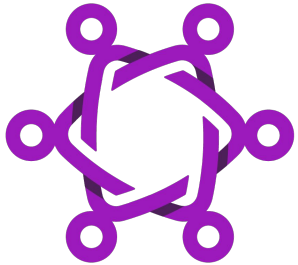
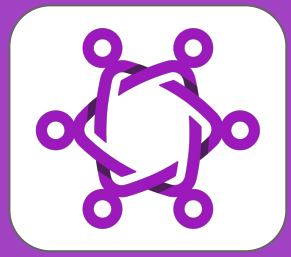


Advancements and Future Directions in Secure Messaging with MLS and MIMI

RWC 2024, Toronto

Richard Barnes, Benjamin Beurdouche, Raphael Robert



What is MLS?

Transport Layer Security

MESSAGING

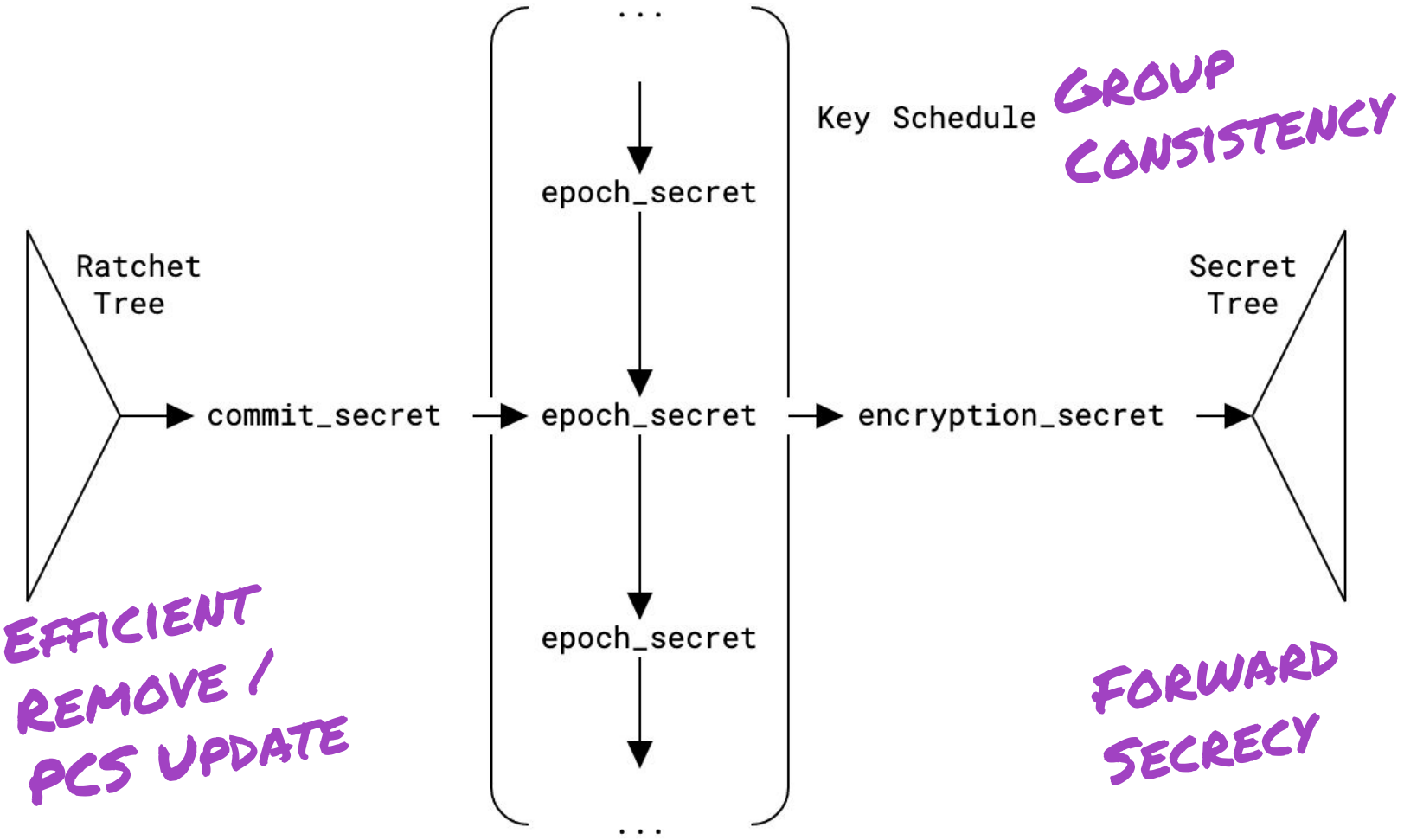
~~Transport~~

Layer

Security

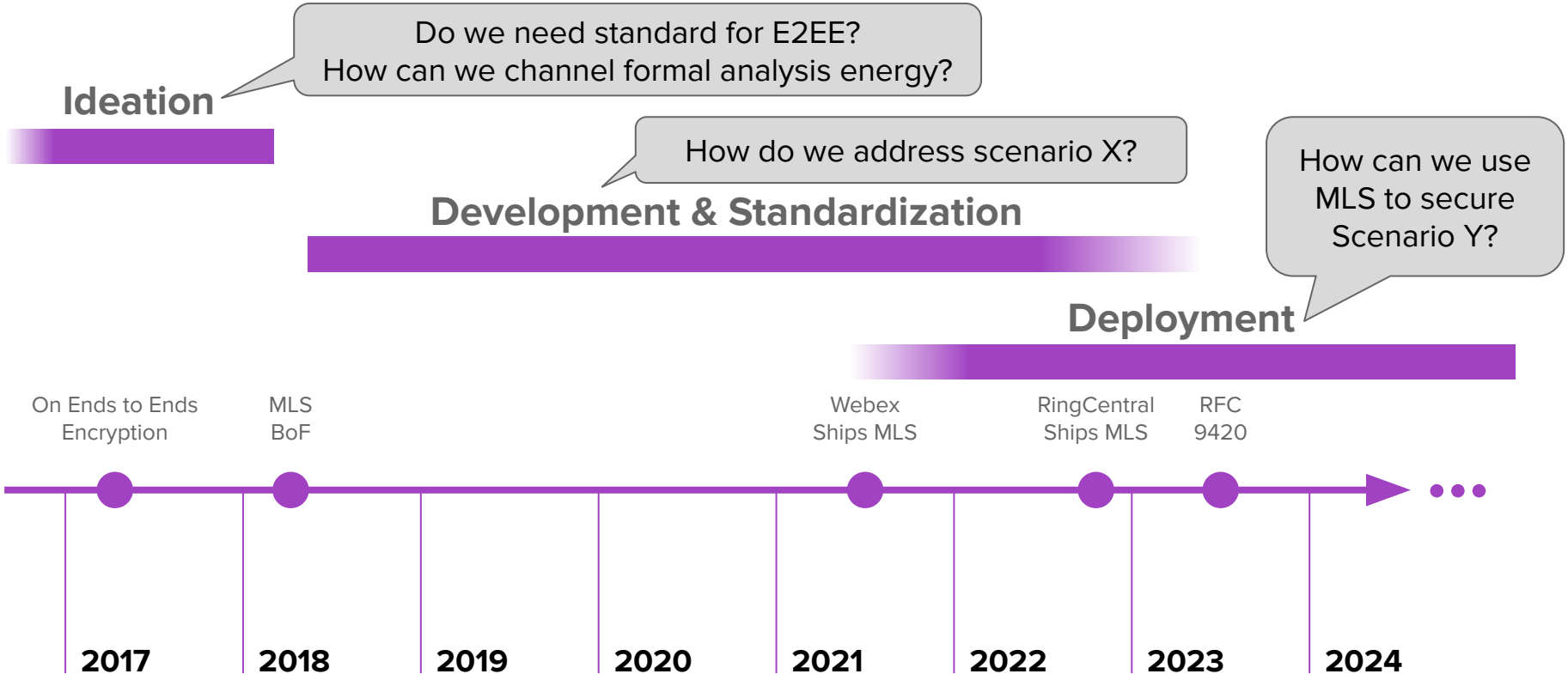
ASYNCHRONOUS
CONTINUOUS
GROUP
AUTHENTICATED
KEY
EXCHANGE

RFC 9420


...
Key Schedule
GROUP CONSISTENCY
epoch_secret
Ratchet Tree
Secret Tree
commit_secret
epoch_secret
encryption_secret
epoch_secret
EFFICIENT REMOVE / PCS UPDATE
FORWARD SECRECY
...

The MLS Standard

Rough timeline



Openness & standardization are great

Included academics & industry from the start

- Push for stronger security properties + deployability
- Positive feedback loop between formal analysis and protocol definition

Now we have many implementations, mostly open-source

- C++, Java, Rust, Go, Kotlin, F*, ...
- All validated to interoperate
- Open foundation for end-to-end encrypted applications

Uniquely strong security for groups

Efficient Full-Group FS / PCS: When someone leaves the group (including replacing a possibly compromised instance), you need to use keys they don't know

Sender Keys: $O(N^2)$ (in practice, nobody bothers)

MLS: O(log N) to O(N) (depending on how the group is managed)

State Agreement: Everyone in the group agrees on whole state of the group, e.g., to prevent "ghost users" added by malicious insiders

Credential-based Authentication: Real applications want to authenticate identifiers, not cryptographic keys. Each MLS participant presents a credential.

Group agreement is double-edged

On the one hand, a critical and highly useful security property

On the other hand, requires that groups have linear history

Prime Directive of MLS Design: Each Commit has exactly one successor

Classic State Machine Replication problem, with the usual solutions:

- Have a centralized server 🌟
- Run a consensus algorithm
- Update MLS to tolerate / heal forks

A quick sketch of the Webex deployment

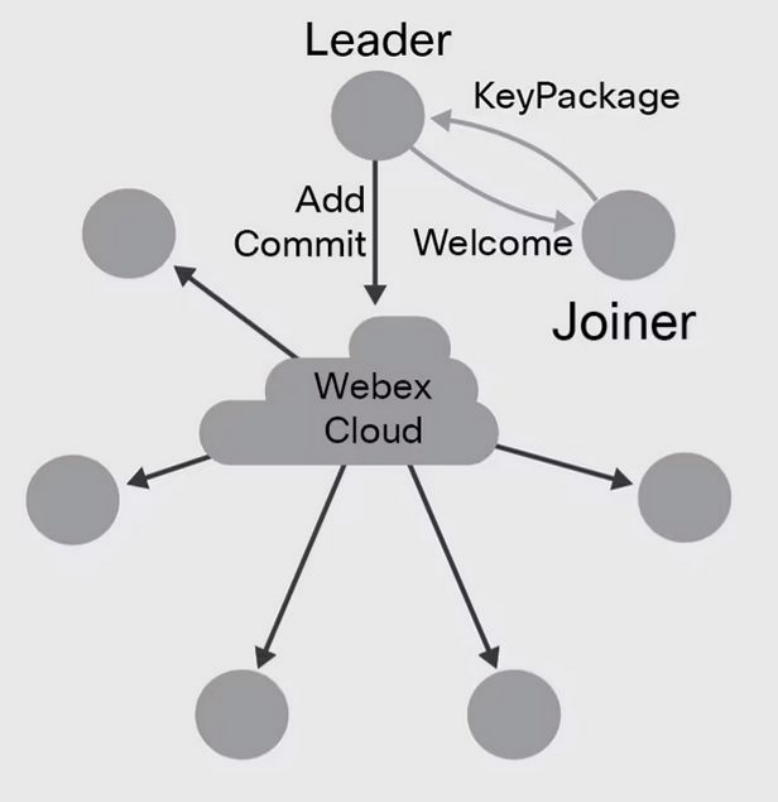
Centralized server routes MLS messages

Only one client commit, a “leader” nominated by the server

Clients track alignment between the Webex participant list and the MLS roster

Authentication that is only available with MLS:

- E2E Identity credentials
- Security code captures the whole state



PQ support is included

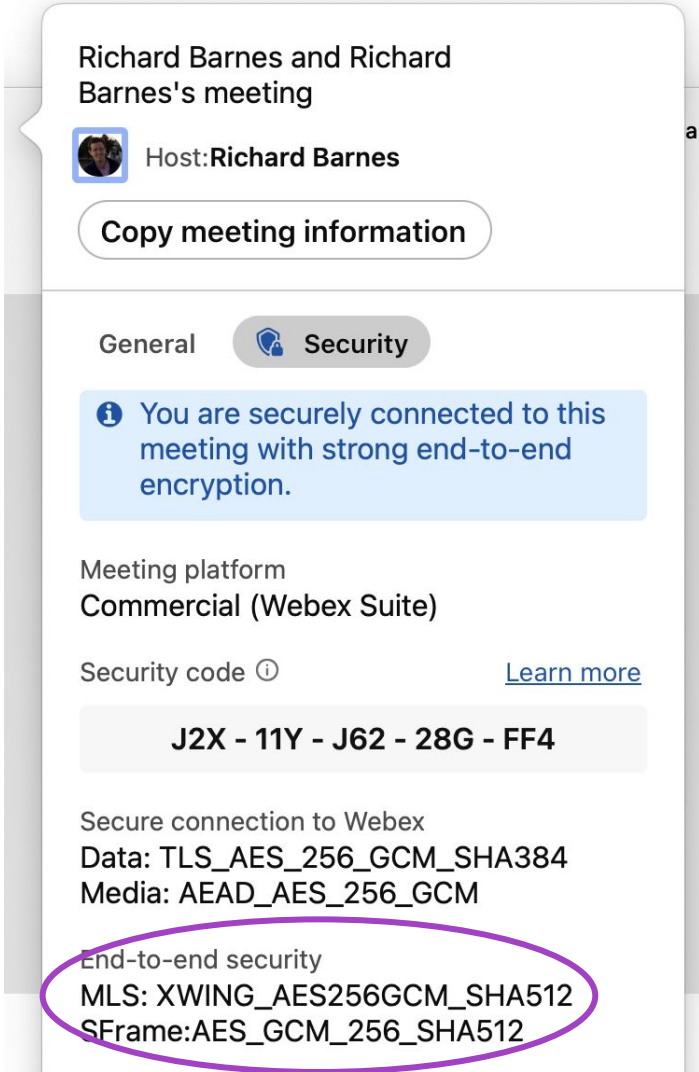
Unlike many protocols, MLS is already based on KEM and has cipher agility

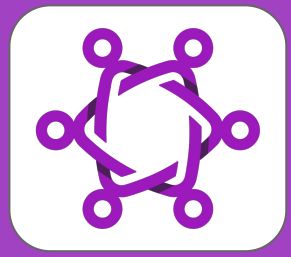
Just a ciphersuite change to add support for PQ

Weekend project to add XWing to Webex

- 2hr to add ML-KEM-768 implementation
- 2hr to add XWing ciphersuite to MLSpp
- No changes to Webex except new cipher suite

Standard ciphersuite in progress (draft-mahy-mls-xwing)





MLS and PQ

Post-Quantum

MLS has support for ciphersuites and cryptographic agility

- Standards are being built which means that we need to experiment to understand the tradeoffs between different schemes for variety of applications
- Strong security as a default

MLS is ready for PQ

- MLS uses abstract KEMs and Signatures
  - eg. Replacing DH-KEM by IND-CCA2 PQ KEMS is trivial
- ML-KEM is not key committing unlike Kyber but HPKE fixes that
- Different kind of hybridization (hybrid crypto v. hybrid groups)

Efficient PCS for Post-Quantum

log(N)* KEMs are enough to provide PCS in **one** group operation

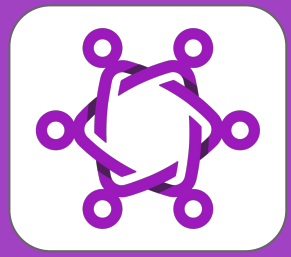
Investigating PQ support for signatures

Long lived groups means that PQ public signature keys do not have to be fetched very often

- Providing hybrid security for signatures is a challenge [Hale et al.]
- An intuition is that the need for MLS is short signatures

It is still early days for PQ signature schemes

- MLS is ready to handle those new signature schemes



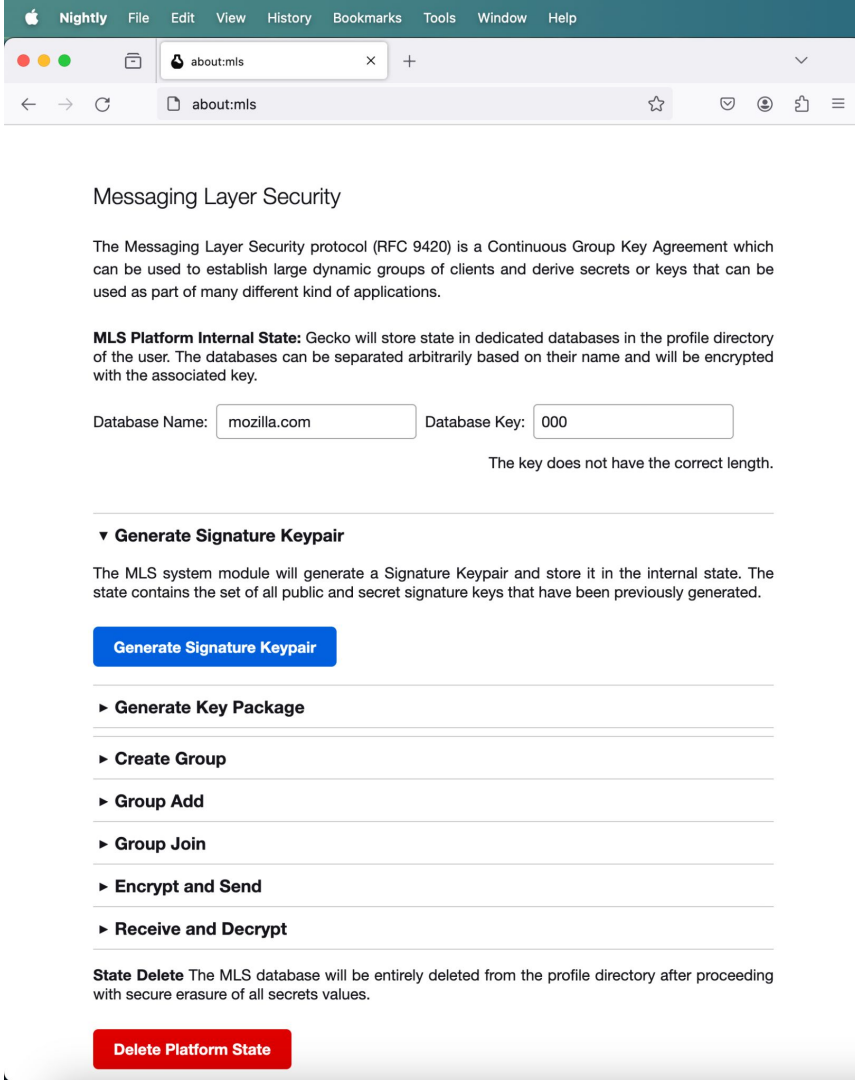
MLS as a Platform

Integration in Firefox

Experimenting with Web Platform integration

- Ease of use for developers and users
  - Standardization / alignment of the API
  - Collaboration with implementers (mls-rs, OpenMLS, mlspp...)
  - Many thanks to Marta, Anh, Raphael... !!
- Performance
  - Native implementation (Rust, Formally verified C/C++...)
- Security
  - Constant-time cryptography
  - No secret manipulation in the page
  - Secure key storage
  - Storage isolation
  - Reduce trust assumptions related to the application

Coming soon to Firefox Nightly...



Integration in Firefox

Open questions and next steps

- Defining an API has the side effect of constraining functionality
  - Ensure that the basic API covers “enough”
  - Ensure that it is safe and easy to use
- Discuss with applications and determine what are the possible use cases enabled by this
- Discuss standardization with other platforms

Please reach out if you are interested in using this!

Building cross-platform support

Secure 1:1/Group Messaging

- MIMI, IoT, Hypervisors, Enclaves, MPC...

Video Conferencing

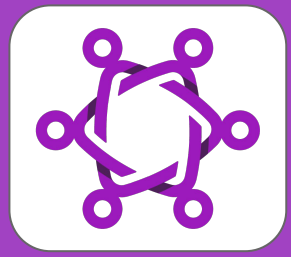
- WebRTC / SFrame, Media-over-QUIC...

Encrypted Storage/Backup

Password Managers

Shared state synchronization

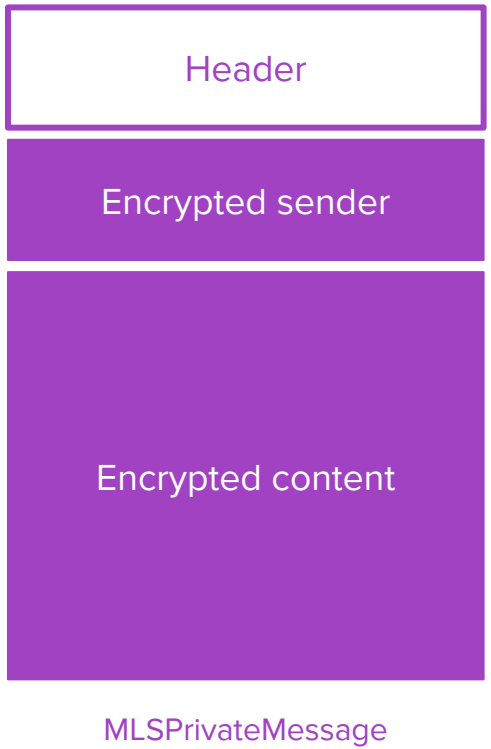
... join us, it is all End-to-End secure!



MLS Extensions

More metadata privacy

- Status quo: Built-in mechanisms
- Server assistance for scalability
- Other techniques



More metadata privacy

- Status quo: Built-in mechanisms
- Server assistance for scalability
- Other techniques

More metadata privacy

- Status quo: Built-in mechanisms
- Server assistance for scalability
- Other techniques

Ongoing work on MLS extensions

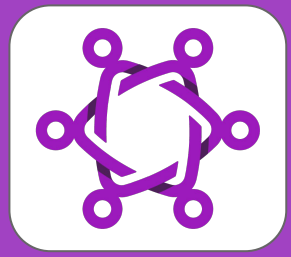
- Safe extensions
- Virtual clients
- AppAck: Detect dropped messages
- Last Resort KeyPackage
- Verifiable credentials & multi-credentials

Deniability

- Status quo
- Trade-off between deniability and unknown key share attacks
- Attacks
- PQ situation
- Deniability in MLS?

More Instant Messaging Interop (MIMI)

- Digital Markets Act (DMA)
- MIMI inception
- MIMI focus areas



Finally

MLS is here, and getting better

MLS as an open, standardized group AKE with uniquely strong security

- Group agreement, strong identity, built-in PQ support…

Platforms are invested in defining a useful tool for users and applications

- Major companies already have deployed MLS and speed is picking up

MIMI is bringing MLS to the messaging ecosystem, and improving privacy

SFrame and MoQ are bringing MLS to the video conferencing ecosystem

MLS is a tool to securely establish groups and secrets that can be used for your applications.

Thanks to the MLS Contributors!

Joël Alwen
Richard Barnes
Benjamin Beurdouche
Karthikeyan Bhargavan
Katriel Cohn-Gordon
Cas Cremers
Alan Đuric
Britta Hale
Srinivas Inguva
Konrad Kohbrok
Albert Kwon
Tom Leavy
Rohan Mahy
Brendan McMillion
Jon Millican
Marta Mularczyk
Emad Omara
Eric Rescorla
Raphaël Robert
Michael Rosenberg
Théophile Wallez
Thyla van der Merwe

... and many authors of cryptographic analyses