Report on Originator traceability in WhatsApp messages

V. Kamakoti,

Professor, Department of Computer Science and Engineering

IIT Madras, Chennai – 600036

As directed by The Hon'ble High Court of Madras, I am submitting this technical report detailing how ***originator information*** of a WhatsApp message could be traced. We provide two suggestions for the same to The Hon'ble High Court of Madras. However, WhatsApp Inc. may have other methods for extracting originator information.

The following terminologies are used in this document.

WhatsApp Server: The intermediate computing facility which coordinates the messaging mechanism.

WhatsApp Software: The software installed by the WhatsApp user on the mobile and/or end devices.

Key: A computer generated data analogous to a password used to lock (encrypt) or unlock (decrypt) a cryptographic function (such as Encryption / Decryption)

Encryption: A mechanism that will convert a data/message (human readable) into a garbled (human non-readable) form using a key **E**.

Decryption: This is the opposite of encryption that converts the garbled (human non-readable) form to the data/original message (human readable) using a key **D**.

Asymmetric Encryption-Decryption: The two keys '**E**' and '**D**' are different. Normally '**E**' is called public key and '**D**' is called private key.

Public Key : One of two keys used in Asymmetric Encryption-Decryption typically used to encrypt(lock) data/message.

Private Key : One of two keys used in Asymmetric Encryption-Decryption typically used to decrypt(unlock) data/message.

Fig 1 explains a generic asymmetric encryption-decryption scheme.

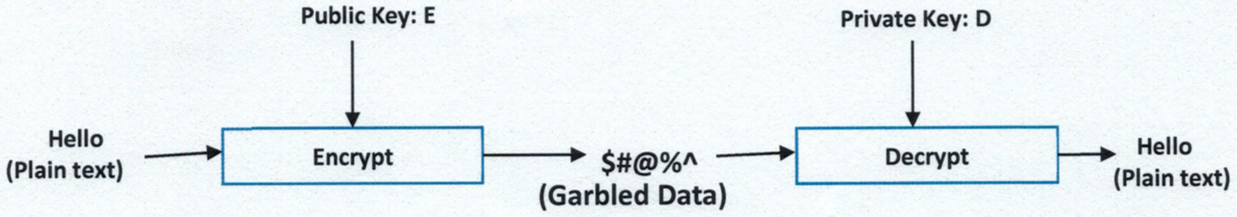


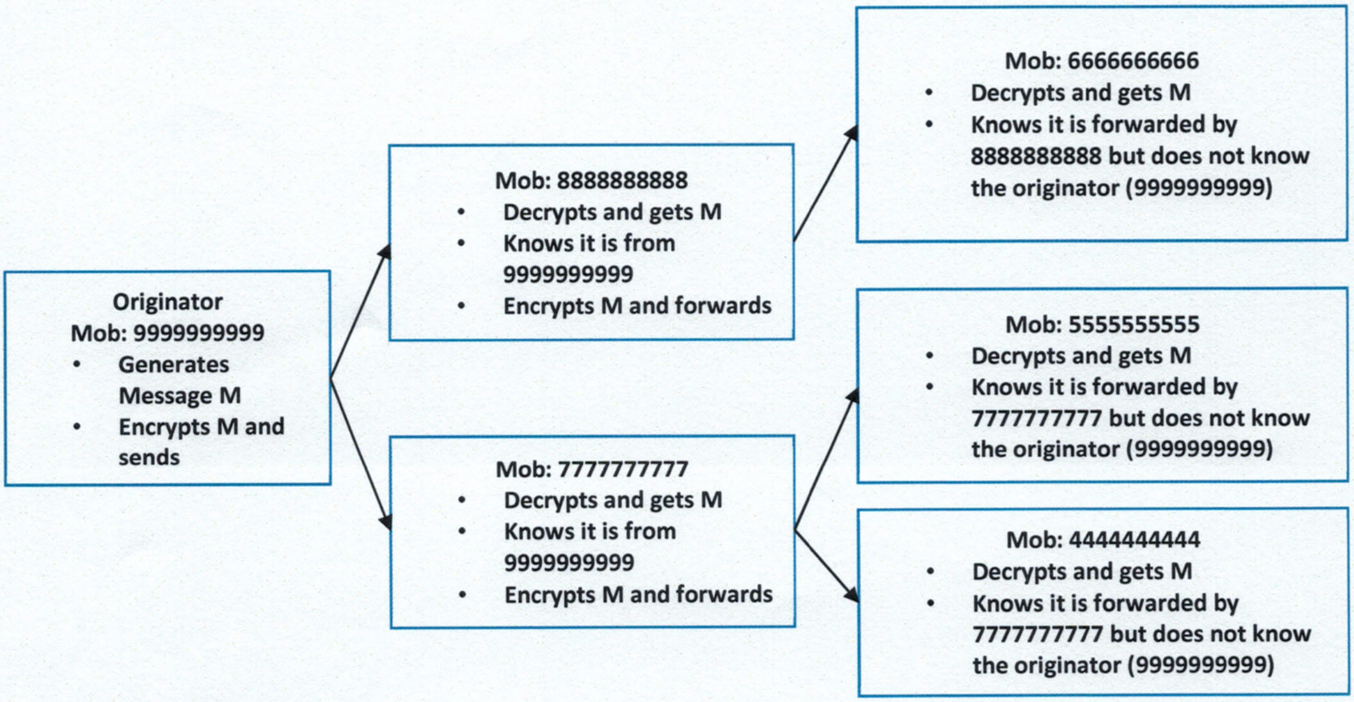
Fig 1: Asymmetric Encryption-Decryption Scheme

V. Kamakoti

प्रो. वी. कामकोटि
Prof. V. KAMAKOTI
सह-डीन / ASSOCIATE DEAN
औद्योगिक परामर्श एवं प्रायोजित अनुसंधान
INDUSTRIAL CONSULTANCY & SPONSORED RESEARCH

In the Fig 1, the plain text, "Hello" (in this case), gets encrypted using a public Key **E** and converted to garbled data at the transmission end. The garbled data gets decrypted back to the plain text using a private key **D** at the receiving end. ***The point to be noted is that it is impossible to convert the garbled data back to the plain text without the private key "D".***

The Fig 2. illustrates the current functioning of WhatsApp messaging system (as perceived by its users), wherein, the recipient of a forwarded message will not know the originator information



Originator
Mob: 9999999999
- **Generates Message M**
- **Encrypts M and sends**

Mob: 8888888888
- **Decrypts and gets M**
- **Knows it is from 9999999999**
- **Encrypts M and forwards**

Mob: 7777777777
- **Decrypts and gets M**
- **Knows it is from 9999999999**
- **Encrypts M and forwards**

Mob: 6666666666
- **Decrypts and gets M**
- **Knows it is forwarded by 8888888888 but does not know the originator (9999999999)**

Mob: 5555555555
- **Decrypts and gets M**
- **Knows it is forwarded by 7777777777 but does not know the originator (9999999999)**

Mob: 4444444444
- **Decrypts and gets M**
- **Knows it is forwarded by 7777777777 but does not know the originator (9999999999)**

Fig 2: Current Functioning of WhatsApp Message forwarding.

Explanation of Figure 2

Whenever a registered user of WhatsApp **creates/originates** a message 'M", he/she is designated as the **sender** of the message. When the sender wishes to send to multiple recipients and when these recipients in turn, intend to forward the received message, the following mechanism is followed by WhatsApp

WhatsApp software residing at the end device of the sender encrypts both the message and the sender information and sends this to every recipient of the message.

Each of the recipient of the message from (the sender) decrypts the message (M) and the sender information. Thus, all recipients know the sender information of the message received.

When any of the recipients, R, wishes to forward the received message (M), WhatsApp software designates R as a sender, encrypts M along with the user information of R and enables **the forward**.

प्रो. वी. कामकोटि
Prof. V. KAMAKOTI
सह-डीन / ASSOCIATE DEAN
औद्योगिक परामर्श एवं प्रायोजित अनुसंधान

The WhatsApp software at the end device of every recipient decrypts and gets the message and knows the sender from whom the message (M) has come.

All forwarded messages always carry the information about the forwarder and designate the message M with a label "Forwarded" by the WhatsApp software. As of now, the recipients of any forwarded message do not know the creator/originator of the same.

The First Proposal

The Fig 3 illustrates the first proposal wherein every receiver of a forwarded message will get to know its originator.

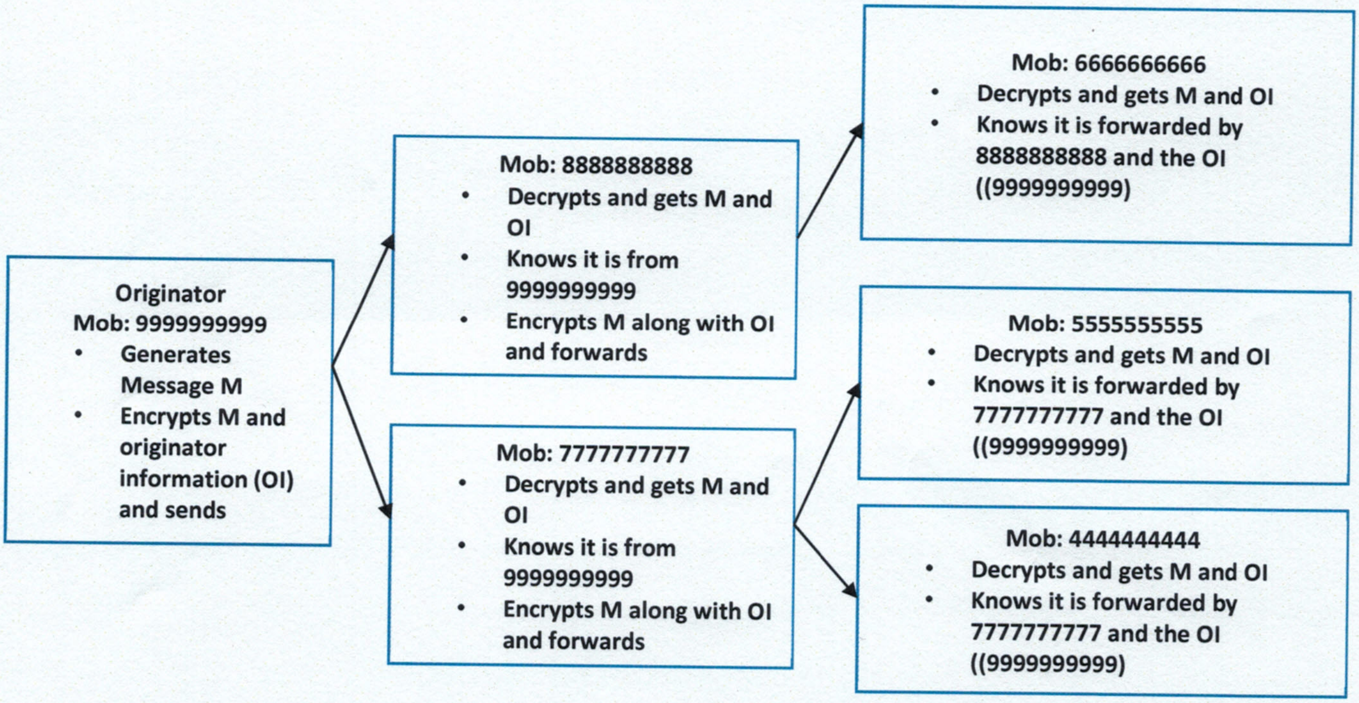

Originator
Mob: 9999999999
• Generates Message M
• Encrypts M and originator information (OI) and sends
Mob: 8888888888
• Decrypts and gets M and OI
• Knows it is from 9999999999
• Encrypts M along with OI and forwards
Mob: 7777777777
• Decrypts and gets M and OI
• Knows it is from 9999999999
• Encrypts M along with OI and forwards
Mob: 6666666666
• Decrypts and gets M and OI
• Knows it is forwarded by 8888888888 and the OI ((9999999999)
Mob: 5555555555
• Decrypts and gets M and OI
• Knows it is forwarded by 7777777777 and the OI ((9999999999)
Mob: 4444444444
• Decrypts and gets M and OI
• Knows it is forwarded by 7777777777 and the OI ((9999999999)

Fig 3: Proposal 1 for Originator Tracking in forwarded messages.

Explanation of Figure 3

Whenever a registered user of WhatsApp **creates** a message 'M", he/she is designated as the **originator** of the message. When the originator wishes to send to multiple recipients, and, when these recipients in turn, intend to forward the message received, the following mechanism is proposed.

WhatsApp software residing at the end device of the originator encrypts both the message and the originator information (OI) and sends this to every recipient of the message.

Each of the recipient of the message from (the originator) decrypts the message (M) and the OI. Thus, all recipients know the originator information of the message received. When any of these recipients wishes to forward the received message (M) it is proposed that the WhatsApp software encrypts M along with

प्रो. वी. कामकोटि
Prof. V. KAMAKOTI
सह-डीन / ASSOCIATE DEAN

the OI it received and then forwards. The recipients of this forwarded message will decrypt and get to know the message, the forwarder identity and the O.I.

Whenever, a message is modified (such as copy and paste, adding text to media content like images, audio, document and video) by a user, that user becomes the originator. In this proposal, every recipient of a message will know its originator.

The Second Proposal

In case the Hon'ble High Court feels that the originator information need not be disclosed to every recipient, then the following proposal may be considered. The Fig 4. explains this proposal.

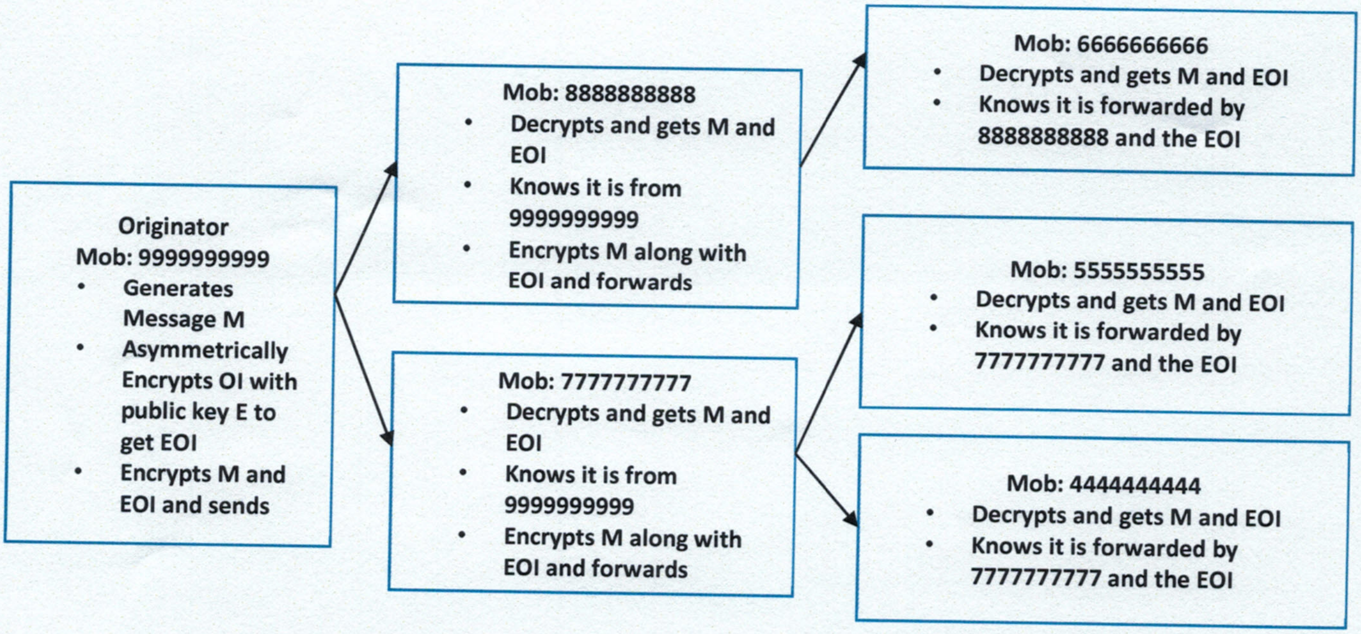

Originator
Mob: 9999999999
• Generates Message M
• Asymmetrically Encrypts OI with public key E to get EOI
• Encrypts M and EOI and sends
Mob: 8888888888
• Decrypts and gets M and EOI
• Knows it is from 9999999999
• Encrypts M along with EOI and forwards
Mob: 7777777777
• Decrypts and gets M and EOI
• Knows it is from 9999999999
• Encrypts M along with EOI and forwards
Mob: 6666666666
• Decrypts and gets M and EOI
• Knows it is forwarded by 8888888888 and the EOI
Mob: 5555555555
• Decrypts and gets M and EOI
• Knows it is forwarded by 7777777777 and the EOI
Mob: 4444444444
• Decrypts and gets M and EOI
• Knows it is forwarded by 7777777777 and the EOI

Fig 4: Proposal 2 for Originator Tracking in forwarded messages.

Explanation of Figure 4

This case is similar to proposal 1 as illustrated in Fig. 3 except for the point that whenever a message is created/originated the OI is encrypted using a public key **E** provided by WhatsApp. The corresponding private key **D** will be known only to WhatsApp. Note that, the (public key **E**, private key **D**) pair is generated and maintained by WhatsApp. As illustrated in Fig. 4, The encrypted **OI**, denoted by **EOI**, is attached to M and then, the rest of the process is the same as in proposal 1. From Fig. 4, note that the recipients of the forwarded message will only get the encrypted form of the originator information (EOI). As they do not have access to the private key **D**, they will not be in a position to decrypt EOI to get the OI.

Typically, when a recipient receives an objectionable message, he/she can forward the same to the Law Enforcement Agency as a WhatsApp message. The LEA will have access to the message and the EOI. The

प्रो. वी. कामकोटि
Prof. V. KAMAKOTI
सह-डीन / ASSOCIATE DEAN
औद्योगिक परामर्श एवं प्रायोजित अनुसंधान

V. Kamakoti

LEA submits the EOI to WhatsApp. As WhatsApp has access to the private key **D**, it can decrypt EOI to get the OI and pass on the OI information to the LEA.

Access of phone numbers and device identifiers to WhatsApp

It is also important to note that WhatsApp has access to individual phone numbers and device identifiers even in its current implementation as per their submission to the Hon'ble High Court of Madras.

Device and Connection information (As submitted by WhatsApp).

*"We collect **device specific information** when you install, access, or use our Services. This includes information such as hardware model, operating system information, browser information, IP address, mobile network information **including phone number and device identifiers**. We collect device location information if you use our location features such as when you choose to share your location with your contacts, view location nearby or those others have shared with you, and the like, and for **diagnostics and trouble-shooting purposes** such as if you are having trouble with your **app's location features** "*

In both of my proposals it is to be noted that WhatsApp do not have access to OI through our process. They get access to OI only when the LEA submits the EOI and request for the OI.

V. Kamakoti

Submitted and Signed by Prof Kamakoti

Date 31/7/2019

प्रो. वी. कामकोटि
Prof. V. KAMAKOTI
सह-डीन / ASSOCIATE DEAN
औद्योगिक परामर्श एवं प्रायोजित अनुसंधान
INDUSTRIAL CONSULTANCY & SPONSORED RESEARCH
आईआईटी मद्रास, चेन्नै 600036
IIT MADRAS, CHENNAI-600 036.