BIBLIOGRAPHY

[1] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the internet of things," *Electronics*, vol. 13, no. 16, 2024.

[2] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," 2016-04-28 2016.

[3] H. Yu and R. Ren, "Certificateless elliptic curve aggregate signcryption scheme," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2347–2354, 2022.

[4] T.-H. Nguyen, B. Kieu-Do-Nguyen, C.-K. Pham, and T.-T. Hoang, "High-speed ntt accelerator for crystal-kyber and crystal-dilithium," *IEEE Access*, vol. 12, pp. 34 918–34 930, 2024.

[5] S. D. Matteo, I. Sarno, and S. Saponara, "Cryphtor: A memory-unified ntt-based hardware accelerator for post-quantum crystals algorithms," *IEEE Access*, vol. 12, pp. 25 501–25 511, 2024.

[6] D. C. Lawo, R. Frantz, A. C. Aguilera, X. A. I. Clemente, M. P. Podleś, J. L. Imaña, I. T. Monroy, and J. J. V. Olmos, "Falcon/kyber and dilithium/kyber network stack on nvidia's data processing unit platform," *IEEE Access*, vol. 12, pp. 38 048–38 056, 2024.

[7] M. A. Ehsan, W. Alayed, A. U. Rehman, W. u. Hassan, and A. Zeeshan, "Post-quantum kems for iot: A study of kyber and ntru," *Symmetry*, vol. 17, no. 6, 2025. [Online]. Available: https://www.mdpi.com/2073-8994/17/6/881

[8] S. Sattar, M. Shafiq, and A. Abbas, "Benchmarking post-quantum digital signature algorithms on resource-constrained devices," *Symmetry*, vol. 13, no. 5, p. 881, 2021.

[9] T. X. Pham, P. Duong-Ngoc, and H. Lee, "An efficient unified polynomial arithmetic unit for crystals-dilithium," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 12, pp. 4854–4864, Dec 2023.

[10] J. I. E. Pablos, M. E. Marriaga, and L. P. d. Pozo, "Design and implementation of a post-quantum group authenticated key exchange protocol with the liboqs library: A comparative performance analysis from classic mceliece, kyber, ntru, and saber," *IEEE Access*, vol. 10, pp. 120 951–120 983, 2022.

[11] N. Gupta, A. Jati, A. K. Chauhan, and A. Chattopadhyay, "Pqc acceleration using gpus: Frodokem, newhope, and kyber," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 3, pp. 575–586, March 2021.

[12] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, July 2020.

[13] Y. Quan, "Improving bitcoin's post-quantum transaction efficiency with a novel lattice-based aggregate signature scheme based on crystals-dilithium and a stark protocol," *IEEE Access*, vol. 10, pp. 132 472–132 482, 2022.

[14] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevičius, A.-A. O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36 038–36 077, 2021.

[15] L. D. E. K. T. L. V. L. J. M. S. P. S. G. S. D. S. Roberto Avanzi, Joppe Bos, "Crystals-kyber: Algorithm specification and supporting documentation," CRYSTALS, Tech. Rep., 2021.

[16] A. Aikata, A. C. Mert, M. Imran, S. Pagliarini, and S. S. Roy, "Kali: A crystal for post-quantum security using kyber and dilithium," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 2, pp. 747–758, Feb 2023.

[17] E. K. T. L. V. L. P. S. G. S. Shi Bai, Léo Ducas and D. Stehlé, "Crystals-dilithium: Algorithm specification and supporting documentation," CRYSTALS, Tech. Rep., 2021.

[18] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72 514–72 550, 2018.

[19] U. . S. K. Pejman Panahi, Cüneyt Bayılmış, "Performance evaluation of lightweight encryption algorithms for iot-based applications," *Arab J Sci Eng*, 2021.

[20] V.-T. Nguyen, T. D. Nguyen, and M.-T. Le, "Performance evaluation of crystals-kyber on raspberry pi for post-quantum iot security," *SN Computer Science*, vol. 6, no. 1, pp. 1–12, 2025.

[21] J. Yan, L. Wang, M. Li, H. Ahmad, J. Yue, and W. Yao, "Attribute-based signcryption from lattices in the standard model," *IEEE Access*, vol. 7, pp. 56 039–56 050, 2019.

[22] X. Yang, H. Cao, W. Li, and H. Xuan, "Improved lattice-based signcryption in the standard model," *IEEE Access*, vol. 7, pp. 155 552–155 562, 2019.

[23] Y. Shi, J. Han, X. Wang, J. Gao, and H. Fan, "An obfuscatable aggregatable signcryption scheme for unattended devices in iot systems," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 1067–1081, Aug 2017.

[24] J. Yu, S. Liu, S. Wang, Y. Xiao, and B. Yan, "Lh-absc: A lightweight hybrid attribute-based signcryption scheme for cloud-fog-assisted iot," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7949–7966, Sep. 2020.

[25] Y. Ming, X. Yu, and X. Shen, "Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare internet of things," *IEEE Access*, vol. 8, pp. 153 561–153 576, 2020.

[26] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari, S. S. Ullah, M. A. Khan, and S. J. Khattak, "A lightweight and formally secure certificate based signcryption with proxy re-encryption (cbsre) for internet of things enabled smart grid," *IEEE Access*, vol. 8, pp. 93 230–93 248, 2020.

[27] L. Pang, M. Wei, and H. Li, "Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ecc," *IEEE Access*, vol. 7, pp. 24 511–24 526, 2019.

[28] I. Ullah, A. Alkhalifah, S. U. Rehman, N. Kumar, and M. A. Khan, "An anonymous certificateless signcryption scheme for internet of health things," *IEEE Access*, vol. 9, pp. 101 207–101 216, 2021.

[29] S. Ricci, P. Dzurenda, J. Hajny, and L. Malina, "Privacy-enhancing group signcryption scheme," *IEEE Access*, vol. 9, pp. 136 529–136 551, 2021.

[30] I. Ullah, A. Alomari, A. M. Abdullah, N. Kumar, A. Alsirhani, F. Noor, S. Hussain, and M. A. Khan, "Certificate-based signcryption scheme for securing wireless communication in industrial internet of things," *IEEE Access*, vol. 10, pp. 105 182–105 194, 2022.