Signal & The Double Ratchet

Bobby Picciotti

Signal - A History

- Signal - both an app and the underlying protocol
  - Focuses on secure conversations
- Originally RedPhone & TextSecure
  - Proprietary and released in 2010
  - The company Whisper Systems was acquired by Twitter in 2011
    - Then released both apps under GPLv3
- Open Whisper Systems was founded in 2012
  - The Signal Protocol was released in 2014 and the Signal app was released for iOS with only voice calling abilities
  - Moxie Marlinspike was the founder
  - Later would be merged with TextSecure features

Why is it Important

- WhatsApp, Facebook Messenger, Google Allo
  - First two have a billion users each
- “Despite its importance and novelty, there has been little to no academic analysis of the Signal protocol.”
- Has been a driving force for encryption in “real world” use

Features of the Double Ratchet

- Forward secrecy
  - A future compromise doesn’t invalidate current security
- Future secrecy
  - Compromise of ephemeral key will be “healed”
- Asynchronicity
  - Allows for receiving messages out of order
- Message Unlinkability

The Primitives

- The Diffie-Hellman Ratchet
  - Elliptic Curve Diffie Hellman
    - Using Curve 25519 (The default of OpenSSH and many others)
    - Fast and 128 bits of security
  - X3DH
- Symmetric Encryption
  - AES
    - Cipher Block Chaining mode
    - Counter mode
- Message Authentication Codes
  - HMAC using SHA-2 (256 bit)

X3DH

- Supports X25519 or X448
- Allows for key exchange where one party may be unavailable
  - The exchange happens through an available third party “server”
- Bob places his public identity key, and a signed prekey
  - Alice gets these and forms an initial message with it
  - Bob then processes the message
- The pre-key is replaced frequently
- The protocol has a fallback if no pre-key is published
  - However, replay is possible without a signed pre-key

Quick Look at X3DH Keys

$DH1 = DH(IK_A, SPK_B)$

$DH2 = DH(EK_A, IK_B)$

$DH3 = DH(EK_A, SPK_B)$

$SK = KDF(DH1 \,||\, DH2 \,||\, DH3)$

And if a pre-key is provided

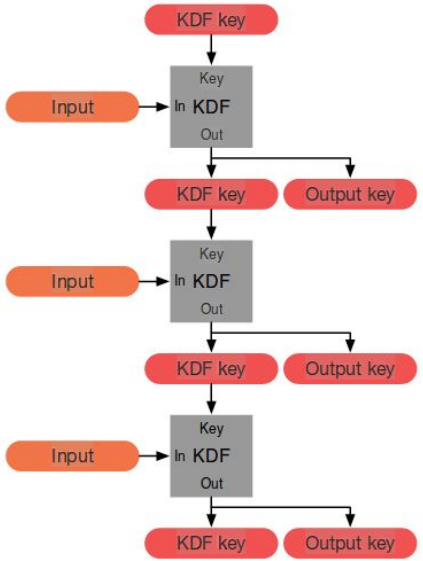
$DH4 = DH(EK_A, OPK_B)$

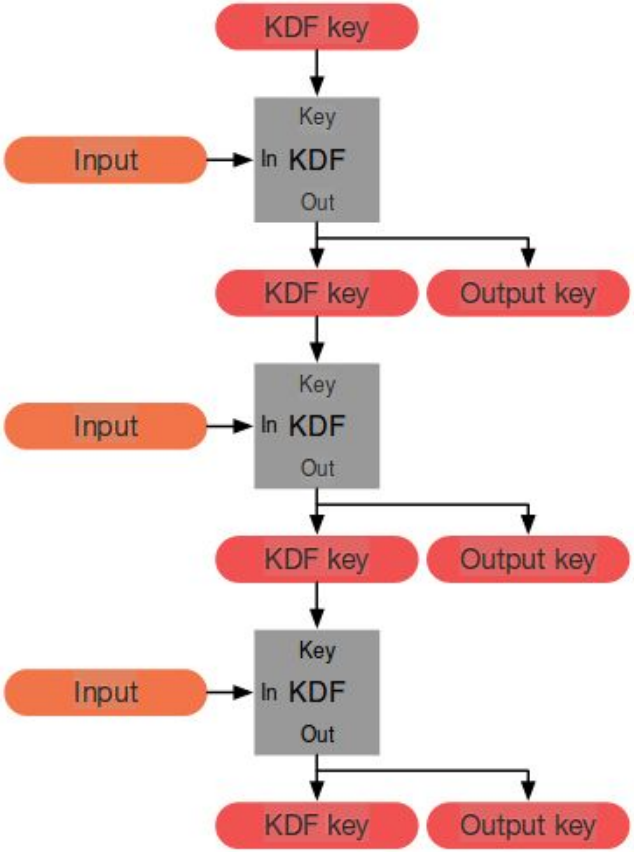
$SK = KDF(DH1 \,||\, DH2 \,||\, DH3 \,||\, DH4)$

- IK_B = Bob's identity key
- SPK_B = Bob's signed prekey
- $Sig(IK_B, Encode(SPK_B))$ = Bob's pre-key signature
- OPK_B = Bob's one-time prekey

KDF Chains

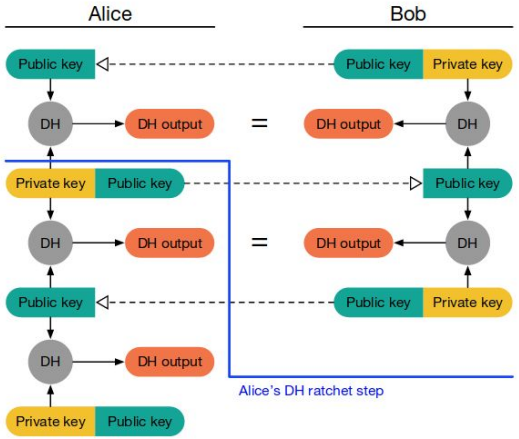
- KDF chains
  - “Key Derivation Function”
  - Takes secret, random KDF key and input data
  - Output split into new KDF key and an output key
- Three chains are used
  - Root
    - Input: Diffie-Hellman output secrets
    - Output: Used as KDF keys for other two chains
  - Sending & Receiving
    - Input: Root chain output
    - Output: Used to encrypt messages

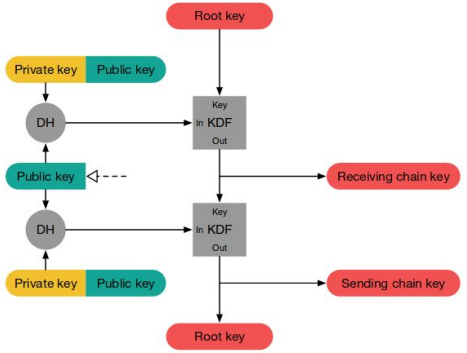


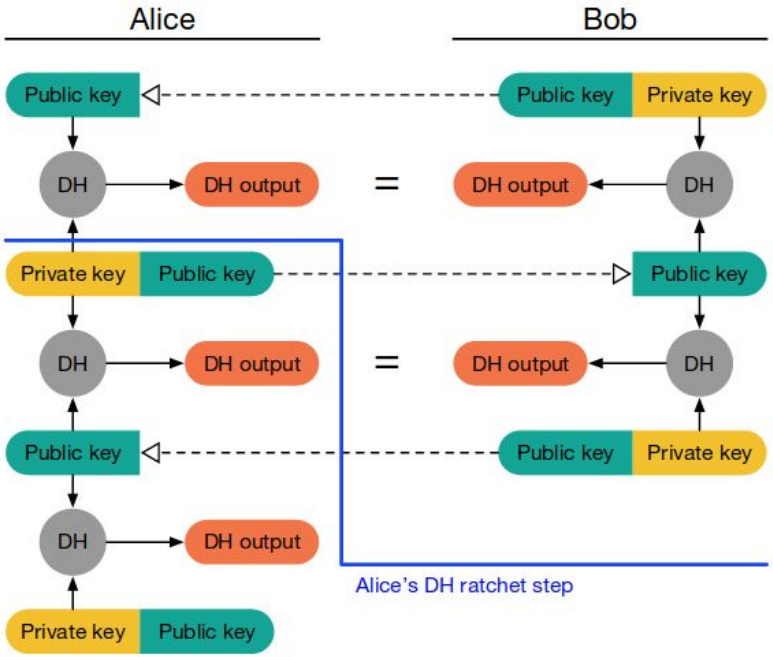

KDF key
Key
Input
In KDF
Out
KDF key
Output key
Key
Input
In KDF
Out
KDF key
Output key
Key
Input
In KDF
Out
KDF key
Output key

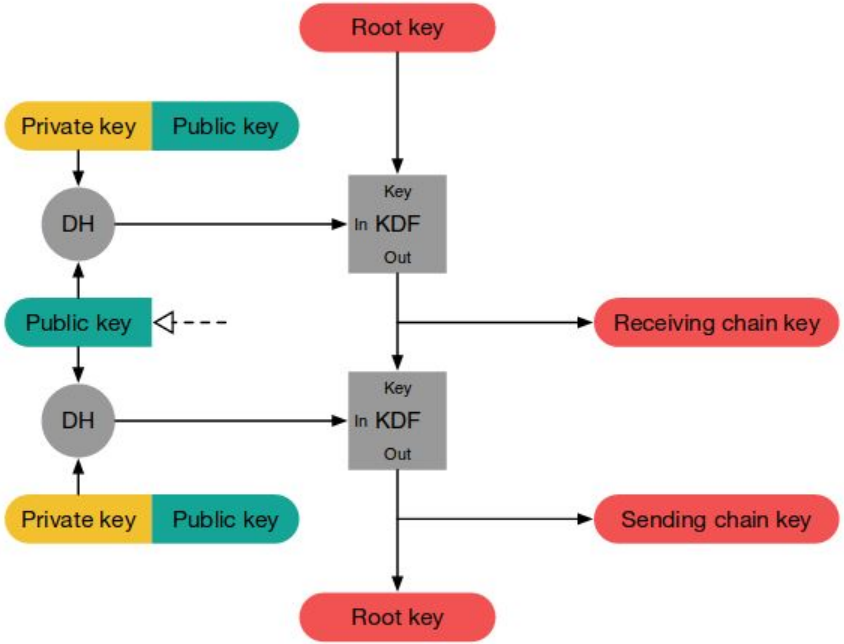
A Double Ratchet

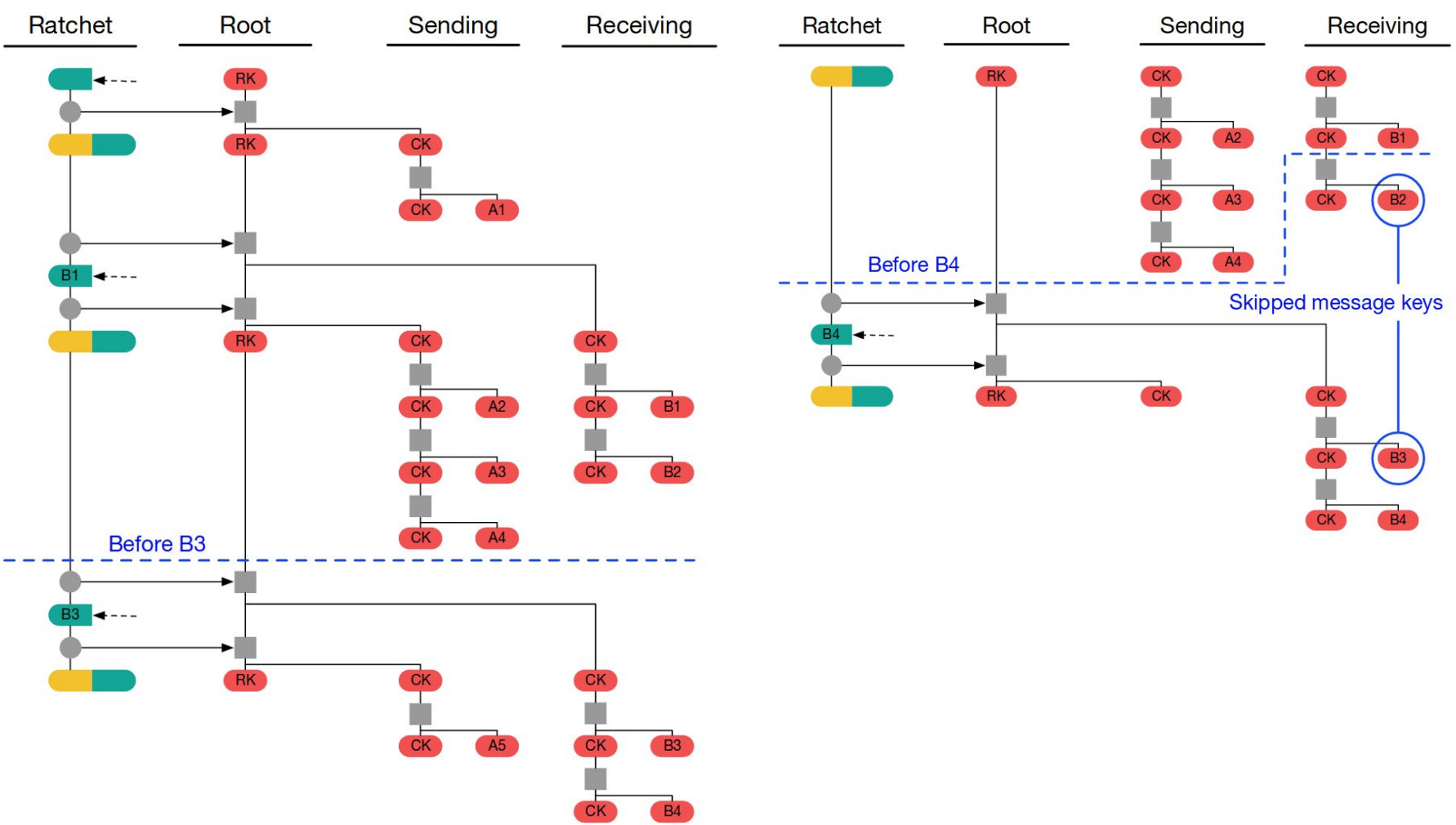
- The Diffie-Hellman Ratchet
  - The Root chain is fed with the DH secret output
    - Add resilience to break in
  - The DH keys are changed frequently
    - Deriving the new key forms the first ratchet
  - The Root chain is updated twice each DH ratchet
- The Symmetric Ratchet
  - These chains are ratcheted for each message
  - Ensure each message has a unique key
  - Keys can be deleted after use
  - Keys for missed messages are stored






Alice
Bob
Public key
Public key
Private key
DH
DH output
=
DH output
DH
Private key
Public key
Public key
DH
DH output
=
DH output
DH
Public key
Public key
Private key
DH
DH output
Alice's DH ratchet step
Private key
Public key


Root key
Private key
Public key
DH
Key
In KDF
Out
Public key
Receiving chain key
DH
Key
In KDF
Out
Private key
Public key
Sending chain key
Root key


Ratchet
Root
Sending
Receiving
RK
RK
CK
CK
A1
B1
RK
CK
CK
A2
CK
A3
CK
A4
CK
CK
B1
CK
B2
Before B3
B3
RK
CK
CK
A5
CK
CK
B3
CK
B4
Ratchet
Root
Sending
Receiving
RK
CK
CK
A2
CK
A3
CK
A4
CK
CK
B1
CK
B2
Before B4
Skipped message keys
B4
RK
CK
CK
CK
B3
CK
B4

Sources

- https://whispersystems.org/docs/specifications/doubleratchet/doubleratchet.pdf
- https://whispersystems.org/docs/specifications/x3dh/
- https://whispersystems.org/blog/advanced-ratcheting/
- https://eprint.iacr.org/2016/1013.pdf
- https://www.cs.bris.ac.uk/Research/CryptographySecurity/RWC/2017/luke.garratt.pdf