8-bit 구현 Ring-LWE 암호화에서 단순전력분석 대응방안

Countermeasure of Simple Power Analysis in Ring-LWE Implementation on 8-bit Microcontroller

문 재 근, 정 임 영
경북대학교 전자공학부

Jaegeun Moon, Im Y. Jung
School of Electronics Engineering, Kyungpook National University

요약

이 논문에서는 8bit 마이크로컨트롤러 상에서 덧셈 연산을 이용한 공격을 방어하는 알고리즘을 제시한다.

1. 서론

암호는 통신을 통해 송·수신하는 데이터를 원하지 않는 상대로부터 지키기 위해 설계되었다. 특히 IoT 시대가 되어 기기들을 통해 많은 정보들이 전송하게 되어 암호의 중요성은 더욱 증가하였다.

양자 컴퓨터 이론이 등장함에 따라 양자 컴퓨터의 등장에도 안전한 post-quantum 암호에 관한 연구가 진행되고 있다.

Post-quantum 암호 연구의 일환으로 Lattice를 기반으로 한 암호에 관한 연구가 진행되고 있다. Lattice 중 현재 활발히 연구가 진행되고 있는 대상으로는 Learning with Error (LWE)가 있다[1].

그럼에도 불구하고 LWE를 실제 구현하면 자원소모가 심해 실질적인 암호로 사용하기 힘들다는 지적이 있었다. 이를 개선하기 위해 LWE의 변형인 Ring-LWE가 제안되었다[2].

그러나 암호는 수학적 안전성을 기반으로 설계되었음에도 불구하고 컴퓨터 등의 전자 기기들에 구현이 되는 과정에서 생각지 못한 정보 유출 가능성이 생기게 된다. 이를 이용한 공격이 부채널 공격이다[3].

단순전력분석를 통해 8-bit 마이크로콘트롤러에서 구현된 Ring-LWE를 공격하는 방법이 제시되었으나 아직까지 그 대응방안은 제시되지 않았다.

2. 관련 연구

이 연구는 modulo 연산에서 reduction이 일어날 때와 일어나지 않을 때의 차이로 인해 두 경우가 구분이 가능한 것이 밝혀졌다[4].

알고리즘 1: Ring-LWE 암호화의 덧셈과 modulo 연산 ($x \in Z_q^n$, $y \in Z_q^n$)

```
result ← x + y
if result 〉 q
    result ← result - q
end
return result
```

알고리즘 1에서 알 수 있듯이 피제수가 제수보다 크게 되면 뺄셈을 연산하고 그렇지 않으면 아무런 연산을 하지 않는다. 이로 인해 두 경우 사이에 연산 시간이 차이가 발생하여 구분 가능하다.

3. 제안 알고리즘

단순전력분석에 대해 안전하기 위해서는 항상 일정한 흐름으로 진행되어야 한다. 따라서 본 논문은 피제수의 값에 상관없이 항상 일정한 흐름을 갖는 알고리즘을 제안한다.

알고리즘 2: q = 7681일 때 제안 알고리즘 ($x \in Z_q^n$, $y \in Z_q^n$)

```
result ← x + y
q ← 7681
temp ← result
for i ← 1 to 8 do
        temp ← temp | result 〉〉 i
end
for i ← 9 to 12 do
        temp ← temp & result 〉〉 i
```

```
end
temp ← temp | result >> 13
temp ← temp & 0x01
temp ← temp * q
result ← result - temp
return result
```

4. 평가

modulo 연산 과정에서 분기점이 없기 때문에 어느 경우에도 같은 흐름을 수행하게 된다는 것을 알 수 있다.

그러나 알고리즘 1을 수행하면 q = 7681 기준으로 최소 7 cycle, 최대 8 cycle 만에 연산이 끝나지만 제안한 알고리즘은 35 cycle이 소요된다.

5. 결론

이 논문은 8-bit Ring-LWE 암호화에서 단순전력분석의 대응방안을 제시하였다. 제시한 방안은 항상 일정한 흐름을 가지기 때문에 단순전력분석으로부터 안전할 수 있다. 그러나 기존의 알고리즘에 비해 상당한 성능 저하를 야기할 것으로 보인다.

따라서 이 알고리즘을 경량화하는 연구가 추가로 필요하다.

▌참 고 문 헌▐

[1] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography." Journal of the ACM (JACM), Vol. 56, Issue 6, No. 34, 2009.

[2] V. Lyubashevsky, C. Peikert and O. Regev, "On ideal lattices and learning with errors over rings." Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 1 - 23, 2010.

[3] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." Advances in Cryptology—CRYPTO'96, Springer Berlin/Heidelberg, pp. 104 – 113, 1996.

[4] A. Park, D. G. Han, "Chosen ciphertext Simple Power Analysis on software 8-bit implementation of ring-LWE encryption." In Hardware-Oriented Security and Trust (AsianHOST), IEEE Asian, pp. 1 - 6, 2016.