Лаба 1

# ФИО

Голосов Н. В., Симонов И. А. (6112-100503)

# Topic

Hardware Security; Static Random Access Storage; RRAM

# Описание предметной области

Данный топик охватывает исследования в области использования RRAM и SRAM для хранения и защиты информации.

# Недостаток (Gap)

RRAM и SRAM уязвимо к физическим атакам, таким как взлом, перехват данных или вредоносная модификация компонентов.

# Идея

Использовать комплексную защиту посредством объединения методов Intel SGX, TrustZone для оптимизации хранения и передачи информации.

# Краткий текст обзора

При решении задач надежного хранения и защиты информации используются фундаментальные принципы работы с RRAM и SRAM [2], [4]. Также предоставлено описание механизмов данных структур – [6], [12], [13]. Наибольший всплеск публикаций наблюдался в период с 2015 по 2022. За этот период предложены некоторые высокотехнологичные методы – Intel SGX [9], [11], основывающийся на обеспечении и соблюдении политик доступа к памяти и разрешениях, и TrustZone [8], который выделяется изолированием подпространств процессора для обеспечения безопасности памяти. Были рассмотрены основные концепции методов генерации случайных чисел в пространстве памяти RAM. Этими взаимосвязанными методами стали TRNG и PUF [6], [10]. Для объективного сопоставления различных технологий в устройствах памяти и их использования для разработки средств защиты и вычислительных примитивов были предложены таблицы и графики сравнения [1], [6], [10]. В частности, проходят сравнения между различными технологиями RAM [5], [6]. Плюсом ко всему проведены аналогии технических характеристик их нескольких видов [1]. Сравниваются методы RRAM integration различных годов, продемонстрирована энергоэффективность TRNG на основе различных источников энтропии [10].

Ориентируясь на использование стандартных приемов защиты информации [3], [11] (в том числе современных методик сохранения и обработки [8]) и на анализ уязвимостей средств вычислительной техники (СВТ) на основе существующих видов памяти с произвольным доступом [3] и возможных механизмов блокирования эксплуатации [10], можно сказать, что защита информации находится на достаточно высоком уровне. При решении этой задачи рассматриваются всевозможные методы, начиная от дублирования информации и блокировки ошибочных операций до применения высокотехнологических способов обработки и противодействия непосредственного внедрения в программную составляющую компьютерной системы. Таким образом, текущие публикации дают понять, что каждый тип памяти используется для определенных целей: RRAM обладает высокой устойчивостью к физическим атакам и может быть использован для создания защищенных хранилищ данных. SRAM же обладает быстрой скоростью доступа и возможностью хранения данных без постоянного обновления.

Однако у них есть общие недостатки – типы данных подвержены физическим атакам и взломам, поэтому важно учитывать потенциальные уязвимости и риски.

В нашей статье мы предлагаем решение, способное устранить этот недостаток. Совместное использование методов Intel SGX и TrustZone и применение комплексной защиты предоставляет возможность наиболее эффективно обезопасить важные данные и информацию.

References

1. Коротин, Александр Михайлович. «Перспективные виды памяти с произвольным доступом и новые уязвимости СВТ на их основе». *Безопасность информационных технологий* 21, вып. 3 (2014 г.). <https://bit.mephi.ru/index.php/bit/article/view/169>.
2. *Методы и средства повышения надежности модулей памяти компьютеров*, 2018. <https://elibrary.ru/item.asp?id=35314246>.
3. «Система Хранения Данных В Соответствии С Профилем Хранения Данных», 2020 г. <https://elibrary.ru/item.asp?id=48376635>.
4. «Способы Сохранения Данных В Энергонезависимых Запоминающих Устройствах», 2003 г. <https://elibrary.ru/item.asp?id=37990516>.
5. Abbasian, Erfan, Morteza Gholipour, и Farzaneh Izadinasab. «Performance Evaluation of GNRFET and TMDFET Devices in Static Random Access Memory Cells Design». *International Journal of Circuit Theory and Applications* 49, вып. 11 (2021 г.): 3630–52. <https://doi.org/10.1002/cta.3108>.
6. Carboni, Roberto, и Daniele Ielmini. «Stochastic Memory Devices for Security and Computing». *Advanced Electronic Materials* 5, вып. 9 ( 2019 г.): 1900198. <https://doi.org/10.1002/aelm.201900198>.
7. Chen, Hong-Yu, Stefano Brivio, Che-Chia Chang, Jacopo Frascaroli, Tuo-Hung Hou, Boris Hudec, Ming Liu, и др. «Resistive Random Access Memory (RRAM) Technology: From Material, Device, Selector, 3D Integration to Bottom-up Fabrication». *Journal of Electroceramics* 39, вып. 1 (2017 г.): 21–38. <https://doi.org/10.1007/s10832-017-0095-9>.
8. Gross, Mathieu, Nisha Jacob, Andreas Zankl, и Georg Sigl. «Breaking TrustZone Memory Isolation and Secure Boot through Malicious Hardware on a Modern FPGA-SoC». *Journal of Cryptographic Engineering* 12, вып. 2 (2022 г.): 181–96. <https://doi.org/10.1007/s13389-021-00273-8>.
9. Jin, Yier. «Introduction to Hardware Security». *Electronics* 4, вып. 4 (2015 г.): 763–84. <https://doi.org/10.3390/electronics4040763>.
10. Rajendran, Gokulnath, Writam Banerjee, Anupam Chattopadhyay, и Mohamed M. Sabry Aly. «Application of Resistive Random Access Memory in Hardware Security: A Review». *Advanced Electronic Materials* 7, вып. 12 (2021 г.): 2100536. <https://doi.org/10.1002/aelm.202100536>.
11. Schunter, Matthias. «Intel Software Guard Extensions: Introduction and Open Research Challenges». В *Proceedings of the 2016 ACM Workshop on Software PROtection*, 1. SPRO ’16. New York, NY, USA: Association for Computing Machinery, 2016. <https://doi.org/10.1145/2995306.2995307>.
12. Wang, Hong, и Xiaobing Yan. «Overview of Resistive Random Access Memory (RRAM): Materials, Filament Mechanisms, Performance Optimization, and Prospects». *Physica Status Solidi (RRL) – Rapid Research Letters* 13, вып. 9 (2019 г.): 1900073. <https://doi.org/10.1002/pssr.201900073>.
13. Zahoor, Furqan, Tun Zainal Azni Zulkifli, и Farooq Ahmad Khanday. «Resistive Random Access Memory (RRAM): An Overview of Materials, Switching Mechanism, Performance, Multilevel Cell (Mlc) Storage, Modeling, and Applications». *Nanoscale Research Letters* 15, вып. 1 (2020 г.): 90. <https://doi.org/10.1186/s11671-020-03299-9>.