NTNU

Norwegian University of
Science and Technology

Challenges in End-to-End Encrypted Group Messaging

Tjerand Silde

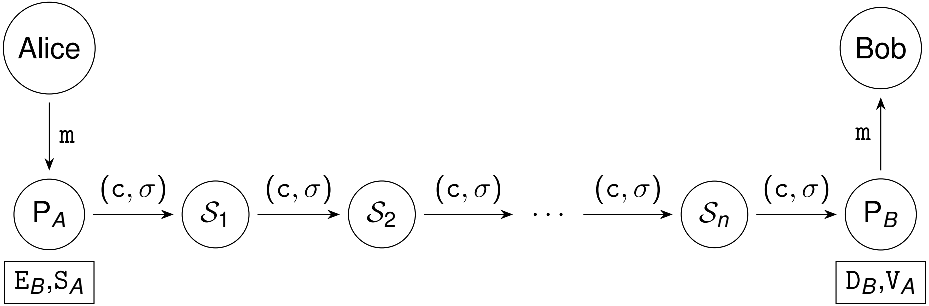
This Work

"Where the Rubber Meets the Road" = Implementing Group Messaging in Practice

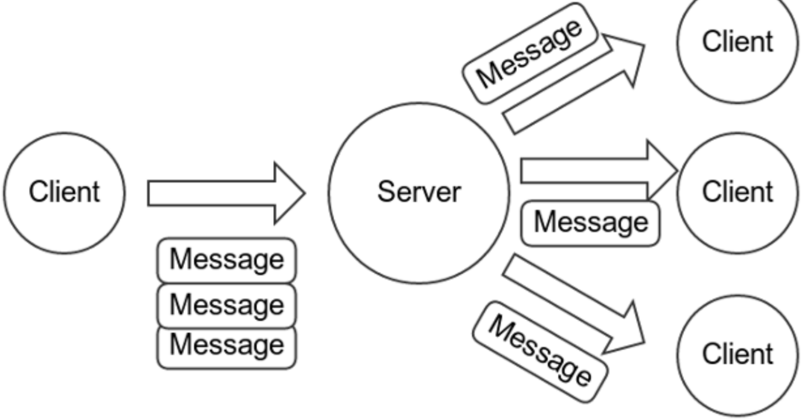
- Minimal Requirement: End-to-End Encryption
- Analyze: Challenges, Treadeoffs and Features
- Document: Applications Used in Practice, e.g.

  Signal, Whatsapp, Wire, iMessage, Keybase, Threema, Crypho,...
- Compare with Messaging Layer Security Standardization Effort.
- Study the Design, not the Code.

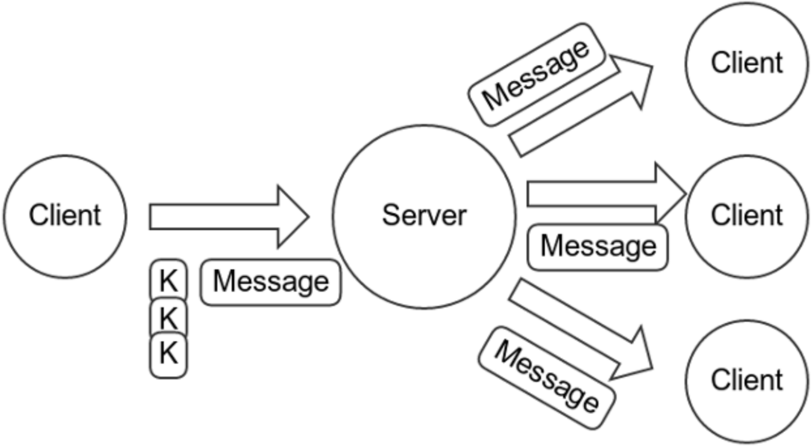
End-to-End Encryption for Alice and Bob



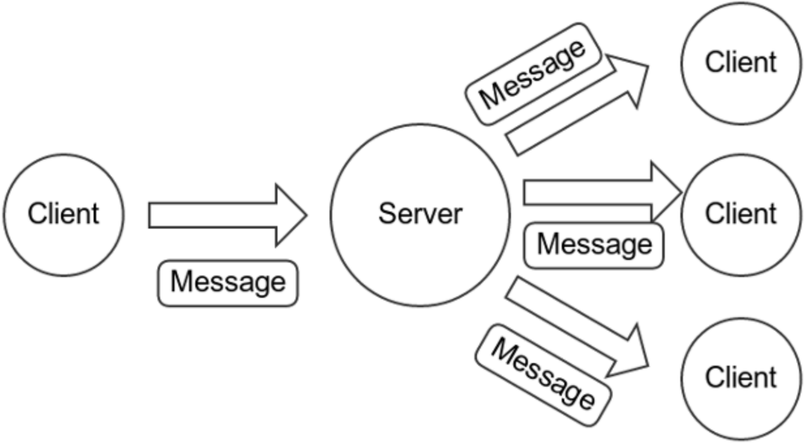
Encrypt Message Individually to Everyone in the Group



Encrypt Decryption Key to Everyone in the Group



Encrypt with Group Key Known to the Group Members



Challenges / Features / Solutions I

- Forward Secrecy and Post-Compromise
  - Double Ratcheting
  - Message Dependent Keys
  - Static Long-Term Keys
- Authentication of Members
  - Trust Only First Use (TOFU)
  - External Social Graph
  - Security Numbers

Challenges / Features / Solutions II

- Adding or Removing Members
  - List Structure
  - Tree Structure
  - "Lazy" Update
  - Multi-Device Users
- Deniability of Messages
  - Ephemeral Keys instead of Signatures
  - Shared MAC-Keys for Groups

Challenges / Features / Solutions III

- Privacy of Social Graph and Metadata
  - Use Software Guard Extensions for Set Intersection
  - External Social Graph
  - Encrypted Metadata
  - Anonymous Credentials
  - Server Knows All Metadata
- Communicating with Offline Parties
  - Pre-Shared Pre-Keys with Server
  - Only Use Static Public Keys

Challenges / Features / Solutions IV

— Backup and Restore Conversations

- No Access to Backups
- Local Encrypted Backup
- Plaintext Backup in Cloud

Summary

Schemes:	FS	PCS	MP	D	A	PWC	EMK	GK
Signal	✓	✓	✓	✓	✗			✓
WhatsApp	✓	✓	✗	✓	✗			✓
Keybase	✗	✗	✗	✗	$			✓
iMessage	✗	✗	✗	✗	✗	✓	✓†	
Crypho	✗	✗	✗	✗	$			✓
Wire	✓	✓	✗	✓	$	✓		
Threema	✗	✗	✗	✗	$	✓	✓†	

Thank You! Questions?