Akleylek, Sedat, and Meryem Soysaldı. “A New Lattice-Based Authentication Scheme for IoT.” *Journal of Information Security and Applications* 64 (February 1, 2022): 103053. https://doi.org/10.1016/j.jisa.2021.103053.

Alani, Mohammed M. “Applications of Machine Learning in Cryptography: A Survey.” In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 23–27. ICCSP ’19. New York, NY, USA: Association for Computing Machinery, 2019. https://doi.org/10.1145/3309074.3309092.

Banegas, Gustavo, Daniel J. Bernstein, Iggy van Hoof, and Tanja Lange. “Concrete Quantum Cryptanalysis of Binary Elliptic Curves,” 2020. Cryptology ePrint Archive. https://eprint.iacr.org/2020/1296.

Banegas, Gustavo, Koen Zandberg, Adrian Herrmann, Emmanuel Baccelli, and Benjamin Smith. “Quantum-Resistant Security for Software Updates on Low-Power Networked Embedded Devices.” arXiv, June 11, 2021. https://doi.org/10.48550/arXiv.2106.05577.

Bennett, Charles H., Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. “Strengths and Weaknesses of Quantum Computing.” *SIAM Journal on Computing* 26, no. 5 (October 1997): 1510–23. https://doi.org/10.1137/S0097539796300933.

Blanco-Chacón, Iván. *RING LEARNING WITH ERRORS: A CROSSROADS BETWEEN POSTQUANTUM CRYPTOGRAPHY, MACHINE LEARNING AND NUMBER THEORY*, 2019.

Cesare, Chris. “Online Security Braces for Quantum Revolution.” *Nature* 525, no. 7568 (September 1, 2015): 167–68. https://doi.org/10.1038/525167a.

Dhillon, Parwinder Kaur, and Sheetal Kalra. “Elliptic Curve Cryptography for Real Time Embedded Systems in IoT Networks.” In *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)*, 1–6, 2016. https://doi.org/10.1109/WECON.2016.7993462.

Ebrahimi, Shahriar, Siavash Bayat-Sarmadi, and Hatameh Mosanaei-Boorani. “Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT.” *IEEE Internet of Things Journal* 6, no. 3 (June 2019): 5500–5507. https://doi.org/10.1109/JIOT.2019.2903082.

Gisin, Nicolas, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. “Quantum Cryptography.” *Reviews of Modern Physics* 74, no. 1 (March 8, 2002): 145–95. https://doi.org/10.1103/RevModPhys.74.145.

Guillen, Oscar M., Thomas Pöppelmann, Jose M. Bermudo Mera, Elena Fuentes Bongenaar, Georg Sigl, and Johanna Sepulveda. “Towards Post-Quantum Security for IoT Endpoints with NTRU.” In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, 698–703, 2017. https://doi.org/10.23919/DATE.2017.7927079.

Hekkala, Julius, Mari Muurman, Kimmo Halunen, and Visa Vallivaara. “Implementing Post-Quantum Cryptography for Developers.” *SN Computer Science* 4, no. 4 (April 29, 2023): 365. https://doi.org/10.1007/s42979-023-01724-1.

Kabanov, I. S., R. R. Yunusov, Y. V. Kurochkin, and A. K. Fedorov. “Practical Cryptographic Strategies in the Post-Quantum Era.” *AIP Conference Proceedings* 1936, no. 1 (February 28, 2018): 020021. https://doi.org/10.1063/1.5025459.

Kaur, Veerpal, Gagandeep Kaur, gamini dhiman, Ruchika Bindal, and Mukul Kumar. “Adaptability of Machine Learning in Cryptography.” *Solid State Technology* 63 (September 29, 2021): 2874–80.

Khalid, Ayesha, Sarah McCarthy, Maire O’Neill, and Weiqiang Liu. “Lattice-Based Cryptography for IoT in A Quantum World: Are We Ready?” In *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 194–99, 2019. https://doi.org/10.1109/IWASI.2019.8791343.

Lerman, Liran, Gianluca Bontempi, and Olivier Markowitch. “Power Analysis Attack: An Approach Based on Machine Learning.” *International Journal of Applied Cryptography* 3, no. 2 (January 2014): 97–115. https://doi.org/10.1504/IJACT.2014.062722.

Liu, Zhe, and Hwajeong Seo. “IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms.” *IEEE Transactions on Information Forensics and Security* 14, no. 3 (March 2019): 720–29. https://doi.org/10.1109/TIFS.2018.2856123.

Malina, Lukas, Lucie Popelova, Petr Dzurenda, Jan Hajny, and Zdenek Martinasek. “On Feasibility of Post-Quantum Cryptography on Small Devices.” *IFAC-PapersOnLine*, 15th IFAC Conference on Programmable Devices and Embedded Systems PDeS 2018, 51, no. 6 (January 1, 2018): 462–67. https://doi.org/10.1016/j.ifacol.2018.07.104.

P C, Sajimon, Kurunandan Jain, and Prabhakar Krishnan. “Analysis of Post-Quantum Cryptography for Internet of Things.” In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 387–94, 2022. https://doi.org/10.1109/ICICCS53718.2022.9787987.

Pirandola, S., U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, et al. “Advances in Quantum Cryptography.” *Advances in Optics and Photonics* 12, no. 4 (December 31, 2020): 1012–1236. https://doi.org/10.1364/AOP.361502.

Portmann, Christopher, and Renato Renner. “Security in Quantum Cryptography.” *Reviews of Modern Physics* 94, no. 2 (June 29, 2022): 025008. https://doi.org/10.1103/RevModPhys.94.025008.

Ristov, Riste, and Saso Koceski. “Quantum Resilient Public Key Cryptography in Internet of Things.” In *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, 1–4, 2023. https://doi.org/10.1109/MECO58584.2023.10154994.

Rivest, Ronald L. “Cryptography and Machine Learning.” In *Advances in Cryptology — ASIACRYPT ’91*, edited by Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, 427–39. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1993. https://doi.org/10.1007/3-540-57332-1_36.

Roetteler, Martin, Michael Naehrig, Krysta M. Svore, and Kristin Lauter. “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms.” In *Advances in Cryptology – ASIACRYPT 2017*, edited by Tsuyoshi Takagi and Thomas Peyrin, 241–70. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-70697-9_9.

Routray, Sudhir K., Mahesh K. Jha, Laxmi Sharma, Rahul Nyamangoudar, Abhishek Javali, and Sutapa Sarkar. “Quantum Cryptography for IoT: APerspective.” In *2017 International Conference on IoT and Application (ICIOT)*, 1–4, 2017. https://doi.org/10.1109/ICIOTA.2017.8073638.

Schöffel, Maximilian, Frederik Lauer, Carl C. Rheinländer, and Norbert Wehn. “On the Energy Costs of Post-Quantum KEMs in TLS-Based Low-Power Secure IoT.” In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, 158–68. IoTDI ’21. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3450268.3453528.

Seyhan, Kübra, Tu N. Nguyen, Sedat Akleylek, and Korhan Cengiz. “Lattice-Based Cryptosystems for the Security of Resource-Constrained IoT Devices in Post-Quantum World: A Survey.” *Cluster Computing* 25, no. 3 (June 1, 2022): 1729–48. https://doi.org/10.1007/s10586-021-03380-7.

Shor, Peter W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” *SIAM Journal on Computing* 26, no. 5 (October 1997): 1484–1509. https://doi.org/10.1137/S0097539795293172.

Singh, Saurabh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. “Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions.” *Journal of Ambient Intelligence and Humanized Computing*, May 24, 2017. https://doi.org/10.1007/s12652-017-0494-4.

Sooksatra, Korn, and Pablo Rivas. “A Review of Machine Learning and Cryptography Applications.” In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 591–97, 2020. https://doi.org/10.1109/CSCI51800.2020.00105.

Taran, Olga, Shideh Rezaeifar, and Slava Voloshynovskiy. “Bridging Machine Learning and Cryptography in Defence against Adversarial Attacks.” arXiv, September 5, 2018. https://doi.org/10.48550/arXiv.1809.01715.

Tiwari, Harsh Durga, and Jae Hyung Kim. “Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices.” *ETRI Journal* 40, no. 3 (2018): 396–409. https://doi.org/10.4218/etrij.2017-0220.

Usman, Muhammad. “Lightweight Encryption for the Low Powered IoT Devices.” arXiv, December 2, 2020. https://doi.org/10.48550/arXiv.2012.00193.

Westerbaan, Bas, and Douglas Stebila. “X25519Kyber768Draft00 Hybrid Post-Quantum Key Agreement.” Internet Draft. Internet Engineering Task Force, March 31, 2023. https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00-02.

Yi, Haibo. “Machine Learning Method with Applications in Hardware Security of Post-Quantum Cryptography.” *Journal of Grid Computing* 21, no. 2 (March 20, 2023): 19. https://doi.org/10.1007/s10723-023-09643-4.

Younan, Mina, Mohamed Elhoseny, Abdelmgeid A. Ali, and Essam H. Houssein. “Quantum Chain of Things (QCoT): A New Paradigm for Integrating Quantum Computing, Blockchain, and Internet of Things.” In *2021 17th International Computer Engineering Conference (ICENCO)*, 101–6, 2021. https://doi.org/10.1109/ICENCO49852.2021.9698947.