ARM 신뢰 실행 환경에서 SIMD를 활용한 Kyber KEM 타이밍 기반 부채널 공격 억제

정세현 [1], 오현영 [2*]
[1] 가천대학교 AI · 소프트웨어학부 학부생
[2] 가천대학교 AI · 소프트웨어학부 교수
jjsshh3116@ gachon.ac.kr, hyoh@ gachon.ac.kr

Mitigating Kyber KEM Timing-Based Side-Channel Attacks Using SIMD in ARM Trusted Execution Environment

Se-Hyeon Jeong, Hyunyoung Oh
Dept. of AI·Software, Gachon University

요 약

본 논문은 Kyber 알고리즘의 타이밍 기반 부채널 공격 취약점을 분석하고, 이를 완화하기 위해 Secure World 내에서 SIMD 병렬 처리를 적용한 방어 기법을 제안한다. 제안 기법은 민감한 t 값에 따른 연산 시간의 편차를 기존 Kyber 대비 약 17.93% 더 적은 표준편차가 측정되어 타이밍 정보 유출을 어렵게 만들며, Raspberry pi 3B 환경에서 약 7.18%의 성능 향상을 확인하였다.

1. 서론 및 배경

사물인터넷(IoT)의 발전으로 많은 디바이스에서 다양한 서비스 요청을 송수신하며 사용자에게 편리한 기능을 제공하고 있다. 이러한 디바이스의 확산은 공격자가 노릴 수 있는 공격 표면(Attack Surface)을 급격히 증가시키며, 이에 따라 임베디드 장치의 보안 문제를 해결하기 위한 암호 기법들이 연구되었다[1].

그러나 소인수분해나 이산로그와 같은 수학적 난제를 기반으로한 현대 암호학 체계는 양자 컴퓨터 원리를 이용한 쇼어 알고리즘(Shor's Algorithm)으로 쉽게 깨진다[2]. 이러한 위협에 대응하기 위해 양자 내성 암호(Post-Quantum Cryptography, PQC)가 새롭게 대두되고 있다. 다양한 PQC 알고리즘 중 격자 기반 암호(Lattice-Based Cryptography)인 Kyber[3] 키 캡슐화 방식(Key Encapsulation Mechanism, KEM)은 수행 시간, 메모리 사용량, 에너지 소모 측면에서 IoT 디바이스와 같은 자원 제약적 환경에 사용하기 적절하다[4].

위와 같은 키 캡슐화 암호를 사용해도 기밀성과 무결성 문제가 여전히 남아있다. 이를 보완하기 임베디드 시스템에 널리 사용되는 보안 기술인 ARM TrustZone 을 활용하는 연구가 진행되었다[5]. 하지만 이 기술에는 부채널 공격(Side-Channel Attack) 취약점이 존재하며, 특정 값에 따라 나눗셈 연산 수행 시간이 변화는 특성을 이용한 타이밍 기반 부채널 공격으로 Kyber 의 비밀 키 값이 유출되었다[6].

타이밍 기반 부채널 공격을 억제하기 위해 입력 값에 따라 연산 수행 시간이 변화는 명령어를 상수 시간 명령어로 변환하는 기법이나 잡음 주입(Noise Injection) 방식이 제안되었다[7]. 그러나 이러한 방식은 기존 연산보다 성능이 저하되는 단점이 있다.

본 연구는 TrustZone 을 이용해 Kyber KEM 알고리즘의 기밀성과 무결성을 달성하고 SIMD 를 활용해 타이밍 기반 부채널 공격을 억제하는 방법을 제안한다.

2. 타이밍 기반 부채널 공격 방법

Kyber KEM 의 공유 비밀 키 복호화 과정은 송신자로부터 수신한 암호문과 수신자가 보유한 비밀 키를 이용하여 공유 비밀 키를 재구성한다. 이때 복호화 연산은 다항식 기반의 연산으로 수행된다. 선행 연구에서는 특정 값에 따라 나눗셈 연산 시간의 차이를 분명하게 만들기 위해 강제로 마지막 항 계수만 208 로 고정하고, 나머지 차항의 계수는 2081 로 설정하여 실험 환경을 구성했다[6] .

```
t = (((t << 1) + KYBER_Q / 2) / KYBER_Q) & 1;
```

(그림 1) 타이밍 공격에 취약한 기존 kyber 코드

(그림 1)은 Kyber 복호화 과정에서 사용되는 핵심 연산으로, 비밀 값 t 의 값에 따라 연산 수행 시간이 변한다. 공격자는 이 연산에 입력되는 t 값을 제어함으로써 연산 시간이 어떻게 변화하는지를 측정하고, 이를 통해 공유 비밀 키의 값을 역추론할 수 있다.

공격자는 특정 입력 값의 연산 속도를 정밀하게 관측하고, 해당 속도에 대응하는 t 값을 사전 테이블과 비교하여 전체 공유 비밀 키를 순차적으로 유추할 수 있다.

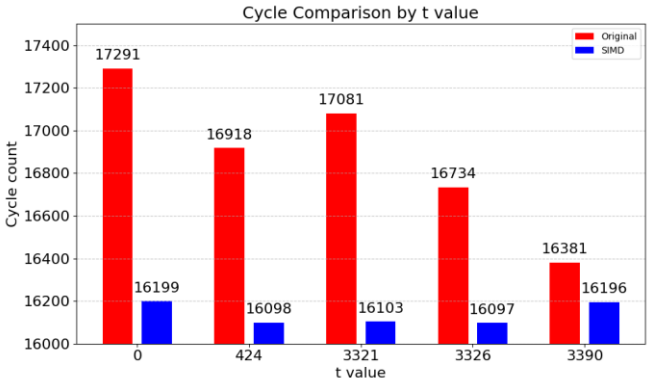
* 교신저자

3. SIMD 기반 타이밍 완화 기법

제안하는 방어 기법은 Secure World 내에서 128-bit SIMD 레지스터를 활용하여, 복호화 연산에 사용되는 다수의 t 값을 병렬로 처리하는 구조를 따른다. 타이밍 공격에 취약한 기존 코드를 vshlq_n_s16, vaddq_s16, vdivq_f32_s32, vdupq_n_s16 등의 SIMD 명령어 조합을 활용해 재구현하였다. SIMD 기반 병렬 연산은 입력 값 간의 타이밍 편차를 평균화시키는 효과를 가지며, 결과적으로 t 값의 변화가 전체 연산 시간에 미치는 영향을 완화한다. 이는 타이밍 기반 부채널 공격의 민감도를 저하시켜, 공격의 정밀도 및 성공 가능성을 낮춘다.

4. 실험 및 평가

실험 환경은 Raspberry pi 3B 보드에 OP-TEE(v4.5.0) 운영체제를 사용했으며 Kyber-1024 을 기준으로 성능을 측정했다. 또한 Daniel J. et al[6].에서 설정한 컴파일 최적화 플래그와 다항식 계수를 동일하게 사용하였다.



(그림 2) 특정 t 값에 따른 CPU Cycle 지표

빨간색 바는 기존 Kyber 연산, 파란색 바는 SIMD 를 적용한 코드의 특정 t 값(0, 424, 3321, 3326, 3390)에 따른 CPU Cycle 을 의미하며, 100 번 실행해 평균값을 구한 지표이다. 기존 방식은 최대 910 Cycle 부터 최소 163 Cycle 의 차이를 보이지만, SIMD 를 적용한 경우 최대 102 Cycle 차이를 보인다. 이는 기존 방식의 최소 Cycle 차이보다 더 적은 수치를 달성했다. 또한 약 6.33%의 성능 향상도 관찰되었다. 따라서 특정 값에 따라 시간이 변화는 연산에 SIMD 를 적용하면 시간 변화의 민감도를 크게 낮출 수 있어 타이밍 기반 부채널 공격을 억제할 수 있다.

<표 1> 전체 t 값에 따른 Kyber Cycle 통계

	Original Kyber	SIMD Kyber	Improvement
Average	16560.28 cycle	16112.83 cycle	2.7%
Standard Deviation	84.92 cycle	69.7 cycle	17.93%
Min Value	16281.82 cycle	16000.04 cycle	-
Max Value	17340.67 cycle	16890.62 cycle	-
Cycle range	1058.85 cycle	890.58 cycle	15.91%

암호 키 복호화 과정에서 비밀 값 t 값의 따른 cycle 통계를 계산한 결과이며, 100 회 실행해 구한 지표이다. SIMD 를 적용한 Kyber 에서 약 69.7 cycle 의 표준 분포 값이 측정되었으며, 기존 Kyber 대비 약 17.93% 더 적은 표준편차가 측정되었다. 또한 기존 Kyber 에서 t 값에 따라 관측된 값의 범위는 1056.85 cycle 이며, SIMD 를 적용하면 분포 범위가 약 15.91% 좁아졌다.

<표 2> OP-TEE 에서 Kyber 실행 시간 측정 표

	시간
Normal World	2.02 ms
Secure World	2.62 ms
SW + SIMD	2.43 ms

OP-TEE 에서 일반 환경과 보안 환경에서 Kyber KEM 알고리즘 수행 시간 측정을 진행하였다. Secure World 특성상 Normal World 보다 코드 수행 시간이 느리기 때문에 Secure World 에서 약 29.7%의 성능 저하를 보인다. 또한 타이밍 기반 부채널 공격을 억제하기 위해 SIMD 를 적용한 Kyber 은 Secure World 에서 실행된 기존 Kyber 대비 약 7.16%의 성능 향상을 보인다. 그러나 여전히 Normal World 에서 실행된 Kyber 보다 느린 성능을 보인다. SIMD 레지스터에 데이터를 로드하는 과정과, 정수형 데이터에 대해 SIMD 명령어가 나눗셈 연산을 직접 지원하지 않기 때문에 실수형으로 변환하여 연산을 수행한 후 다시 정수형으로 변환하는 과정에서 추가적인 오버헤드가 발생한다. 이러한 이유로 기대했던 만큼의 성능 향상이 나타나지 않은 것으로 분석된다. 하지만 그 성능의 차이가 미미하며, Secure World 에서 실행함으로써 얻을 수 있는 보안적 이점이 크기 때문에 Kyber 를 해당 환경에서 사용하는 것은 충분히 타당하다.

5. 결론

특정 값에 따라 연산 수행 시간이 달라지는 특성을 이용해 비밀 값을 유추할 수 있는 타이밍 기반 부채널 공격은 SIMD 를 활용한 병렬 연산 처리를 통해 타이밍 편차를 줄임으로써 그 효과를 저하시킬 수 있다. 또한, 병렬 처리 방식은 일정 수준의 성능 향상도 함께 제공하며, TrustZone 과 결합할 경우 기밀성과 무결성을 동시에 보장할 수 있기 때문에, Kyber 을 Secure World 내에서 실행하는 것은 충분히 실용적이다.

사사문구

이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (No. RS-2024-00337414, SW 공급망 운영환경에서 역공학 한계를 넘어서는 자동화된 마이크로 보안 패치 기술 개발).

참고문헌

[1] Dhanda, et al., "Lightweight cryptography: a solution to secure IoT.", Wireless Personal Communications 112.3, 2020, 1947-1980.
[2] Ugwuishiwu, C. H., et al., "An overview of quantum cryptography and shor's algorithm.", Int. J. Adv. Trends Comput. Sci. Eng 9.5, 2020.
[3] CRYSTALS-Kyber. (n.d.). CRYSTALS-Kyber: Post-Quantum Cryptography. Retrieved April 8, 2025, from https://pq-crystals.org/kyber/.
[4] Halak, Basel, et al., "Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices.", IEEE Access 12, 2024, 8791-8805.
[5] Andrade, Ewerton et al., "Post-Quantum Algorithms on ARM Trusted Execution Environment (TEE): findings of this industrial challenge.", Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing, 2024.
[6] Bernstein, Daniel J. et al., "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations.", Cryptology ePrint Archive, 2024.
[7] Zhang, Jiliang, et al., "Timing side-channel attacks and countermeasures in CPU microarchitectures.", ACM Computing Surveys 56.7, 2024, 1-40.