TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security

Théophile Wallez, *Inria Paris*
Jonathan Protzenko, *Microsoft Azure Research*
Karthikeyan Bhargavan, *Cryspen*

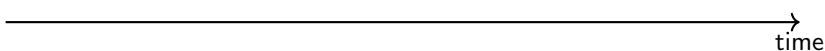
What is Messaging Layer Security (MLS)

Secure group messaging

. . .

Secure group messaging

Signal WhatsApp matrix . . .

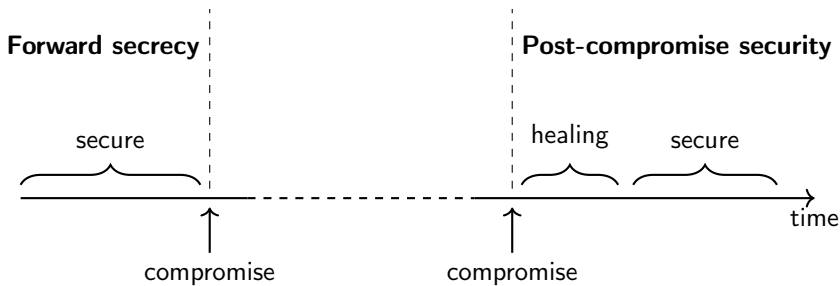


Secure group messaging

Signal WhatsApp matrix . . .

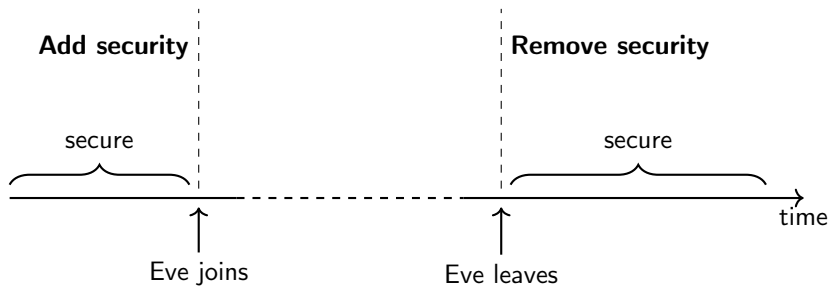
Secure group messaging

Signal WhatsApp matrix . . .

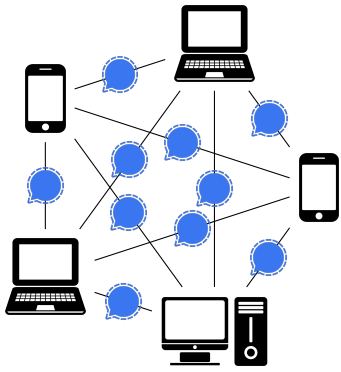


Secure group messaging

Signal WhatsApp matrix . . .

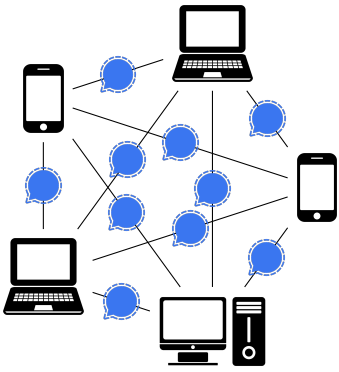


State of the art, before MLS



N devices
$O(N^2)$ Signal channels!
Slow for large N, e.g. $N \simeq 1000$

State of the art, before MLS



N devices
$O(N^2)$ Signal channels!
Slow for large N, e.g. $N \simeq 1000$

IETF®

↓

MLS

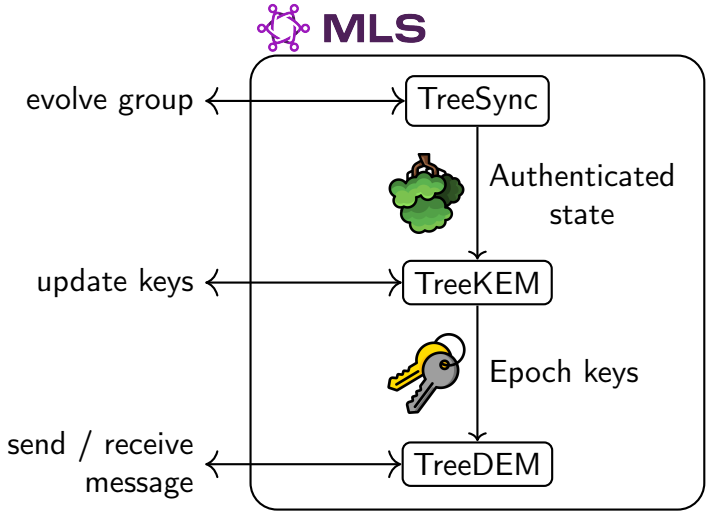
↓

RFC 9420

Design constraints:
Secure, efficient, asynchronous, dynamic groups

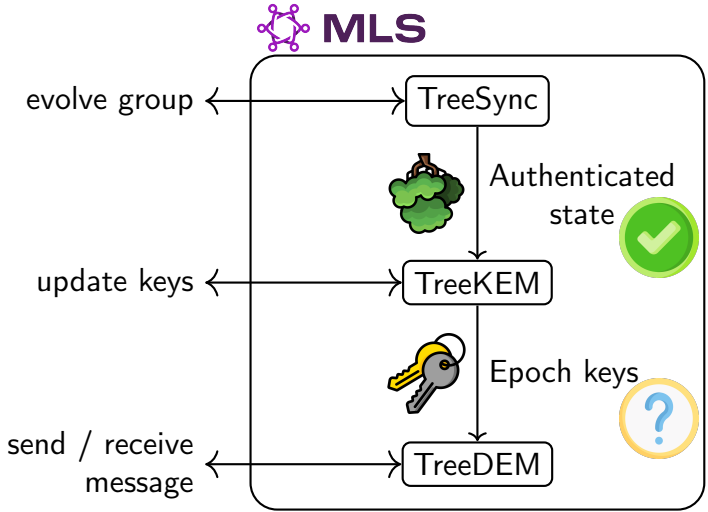
Prior work: Modularizing MLS

("TreeSync: . . . ", USENIX Security '23)



Prior work: Modularizing MLS

("TreeSync: . . . ", USENIX Security '23)



Our contributions

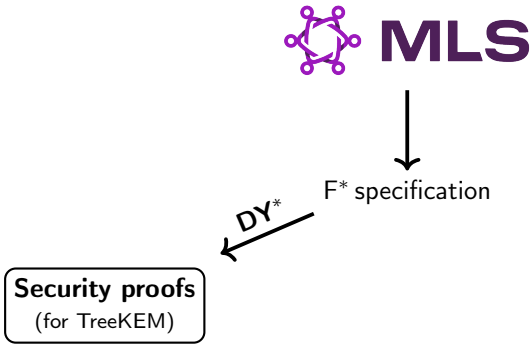
A security theorem for TreeKEM

Yes, TreeKEM does guarantee*:

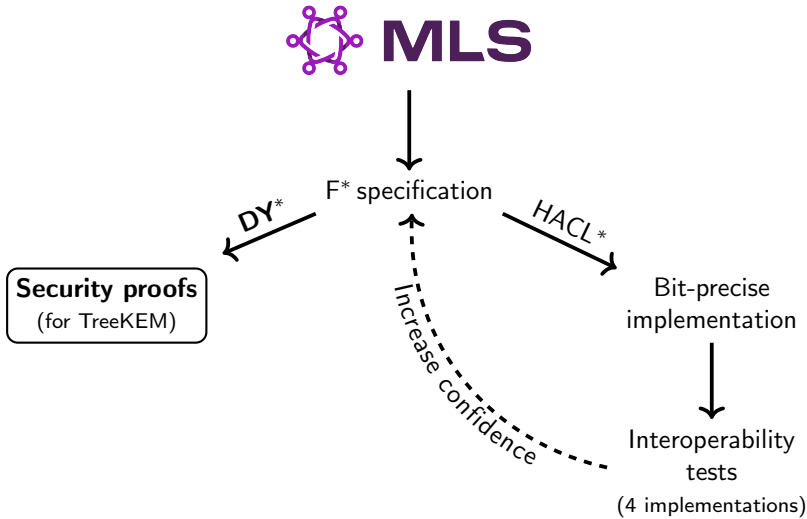
- add security
- remove security
- forward secrecy
- post-compromise security

*

Symbolic analysis on bit-precise, interoperable specifications



Symbolic analysis on bit-precise, interoperable specifications



Improving MLS deployment policies

Our security theorem always implies:

- add security
- remove security

And implies (assuming deployment policies we specify):

- forward secrecy
- post-compromise security

Some of these deployment policies were missing from the MLS architecture document, we notified the working group.

Conclusion

Our contributions:

- prove the security of TreeKEM in the symbolic model
- do proofs on an bit-precise, executable, interoperable specification
- help the MLS Working Group to improve the architecture document

Future work: security proofs for TreeDEM, prove efficient implementations.

</> `https://github.com/Inria-Prosecco/treekem-artifact`

✉ `theophile.wallez@inria.fr`
🌐 `https://www.twal.org/`
@twal.org