RISC-V 프로세서에 대한 전력 분석 완화 기법 연구

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

rkdrlqhd@snu.ac.kr, ypaek@snu.ac.kr

A study of Power analysis Attack Mitigation for RISC-V processor

Kibong Kang[1], Yunheung Paek[1]
[1]Dept. of Electronic and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

2010 년 UC Berkely 에서 개발한 RISC-V ISA 는 x86, Arm 과 다르게 Free Open-source 라는 장점으로 인해 많은 연구와 개발이 이루어지고 있다. RISC-V ISA 는 RISC 명령어셋을 활용하며 서버 및 데스트탑 CPU 부터 IoT 디바이스까지 여러 방면에서 상용을 위한 노력이 계속되고 있다. 하지만 상용 CPU 에 비해 부채널 공격 방어 기법이 제한적으로 구현되어 있는 것을 확인하였고 특히 부채널 공격 중 전력 분석(Power Analysis)에 대한 방어 기법이 부족한 것을 확인하였다. 따라서 본 논문에서는 RISC-V 를 포함한 여러 아키텍처에 대해 전력 분석 및 하드웨어 방어 기법을 분석하고, RISC-V 에 추가적으로 적용되어야 할 방어 기법에 대해 서술한다.

1. 서론

RISC-V 는 2010 년 UC Berkley 에서 제시한 Free Open-source ISA 로 단순히 학술 및 연구용이 아닌 상용화를 목표로 개발을 진행하고 있다. Arm 아키텍처의 지속적인 개런티 지불과 응용, 변경이 어렵다는 단점에 반해, RISC-V 는 최신 버전을 무료로 즉시 다운로드 및 사용할 수 있고 용도와 상황에 따른 변경이 용이하다는 장점이 있다. 그로 인해 Google 은 RISC-V Summit 에서 RISC-V 에 대한 안드로이드 지원을 발표하였고, Apple 은 자사 제품 내 RISC-V embedded core 의 비중을 늘리고 있으며 RISC-V High performance Programmer 를 채용하고 있다. 이처럼 산업계에서 RISC-V 아키텍처를 적용하려는 움직임이 늘고 있다.

하지만 RISC-V 의 특성 상 작업이 진행될수록 파편화가 심해지고, 이를 완화하기 위해 몇 가지 확장을 묶는 표준화 작업을 진행하였으나 개발되는 코어 별로 적용되는 보안 기능이 상이하다는 한계점이 있다. 일부 보안 확장이 적용되어 있는 CV32e40s, Ibex core 조차 특정 부채널 공격에 대한 방어 기법이 부족한 것을 확인하였다.

따라서 본 논문에서는 RISC-V 및 여러 아키텍처에서 이루어진 부채널 공격 중 전력 분석 공격 및 하드웨어 기반 방어 기법 연구를 분석하고, 향후 개발되는 RISC-V 아키텍처에 적용되어야 할 전력 분석 방어 기법에 대해 서술한다.

섹션 2,3 에서는 부채널 공격과 전력 분석의 종류, 그에 대한 방어기법에 대해서 설명한다. 섹션 4 에서 분석한 RISC-V 코어에 대해 정리하고, 마지막으로 섹션 5 에서 추후 적용되어야할 전력 분석 방어 기법에 대하여 서술한다.

2. 부채널 공격

부채널 공격이란 암호 알고리즘에 대해 소프트웨어적으로 시스템의 취약점을 공격하는 것이 아닌, 물리적인 정보를 기반으로 암호를 유추하는 공격 기법이다. 부채널 공격의 목표는 얻어진 정보를 기반으로 비밀 키를 복원하거나 개인 정보를 탈취하는 것이며, 한 번 혹은 여러 번의 실행을 통해 관련 정보를 추출하여 공격을 진행한다.

공격 방식으로는 각 instruction 의 입력 값에 대한 실행 시간 차이를 측정하여 암호를 유추하는 timing

attack[1], 암호 알고리즘 실행 과정에서 소모되는 전력을 기반으로 비교 및 추가 연산을 진행하여 암호를 유추하는 power analysis[2][3][4], 장비 실행 시 발생하는 전자파를 분석하여 출력값을 유추하는 EM attack[5], 추측 실행(speculative execution)을 기반으로 데이터 접근 시간을 측정하여 접근 불가능한 영역(커널, 다른 프로세스)의 정보를 추출하는 Cache Side-channel Attack[6][7] 등이 있다.

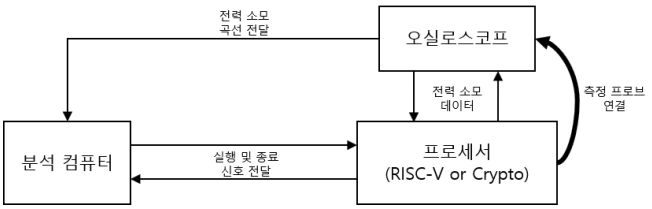

그림 1 전력 분석 환경 구성

2-1. 전력 분석 (Power Analysis)

전력 분석은 부채널 공격 기법 중 하나로 알고리즘 실행 과정에서 특정 연산 수행 시 소모되는 전력을 측정하고 측정값을 기반으로 분석을 통해 연산에 사용된 값을 유추한다. CMOS 기반 회로는 CMOS 특성상 0 을 나타낼 때와 1 을 나타낼 때의 전력 소모 값이 다르기 때문에 특정 연산을 진행함에 있어 전력 분석을 통해 그 차이를 확인할 수 있고, 여러 번의 수행으로 평균 값을 구하는 것도 가능하다.

분석 환경은 그림 1 과 같이 구성하며, 분석 컴퓨터에서 실행 신호를 전달하면 프로세서에서 관련 프로그램 실행과 동시에 오실로스코프에서는 전력 측정을 진행한다. 측정 종료 시 오실로스코프에서 전력 소모 곡선을 분석 컴퓨터로 가져와 전력 분석을 진행하게 된다.

Simple Power Analysis (SPA). 실행 1 회에 대한 전력 소모 곡선을 분석하여 암호 알고리즘의 비밀 키를 유추하는 방식으로, 각 instruction 이 0 또는 1 에 대해 연산이 달라짐에 따라 명확한 전력 소모의 차이가 있을 때 전력 곡선상의 전력 소모 값을 기반으로 비밀키를 복원한다. [2]에서는 RSA 의 비밀키가 1 일 때 곱셈을 진행한 후 해당 값을 제곱하는 성질을 이용하여 FPGA 에 구현된 4 개의 RSA processor 에 대해 SPA attack 을 진행하였고, 그 결과 성공적으로 1024-bit 비밀키를 복원하였다.

Differential Power Analysis (DPA). 여러 번의 실행을 통해 전력 곡선들의 평균값을 구한 후 각 키들의 값을 측정한 곡선들과 비교해 올바른 비밀키를 유추하는 공격 기법이다. 특정 연산의 입력 데이터를 유추하는데 효과적이고 필요한 연산 수가 적어 빠르게 진행할 수 있다. 하지만 많은 전력 곡선이 필요하고 공격 대상에 따라 성공률의 차이가 나기 때문에 적합한 대상을 선정하는 것이 중요하다. [6]에서는 DES 에 대한 DPA attack 을 진행하였으며, 올바른 키 값을 유추했을 때 하나의 peak 가 생성된다는 것을 보였다. 이를 기반으로 대부분의 smart card 에 대해 15 번 가량의 trace 를 추출하면 key 를 추출할 수 있다고 언급하고 있다.

Correlation Power Analysis (CPA). 여러 번의 실행 후 전력 곡선의 각 포인트에 대한 상관분석을 진행하여 비밀키를 추출하는 공격 기법이다. 특정 연산의 출력 데이터를 추출하는데 효과적이고 공격 성공률이 높지만, 곡선의 모든 포인트에 대해 상관 분석을 진행하기 때문에 연산이 많고 오래 걸린다는 단점이 있다. [7]에서는 8-bit chip 에 구현되어 있는 XOR 알고리즘을 대상으로 공격을 진행하였고, 입력값을 0 부터 255 까지 모두 실행하며 전력 곡선을 추출하고 이를 기반으로 8byte 의 key 를 복원하는 작업을 진행하였다.

3. 전력 분석에 대한 방어 기법

[8]에서는 first-order power or electromagnetic attack 을 방어하기 위해 memory 주소와 4 개의 seed 값을 기반으로 필요 시 mask share 를 생성하여 memory 에 write 할 때 masking 하고, read 할 때 제거하는 기법을 적용하였다. 그 후 t-test[9] 기법을 통해 공격에 대한 안전성을 확인하였다. t-test 는 통계적으로 독립된 두 집단의 평균의 차이가 있는 지 확인하는 방법으로, 특정 값이 평균을 벗어나는 peak 가 존재한다면 t-test 를 통과하지 못하였다는 것을 의미하고, 해당 peak 를 기반으로 유의미한 정보를 추출하여 공격을 진행할 수 있다. [10]에서는 ISE(Instruction Set Extention)를 통해 새로운 instruction ‘custom-0’을 생성하였다. Processor 는 이 instruction 을 통해 dummy instruction 의 빈도수, 동작, 사용할 register 등을 설정하고 빈도수만큼 dummy instruction 을 생성, 삽입하게 된다. 삽입된 dummy instruction 은 DPA 분석 과정에서 전력 곡선의 alignment 를 방해하게 되고, 그로 인해 적합한 입력을 찾을 수 없게 한다. 안전성 검증은 t-test 를 통해 진행하였고, peak 를 확인할 수 없었다. [11]에서는 compile-time 에 basic block 을 분석하고, shuffle 이 가능한 n 개의 instruction 을 묶어서 m 개의 block 을 만든 후 shuffle(m,n) instruction 을 삽입하여 run-time 에 하드웨어적으로 shuffle 을 진행하도록 하였다. Shuffle instruction 을 확인하면, TRNG 를 통해 Random permutation 을 진행하게 되고, block 의 순서가 random 하게 바뀌어 전력 추출 과정에서 일정하지 않은 전력 곡선을 얻게 된다. 그렇기 때문에 DPA 와 CPA 를 진행하였고, peak 가 등장하지 않는 것으로 연구의 안전성을 검증하였다. [12]에서는 Memory bus 와 register data 가 변경될 때 전력 소모 값이 변하는 transition effect 를 기반으로 power analysis 를 진행하는 Hamming distance leakage model 에 대해 비밀 키에 대한 정보가 유출되지 않도록 비밀 키가 사용되는 instruction 의 순서를 compile time 에 변경하여 실행하는 방법을 제시하였고, [13]은 [14]의 ELMO 라는 tool 을 사용하여 simulation-based leakage analysis 를 진행한 후 compile-time 에 해당 leakage 를 constraint 에 기반하여 수정하는 방식으로 transition effect 를 제거하는 연

구를 진행하였다. 최종적으로 변경된 암호 알고리즘은 t-test 의 threshold 인 ±4.5 를 넘지 않는 것을 확인하였다.

4. RISC-V Core 분석

RISC-V 코어를 분석하기 이전에, 일부 프로세서에 보안 기능이 추가된 것을 확인하였고, 그 중 verification 이 가능한 코어를 선별하여 CV32e40s 와 Ibex 를 대상으로 부채널 공격에 대한 방어 기법을 조사하였다.

CV32e40s 32-bit 4-stage pipelined RISC-V 코어로, CV32e40 시리즈 중 Xsecure extension 이 적용된 모델이다. In-order processor 로 Branch predictor 와 speculative execution 등이 존재하지 않는 저성능 디바이스이나, Xsecure extension 이 적용되어 일부 하드웨어 보안 기능을 사용할 수 있다. 이 확장에 포함된 전력 분석 관련 방어 기법은 Dummy instruction insertion, Data independent timing 이고, 해당 기능은 특정 register 를 통해 on-off 할 수 있다.

Ibex 32-bit 2-stage pipelined RISC-V 코어로, 4 단계로 verification 이 가능하며, 초저전력 저성능 디바이스를 대상으로 개발되었다. CV32e40s 와 마찬가지로 전력 분석 관련 방어 기법은 Dummy instruction insertion, Data independent timing 이며, 'cpuctrl' register 를 통해 on-off 가 가능하다.

	CV32e40s	Ibex
Dummy instruction insertion	O	O
Data independent timing	O	O
Polarity	X	X
Masking	X	X

표 1 코어 별 보안 적용 사항

5. 결론

상용 CPU 의 경우 여러 공격에 대한 방어 기법을 모두 적용시킨 후 사용자가 일부 방어 기법을 on-off 할 수 있도록 설정하는 것이 일반적이다. 예를 들어, register data 와 memory bus 를 polarity 와 masking 으로 보호하고, Dummy instruction 기능을 활성화하여 추가적인 방어 수단을 적용하는 것이다. 하지만 RISC-V 의 경우 파편화로 인해 많은 종류의 코어에 표준적인 보안 기능이 정의되어 있지 않고, 일부 기능이 구현되어 있는 CV32e40s, Ibex 코어 또한 표 1 과 같이 Register data 나 memory bus 의 값이 변하면서 발생하는 transition effect 를 막을 수 있는 기본적인 Polarity 나 Masking 기법이 존재하지 않았다. 따라서 leakage 기반의 전력 분석 공격을 막기 위한 두 방법이 우선적으로 적용되어야 하며, 효과적인 하드웨어 기반 방어 기능이 연구되지 않은 것으로 조사되어 이에 대한 연구 및 개발 또한 진행되어야 할 것이다.

ACKNOWLEDGEMENT

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며 (IITP-2023-RS-2023-00256081), 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며 (RS-2023-00277326), 반도체 공동연구소 지원의 결과물이며, 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음.

참고문헌

[1] Kocher, P.C, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology — CRYPTO '96, Santa Barbara, California, USA. 1996. pp.104-113.

[2] Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki and Akashi Satoh, "Chosen-message SPA attacks against FPGA-based RSA hardware implementations," 2008 International Conference on Field Programmable Logic and Applications, Heidelberg, Germany, 2008, pp.35-40.

[3] Kocher, P., Jaffe, J., Jun, B. "Differential Power Analysis," Advances in Cryptology — CRYPTO' 99, Santa Barbara, California, USA, 1999, pp.388-397.

[4] Brier, E., Clavier, C., Olivier, "Correlation Power Analysis with a Leakage Model," Cryptographic Hardware and Embedded Systems - CHES 2004, Cambridge, MA, USA, 2004, pp.16-29.

[5] Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P., "The EM Side—Channel(s)," Cryptographic Hardware and Embedded Systems - CHES 2002, Redwood Shores, CA, USA, 2002, pp.29-45.

[6] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg, "Meltdown: Reading Kernel Memory from User Space," 27th USENIX Security Symposium (USENIX Security 18),Baltimore, MD, USA, 2018, pp.973-990.

[7] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre attacks: exploiting speculative execution." Commun. ACM 63, 7 (July 2020), pp.93–101, 2020.

[8] Elke De Mulder, Samatha Gummalla, and Michael Hutter, "Protecting RISC-V against Side-Channel Attacks," In Proceedings of the 56th Annual Design Automation Conference 2019 (DAC '19), New York, NY, USA, 2019, Article 45, pp.1-4.

[9] Standaert, FX, "How (Not) to Use Welch's T-Test in Side-Channel Security Evaluations," Smart Card Research and Advanced Applications (CARDIS 2018), 2019, pp.65-79.

[10] T. H. Pham, B. Marshall, A. Fell, S. -K. Lam and D. Page, "XDIVINSA: eXtended DIVersifying INStruction Agent to Mitigate Power Side-Channel Leakage," 2021 IEEE 32nd International Conference on Application-specific Systems, Architectures and Processors (ASAP),

NJ, USA, 2021, pp. 179-186.

[11] Ali Galip Bayrak, Nikola Velickovic, Paolo Ienne, and Wayne Burleson, “An architecture-independent instruction shuffler to protect against side-channel attacks,” ACM Trans. Archit. Code Optim. 8, 4, Article 20, pp.1-19, January 2012.

[12] R. M. Tsoupidi, R. C. Lozano, E. Troubitsyna and P. Papadimitratos, "Securing Optimized Code Against Power Side Channels," 2023 IEEE 36th Computer Security Foundations Symposium (CSF), Dubrovnik, Croatia, 2023, pp. 340-355.

[13] Madura A Shelton, Niels Samwel, Lejla Batina, Francesco Regazzoni, Markus Wagner, Yuval Yarom, “ROSITA: Towards Automatic Elimination of Power-Analysis Leakage in Ciphers,” Network and Distributed System Security Symposium (NDSS), 2021

[14] D. McCann, E. Oswald, and C. Whitnall, “Towards practical tools for side channel aware software engineering: ‘grey box’ modelling for instruction leakages,”, USENIX Security, 2017, pp. 199–216.