Graduate School of Fundamental Science and Engineering
Waseda University

博　士　論　文　概　要
Doctoral Dissertation Synopsis

論　文　題　目
Dissertation Title

Studies on Evaluation Platforms for DRAM/NVMM Heterogeneous and Secure Computing Memory Systems

DRAMとNVMMによるヘテロジニアスメモリシステム及びセキュアコンピューティングメモリシステム評価環境の研究

申　請　者
(Applicant Name)
Yu OMORI
大森　侑

Department of Computer Science and Communications Engineering, Research on Advanced Processor Architecture

December, 2022

DRAM-based homogeneous main memory and non-volatile storage devices have been mainstream components of the memory hierarchy in computer systems. They have been used complementary in combination to exploit performance and capacity. However, this traditional memory hierarchy must be more attractive for contemporary computer architectures and workloads. For instance, DL/ML-based AI and IoT computing development have diversified evaluation platforms and requirements. A large AI processing server requires ample memory space to process large models and many input data in parallel. IoT edge devices require a memory system with low power consumption and simple accessibility. Introducing heterogeneous memory systems is a promising approach to dealing with these new demands.

NVMM (Non-Volatile Main Memory) is a new memory device with non-volatile memory cells. It is superior to traditional DRAM-based main memory in capacity and power consumption. NVMM cells can hold data without periodical refresh operations. It is also superior to block storage devices in terms of latency and accessibility. Unlike them, a memory controller can access data on NVMM in a byte unit using memory buses. Thanks to NVMM characteristics, various computer systems can take advantage of heterogeneous memory systems consisting of DRAM and NVMM. An IoT edge device is one of the expected usecases. A memory controller can directly use data on NVMM without the help of complex device drivers provided by an OS. On the other hand, the heterogeneous memory system raises the demands of new optimizations considering the characteristics of NVMM. Optimizations for DRAM-based main memory may severely degrade system performance when directly applied to NVMM due to its long and asymmetric latency. Focusing on byte accessibility and several hundreds access latency, a page cache is redundant for NVMM.

Despite the demand, exploring optimization techniques for NVMM on edge devices is challenging when using existing evaluation platforms. There are few available real NVMMs. Intel Optane DC Persistent Memory (DCPMM) is the existing NVMM; however, it can work on only some specific Intel server grade CPUs due to Intel's particular DDR-T protocol. The lack of NVMM for edge devices results in the widespread use of simulators and emulators. Existing simulators can provide detailed evaluations of DRAM/NVMM heterogeneous memory systems with high flexibility. On the other hand, they are slow to evaluate whole hardware and/or large applications including an OS. While existing emulators can evaluate the whole system in shorter time than simulators, execution cycles of emulated applications are inaccurate. This tradeoff has limited exploration of system-wide optimization techniques for DRAM/NVMM heterogeneous memory systems on edge devices.

In addition, secure computing on edge devices is one of the expected DRAM/NVMM heterogeneous memory systems' usecases. Recent AI/IoT development has shifted inference from cloud servers to edge devices like smartphones and autonomous driving cars. Inference on edge devices requires strict data protection for a trained model for confidentiality and input data for privacy. TEE (Trusted Execution Environment) is an expected solution to realize a lightweight and strictly isolated memory region for both program code and data. However, its strict memory isolation introduces two significant issues of memory systems: auxiliary devices and off-chip memory protection. A program on TEE cannot use any

untrusted software, including device drivers provided by a host OS. Thus, existing TEE has difficulty in utilizing data on an auxiliary device. Besides, TEE itself mainly focuses on on-chip data protection. An adversarial attacker who is capable of bypassing CPUs can access data on the protected region. DMA, off-chip memory bus tapping, and cold-boot attack are examples. These two issues can be solved by extending the memory system with NVMM-based auxiliary storage and MPE (Memory Protection Engine), respectively. While optimization techniques must be explored to exploit their advantages, no existing works are compatible with the combination of TEE, NVMM, and MPE.

This dissertation proposes evaluation platforms for DRAM/NVMM heterogeneous memory systems on edge devices to explore optimization techniques. The first proposal is a hardware NVMM simulator on an FPGA that can solve the tradeoff between existing NVMM simulators and emulators. It provides multiple NVMM architectures and behaviors that are validated against golden models (existing NVMM simulators and a real DCPMM). The proposed simulator also supports DCPMM simulation, which is not considered in existing works. Experimental evaluation using micro-benchmarks and real applications reveals the direction and essential factors in DRAM/NVMM heterogeneous memory systems' optimizations. A second proposal is a hardware simulator having all of TEE, NVMM, and MPE. It integrates the newly implemented MPE into the TEE-compatible NVMM simulator. This hardware simulator is a widely available evaluation platform for TEE, NVMM, and MPE combined systems.

This dissertation consists of 6 chapters.

Chapter 1 "Introduction" describes this dissertation's background, related works, and proposals. This dissertation mainly consists of two contributions: evaluation platforms for DRAM/NVMM heterogeneous memory systems and an evaluation platform for secure computing employing the heterogeneous memory systems. First, traditional memory hierarchy and the necessity of DRAM/NVMM heterogeneous memory systems to satisfy the demands of contemporary architectures and workloads are described. Second, this chapter compares the role of an evaluation platform for DRAM/NVMM heterogeneous memory systems on an FPGA with existing evaluation platforms. The proposed evaluation platform solves existing works' issues, and provides a way to explore system-wide optimization techniques for the heterogeneous memory systems. Third, the necessity and issues of secure computing on edge devices for recent workloads are described. The issues can be solved by combining NVMM and MPE to TEE. However, existing evaluation platforms are not compatible with the combination. The proposed evaluation platform having the combination provides a way to explore secure computing on edge devices.

Chapter 2 "DRAM/NVMM Heterogeneous Memory Simulator on Hard Processor Systems" proposes a hardware DRAM/NVMM heterogeneous memory simulator working on hard processor systems, especially ARM SoC. This chapter consists of 4 parts: NVMM behavior models, simulator implementation, validation of the behavior models, and experimental evaluation. The first part discusses and defines three NVMM behavior models that represent NVMM architectures and behaviors. The Coarse-Grain and Fine-Grain models represent NVMM behaviors with similar architectures to traditional DRAM-based memory. Only the Fine-Grain model can capture memory access characteristics to reduce NVMM latency, such

as access locality. The DCPMM model is a new behavior model that represents the actual DCPMM behavior with some constraints for edge devices. The second part describes the whole simulator implementation: delay injection techniques to simulate NVMM performance based on three behavior models, kernel modification, kernel module, and management library to use the NVMM region effectively. The third part validates the NVMM behavior models by comparing them with golden models (existing NVMM simulators and a real DCPMM). The validation also confirms that the Fine-Grain behavior model can capture an impact of memory access characteristics that is ignored in the Coarse-Grain behavior model. The fourth part evaluates real applications chosen from SPEC CPU 2017 benchmarks on the proposed simulator using three NVMM behavior models. The result shows that the frequency of NVMM accesses, access locality, and bank parallelism are essential factors in exploiting NVMM performance. The last two factors can alleviate the first factor's impact; however, frequent memory accesses spoil them and severely degrade system performance.

Chapter 3 "DRAM/NVMM Heterogeneous Memory Simulator on Soft Processor Systems" proposes a hardware DRAM/NVMM heterogeneous memory simulator working on soft processor systems, especially RISC-V SoC. The Fine-Grain behavior model proposed in Chapter 3 cannot be directly applied to soft processor systems because the model presupposes that a CPU runs sufficiently faster than a memory subsystem. The Fine-Grain model on soft processor systems shows the same behavior as the Coarse-Grain one, even if an application has high access locality. This chapter proposes a new NVMM behavior model, "Extended Fine-Grain", that can exploit access locality even soft processor systems. Besides, the simulator's RISC-V core design is modified so a user program can directly evict a cacheline. Validation using micro benchmarks and experimental evaluation using SPEC CPU 2017 benchmarks shows that the Extended Fine-Grain model can capture an impact of access locality even on soft processor systems, unlike the existing Coarse-Grain and Fine-Grain models. The DCPMM model on the simulator is validated against a real DCPMM.

Chapter 4 "Secure Edge Computing Simulator Employing DRAM/NVMM Heterogeneous Memory Systems" proposes a hardware simulator having all of TEE, DRAM/NVMM heterogeneous memory system, and MPE. Among existing TEEs, this dissertation focuses on open-source RISC-V Keystone TEE that can satisfy various requirements of edge devices. This chapter implements an MPE, then integrates it into the DRAM/NVMM simulator proposed in Chapter 3. The Rocket core on the simulator is compatible with Keystone TEE. The MPE is based on SGX-style Integrity Tree used in Intel SGX TEE. Pipelined modules in the MPE cooperatively work as much as possible to maximize throughput. The MPE is designed to cover a large memory region with limited hardware resources by introducing dynamic tree roots and modules while keeping Tree parallelism. Experimental evaluation on the proposed simulator shows that the MPE incurs 2.55×/4.16× for DRAM read/write, respectively. It also showed that MPE incurs 3.05×/5.40× for simulated DCPMM read/write, respectively.

Chapter 5 "Conclusion" concludes this dissertation.

List of research achievements for application of Doctor of Engineering, Waseda University

Full Name : 大森　侑　　seal or signature

Date Submitted(yyyy/mm/dd): 2022/12/8

種類別 (By Type)	題名、 発表・発行掲載誌名、 発表・発行年月、 連名者（申請者含む） (theme, journal name, date & year of publication, name of authors inc. yourself)
a. Academic papers	◯ Yu Omori and Keiji Kimura, "Open-Source Hardware Memory Protection Engine Integrated With NVMM Simulator", *IEEE Computer Architecture Letters* , Vol.21, No.2, pp.77-80, 2022, Available: https://doi.org/10.1109/LCA.2022.3197777
	◯ Yu Omori and Keiji Kimura, "Non-Volatile Main Memory Emulator for Embedded Systems Employing Three NVMM Behaviour Models", *IEICE Transactions on Information and Systems* , Vol.E104-D, No.5, pp.697-708, 2021, Available: https://doi.org/10.1587/transinf.2020EDP7092
c. Lectures (Reviewed International Conference Papers)	◯ Yu Omori and Keiji Kimura, "Open-Source RISC-V Linux-Compatible NVMM Emulator"', *Sixth Workshop on Computer Architecture Research with RISC-V (CARRV 2022), co-located with ISCA'22* , New York City, USA, Jun. 2022.
	◯ Yu Omori and Keiji Kimura, "Performance Evaluation on NVMM Emulator Employing Fine-Grain Delay Injection", *2019 IEEE Non-Volatile Memory Systems and Applications Symposium (NVMSA)* , pp.1-6, Hangzhou, China, Aug. 2019, Available: https://doi.org/10.1109/NVMSA.2019.8863522
c. Lectures (Domestic Workshop)	Lena Yu, Yu Omori and Keiji Kimura, "Prototype Implementation of Non-Volatile Memory Support for RISC-V Keystone Enclave", *SWoPP2021: Parallel, Distributed and Cooperative Processing Systems and Dependable Computing* , vol.121, No.116, pp.7-12, Jul. 2021
	大森 侑, 木村 啓二, "Linuxが動作可能なRISC-V NVMMエミュレータの実装", *情報処理学会 第236回システム・アーキテクチャ・第194回システムとLSIの設計技術・第56回組込みシステム合同研究発表会(ETNET2021)* , Vol.2021-ARC-244, No.1, pp.1-10, Mar. 2021.
	林 知輝, 大森 侑, 木村 啓二, "整合性ツリーおよび暗号化機構を持つ不揮発性メインメモリエミュレータの実装", *情報処理学会 第236回システム・アーキテクチャ・第194回システムとLSIの設計技術・第56回組込みシステム合同研究発表会(ETNET2021)* , Vol.2021-ARC-244, No.2, pp.1-8, Mar. 2021.
	大森 侑, 木村 啓二, "不揮発性メインメモリエミュレータの評価", *情報処理学会 第227回システム・アーキテクチャ・第187回システムとLSIの設計技術・第50回組込みシステム合同研究発表会（ETNET2019）*, Vol.2019-ARC-235, No.19, pp.1-8, Mar. 2019.