Neuromorphic and In-Memory Computing Based on Memristive Circuits for Predictive Maintenance and Supply-Chain Management and Security

Nikolaos Athanasios Anagnostopoulos*, Nico Mexis*, Elif Bilge Kavun*, Stefan Katzenbeisser*, Tolga Arul*†
* Faculty of Computer Science and Mathematics, University of Passau, 94032 Passau, Germany
Emails: {anagno02, mexis01, kavun01, katzen07, arul01}@ads.uni-passau.de
ORCIDs: N.A.A.: 0000-0003-0243-8594; N.M.: 0000-0003-0181-7648;
E.B.K.: 0000-0003-3193-8440; S.K.: 0009-0005-3608-874X; T.A.: 0000-0002-2078-3976
† Department of Computer Science, Technical University of Darmstadt, 64289 Darmstadt, Germany
Emails: arul@seceng.informatik.tu-darmstadt.de

***Abstract*—In this work, we very briefly explore the use of neuromorphic and in-memory computing modules based on a crossbar array of memristive cells in the framework of predictive maintenance and supply chain management and security.**

***Index Terms*—memristors, in-memory computing, neuromorphic computing, crossbar array, predictive maintenance, supply-chain management, supply-chain security, hardware acceleration**

I. Brief Background Information

Recently, memristors and Resistive Random Access Memory (ReRAM) modules have been finding application in the scientific fields of neuromorphic and in-memory computing due to the intrinsic properties of memristive circuits. In particular, memristors allow for the realisation of neuromorphic and in-memory computing architectures in a cost-effective, resource-efficient, and energy-saving manner. It is also worth noting here that only neuromorphic and in-memory computing architectures allow certain types of Machine-Learning (ML) methods, such as neural networks, to realise their full potential in terms of computational power.

In general, ML methods help to uncover hidden patterns in large amounts of data. Based on these patterns, well-founded insights can be gained and, for example, trends can be identified and anomalies be detected. For this reason, machine-learning methods are increasingly used across almost all classes of devices, from Internet-of-Things (IoT) and household appliances to components in industrial plants and secure infrastructures, to perform, among other things, quality checks, defect tracking, and forecasting of consumption and demand.

ML methods have already been utilised for predicting the wear of materials in the context of predictive maintenance [1]–[3], for supply chain management [4]–[7], and for the detection of hardware Trojans and other supply-chain security threats [8], [9].

Moreover, memristive devices have also been utilised for the realisation of hardware accelerators [10], [11], based on their inherent capability for in-memory computing applications. Hardware acceleration can truly facilitate the operation of machine-learning schemes [12]–[14].

These developments clearly indicate the potential of memristor-based neuromorphic and in-memory computing circuits to be utilised in the context of machine learning and hardware acceleration for predictive maintenance and supply-chain management and security.

II. Short Overview of the Proposed Solution

In this work, we propose the employment of a crossbar array of memristors for the implementation of ML methods using neuromorphic and in-memory computing in order to realise predictive maintenance and supply-chain management and security applications. In general, in contrast to the use of individual memristors that have been bonded together, the utilisation of an interconnected crossbar array allows us to keep the relevant chip area, wiring, and control logic requirements low, while memristors are also compatible with standard CMOS technology [15], thus allowing such a memristor array to be easily integrated with existing hardware.

In general, the vast majority of systems already have embedded components that are used for control and configuration. However, adding machine-learning functionality to the aforementioned embedded components poses a great challenge to manufacturers, due to the resource-constrained nature of embedded components. Thus, we propose to incorporate machine-learning functionality into such resource-constrained

This work has been partially funded by the German Research Foundation – Deutsche ForschungsGemeinschaft (DFG), as part of the Projects "PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories" (project number 440182124) and "NANOSEC: Tamper-Evident PUFs based on Nanostructures for Secure and Robust Hardware Security Primitives" (project number 439892735) of the Priority Program "Nano Security: From Nano-Electronics to Secure Systems" (SPP 2253), and by the Interreg VI-A Programme Germany/Bavaria–Austria 2021–2027 – Programm INTERREG VI-A Bayern–Österreich 2021–2027, as part of the Project "CySeReS-KMU: Cyber Security and Resilience in Supply Chains with focus on SMEs" (project number BA0100016), co-funded by the European Union. We also acknowledge the role of the DFG-funded Priority Program "Memristive Devices Toward Smart Technical Systems" (SPP 2262), which provided the inspiration for this work.

devices by taking advantage of the intrinsic properties of memristive devices to implement this functionality in a lightweight and energy-efficient manner.

In the context of predictive maintenance, wearing parts are to be replaced not at regular intervals but according to their actual wear. Additionally, it should be ensured that a premature failure of the system due to defective wear parts is avoided. For this purpose, sensors that can determine the current wear of the wearing parts are utilised, as well as machine-learning models trained using the relevant sensor data to make precise predictions for the time at which defects are to occur in the corresponding wear parts.

In this case, the weights and structure of such a machine-learning model can be easily implemented using a memristive crossbar structure. Sensor values will form the relevant inputs, while the output will indicate the predicted time intervals at which the different wearing parts are to become defective. Thus, the relevant crossbar structure can be connected to the rest of the embedded system using only a small number of wires and/or pins, and only the related software will need to be adapted to allow for the system evaluation functionality associated with the predictive-maintenance application.

In a similar manner, such a crossbar array structure of memristor cells can also be utilised for supply-chain management and security applications.

It is important to observe here that the same structure can also act as a ReRAM module allowing for computer memory functionality, and as a hardware accelerator component, allowing for a triple functionality that can be utilised in the framework of diverse applications and use cases.

III. Discussion and Conclusion

Here, we have proposed the utilisation of a crossbar array of memristors in order to allow for intrinsic ML functionality to facilitate predictive maintenance and supply-chain management and security applications, especially in the framework of resource-constrained components. In general, the use of memristors in the framework of an embedded sensor component can be utilised to inherently ensure the integrity of such a component or even the overall system itself.

To this end, we observe that memristors are fully compatible with the existing CMOS technology, while the relevant ReRAM components constitute fast computer memories, and usually require a limited number of manufacturing steps in order to be produced. Thus, we note that the use of memristors allows for the realisation of advanced applications, such as ML, in a lightweight, cost-effective, resource-efficient, and energy-saving manner, especially since the relevant components not only can realise ML-based models, but can also be utilised as memories, and potentially even as hardware accelerators.

Finally, it is worth noting that memristive circuits also allow for the creation of hardware security primitives [16], [17], as well as for neural and evolutionary computing, which could be utilised for even more sophisticated Artificial Intelligence (AI) applications.

References

[1] T. P. Carvalho, F. A. A. M. N. Soares, R. Vita, R. da P. Francisco, J. P. Basto, and S. G. S. Alcalá, "A systematic literature review of machine learning methods applied to predictive maintenance," *Computers & Industrial Engineering*, vol. 137, p. 106024, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360835219304838

[2] M. Paolanti, L. Romeo, A. Felicetti, A. Mancini, E. Frontoni, and J. Loncarski, "Machine learning approach for predictive maintenance in industry 4.0," in *2018 14th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*. IEEE, 2018, pp. 1–6.

[3] G. A. Susto, A. Schirru, S. Pampuri, S. McLoone, and A. Beghi, "Machine learning for predictive maintenance: A multiple classifier approach," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 812–820, 2015.

[4] R. Sharma, S. S. Kamble, A. Gunasekaran, V. Kumar, and A. Kumar, "A systematic literature review on machine learning applications for sustainable agriculture supply chain performance," *Computers & Operations Research*, vol. 119, p. 104926, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0305054820300435

[5] H. Wenzel, D. Smit, and S. Sardesai, "A literature review on machine learning in supply chain management," in *Artificial Intelligence and Digital Transformation in Supply Chain Management: Innovative Approaches for Supply Chains. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 27*, W. Kersten, T. Blecker, and C. M. Ringle, Eds. Berlin: epubli GmbH, 2019, pp. 413–441, urn:nbn:de:gbv:830-882.054345; 10419/209196; https://econpapers.repec.org/RePEc:zbw:hiclpr:27. [Online]. Available: http://hdl.handle.net/10419/209380

[6] Z. Dong, W. Liang, Y. Liang, W. Gao, and Y. Lu, "Blockchained supply chain management based on iot tracking and machine learning," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 127, Dec 2022. [Online]. Available: https://doi.org/10.1186/s13638-022-02209-0

[7] M. Schroeder and S. Lodemann, "A systematic investigation of the integration of machine learning into supply chain risk management," *Logistics*, vol. 5, no. 3, 2021. [Online]. Available: https://www.mdpi.com/2305-6290/5/3/62

[8] K. I. Gubbi, B. Saber Latibari, A. Srikanth, T. Sheaves, S. A. Beheshti-Shirazi, S. M. PD, S. Rafatirad, A. Sasan, H. Homayoun, and S. Salehi, "Hardware trojan detection using machine learning: A tutorial," *ACM Trans. Embed. Comput. Syst.*, vol. 22, no. 3, apr 2023. [Online]. Available: https://doi.org/10.1145/3579823

[9] Z. Huang, Q. Wang, Y. Chen, and X. Jiang, "A survey on machine learning against hardware trojan attacks: Recent advances and challenges," *IEEE Access*, vol. 8, pp. 10 796–10 826, 2020.

[10] Y. Halawani, B. Mohammad, M. Al-Qutayri, and S. F. Al-Sarawi, "Memristor-based hardware accelerator for image compression," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 12, pp. 2749–2758, 2018.

[11] I.-A. Fyrigos, V. Ntinas, G. C. Sirakoulis, P. Dimitrakis, and I. Karafyllidis, "Memristor hardware accelerator of quantum computations," in *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*. IEEE, 2019, pp. 799–802.

[12] R. Zhao, W. Luk, X. Niu, H. Shi, and H. Wang, "Hardware acceleration for machine learning," in *2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2017, pp. 645–650.

[13] Y. Chen, T. Chen, Z. Xu, N. Sun, and O. Temam, "Diannao family: Energy-efficient hardware accelerators for machine learning," *Commun. ACM*, vol. 59, no. 11, p. 105–112, oct 2016. [Online]. Available: https://doi.org/10.1145/2996864

[14] L. Du and Y. Du, "Hardware accelerator design for machine learning," in *Machine Learning*, H. Farhadi, Ed. Rijeka: IntechOpen, 2017, ch. 1. [Online]. Available: https://doi.org/10.5772/intechopen.72845

[15] S. Lv, J. Liu, and Z. Geng, "Application of memristors in hardware security: A current state-of-the-art technology," *Advanced Intelligent Systems*, vol. 3, no. 1, p. 2000127, 2021. [Online]. Available: https://doi.org/10.1002/aisy.202000127

[16] F. Frank, T. Arul, N. A. Anagnostopoulos, and S. Katzenbeisser, "Using memristor arrays as physical unclonable functions," in *Computer Security – ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III*. Berlin, Heidelberg: Springer-Verlag, 2022, p. 250–271. [Online]. Available: https://doi.org/10.1007/978-3-031-17143-7_13

[17] C. Aitchison, B. Halak, A. Serb, and T. Prodromakis, "A memristor fingerprinting and characterisation methodology for hardware security," *Scientific Reports*, vol. 13, no. 1, p. 9392, Jun 2023. [Online]. Available: https://doi.org/10.1038/s41598-023-33051-z