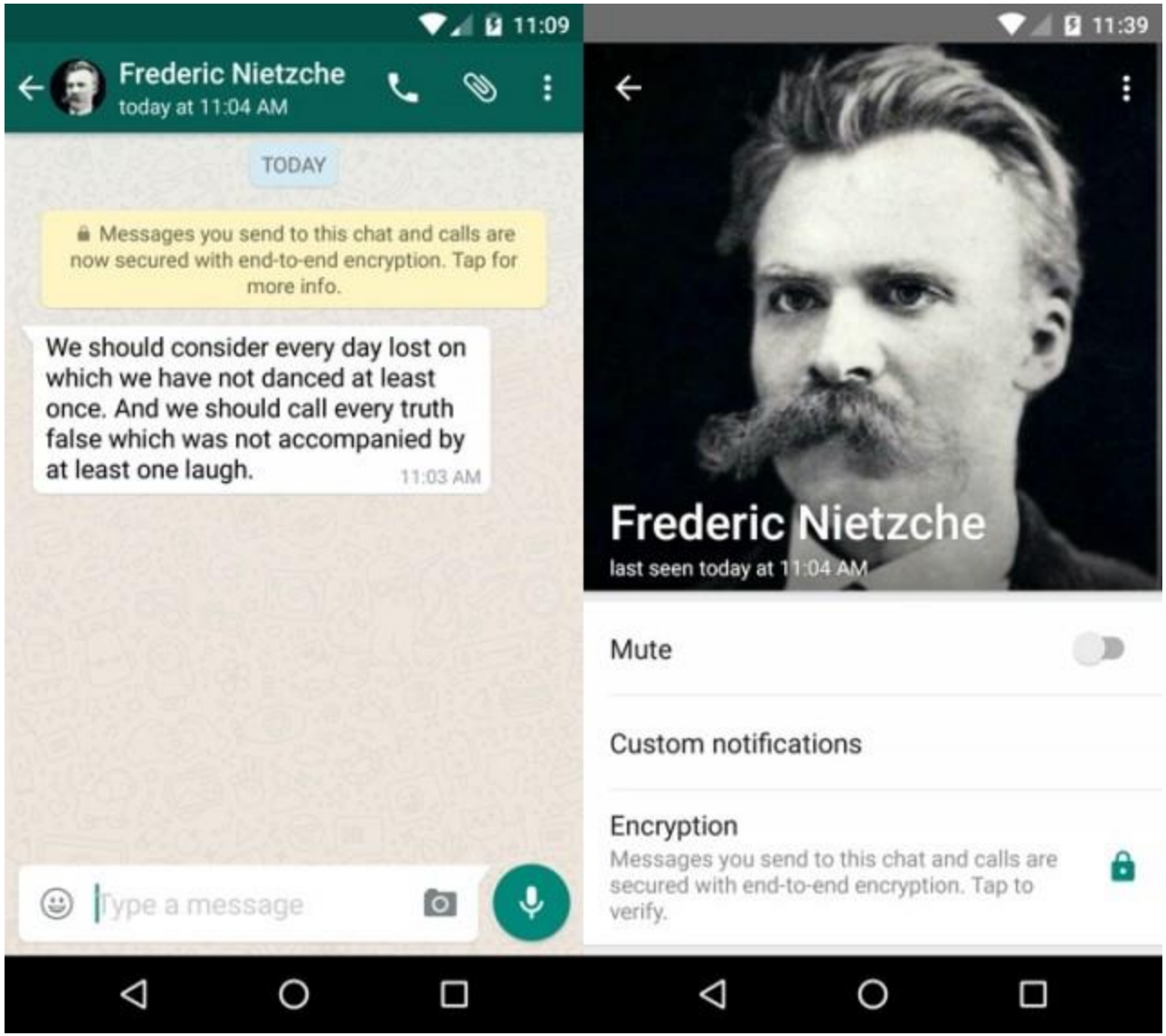
Encrypted Messaging Systems

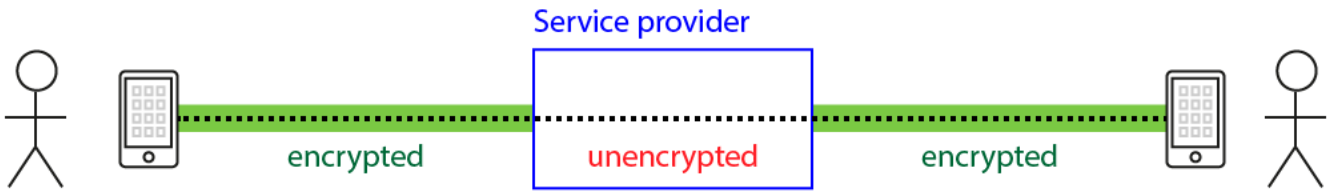
CS 558, Network Security
Boston University
Prof. Sharon Goldberg
May 2, 2017



https://mybroadband.co.za/news/security/160824-how-whatsapp-keeps-your-messages-secret.html

“end-to-end” encryption

Fig. 1a: Encryption in transit



e.g. TLS, email

Fig. 1b: End-to-end encryption

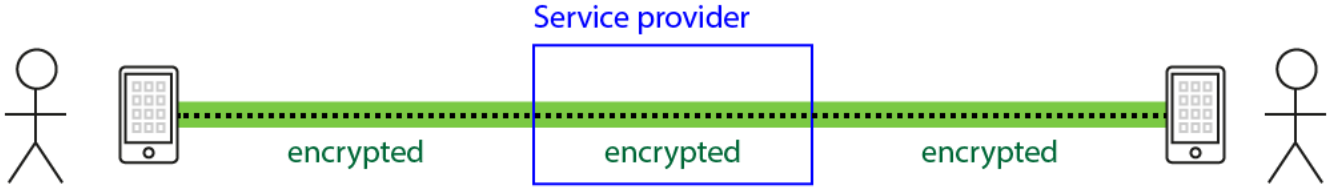
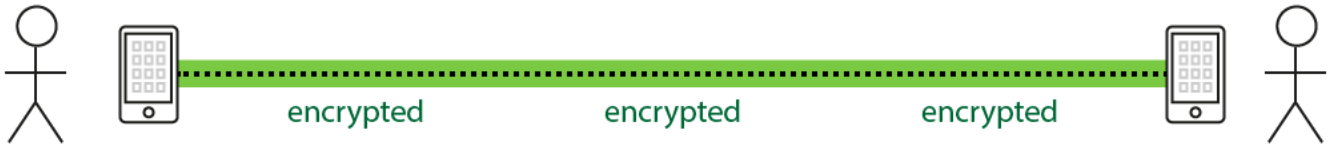


Fig. 1c: End-to-end encryption (no service provider)



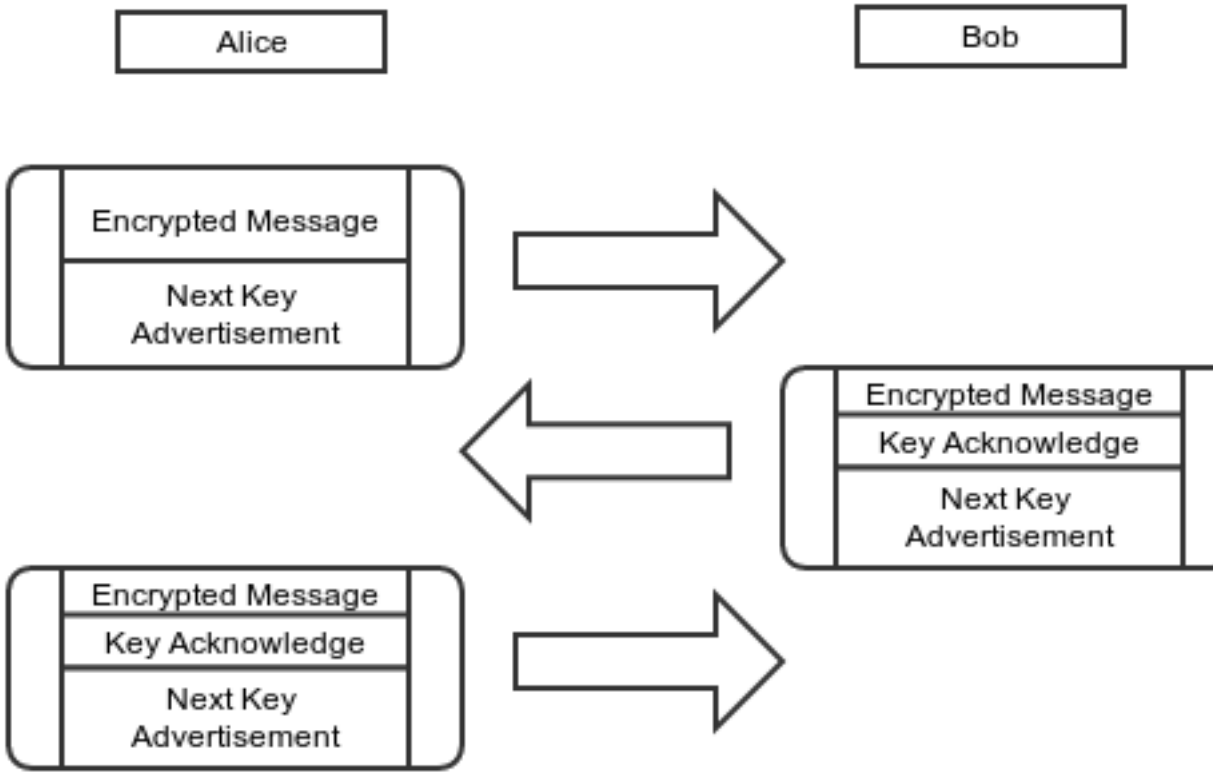
https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/

We look at the signal protocol

All figures and text from:

https://whispersystems.org/blog/advanced-ratcheting/

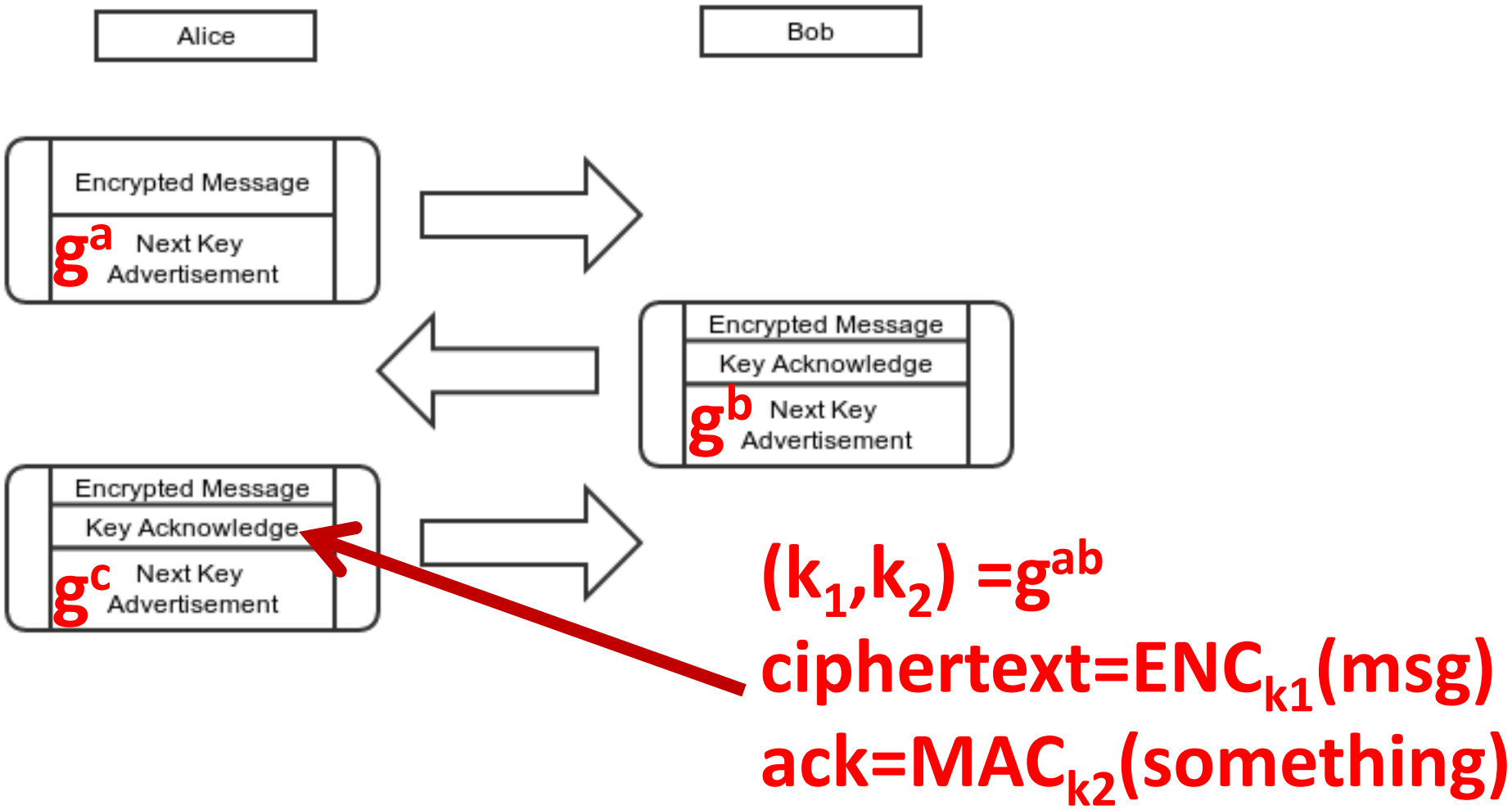
the OTR 3-step Diffie-Hellman ratchet

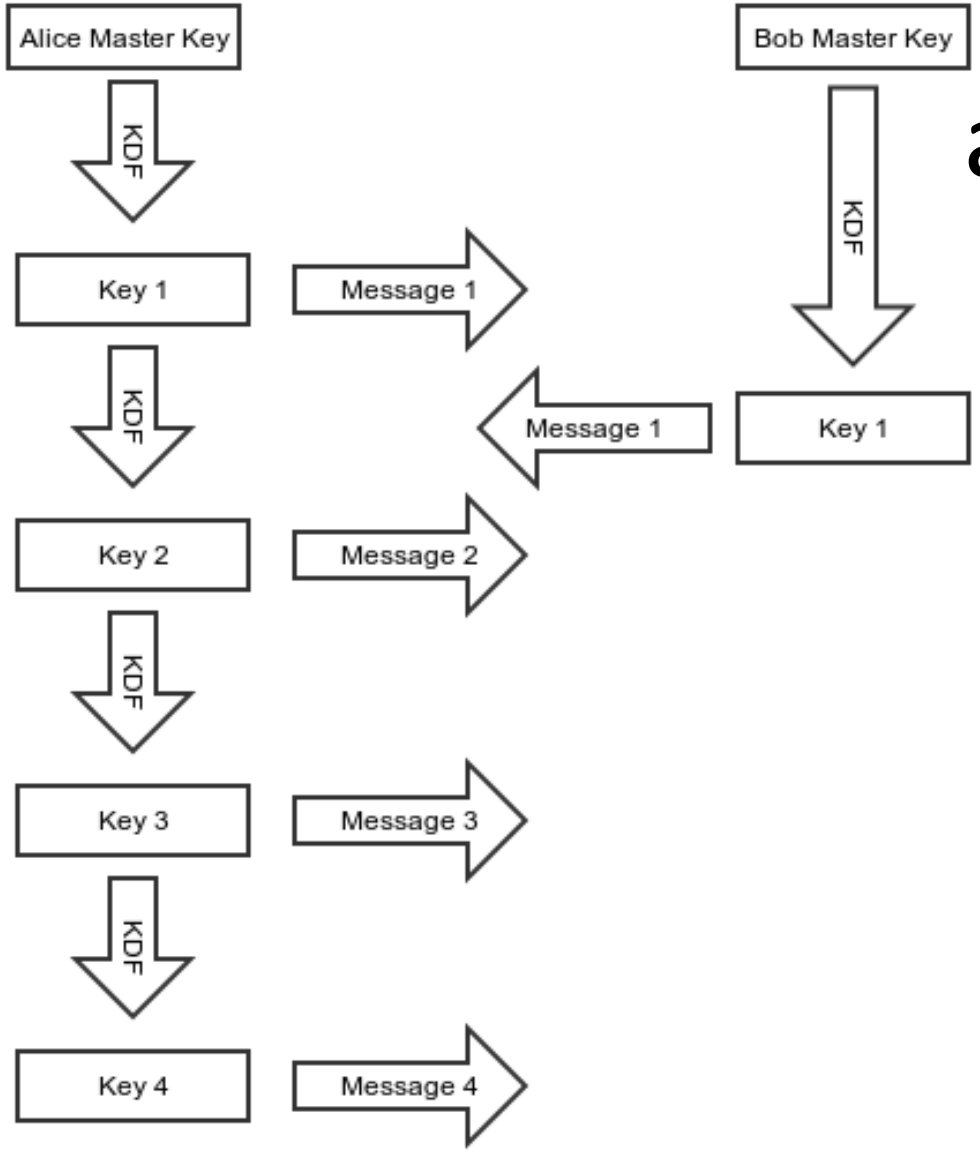



```
struct {
  opaque sender_key_id[4];
  opaque receiver_key_id[4];
  opaque next_key_id[4];
  opaque next_key[32];
  opaque ciphertext[...];
  opaque mac[10];
} OTR_Message;
```

Given the nature of a "three step" ratchet, if a sender transmits something to a receiver, and the receiver doesn't respond for a few days, the sender has to keep the key material used to encrypt that message around for *days*.

the OTR 3-step Diffie-Hellman ratchet



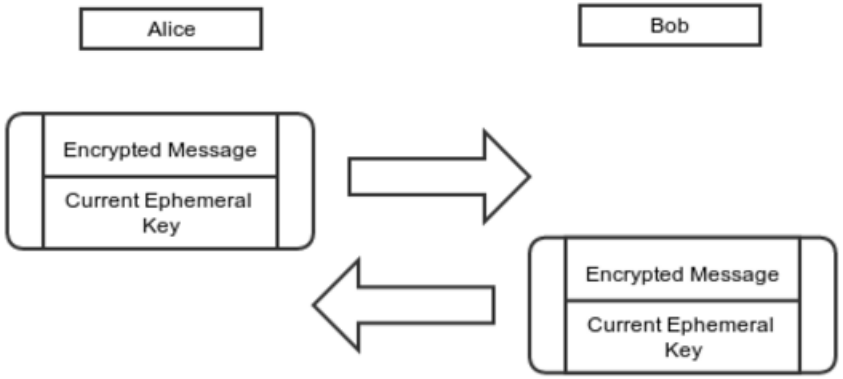


asynch hash ratchet

That key material is sensitive, however, because it can be used to calculate the key material for *every subsequent sequence number*. So a client can't hang on to it forever,

Signal 2-step DH Ratchet (“Chain Keys”)

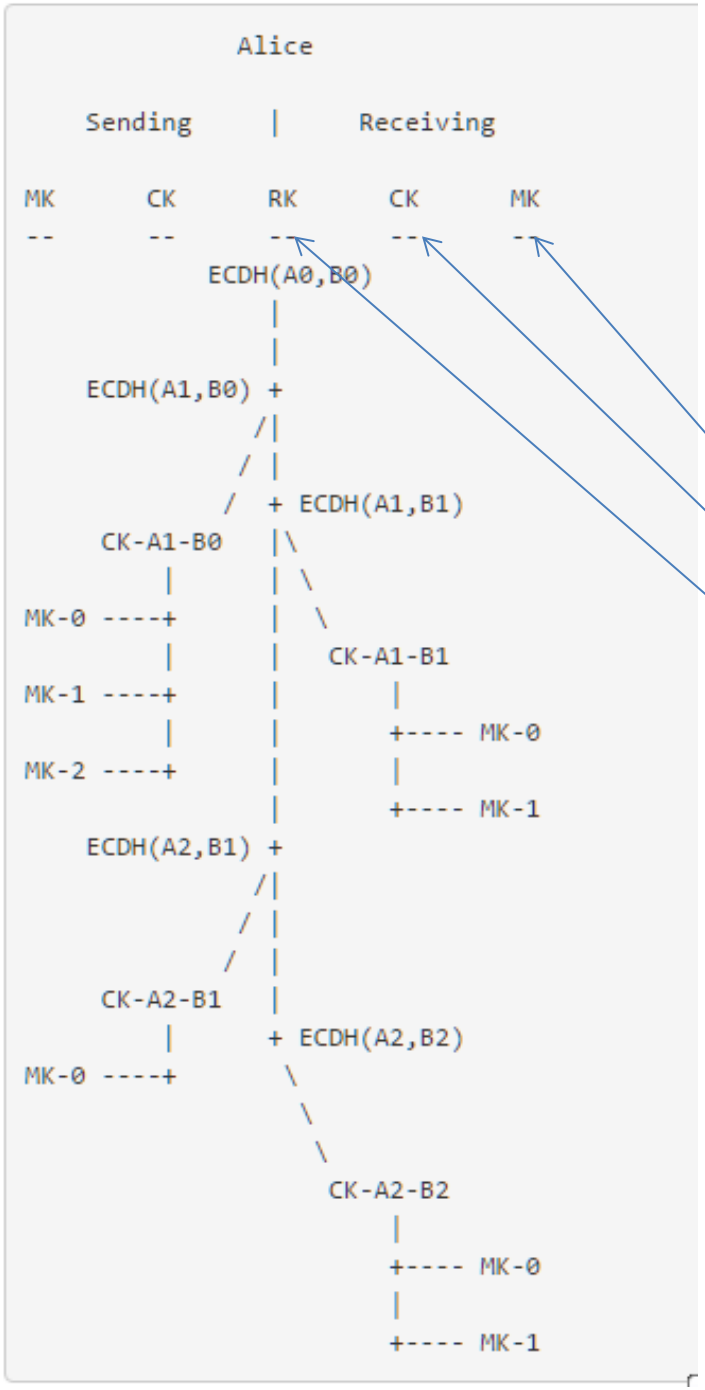
1. Alice generates a new ECDH ephemeral key `A1` and uses it immediately to send a message.
2. Alice receives a message with Bob's new ECDH ephemeral `B1` and can then destroy `A1` and generate `A2` when sending her next message.



This is a best possible case DH ratchet, and it also greatly simplifies the message format, which is now simply:

```
struct {
  opaque sender_ephemeral[32];
  opaque body[...]
  opaque mac[10]
}
```

It also eliminates all the key ID book keeping.



Add a hash-based ratchet between chain keys

Message Key

Chain Key

Root key

The final message format is simply:

```
struct {
  opaque sender_ephemeral_key[32];
  opaque counter[3];
  opaque mac[10];
}
```

But the “metadata” leaks!

Metadata [edit]

The Signal Protocol does not prevent a company from retaining information about when and with whom users communicate.[19][20] There can therefore be differences in how messaging service providers choose to handle this information. For example, WhatsApp's privacy policy states:

> WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information which WhatsApp is legally compelled to collect.[20][21][*needs update?*]

Signal's privacy policy states that recipients' identifiers are only kept on the Signal servers as long as necessary in order to transmit each message.[22] In June 2016, Moxie Marlinspike told *The Intercept* that "the closest piece of information to metadata that the Signal server stores is the last time each user connected to the server, and the precision of this information is reduced to the day, rather than the hour, minute, and second."[20]


THEY'RE ONLY COLLECTING
"METADATA"
memegenerator.net

NYR Daily

‘We Kill People Based on Metadata’

David Cole

Rick Bowmer/AP Photo

The National Security Agency’s $1.5 billion data storage facility in Bluffdale, Utah, June 2013

Content vs Metadata in the Law

- Metadata typically receives a less legal protection than content due to a decision made in *Smith v. Maryland,* 442 U.S. 735 (1979), http://caselaw.findlaw.com/us-supreme-court/442/735.html
- See also: Joseph D. Mornin, "NSA Metadata Collection and the Fourth Amendment ," *Berkeley Technology Law Journal* 29, no. 4 (August 1, 2014), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2042&context=btlj;
- Robert S. Litt, "The Fourth Amendment in the Information Age ," *Yale Law Journal* 126 (April 27, 2016), http://www.yalelawjournal.org/forum/fourth-amendment-information-age;
- Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law," *Harvard Journal of Law and Technology* 30, no. 1 (Fall 2016), jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf; and Orin Kerr, "Relative vs. Absolute Approaches to the Content/Metadata Line," LAWFARE, August 25, 2016, https://www.lawfareblog.com/relativevs-absolute-approaches-contentmetadata-line.

Computer Scientist on Content vs Metadata

- For a study about sensitivity of telephone metadata, see Jonathan Mayer and Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata," Web Policy, March 12, 2014, http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.
- For mobility metadata, see Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility," *Scientific Reports* 3, Article number: 1376 (2013), http://www.nature.com/articles/srep01376 .
- For opinions about the sensitivity of metadata from computer scientists, see Matt Blaze,"Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)," *Wired,* June 19, 2013, https://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/;
- Jane Mayer, "What's the Matter with Metadata?" *New Yorker,* June 6, 2013, http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata; or
- "Written Testimony of Edward W. Felten Professor of Computer Science and Public Affairs, Princeton University," United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013, http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf.