7.1 Signal Protocol (Extra Reading)

For interest only.

The Signal protocols is used to provide key management for end-to-end encryption in messaging applications (like WhatsApp).

Given what we have done so far you can look at what is a modern, complex applied cryptography design. I think that most of what they mention you can start to recognize some things from what we did: Diffie-Hellman (although Elliptic Curve) and HMAC.

I made a summary of it in a few slides:

Signal Encrypted Messaging.pdf

Knowing how Elliptic curve works is not important to understand the overall Signal design, but if you do want to look into it briefly then see:

https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

If you want to see the original source:

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

If you are interested in crypto and messaging, including group messaging, you can watch these computerphile videos:

Messaging/crypto: https://www.youtube.com/watch?v=DXv1boalsDI

Double ratchet: https://www.youtube.com/watch?v=9sO2qdTci-s

Group messaging: https://www.youtube.com/watch?v=Q0_lcKrUdWg