

LINE-BREAK

Cryptanalysis and Reverse Engineering of Letter Sealing

Diego F. Aranha, Thomas Kingo T. Mogensen, Adam Blatchley Hansen

Computer Science @ Aarhus University, DK

linebreak.info

SECURE MESSAGING

Letter



Envelope



Signature / Signet Ring



Postal Service



Message

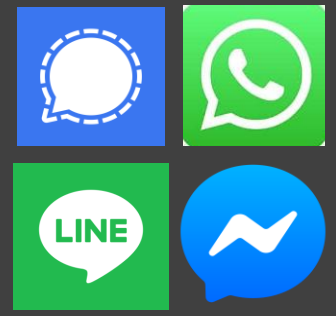


Encryption



Digital Signature





CRYPTOGRAPHY IN THE WILD

Idea formalized by Paterson & Albrecht, meaning:

- *"...to find examples of cryptography being used in standards, products or deployed systems.*
- *"...to analyse them by either finding vulnerabilities and reporting them or by building security models and proofs for the cryptographic cores of these systems"*

Applied to password managers, cloud storage, whistleblowing

Especially E2E messengers: Matrix, Threema, Telegram, Signal

HOW IT STARTED

RWC 2023

March 27-29 2023
Tokyo, Japan

E2EE policy in Japan - LINE

- LINE's E2EE protocol - "Letter Sealing"
  - Default E2EE on 1:1 and group text messaging (content + location data) since 2015
  - Default E2EE on 1:1 phone/ video calls since 2016
- Annual transparency reporting since 2017
- Strong public commitment to E2EE and transparency
  - Encryption report in English and Japanese
  - Encryption White Paper in English and Japanese
- Scandal in 2021 but enjoys public trust generally
  - A Chinese subsidiary was able to access contents of certain messages



HOW IT IS GOING



WHAT IS LINE?

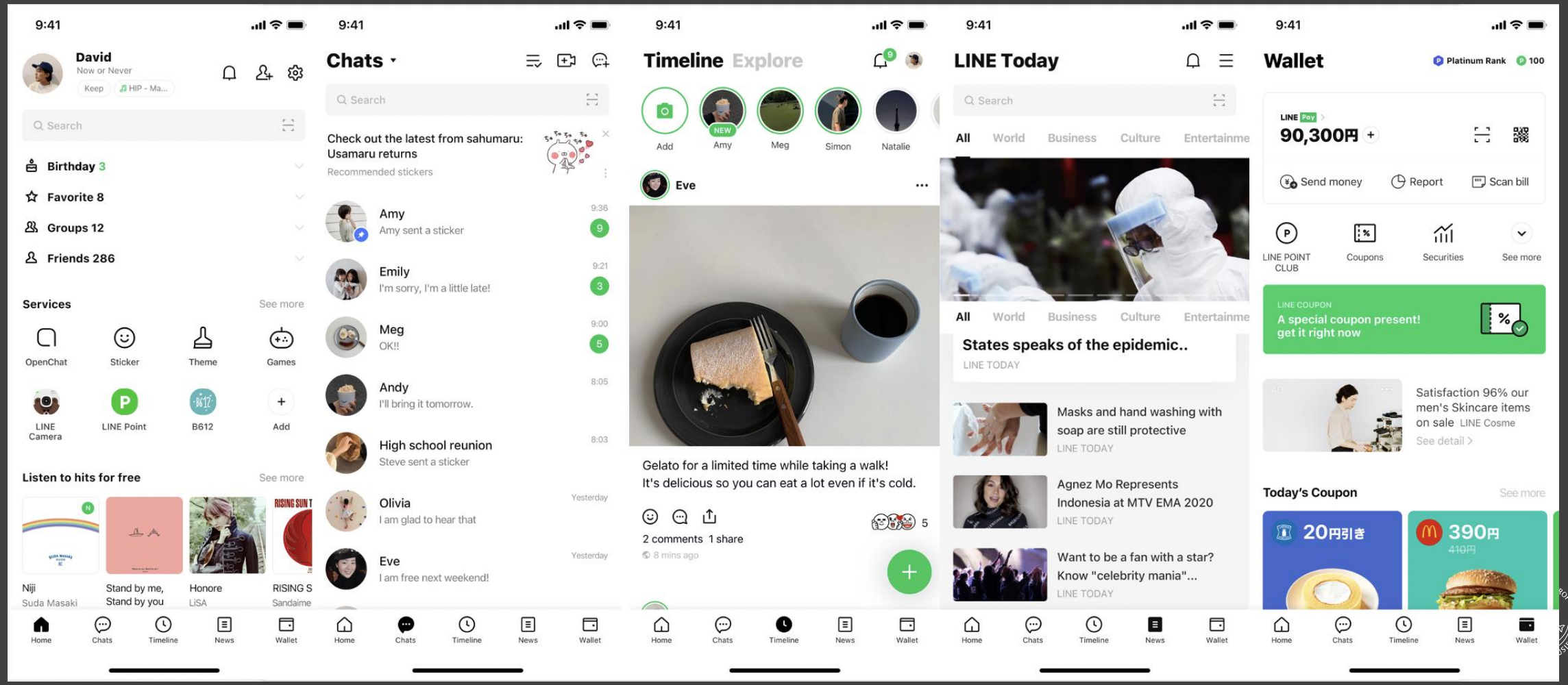
- *Super App*

- LY Corp. HQ in Japan *(Line-Yahoo)*

- 200M monthly users (1B, yearly):
  - Japan: 89M = 85% of pop.
  - Thailand: 51M
  - Taiwan: 21M = 90% of pop.
  - Indonesia: 13M

"*Letter Sealing implies all **end-to-end encrypted (E2EE)** protocols integrated in LINE's messaging [...] Although the first version of Letter Sealing encountered message data integrity issues, Letter Sealing v2 guarantees stronger protection over messages, **with all the issues resolved***"

WHAT IS LINE?


9:41
David
Now or Never
Search
Birthday 3
Favorite 8
Groups 12
Friends 286
Services
See more
OpenChat
Sticker
Theme
Games
LINE Camera
LINE Point
B612
Add
Listen to hits for free
See more
Niji
Suda Masaki
Stand by me, Stand by you
Honore
LiSA
RISING S
Sandaime
Home
Chats
Timeline
News
Wallet
Chats
Search
Check out the latest from sahumaru: Usamaru returns
Recommended stickers
Amy
Amy sent a sticker
9:36
Emily
I'm sorry, I'm a little late!
9:21
Meg
OK!!
9:00
Andy
I'll bring it tomorrow.
8:05
High school reunion
Steve sent a sticker
8:03
Olivia
I am glad to hear that
Yesterday
Eve
I am free next weekend!
Yesterday
Timeline
Explore
Add
Amy
Meg
Simon
Natalie
Eve
Gelato for a limited time while taking a walk!
It's delicious so you can eat a lot even if it's cold.
2 comments 1 share
8 mins ago
5
LINE Today
Search
All
World
Business
Culture
Entertainme
States speaks of the epidemic..
LINE TODAY
Masks and hand washing with soap are still protective
LINE TODAY
Agnez Mo Represents Indonesia at MTV EMA 2020
LINE TODAY
Want to be a fan with a star? Know "celebrity mania"...
LINE TODAY
Wallet
Platinum Rank
100
LINE Pay
90,300円
Send money
Report
Scan bill
LINE POINT CLUB
Coupons
Securities
See more
LINE COUPON
A special coupon present! get it right now
Satisfaction 96% our men's Skincare items on sale LINE Cosme
See detail
Today's Coupon
See more
20円引き
390円
410円

LETTER SEALING V1 X V2



	Version 1	Version 2
Key exchange algorithm	ECDH over Curve25519[5]	
Message encryption algorithm	AES256-CBC	AES256-GCM[6]
Message hash function	SHA-256	N/A
Data authentication	AES-ECB with SHA-256 MAC	AES256-GCM
Message data	Encryption and integrity	
Message metadata	Not protected	Integrity

WHERE IS LS APPLIED?

Message/media type	2015	2016	2017/9	2018/4	2019/10	2020/9	2021/9	2022/8	2024/12
Text	○	○ → ◎	◎	◎	◎	◎	◎	◎	◎
Location	○	○ → ◎	◎	◎	◎	◎	◎	◎	◎
Stickers *2	△	△	○	○	○	○	○	○	○
Image files *3	△	△	○	○	○	○	○	○	◎*5
Voice messages *4	x	x	○	○	○	○	○	○	◎
Video files *4	x	x	○	○	○	○	○	○	◎*5
Other files *3	△	△	○	○	○	○	○	○	◎
Message reaction	n/a	n/a	n/a	n/a	n/a	n/a	○	○	○

Legend: ◎ Letter Sealing (end-to-end encryption) / ○ Transport-level encryption / △ Partially protected / x Not encrypted or not sufficiently encrypted

LETTER SEALING V2

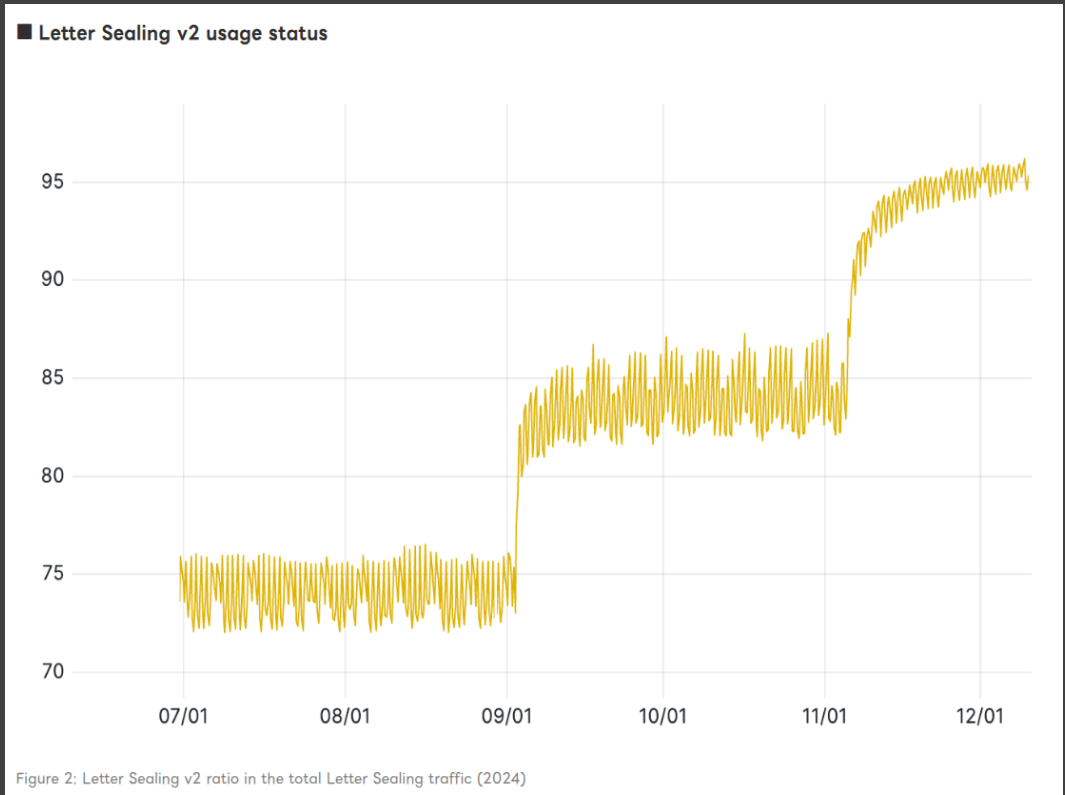
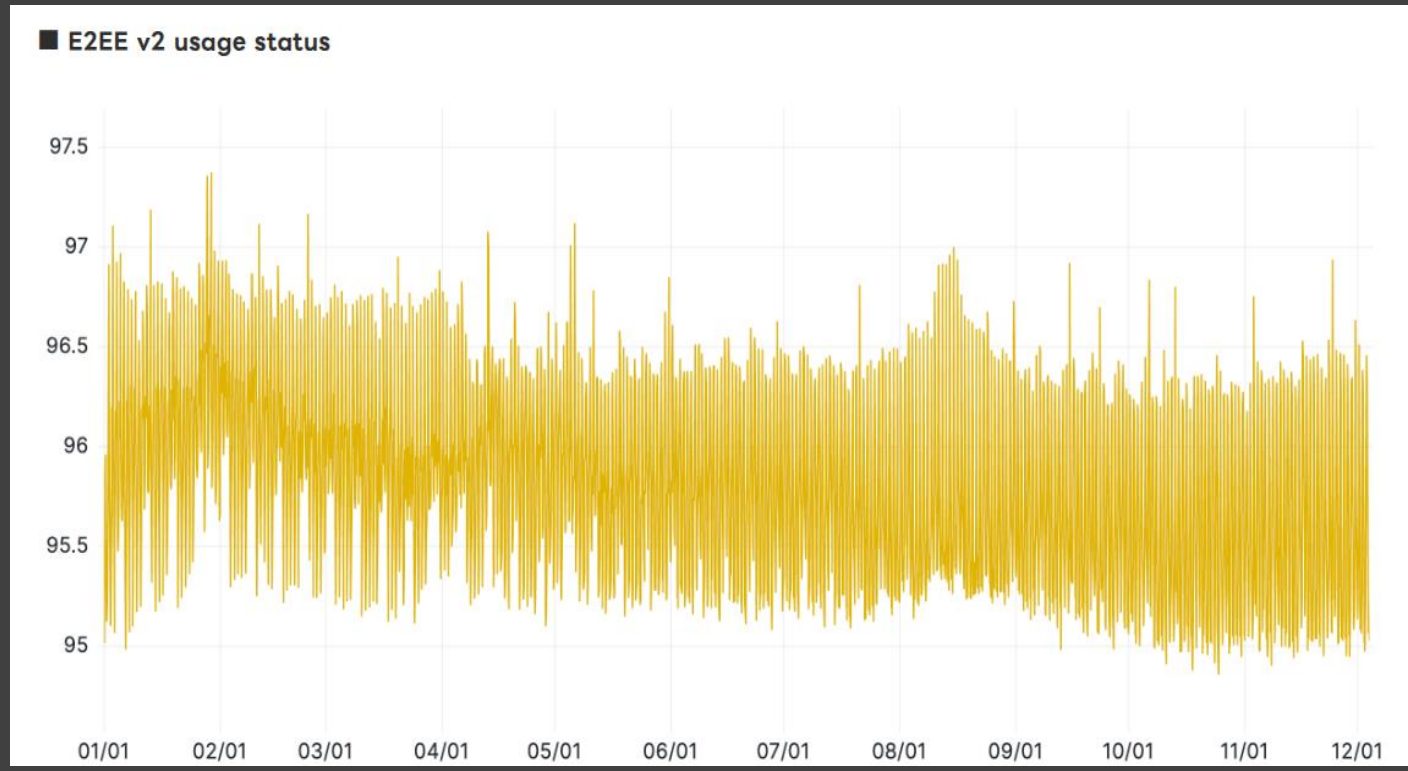


Figure 2: Letter Sealing v2 ratio in the total Letter Sealing traffic (2024)



PRESENTATION OVERVIEW



End-to-End Encryption



Protocol + Implementation



The Fun! + demos

WHAT IS E2EE?

No clear **consensus** definition.



Confidentiality



Integrity

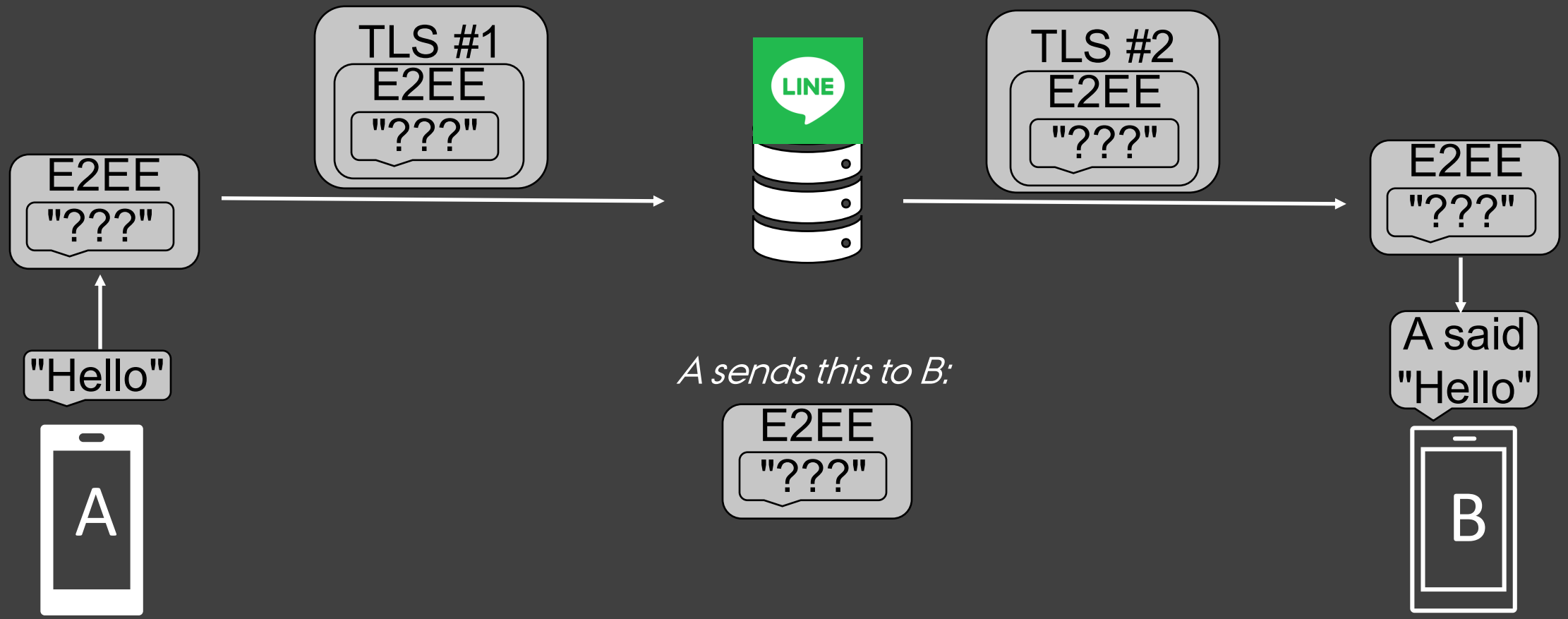


Authentication

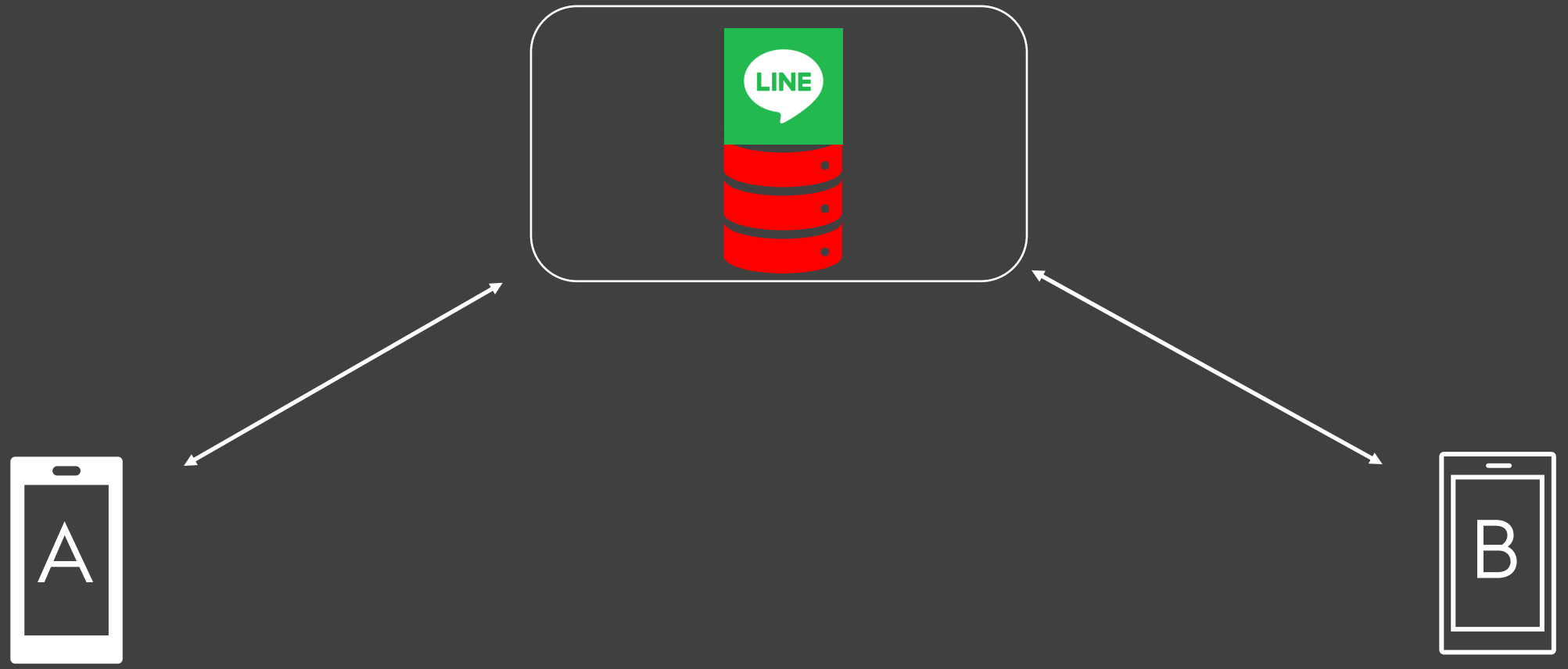


Forward Secrecy

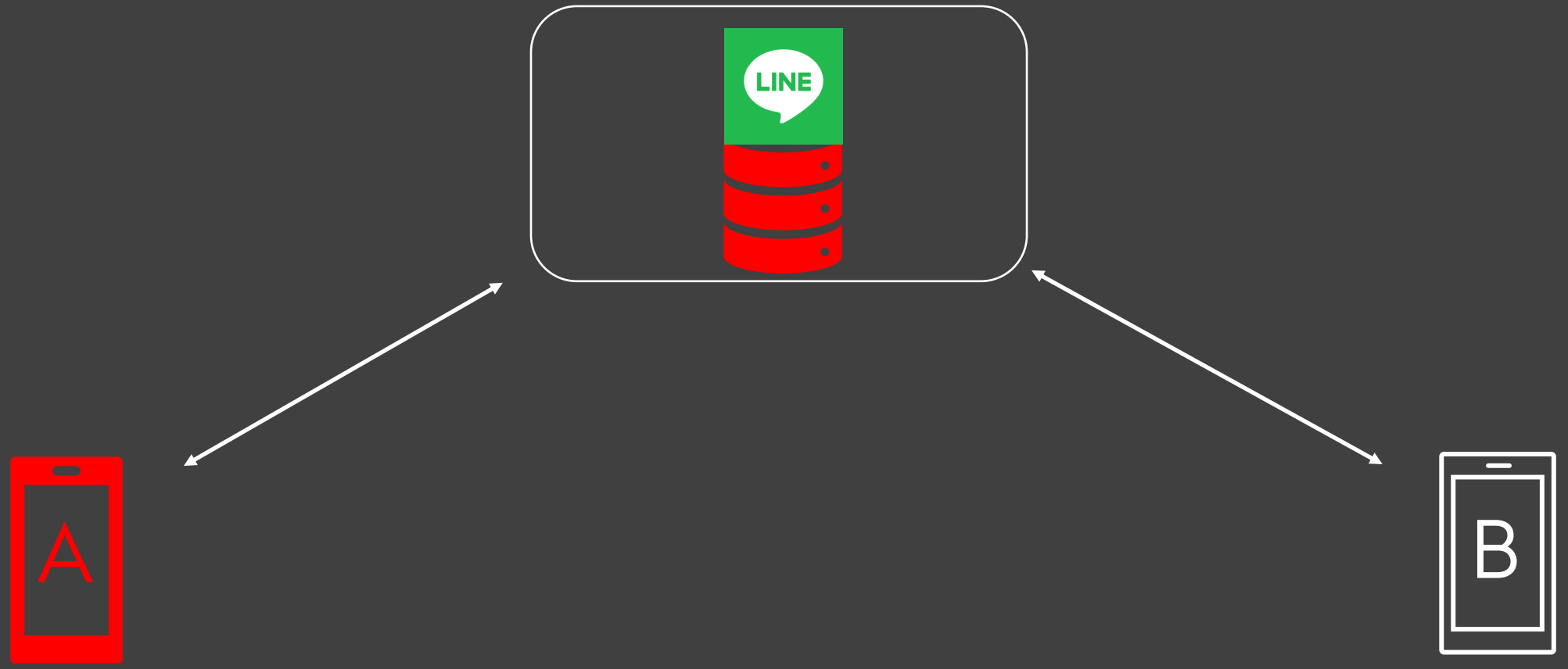
TLS + E2EE


TLS #1
E2EE
"???"
E2EE
"???"
"Hello"
A
LINE
TLS #2
E2EE
"???"
E2EE
"???"
A said
"Hello"
B
A sends this to B:
E2EE
"???"

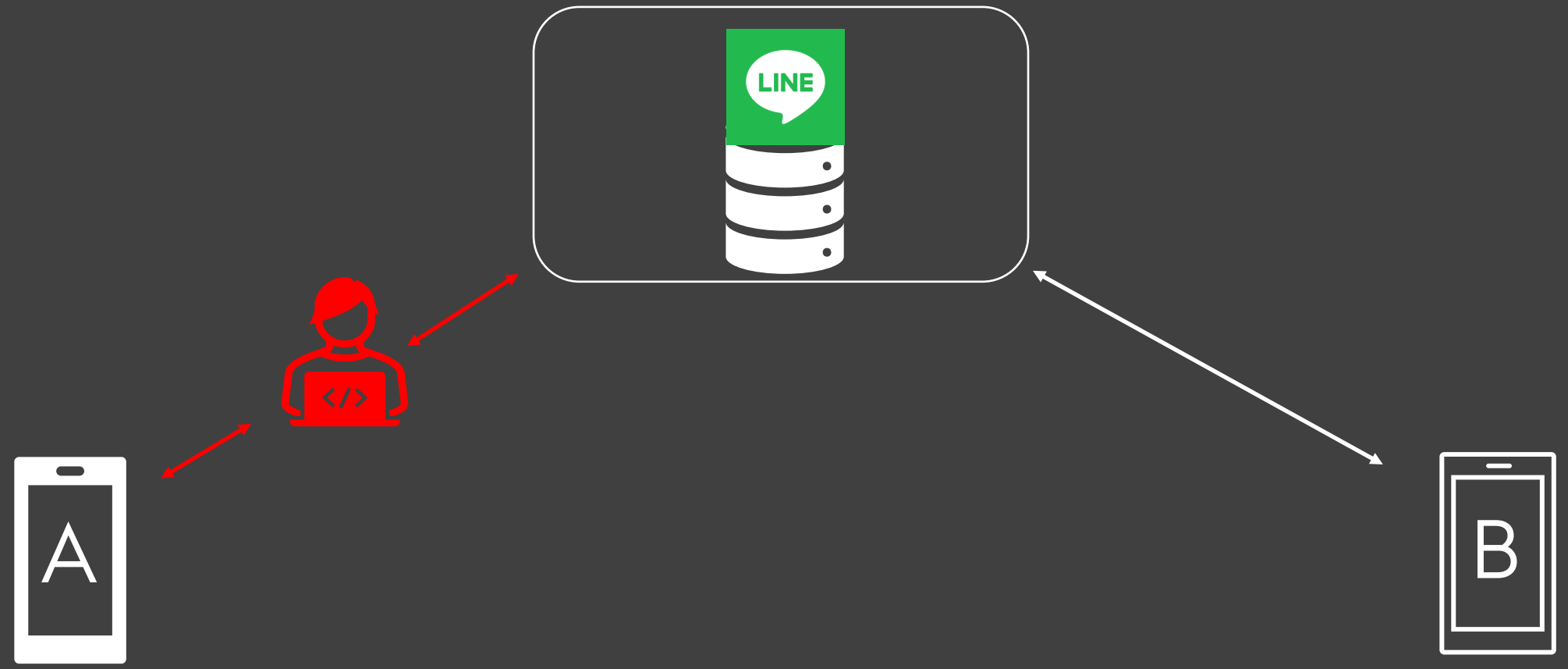
THREAT MODELS: MALICIOUS SERVER (E2EE ADVERSARY)



THREAT MODELS: MALICIOUS SERVER + USER



THREAT MODELS: MACHINE-IN-THE-MIDDLE (MITM)



PRESENTATION OVERVIEW



End-to-End Encryption

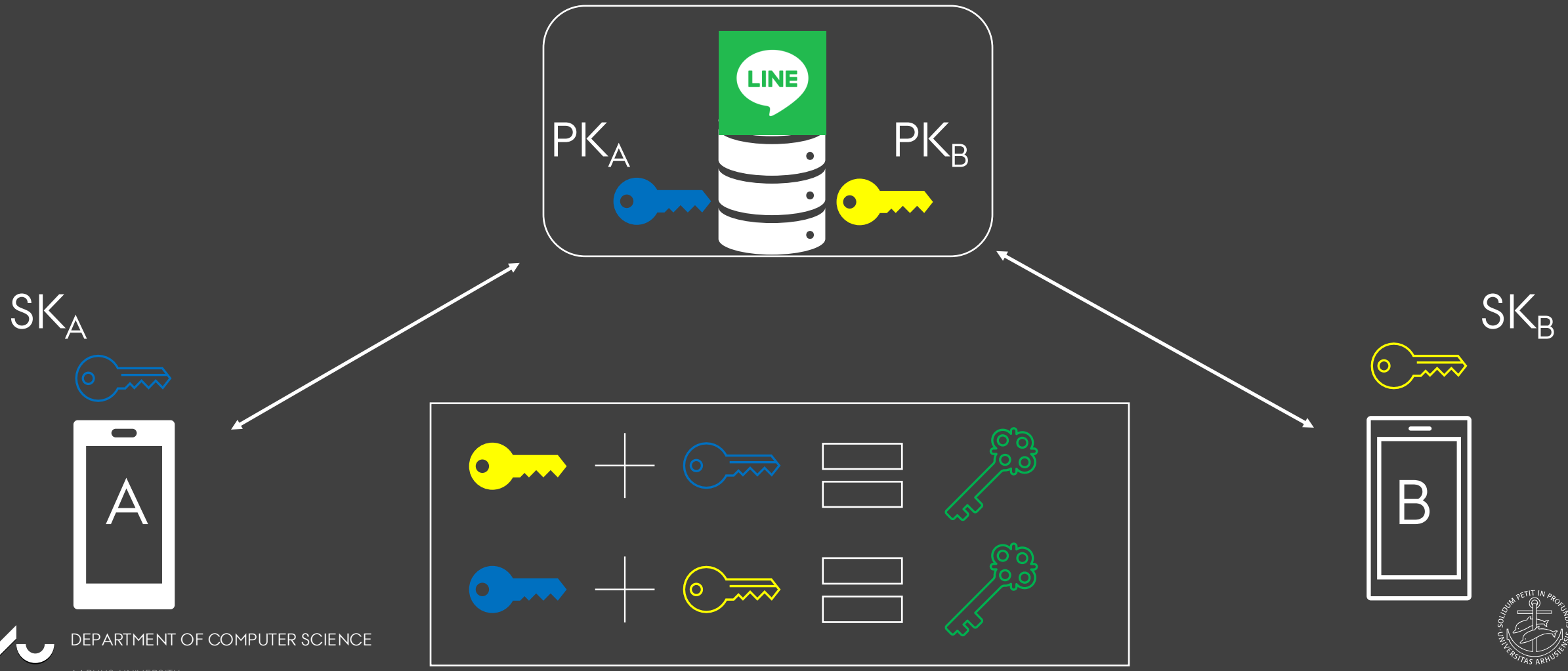


Protocol + Implementation

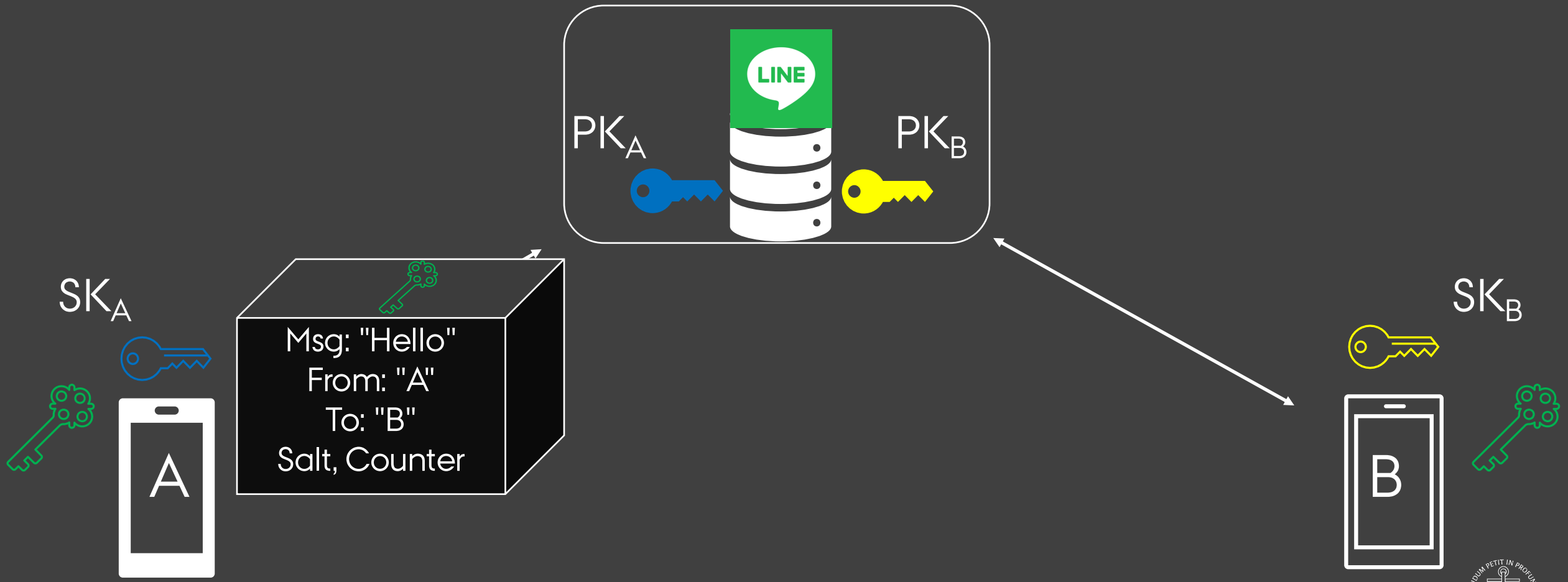


The Fun! + demos

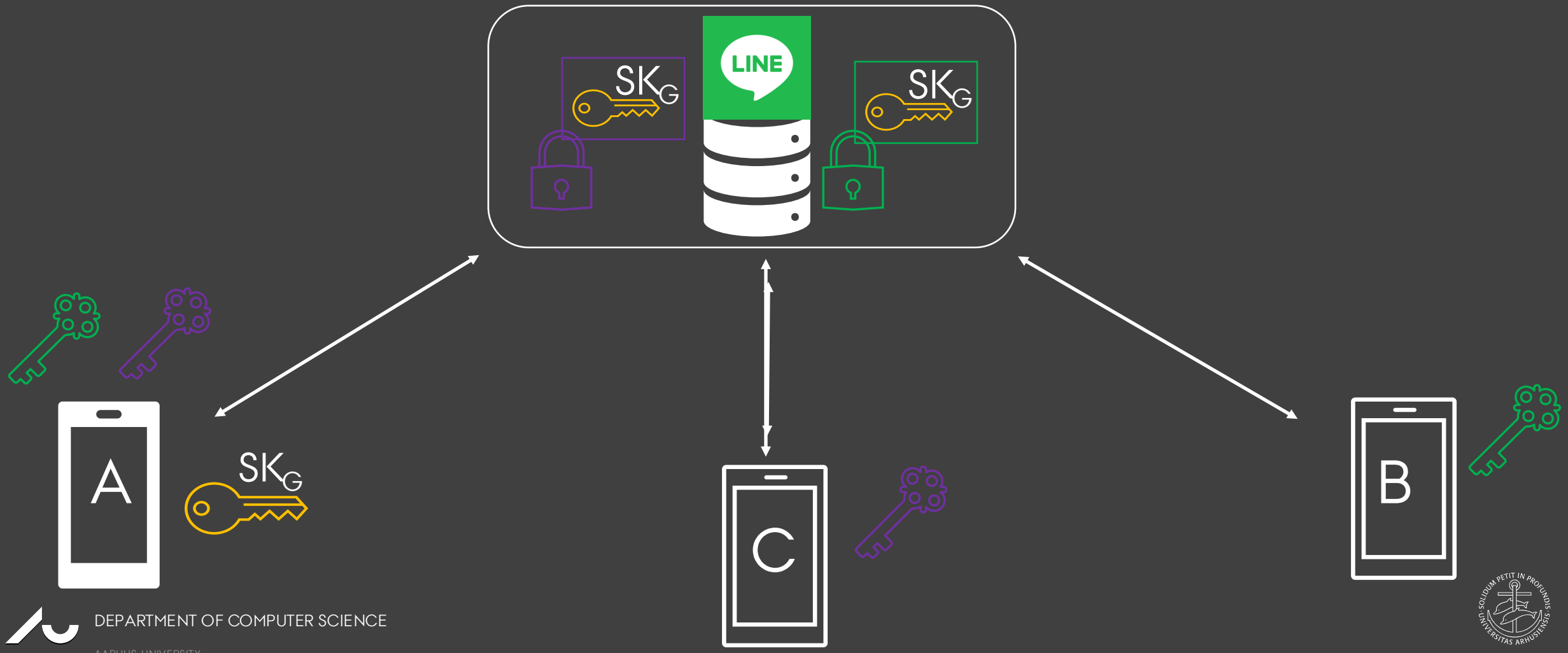
ONE-TO-ONE CHATS: KEY GENERATION



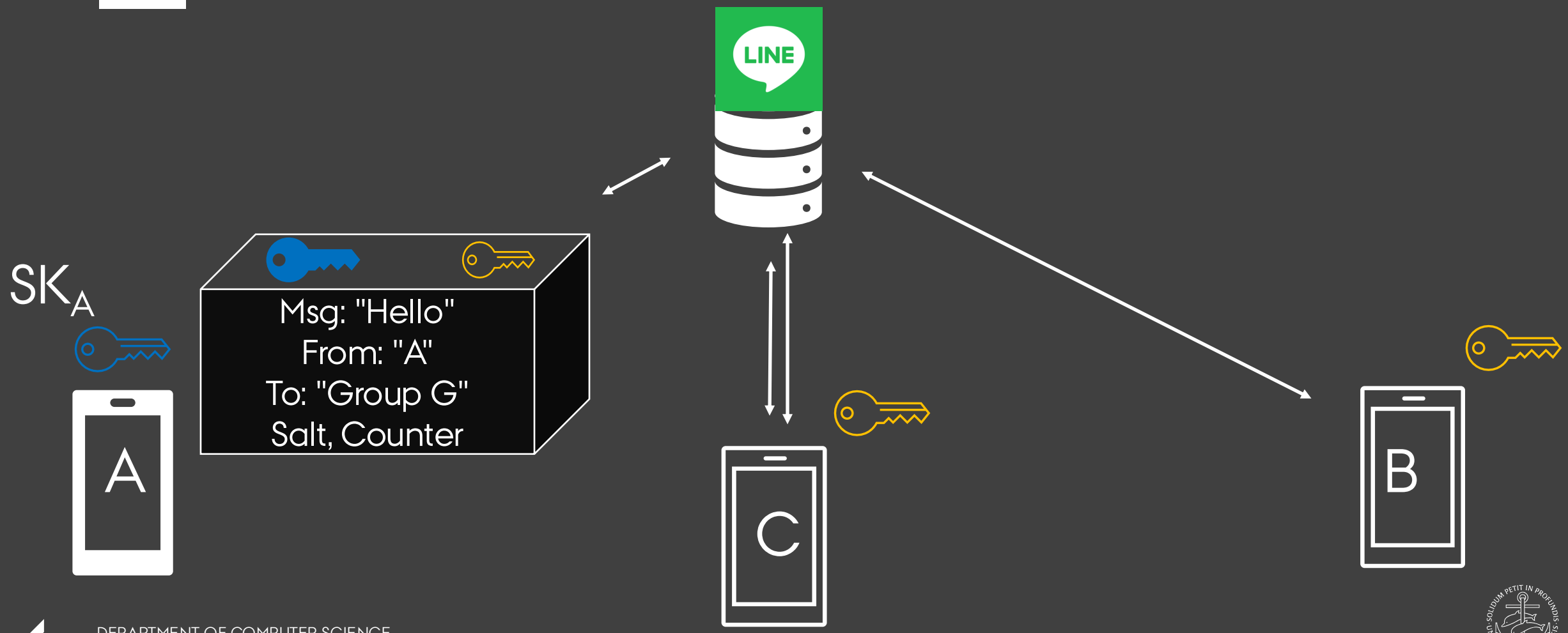
ONE-TO-ONE CHATS: ENCRYPTION



GROUP CHATS: KEY GENERATION



GROUP CHATS: ENCRYPTION



ENCRYPTION IN LSV2

- One-to-one chats:

$$Secret = ECDH(pk_{U_j}, sk_{U_i}) = ECDH(pk_{U_i}, sk_{U_j})$$
$$salt = randombytes(16)$$
$$key = SHA256(Secret||salt||"Key")$$
$$nonce(12) = counter[8]||randombytes(4)$$
$$AAD = recipID||senderID||senderKeyID||recipKeyID||version||type$$
$$(C, tag) = AES_{GCM}(key, nonce, M, AAD)$$
$$Msg = version||type||salt||C||tag||nonce||senderKeyID||recipKeyID$$

*Key Material generated **ONCE***

- Group chats:

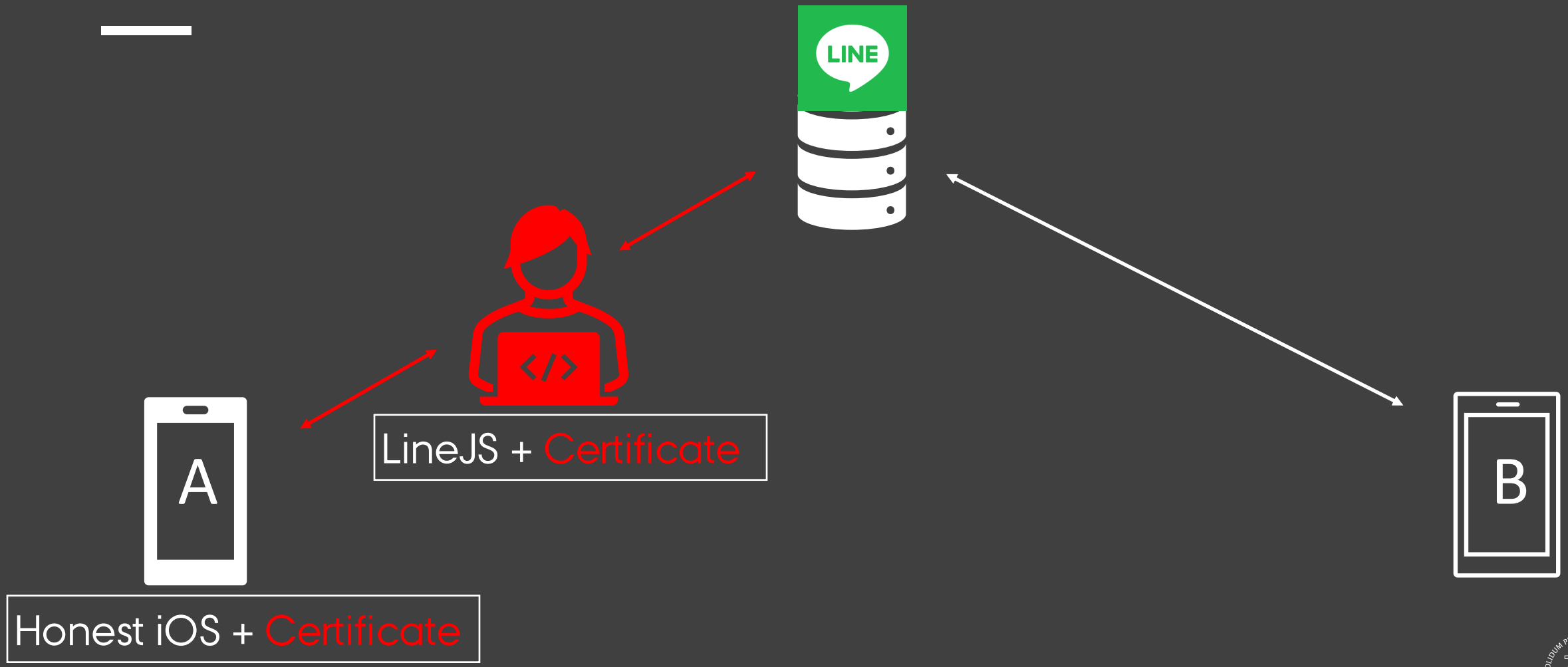
$$Secret = ECDH(sk_g, pk_{U_i})$$
$$salt = randombytes(16)$$
$$key = SHA256(Secret||salt||''Key'')$$
$$nonce(12) = counter[8]||randombytes(4)$$
$$AAD = groupID||senderID||senderKeyID||groupKeyID||version||type$$
$$(C, tag) = AES_{GCM}(key, nonce, M, AAD)$$
$$Msg = version||type||salt||C||tag||nonce||senderKeyID||groupKeyID$$

*Group Key regenerated at **UPDATE***

OVERVIEW OF FINDINGS

Target	Attack	Threat Model
All chats	Replay, reorder, blocking	E2E or MitM attacker
	Impersonation	Malicious user with E2E/MitM
	Plaintext leakage (stickers + URLs)	E2E or MitM attacker

EXPERIMENTAL SETUP



PRESENTATION OVERVIEW



End-to-End Encryption



Protocol + Implementation



The Fun! + demos

REPLAY ATTACKS

Protocol is **stateless** (counters are not synchronized or checked).

```
{
  reqSeq: SenderChatCounter,
  message: {
      to: BobID,
      contentMetadata: { e2eeVersion: "2" },
      contentType = 'NONE'
      chunks: [
        <salt>,
        <C || tag>,
        <nonce = 8-byte reqSeq || 4-byte random>,
        <AliceKeyID>,
        <BobKeyID>
      ],
}
```

In message from Alice to Bob, counters initially match.

Server **adds its own counters**, which can be tampered with by MitM attacker.

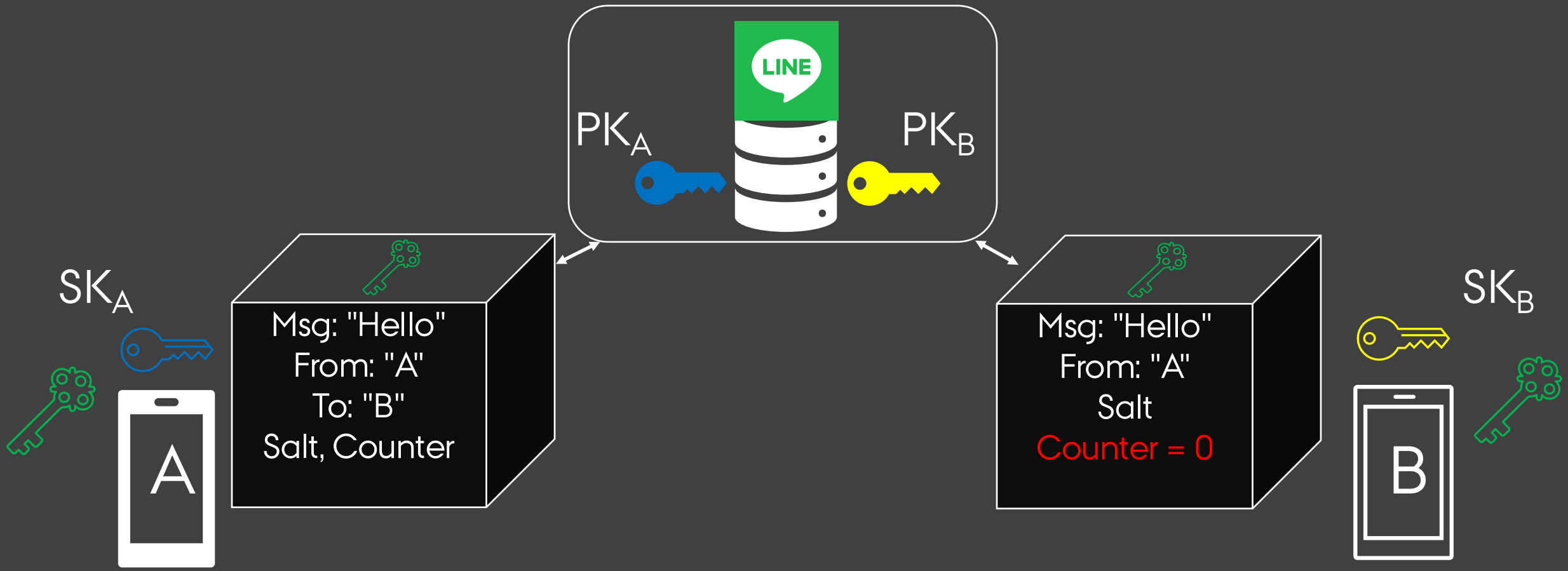
```
{
  revision: 58,
  createdTime: 1744114826322,
  type: "SEND_MESSAGE",
  reqSeq: -1,
  message: {
    from: AliceID,
    id: "5558015208524353O6",
    createdTime: 1744114826320,
  },
}
```

Changed by server without problem.

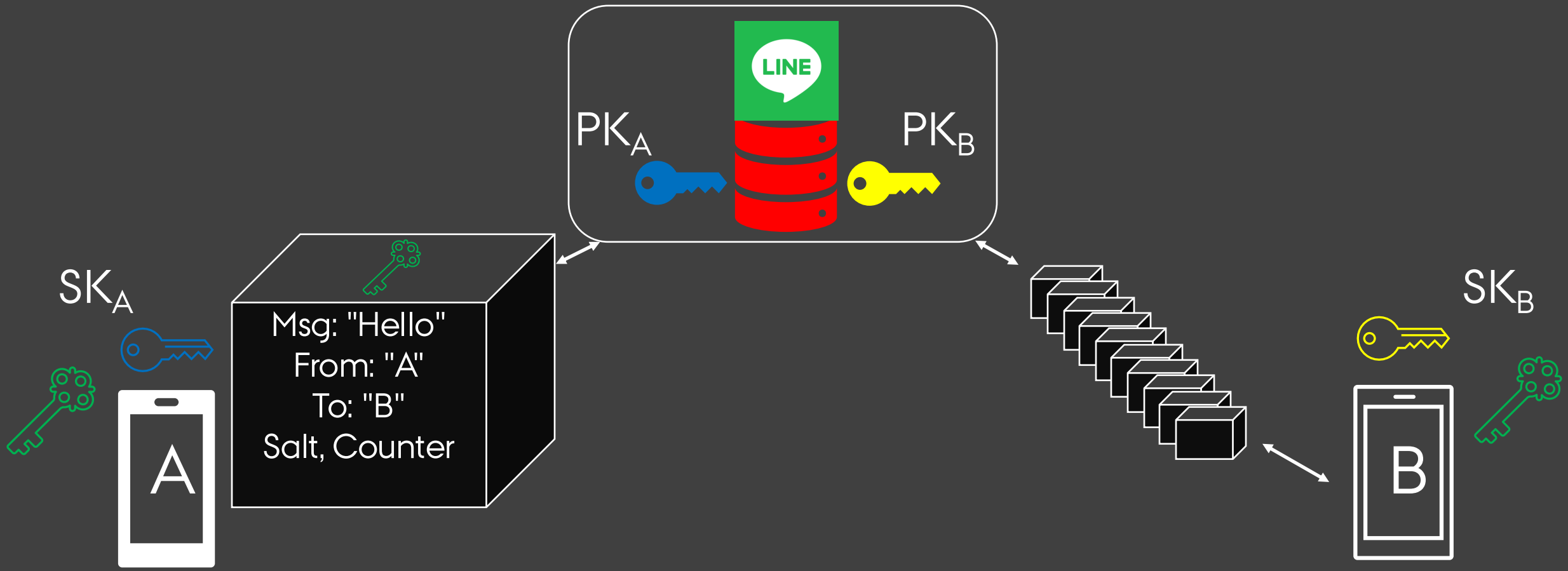
```
{
  ...
  type: "RECEIVE_MESSAGE",
  reqSeq: 0,
  ...
}
```

Changed by server without problem.

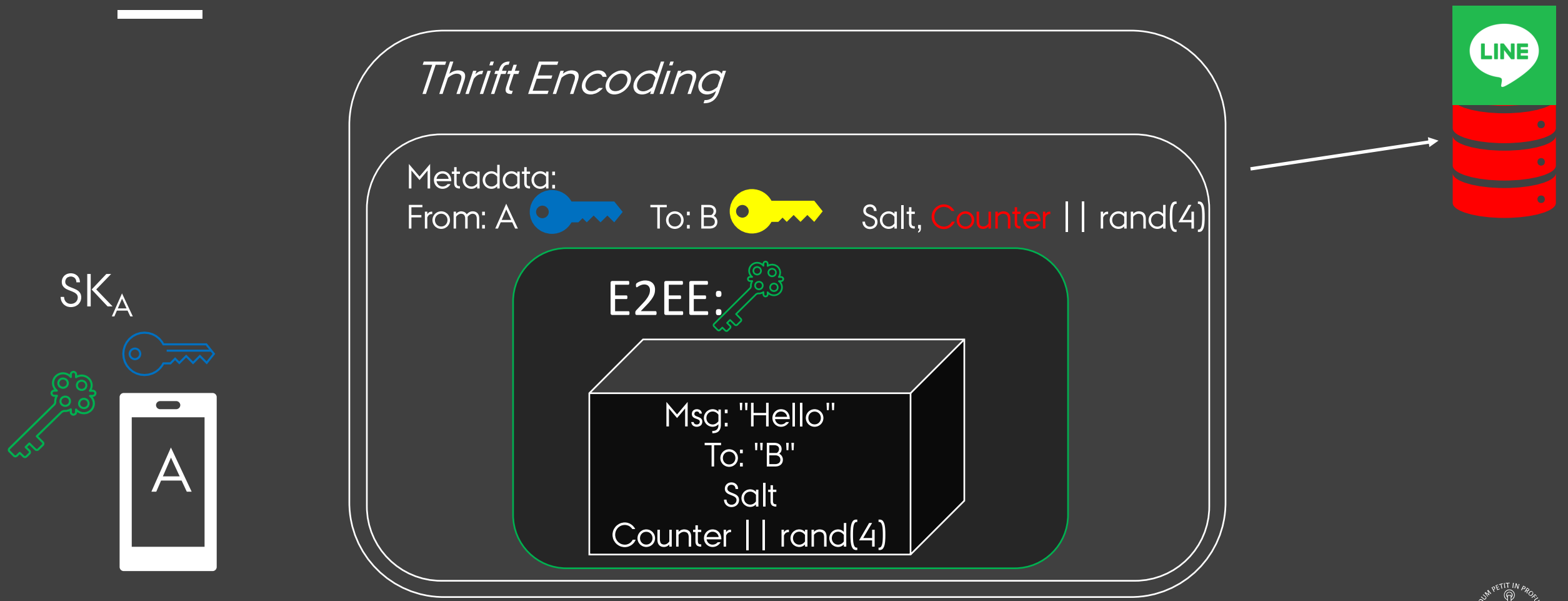
REPLAY ATTACKS: OVERVIEW



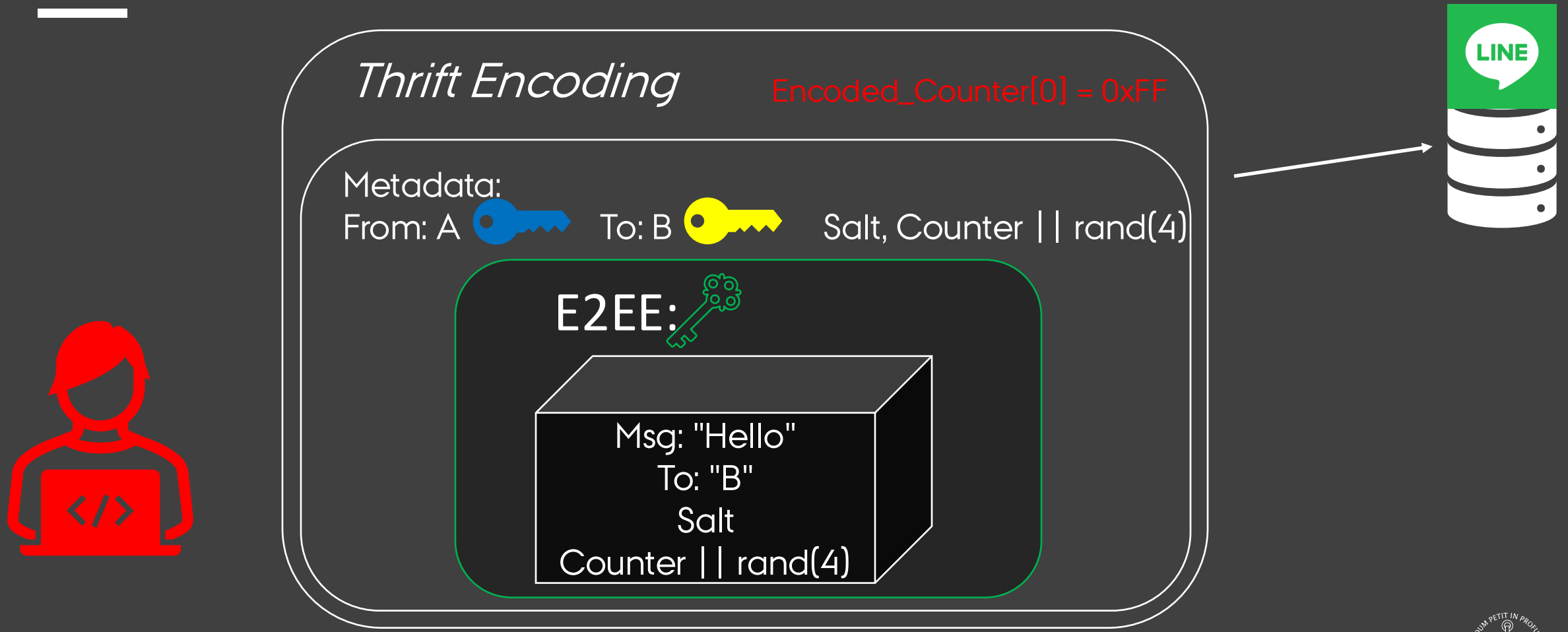
REPLAY ATTACKS: OVERVIEW



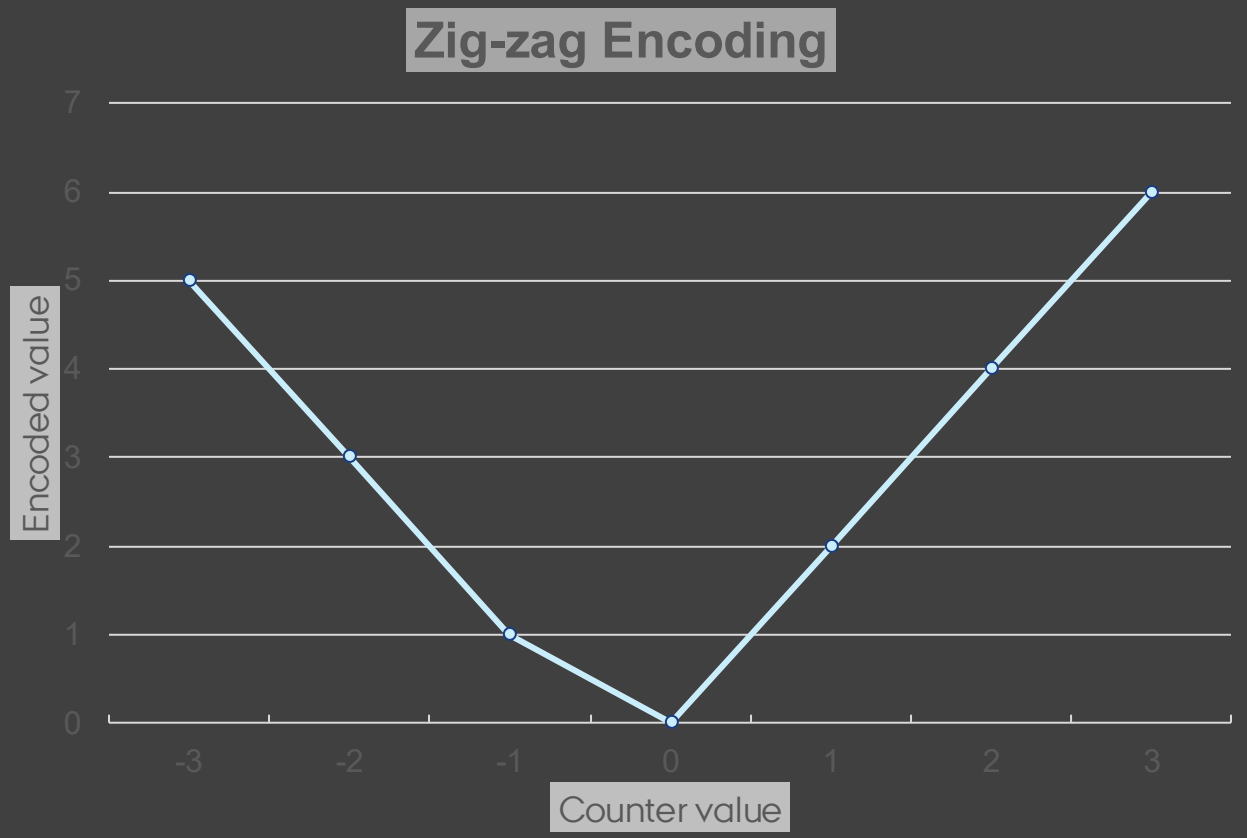
REPLAY ATTACKS: TECHNICAL DETAILS



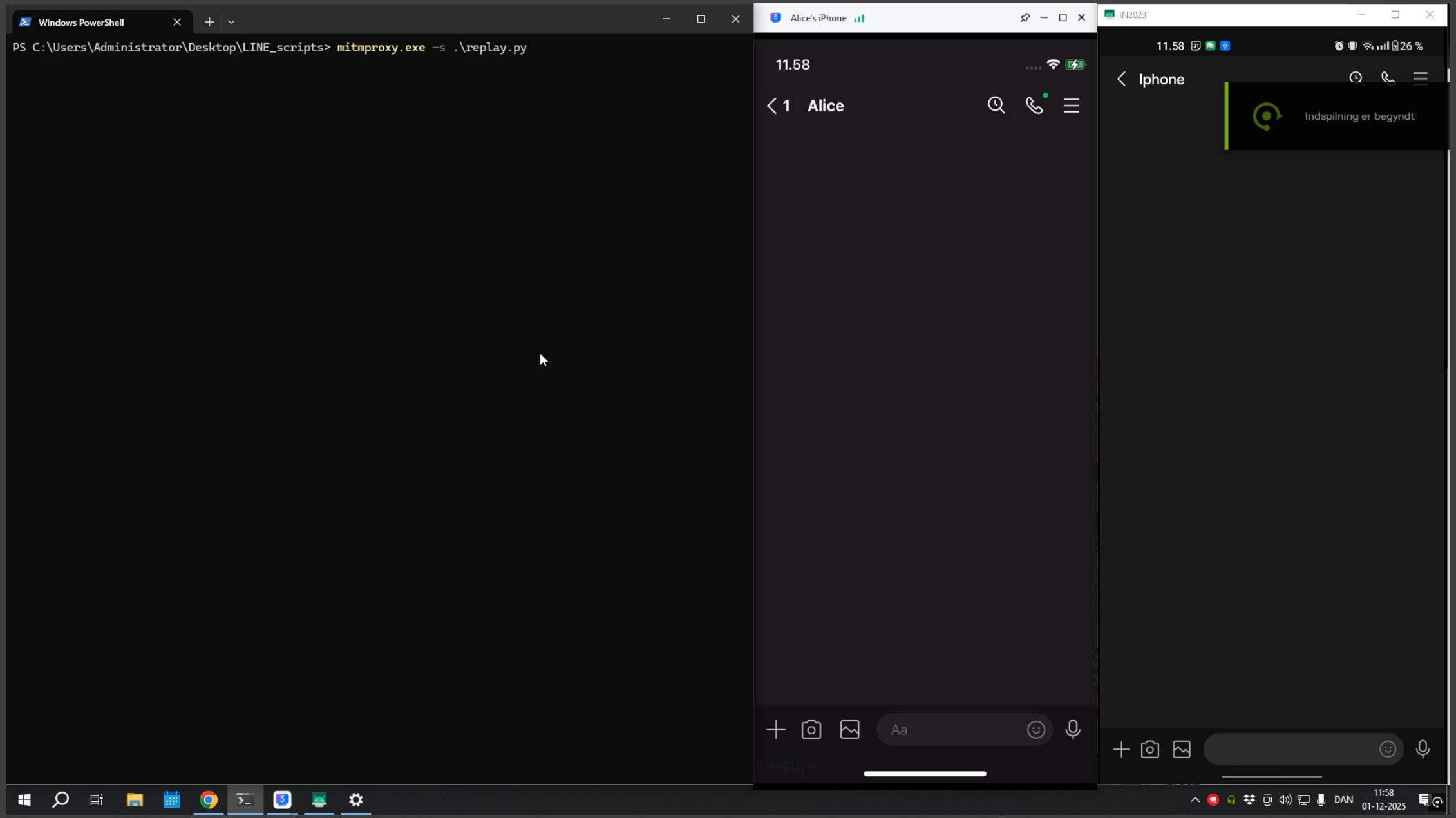
REPLAY ATTACKS: TECHNICAL DETAILS



REPLAY ATTACKS: THRIFT ENCODING

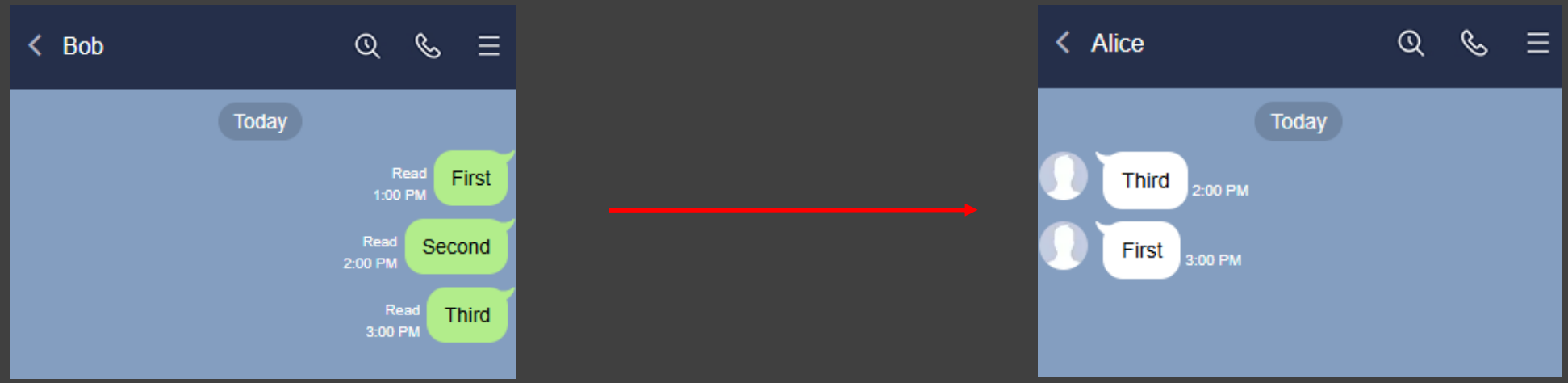


Input	Encoded
Positive	Even
0	0
Negative	Odd


Windows PowerShell
PS C:\Users\Administrator\Desktop\LINE_scripts> mitmproxy.exe -s .\replay.py
Alice's iPhone
11.58
1 Alice
Aa
IN2023
11.58
26 %
Iphone
Indspilning er begyndt
DAN
11:58
01-12-2025

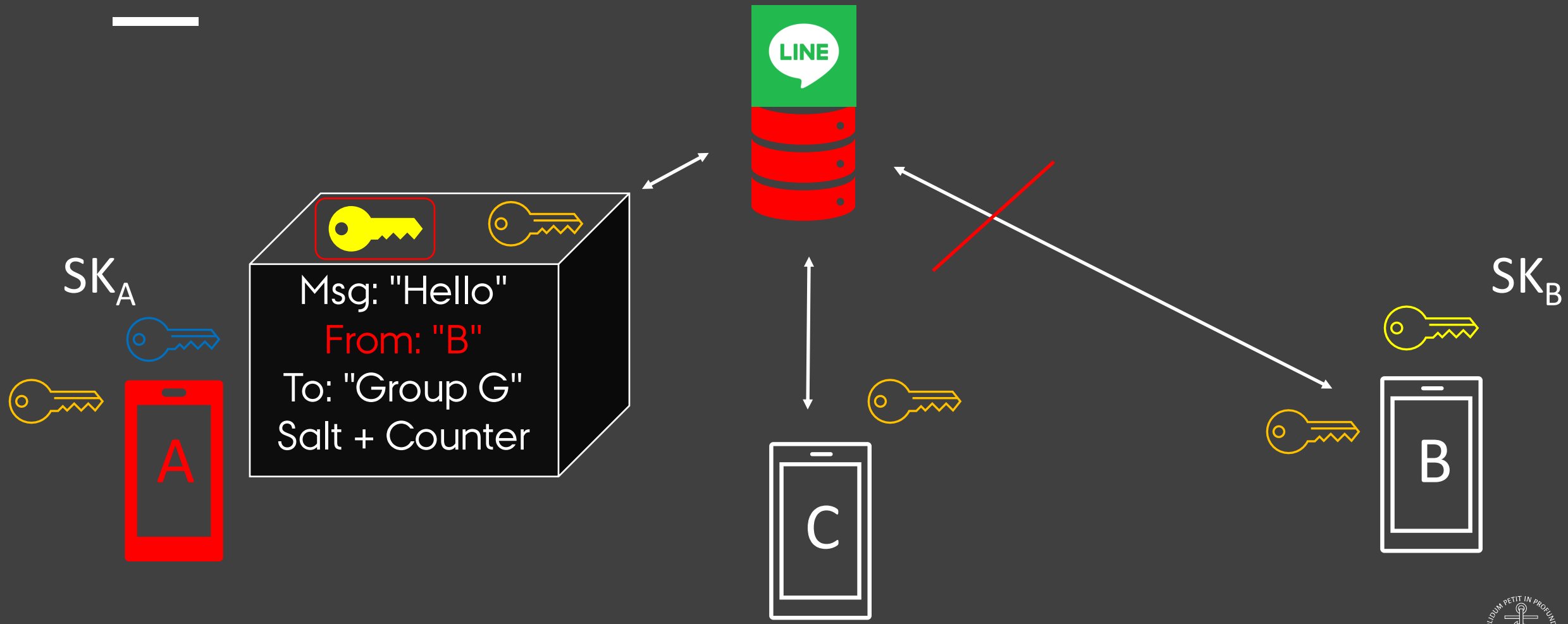
REORDER AND BLOCKING ATTACKS

- There is no way to detect **reordered** messages.
- There is no way to detect **dropped** messages.

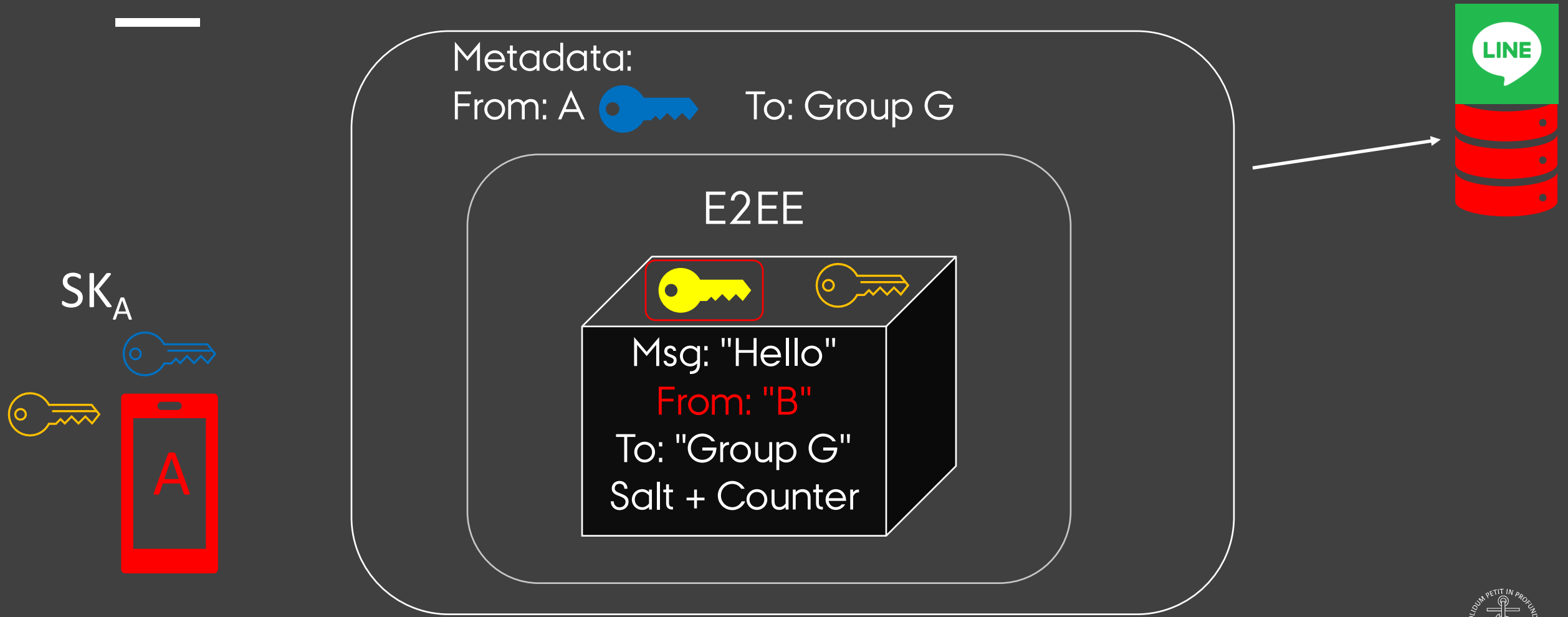


- *Counters could be used to ensure consistent state!*

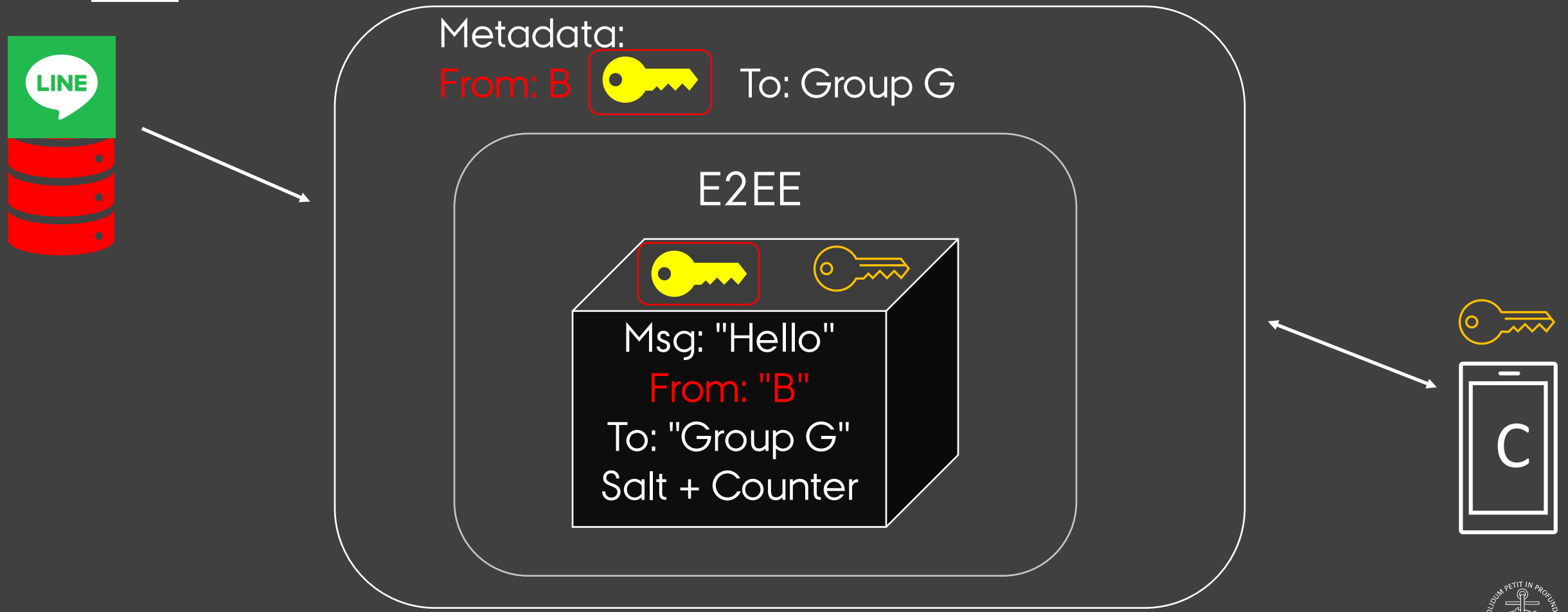
IMPERSONATION ATTACKS: OVERVIEW



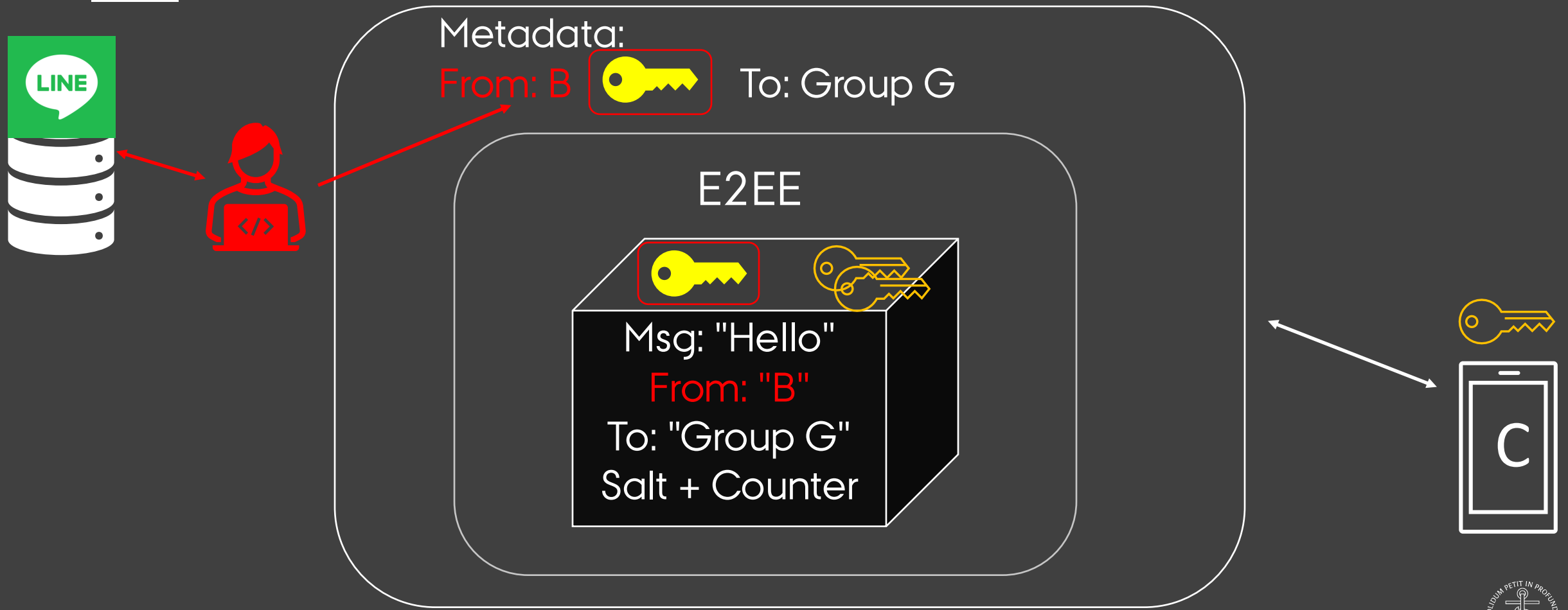
IMPERSONATION ATTACKS: TECHNICAL DETAILS



IMPERSONATION ATTACKS: TECHNICAL DETAILS



IMPERSONATION ATTACKS: TECHNICAL DETAILS



PUTTING IT ALL TOGETHER

E2E attacker capabilities:

- Read receipts and reactions can be forged.
- Messages can be blocked or reordered at will.
- Metadata can be altered without detection.
- Can force key rotation by adding a colluding user.

We conclude that:

- The E2E attacker can **manufacture** a group chat between a subset of users that will look legitimate to others.

STICKER LEAKAGE

Stickers are not sensitive, right?

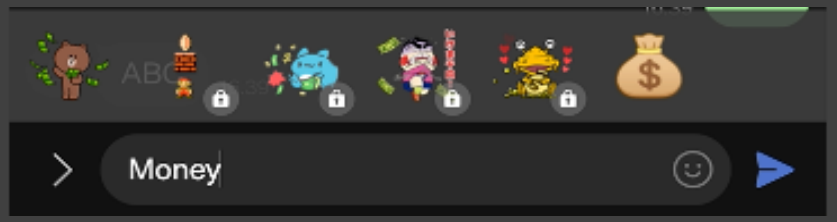
Guess the word matching the stickers:






STICKER LEAKAGE

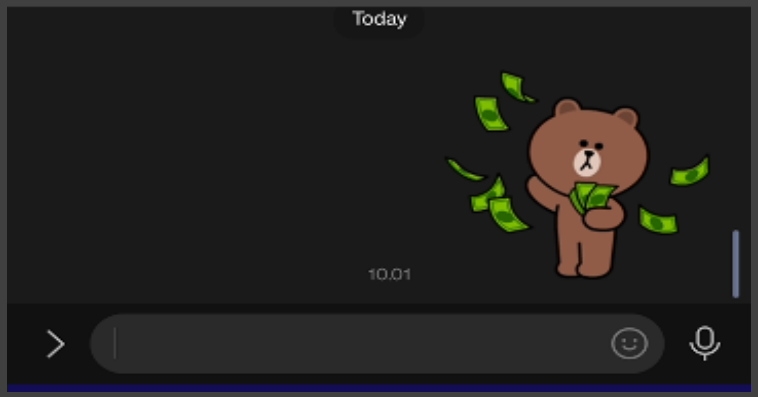
Typing:



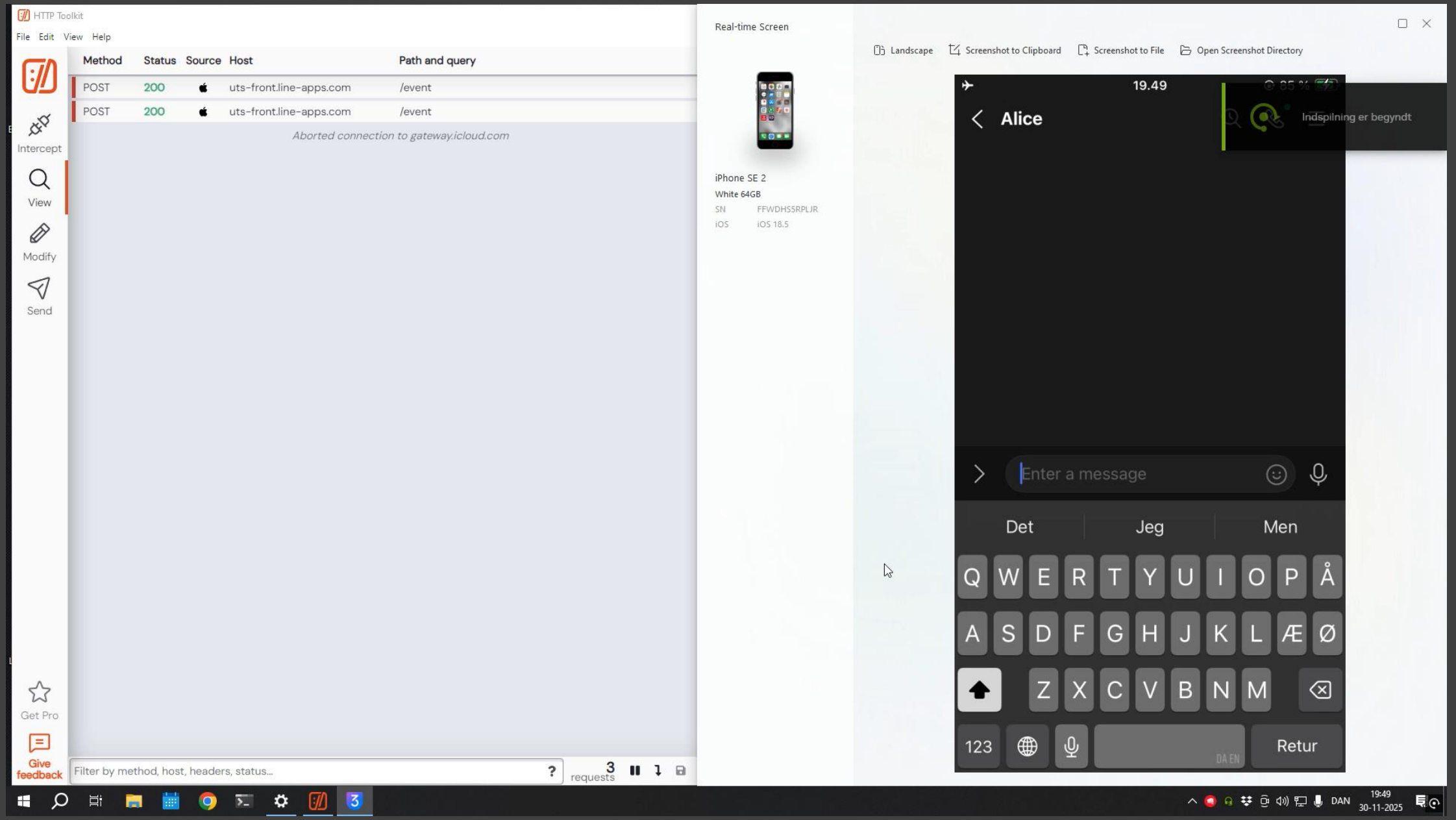
Previewing:



Sending:

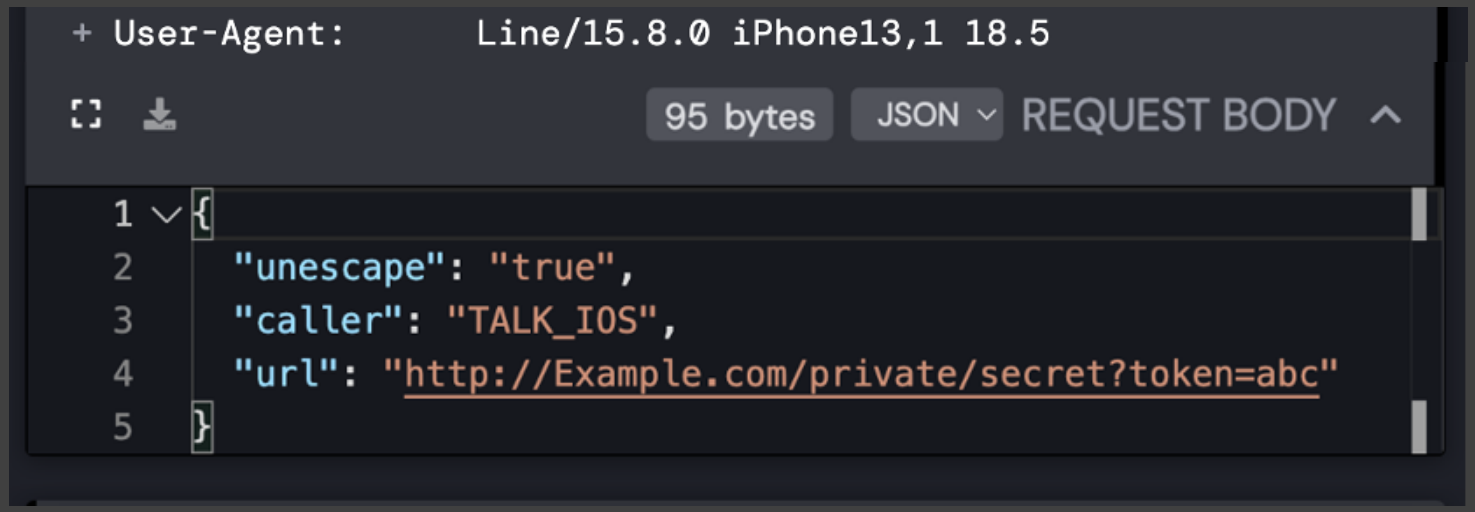


- *"Anonymous lookup" ->* leaks User-Agent
- Allows the server to add spyware stickers


HTTP Toolkit
File Edit View Help
Method Status Source Host Path and query
POST 200 uts-front.line-apps.com /event
POST 200 uts-front.line-apps.com /event
Aborted connection to gateway.icloud.com
Intercept
View
Modify
Send
Get Pro
Give feedback
Filter by method, host, headers, status...
3 requests
Real-time Screen
Landscape
Screenshot to Clipboard
Screenshot to File
Open Screenshot Directory
iPhone SE 2
White 64GB
SN FFWDHS5RPLJR
iOS iOS 18.5
19.49
Alice
Indspilning er begyndt
Enter a message
Det Jeg Men
Q W E R T Y U I O P Å
A S D F G H J K L Æ Ø
Z X C V B N M
123
Retur
DA EN
DAN
19:49
30-11-2025

URL LEAKAGE

Note: In order to generate URL previews, links shared in chats are also sent to LINE's servers.





- Allows the server to censor URLs
- Trade-off between privacy and phishing

VIOLATED SECURITY GOALS

Attack	Violated Security Property
Replay, reorder, blocking	Integrity
Impersonation	Integrity, Authentication
Plaintext leakage (stickers + URLs)	Confidentiality

No continuous key rotation = no Forward Secrecy by design

COORDINATED DISCLOSURE

Disclosure timeline:

- Initial contact in June 2025
- Response by (confused) bug bounty team 2 weeks later
- Routed to CSIRT instead
- First proper response by stakeholders in early August
- Statement provided 2 weeks later
- Minimal feedback on draft and slides
- Insistence on highlighting MITM scenario for experiments

COORDINATED DISCLOSURE

LINE recognizes that replay/block/reorder "*are all limitations inherent in our protocol design, of which we were aware.*"

They "*chose to prioritize user experience, which is why we use the server reception timestamp instead, leading to the cryptographic protocol issues*".

Metadata has "*historically been treated as non-sensitive*", but LINE is "*updating both our threat model and our encryption report accordingly.*"

COORDINATED DISCLOSURE

With regards to impersonation, "*there are checks at the server level preventing impersonated messages from being sent through our infrastructure, but we understand this is not a sufficient countermeasure in the E2EE threat model.*"

Plaintext leakage *"is a result of how we chose to balance privacy with usability.*":

- Private lookups for stickers has been considered, but inefficient at scale
- URL and sticker previews are opt-out features

LINE is committed to *"improving our security and are looking into updating our cryptographic protocol. We will consider how to better address some of the issues you reported, as well as other limitations mentioned in our public encryption report."*

AFTERMATH

Message order

If the time settings on each device are mismatched, the messages may appear out of order. To prevent this, we use the time on our servers to order messages so that they are displayed in the accurate order by time. Message contents are never viewed by anyone other than the sender and receiver with this mechanism.

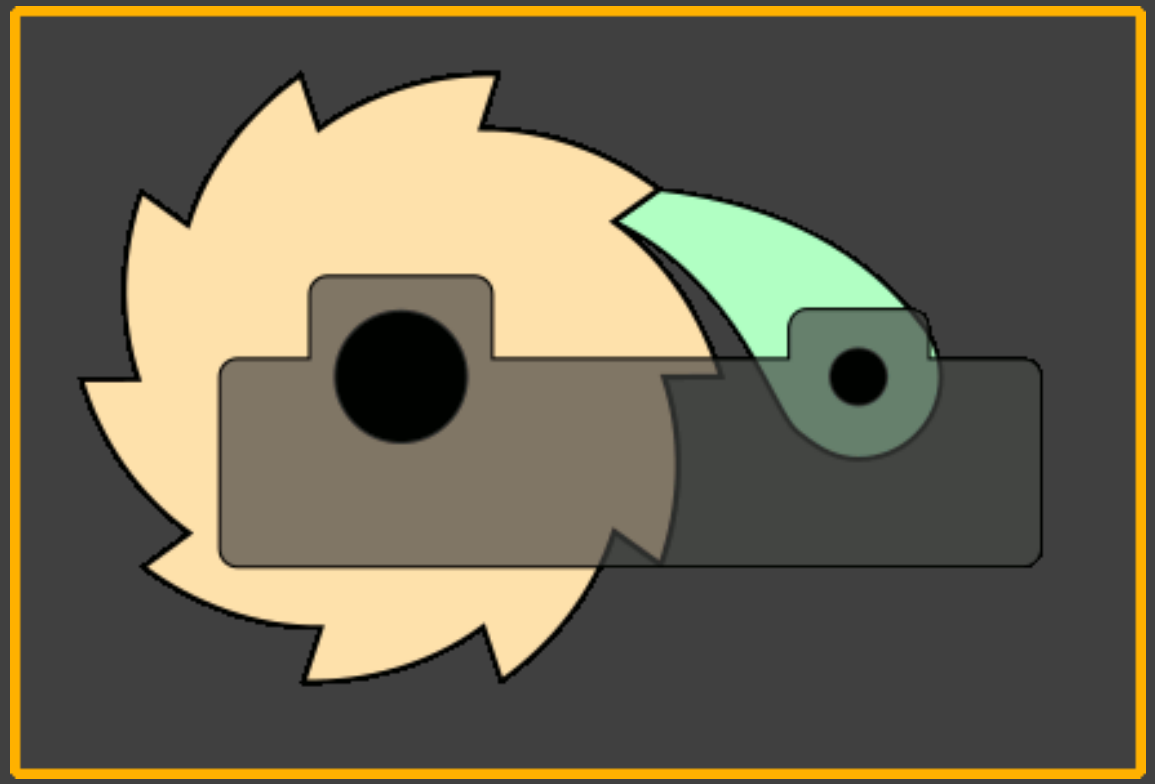
For more information about the efforts we're implementing to protect user information, see Security Initiatives.

URL Previews

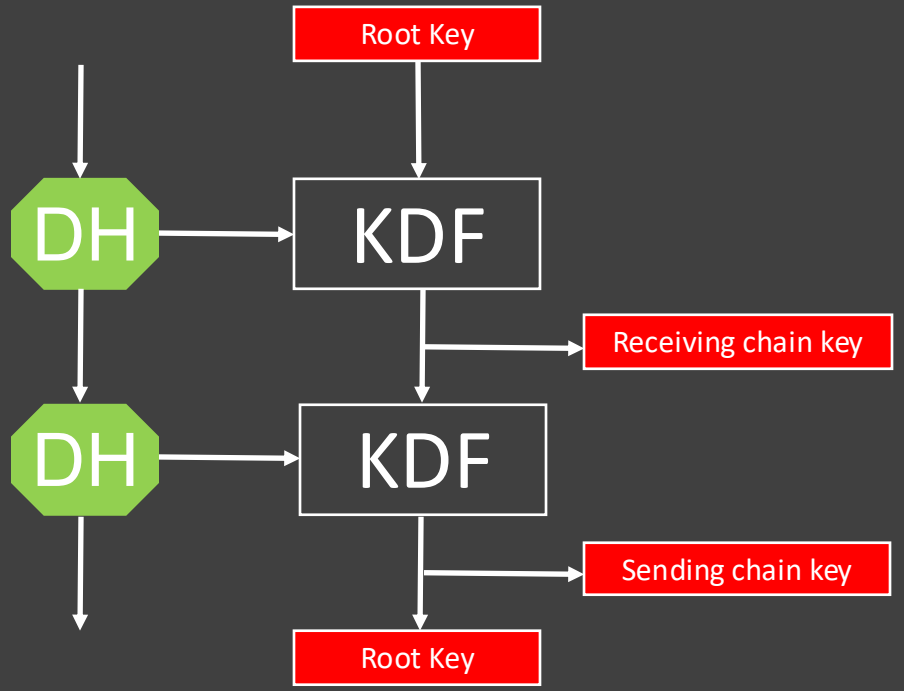
If your device were to access a website directly to create a URL preview, you would be at risk of being tracked (e.g. your IP address being acquired) by the accessed website and others. To prevent this and protect your privacy, we use a secure mechanism where LINE servers access the website on your behalf and generate the preview.
Note: Due to this security feature, URL information is processed on our servers. However, you can turn it off via your settings if you desire.

- Sticker keyword: For LINE to be able to recommend a suitable sticker for the chat context. LINE Privacy teams have designed an hybrid approach, where recommendation models are used locally on the device to list appropriate stickers, and Differential Privacy and Federated Learning techniques are applied when sending user's model differences to the server in order to update the models. This approach does not send plaintext keywords to the server. More information can be found in our Differential Privacy in LINE Federated Learning whitepaper.

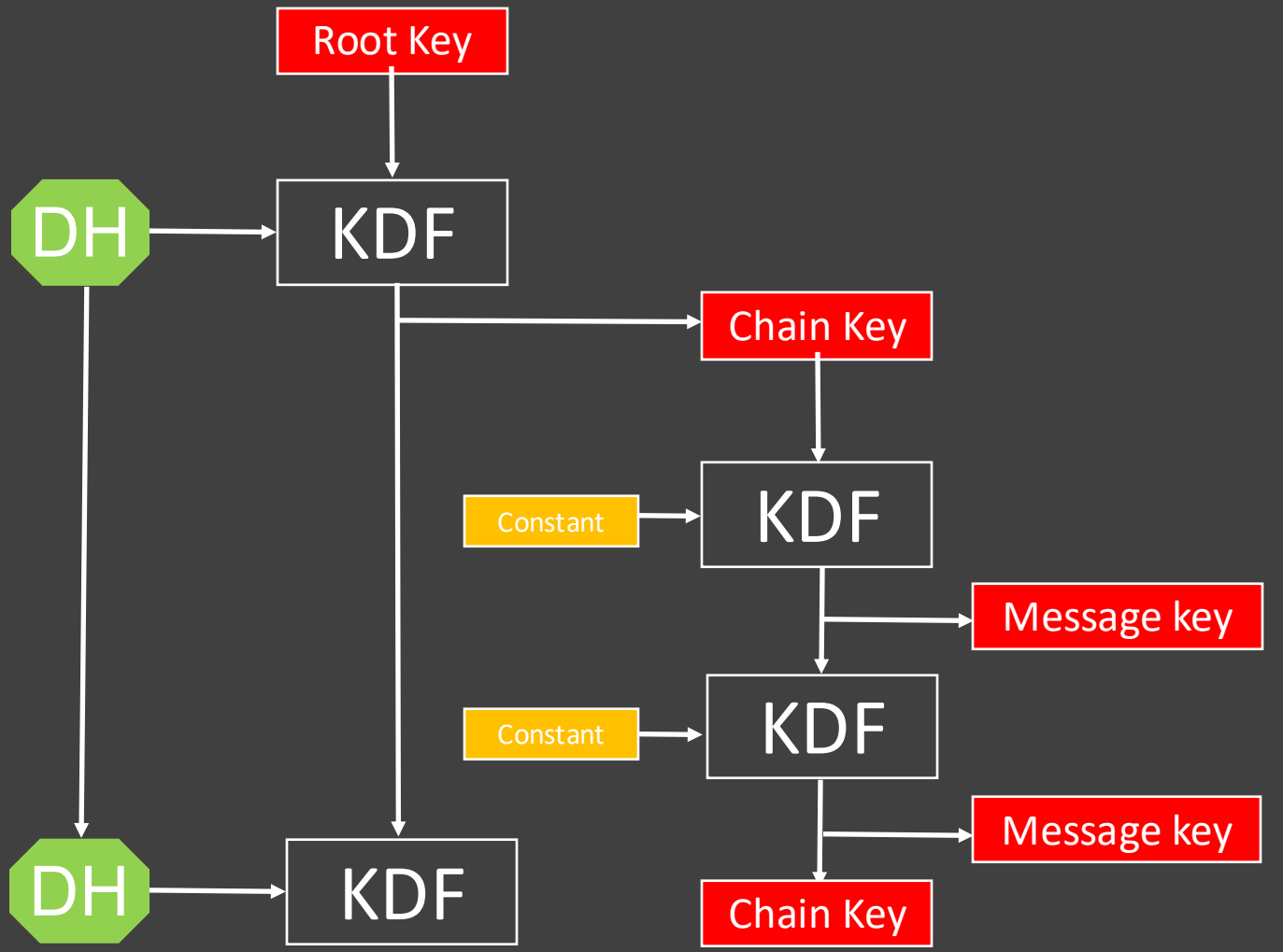
SIGNAL: THE DOUBLE RATCHET



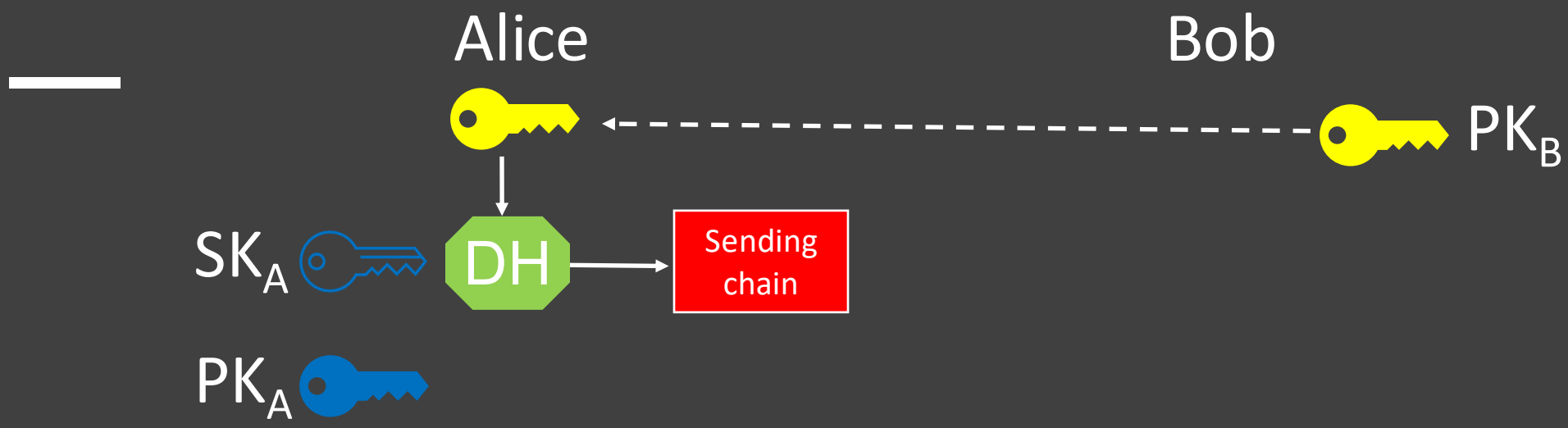
Source: https://commons.wikimedia.org/wiki/File:Ratchet_Drawing.svg
License: CC BY-SA 3.0



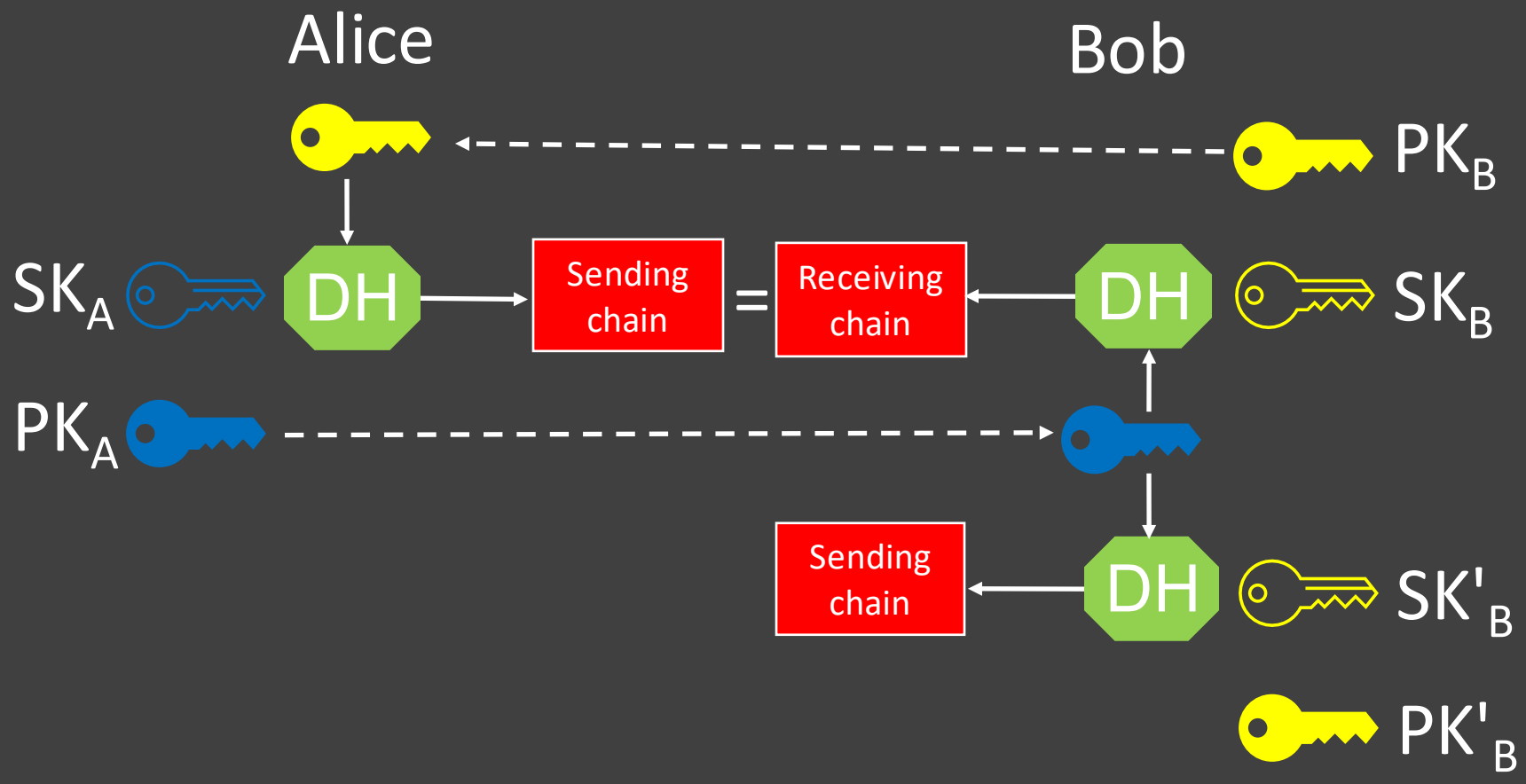
SIGNAL: THE SYMMETRIC RATCHET



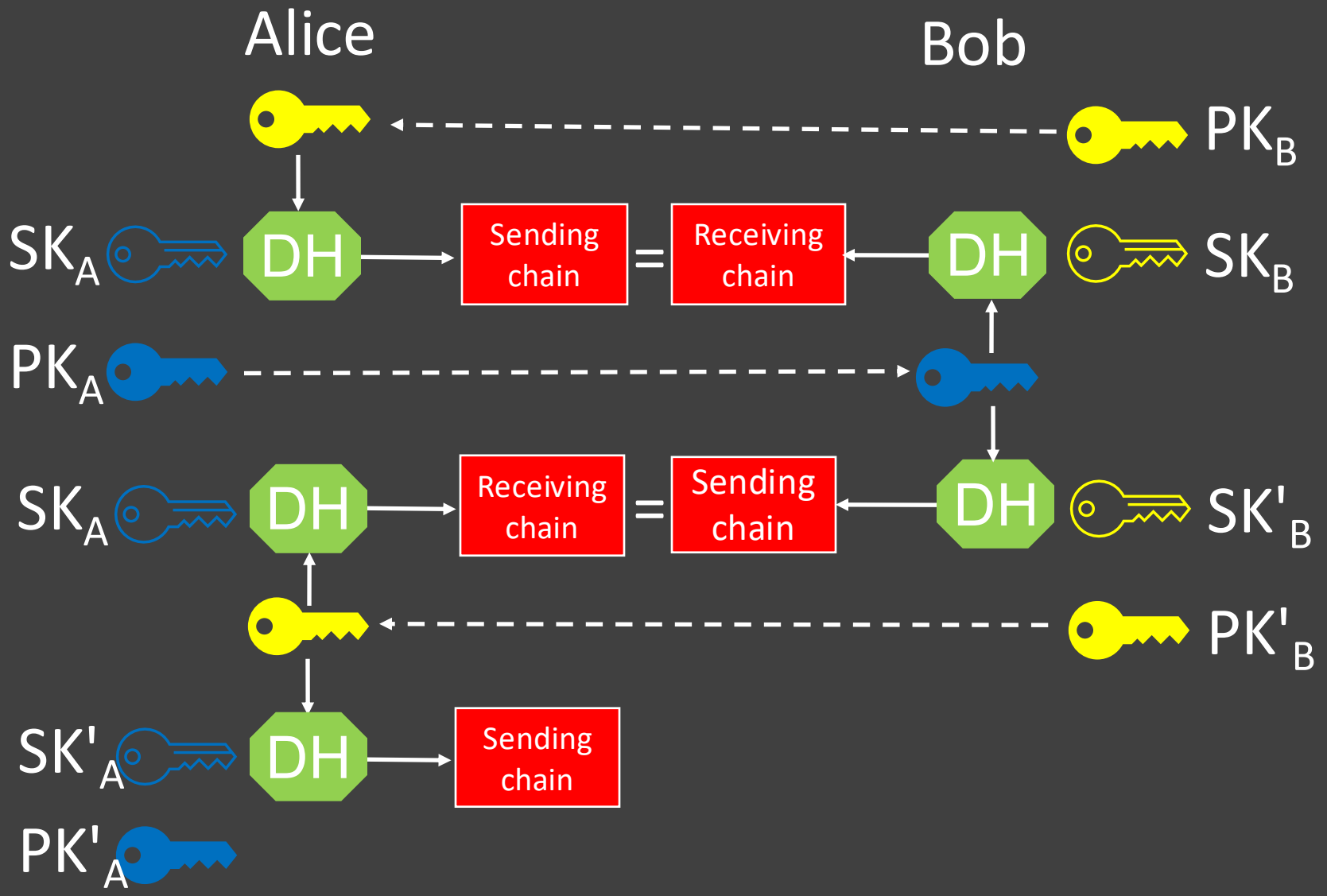
SIGNAL: THE DH RATCHET



SIGNAL: THE DH RATCHET



SIGNAL: THE DH RATCHET



KEY TAKEAWAYS

As a LINE user, you implicitly **trust** the server to:

- Deliver all messages in-order
- Not snoop into what you are typing (stickers + URL)
- Not collude in impersonation attacks

*This is **not** how E2EE is supposed to work.*

KEY TAKEAWAYS

Three lessons to learn:

- Design for security from ground up: reuse standards/best practices
- Include as much as possible in the E2EE scope
- Beware of evolving threat models (critical infra in Taiwan)



linebreak.info


SOLIDUM PETIT IN PROFUNDIS
UNIVERSITAS ARHUSIENSIS

SIGNAL: GROUP CHATS

- Phase 1 (TextSecure, early Signal):
  - Group messages are O(n) encryptions, one per DH Ratchet
  - MAC prevent impersonation)

- Phase 2 (modern Signal & WhatsApp):
  - all members share one symmetric ratchet per sender (MAC can be forged)
  - **Sender keys** and signatures were introduced to prevent impersonation.

PRESS COVERAGE

- LINE Messaging Bugs Open Asian Users to Cyber Espionage: https://www.darkreading.com/application-security/line-messaging-bugs-asian-cyber-espionage

- Examining the design philosophy of LINE Letter Sealing v2 from the official E2EE" perspective, starting with — the server is not trusted (In Japanese): https://innovatopia.jp/cyber-security/cyber-security-news/75019/