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: 8. Februar 2026

# 1 Unternehmen Rubikon


- Strehle, R. (1994). *Verschlüsselt: Der Fall Hans Bühler*. Werd Verlag
- Sassòli, M. (2021). Die Schweizerische Neutralität und der Fall Crypto AG [Open Access]. *Swiss Review of International and European Law*, *31*(4), 523–540. https://archive-ouverte.unige.ch/unige:166084
- Dymydiuk, J. (2020). Rubicon and revelation: The curious robustness of the 'secret' cia–bnd operation with crypto ag [Accepted Manuscript (Open Access) – WRAP Repository]. *Intelligence and National Security*, *35*(5), 641–658. https://doi.org/10.1080/02684527.2020.1774853
- Aldrich, R. J., Müller, P. F., Ridd, D., & Schmidt-Eenboom, E. (2020). Operation rubicon: Sixty years of german-american success in signals intelligence [Accepted Manuscript (Open Access) – WRAP Repository]. *Intelligence and National Security*, *35*(5), 603–607. https://doi.org/10.1080/02684527.2020.1774849
- Dobson, M. J. (2020). Operation rubicon: Germany as an intelligence 'great power'? *Intelligence and National Security*, *35*(5), 608–622. https://doi.org/10.1080/02684527.2019.1682621
- Frik, S. (2007). Boris hagelin and crypto ag: Pioneers of encryption. In R. Anderson & C. E. Landwehr (Hrsg.), *The history of information security* (S. 479–496). Elsevier. https://www.sciencedirect.com/science/article/pii/B9780080454880500273
- Moyes, H. (2020). The cryptographic trojan horse: Operation condor. *Chief Editor Caverlee Dahill, Assistant Editors Kate Brady*, 19–35
- Greenwald, G. (2014). *No place to hide: Edward snowden, the nsa, and the u.s. surveillance state*. Metropolitan Books. https://us.macmillan.com/books/9780805094560/noplace-to-hide
- Brustolin, V., de Oliveira, D., & dos Reis Peron, A. E. (2023). Exploring the relationship between crypto ag and the cia in the use of rigged encryption machines for espionage in brazil. *Cambridge Review of International Affairs*, *36*(1), 54–87. https://doi.org/10.1080/09557571.2022.2123456

# 2 DUAL_EC_PRNG


- Barker, E., & Kelsey, J. (2006, Juni). *Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90* (Special Publication Nr. SP 800-90) (Withdrawn March 14, 2007; provided for historical reference). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.SP.800-90

- National Institute of Standards and Technology. (2025, September). *Recommendation for Random Bit Generator (RBG) Constructions, NIST Special Publication 800-90C* (Special Publication Nr. SP 800-90C) (Final version published 25 September 2025; includes SP 800-90A Rev.1 and SP 800-90B). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.SP.800-90C

- National Institute of Standards and Technology. (2002, Dezember). *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards Publication Nr. FIPS PUB 140-2) (Includes Change Notice 1, December 2002). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.FIPS.140-2

- Young, A., & Yung, M. (1997a). Kleptography: Using Cryptography Against Cryptography. In W. Fumy (Hrsg.), *Advances in Cryptology — EUROCRYPT '97* (S. 62–74). Springer Berlin Heidelberg

- Young, A., & Yung, M. (1997b). The prevalence of kleptographic attacks on discrete-log based cryptosystems. In B. S. Kaliski (Hrsg.), *Advances in Cryptology — CRYPTO '97* (S. 264–276). Springer Berlin Heidelberg

- Brown, D. R. L. (2006). Conjectured Security of the ANSI-NIST Elliptic Curve RNG. https://eprint.iacr.org/2006/117

- Schoenmakers, B., & Sidorenko, A. (2006). Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator. https://eprint.iacr.org/2006/190

- Brown, D. R. L., & Gjøsteen, K. (2007). A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator. https://eprint.iacr.org/2007/048

- Goh, E.-J., Boneh, D., Pinkas, B., & Golle, P. (2003). The Design and Implementation of Protocol-Based Hidden Key Recovery. In J. C. Kwak & R. H. Deng (Hrsg.), *Information Security* (S. 165–179, Bd. 2851). Springer

- Young, A. L., & Yung, M. (2007). Space-Efficient Kleptography Without Random Oracles. *Information Hiding*, *4567*, 112–129

- Checkoway, S., Fredrikson, M., Niederhagen, R., Everspaugh, A., Green, M., Lange, T., Ristenpart, T., Bernstein, D. J., Maskiewicz, J., & Shacham, H. (2014). On the

Practical Exploitability of Dual EC in TLS Implementations. *Proceedings of the 23rd USENIX Security Symposium*, 319–335

- Wertheimer, M. (2015). Encryption and the NSA Role in International Standards. *Notices of the American Mathematical Society*, *62*(2), 165–167. https://doi.org/10.1090/noti1213

# 3 Huawei 5G

- Voelsen, D. (2019). 5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik. *SWP-Aktuell*, (5/2019). Verfügbar 13. Dezember 2023 unter https://www.ssoar.info/ssoar/bitstream/handle/document/61663/ssoar-2019-voelsen-5G_Huawei_und_die_Sicherheit.pdf

- Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)*, *28*, 1–26. Verfügbar 13. Dezember 2023 unter https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

- Tekir, G. (2020). Huawei, 5G network and digital geopolitics. *International Journal of Politics and Security*, *2*(4 (Çin Özel Sayısı)), 113–135. Verfügbar 13. Dezember 2023 unter https://www.researchgate.net/publication/343949557_Huawei_5G_Network_and_Digital_Geopolitics

- Rühlig, T. (2020). Who controls Huawei. *Implications for Europe*. Verfügbar 13. Dezember 2023 unter https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf

- Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development and Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680

- Krolikowski, A., & Hall, T. H. (2023). Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany. *Japanese Journal of Political Science*, *24*(2), 171–189. https://doi.org/10.1017/S146810992200038X

## 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.

Aldrich, R. J., Müller, P. F., Ridd, D., & Schmidt-Eenboom, E. (2020). Operation rubicon: Sixty years of german-american success in signals intelligence [Accepted Manuscript (Open Access) – WRAP Repository]. *Intelligence and National Security*, *35*(5), 603–607. https://doi.org/10.1080/02684527.2020.1774849

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.

Alkhulaifi, A., & El-Alfy, E.-S. M. (2020). Exploring Lattice-based Post-Quantum Signature for JWT Authentication: Review and Case Study. *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 1–5. https://doi.org/10.1109/VTC2020-Spring48590.2020.9129505

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. 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. https://eprint.iacr.org/2021/1083

Alwen, J., Coretti, S., Jost, D., & Mularczyk, M. (2020a). Continuous Group Key Agreement with Active Security. https://eprint.iacr.org/2020/752

Alwen, J., Coretti, S., Jost, D., & Mularczyk, M. (2020b). 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

Barker, E., & Kelsey, J. (2006, Juni). *Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90*

(Special Publication Nr. SP 800-90) (Withdrawn March 14, 2007; provided for historical reference). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.SP.800-90

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.

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of statistical physics*, *22*(5), 563–591.

Benioff, P. A. (1982). Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: Application to Turing machines. *International Journal of Theoretical Physics*, *21*(3), 177–201.

Bennett, C. H., & Brassard, G. (1984). An update on quantum cryptography. *Workshop on the theory and application of cryptographic techniques*, 475–480.

Bernstein, E., & Vazirani, U. (1993). Quantum complexity theory. *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, 11–20.

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.

Brickell, E. F. (1989). Some ideal secret sharing schemes. *Workshop on the Theory and Application of of Cryptographic Techniques*, 468–475.

Brown, D. R. L. (2006). Conjectured Security of the ANSI-NIST Elliptic Curve RNG. https://eprint.iacr.org/2006/117

Brown, D. R. L., & Gjøsteen, K. (2007). A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator. https://eprint.iacr.org/2007/048

Brustolin, V., de Oliveira, D., & dos Reis Peron, A. E. (2023). Exploring the relationship between crypto ag and the cia in the use of rigged encryption machines for espionage in brazil. *Cambridge Review of International Affairs*, *36*(1), 54–87. https://doi.org/10.1080/09557571.2022.2123456

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

Buchmann, J., Coronado, C., Döring, M., Engelbert, D., Ludwig, C., Overbeck, R., Schmidt, A., Vollmer, U., & Weinmann, R.-P. (2004). Post-quantum signatures. *Cryptology ePrint Archive*. https://eprint.iacr.org/2004/297.pdf

Cai, J.-Y. (2024). Shor's algorithm does not factor large integers in the presence of noise. *Science China Information Sciences*, *67*(7). https://doi.org/10.1007/s11432-023-3961-3

Canetti, R., Chen, Y., Holmgren, J., Lombardi, A., Rothblum, G. N., Rothblum, R. D., & Wichs, D. (2019). Fiat-Shamir: from practice to theory. *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 1082–1090.

Checkoway, S., Fredrikson, M., Niederhagen, R., Everspaugh, A., Green, M., Lange, T., Ristenpart, T., Bernstein, D. J., Maskiewicz, J., & Shacham, H. (2014). On the Practical Exploitability of Dual EC in TLS Implementations. *Proceedings of the 23rd USENIX Security Symposium*, 319–335.

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

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *400*(1818), 97–117.

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.

Dobson, M. J. (2020). Operation rubicon: Germany as an intelligence 'great power'? *Intelligence and National Security*, *35*(5), 608–622. https://doi.org/10.1080/02684527.2019.1682621

Duits, I. (2019). *The post-quantum Signal protocol: Secure chat in a quantum world* [Magisterarb., University of Twente].

Dymydiuk, J. (2020). Rubicon and revelation: The curious robustness of the 'secret' cia–bnd operation with crypto ag [Accepted Manuscript (Open Access) – WRAP Repository]. *Intelligence and National Security*, *35*(5), 641–658. https://doi.org/10.1080/02684527.2020.1774853

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical review*, *47*(10), 777.

El Ioini, N., & Pahl, C. (2018). A review of distributed ledger technologies. *On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II*, 277–288.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 1–15.

Fefferman, B., Ghosh, S., Sinha, M., & Yuen, H. (2025). The Hardness of Learning Quantum Circuits and its Cryptographic Applications. https://arxiv.org/abs/2504.15343

Feynman, R. P. (1986). Quantum mechanical computers. *Found. Phys.*, *16*(6), 507–532.

Fiat, A., & Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. *Conference on the theory and application of cryptographic techniques*, 186–194.

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development and Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680

Frik, S. (2007). Boris hagelin and crypto ag: Pioneers of encryption. In R. Anderson & C. E. Landwehr (Hrsg.), *The history of information security* (S. 479–496). Elsevier. https://www.sciencedirect.com/science/article/pii/B9780080454880500273

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

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Goh, E.-J., Boneh, D., Pinkas, B., & Golle, P. (2003). The Design and Implementation of Protocol-Based Hidden Key Recovery. In J. C. Kwak & R. H. Deng (Hrsg.), *Information Security* (S. 165–179, Bd. 2851). Springer.

Gottesman, D. (2000). Theory of quantum secret sharing. *Physical Review A*, *61*(4), 042311.

Greenwald, G. (2014). *No place to hide: Edward snowden, the nsa, and the u.s. surveillance state*. Metropolitan Books. https://us.macmillan.com/books/9780805094560/noplace-to-hide

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219.

Halang, W. A., & Fitz, R. (2018). Informationstheoretisch sichere Datenverschlüsselung. In *Nicht hackbare Rechner und nicht brechbare Kryptographie* (S. 147–156). Springer.

Hashimoto, K., Katsumata, S., & Pascual-Perez, G. (2025). Exploring How to Authenticate Application Messages in MLS: More Efficient, Post-Quantum, and Anonymous Blocklistable. 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., & 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

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)*, *28*, 1–26. Verfügbar 13. Dezember 2023 unter https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Kaucher, A. (2018). *Blockchain: Funktionsweise und Applikationsmöglichkeiten*. Hochschule Bonn-Rhein-Sieg. https://www.h-brs.de/files/2018-01-14_seminar_alexander_kaucher_final.pdf

Khurana, D., & Tomer, K. (2024). Founding Quantum Cryptography on Quantum Advantage, or, Towards Cryptography from #P-Hardness. https://arxiv.org/abs/2409.15248

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

Kretschmer, W. (2021). Quantum Pseudorandomness and Classical Complexity. https://doi.org/10.4230/LIPICS.TQC.2021.2

Kretschmer, W., Qian, L., Sinha, M., & Tal, A. (2023). Quantum cryptography in algorithmica. *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, 1589–1602.

Krolikowski, A., & Hall, T. H. (2023). Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany. *Japanese Journal of Political Science*, *24*(2), 171–189. https://doi.org/10.1017/S146810992200038X

*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.

Lykousas, N., & Patsakis, C. (2023). Tales from the Git: Automating the detection of secrets on code and assessing developers' passwords choices.

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].

McCullagh, A., & Caelli, W. (2000). Non-repudiation in the digital environment.

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.

*Module-Lattice-Based Digital Signature Standard: FIPS 204*. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.204

*Module-Lattice-Based Key-Encapsulation Mechanism Standard: FIPS 203*. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.203

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

Moyes, H. (2020). The cryptographic trojan horse: Operation condor. *Chief Editor Caverlee Dahill, Assistant Editors Kate Brady*, 19–35.

Moyón, F., Angermeir, F., & Mendez, D. (2024). Industrial Challenges in Secure Continuous Development. *arXiv preprint arXiv:2401.06529*.

National Institute of Standards and Technology. (2002, Dezember). *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards Publication Nr. FIPS PUB 140-2) (Includes Change Notice 1, December 2002). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.FIPS.140-2

National Institute of Standards and Technology. (2025, September). *Recommendation for Random Bit Generator (RBG) Constructions, NIST Special Publication 800-90C* (Special Publication Nr. SP 800-90C) (Final version published 25 September 2025; includes SP 800-90A Rev.1 and SP 800-90B). National Institute of Standards und Technology. Gaithersburg. https://doi.org/10.6028/NIST.SP.800-90C

Pecka, N., ben Othmane, L., & Valani, A. (2022). Making Secure Software Insecure without Changing Its Code: The Possibilities and Impacts of Attacks on the DevOps Pipeline.

Preskill, J. (2012). Quantum computing and the entanglement frontier. https://arxiv.org/abs/1203.5813

*Recommendation for Stateful Hash-Based Signature Schemes: NIST Special Publication 800-208*. (2020). National Institute of Standards & Technology. Verfügbar 19. August 2025 unter https://doi.org/10.6028/NIST.SP.800-208

Roe, M. (2010). *Cryptography and evidence* (Techn. Ber.). University of Cambridge, Computer Laboratory.

Rühlig, T. (2020). Who controls Huawei. *Implications for Europe*. Verfügbar 13. Dezember 2023 unter https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf

Sassòli, M. (2021). Die Schweizerische Neutralität und der Fall Crypto AG [Open Access]. *Swiss Review of International and European Law*, *31*(4), 523–540. https://archive-ouverte.unige.ch/unige:166084

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (2016). *Blockchain: Grundlagen, Anwendungen und Potenziale*. Fraunhofer-Institut für Angewandte Informationstechnik. https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf

Schoenmakers, B., & Sidorenko, A. (2006). Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator. https://eprint.iacr.org/2006/190

Shamim, M. S. I., Bhuiyan, F. A., & Rahman, A. (2020). XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices. *CoRR*, *abs/2006.15275*. https://arxiv.org/abs/2006.15275

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology: Proceedings of CRYPTO 84 4*, 47–53.

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/s0097539795293172

Soler, D., Dafonte, C., Fernández-Veiga, M., Vilas, A. F., & Nóvoa, F. J. (2025). Experimental Analysis of Efficiency of the Messaging Layer Security for Multiple Delivery Services. *arXiv preprint arXiv:2502.18303*.

Stadler, M. (1996). Publicly verifiable secret sharing. *International Conference on the Theory and Applications of Cryptographic Techniques*, 190–199.

*Stateless Hash-Based Digital Signature Standard: FIPS 205*. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.205

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

Strehle, R. (1994). *Verschlüsselt: Der Fall Hans Bühler*. Werd Verlag.

Tekir, G. (2020). Huawei, 5G network and digital geopolitics. *International Journal of Politics and Security*, *2*(4 (Çin Özel Sayısı)), 113–135. Verfügbar 13. Dezember 2023 unter https://www.researchgate.net/publication/343949557_Huawei_5G_Network_and_Digital_Geopolitics

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

Voelsen, D. (2019). 5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik. *SWP-Aktuell*, (5/2019). Verfügbar 13. Dezember 2023 unter https://www.ssoar.info/ssoar/bitstream/handle/document/61663/ssoar-2019-voelsen-5G_Huawei_und_die_Sicherheit.pdf

Voggenreiter, M., Angermeir, F., Moyón, F., Schöpp, U., & Bonvin, P. (2024). Automated Security Findings Management: A Case Study in Industrial DevOps. *arXiv preprint arXiv:2401.06602*.

Von Neumann, J. (1932). Mathematische Grundlagen der Quantenmechanik. https://gdz.sub.uni-goettingen.de/id/PPN379400774

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

Wallez, T., Protzenko, J., Beurdouche, B., & Bhargavan, K. (2023). {TreeSync}: authenticated group management for messaging layer security. *32nd USENIX Security Symposium (USENIX Security 23)*, 1217–1233.

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

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

Weierud, F., & Zabell, S. (2020). German mathematicians and cryptology in WWII. *Cryptologia*, *44*(2), 97–171.

Wertheimer, M. (2015). Encryption and the NSA Role in International Standards. *Notices of the American Mathematical Society*, *62*(2), 165–167. https://doi.org/10.1090/noti1213

Young, A., & Yung, M. (1997a). Kleptography: Using Cryptography Against Cryptography. In W. Fumy (Hrsg.), *Advances in Cryptology — EUROCRYPT '97* (S. 62–74). Springer Berlin Heidelberg.

Young, A., & Yung, M. (1997b). The prevalence of kleptographic attacks on discrete-log based cryptosystems. In B. S. Kaliski (Hrsg.), *Advances in Cryptology — CRYPTO '97* (S. 264–276). Springer Berlin Heidelberg.

Young, A. L., & Yung, M. (2007). Space-Efficient Kleptography Without Random Oracles. *Information Hiding*, *4567*, 112–129.

Yu, H., McCuller, L., Tse, M., Kijbunchoo, N., Barsotti, L., & Mavalvala, N. (2020). Quantum correlations between light and the kilogram-mass mirrors of LIGO. *Nature*, *583*(7814), 43–47.