RISC-V 코어의 보안 기능 구현을 위한 Dhrystone 기반 연산 성능 분석

강기봉 [1], 황윤성 [1], 유준승 [1], 백윤흥 [1]
[1] 서울대학교 전기 • 정보공학부, 서울대학교 반도체 공동연구소

rkdrlqhd@snu.ac.kr, leo6121@snu.ac.kr, jsyou@sor.snu.ac.kr, ypaek@snu.ac.kr

Performance Analysis of RISC-V Cores for Security Feature Implementation

Ki-bong Kang[1], Yun-seong Hwang[1], Jun-seung You[1], Yun-heung Paek[2]
[1]Dept. of Electronic and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

RISC-V 는 Open-source ISA 로 2010 년 제안된 이후 상용화를 위해 많은 연구가 진행되고 있다. 다양한 하드웨어적 보안 기법과 최적화가 이루어지고 있지만, 오픈소스 RISC-V 코어에 부채널 공격에 대한 방어 기법이 부족한 것을 확인하였기에 상용화할 RISC-V 코어에 부채널 공격 방어 기법이 적용되어야 더욱 안전한 사용이 가능하다. 또한 기존에 개발된 코어에 대한 통일된 환경에서의 성능 비교 및 분석은 따로 진행되지 않아 상용화할 코어를 선정할 근거 역시 부족한 상황이다. 따라서 본 논문에서는 부채널 공격 방어 기법을 구현할 RISC-V 코어를 선정하기 위해 각 코어에 대한 성능 분석 및 비교를 진행한다. 이를 통해 기존 시스템의 보안 코어를 대체할 수 있는 코어를 선별하여 추후 방어 기법 구현에 활용한다.

1. 서론

2010 년 UC Berkeley 에서 RISC-V ISA 를 오픈소스로 공개한 이후, 많은 개발자들이 해당 오픈소스를 활용하여 코어를 개발하고 다양한 기능을 구현하고 있다. ‘Keystone’ 프로젝트를 통해 RISC-V 에서 Enclave 를 구현하여 신뢰실행환경을 구축하거나[1], ‘PMP’ 기능을 사용하여 코어의 물리적 메모리 접근을 제어하는 등의 보안 기능이 구현되었고[2], 오픈소스 코어는 이 기능들을 활용하여 자체적인 보안 수준을 향상시킬 수 있다. 하지만 최근 연구되고 있는 Ciphertext 부채널 공격[3]에 대한 보안 기능은 별도로 연구되거나 오픈소스로 공개되어 있지 않은 상황이다. 해당 공격은 AMD SEV 환경에서 malicious hypervisor 를 활용하여 부채널 공격을 진행하며, 공격을 통해 16byte plaintext 를 추출할 수 있다. 이에 대한 소프트웨어적 방어 기법이 소프트웨어로 연구되었으나[4] 하드웨어적으로 RISC-V ISA 에 구현되어 있는 방어 기법은 없어 효과적인 하드웨어적 방어 기법 구현이 필요하다.

방어 기법을 RISC-V ISA 에 적용하는 연구에 앞서 기존 시스템에서 사용하는 코어와 비슷한 수준의 RISC-V 코어를 선정하여 코어를 변경하더라도 실제 운용 과정에서 성능이 하락하지 않도록 해야 한다. 따라서 본 연구에서는 방어 기법을 구현하기 전 다양한 RISC-V 코어를 조사하고 해당 코어들에 대해 동일한 Benchmark 프로그램을 실행하여 ARM 의 상용 보안 코어와 성능을 비교한다. 이 비교를 통해 연구할 코어에 대한 상용성과 적합성을 판단하고 추후 연구를 위한 코어를 선정한다.

섹션 2,3 에서는 Ciphertext 부채널 공격과 Dhrystone Benchmark 에 대해 설명한다. 섹션 4 에서는 선정한 RISC-V 코어를 간략히 정리하고 섹션 5 에서 각 코어에 대한 Dhrystone test 를 진행하여 결과를 분석한다. 마지막으로 섹션 6 에서는 분석 결과를 기반으로 연구 대상 코어를 선정하고, 구현할 방어 기법에 대해 서술한다.

2. Ciphertext 부채널 공격

Ciphertext 부채널 공격은 AMD 의 신뢰실행환경인

SEV 를 대상으로 한 공격으로 AMD-SEV 가 사용하는 Xor-Encrypt-Xor(XEX) 모드가 deterministic 하다는 점을 이용한다. XEX 모드는 같은 memory 주소에 같은 plaintext 를 encryption 하여 저장할 경우 항상 같은 값을 출력한다. 이를 통해 VMSA(VM save area)에 저장되어 있는 호스트의 암호화된 register 값을 malicious hypervisor 를 통해 알아내고 이를 기반으로 plaintext 를 복구하는 등의 공격을 진행할 수 있다. 이 공격은 AMD-SEV 에 encryption state 와 secure nested page 를 추가한 SEV-ES, SEV-SNP 에서도 가능하며[5], [4]에서는 이 공격에 대한 소프트웨어적 방어 기법을 구현하였으나 mask value 와 secrecy value 를 secret data 만큼 할당해야 한다는 문제점과 소프트웨어 내에서의 처리로 인한 딜레이 발생의 문제가 존재한다. 이는 컴퓨팅 자원이 부족한 임베디드 시스템 등에는 적용하기 어렵고, 결과적으로 임베디드 시스템에서는 소프트웨어가 아닌 다른 방식의 보호 기법 적용이 필요하다.

3. Dhrystone Test

Dhrystone test 는 RISC 와 CISC 의 명령어 처리 속도를 직접적으로 비교하기 어려워 고안된 벤치마크로 정수 연산에 대한 처리 성능을 측정한다. 1987 년 Reinhold P. Weicker 가 개발하였으며 벤치마크 실행을 통해 정규화된 수치를 구할 수 있어 여러 CPU/AP 제조사에서 코어의 성능을 DIMPS 수치로 제시한다.

Dhrystone Test 진행 과정은 다음과 같다.

1. 테스트 CPU 에서 Dhrystone 의 C 코드를 실행한 후 해당 CPU 의 Dhrystone score 를 구한다.
2. 측정된 score 를 1757 로 나누어 Dhrystone MIPS(DMIPS) 을 구한다.
3. 측정된 DMIPS 값을 CPU 의 frequency 로 나누어주어 DMIPS/MHz 를 구한다.

처음 고안된 이후 여러 버전이 존재하며, 버전 별로 동일한 코어에 대해서도 약간의 오차가 발생하기 때문에 실험 과정에서 동일한 dhrystone 코드를 사용할 필요가 있다.

4. RISC-V 코어 분석

여러 RISC-V 코어의 성능을 테스트하기 전 verification 이 가능한 코어를 선별하여 지원가능 명령어 종류, 파이프라인, 레지스터 사이즈, 보안 기능 여부 등을 조사하였다. 또한 시뮬레이션 과정에서 올바른 분석을 위해 코어 개발자가 제공하는 시뮬레이션 환경을 확인하였다.

4-1. CV32e40p

CV32e40p 는 32-bit 4-stage pipelined RISC-V 코어로, CV32e40 시리즈 중 FPU, hardware loop 등이 적용된 모델이다. In-order processor 로 Branch predictor 와 speculative execution 등이 존재하지 않고, 추가적인 보안 기능이 적용되어 있지 않다. 기본적으로 RV32I instruction set 을 사용하며, 경우에 따라 C,M,F 등 다양한 extension 을 추가할 수 있다. OBI(Open Bus Interface) bus protocol 을 사용하여 다른 디바이스와 연결할 수 있다. 제공하는 시뮬레이션 환경은 Verilator, Xcelium, Modelsim 등이 있으며 Systemverilog 로 작성되었다.

4-2. Picorv32

Picorv32 는 32-bit multicycle RISC-V 코어로, 파이프라인이 없는 CPU 이다. In-order processor 이며 추가적인 보안 기능 또한 적용되어 있지 않다. RV32E,RV32I[M][C] instruction set 을 사용하고, 저전력 저성능 디바이스를 대상으로 개발되었다. AXI (Advanced eXtensible Interface) bus protocol 을 사용하여 다른 디바이스와 연결할 수 있고, PCPI(Pico Co-Processor Interface)를 통해 mul, div 등의 연산을 지원한다. 제공되는 시뮬레이션 환경은 Icarus Verilog (Iverilog)와 Verilator 이며 verilog 로 작성되었다. 공개되어 있는 DMIPS/MHz 수치는 0.516 이다.

4-3. DarkRISCV

DarkRISCV 는 32-bit 2(3)-stage pipelined RISC-V 코어로 사용자가 pipeline 개수를 선택할 수 있다. 별도의 Branch predictor 나 speculative execution 이 존재하지 않으며 추가적인 보안 기능 또한 적용되어 있지 않다. RV32E, RV32I 에 대한 대부분의 instruction 을 지원하며 사용자에 따른 기능 추가를 위해 다양한 옵션(16×16 MAC instruction, Harvard or Von neumann)을 지원한다. 제공되는 시뮬레이션 환경은 Icarus verilog(Iverilog)와 Xilinx ISE 이며 verilog 로 작성되었다.

Core	DMIPS/MHz	Pipeline Stage	ISA
CV32e40p	0.566	4	RV32I
Picorv32	0.503(Verilator) 0.528(Iverilog)	1	RV32I
DarkRISCV	1.140	2	RV32I
Kronos	0.7105	3	RV32I
biRISC-V	1.9	6~7	RV32I
ARM SC300	1.25	3	ARMv8-M
ARM M35P	1.50	3	ARMv7-M

표 1. 코어 선정을 위한 DMIPS/MHz 측정/조사 결과

5. 실험 결과

조사한 세 종류의 코어를 기반으로 dhrystone test 를 진행하였다. Dhrystone test 의 실행 및 Score 측정은 Verilator 와 Icarus verilog 중 코어에서 제공하는 시뮬레이터를 사용하여 측정하였으며, Picorv32 는 두 시뮬레이터에서 모두 측정하였다. Dhrystone test 의 version 은 2.1 이며 RISC-V 코어의 특성상 컴파일에 std library 를 포함할 때 에러가 발생하는 코어가 있기 때문에 이를 해결하기 위해 Dhrystone test code 에 inline 으로 함수를 구현하였다. 최대한 성능에 영향을 주지 않도록 컴파일 옵션을 통일하였으며, 시뮬레이션은 100MHz 에서 진행하였다. 그 외에도, 공개되어 있는 RISC-V 코어 중 Dhrystone score 가 공개되어 있는 Kronos 와 biRISC-V 에 대해 조사를 진행하였고, 상용 임베디드 시스템에서 사용하는 보안 코어인 ARM SC300 과 M35P 를 추가로 조사하였다.

측정 및 조사 결과는 표 1 과 같다. CV32e40p 는 Verilator 실행 환경에서 0.566 DMIPS/MHz 를 얻었고, Picorv32 는 Verilator 에서는 0.503 DMIPS/MHz, Iverilog 에서는 0.528 DMIPS/MHz 를 얻었다. DarkRISCV 는 Iverilog 에서 1.140 DMIPS/MHz 라는 수치를 얻었다. 그 외에도 Kronos 와 biRISC-V 의 경우 각각 0.7105 DMIPS/MHz 와 1.9 DMIPS/MHz 라는 수치를 Document 및 자체 페이지에서 확인할 수 있었고, ARM SC300 과 M35P 의 경우 ARM 의 공식 홈페이지에 나와있는 정보를 참고하여 각각 1.25 , 1.50 라는 값을 확인하였다.

임베디드 시스템에서 가장 많이 사용되는 ARM 의 보안 코어가 1.25 이상의 DMIPS/MHz 값을 가지고 있으므로, 이를 대체할 코어 또한 비슷한 성능을 보여야 할 것이다. Picorv32 의 경우 저전력/저성능의 코어로 ARM 코어를 대체하기엔 성능적인 면에서 부족하다는 것을 확인할 수 있다. Pipeline 이 4 개여서 다른 코어에 비해 성능이 우수할 것으로 예측한 CV32e40p 의 경우에도 pipeline 이 1 개인 Picorv32 와 큰 차이가 나지 않는 것을 확인하였다. 이는 pipeline 이 동작하지 않는 것과 다름이 없는 수준으로 코어가 가진 스펙에 비해 성능이 안 좋아 ARM 코어 대신 사용하기엔 어려움이 예상된다. 그에 반해 DarkRISCV 의 경우 pipeline 의 개수는 2 이지만 측정된 성능은 1.140 으로 ARM SC300 이나 M35P 와 큰 차이가 나지 않았다. Kronos 의 경우 실제 성능이 ARM 코어에 비해 부족하며 biRISC-V 는 코어가 비교적 간단해야 할 임베디드 시스템에서 사용하기에 6~7 stage 라는 너무 많은 pipeline stage 를 가지고 있기 때문에 ARM 코어를 대체하기에는 적합하지 않다.

따라서 분석 결과 추후 ARM 코어를 대체할 수 있으며 Ciphertext side-channel 연구에도 적합한 코어는 DarkRISCV 라고 할 수 있다.

6. 결론 및 추후 연구 방향

본 연구는 상용 ARM 보안 코어를 대체할 RISC-V 코어를 정하기 위해 다양한 오픈소스 코어에 대해 동일한 Benchmark 를 사용하여 DMIPS/MHz 를 측정하고, 측정된 점수를 기반으로 분석을 진행했다. 이 과정에서 별도로 존재하지 않는 CV32e40p, Picorv32, DarkRISCV 의 DMIPS/MHz 를 구하였고, 다른 Core 와의 DMIPS/MHz 비교를 통해 DarkRISCV 가 성능적으로 기존의 임베디드 시스템에서 많이 사용되는 ARM 보안 코어를 대체하기에 적합하다는 것을 확인하였다.

이를 통해 추후 연구에서는 Ciphertext side-channel 방어 기법의 하드웨어적 구현 위해 DarkRISCV 에 Keystone 을 적용하여 TEE 환경을 구현하고, 해당 TEE 환경에서도 Ciphertext side-channel 취약점이 존재하는지 확인한 후 해당 문제점을 해결할 수 있는 방어 기법을 구현할 예정이다. 이를 통해 기존의 ARM 코어를 대체할 수 있는 오픈소스 보안 코어를 개발하는 것이 목표이다.

ACKNOWLEDGEMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며(RS-2023-00277326), 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었으며, 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며(No.2021-0-00528, 하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발), 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며(IITP-2023-RS-2023-00256081), 반도체 공동연구소 지원의 결과물임을 밝힙니다.

참고문헌

[1] Lee, Dayeol, et al. "Keystone: A framework for architecting tees." arXiv preprint arXiv:1907.10119 (2019).

[2] Cheang, Kevin, et al. "Verifying RISC-V physical memory protection." arXiv preprint arXiv:2211.02179 (2022).

[3] Li, Mengyuan, et al. "{CIPHERLEAKS}: Breaking Constant-time Cryptography on {AMD}{SEV} via the Ciphertext Side Channel." 30th USENIX Security Symposium (USENIX Security 21). 2021.

[4] Wichelmann, Jan, et al. "Cipherfix: Mitigating Ciphertext {Side-Channel} Attacks in Software." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

[5] Li, Mengyuan, et al. "A systematic look at ciphertext side channels on AMD SEV-SNP." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.