[5] Utsav Banerjee, Tenzin S. Ukyab, and Anantha P. Chandrakasan. 2019. Sapphire: A configurable crypto-processor for

post-quantum lattice-based protocols. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019, 4 (2019), 17–61.

[9] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. 2011. XMSS - A practical forward secure signature scheme

based on minimal security assumptions. In International Workshop on Post-quantum Cryptography. Springer, 117–129.

[11] Fabio Campos, Tim Kohlstadt, Steffen Reith, and Marc Stöttinger. 2020. LMS vs XMSS: Comparison of stateful hash-

based signature schemes on ARM Cortex-M4. IACR Cryptol. ePrint Arch. 2020 (2020), 470.

[12] Yuan Cao, Yanze Wu, Wen Wang, Xu Lu, Shuai Chen, Jing Ye, and Chip-Hong Chang. 2022. An efficient full hardware

implementation of extended Merkle signature scheme. IEEE Transactions on Circuits and Systems I: Regular Papers 69,

2 (2022), 682–693. https://doi.org/10.1109/TCSI.2021.3115786

[16] Jintai Ding and Dieter Schmidt. 2005. Rainbow, a new multivariable polynomial signature scheme. In International

Conference on Applied Cryptography and Network Security. Springer, 164–175.

[19] E. Eaton. 2017. Leighton-Micali hash-based signatures in the quantum random-oracle model. In Selected Areas in

Cryptography - SAC’17 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers

(2017), C. Adams and J. Camenisch, (Eds.). Vol. 10719 of Lecture Notes in Computer Science, Springer, 263–280.

[21] Ahmed Ferozpuri and Kris Gaj. 2018. High-speed FPGA implementation of the NIST round 1 rainbow signature

scheme. In 2018 International Conference on ReConFigurable Computing and FPGAs (ReConFig’18). IEEE, 1–8.

[25] Andreas Hülsing, Denis Butin, Stefan Gazdag, Joost Rijneveld, and Aziz Mohaisen. 2018. XMSS: eXtended Merkle

signature scheme. Internet Research Task Force (IRTF), RFC 8391 (2018), 1–74.

[28] Panos Kampanakis and Scott Fluhrer. 2017. LMS vs XMSS: Comparion of two hash-based signature standards. IACR

Cryptology ePrint Archive: Report 2017/349 (2017).

[29] Matthias J. Kannwischer, Aymeric Genêt, Denis Butin, Juliane Krämer, and Johannes Buchmann. 2018. Differential

power analysis of XMSS and SPHINCS. In International Workshop on Constructive Side-channel Analysis and Secure

Design. Springer, 168–188.

[33] Georg Land, Pascal Sasdrich, and Tim Güneysu. 2021. A hard crystal - Implementing dilithium on reconfigurable

hardware. In Smart Card Research and Advanced Applications - 20th International Conference (CARDIS’21), Revised Se-

lected Papers (Lecture Notes in Computer Science), Vincent Grosso and Thomas Pöppelmann (Eds.), Vol. 13173. Springer,

210–230. https://doi.org/10.1007/978-3-030-97348-3\_12

[34] David McGrew, Michael Curcio, and Scott Fluhrer. 2019. Leighton-Micali hash-based signatures. Internet Research Task

Force (IRTF), RFC 8544 (2019).

[36] Prashanth Mohan, Wen Wang, Bernhard Jungk, Ruben Niederhagen, Jakub Szefer, and Ken Mai. 2020. ASIC accelerator

in 28 nm for the post-quantum digital signature scheme XMSS. In 2020 IEEE 38th International Conference on Computer

Design (ICCD’20). IEEE, 656–662.

[37] Dustin Moody. 2019. Round 2 of NIST PQC competition. PQCrypto (2019).

[38] D. T. Nguyen, V. B. Dang, and K. Gaj. 2019. A high-level synthesis approach to the software/hardware codesign of NTT-

based post-quantum cryptography algorithms. In 2019 International Conference on Field-programmable Technology

(ICFPT’19). 371–374. https://doi.org/10.1109/ICFPT47387.2019.00070

[39] Lucas Pandolfo Perin, Gustavo Zambonin, Douglas Marcelino Beppler Martins, Ricardo Felipe Custódio, and Jean Ever-

son Martina. 2018. Tuning the Winternitz hash-based digital signature scheme. In 2018 IEEE Symposium on Computers

and Communications (ISCC’18). IEEE, 537–542. https://doi.org/10.1109/ISCC.2018.8538642

[42] Yifeng Song, Xiao Hu, Wenhao Wang, Jing Tian, and Zhongfeng Wang. 2021. High-speed and scalable FPGA imple-

mentation of the key generation for the Leighton-Micali signature protocol. In 2021 IEEE International Symposium on

Circuits and Systems (ISCAS’21). 1–5. https://doi.org/10.1109/ISCAS51556.2021.9401177

[44] Jan Philipp Thoma and Tim Güneysu. 2021. A configurable hardware implementation of XMSS. Cryptology ePrint

Archive (2021).

[46] Wen Wang, Bernhard Jungk, Julian Wälde, Shuwen Deng, Naina Gupta, Jakub Szefer, and Ruben Niederhagen. 2019.

XMSS and embedded systems. In International Conference on Selected Areas in Cryptography. Springer, 523–550.

[47] Kacper Zujko. 2020. Improving differential power analysis of XMSS. In The Book of Articles National Scientific Confer-

ence “Science and Young Researchers” IV edition. 112.