

OTR and Signal

CSE 468 Fall 2023

jedimaestro@asu.edu

[https://en.wikipedia.org/wiki/Source_\(journalism\)](https://en.wikipedia.org/wiki/Source_(journalism))

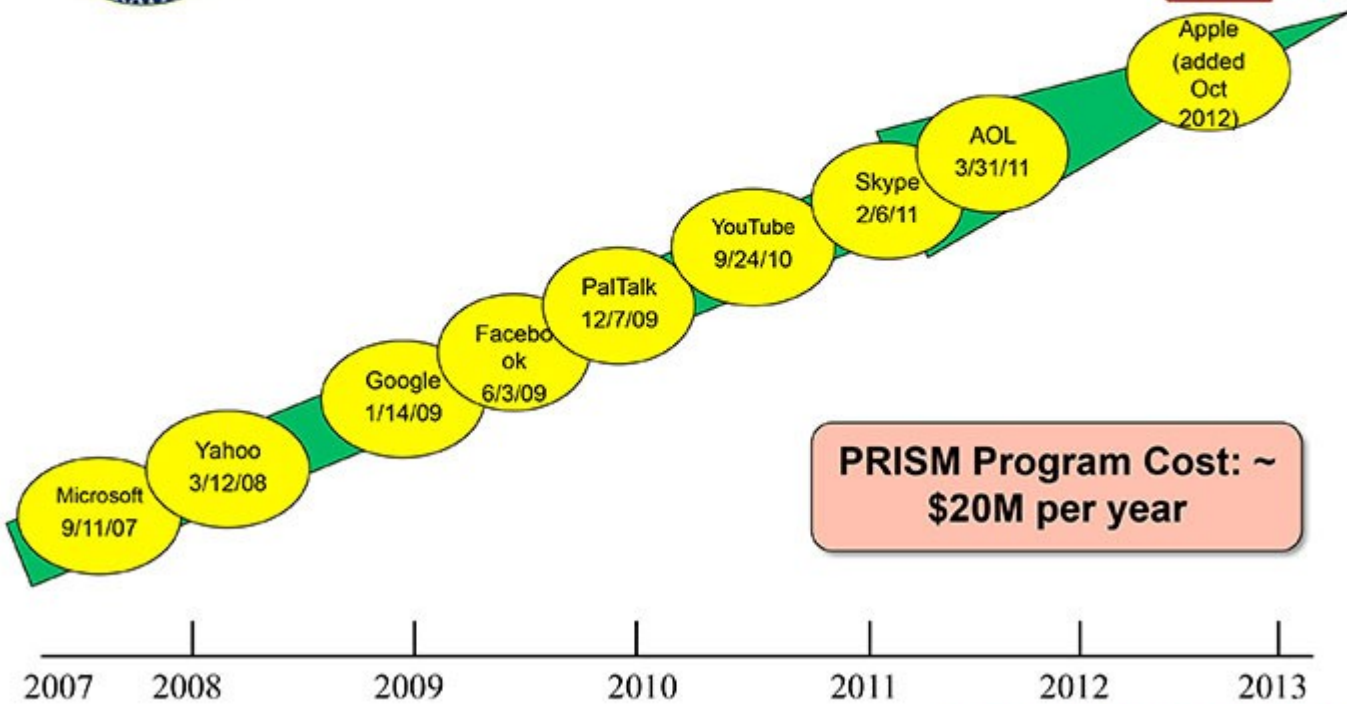
- **"On the record"**: all that is said can be quoted and attributed.
- **"Unattributable"**: what is said can be reported but not attributed.
- **"Off the record"**: the information is provided to inform a decision or provide a confidential explanation, not for publication.



<https://www.theguardian.com/film/2014/oct/11/citizenfour-review-snowden-vindicated-poitras-nsa-journalism>



(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ \$20M per year

OTR

- Off-The-Record messaging
- 2004, Nikita Borisov, Ian Goldberg, Eric Brewer. "Off-the-Record Communication, or, Why Not To Use PGP"
- (PGP is from 1991, basically RSA for email)



<https://otr.cypherpunks.ca/help/3.2.0/authenticate.php?lang=en>

Requirements, OTR vs. TLS...

- Forward secrecy
 - Both OTR and TLS care, for different reasons
- Deniable authentication *a.k.a.* off-the-record
 - TLS doesn't care about this, OTR does
- Future secrecy
 - TLS doesn't care about this, OTR does it by accident
- Out-of-order messages, parties offline for long periods of time, groups...
 - TLS doesn't need to worry about any of these, nor does OTR (Signal does)

Off-The-Record (OTR) Messaging

- Based on Diffie-Hellman and AES, and originally SHA-1
 - There are new versions
- Deniable Authentication
 - “Off the record” in journalism
- Forward secrecy
 - Ephemeral key exchange
- Future secrecy (not a design goal, but has it)

Deniable Authentication

- Concept of “malleability”
- Basic idea has two parts:
 - Hash the decryption key for a message, use the hash digest as an authentication key
 - Reveal the authentication key in the next message

Forward secrecy

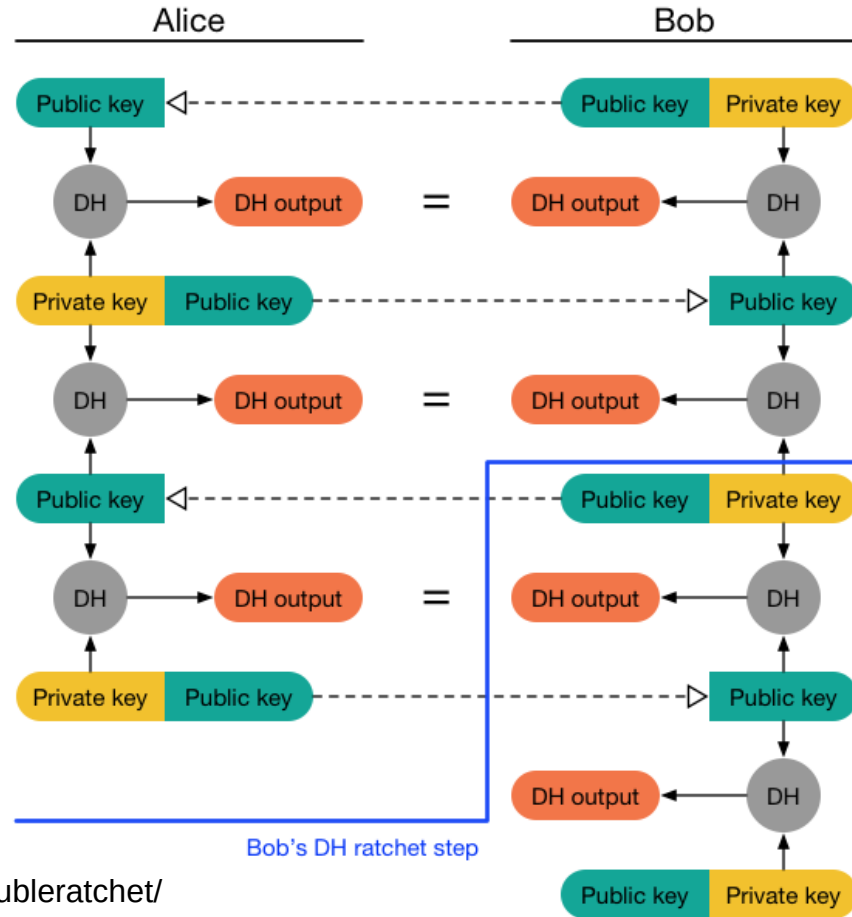
- If Alice or Bob's key is compromised, past messages cannot be decrypted by the adversary

Ratchet in sailing...



<https://www.westmarine.com/harken-snubbair-ratcheting-drum-19471861.html>

Forward Secrecy (ratchet)

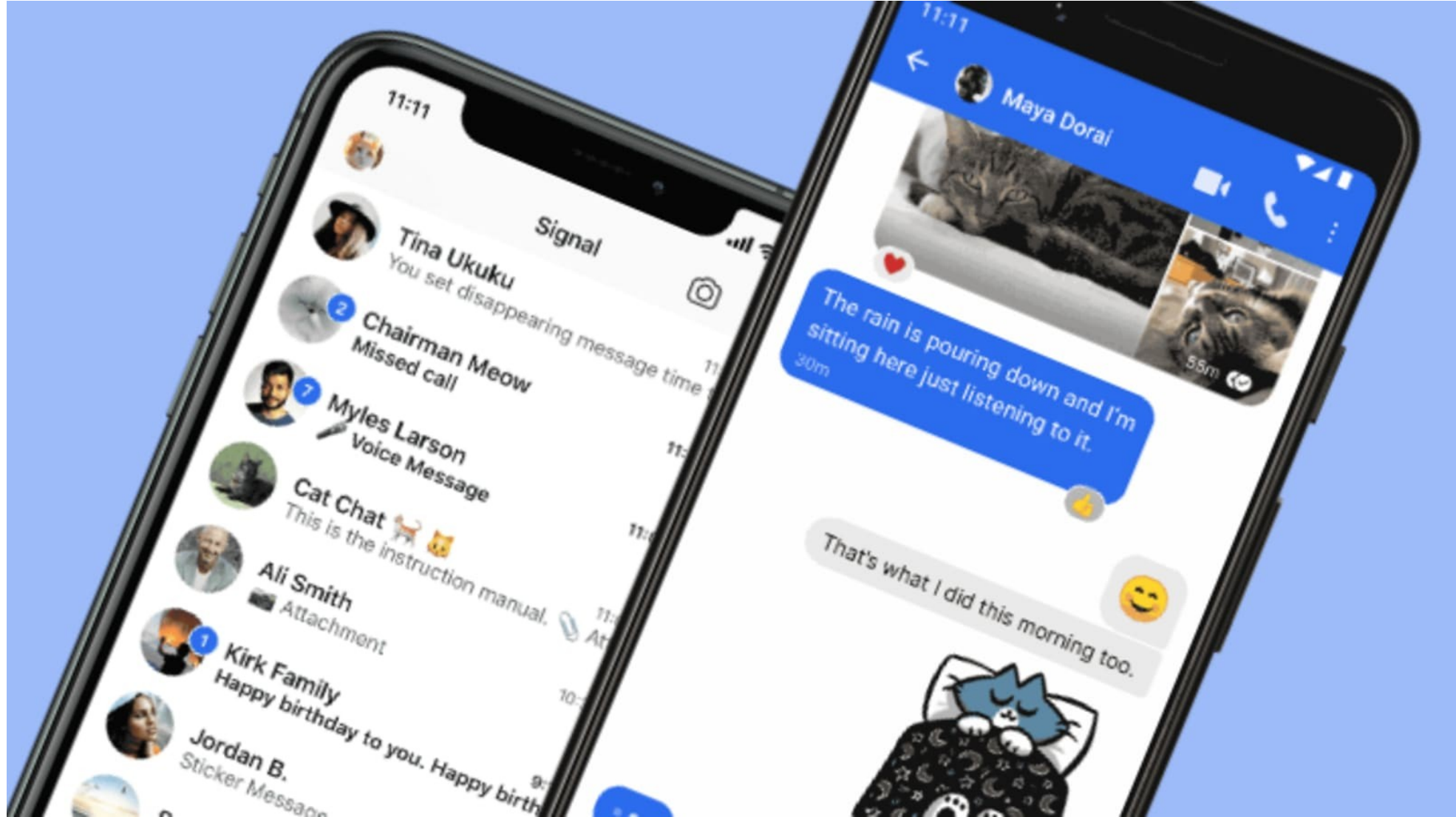


Future Secrecy

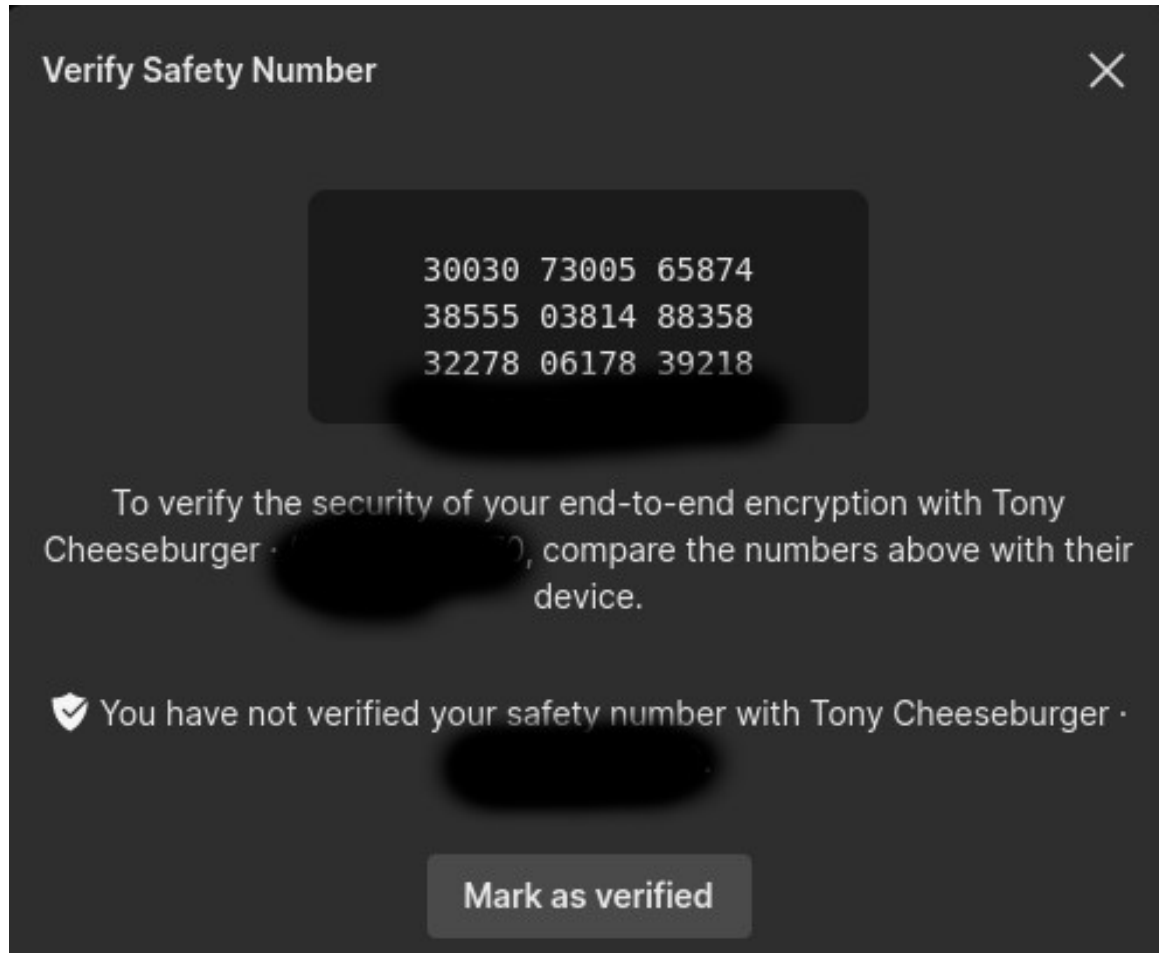
- *Future* secrecy is not the same as *forward* secrecy, and is in fact sometimes called *backward* secrecy
- If a private key is compromised, the attacker needs to intercept every message thereafter or else the crypto will “self heal”
- We get this for free because of the Diffie-Hellman key exchange every time we ratchet in OTR

Signal

- Multiple devices, some or all can be offline for long periods of time
- Group messages



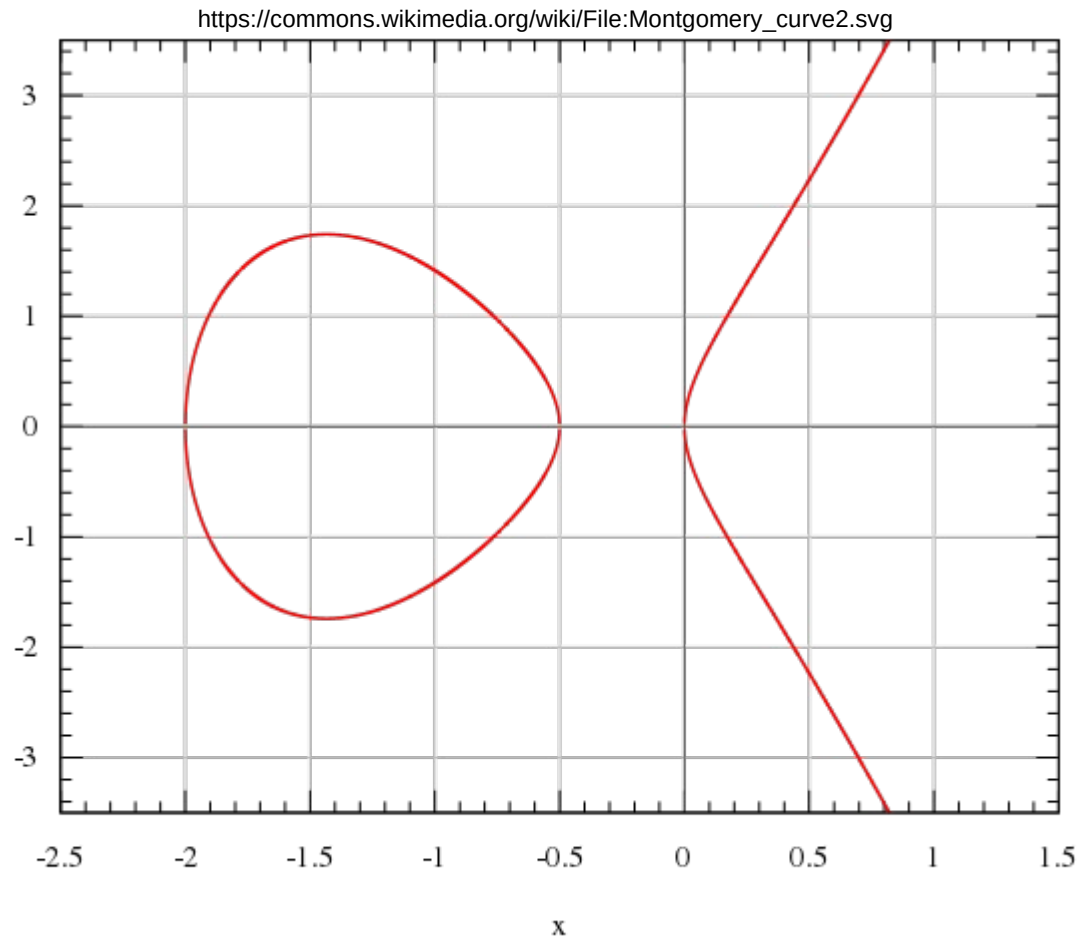
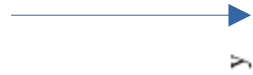
Typical authentication



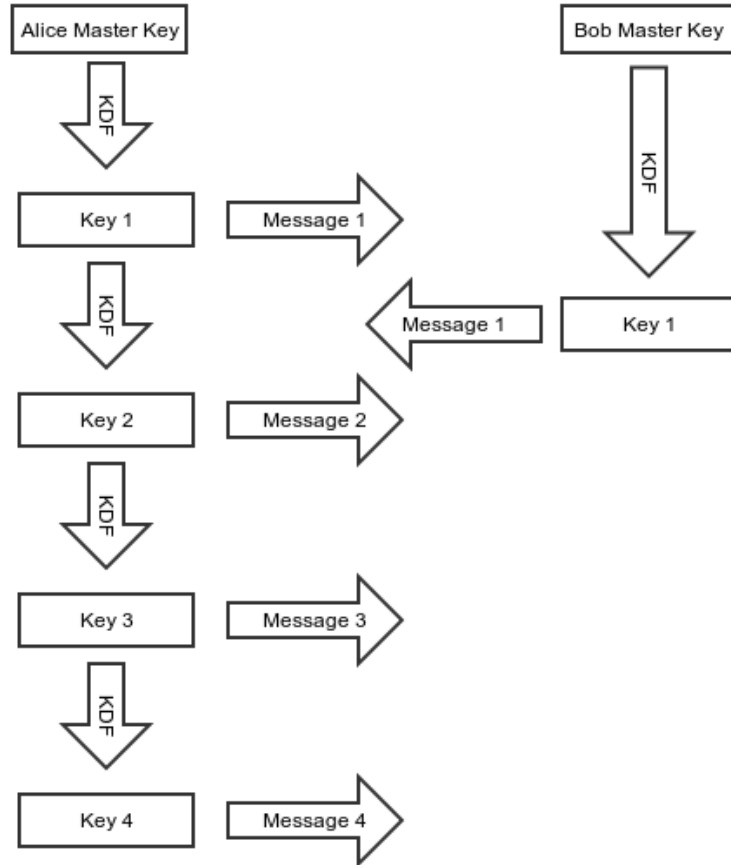
Signal encryption basics

- AES-256 in CBC mode
 - Why not a stream cipher?
- HMAC-256 with SHA-256 (SHA-2)
- Curve25519 for key exchange and signatures

Elliptic
Curve



Silent Circle SCIMP ratchet



Tradeoffs

- Both have forward secrecy, but SCIMP's is better
 - In synchronous case, can ratchet and delete old key right away if Bob acknowledges it and ratchets, too
- OTR ratchet not great for multiple devices, devices that go offline
- SCIMP ratchet leaves key material around for a long time if messages are lost or out of order
- OTR ratchet “self heals”, *i.e.*, future/backward secrecy

X3DH

IK = Identity Key

EK = Ephemeral Key

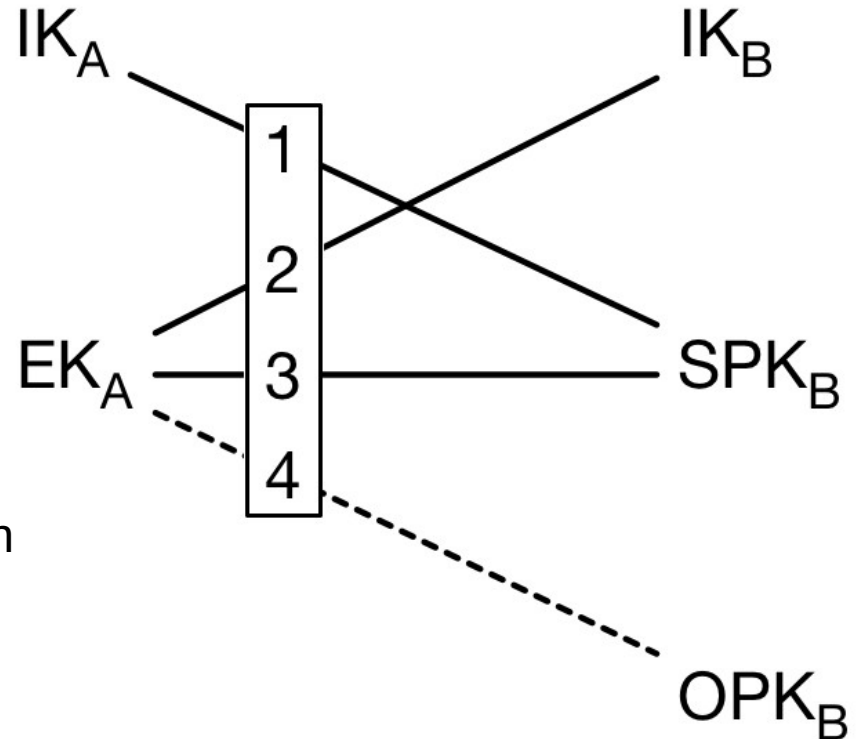
SPK = Signed Pre-Key

OPK = One-Time Pre-Key

$SK = KDF(DH1 \parallel DH2 \parallel DH3 \parallel DH4)$

Alice's first message encrypts the two on the left, authentication for Bob's SPK comes from the signature.

Deniability?





Monitor your web services
for cyber threats with the
CrowdSec Console

[Sign Up Now](#)

Signal Messenger Introduces PQXDH Quantum-Resistant Encryption

📅 Sep 20, 2023 👤 THN

Encryption / Privacy



Foster
collaboration
between
ITops and
SecOps using
**Endpoint
Central.**



ManageEngine
Endpoint Central

[FREE TRIAL](#)



Two key differences with Signal:
-Federated
-No deniability

Messaging Layer Security (MLS)



Messaging Layer Security (MLS) is an IETF working group building a modern, efficient, secure group messaging protocol.

[View My GitHub Profile](#)

Resources

- <https://signal.org/blog/advanced-ratcheting/>
- https://en.wikipedia.org/wiki/Off-the-Record_Messaging
- https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm
- <https://signal.org/docs/specifications/doubleratchet/>
- <https://signal.org/docs/specifications/x3dh/>
- <https://www.youtube.com/watch?v=7WnwSovjYMs>
- [https://en.wikipedia.org/wiki/Global_surveillance_disclosures_\(2013%E2%80%93present\)](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present))
- [https://en.wikipedia.org/wiki/Global_surveillance_disclosures_\(2013%E2%80%93present\)](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present))
- <https://thehackernews.com/2023/09/signal-messenger-introduces-pqxdh.html>