OTR (review) and Signal

CSE 539 Spring 2023

jedimaestro@asu.edu

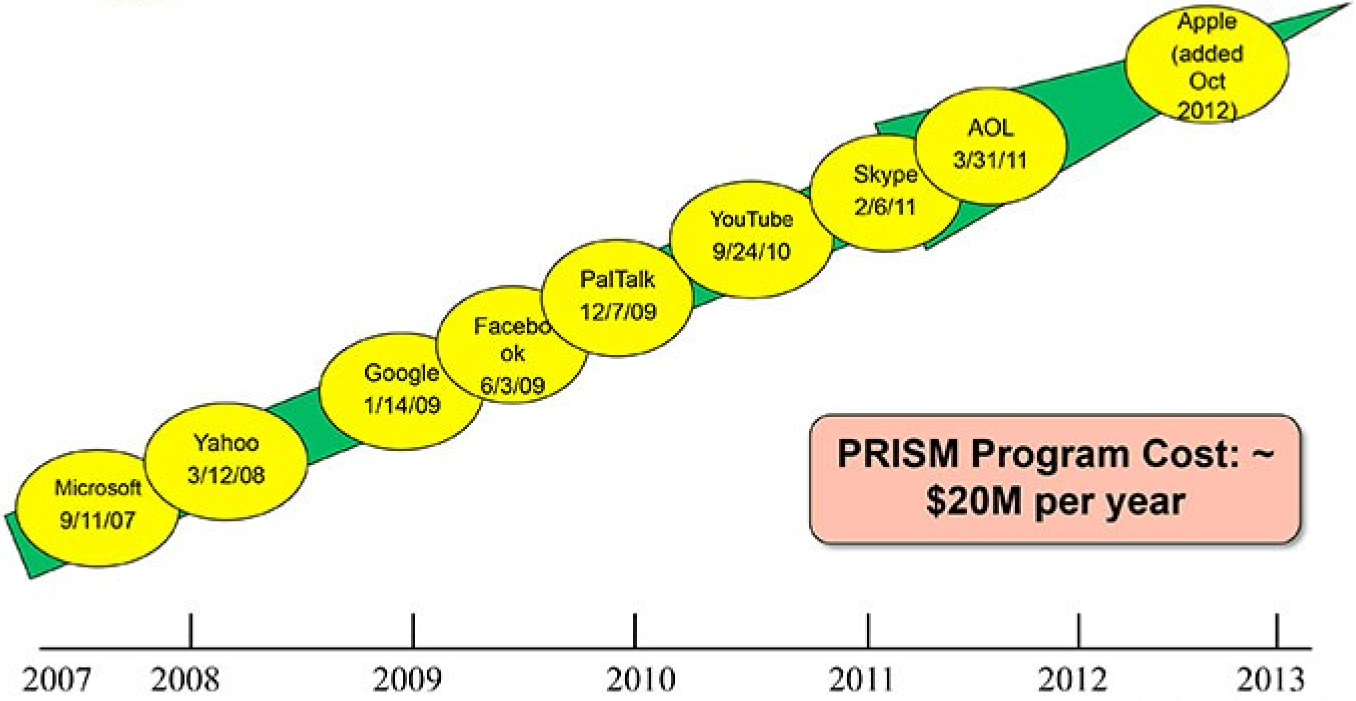
https://en.wikipedia.org/wiki/Source_(journalism)

- **"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- **"Off the record"**: the information is provided to inform a decision or provide a confidential explanation, not for publication.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

TOP SECRET//SI//ORCON//NOFORN

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



Microsoft 9/11/07

Yahoo 3/12/08

Google 1/14/09

Facebo ok 6/3/09

PalTalk 12/7/09

YouTube 9/24/10

Skype 2/6/11

AOL 3/31/11

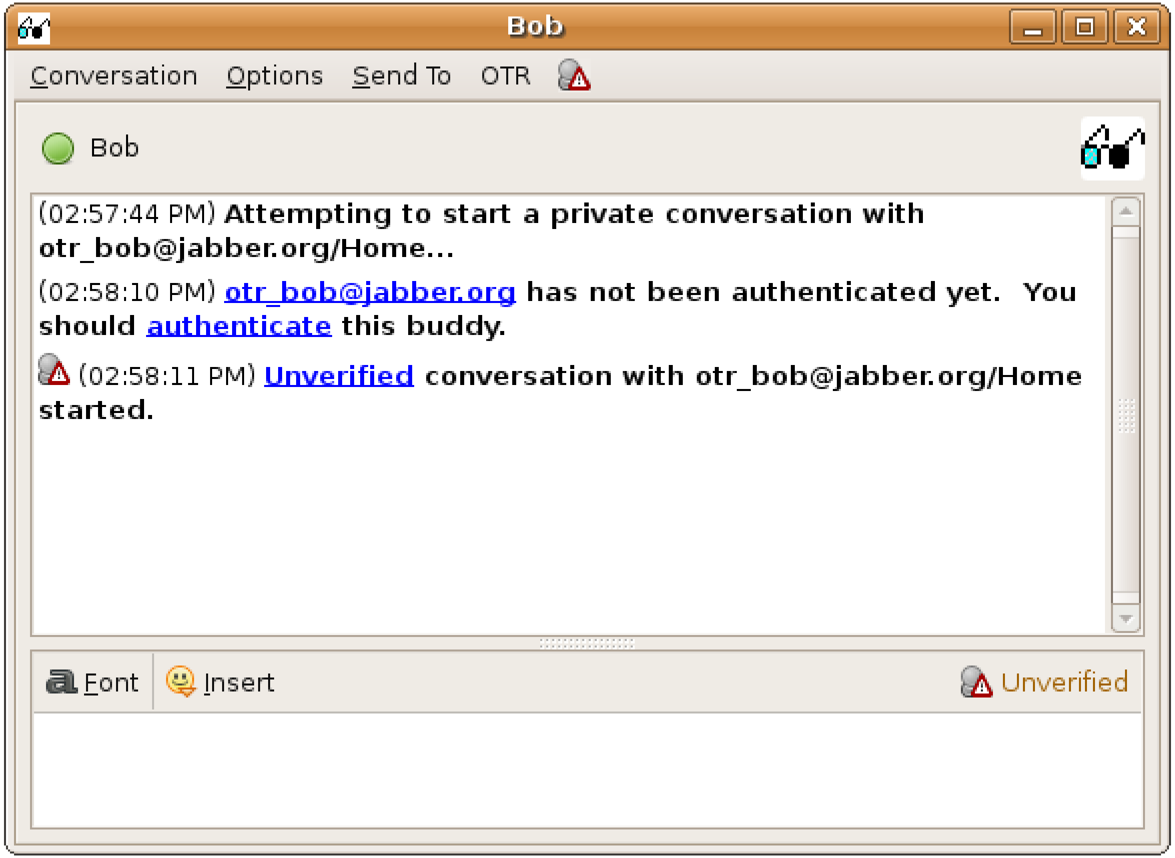
Apple (added Oct 2012)

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

OTR (review)

- 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)



(02:57:44 PM) **Attempting to start a private conversation with otr_bob@jabber.org/Home...**

(02:58:10 PM) **otr_bob@jabber.org has not been authenticated yet. You should authenticate this buddy.**

(02:58:11 PM) **Unverified conversation with otr_bob@jabber.org/Home started.**

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)

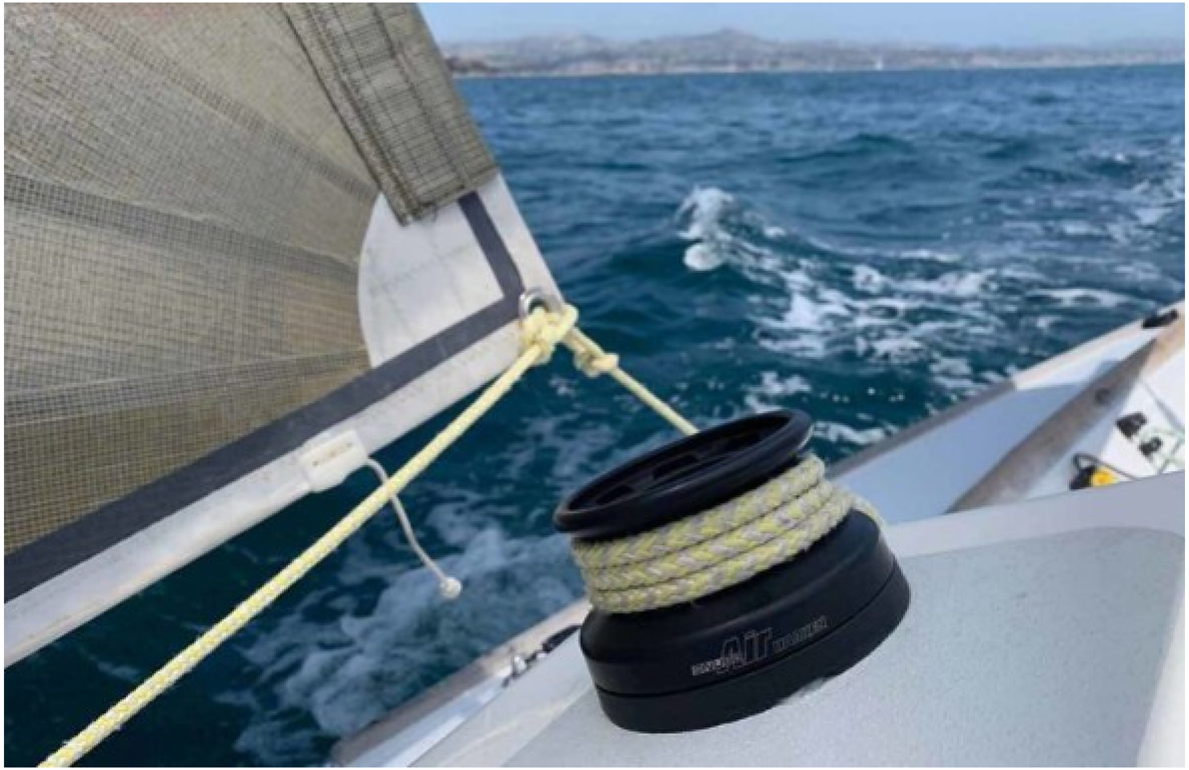
Deniable Authentication

- 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

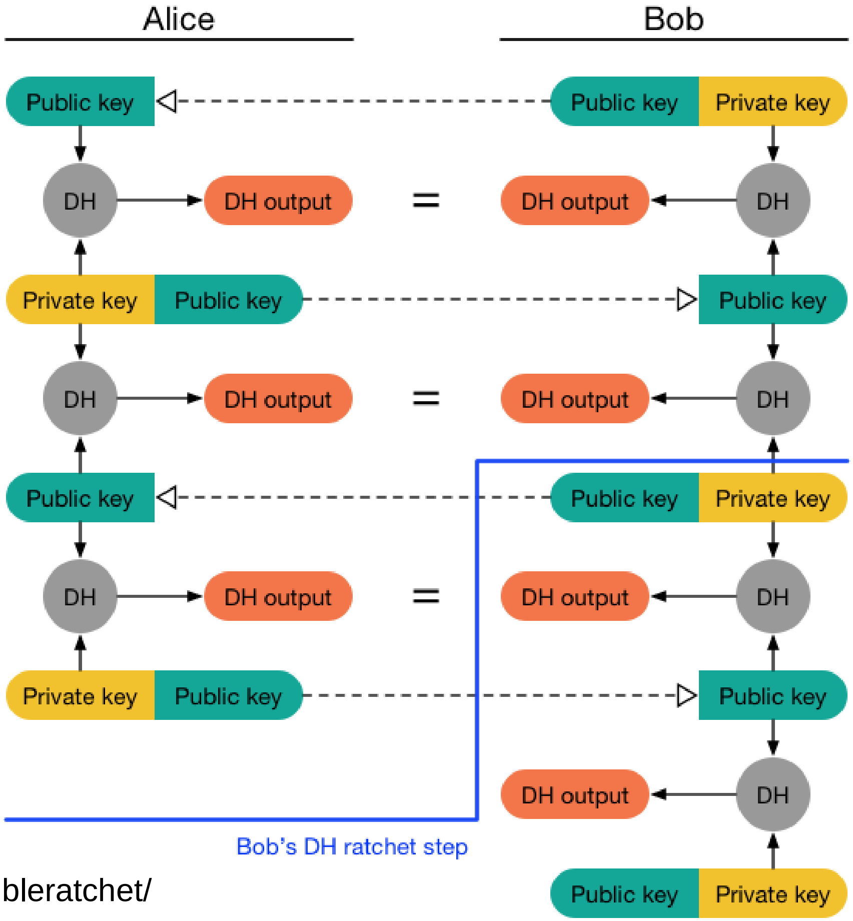
- If Alice or Bob’s key is compromised, past messages cannot be decrypted by the adversary

Ratchet in sailing...



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

Forward Secrecy (ratchet)



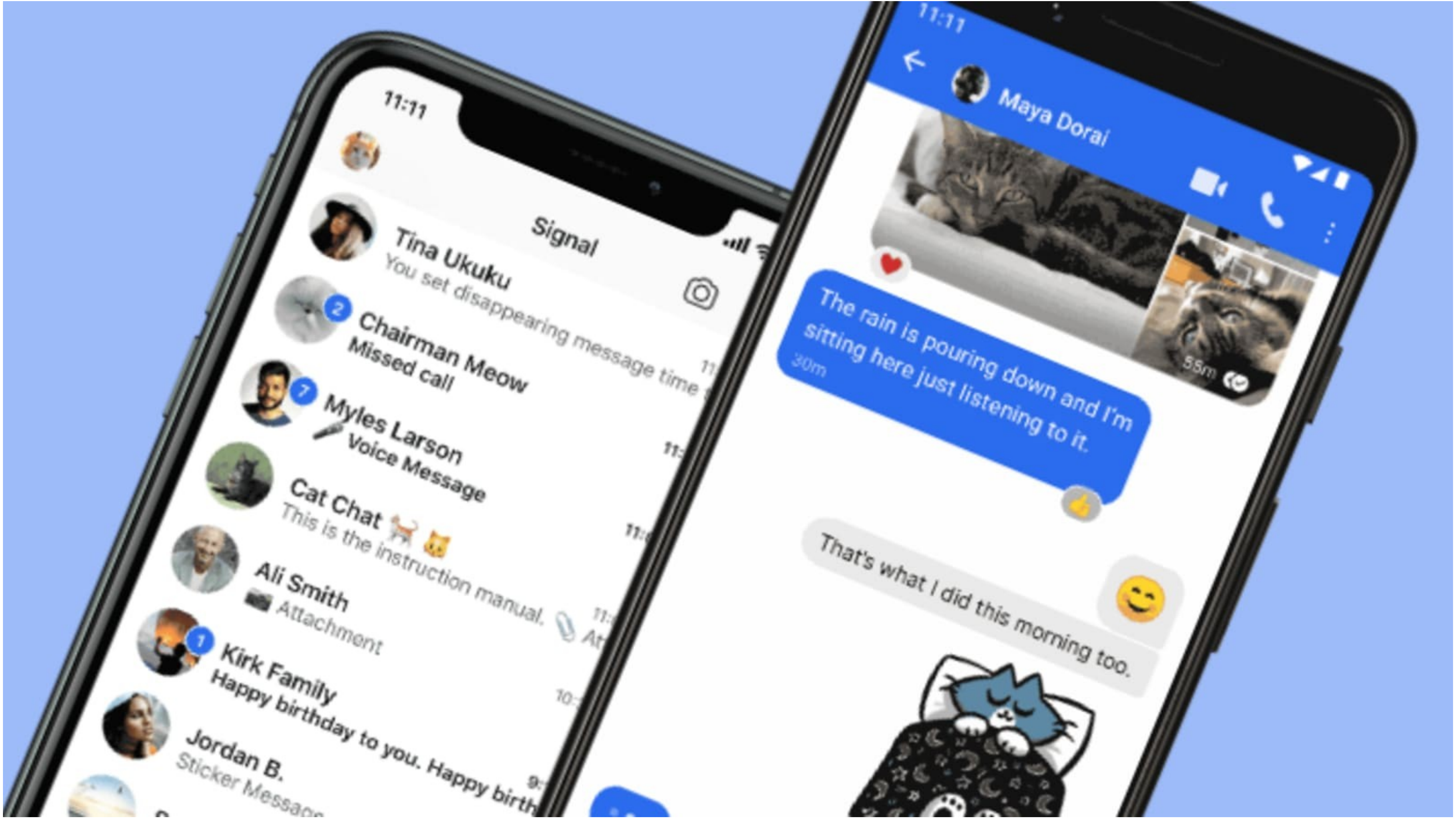
https://signal.org/docs/specifications/doubleratchet/

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



Tina Ukuku
You set disappearing message time

Chairman Meow
Missed call

Myles Larson
Voice Message

Cat Chat 🐈 🐱
This is the instruction manual. 📎 At

Ali Smith
Attachment

Kirk Family
Happy birthday to you. Happy birth

Jordan B.
Sticker Message

Maya Dorai

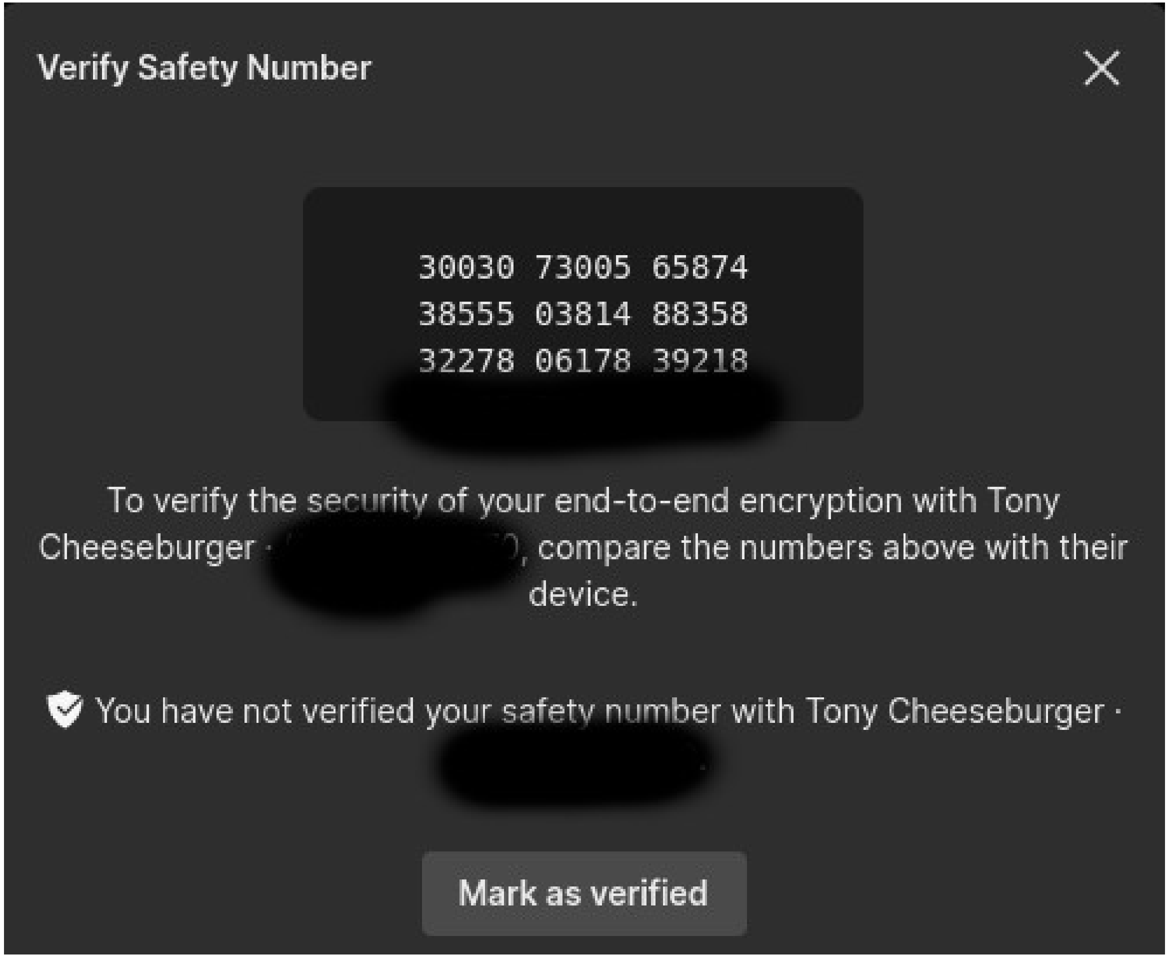
55m

The rain is pouring down and I'm sitting here just listening to it.
30m

That's what I did this morning too.

https://www.cnbc.com/2021/01/12/how-to-use-signal-instead-of-whatsapp.html

Typical authentication



Verify Safety Number

```
30030 73005 65874
38555 03814 88358
32278 06178 39218
```

[redacted]

To verify the security of your end-to-end encryption with Tony Cheeseburger · [redacted], compare the numbers above with their device.

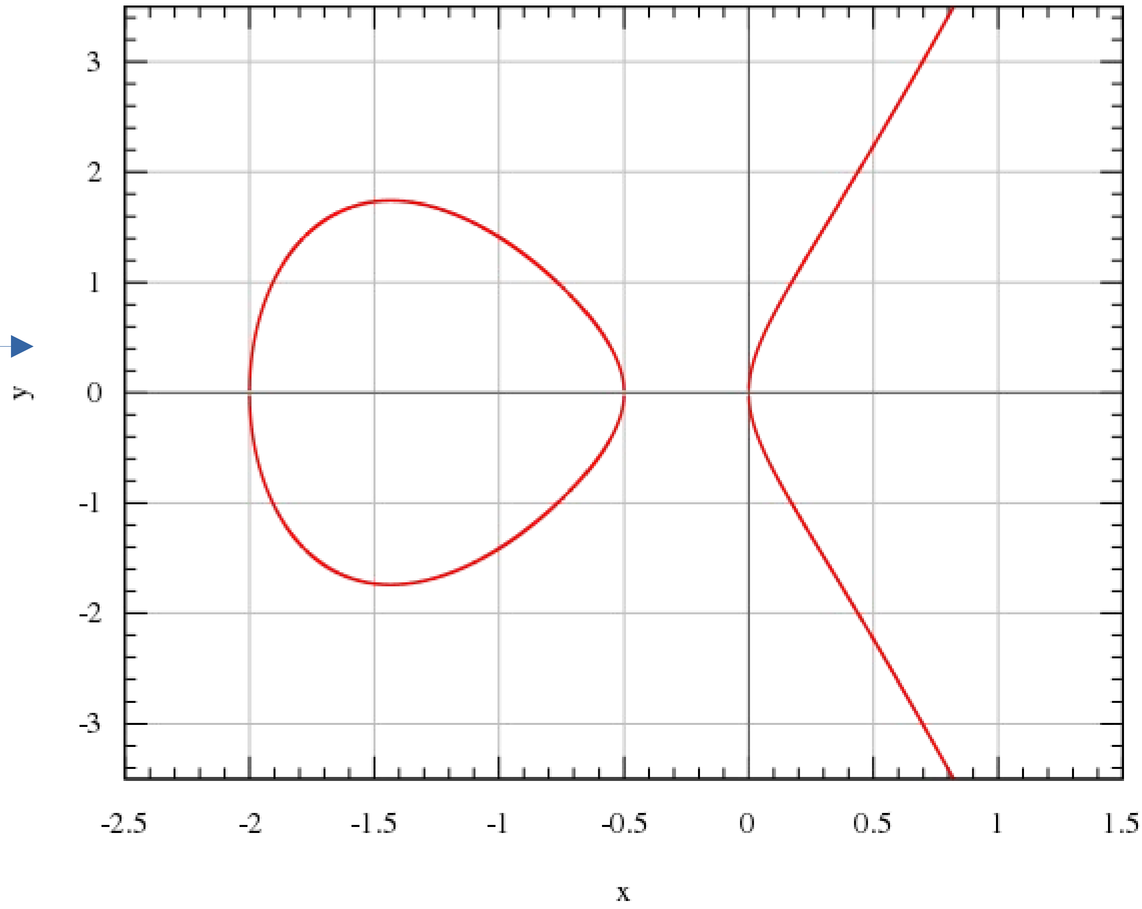
✓ You have not verified your safety number with Tony Cheeseburger · [redacted]

Signal encryption basics

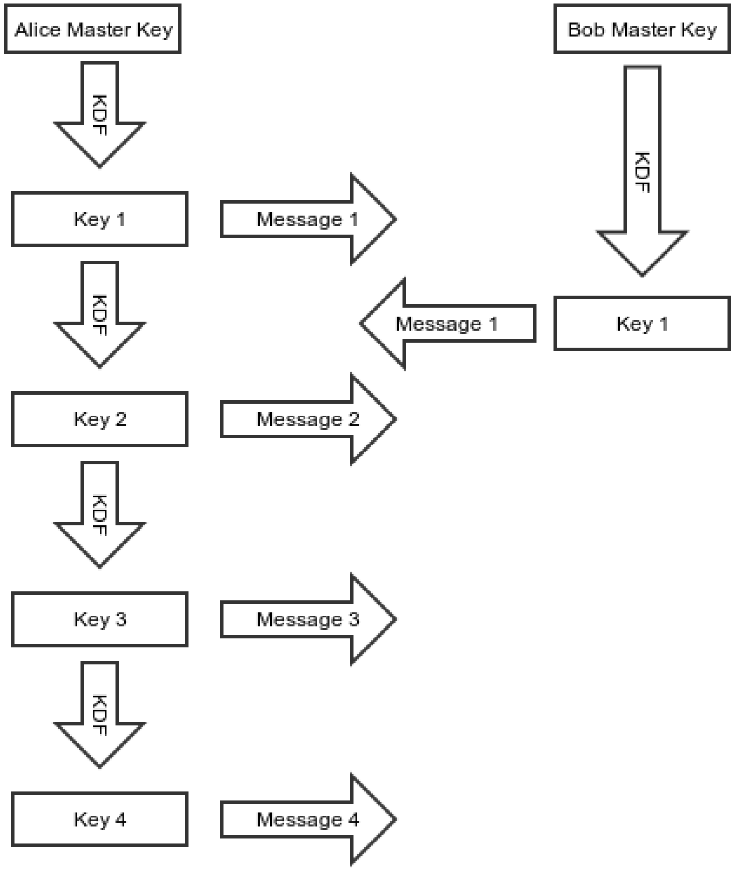
- AES-256 in CBC mode
  - Why not a stream cipher?
- HMAC-256 with SHA-256 (SHA-2)
  - Why not Gallois Counter Mode (which is SHA-3)?
- Curve25519 for key exchange and signatures

Elliptic Curve

https://commons.wikimedia.org/wiki/File:Montgomery_curve2.svg



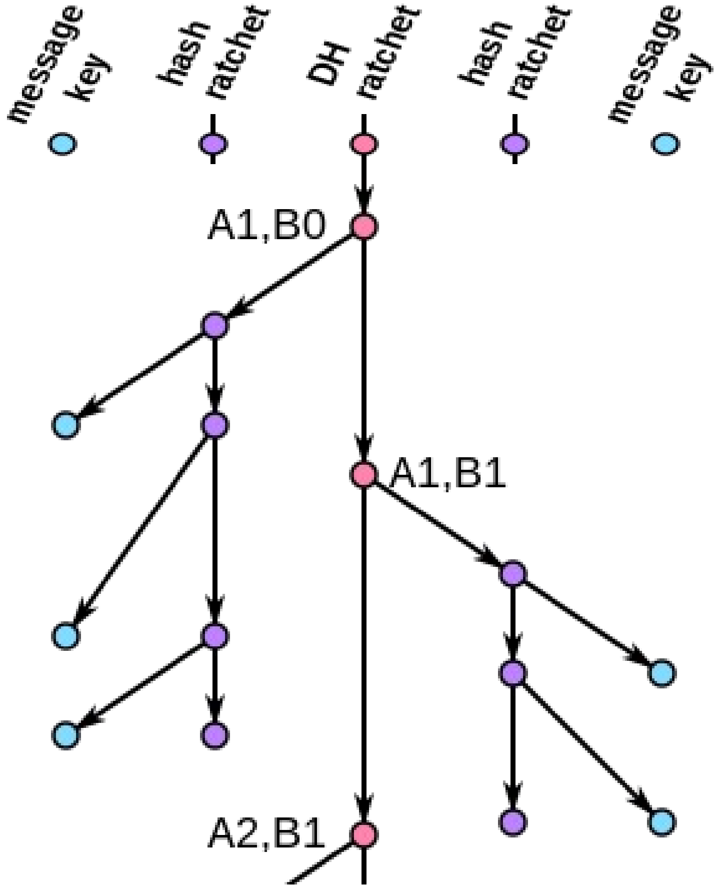
Silent Circle SCIMP ratchet



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 sececy

Double Ratchet



https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm

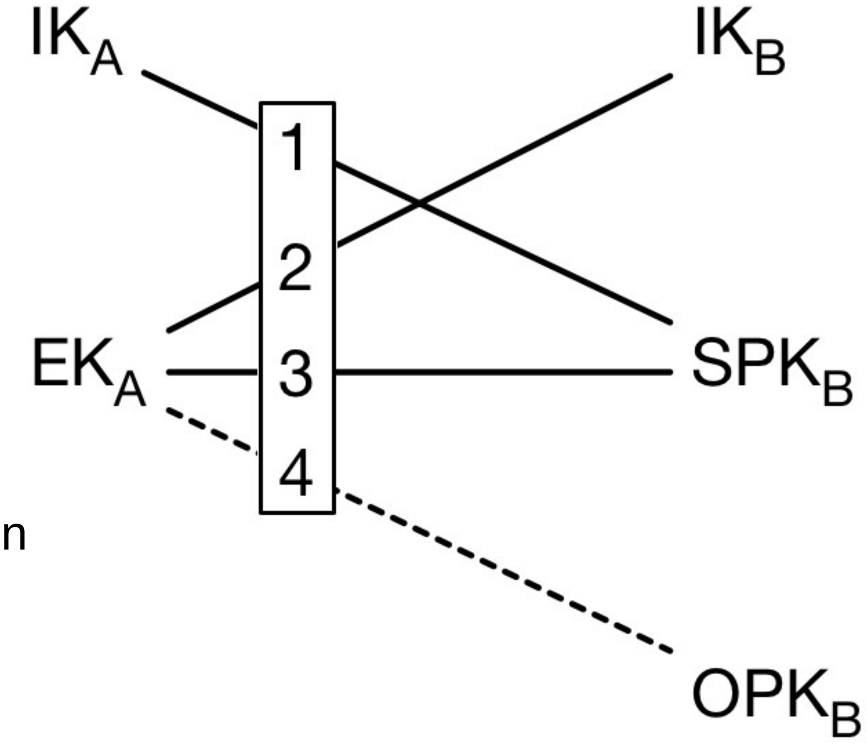
X3DH

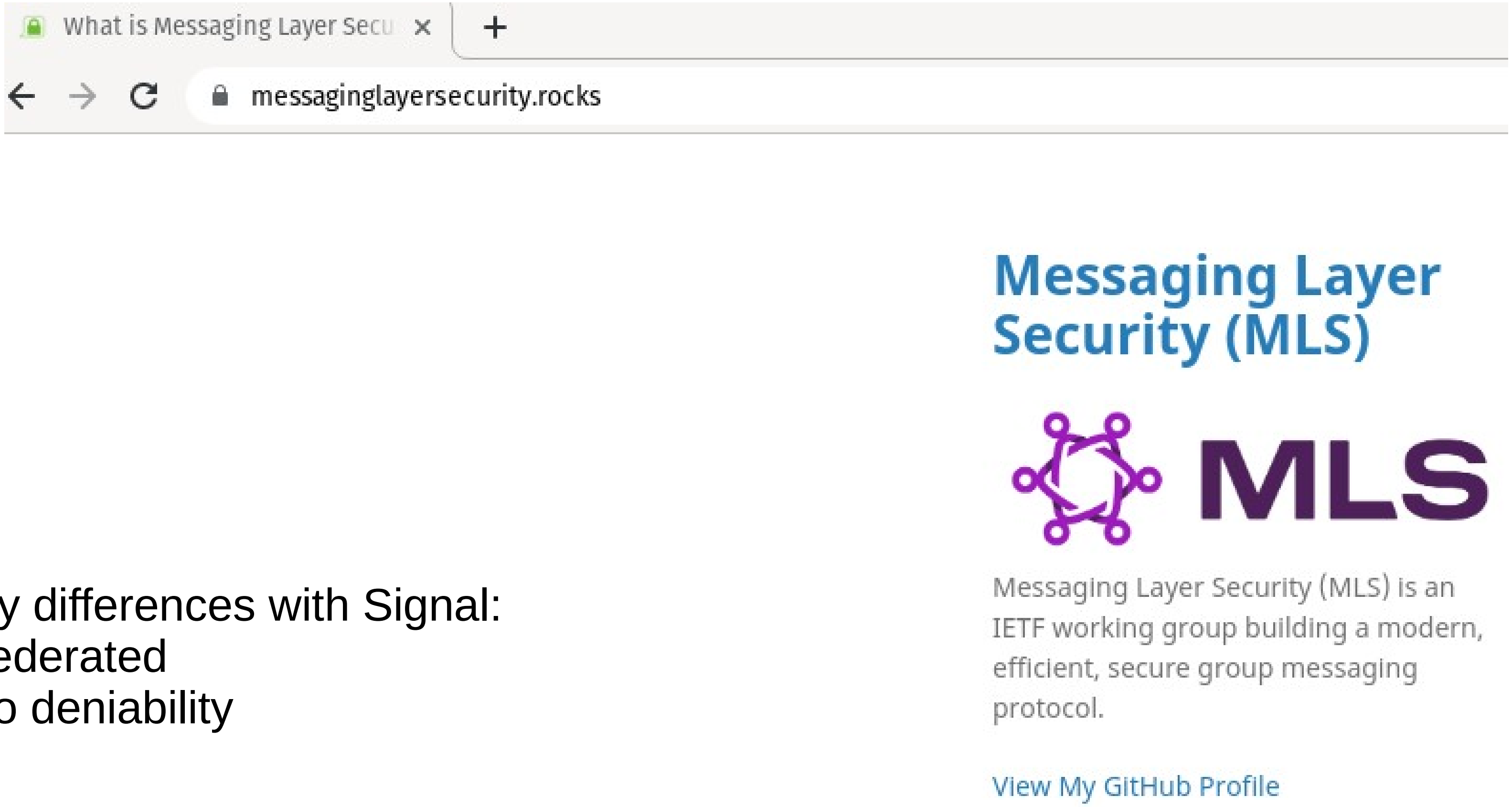
IK = Identity Key
EK = Ephemeral Key
SPK = Signed Pre-Key
OPK = One-Time Pre-Key

SK = KDF(DH1 || DH2 || DH3 || DH4)

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

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

Two key differences with Signal:

- Federated
- No deniability

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)