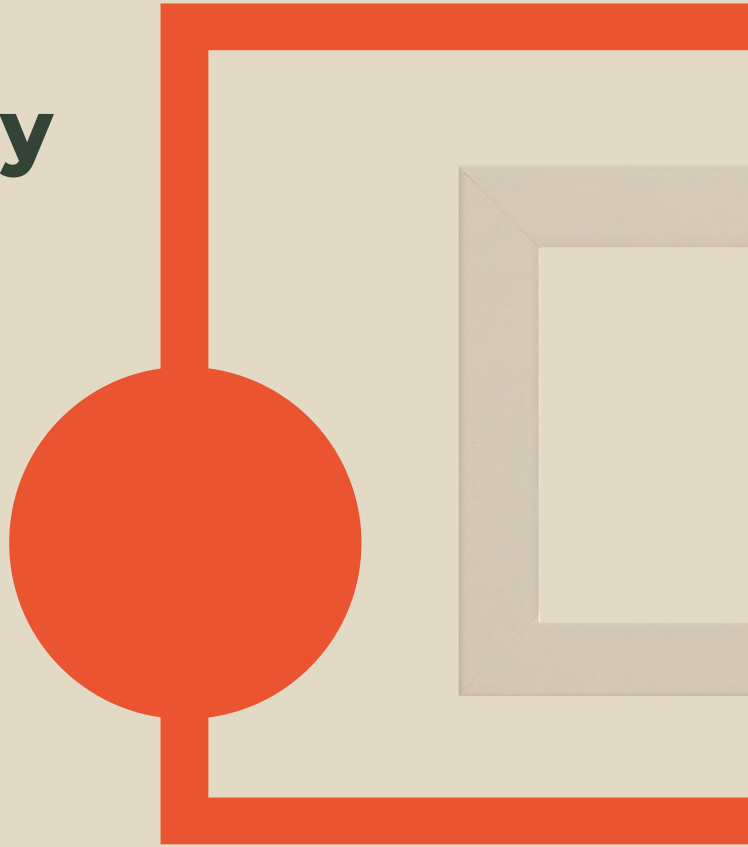
DP-3T: Ensuring Cryptographic Security & Privacy in COVID-19 Contact Tracing

Isha Agarwal & Minseo Kim

Mentor: Talia Blum



Overview

Section 1: DP-3T

Overview of how the algorithm works

Section 2: Security Analysis

Vulnerabilities and strengths of the algorithm

Section 3: Solutions

Proposed solutions to fix vulnerabilities

DP-3T

How the algorithm works

What's more important to you? Privacy or safety?

Students, drag the icon!

Definition of Contact Tracing

“Contact tracing is an effective disease control strategy that involves identifying cases and their contacts then working with them to interrupt disease transmission. This includes asking cases to isolate and contacts to quarantine at home voluntarily. Contact tracing is a key strategy to prevent the further spread of COVID-19.”

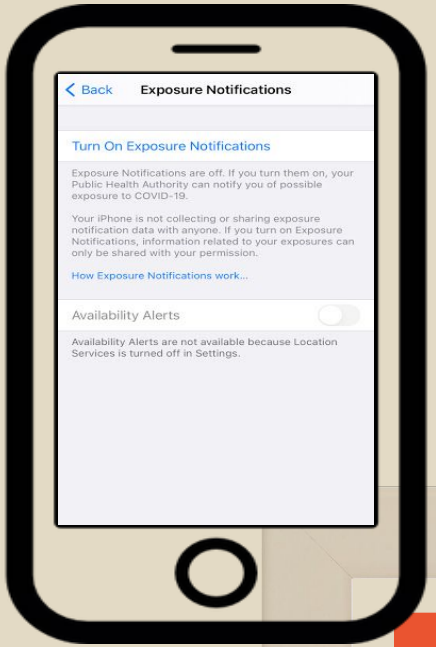
— The CDC

Problems With Contact Tracing

1. How to figure out everyone someone came into close contact with?
2. How do we preserve someone’s privacy when tracing close contacts?

What is DP-3T?

- Stands for *Decentralized Privacy-Preserving Proximity Tracing*
- Digital contact tracing protocol
- Protects privacy of users
- Available on your iPhone



Meet the Characters

Alex
Pronouns: They/Them

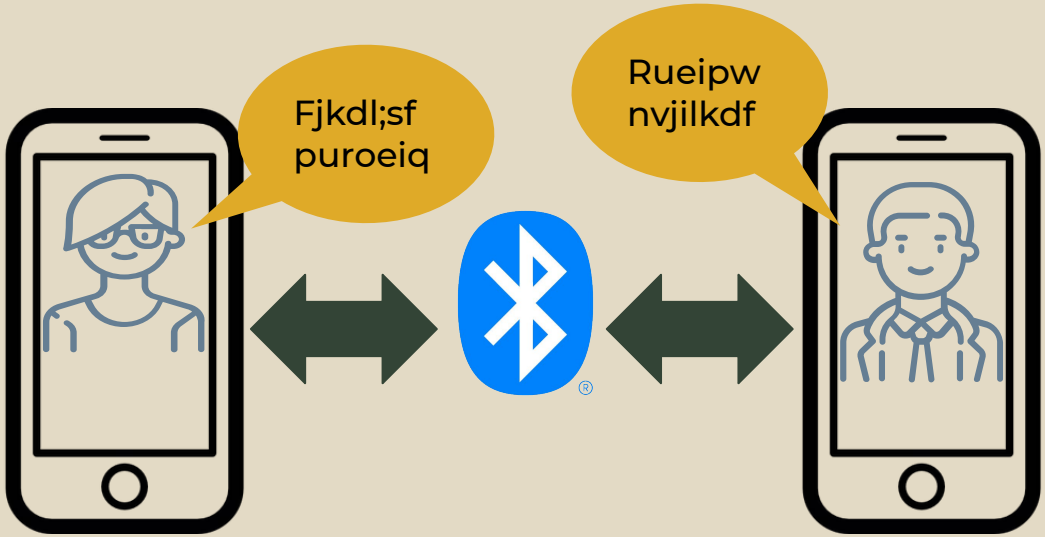
Bob
Pronouns: He/Him

Generating EphIDs Keys

- Alex and Bob's phone generate random keys, called *EphIDs*
- Phone broadcasts EphIDs throughout the day

Device Handshake

- Each phone *says* and *hears* random keys
- Phone stores all the EphIDs it hears and says



Reporting Infections

- Bob informs the app he tested positive for COVID-19
- Upload all codes that his phone “said” to the *hospital database*

Notifying Close Contacts

- Alex’s phone regularly checks the hospital database
- Finds Bob’s EphID
- Alerts Alex they are a close contact

Hospital Database
Rueipw
nvjilkdf
fjkweuip
fjkd;sjfkl

Codes Alex heard
fzxvvcx
Rueipw
mbvncx
nvjilkdf

Review time!

What is the correct order of the four stages of the DP-3T algorithm?

Students choose an option

Security Analysis

Advantages &
Potential Vulnerabilities of DP-3T

DP-3T Advantages

- Preserves user’s anonymity in the application
- Doesn’t track exact location
- Minimal work by user - automatic transparent Bluetooth processes

Problem Cases

Scenario #1: a user who is a close contact isn't notified

Scenario #2: a user who isn't a close contact is notified (false positive and diagnosis)

Scenario #3: an attacker is able to track a user by their EphIDs

Overview of Vulnerabilities

1

Backend Server

Hackers may upload unauthorized keys to or remove keys from the hospital database.

Eavesdropping

2

Easy for an attacker to intercept the connection and determine the “heard” and “said” EphID’s.

1

Backend Server

- Upload secret keys without authorization from the hospital server
- Self-reported process: one could lie and have their secret key uploaded
- Direct attack on the server

#1: Observation and upload

#2: Server security breach

#3: Server EphID’s data alteration

2

“Eve’s-dropping”

Bluetooth L0 (2014): 2^64 complexity

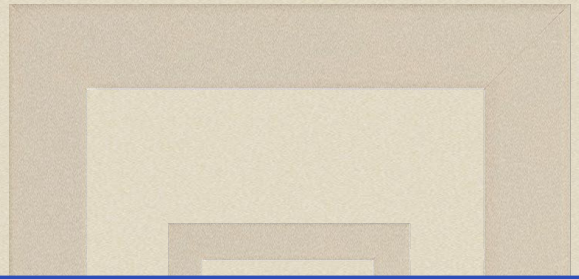
Bluetooth LE: Upgrade! However, still security concerns:

- Anyone can freely connect and exchange data, and listen in
- Man-To-Man (MTM) Attack

Eavesdropper Eve

Proposed Solutions

How can we solve these vulnerabilities?



OUR SOLUTIONS

HYBRID ENCRYPTION

AES-RSA hybrid encryption method instead of AES-CCM.

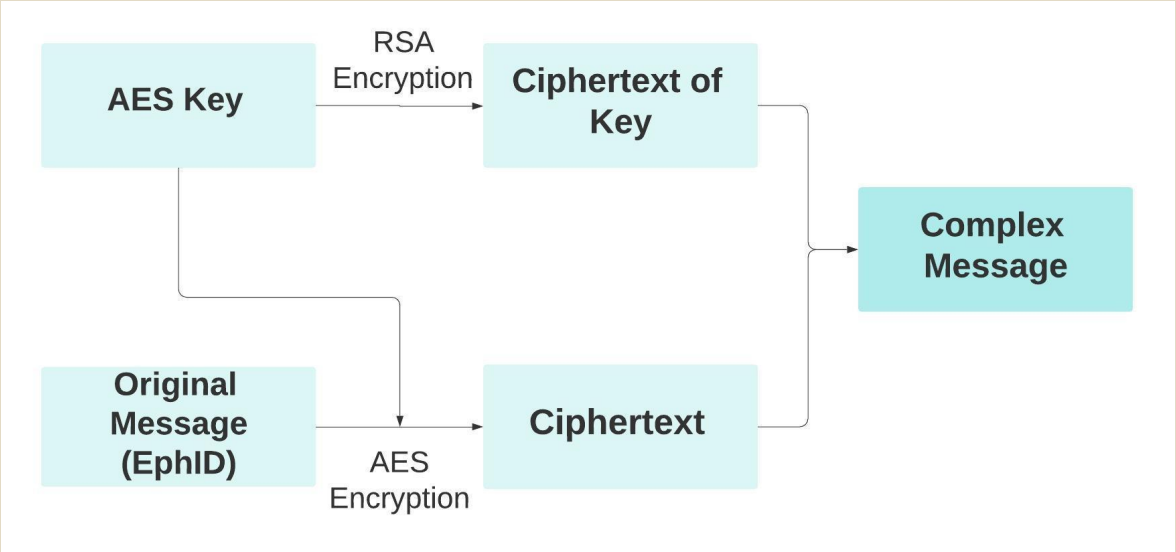
BB84

The first quantum cryptographic protocol developed. It acts as an effective verification mechanism to determine if hackers have tuned in or have altered data to create false diagnoses.

AES-RSA ENCRYPTION

AES-RSA Encryption

- Combine AES and RSA to encrypt bluetooth messages
- AES encrypts message
- RSA encrypts message key
- Send *complex message* = encrypted message + encrypted key

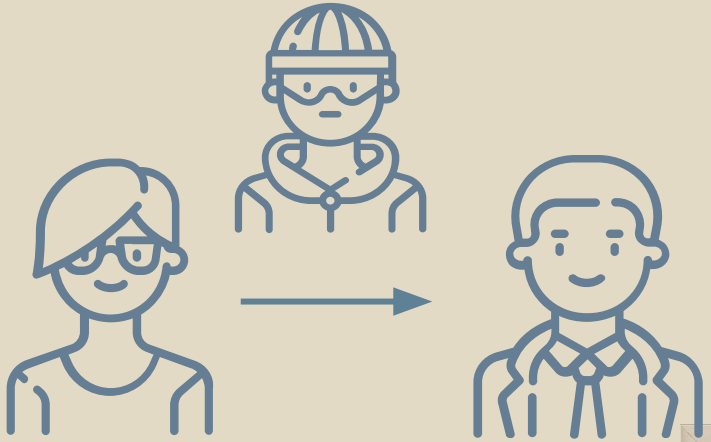


BACK TO THE FUTURE: BB84!

BB84—not BB8!

Alex wishes to send a private key, or in our case an EphID by Bluetooth, to Bob. They begin with two strings of bits: a and b, both n bits long.

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$$



BB84 Quantum Mechanics

Superposition: state of ambiguity where quantum bits (qubits) can be both 0 and 1 simultaneously

Entanglement: Two qubits become related; change to one affects the other

STATES

$$
\begin{aligned}
|\psi_{00}\rangle &= |0\rangle\,, \\
|\psi_{10}\rangle &= |1\rangle\,, \\
|\psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,, \\
|\psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\,.
\end{aligned}
$$

BB84 Result

Eavesdropper Eve is caught! BB84: Verification system

- Ensures secure connection
- No data manipulation, thus:
  - No false positives (“collisions”)
  - No Bluetooth connection interference
  - No wrong information

Would you enable the DP-3T algorithm on your phone after listening our presentation?

Students, drag the icon!

BIBLIOGRAPHIC REFERENCES

- “Contact Tracing – CDC’s Role and Approach.” *CDC*, CDC, 15 Jan. 2021, www.cdc.gov/coronavirus/2019-ncov/downloads/php/contact-tracing-CDC-role-and-approach.pdf.
- *Exposure Notification - Cryptography Specification*. Apple and Google, Apr. 2020, covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf?1.
- Rege, Komal, et al. *Bluetooth Communication Using Hybrid Encryption Algorithm Based on AES and RSA*. International Journal of Computer Applications, citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.8867&rep=rep1&type=pdf.
- Ronen, Eyal, et al. “IoT Goes Nuclear: Creating a ZigBee Chain Reaction.” *Eyal Ronen*, 21 Nov. 2018, eyalro.net/project/iotworm.html.
- Sanderson, Grant, director. *The DP-3T Algorithm for Contact Tracing (via Nicky Case)*. *YouTube*, YouTube, 14 May 2020, www.youtube.com/watch?v=D__UaR5MQao.
- Troncoso, Carmela, et al.. *Decentralized Privacy-Preserving Proximity Tracing*. 25 May 2020, github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.
- Wikipedia contributors. "BB84." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 3 Jan. 2021. Web.

Image credits

- “Collection of Warning Icons (52).” *Free Warning Icons, Download Free Warning Icons Png Images, Free ClipArts on Clipart Library*, clipart-library.com/warning-icons.html.
- “Contact Tracing.” *Delaware's Coronavirus Official Website*, 19 Jan. 2021, coronavirus.delaware.gov/contact-tracing/.
- “Download Free Phone Icons Transparent PNGs.” *Stick PNG*, Stick PNG, www.stickpng.com/cat/electronics/phone-icons?page=1.
- “Smartphone with Yellow Speech Bubble Icon Vector Image on VectorStock.” *VectorStock*, 20 Sept. 2016, www.vectorstock.com/royalty-free-vector/smartphone-with-yellow-speech-bubble-icon-vector-10712724.

THANKS!

Any questions?