Literature Review
September 2025

Ian Barnaby

ACM Reference Format:
Ian Barnaby. 2025. Literature Review September 2025. In . ACM, New York, NY, USA, 1 page. 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 [1]

This paper demonstrates a technique for covert data storage in ReRAM devices. 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 Paper 2 - Ian

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

Conference'17, Washington, DC, USA

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