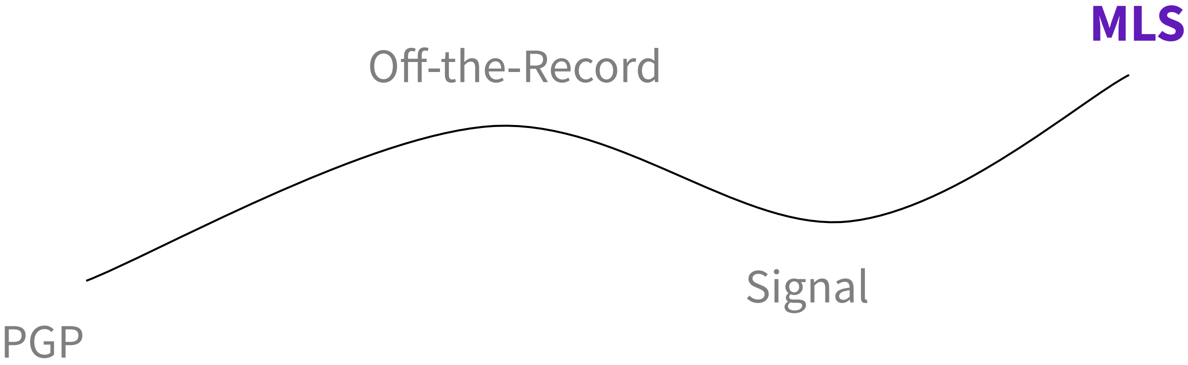
Messaging Layer Security (MLS)

towards more end-to-end encryption

Raphael Robert, PTS 2025 🧂

Introduction

History of end-to-end encryption



PGP

Off-the-Record

Signal

MLS

What is missing?

- More versatility
- Better suited for group chats
- Fully specified standard
- Permissively licensed open-source implementations

Combined experience

moz://a

Inria

aws wickr

NYU PARIS

Phoenix R&D

CLOUDFLARE®

Google

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

ACLU

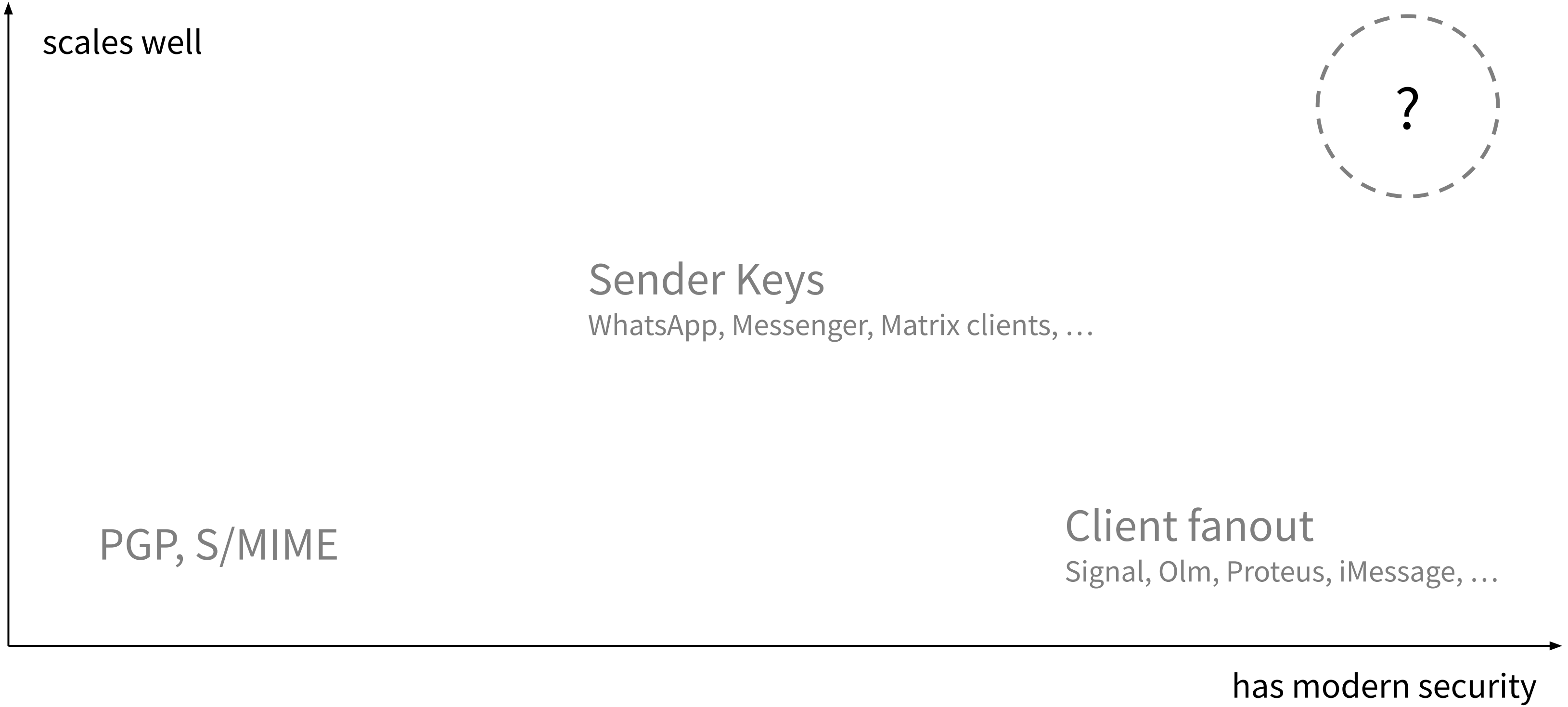
Meta

wire™

UNIVERSITY OF OXFORD
DOMI NVS ILLV MINA TIO MEA

cisco

Modern security vs Scaling



scales well

?

Sender Keys

WhatsApp, Messenger, Matrix clients, …

PGP, S/MIME

Client fanout

Signal, Olm, Proteus, iMessage, …

has modern security

Functional properties

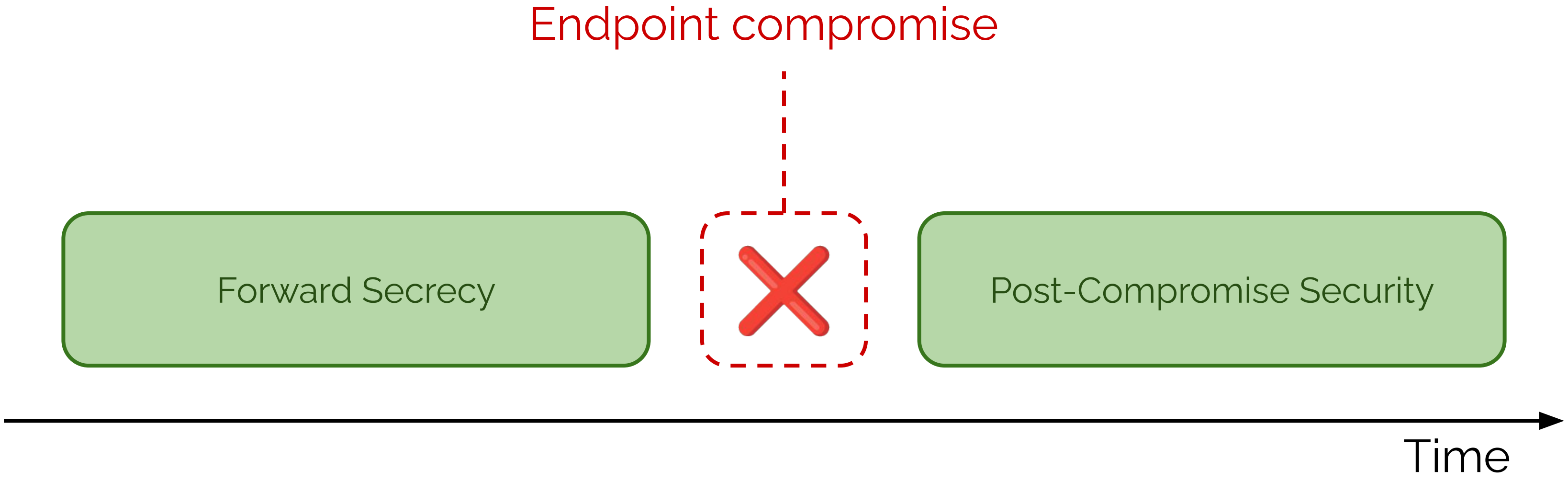
- **Async** - Support sessions where no two members are online at the same time
- **Group Messaging** - Support large, dynamic groups with efficient scaling
- **Multi-device support** - Users should be able to use more than one device
- **Extensibility** - Make the protocol extensible for different use cases
- **Federation** - Members of groups should not be limited to only one server/service
- **Usable** - Focus on a practical drop-in for existing applications

MLS Security Properties

Going beyond OTR & Signal

- Confidentiality & authentication
- Forward Secrecy (FS)
- Post-Compromise Security (PCS)
- Agreement on group state (including membership)
- Informal: transcript consistency

Forward Secrecy & Post-Compromise Security



Endpoint compromise

Forward Secrecy

❌

Post-Compromise Security

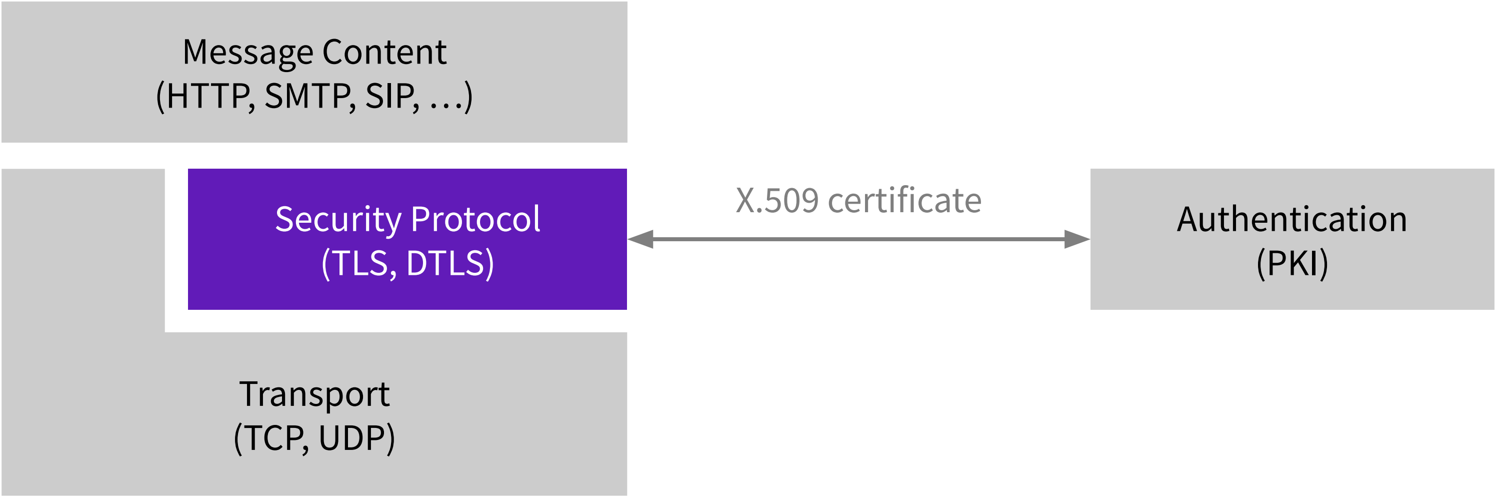
Time

Ingredients

- Asynchronous Ratcheting Trees
- Make IETF your home
- Kick it like TLS 1.3
- Give intermediary drafts to academia for analysis
- Listen to academia

MLS

Scope of TLS



Message Content
(HTTP, SMTP, SIP, …)

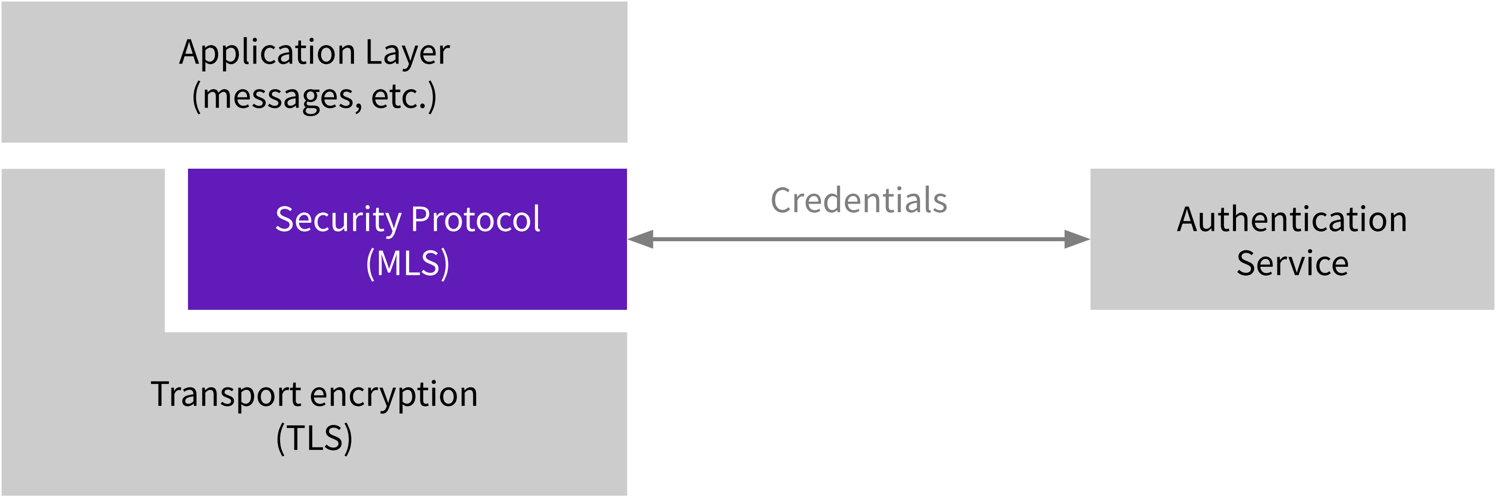
Security Protocol
(TLS, DTLS)

X.509 certificate

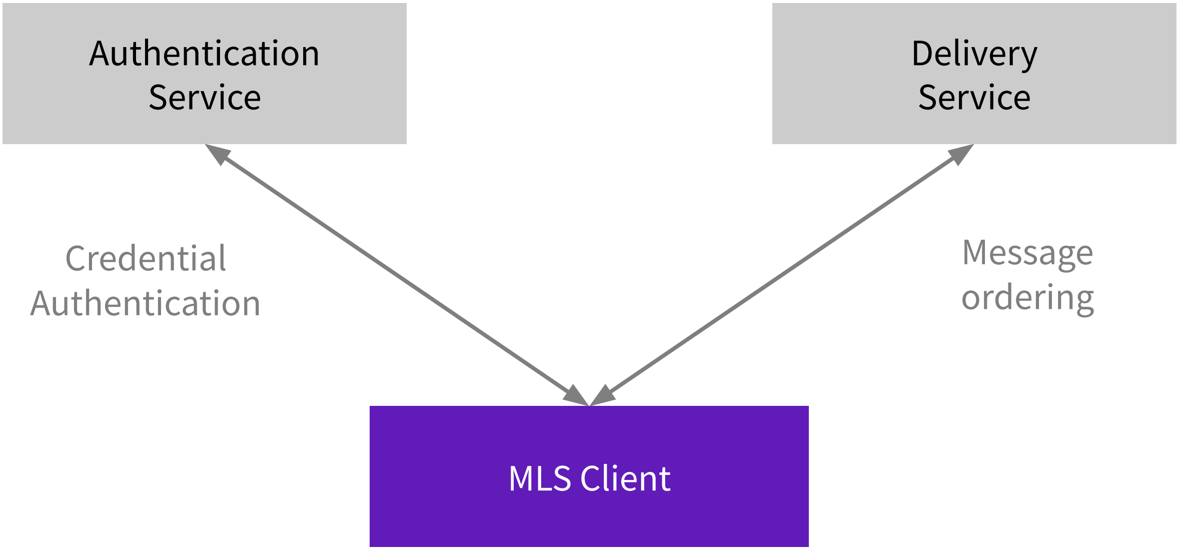
Authentication
(PKI)

Transport
(TCP, UDP)

Scope of MLS


Application Layer
(messages, etc.)
Security Protocol
(MLS)
Credentials
Authentication
Service
Transport encryption
(TLS)

Architecture of MLS



Authentication Service

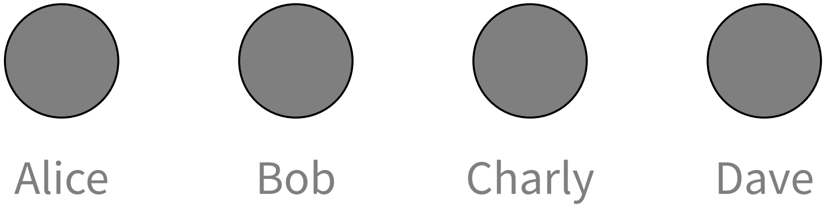
Delivery Service

Credential Authentication

Message ordering

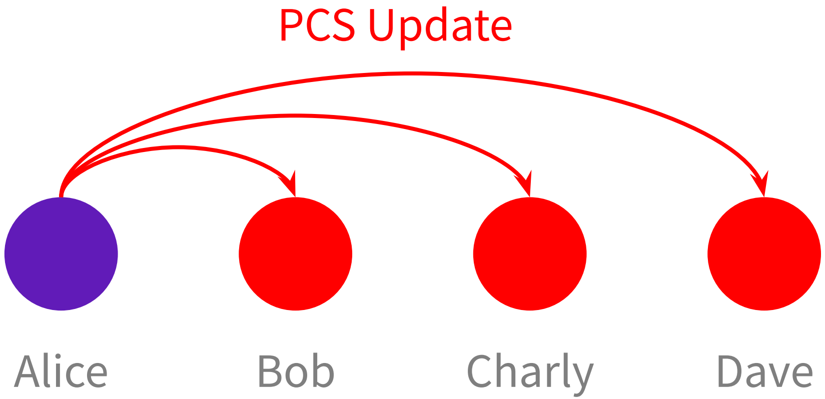
MLS Client

Groups in 1-to-1 protocols

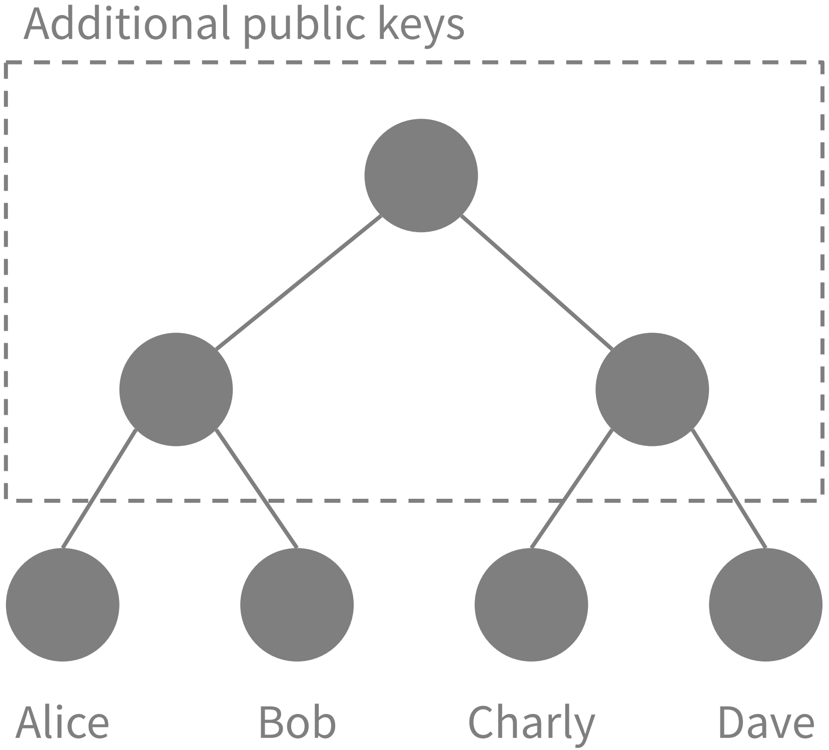


Alice Bob Charly Dave

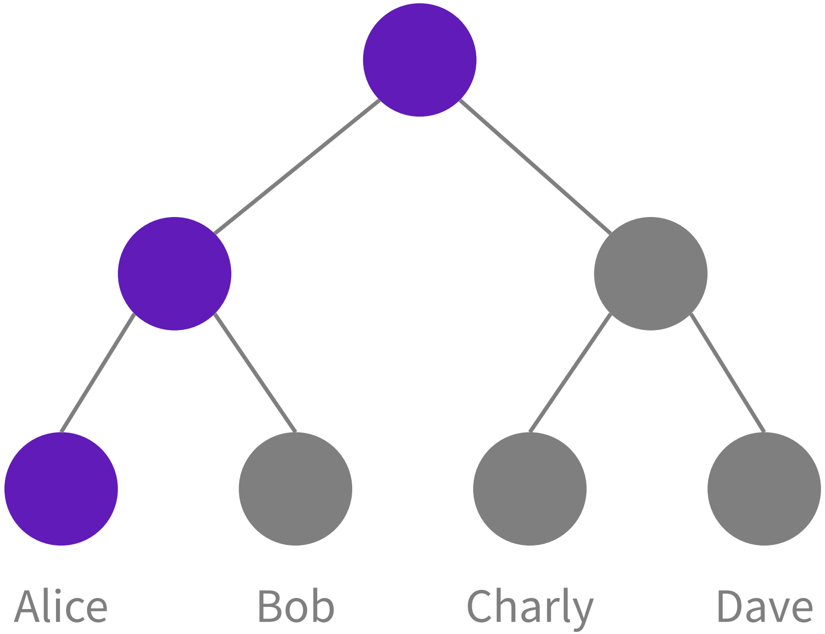
Groups in 1-to-1 protocols: Fanout



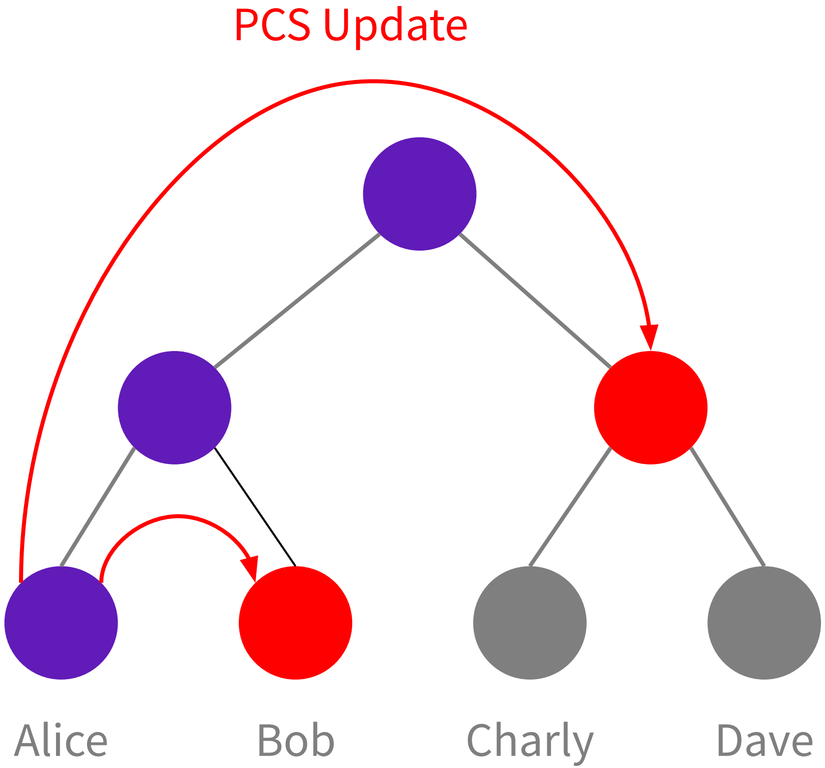
Groups in MLS



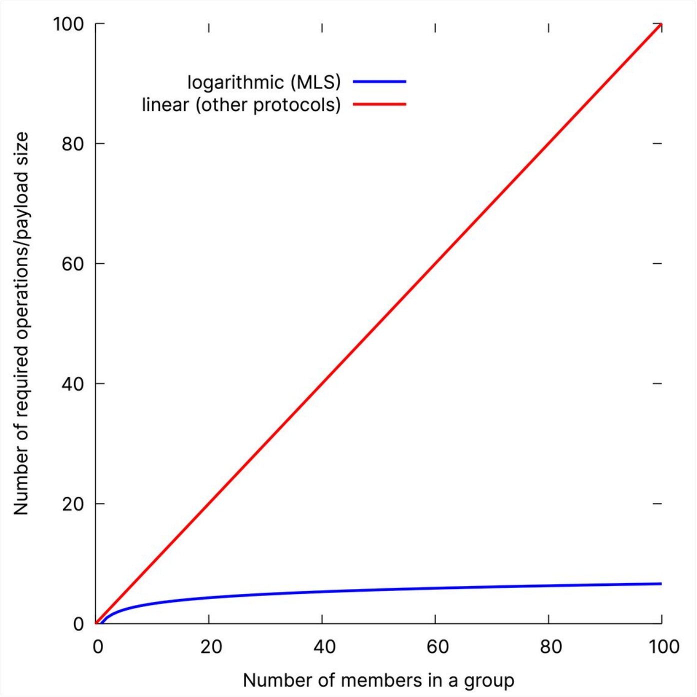
Groups in MLS



Fanout in MLS



Example: Group with 100.000 members



100k

vs

17

Example: PQ secure updates

- Group size: **1000**
- Update size for ML-KEM 768: **1 KB**
- Linear fanout payload size: **1 MB** to upload – **1 GB** to download
- MLS payload size: **10 KB** to upload – **10 MB** to download

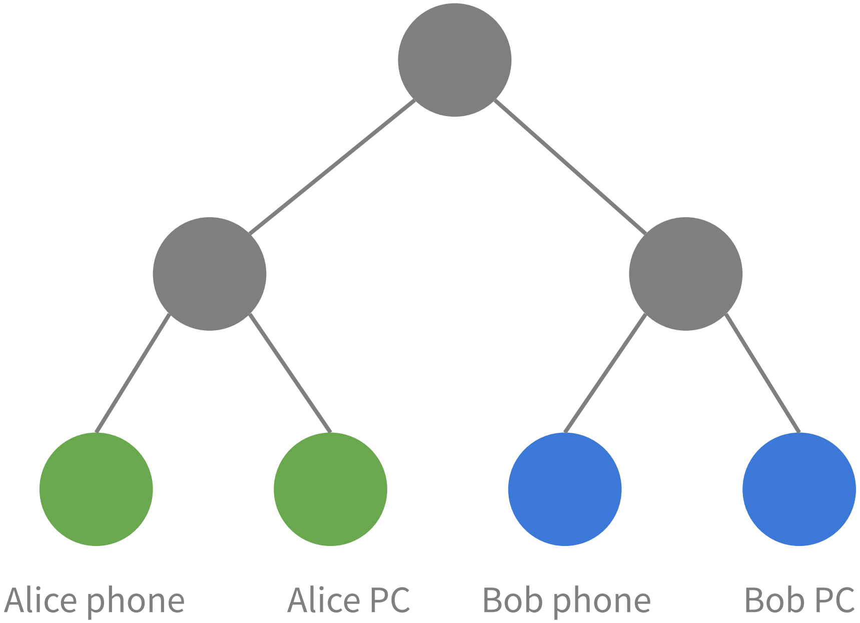
Extensions & variations

Extensions: Hybrid combiner

- Problem statement: Achieving PCS with a hybrid cipher suite is expensive because keys are large (30x larger)
- High frequency updates are unnecessary right now
- Solution: Separate the updates
- Use exporter and PSK injection
- Bonus: we get cheaper PQ authenticity

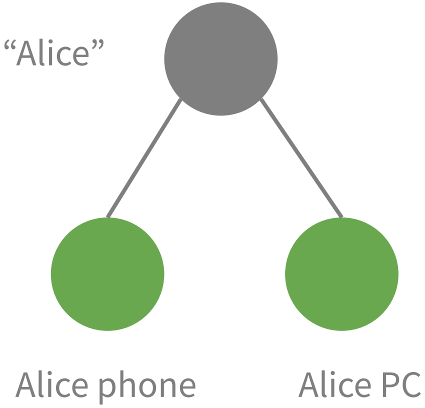
Extensions: Virtual clients

Status quo for multi-device accounts



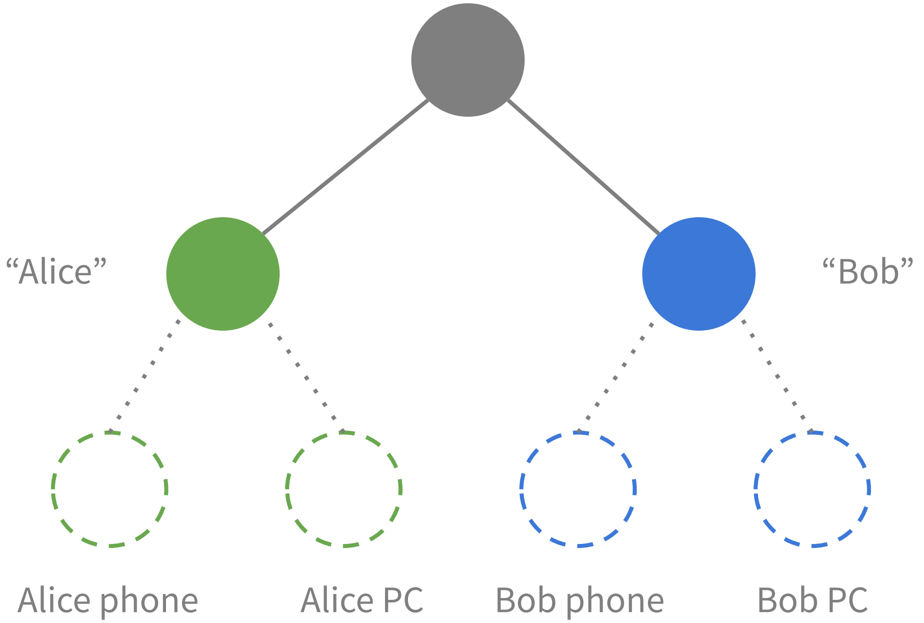
Extensions: Virtual clients

Intra-account sync



Extensions: Virtual clients

Combine intra-account sync and groups



Variation: Decentralized MLS

- MLS requires ordered handshake messages
- Easy when there is a server, not so easy when there is none
- We can fork groups, reconcile later (e.g. with a DAG)
- If we allow forks, FS suffers from that
- Solution: We slightly change how the key schedule works and use a PPRF

Ecosystem

MLS Implementations

- Currently available: RFC-compatible implementations in Rust & C++
- We are working on a community implementation: OpenMLS
- In the works: Java, TS, Go, Ruby, F*

Deployments

Large deployments:

- In production: Cisco Webex, Discord
- Planned: Google & Apple for RCS

Other deployments:

- Wire, Cloudflare Orange Meets, Germ Networks, Matrix (planned), XMPP (planned), Phoenix R&D (planned)

More Instant Messaging Interoperability (MIMI)

- New-ish IETF working group
- Goal: minimal agreement required for interoperability
- Components:
  - Server-to-server protocol
  - Client-to-client protocol
  - MLS, content format, policies

Metadata reduction in MIMI

- Metadata protection is important
- Signal set a good precedent
- Can we do the same with MLS?

Fin

Thank you!

Raphael Robert

🔗 mastodon.social/raphaelrobert

Write us at **hello@phnx.im**