IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204172 |

A Review on Local Memory Bus Controller with ECC

Guruprasad R [1], **Nitin Manohar Mishra** [1], **Rajendra Gurukar** [1], **Swathi** [1], **Dr. C M Patil** [2]

8th Semester Students, Department of ECE, Vidyavardhaka College of Engineering, Mysuru, India [1]

Professor & Head, Department of ECE, Vidyavardhaka College of Engineering, Mysuru, India[2]

ABSTRACT : This project focuses on enhancing data reliability in computer systems by adding error correction code (ecc) features to the local memory bus controller (lmbc). the lmbc manages data flow between the cpu and system memory, with ecc technology crucial for spotting and fixing memory errors. the project highlights the importance of strong memory systems in modern computing, pointing out the risks of data corruption, system instability, and security issues linked to memory errors. the proposed solution involves integrating a hamming code-based ecc feature into the lmbc to boost data reliability, improving overall stability and security. the approach includes careful ecc algorithm selection, smooth integration with memory transport, and effective data validation and correction methods. this solution is especially useful for critical missions and high-performance computing tasks. in summary, the project aims to fortify computer systems, ensuring better data integrity through a comprehensive ecc-enabled lmbc design. keywords: data reliability, error correction code (ecc), local memory bus controller (lmbc), strong memory systems, critical computing.

I.INTRODUCTION

In the fast-evolving realm of computer systems, data reliability is key. The Local Memory Bus Controller (LMBC) is a vital link between the central processing unit (CPU) and system memory. Ensuring the trustworthiness and accuracy of data transfer is crucial, especially in critical tasks like servers, workstations, and industrial systems.

This paper explores a significant advancement: using Error-Correcting Code (ECC) in the LMBC to enhance data reliability, availability, and ECC is an advanced technique providing an extra shield against data errors in memory. It can spot and fix single-bit errors and spot multiple-bit errors. This capability significantly boosts data reliability by mitigating the impact of various factors causing data corruption, like cosmic rays, electromagnetic interferences, and manufacturing defects in memory modules reliability.

In this era of growing reliance on digital data, the vulnerability of systems to data corruption poses a significant risk. Traditional LMBCs, while efficient in data transfer, lack the robust error-detection and correction features needed to prevent and recover from data corruption. Data corruption can lead to system crashes, data loss, and downtime, with serious consequences in critical applications. Integrating ECC within the LMBC becomes crucial to address these concerns.

By the end of this study, we aim to highlight the advantages and potential challenges of adopting ECC in LMBCs, offering insights into its feasibility, performance implications, and overall impact on the reliability and stability of computer systems. This conclusion marks a crucial step toward strengthening the data reliability of computer systems, particularly those operating in mission-critical environments, and has the potential to reshape the landscape of data reliability and availability in the digital age.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204172 |

II. ECC IN A MEMORY SYSTEM

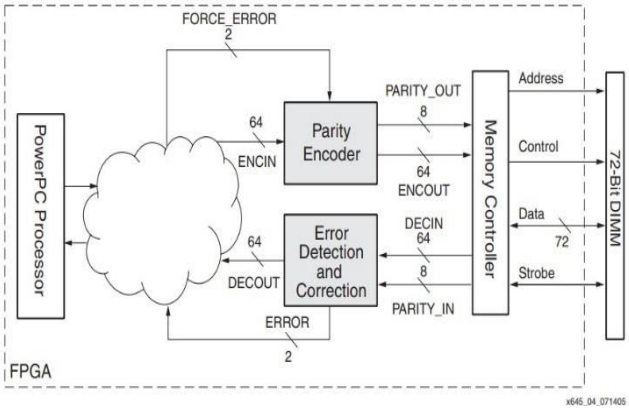

Figure 1: ECC in a Memory system [Single Error Correction and Double Error Detection – Simon Tam]

The over piece chart employing a DDR memory controller with ECC capacities. The DDR DIMM in this case could be a. Micron MT18VDDT6472G, an ECC arrangement module. The reference plan includes a equality encoder and equality decoder unit. The encoder actualizes the work of the generator framework, whereas the decoder is responsible for mistake discovery and adjustment. Also, the demonstrative capacities are backed. These capacities are portrayed within the taking after area.

III. LITERATURE REVIEW

[1] Miguel Costa and Srikanth Beerla's innovative technique, outlined in their research, introduces a groundbreaking approach to tackle the complexities of eFuse reliability and abandonment issues. By integrating a custom ECC module with a near-industry-standard BISR controller, they aim to enhance error detection and correction capabilities in eFuses. This novel method not only significantly reduces range overhead but also showcases its potential for diverse industry applications, promising improved efficiency and reliability in memory repair plans.

[2] Jungrae Kim's introduction of the All-Inclusive ECC (AIECC) marks a significant advancement in ensuring robust memory protection by addressing signal vulnerabilities and enhancing end-to-end data integrity. AIECC's ability to detect nearly 100% of CCCA errors and prevent transmission errors from compromising memory data integrity without additional overhead underscores its value as a comprehensive solution for data security .

[3] Shalini Ghosh's strategy to minimize control usage in ECC circuitry, focusing on SEC-DED codes like Hamming and Hsiao codes, represents a critical step towards optimizing memory systems. Supported by industry giants like Hewlett-Packard Enterprise and the National Science Foundation, this research delves into the application of simulated annealing and genetic algorithms to reduce control while maintaining area and delay constraints. The significant control reductions demonstrated for various error-correcting codes highlight the potential for enhanced efficiency and performance in memory systems.

[4] R. Way's proposal emphasizes the pivotal role of ECC within the Polyp multiprocessor system, underlining its significance in ensuring fault-tolerant data transfer across transport systems and memory storage. By leveraging forward and reverse equipment error recovery techniques (FHER and BHER), the ECC plays a crucial role in detecting and correcting errors, adapting to diverse transfer modes seamlessly. This approach not only enhances fault tolerance but also underscores the importance of decentralized error correction mechanisms within complex systems like Polyp, promising improved reliability and performance across various applications.

[5] Aniruddha N. Udipi's proposal introduces LOT-ECC, a novel reliability enhancement mechanism for memory systems that tackles limitations in existing error correction mechanisms. LOT-ECC separates error detection and correction using simple checksum and parity codes, offering robust fault-tolerance while minimizing power consumption and reducing latency. It is compatible with standard DRAMs and operating systems, and suggests the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204172 |

adoption of heterogeneous DIMMs to extend its reliability feature to wider memory components. The proposed mechanism offers significant power savings, implementation flexibility, and addresses various types of memory errors. Performance and power consumption of LOT-ECC are evaluated against existing reliability models, presenting options for optimizing storage overhead and access granularity. LOT-ECC demonstrates effectiveness across designs with different combinations of parameters, providing reliable guarantees while minimizing power usage and enhancing performance.

[6] Xiaochen Guo's project introduces the Sanitizer architecture, designed to address challenges in error correction and scrubbing in future spin-torque transfer magneto-resistive RAM (STT-MRAM) based main memories. Sanitizer employs a progressive ECC mechanism with local and global ECC to reduce over-fetching overhead and incorporates proactive scrubbing to anticipate and schedule cleaning operations prior to memory accesses. It also includes a differential update to global ECC bits, a careful data format for parallel access to global ECC bits, and support for chipkill ECC to optimize write operations and enhance memory reliability. The architecture is evaluated using various benchmarks, demonstrating a 1.22× performance improvement and a 22% reduction in system energy compared to conventional STT-MRAM systems. Parameters, ECC codeword size configurations, and hardware structures of Sanitizer are detailed, along with comparisons to performance and system energy savings. The study concludes that as technology transitions to non-volatile memories like STT-MRAM, Sanitizer will play a crucial role in mitigating the impact of costly ECC checks.

[7] Jishen Zhao's project focuses on adaptive granularity and ECC schemes to accommodate diverse memory behaviors. The system is evaluated using a combination of application profiling and cycle-level simulations. MAGE demonstrates superior performance and power consumption compared to baseline solutions across all workloads. It achieves the highest instructions per cycle (IPC) and power efficiency, resulting in the best system energy-delay product (EDP) for all workloads. The architecture's flexibility to different access granularity preferences of memory pages within applications results in significant improvements in performance and power efficiency. MAGE substantially reduces L2 cache misses, leading to better performance and power efficiency. The report also discusses the evaluation of reliability, performance, and power efficiency of standard structures with fixed modes and MAGE in the context of near-future 100 peta FLOPS systems. MAGE's mean time to failure (MTTF) is higher than FG-S and MG-C, but 5X lower than CG-D. MAGE outperforms both FG-S and MG-C solutions in all aspects, including performance, power efficiency, and reliability.

[8] Lucian Cojocar's proposal introduces ECCploit, a Rowhammer attack exploiting undocumented ECC usage details, a novel memory controller side channel, and data-driven bit flips. ECCploit can be utilized for profit-enhancing attacks on ECC-based systems. The study found that even with an imperfect page table spraying technique, unauthorized memory pages could be mapped with a 39.9% success rate and a 2.5D44 success rate for page table pages. They also tested with RSA keys and found that ECCploit may efficiently factorize flawed keys. The paper addresses the challenges of reverse engineering ECC capabilities, triggering Rowhammer corruptions on ECC memory, and exploiting the system given that Rowhammer-based ECC corruptions corrupt multiple bits simultaneously. It also discusses the impact of ECC-based exploitation techniques on the success of the attack compared to conventional Rowhammer exploits. The study concludes that reliable Rowhammer attacks are possible, even if the system reports ECC events accurately, and highlights the need for enhanced protections against these attacks.

[9] Seong-Lyong Gong proposes a novel memory security scheme called CLEAN ECC, designed to balance fine-grained memory access and robust error correction codes (ECC). The scheme's performance, reliability, and hardware overhead are evaluated using multi SPEC CPU2006 benchmarks and Monte Carlo simulations. Results show that CLEAN ECC improves system performance and efficiency, reduces memory power consumption, and demonstrates high reliability comparable to standard Chipkill systems. The paper also discusses related work on memory security schemes and presents key takeaway points from the evaluation. Overall, the report presents and evaluates the CLEAN ECC scheme as a promising solution for memory security in high-performance computing systems

[10] S. Pontarelli proposes a method using redundant CAM elements and single parity bit encoding for error detection and correction. The paper provides a comprehensive examination of CAM properties, the effects of Single Event Upsets (SEU), and proposed error correction methods. It also explores the application of the proposed method in a CAM/RAM hybrid system, aiming to address SEU effects in CAM while ensuring system-level reliability. The report presents a novel approach for error detection and correction in CAM, offering a detailed analysis of the proposed

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204172 |

approach and its suitability to different CAM configurations and scenarios. The method shows promise in addressing SEU effects while ensuring the reliability of CAM systems.

[11] Marco Ottavi's proposal effectively identifies and corrects errors in CAMs, with low penalties in terms of area and power consumption. The paper provides an in-depth analysis of CAM design, the impacts of soft errors, and the use of Bloom filters for error detection. It also includes experimental results and simulations to evaluate the effectiveness of the proposed solution. The authors, Salvatore Pontarelli and Marco Ottavi, have extensive experience in microelectronics and telecommunications, focusing on error-detection and correction codes, fault tolerance in digital systems, and the development of highly reliable systems for space applications. Their research interests also include the use of post-CMOS technologies for implementing digital circuits at subnanometric integration scale. The report serves as a valuable resource for researchers and engineers working in the field of error detection and correction in high-speed network systems and chips.

[12] Nandivada Sridevi proposes an approach focusing on the implementation of error correction codes to address memory issues. The main objective is to extend the SEC-DED code to the SEC-DED-DAEC code, capable of single error correction, double error detection, and double adjacent error correction. The authors review various error correction methods, including the (7,4) Hamming code, SEC-DED code, and SEC-DED-DAEC code, and their applications in memory systems. They propose and implement the SEC-DED-DAEC code, demonstrating its effectiveness in detecting and correcting errors adjacent up to 2 bits. The paper also discusses the encoding and decoding processes of these error correction codes along with simulation results verified using Verilog coding in the Xilinx ISE 14.7 tool. The proposed method shows promise in advancing the reliability and performance of memory applications in the presence of soft errors.

IV. CONCLUSION

The ECC functions described in this application note are made possible by Hamming code, a relatively simple yet powerful ECC code. It involves transmitting data with multiple check bits (parity) and decoding the associated check bits when receiving data to detect errors. The check bits are parallel parity bits generated from XORing certain bits in the original data word. If bit error(s) are introduced in the codeword, several check bits show parity errors after decoding the retrieved codeword. The combination of these check bit errors displays the nature of the error. In addition, the position of any single bit error is identified from the check bits.

REFERENCES

[1] Miguel Costa, Srikanth Beerla,"Enabling ECC and Repair Features in an eFuse Box for Memory Repair Applications, “Published in: 2021 22nd International Symposium on Quality Electronic Design (ISQED), https://doi.org/10.1109/ISQED51717.2021.9424327

[2] Jungrae Kim, Michael Sullivan, Sangkug Lym, Mattan Erez, "All-Inclusive ECC: Thorough End-to-End Protection for Reliable Computer Memory," ACM SIGARCH Computer Architecture News, Volume: 44, Issue 3, pp 622–633, https://doi.org/10.1145/3007787.3001203

[3] S. Ghosh, S. Basu, N.A. Touba, "Reducing power consumption in memory ECC checkers," Published in: 2004 International Conference on Test
https://DOI:10.1109/TEST.2004.1387407

[4] R. Männer, O. Stucky, "Fault-Tolerant Data Transfer in a Multiprocessor System by Forward and Backward Hardware Error Recovery," The Computer Journal, Volume 35, Issue 4, August 1992, Pages 361–368 ; https://doi.org/10.1093/comjnl/35.4.361

[5]Aniruddha N. Udipi, Naveen Muralimanohar, Rajeev Balsubramonian, Al Davis, Norman P. Jouppi, "LOT-ECC: localized and tiered reliability mechanisms for commodity memory systems, " ACM SIGARCH Computer Architecture News, Volume 40, Issue-3, pp 285–296, https://doi.org/10.1145/2366231.2337192.

[6] Xiaochen Guo, Mahdi Nazm Bojnordi, Qing Guo; Engin Ipek, "Sanitizer: Mitigating the Impact of Expensive ECC Checks on STT-MRAM Based Main Memories ," Published in: IEEE Transactions on Computers (Volume: 67, Issue: 6, 01 June 2018), https://doi:10.1109/TC.2017.277915

[7] Sheng Li, Doe Hyun Yoon, Ke Chen, Jishen Zhao, Jung Ho Ahn, Jay B. Brockman, Yuan Xie, "Sanitizer: Mitigating the Impact of Expensive ECC Checks on STT-MRAM Based Main Memories ," Published in: IEEE Transactions on Computers (Volume: 67, Issue: 6, 01 June 2018), https://doi:10.1109/TC.2017.2779151

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204172 |

[8] Lucian Cojocar, Kaveh Razavi, Cristiano Giuffrida, Herbert Bos, "Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks ," Published in: 2019 IEEE Symposium on Security and Privacy (SP) , https://doi:10.1109/SP.2019.00089

[9] Seong-Lyong Gong, Minsoo Rhu, Jungrae Kim, Jinsuk Chung, Mattan Erez , "CLEAN-ECC: high reliability ECC for adaptive granularity memory system ," MICRO-48: Proceedings of the 48th International Symposium on Microarchitecture , December-2015 , Pages-611–622 , https://doi.org/10.1145/2830772.2830799

[10] S. Pontarelli, M. Ottavi, A. Salsano , "Error Detection and Correction in Content Addressable Memories ," Published in: 2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems , https://doi:10.1109/DFT.2010

[11] Salvatore Pontarelli, Marco Ottavi, " Error Detection and Correction in Content Addressable Memories by Using Bloom Filters ," Published in: IEEE Transactions on Computers (Volume: 62, Issue: 6, June 2013) , Page(s): 1111 - 1126 , https://doi:10.1109/TC.2012.56

[12] Nandivada Sridevi, K. Jamal, Kiran Mannem ,"Implementation of Error Correction Techniques in Memory Applications ,"Published in: 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), https://DOI:10.1109/ICCMC51019.2021.9418432

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details