**Name: Rana Mohamed Hamed**

**Department: Computer science**

**ID: 201800041**

**Viber Instant Messaging System**

First of all: a collection of devices registered with viber for the same mobile number, An account is made up of one primary device and optional secondary devices, message is sent or received by any device is displayed on all other devices.

**How the Key is generated?**

ID-Key is generated for the primary device along term 256 bit curve-25519 key pair used to identify a viber account.

Pre-keys: are a set of medium curve term 256 bit curve-25519 key pairs, that are used to setup “one to one” secure sessions between devices, it is generated separately.

If (Alice) Wishing to establish a session with a peer (Bob):

* Sends a query to the viber server with the recipient’s phone number, the server responds with the peer public ID Key and a series of peer public PreKeys, one for each device registered by Bob account.
* Alice device then generates two 256 bit curve-25519 as its own handshake and ratchet keys, then derives the root keys

The RootKey is then used to derive the ***session key:***

DH indicates the use of Elliptic-Curve Diffie- Hellman key exchange algorithm

HS indicates handshake key

” Alice“ then sends to “Bob” a session start message containing its own public ID an identifier of “Bob’s” pre-key that is used for this session and its own handshake and ratchet, when Bob goes online and retrieve this message, it can reconstruct the same root and sessions keys using the same DH procedures.

**How message is exchanged:**

The message sent from a sender has to be encrypted for every session and for every device the target user has. To accomplish this:

* An ephemeral one time 128 bit symmetric key is generated and is used to encrypt the message body using salsa20 encryption algorithm.
* This ephemeral is encrypted using each recipient’s key.
* The sender sends a unified message to the sender containing one encrypted cyphertext and a set of encrypted ephemeral keys, a server side fan-out slices this message and delivers the relevant part to each target device.

The two devices takes turns in advancing the session keys in a process called Ratchet, each time the direction of the message changes, the device whose turn it is randomly generates a new Ratchet key pair.

With being the private part of the newly deriver key-pair, alongside each message, the public part of is also sent.

Then the recipient:

* Runs DH with the last private ratchet together with the sender public ratchet.