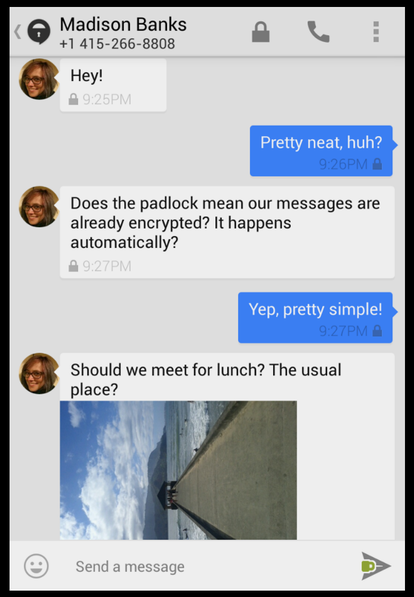
OPEN

whispersystems

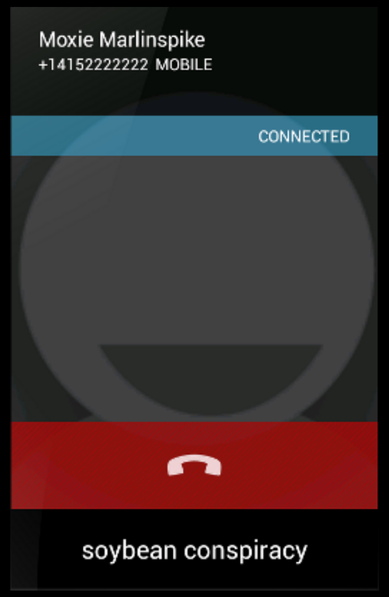
@FredericJacobs

What?

Security, simplified.



TextSecure



RedPhone

TextSecure

Protocols

We live
asynchronously

Perfect Forward Secrecy

Perfect Future Secrecy

Deniability

General Approach

Message Protocols	**Session protocols**
Examples : PGP, S/MIME Asynchronous Problems: Conversation Integrity, forward secrecy, deniability	Examples: OTR, SSL, SSH Synchronous Short-lived session
Axolotl Examples: TextSecure, Pond Asynchronous with all great features of short lived protocols Forward secrecy, deniability, conversation integrity …	


Axolotl

Protocols	WhatsApp	iMessage	Threema	MTProto (Telegram)	SCIMP (SilentText)	Axolotl (TextSecure)	OTR
End-to-End Encryption	No	Yes (no control on key management)	Yes	Yes	Yes	Yes	Yes
PFS	No	No	No	No	Yes	Yes	Yes
Perfect Future Secrecy	No	No	No	No	No	Yes	Yes
Multi-Party Encrypted Chats	No	Yes	Yes	No	Yes	Yes	No
Multi-Device Encrypted Chats	No	Yes	No	No	No	Yes (not yet implemented)	No

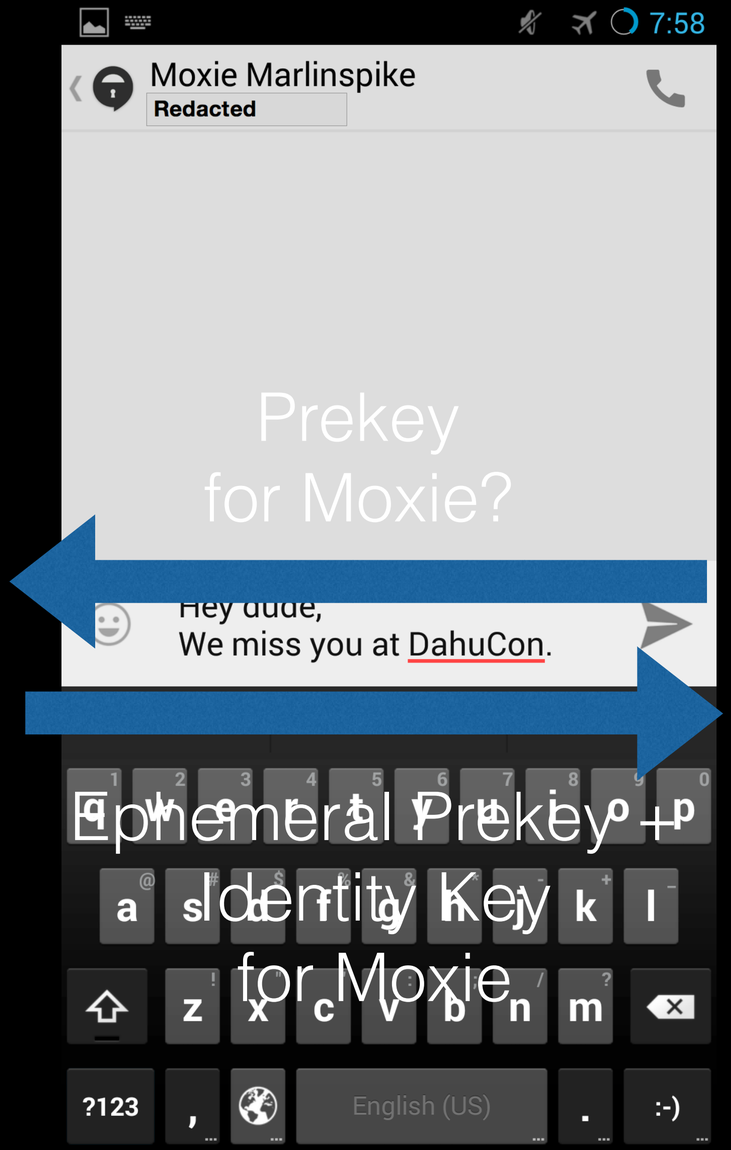
Axolotl Outline

- **Basic features**
  - Authentication
  - Handshake
  - Forward-secrecy ratcheting
- **Advanced (not covered in this talk)**
  - Multi-party
  - Multi-device

Contact Discovery

Authentication

TextSecure
Server



Handshaking

Shared Secret = HKDF(3-Way DH)

Moxie's Identity Key

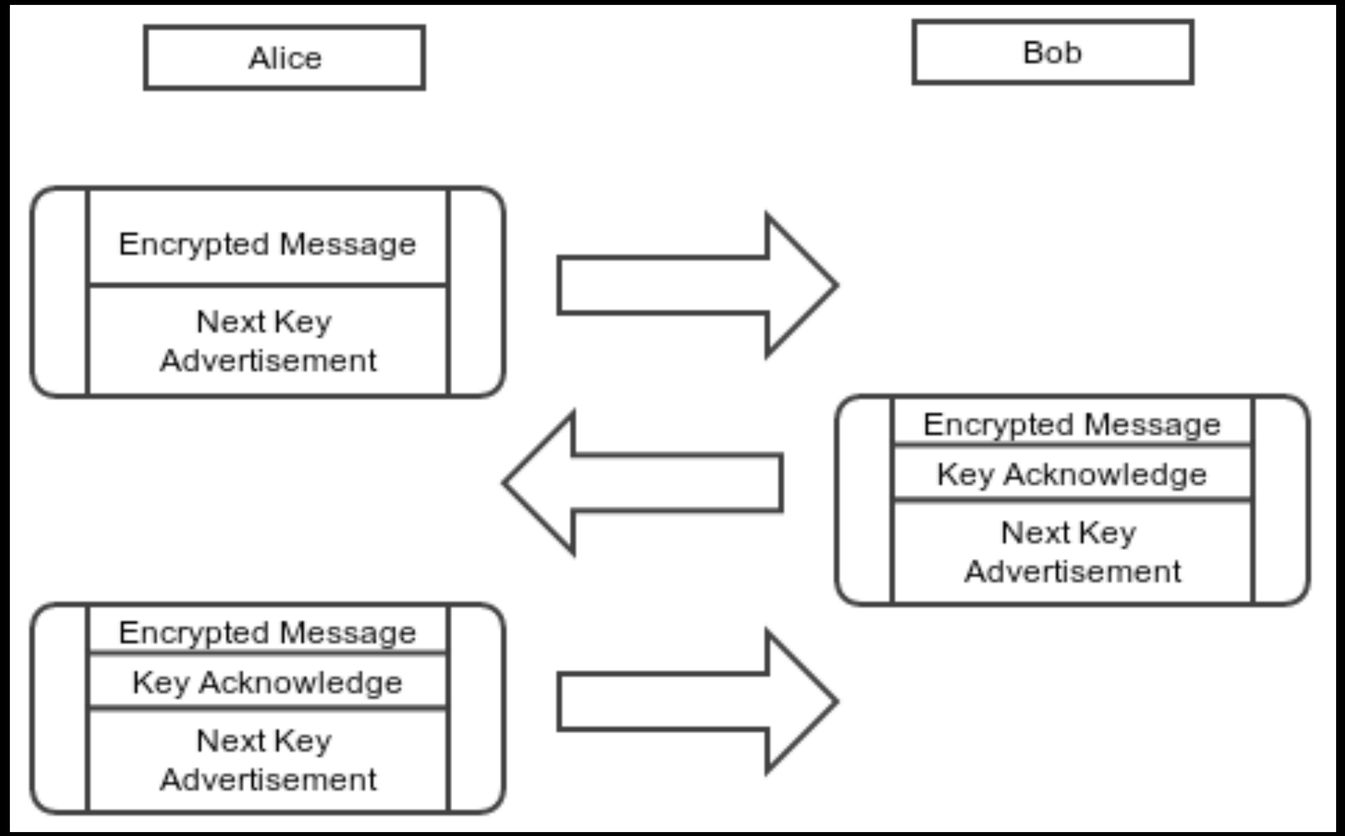
My Identity Key

Moxie's
ephemeral prekey

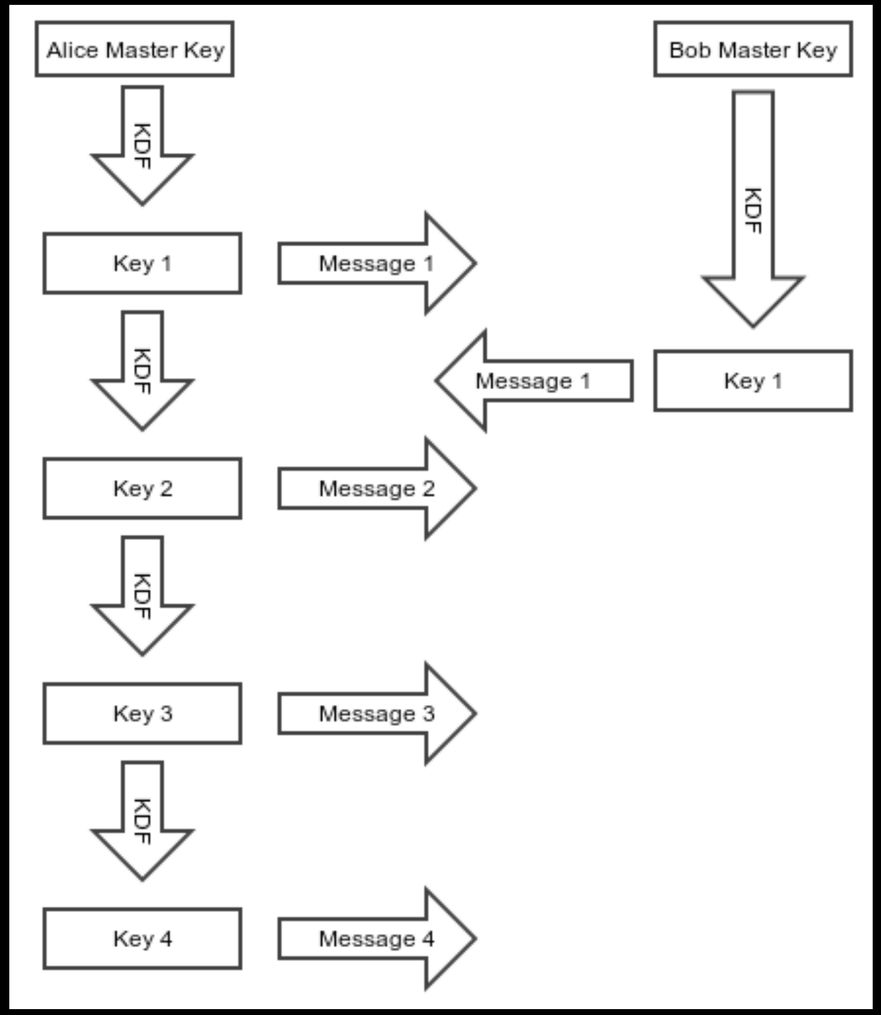
My ephemeral key

Ratcheting

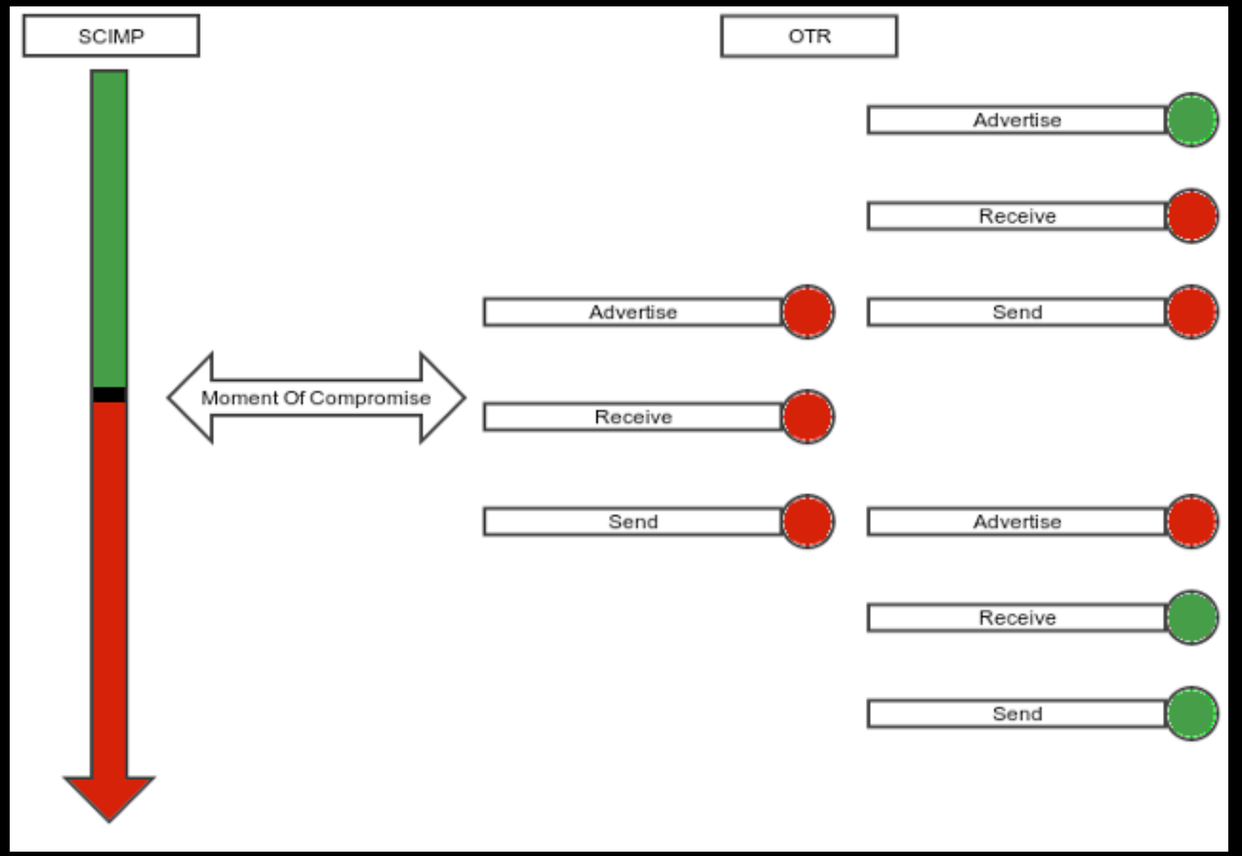
OTR-Ratchet
(three step ratchet)



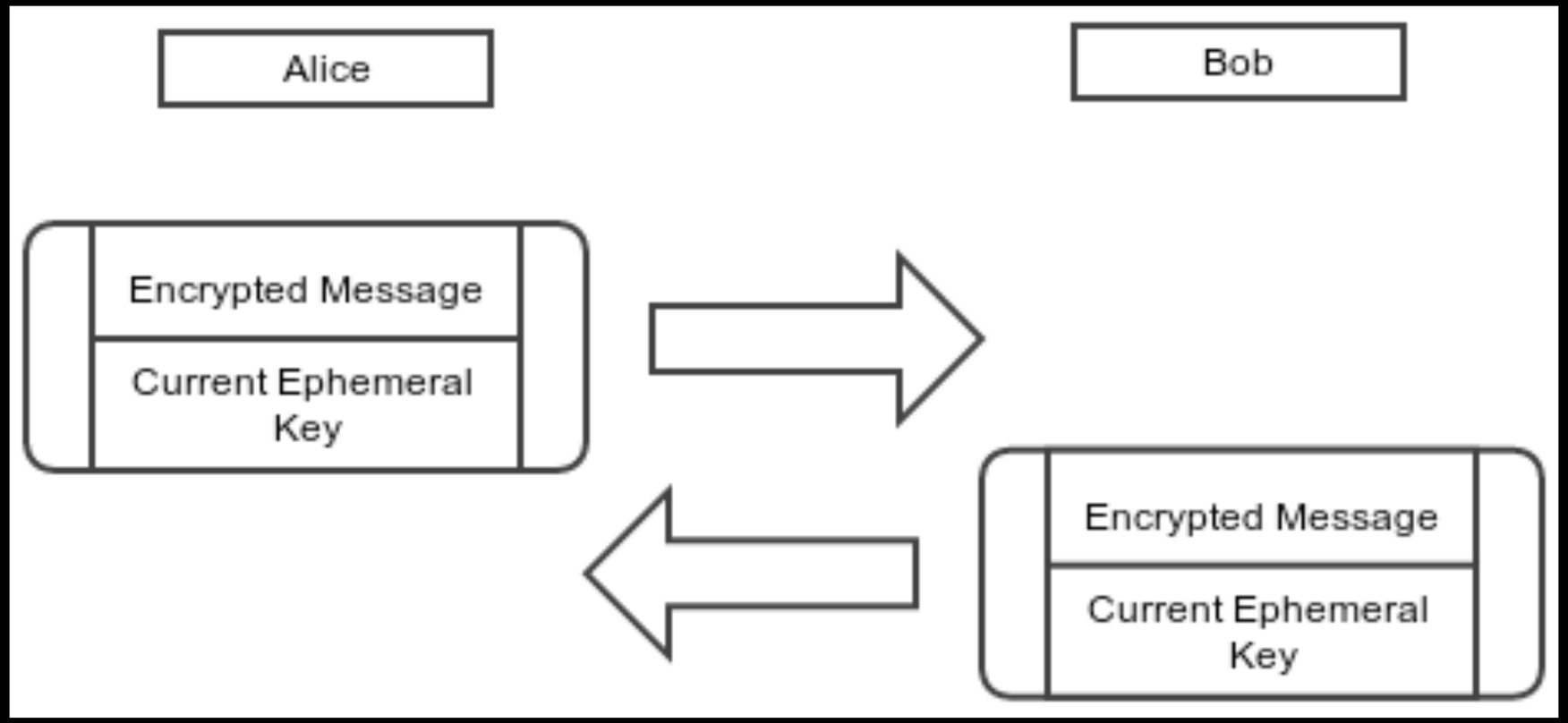
SCIMP-Ratchet (hash-based ratchet)



OTR Ratchet	Silent Circle Ratchet
Excellent Perfect Forward & Future Secrecy	Excellent Perfect Forward Secrecy. But if message key gets compromised, all future conversations will be compromised.



Axolotl-Ratchet



A leap into the future

Such Crypto

Wow

Thanks
Questions?

Very
Datalove