Sichere Verschlüsselung in Gruppen mit dem MLS-Protokoll

Stefan Schumacher

Kieler Open Source und Linux-Tage 2025

$ Id: MLS-Protokoll-Input.tex,v 1.13 2025/09/20 06:01:35 stefan Exp $

$Id: MLS-Protokoll-Input.tex,v 1.13 2025/09/20 06:01:35 stefan Exp $

cryptomancer.de

1 Einführung

Über mich

- Geek, Nerd, Hacker
- Robotron KC85/3 Mitte der 80er Jahre
- Kryptographie seit 30 Jahren
- einige Jahre NetBSD-Entwickler
- ehem. Sicherheitsforscher u.a. Fach-Didaktik der Kryptographie
- jetzt Sicherheitsarchitekt bei einem öffentlichen IT-Dienstleister

Glossar

symmetrisches Kryptosystem ein geteilter geheimer Schlüssel für Verschlüsselung/Entschlüsselung nötig

asymmetrisches Kryptosystem kein geteilter geheimer Schlüssel für Verschlüsselung/Entschlüsselung nötig

Diffie-Hellmann Key Exchange (DH KEX): Protokoll zur Schlüsselvereinbarung, Alice und Bob können über einen öffentlichen (abhörbaren) Kanal einen geheimen Schlüssel für symmetrische Kryptographie vereinbaren

Key Derivation Function Schlüsselableitungsfunktion, leitet $1..n$ neue Schlüssel aus einem geheimen Schlüssel ab

(Perfect) Forward Secrecy (PFS) Sitzungsschlüssel werden so vereinbart, dass nach einem Einbruch *vergangene* Sitzungsschlüssel nicht gebrochen werden können (break-backward protection)

PSK Pre Shared Key, symmetrisches Verfahren mit vorher geteiltem geheimen Schlüssel

HPKE Hybrid Public Key Encryption: Symmetrischer Session-Key wird mit einem asymmetrischen Key-Encryption-Key verschlüsselt

Break-in recovery Sitzungsschlüssel werden so vereinbart, dass nach einem Einbruch auch *zukünftige* Sitzungsschlüssel nicht gebrochen werden können (break-forward protection)

persistent nicht-flüchtig, Langzeitschlüssel/ID-Schlüssel

ephemeral flüchtig, Sizungsschlüssel, wird aus dem Langzeitschlüssel abgeleitet

E2EE / Ende-zu-Ende Verschlüsselung Kommunikation wird zwischen Alice und Bob so verschlüsselt, das niemand dazwischen mitlauschen kann, egal ob ISP oder Server-Betreiber

Merkle-Tree Binärbaum, in dem jeder Knoten den Hash über alle seine Unterbäume bildet

Authentizität Echtheit des Absenders (Web of Trust/Zertifikate)

Integrität Daten wurden nicht verändert (Signatur)

Zurechenbarkeit Nachrichten sind dem zuzuordnen, der sie abgeschickt hat

Verbindlichkeit Sender kann Urheberschaft gesendeter Nachrichten nicht abstreiten

plausible Deniability Gegenteil zu Zurechenbarkeit && Verbindlichkeit, Alice und Bob können sich sicher sein, dass sie mit Bob bzw. Alice kommunizieren, aber Mallory kann nicht beweisen, dass Alice und Bob kommuniziert haben, im Englischen auch Off-the-Record genannt

Malleability Formbarkeit kryptographischer Nachrichten, d.h. Zurechenbarkeit && Verbindlichkeit können ausgehebelt werden

Mitgliedschaftsauthentifizierung jeder Teilnehmer kann alle Mitgliedschaften in der Gruppe überprüfen

Device (Matrix) *alle* End-Geräte eines Nutzers

Client (MLS) Mitglieder einer Gruppe

Epoche (MLS) Zustand einer Gruppe zu einem Zeitpunkt

LeafNode (MLS) Eigenschaft eines jeden Mitglieds mit Identität, Credentials und Fähigkeiten

Attestation Beglaubigung der Integrität und Authentizität von Daten

Formelzeichen M: Message/Nachricht; K: Key S: Secret/Geheimnis pub: public $priv$: private sig: signature enc: decryption

2 Matrix - 3DH-KEX und DoubleRatchet

Matrix

- Application-Layer-Kommunikationsprotokoll für föderierte Echtzeitkommunikation
- sicheres Verbreiten und Speichern von JSON-Nachrichten
- geteilter Zustand *nicht* direkte Nachrichten zwischen Partnern
- HTTP und WebRTC
- VoIP, IoT, IM
- Ziel: generisches Messaging- und Datensynchronisationsprotkokoll

Literatur:

- [1] P. D. Chowdhury u. a., „Threat Models over Space and Time: A Case Study of E2EE Messaging Applications," *arXiv preprint arXiv:2301.05653*, 2023

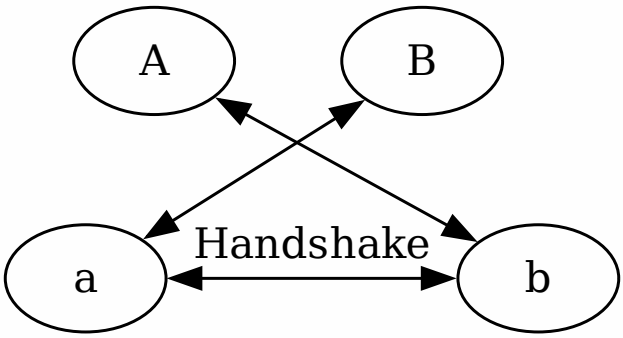
Triple Diffie-Hellman Key Exchange

- 3DH-KEX: Alice und Bob leiten ephemerale Schlüssel (a,b) ab und führen 3 Handshakes zwischen den ID-Schlüsseln und ephemeralen Schlüsseln
- Danach werden 3 geteilte Geheimnisse abgeleitet: S^{aB}, S^{Ab}, S^{ab}
- Algorithmische und Protokoll-Komplexität reduziert, Formbarkeit erhöht, Nutzlast verringert, Forward Secrecy beibehalten
- 3DH-KEX: Nur zum Aufbau einer Session, danach nicht mehr verwendet

Literatur:

- [2] F. van der Have, „The X3DH Protocol: A Proof of Security," Diss., Raboud Uni, 2022
- [3] M. R. Albrecht u. a., „Practically-exploitable Cryptographic Vulnerabilities in Matrix," in *2023 IEEE Symposium on Security and Privacy (SP)*, IEEE Computer Society, 2022, S. 1419–1436
- [4] J. P. Degabriele u. a., *On the Joint Security of Encryption and Signature in EMV*, Cryptology ePrint Archive, Paper 2011/615, https://eprint.iacr.org/2011/615, 2011. Adresse: https://eprint.iacr.org/2011/615
- [5] C. Cremers und M. Feltz, *One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability*, Cryptology ePrint Archive, Paper 2011/300, https://eprint.iacr.org/2011/300, 2011. Adresse: https://eprint.iacr.org/2011/300
- [6] M. Marlinspike, „The Double Ratchet Algorithm," Tech Report, 20. Nov. 2016
- [7] V. Moscaritolo, G. Belvin und P. Zimmermann, „Silent circle instant messaging protocol protocol specification," *Online, White Paper*, S. 47, 2012
- [8] J. Alwen, S. Coretti und Y. Dodis, „The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol," in *IACR Cryptol. ePrint Arch.*, 2018. Adresse: https://cs.nyu.edu/~dodis/ps/signal.pdf
- [9] K. Cohn-Gordon u. a., „A Formal Security Analysis of the Signal Messaging Protocol," *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, S. 451–466, 2017. Adresse: https://eprint.iacr.org/2016/1013.pdf
- [10] J. Alwen, S. Coretti und Y. Dodis, „The double ratchet: security notions, proofs, and modularization for the signal protocol," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2019, S. 129–158. Adresse: https://eprint.iacr.org/2018/1037.pdf
- [11] J. Jaeger und I. Stepanovs, „Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging.," *IACR Cryptology ePrint Archive*, Jg. 2018, 2018. Adresse: https://eprint.iacr.org/2018/553.pdf
- [12] A. Bienstock u. a., „A More Complete Analysis of the Signal Double Ratchet Algorithm," 2022, https://eprint.iacr.org/2022/355. Adresse: https://eprint.iacr.org/2022/355

Triple Diffie-Hellman Key Exchange



Matrix und große Räume

- für jede Nachricht wird ein eigener neuer ephemeraler Schlüssel aus dem Session-Schlüsselpaar von Alice und Bob abgeleitet
- private Schlüssel nach der Nachricht vernichtet
- Jeder Sender hat eine eigene Ratsche (*outbound session* um Nachrichten an einen Raum zu verschlüsseln
- Raum-Mitglieder können die Ratschen-Historie lokal speichern, um die Nachrichten-Historie lokal zu speichern
- Kann vorwärts gespult werden, damit neue Mitglieder alte Nachrichten nicht lesen können
- Problem: n:n-Kommunikation mit $n \gg 1$ benötigt $\frac{n*n-1}{2}$ Verbindungen
- vollständiger Graph: n=25$\rightsquigarrow$ 300 ; n=50.000$\rightsquigarrow$ 1.249.975.000

Matrix und MLS

- https://opencode.de/de/software/synapse-mit-mls-4201
- https://matrix.org/blog/2023/07/a-giant-leap-with-mls/
- https://arewemlsyet.com/

3 Messaging Layer Security Protocol

3.1 Fähigkeiten

Messaging Layer Security

- Sicherheitsschicht für Ende-zu-Ende-Verschlüsselung
- sicheres und effizientes Protokoll
- Application Layer
- für große Gruppen mit bis zur 50 000 Teilnehmern
- Idee dazu 2016 auf der IETF96 in Berlin geboren
- 2017: Asynchronous Ratcheting Trees
- 29.3.2023: MLS von der IETF als neuer Standard verabschiedet
- Draft für PQC (ML-KEM) läuft

Messaging Layer Security

- Schlüssel-Einigungs-Protokoll für Gruppen
- für z.B. Instant Messaging
- Schutz gegen Abhören, Manipulation, gefälschte Nachrichten,
- Forward Secrecy und Post Compromise Security
- Geteilter, geschützter Gruppen-Zustand (Mitgliedschaft, krypt. Eigenschaften ...)
- Nachrichten-Konsistenz in Gruppe: jedes Mitglied erhält die gleiche Nachricht
- Architektur *und* Protokoll
- *kein* Nachrichtenprotokoll
- MLS soll in XMPP oder Matrix eingebettet werden
- MLS kann auch ohne kryptographische Absicherung eingesetzt werden
- kann föderiert werden

Literatur:

- [13] J. Alwen u. a., „Continuous group key agreement with active security," in *Theory of Cryptography Conference*, Springer, 2020, S. 261–290. Adresse: https://eprint.iacr.org/2020/752.pdf
- [14] K. Hashimoto, S. Katsumata und T. Prest, *How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum*, Cryptology ePrint Archive, Paper 2022/1533, 2022. DOI: 10.1145/3548606.3560679. Adresse: https://eprint.iacr.org/2022/1533
- [15] N. Kobeissi, K. Bhargavan und B. Blanchet, „Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, S. 435–450. DOI: 10.1109/EuroSP.2017.38

Logischer Aufbau

- *Clients* bilden *Gruppen*
- Gruppen bilden *Epochen*, z.B. wenn sich Eigenschaften der Gruppe ändern
- Jede Gruppe wird als Baum repräsentiert
- Gruppenmitglieder sind Blätter des Baumes
- Untergruppen des Baumes können effizient verschlüsseln
- jeder Client hat ein `LeafNode` mit Identität, Credentials und Fähigkeiten
- Fähigkeiten: des eingesetzten MLS-Protokolls und/oder Erweiterungen

3.2 Architektur

Abstrakte Dienste

Authentication Service (AS)

- attestiert die Beziehung von öffentlichen MLS-Schlüsseln und der Identität
- generiert Credentials die diese Beziehung codieren
- validiert diese Credentials

Delivery Service (DS)

- verteilt Nachrichten an Gruppenmitglieder
- speichert und verteilt öffentliche Schlüssel (`KeyPackage`), die benötigt werden um geheime Gruppenschlüssel auszuhandeln

Dienste können im Netz verteilt sein

Synchronität

- jede MLS-Operation kann asynchron ausgeführt werden
- Gruppen-Schlüssel können aktualisiert werden
- Mitglieder entfernen oder reinlassen
- Nachrichten verschicken
- Transportschicht des Messengers muss dafür sorgen dass MLS-Nachrichten asynchron und verlässlich zugestellt werden

Access Control

- Alle Gruppenmitglieder mit Zugriff auf den Gruppenschlüssel können Gruppen-Operationen starten
- jedes Gruppenmitglied kann Mitglieder entfernen/reinlassen
- Messenger muss Access Control implementieren
- z.B. Gruppenadministratoren ernennen oder offene Foren zulassen
- Handshake-Nachrichten können unverschlüsselt gesendet werden z.B. für ACL
- Transportverschlüsselung wichtig!

TreeSync Protokoll

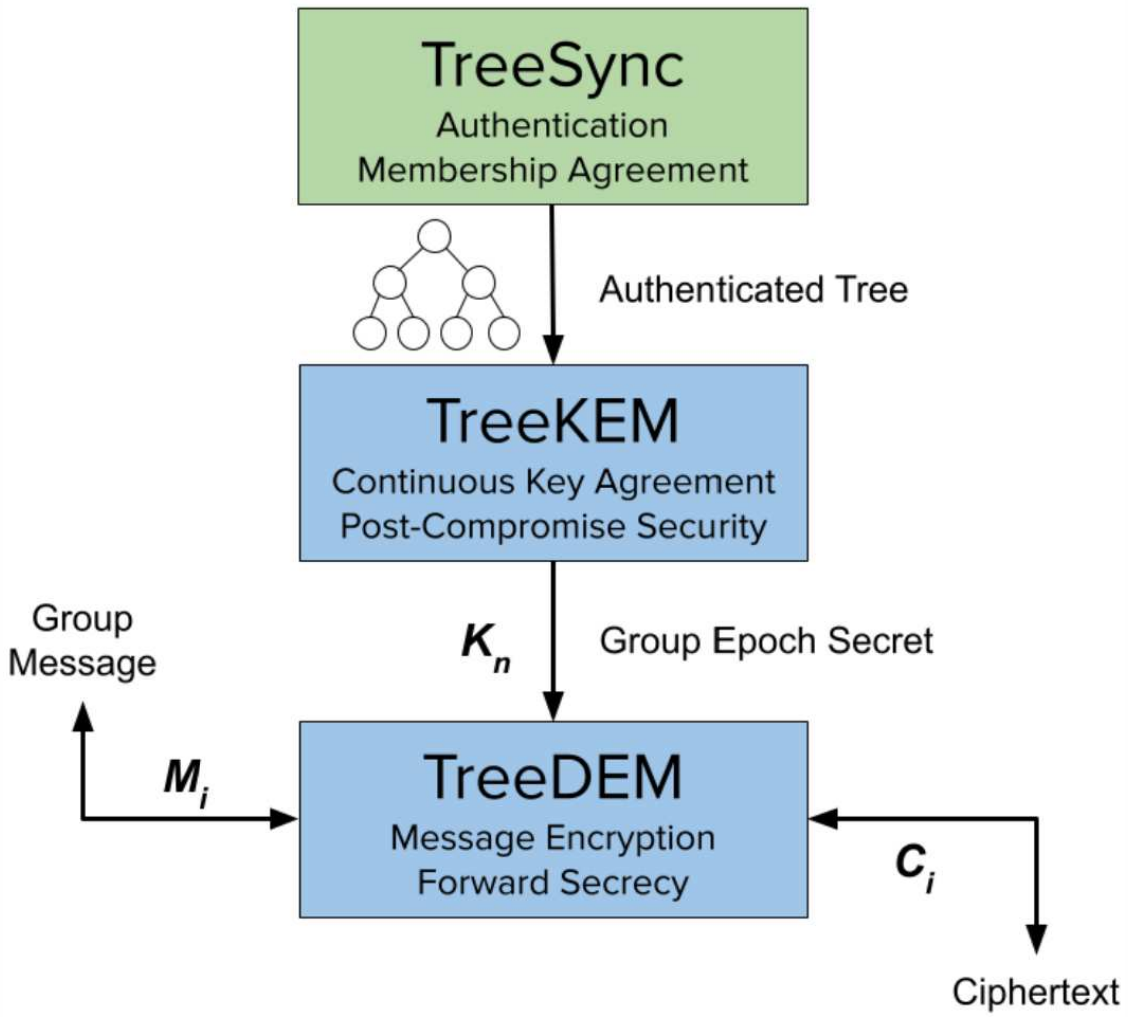
- synchronisiert den geteilten Gruppen-Zustand zwischen den Gruppenmitgliedern
- als Binär-Baum
- jedes Blatt repräsentiert ein Mitglied
- Gruppenzustand wird über Signaturen in Merkle-Bäumen authentifiziert
- Datenstruktur des Baumes stellt eine interne Integritäts-Invariante sicher
- authentifizierter, synchronisierter Zustand wird an TreeKEM übergeben

TreeKEM Protokoll

- ermöglicht es jedem Gruppenmitglied seine geheimen Schlüssel zu nutzen
- auf der Sequenz von authentifizierten Zuständen aus TreeSync
- um eine Sequenz von Gruppen-Schlüsseln (sog. Epochen-Geheimnissen) abzuleiten
- nutzt Baumstruktur für effiziente Updates: logarithmische Anzahl an Verschlüsselungen und 1 Entschlüsselungen
- Post Compromise Security und Schutz gegen ehemalige Gruppenmitglieder

TreeDEM Protokoll

- nimmt das Epochen-Geheimnis von TreeKEM
- leitet davon Nachrichten-Verschlüsselungs-Schlüssel für jedes Gruppenmitglied ab
- nach jeder Nachricht wird der Nachrichten-Verschlüsselungs-Schlüssel weiter geratscht
- um Forward Secrecy zu bekommen



aus [16]

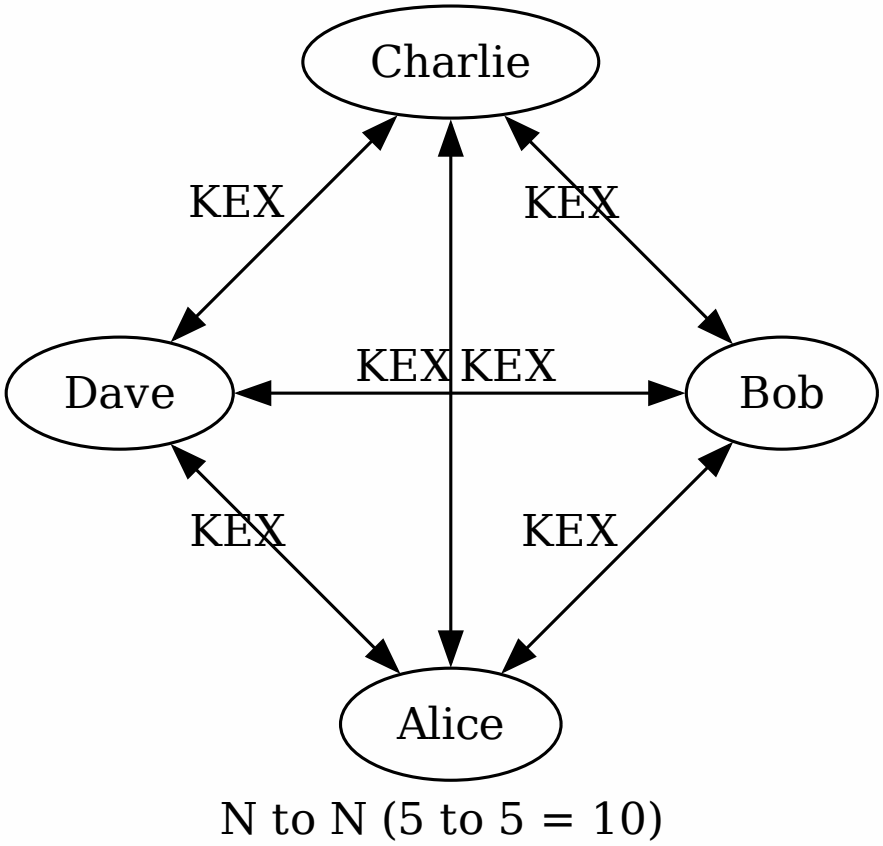
Literatur:

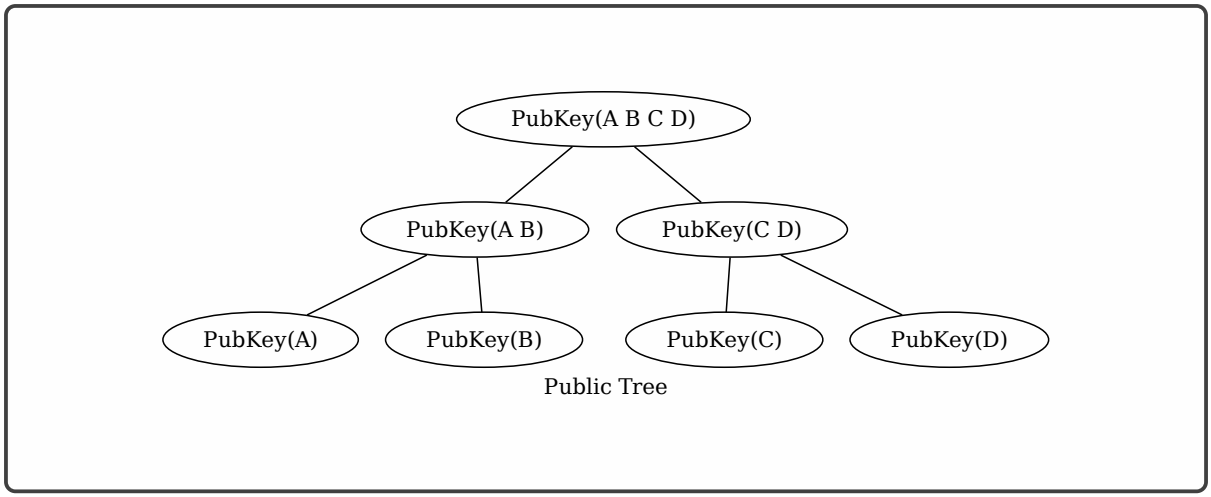
- [16] T. Wallez, J. Protzenko und K. Bhargavan, *TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security*, Cryptology ePrint Archive, Paper 2025/410, 2025. Adresse: https://eprint.iacr.org/2025/410
- [17] T. Wallez u. a., „{TreeSync}: authenticated group management for messaging layer security," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, S. 1217–1233
- [18] T. Wallez, J. Protzenko und K. Bhargavan, „TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security," in *2025 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2025, S. 4375–4390
- [19] C. Cremers u. a., *ETK: External-Operations TreeKEM and the Security of MLS in RFC 9420*, Cryptology ePrint Archive, Paper 2025/229, 2025. Adresse: https://eprint.iacr.org/2025/229
- [20] T. Wallez u. a., *TreeSync: Authenticated Group Management for Messaging Layer Security*, Cryptology ePrint Archive, Paper 2022/1732, 2022. Adresse: https://eprint.iacr.org/2022/1732
- [21] J. Alwen u. a., *Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement*, Cryptology ePrint Archive, Paper 2019/1489, 2019. Adresse: https://eprint.iacr.org/2019/1489

3.3 Ratschenbaum

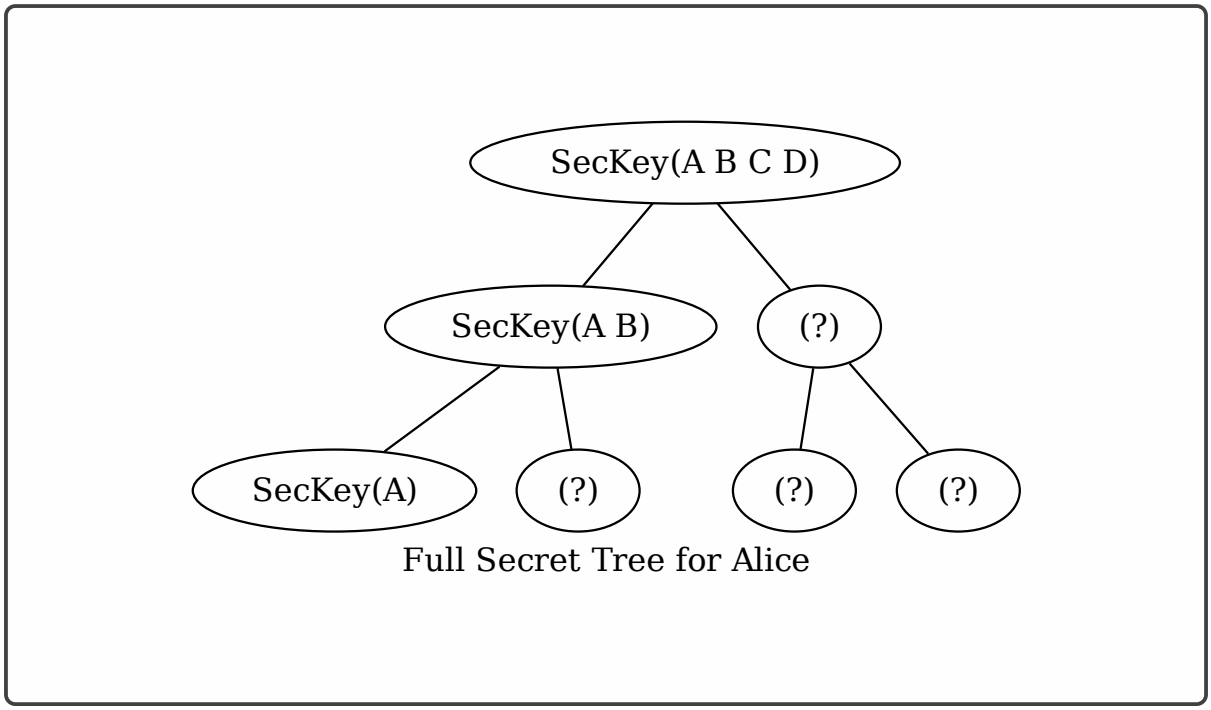
Ratschenbäume

- MLS nutzt ebenfalls Ratschen-Bäume
- als perfekt ausbalancierte Binär-Bäume
- Jedes Gruppenmitglied ist einem Blatt zugeordnet
- Pfad zur Wurzel enthält alle geheime Schlüssel, die das Mitglied kennt
- Der geheime Schlüssel in einem Knoten ist einem Mitglied nur bekannt, wenn der Unterbaum des betreffenden Knoten das Blatt des Mitglied beinhaltet

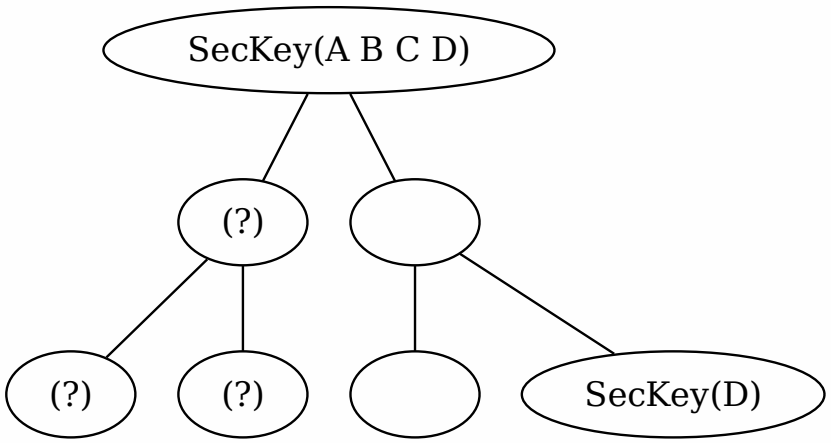




Public Tree



Full Secret Tree for Alice



Secret Tree with hole for Dave

3.4 Sicherheitseigenschaften

Sicherheitseigenschaften

- Nachrichten: E2EE sichert Vertraulichkeit und Integrität *aber* Metadaten ohne TLS sichtbar
- Gruppengeheimnisse: werden aus dem Ratschenbaum abgeleitet, Private Schlüssel sind nur Mitgliedern des Unterbaumes (der Gruppe) bekannt, C können an alle $n-1$ Mitglieder mit logarithmischen Aufwand verschickt werden. Schlüsselrotation und Mitglieder-Entfernung effizient möglich (logarithmisch)
- Vertraulichkeit des Absenders: Nachricht und Absenderdaten werden mittels AEAD-Ciphersuiten verschlüsselt, die einen privaten Schlüssel des Absenders nutzen. Nachrichten sind damit de facto kollisionsresistent

Literatur:

- [22] M. Bellare, R. Ng und B. Tackmann, „Nonces Are Noticed: AEAD Revisited," in *Advances in Cryptology – CRYPTO 2019*, A. Boldyreva und D. Micciancio, Hrsg., Cham: Springer International Publishing, 2019, S. 235–265, ISBN: 978-3-030-26948-7
- [23] C. Brzuska, E. Cornelissen und K. Kohbrok, *Cryptographic Security of the MLS RFC, Draft 11*, Cryptology ePrint Archive, Paper 2021/137, 2021. Adresse: https://eprint.iacr.org/2021/137
- [24] J. Alwen u. a., *Security Analysis and Improvements for the IETF MLS Standard for Group Messaging*, Cryptology ePrint Archive, Paper 2019/1189, 2019. Adresse: https://eprint.iacr.org/2019/1189
- [25] J. Alwen u. a., *Modular Design of Secure Group Messaging Protocols and the Security of MLS*, Cryptology ePrint Archive, Paper 2021/1083, 2021. Adresse: https://eprint.iacr.org/2021/1083
- [26] J. Alwen, D. Jost und M. Mularczyk, *On The Insider Security of MLS*, Cryptology ePrint Archive, Paper 2020/1327, 2020. Adresse: https://eprint.iacr.org/2020/1327

- [27] K. Cohn-Gordon u. a., *On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees*, Cryptology ePrint Archive, Paper 2017/666, 2017. Adresse: https://eprint.iacr.org/2017/666
- [28] N. Giancecchi, „Analysis and Implementation of the Messaging Layer Security Protocol," Diss. Adresse: https://amslaurea.unibo.it/id/eprint/18467/

Sicherheitseigenschaften

- Authentizität: AEAD-Ciphersuiten, kryptographische Signatur unter jeder Nachricht Signaturschlüssel verifiziert Identität des Mitglieds!
- Authentizität: *zusätzliche* Absicherung durch PSK in Applikation
- Gruppen-Fragmentierung: böswilliges Gruppenmitglied kann individuelle Update-Pfade erzeugen und Opfer aus dem Ratschen-Braum zwingen
  Applikation sollte Proposals von n Gruppenmitgliedern akzeptieren bevor diese committed werden

Gruppen-Metadaten

Unverschlüsselt:

- KeyPackage Nachrichten
- GroupInfo Nachrichten
- Der unverschlüsselte Teil der Welcome-Nachricht
- Proposal oder Commits die als PublicMessage gesendet werden
- Unverschlüsselte Header in PrivateMessage Nachrichten
- Die Länge von verschlüsselten Welcome und PrivateMessage Nachrichten

Transportverschlüsselung empfohlen!

Forward Secrecy

Forward Secrecy

- zwischen einzelnen Epochen: alte private Schlüssel werden aus dem Ratschen-Baum gelöscht
- in einer Epoche: private Nachrichtenschlüssel werden nach Verschlüsselung der Nachricht gelöscht
- NB: private Nachrichtenschlüssel werden zwischen allen Gruppenmitgliedern geteilt!
- Gefahr bei Offline-Mitgliedern! Applikation sollte Offline-Mitglieder entfernen können

Post-Compromise Security

Post-Compromise Security zwischen einzelnen Epochen:

- AktualPost Quantum Cryptography isierung der Blatt-Schlüssel der Mitglieder im Ratschen-Baum
  zukünftige Nachrichten werden mit neuen Schlüsseln verschlüsselt
- NB: PCS gilt erst gruppenweit, wenn alle Mitglieder den Update-Proposal commited haben!

KeyPackages

- enthalten u.a. den InitKey
- InitKey muss zur gewählten CipherSuite passen
- und einzigartig sein
- Mehrfach genutzte KeyPackages gefährden beides!
- Wiederbenutzung ist Ultima Ration gegen DoS-Attacke
- Applikation sollte KeyPackages regelmäßig neu generieren
- KeyPackage darf nicht kompromittiert werden!

Post Quantum Cryptography

- Post Quantum Cryptography
- Draft offen
- https://datatracker.ietf.org/doc/draft-ietf-mls-pq-ciphersuites/
- Mehr dazu in meinem 3. Vortrag zur Kryptokalypse

Kontakt

Fragen?

- cryptomancer.de
- kaishakunin.com
- https://mastodon.social/@0xKaishakunin
- 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF
- Matrix: @SchumaSte:matrix.org

Literatur

[1] P. D. Chowdhury u. a., „Threat Models over Space and Time: A Case Study of E2EE Messaging Applications," *arXiv preprint arXiv:2301.05653*, 2023.

[2] F. van der Have, „The X3DH Protocol: A Proof of Security," Diss., Raboud Uni, 2022.

[3] M. R. Albrecht, S. Celi, B. Dowling und D. Jones, „Practically-exploitable Cryptographic Vulnerabilities in Matrix," in *2023 IEEE Symposium on Security and Privacy (SP)*, IEEE Computer Society, 2022, S. 1419–1436.

[4] J. P. Degabriele, A. Lehmann, K. G. Paterson, N. P. Smart und M. Strefler, *On the Joint Security of Encryption and Signature in EMV*, Cryptology ePrint Archive, Paper 2011/615, https://eprint.iacr.org/2011/615, 2011. Adresse: https://eprint.iacr.org/2011/615.

[5] C. Cremers und M. Feltz, *One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability*, Cryptology ePrint Archive, Paper 2011/300, https://eprint.iacr.org/2011/300, 2011. Adresse: https://eprint.iacr.org/2011/300.

[6] M. Marlinspike, „The Double Ratchet Algorithm," Tech Report, 20. Nov. 2016.

[7] V. Moscaritolo, G. Belvin und P. Zimmermann, „Silent circle instant messaging protocol protocol specification," *Online, White Paper*, S. 47, 2012.

[8] J. Alwen, S. Coretti und Y. Dodis, „The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol," in *IACR Cryptol. ePrint Arch.*, 2018. Adresse: https://cs.nyu.edu/~dodis/ps/signal.pdf.

[9] K. Cohn-Gordon, C. J. F. Cremers, B. Dowling, L. Garratt und D. Stebila, „A Formal Security Analysis of the Signal Messaging Protocol," *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, S. 451–466, 2017. Adresse: https://eprint.iacr.org/2016/1013.pdf.

[10] J. Alwen, S. Coretti und Y. Dodis, „The double ratchet: security notions, proofs, and modularization for the signal protocol," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2019, S. 129–158. Adresse: https://eprint.iacr.org/2018/1037.pdf.

[11] J. Jaeger und I. Stepanovs, „Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging.," *IACR Cryptology ePrint Archive*, Jg. 2018, 2018. Adresse: https://eprint.iacr.org/2018/553.pdf.

[12] A. Bienstock, J. Fairoze, S. Garg, P. Mukherjee und S. Raghuraman, „A More Complete Analysis of the Signal Double Ratchet Algorithm," 2022, https://eprint.iacr.org/2022/355. Adresse: https://eprint.iacr.org/2022/355.

[13] J. Alwen, S. Coretti, D. Jost und M. Mularczyk, „Continuous group key agreement with active security," in *Theory of Cryptography Conference*, Springer, 2020, S. 261–290. Adresse: https://eprint.iacr.org/2020/752.pdf.

[14] K. Hashimoto, S. Katsumata und T. Prest, *How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum*, Cryptology ePrint Archive, Paper 2022/1533, 2022. DOI: 10.1145/3548606.3560679. Adresse: https://eprint.iacr.org/2022/1533.

[15] N. Kobeissi, K. Bhargavan und B. Blanchet, „Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, S. 435–450. DOI: 10.1109/EuroSP.2017.38.

[16] T. Wallez, J. Protzenko und K. Bhargavan, *TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security*, Cryptology ePrint Archive, Paper 2025/410, 2025. Adresse: https://eprint.iacr.org/2025/410.

[17] T. Wallez, J. Protzenko, B. Beurdouche und K. Bhargavan, „{TreeSync}: authenticated group management for messaging layer security," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, S. 1217–1233.

[18] T. Wallez, J. Protzenko und K. Bhargavan, „TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security," in *2025 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2025, S. 4375–4390.

[19] C. Cremers, E. Günsay, V. Wesselkamp und M. Zhao, *ETK: External-Operations TreeKEM and the Security of MLS in RFC 9420*, Cryptology ePrint Archive, Paper 2025/229, 2025. Adresse: https://eprint.iacr.org/2025/229.

[20] T. Wallez, J. Protzenko, B. Beurdouche und K. Bhargavan, *TreeSync: Authenticated Group Management for Messaging Layer Security*, Cryptology ePrint Archive, Paper 2022/1732, 2022. Adresse: https://eprint.iacr.org/2022/1732.

[21] J. Alwen u. a., *Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement*, Cryptology ePrint Archive, Paper 2019/1489, 2019. Adresse: https://eprint.iacr.org/2019/1489.

[22] M. Bellare, R. Ng und B. Tackmann, „Nonces Are Noticed: AEAD Revisited," in *Advances in Cryptology – CRYPTO 2019*, A. Boldyreva und D. Micciancio, Hrsg., Cham: Springer International Publishing, 2019, S. 235–265, ISBN: 978-3-030-26948-7.

[23] C. Brzuska, E. Cornelissen und K. Kohbrok, *Cryptographic Security of the MLS RFC, Draft 11*, Cryptology ePrint Archive, Paper 2021/137, 2021. Adresse: https://eprint.iacr.org/2021/137.

[24] J. Alwen, S. Coretti, Y. Dodis und Y. Tselekounis, *Security Analysis and Improvements for the IETF MLS Standard for Group Messaging*, Cryptology ePrint Archive, Paper 2019/1189, 2019. Adresse: https://eprint.iacr.org/2019/1189.

[25] J. Alwen, S. Coretti, Y. Dodis und Y. Tselekounis, *Modular Design of Secure Group Messaging Protocols and the Security of MLS*, Cryptology ePrint Archive, Paper 2021/1083, 2021. Adresse: https://eprint.iacr.org/2021/1083.

[26] J. Alwen, D. Jost und M. Mularczyk, *On The Insider Security of MLS*, Cryptology ePrint Archive, Paper 2020/1327, 2020. Adresse: https://eprint.iacr.org/2020/1327.

[27] K. Cohn-Gordon, C. Cremers, L. Garratt, J. Millican und K. Milner, *On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees*, Cryptology ePrint Archive, Paper 2017/666, 2017. Adresse: https://eprint.iacr.org/2017/666.

[28] N. Giancecchi, „Analysis and Implementation of the Messaging Layer Security Protocol," Diss. Adresse: https://amslaurea.unibo.it/id/eprint/18467/.

[29] N. Borisov, I. Goldberg und E. Brewer, „Off-the-record communication, or, why not to use PGP," in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, 2004, S. 77–84.

[30] M. Di Raimondo, R. Gennaro und H. Krawczyk, „Secure off-the-record messaging," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 2005, S. 81–89.

[31] C. Alexander und I. Goldberg, „Improved user authentication in off-the-record messaging," in *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, 2007, S. 41–47.

[32] „Kryptographische Verfahren, Empfehlungen und Schlüssellängen," Bonn, Technische Richtlinie TR-02102-1 2022-01, 2022.

[33] „Kryptographische Verfahren, Verwendung von Transport Layer Security (TLS)," Bonn, Technische Richtlinie des BSI TR-02102-2 2022/01, 2022.

[34] V. Vehkaoja, „End-to-end encryption protocol for internet of things devices," *University of Oulu, degree programme in computer science and engineering, Master's Thesis*, Jg. 38, 2017. Adresse: http://jultika.oulu.fi/files/nbnfioulu-201706022469.pdf.

[35] D. Stebila, *Security analysis of the iMessage PQ3 protocol*, Cryptology ePrint Archive, Paper 2024/357, 2024. Adresse: https://eprint.iacr.org/2024/357.

[36] K. Hashimoto, S. Katsumata und G. Pascual-Perez, *Exploring How to Authenticate Application Messages in MLS: More Efficient, Post-Quantum, and Anonymous Blocklistable*, Cryptology ePrint Archive, Paper 2025/426, 2025. Adresse: https://eprint.iacr.org/2025/426.

[37] J. Alwen, S. Coretti, D. Jost und M. Mularczyk, *Continuous Group Key Agreement with Active Security*, Cryptology ePrint Archive, Paper 2020/752, 2020. Adresse: https://eprint.iacr.org/2020/752.

[38] J. Alwen, D. Hartmann, E. Kiltz und M. Mularczyk, *Server-Aided Continuous Group Key Agreement*, Cryptology ePrint Archive, Paper 2021/1456, 2021. DOI: 10.1145/3548606.3560632. Adresse: https://eprint.iacr.org/2021/1456.

[39] B. Miller, L. Huang, A. D. Joseph und J. D. Tygar, „I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis," in *Privacy Enhancing Technologies*, E. De Cristofaro und S. J. Murdoch, Hrsg., Cham: Springer International Publishing, 2014, S. 143–163, ISBN: 978-3-319-08506-7.

[40] M. Husák, M. Čermák, T. Jirsík und P. Čeleda, „HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting," *EURASIP Journal on Information Security*, Jg. 2016, Nr. 1, S. 6, 2016.

[41] E. Marstrander, „Use of Messaging Layer Security in a Military UAV Swarm," Magisterarb., NTNU, 2023.

[42] D. Soler, C. Dafonte, M. Fernández-Veiga, A. F. Vilas und F. J. Nóvoa, „Experimental Analysis of Efficiency of the Messaging Layer Security for Multiple Delivery Services," *arXiv preprint arXiv:2502.18303*, 2025.