Literature Review

September 2025

Ian Barnaby

ACM Reference Format:

Ian Barnaby. 2025. Literature Review September 2025. In . ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

This project aims to research and design an asymmetric encryption method targeting a processor and AI accelerator pair. In the theorized application, the accelerator is taken as a trusted base holding the IP of a neural network. It is therefore desired to have an encryption scheme between CPU and accelerator to prevent malicious actors from performing snooping attacks on the bus connecting the accelerator and processor. This project specifically considers accelerators utilizing non-volatile memory to perform compute in-memory operations. These types of devices have been demonstrated to allow for information to be encoded in physical device properties, without being stored in the current state of the cell. In the proposed encryption mechanism, values encoded in the memory cells are used to generate a private/public key pair, used to encrypt processor/accelerator communication.

2 Relevant Background

This literature review focuses on literature regarding the relevant NVM devices/device properties, asymmetric encryption, PUF-based key generation, fault injection defense

3 Search Terms

In searching for papers, databases such as EngineeringVillage and IEEEXplore were used. Search terms included terms such as, but not limited to:

-

4 Paper Reviews

4.1 Hiding Information for Secure and Covert Data Storage in Commercial ReRAM Chips

This paper demonstrates a technique for covert data storage in ReRAM devices [1]. The researchers state that the set/reset time of a ReRAM cell changes with each write cycle. This occurs due to oxygen vacancies in the oxide layer used to construct the conductive filament and limits the total number of write cycles the cell can handle before it no longer functions. The researchers have observed that, once the set/reset characteristics of a cell have been altered, they can reliable determine cells with more or less "wear". By setting a point at which set/reset times can be read as binary "1" or "0", cells can intentially be worn down to encode values in the set/reset time. The researchers demonstrate that fresh cells can be worn down in desired bit patterns, and the data can be be reliably recovered until a threshold is reached. After a certain number of write cycles, the data encoded in the set/reset time becomes too noisy. As such, this paper provides the basis for this work of establishing a method of encoding data within ReRAM cells separate from the memory values, that changes based on how many writes have been issued to the device.

4.2 Overview of NVM Devices

The above paper has proven the potential for data encoding in ReRAM, but other NVM technologies are worthy of review. As NVM and CIM are unsolved fields, commercial applications may move away from ReRAM. There are three other types of NVM technologies deserving particular attention: ECM, phase-change, and magnetic memory.

4.2.1 ECM. ECM (electrochemical metallization) memory operates on a similar principle to ReRAM: a low resistance state is created by forming a conductive filament between two electrodes, and a high resistance state is created by destruction of the filament. In ReRAM (also called valence change memory), this conductive filament is formed by oxygen vacancies in an exotic metal oxide layer. In ECM, this conductive filament is formed by the migration of metal ions from an active electrode towards an inert electrode through an oxide layer. An existing work demonstrates the set/reset characteristics of ECM in regards to endurance [2], supporting that set/reset characteristics change over many write cycles. While further study would be required to determine if the same technique can be reliably applied to ECM, the required behavior is present.

4.2.2 PCM. PCM (phase change memory) differs in that it does not utilize a conductive filament. In PCM, a layer of thin chalcogenide is deposited between two conducting contacts. By applying a moderate current pulse, the chalcogenide layer is heated, forming a conducting crystalline layer, creating a low resistance state. By applying a short, high current pulse, the chalcogenide layer is melted, rapidly cooling into a non-conducting amorphous layer, creating a high resistance state. An existing work demonstrates, similarly to ECM, that the set/reset characteristics change over time, studied in terms of device endurance [3]. Again, further study would be required to determine if the same technique can be applied, but the required behavior is present.

4.2.3 STT-MRAM. STT-MRAM (spin transfer torque magnetic RAM) operates on a substantially different principle than any of the above technologies. An STT-MRAM cell consists of a reference magnetic layer (magnetization direction is fixed), free magnetic layer (magnetization direction is variable) and a tunneling barrier

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

between the two. The state encoding is determined by the direction of an applied spin-polarized current. Applied in one direction, spin-polarized electrons align the free layer to the reference layer, creating a low resistance state. Applied in the opposite direction, the free layer is forced to align opposite to the reference layer, creating a high resistance state. Existing works studying the endurance of STT-MRAM in deep learning applications demonstrate devices capable of $>10^{12}$ write cycles with little to no timing drift [4]. As MRAM does not rely on a filament creation or phase change, only magnetization direction, this makes intuitive sense. Unlike the previous technologies, STT-MRAM does not display the required behavior, and the encoding technique is unlikely work.

4.3 Paper 3 - Ryn

4.4 Paper 4 - Ryn

4.5 Paper 5 - Tome

4.6 Paper 6 - Tome

5 Summary of Field

References

[1] Farah Ferdaus, B. M. S. Bahar Talukder, and Md. Tauhidur Rahman. 2024. Hiding Information for Secure and Covert Data Storage in Commercial ReRAM Chips. *IEEE Transactions on Information Forensics and Security* 19 (2024), 3608–3619. doi:10.1109/TIFS.2024.3364845

[2] J. Q. Huang, L. P. Shi, E. G. Yeo, K. J. Yi, and R. Zhao. 2012. Electrochemical Metallization Resistive Memory Devices Using ZnS-SiO_2 as a Solid Electrolyte. *IEEE Electron Device Letters* 33, 1 (2012), 98–100. doi:10.1109/LED.2011.2173457

[3] Wu Lei, Cai Daolin, Chen Yifeng, Liu Yuanguang, Yan Shuai, Li Yang, Yu Li, Xie Li, and Song Zhitang. 2021//. Impact of Continuous RESET/SET Operations on Endurance Characteristic of Phase Change Memory. *Journal of Shanghai Jiao Tong University* 55, 9 (2021//), 1134 – 41.

[4] Z. Wei, W. Kim, Z. Wang, L. Hu, D. Jung, J. Zhang, and Y. Huai. 2022. Accurate and Fast STT-MRAM Endurance Evaluation Using a Novel Metric for Asymmetric Bipolar Stress and Deep Learning. In *2022 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits)*. 373–374. doi:10.1109/VLSITechnologyandCir46769.2022.9830351