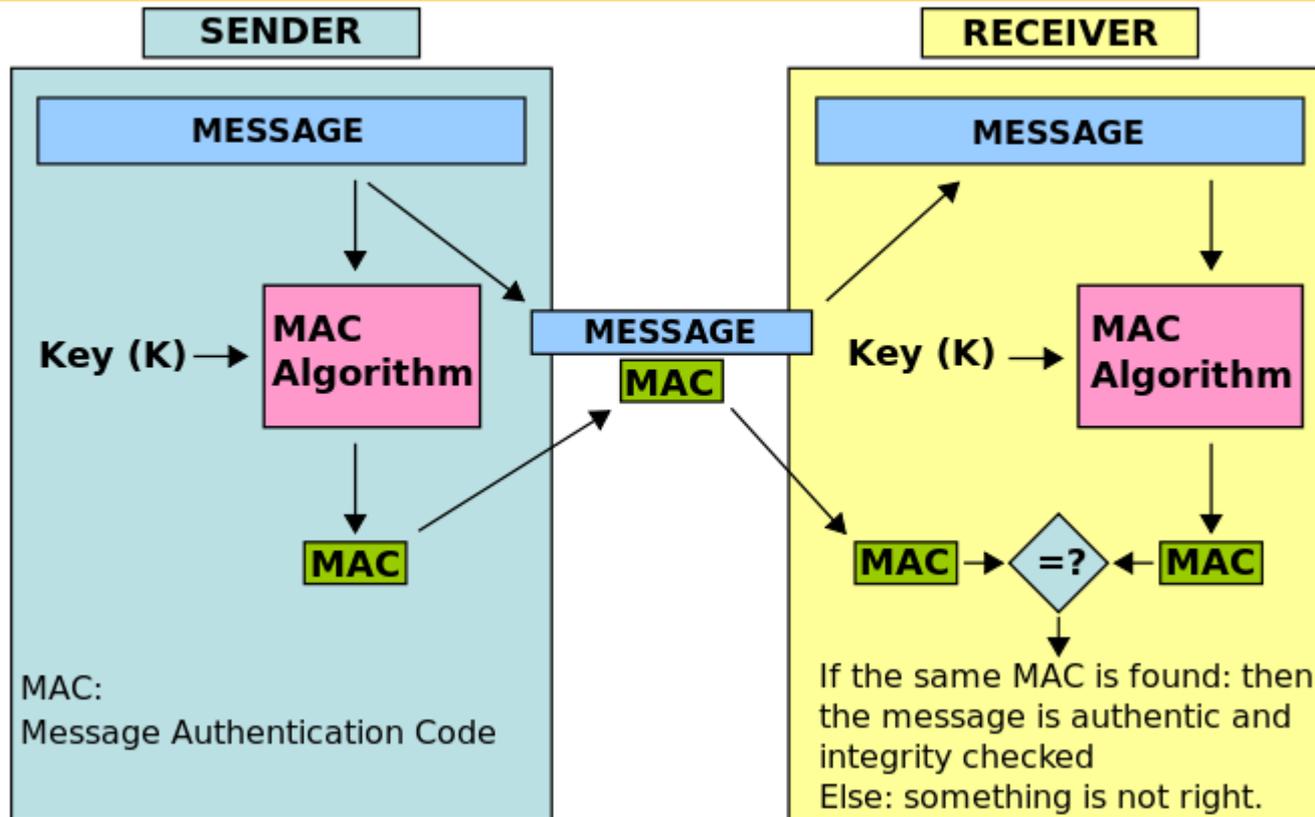https://www.youtube.com/watch?v=2o3Hs-JDWLs

WPA

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)
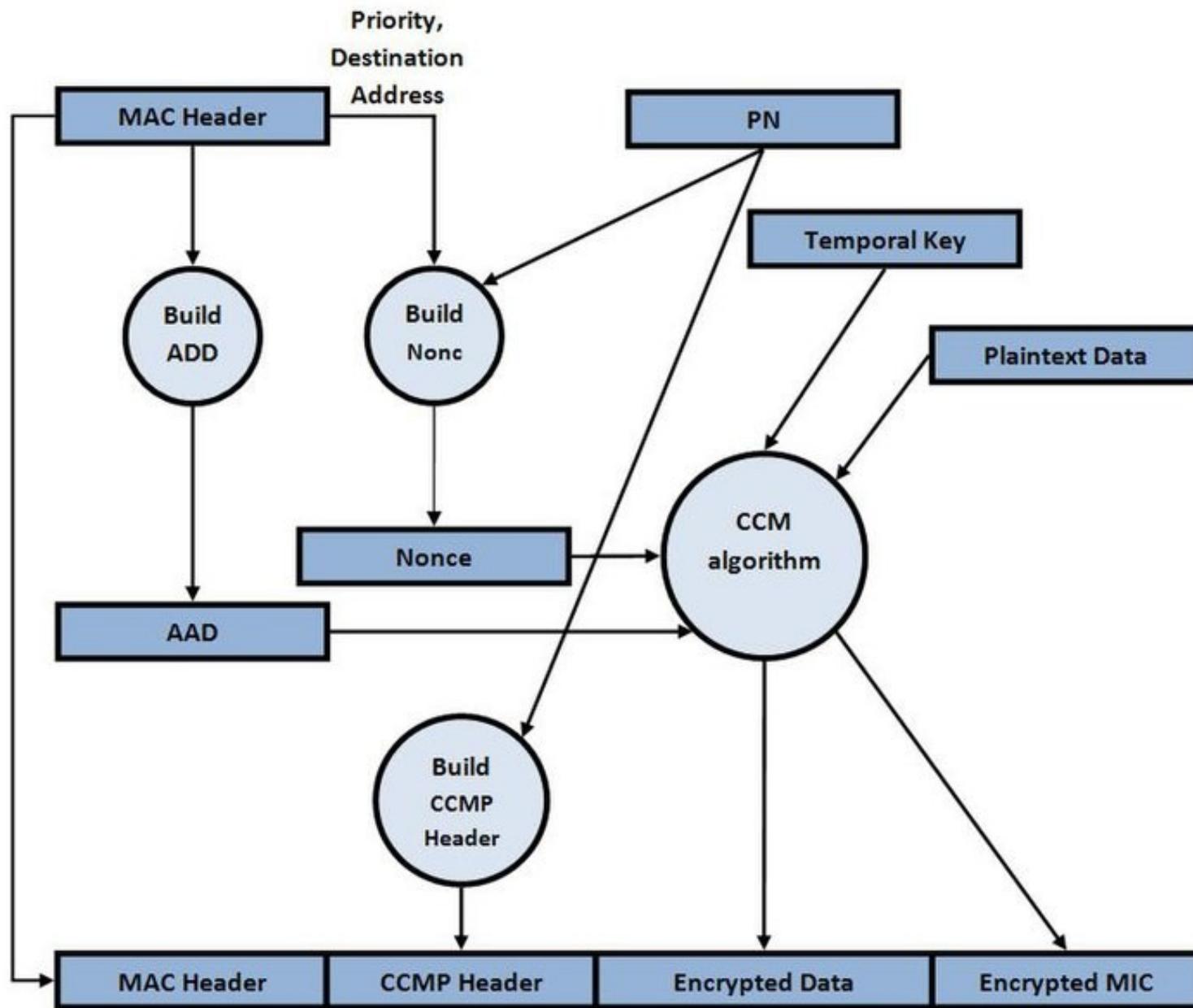
    -Same thing as a Message Authentication Code (MAC)

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)

https://en.wikipedia.org/wiki/File:CCMP_-_Encryption_and_Encapsulation.JPG

KRACK attacks

-https://www.krackattacks.com/

-https://blog.cryptographyengineering.com/2017/10/16/falling-through-the-kracks/

Crypto protocol and handshake

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
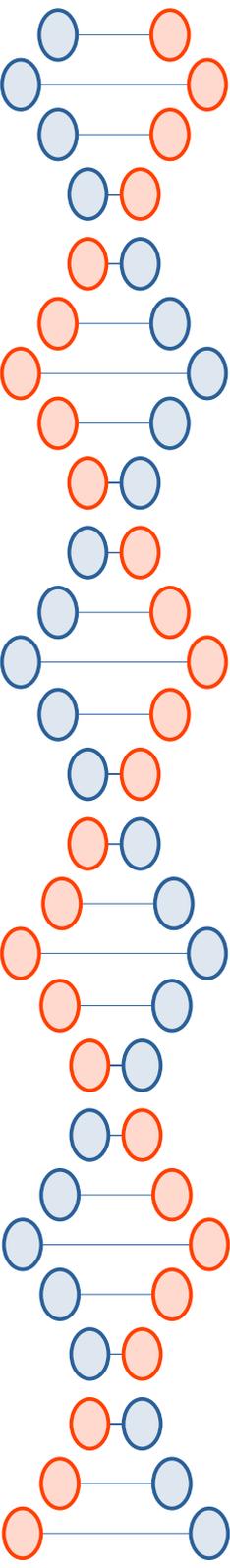
- Still vulnerable to KRACK

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/)
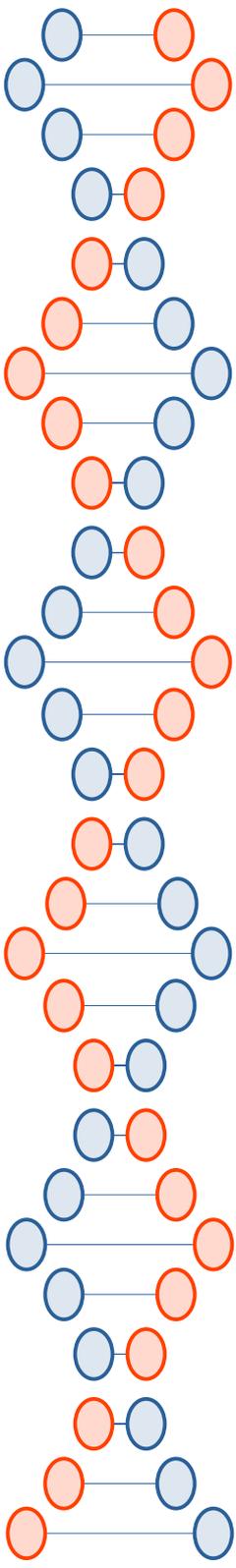
Dragonblood attacks (2019)

- 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

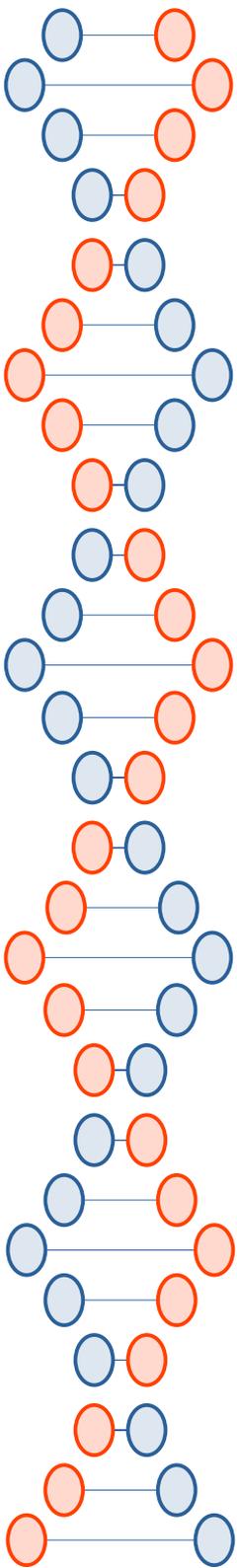# Convert password to MODP element

```
for (counter = 1; counter < 256; counter++)

    value = hash(pw, counter, addr1, addr2)

    if value >= p: continue

    P = value^((p-1)/q)

    return P
```

16
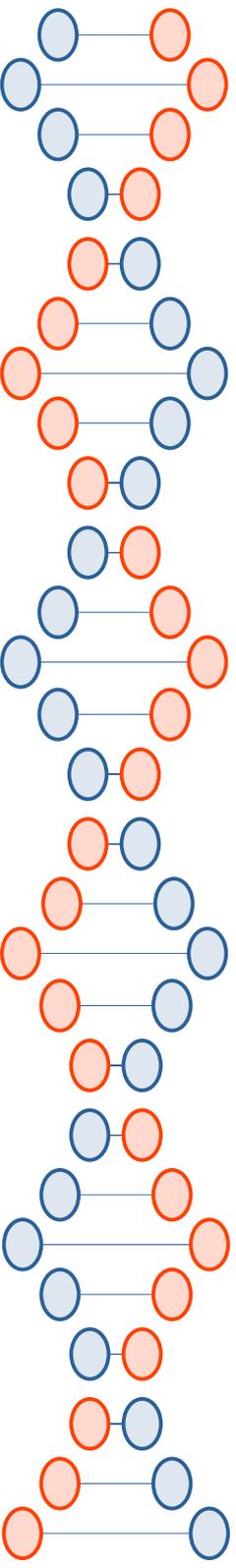
# Leaked information: #iterations needed

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

26

23

Leaked information: #iterations needed

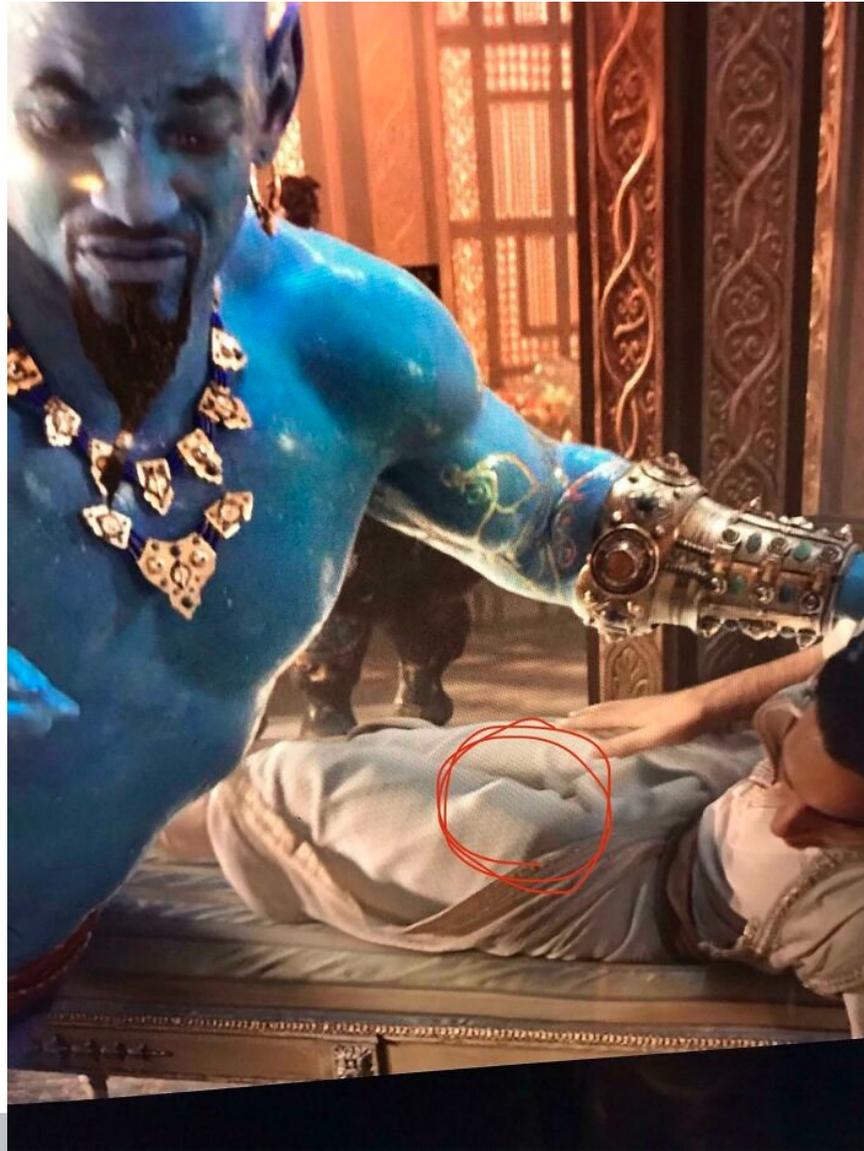| Client address	addrA	addrB	addrC
Measured			

Forms a signature of the password

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

28

Raspberry Pi 1 B+: differences are measurable

Hostap AP: ~75 measurements / address
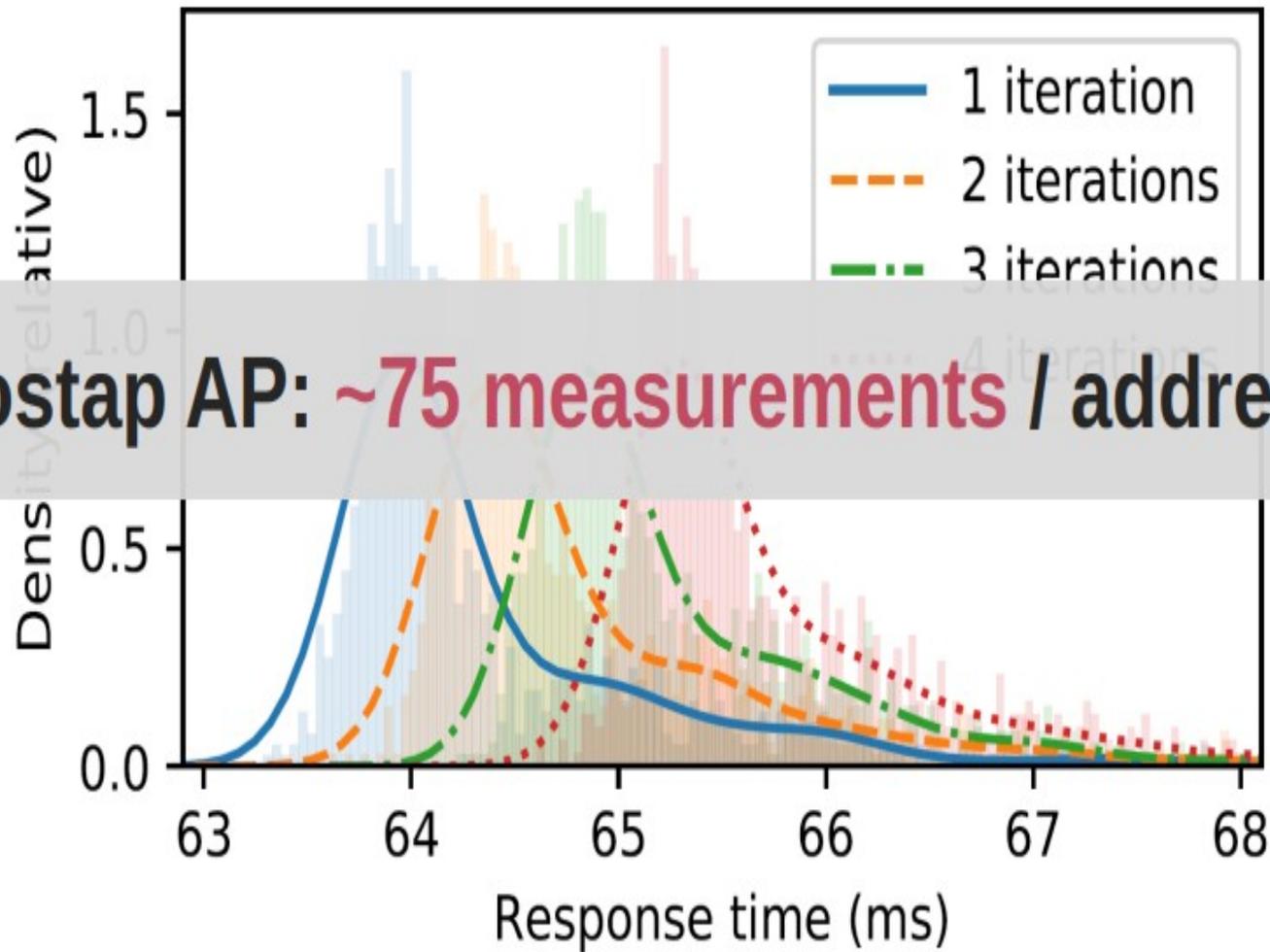
Other applications of radio

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

5G

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

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/

Wired networks

Ethernet

CAN bus

FPD-Link

SONET

ATM

PPP, tunnels, etc.