Meine Bibliographie-Sammlung zu diversen Kryptographie-Vorträgen. Unsortiert und u.U. mit doppelten Einträgen. Sortiert nach den Vorträgen, in denen die Bib erzeugt wurde.

Stand: 11. Juni 2026

1 Signal, Matrix, MLS, SPQR

- Chowdhury, P. D., Sameen, M., Blessing, J., Boucher, N., Gardiner, J., Burrows, T., Anderson, R., & Rashid, A. (2023). Threat Models over Space and Time: A Case Study of E2EE Messaging Applications. *arXiv preprint arXiv:2301.05653*
- Albrecht, M. R., Celi, S., Dowling, B., & Jones, D. (2022). Practically-exploitable Cryptographic Vulnerabilities in Matrix. *2023 IEEE Symposium on Security and Privacy (SP)*, 1419–1436
- van der Have, F. (2022). *The X3DH Protocol: A Proof of Security* [Diss., Raboud Uni]
- Degabriele, J. P., Lehmann, A., Paterson, K. G., Smart, N. P., & Strefler, M. (2011). On the Joint Security of Encryption and Signature in EMV [https://eprint.iacr.org/2011/615]. https://eprint.iacr.org/2011/615
- Cremers, C., & Feltz, M. (2011). One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability [https://eprint.iacr.org/2011/300]. https://eprint.iacr.org/2011/300
- Marlinspike, M. (2016, 20. November). *The Double Ratchet Algorithm* (T. Perrin, Hrsg.; Tech Report)
- Borisov, N., Goldberg, I., & Brewer, E. (2004). Off-the-record communication, or, why not to use PGP. *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, 77–84
- Di Raimondo, M., Gennaro, R., & Krawczyk, H. (2005). Secure off-the-record messaging. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 81–89
- Alexander, C., & Goldberg, I. (2007). Improved user authentication in off-the-record messaging. *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, 41–47
- Moscaritolo, V., Belvin, G., & Zimmermann, P. (2012). Silent circle instant messaging protocol protocol specification. *Online, White Paper*, 47
- *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* (Technische Richtlinie Nr. TR-02102-1 2022-01). (2022a). Bonn, Bundesamt für Sicherheit in der Informationstechnik
- *Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)* (Technische Richtlinie des BSI Nr. TR-02102-2 2022/01). (2022b). Bonn, Bundesamt für Sicherheit in der Informationstechnik
- Alwen, J., Coretti, S., & Dodis, Y. (2018). The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol. *IACR Cryptol. ePrint Arch.* https://cs.nyu.edu/~dodis/ps/signal.pdf

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

- Alwen, J., Coretti, S., & Dodis, Y. (2019). The double ratchet: security notions, proofs, and modularization for the signal protocol. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 129–158. https://eprint.iacr.org/2018/1037.pdf

- Jaeger, J., & Stepanovs, I. (2018). Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging. *IACR Cryptology ePrint Archive*, *2018*. https://eprint.iacr.org/2018/553.pdf

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

- Bienstock, A., Fairoze, J., Garg, S., Mukherjee, P., & Raghuraman, S. (2022). A More Complete Analysis of the Signal Double Ratchet Algorithm [https://eprint.iacr.org/2022/355]. Cryptology ePrint Archive, Paper 2022/355. https://eprint.iacr.org/2022/355

- Stebila, D. (2024). Security analysis of the iMessage PQ3 protocol. https://eprint.iacr.org/2024/357

- Hashimoto, K., Katsumata, S., & Prest, T. (2022). How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum. https://doi.org/10.1145/3548606.3560679

- Kobeissi, N., Bhargavan, K., & Blanchet, B. (2017). Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 435–450. https://doi.org/10.1109/EuroSP.2017.38

- Hashimoto, K., Katsumata, S., & Pascual-Perez, G. (2025). *Exploring how to authenticate application messages in mls: More efficient, post-quantum, and anonymous blocklistable*. 2025/426. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2025/426

- Alwen, J., Capretto, M., Cueto, M., Kamath, C., Klein, K., Markov, I., Pascual-Perez, G., Pietrzak, K., Walter, M., & Yeo, M. (2019). Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement. https://eprint.iacr.org/2019/1489

- Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. (2019). *Security analysis and improvements for the ietf mls standard for group messaging*. 2019/1189. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2019/1189

- Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. (2021). *Modular design of secure group messaging protocols and the security of mls*. 2021/1083. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2021/1083
- Alwen, J., Coretti, S., Jost, D., & Mularczyk, M. (2020). Continuous group key agreement with active security. *Theory of Cryptography Conference*, 261–290. https://eprint.iacr.org/2020/752.pdf
- Alwen, J., Hartmann, D., Kiltz, E., & Mularczyk, M. (2021). Server-Aided Continuous Group Key Agreement. https://doi.org/10.1145/3548606.3560632
- Alwen, J., Jost, D., & Mularczyk, M. (2020). On The Insider Security of MLS. https://eprint.iacr.org/2020/1327
- Wallez, T., Protzenko, J., & Bhargavan, K. (2025). TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security. *IEEE*. https://eprint.iacr.org/2025/410
- Wallez, T., Protzenko, J., Beurdouche, B., & Bhargavan, K. (2023). *TreeSync: Authenticated Group Management for Messaging Layer Security*. https://eprint.iacr.org/2022/1732
- Cremers, C., Günsay, E., Wesselkamp, V., & Zhao, M. (2025). ETK: External-Operations TreeKEM and the Security of MLS in RFC 9420. https://eprint.iacr.org/2025/229
- Brzuska, C., Cornelissen, E., & Kohbrok, K. (2021). Cryptographic Security of the MLS RFC, Draft 11. https://eprint.iacr.org/2021/137
- Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. (2017). On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees. https://eprint.iacr.org/2017/666
- Miller, B., Huang, L., Joseph, A. D., & Tygar, J. D. (2014). I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis. In E. De Cristofaro & S. J. Murdoch (Hrsg.), *Privacy Enhancing Technologies* (S. 143–163). Springer International Publishing
- Bellare, M., Ng, R., & Tackmann, B. (2019). Nonces Are Noticed: AEAD Revisited. In A. Boldyreva & D. Micciancio (Hrsg.), *Advances in Cryptology – CRYPTO 2019* (S. 235–265). Springer International Publishing
- Husák, M., Čermák, M., Jirsík, T., & Čeleda, P. (2016). HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting. *EURASIP Journal on Information Security*, *2016*(1), 6
- Giancecchi, N. (n. d.). *Analysis and Implementation of the Messaging Layer Security Protocol* [Diss.]. https://amslaurea.unibo.it/id/eprint/18467/

- Marstrander, E. (2023). *Use of Messaging Layer Security in a Military UAV Swarm* [Magisterarb., NTNU]
- Soler, D., Dafonte, C., Fernández-Veiga, M., Fernández Vilas, A., & Nóvoa, F. J. (2025, Februar). *Experimental analysis of efficiency of the messaging layer security for multiple delivery services*. arXiv: 2502.18303 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2502.18303
- Jaeger, J., & Kumar, A. (2025). *Analyzing group chat encryption in mls, session, signal, and matrix*. 2025/554. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2025/554
- Azari, K., & Ellison, A. (2024). *Tighter provable security for treekem*. 2024/1878. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2024/1878
- Soler, D., Dafonte, C., Fernández-Veiga, M., Fernández Vilas, A., & Nóvoa, F. J. (2024, Mai). *Attribute-based authentication in secure group messaging for distributed environments*. arXiv: 2405.12042 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2405.12042
- Kundu, A., Chakraborty, V., & Kompella, R. (2026, April). *Post-quantum cryptographic analysis of message transformations across the network stack*. arXiv: 2604.08480 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2604.08480
- Balbás, D., Collins, D., & Gajland, P. (2023, Januar). *Analysis and improvements of the sender keys protocol for group messaging*. arXiv: 2301.07045 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2301.07045
- Brendel, J., Fiedler, R., Günther, F., Janson, C., & Stebila, D. (2021). Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake. https://doi.org/10.1007/978-3-030-97131-1_1
- Auerbach, B., Dodis, Y., Jost, D., Katsumata, S., Prest, T., & Schmidt, R. (2025, September). *Post-quantum ratcheting for signal*. Verfügbar 18. April 2026 unter https://csrc.nist.gov/csrc/media/events/2025/sixth-pqc-standardization-conference/post-quantum%20ratcheting%20for%20signal.pdf

Literatur

Albrecht, M. R., Celi, S., Dowling, B., & Jones, D. (2022). Practically-exploitable Cryptographic Vulnerabilities in Matrix. *2023 IEEE Symposium on Security and Privacy (SP)*, 1419–1436.

Alexander, C., & Goldberg, I. (2007). Improved user authentication in off-the-record messaging. *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, 41–47.

Alwen, J., Capretto, M., Cueto, M., Kamath, C., Klein, K., Markov, I., Pascual-Perez, G., Pietrzak, K., Walter, M., & Yeo, M. (2019). Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement. https://eprint.iacr.org/2019/1489

Alwen, J., Coretti, S., & Dodis, Y. (2018). The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol. *IACR Cryptol. ePrint Arch.* https://cs.nyu.edu/~dodis/ps/signal.pdf

Alwen, J., Coretti, S., & Dodis, Y. (2019). The double ratchet: security notions, proofs, and modularization for the signal protocol. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 129–158. https://eprint.iacr.org/2018/1037.pdf

Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. (2019). *Security analysis and improvements for the ietf mls standard for group messaging*. 2019/1189. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2019/1189

Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. (2021). *Modular design of secure group messaging protocols and the security of mls*. 2021/1083. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2021/1083

Alwen, J., Coretti, S., Jost, D., & Mularczyk, M. (2020). Continuous group key agreement with active security. *Theory of Cryptography Conference*, 261–290. https://eprint.iacr.org/2020/752.pdf

Alwen, J., Hartmann, D., Kiltz, E., & Mularczyk, M. (2021). Server-Aided Continuous Group Key Agreement. https://doi.org/10.1145/3548606.3560632

Alwen, J., Jost, D., & Mularczyk, M. (2020). On The Insider Security of MLS. https://eprint.iacr.org/2020/1327

Auerbach, B., Dodis, Y., Jost, D., Katsumata, S., Prest, T., & Schmidt, R. (2025, September). *Post-quantum ratcheting for signal*. Verfügbar 18. April 2026 unter https://csrc.nist.gov/csrc/media/events/2025/sixth-pqc-standardization-conference/post-quantum%20ratcheting%20for%20signal.pdf

Azari, K., & Ellison, A. (2024). *Tighter provable security for treekem*. 2024/1878. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2024/1878

Balbás, D., Collins, D., & Gajland, P. (2023, Januar). *Analysis and improvements of the sender keys protocol for group messaging*. arXiv: 2301.07045 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2301.07045

Bellare, M., Ng, R., & Tackmann, B. (2019). Nonces Are Noticed: AEAD Revisited. In A. Boldyreva & D. Micciancio (Hrsg.), *Advances in Cryptology – CRYPTO 2019* (S. 235–265). Springer International Publishing.

Bienstock, A., Fairoze, J., Garg, S., Mukherjee, P., & Raghuraman, S. (2022). A More Complete Analysis of the Signal Double Ratchet Algorithm [https://eprint.iacr.org/2022/355]. Cryptology ePrint Archive, Paper 2022/355. https://eprint.iacr.org/2022/355

Borisov, N., Goldberg, I., & Brewer, E. (2004). Off-the-record communication, or, why not to use PGP. *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, 77–84.

Brendel, J., Fiedler, R., Günther, F., Janson, C., & Stebila, D. (2021). Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake. https://doi.org/10.1007/978-3-030-97131-1_1

Brzuska, C., Cornelissen, E., & Kohbrok, K. (2021). Cryptographic Security of the MLS RFC, Draft 11. https://eprint.iacr.org/2021/137

Chowdhury, P. D., Sameen, M., Blessing, J., Boucher, N., Gardiner, J., Burrows, T., Anderson, R., & Rashid, A. (2023). Threat Models over Space and Time: A Case Study of E2EE Messaging Applications. *arXiv preprint arXiv:2301.05653*.

Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. (2017). On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees. https://eprint.iacr.org/2017/666

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

Cremers, C., & Feltz, M. (2011). One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability [https://eprint.iacr.org/2011/300]. https://eprint.iacr.org/2011/300

Cremers, C., Günsay, E., Wesselkamp, V., & Zhao, M. (2025). ETK: External-Operations TreeKEM and the Security of MLS in RFC 9420. https://eprint.iacr.org/2025/229

Degabriele, J. P., Lehmann, A., Paterson, K. G., Smart, N. P., & Strefler, M. (2011). On the Joint Security of Encryption and Signature in EMV [https://eprint.iacr.org/2011/615]. https://eprint.iacr.org/2011/615

Di Raimondo, M., Gennaro, R., & Krawczyk, H. (2005). Secure off-the-record messaging. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 81–89.

Giancecchi, N. (n. d.). *Analysis and Implementation of the Messaging Layer Security Protocol* [Diss.]. https://amslaurea.unibo.it/id/eprint/18467/

Hashimoto, K., Katsumata, S., & Pascual-Perez, G. (2025). *Exploring how to authenticate application messages in mls: More efficient, post-quantum, and anonymous blocklistable*. 2025/426. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2025/426

Hashimoto, K., Katsumata, S., & Prest, T. (2022). How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum. https://doi.org/10.1145/3548606.3560679

Husák, M., Čermák, M., Jirsík, T., & Čeleda, P. (2016). HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting. *EURASIP Journal on Information Security*, *2016*(1), 6.

Jaeger, J., & Kumar, A. (2025). *Analyzing group chat encryption in mls, session, signal, and matrix*. 2025/554. Verfügbar 18. April 2026 unter https://eprint.iacr.org/2025/554

Jaeger, J., & Stepanovs, I. (2018). Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging. *IACR Cryptology ePrint Archive*, *2018*. https://eprint.iacr.org/2018/553.pdf

Kobeissi, N., Bhargavan, K., & Blanchet, B. (2017). Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 435–450. https://doi.org/10.1109/EuroSP.2017.38

Kryptographische Verfahren: Empfehlungen und Schlüssellängen (Technische Richtlinie Nr. TR-02102-1 2022-01). (2022a). Bonn, Bundesamt für Sicherheit in der Informationstechnik.

Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS) (Technische Richtlinie des BSI Nr. TR-02102-2 2022/01). (2022b). Bonn, Bundesamt für Sicherheit in der Informationstechnik.

Kundu, A., Chakraborty, V., & Kompella, R. (2026, April). *Post-quantum cryptographic analysis of message transformations across the network stack*. arXiv: 2604.08480 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2604.08480

Marlinspike, M. (2016, 20. November). *The Double Ratchet Algorithm* (T. Perrin, Hrsg.; Tech Report).

Marstrander, E. (2023). *Use of Messaging Layer Security in a Military UAV Swarm* [Magisterarb., NTNU].

Miller, B., Huang, L., Joseph, A. D., & Tygar, J. D. (2014). I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis. In E. De Cristofaro & S. J. Murdoch (Hrsg.), *Privacy Enhancing Technologies* (S. 143–163). Springer International Publishing.

Moscaritolo, V., Belvin, G., & Zimmermann, P. (2012). Silent circle instant messaging protocol protocol specification. *Online, White Paper*, 47.

Soler, D., Dafonte, C., Fernández-Veiga, M., Fernández Vilas, A., & Nóvoa, F. J. (2024, Mai). *Attribute-based authentication in secure group messaging for distributed environments*. arXiv: 2405.12042 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2405.12042

Soler, D., Dafonte, C., Fernández-Veiga, M., Fernández Vilas, A., & Nóvoa, F. J. (2025, Februar). *Experimental analysis of efficiency of the messaging layer security for multiple delivery services*. arXiv: 2502.18303 [cs.CR]. Verfügbar 18. April 2026 unter https://arxiv.org/abs/2502.18303

Stebila, D. (2024). Security analysis of the iMessage PQ3 protocol. https://eprint.iacr.org/2024/357

van der Have, F. (2022). *The X3DH Protocol: A Proof of Security* [Diss., Raboud Uni].

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

Wallez, T., Protzenko, J., Beurdouche, B., & Bhargavan, K. (2023). *TreeSync: Authenticated Group Management for Messaging Layer Security*. https://eprint.iacr.org/2022/1732

Wallez, T., Protzenko, J., & Bhargavan, K. (2025). TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security. *IEEE*. https://eprint.iacr.org/2025/410