OQS 프로젝트 중 격자 기반 키 교환 방식의 타이밍 등 공격 분석1)

안형철* 한성호* 최낙준* 김광조*

*카이스트 정보보호대학원

Timing and Fault Attacks on Lattice-based Key Exchange Protocols in Open Quantum Safe Project

Hyeongcheol An* Seongho Han* Nakjun Choi* Kwangjo Kim**

*Graduate School of Information Security, KAIST.

요 약

Open Quantum Safe(OQS)는 현재 Stebila 등에 의하여 포스트 양자 암호(Post Quantum Cryptography)의 키 교환 프로토콜을 OpenSSL에 결합하는 오픈소스 프로젝트로 그 중 래티스(lattice) 기반 키 교환 프로토콜은 총 5 가지의 Frodo, Kyber, BCNS, MSrln, NewHope가 있다. 본 논문에서는 OQS의 래티스 기반 키 교환 프로토콜을 구현 SW상에서 검증이 용이한 타이밍공격(timing attack)과 오류 주입공격(fault attack)의 부채널공격 관점에서 안전성을 검증하고 이러한 부채널공격에 대하여 안전하게 구현할 수 있는 방법을 제시한다.

I. 서론

현재 키 교환 과정에서 널리 사용하고 있는 DH(Diffie-Hellman), ECDH(Elliptic Curve Diffie-Hellman) 키 교환 프로토콜은 이산 대수 문제 및 소인수 분해 문제의 어려움에 기반하기 때문에 Shor 알고리즘[1]에 따라 양자컴퓨터의 공격에 다항식 시간에 해독이 가능하다. 이에 NIST는 2017년 11월까지 양자 컴퓨터를 이용한 공격에도 안전한 포스트 양자 암호(Post Quantum Cryptography, PQC)를 공모하고 있으며, 그 중 이미 래티스(lattice) 기반 암호 프리미티브가 많이 있다.

1) 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)과 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01006812)

본 논문에서는 Open Quantum Safe(OQS)[3, 4] 프로젝트에 대하여 설명하고 구현 SW 상에서 검증이 용이한 타이밍공격(timing attack)과 오류 주입공격(fault attack) 관점에서 분석하고자 한다. OQS 프로젝트에서 래티스 기반 키 교환 프로토콜은 총 5 종류인 Frodo[5], Kyber[6], BCNS[7], MSrln[8], NewHope[9]가 있으며 각각에 대하여 부채널 공격 여부와 개선책을 논의하고 한다.

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 널리 알려진 LWE(Learning-with-Errors), Ring-LWE, Module-LWE 문제에 대하여 간략히 설명하고, Ⅲ장은 OQS 프로젝트에 대하여 소개하고, Ⅳ장에서는 OQS 프로젝트 중 5개의 래티스 기반 키 교환 프로토콜에 대한 타이밍공격 및 오류주입공격과 개선책에 대하여 논하고, Ⅴ장에서는 결론과 본 논문 성과를 확장하여 메모리 취약점을 통한 부채널공격에 대한 가능성을 제시한다.

II. 배경지식

2.1 LWE 문제

LWE는 기계학습에서 시작된 문제로, 패리티(parity) 학습 문제의 일반화된 형태이다. LWE는 평균적인 래티스 문제가 가장 최악의 경우(worst case)만큼 어렵기 때문에 공개키 암호 등의 설계에 많이 사용된다. LWE 분포 $A_{s,\chi}$는 벡터 $s \in Z_q^n$이 주어졌을 때, 임의의 $a \in Z_q^n$를 균일하게 선택하고 에러 e는 분포 χ에서 추출하고, $(a, b = < s, a > + e \bmod q)$를 계산한다. 래티스 기반 암호에서 주로 쓰이는 결정문제(decision problem)는 $A_{s,\chi}$로부터 선택한 m개의 주어진 샘플 (a_i, b_i)과 $Z_q^n \times Z_q$로부터 선택한 m개의 임의의 샘플 (a_i, b_i)간에 구별이 어려움을 이용한다.

2.2 Ring-LWE 문제

Ring-LWE는 LWE 문제를 유한체(finite field) 상의 다항식 환(ring) 위에서 정의한 문제이다. Ring-LWE 문제의 해는 래티스의 NP-Hard 문제인 SVP(Shortest Vector Problem)으로 환원 될 수 있다. Ring-LWE 분포 $A_{s,\chi}$는 $s \in Z_q^n$이 주어져 있을 때, 임의의 $a \in Z_q^n$를 균일하게 선택한다. 에러 e를 분포 χ에서 추출하고, $Z_q[x]/\Phi(x)$ 위에서 $(a_i, b_i = a_i(x)s(x) + e_i(x))$ 계산한다. Ring-LWE의 결정문제는 $A_{s,\chi}$로부터 선택한 m개의 독립 샘플 (a_i, b_i)과 $Z_q[x]/\Phi(x)$로부터 임의의 m개의 샘플 (a_i, b_i)을 구별하는 것이다.

2.3 Module-LWE 문제

Module-LWE[10]는 LWE와 Ring-LWE를 일반화한 것이다. LWE 분포에서 a_i는 $(Z_q[x]/\Phi(x))^k$로부터 균일하게 추출하고, s는 β_η^k로부터 추출한다. e_i는 β_η로부터 새롭게 추출한다. 여기서 β_η는 이항분포이다. 결정문제는 $A_{s,\chi}$로부터 선택한 m개의 독립 샘플 (a_i, b_i)과 $(Z_q[x]/\Phi(x))^k \times \beta_\eta$로부터 임의의 m개의 샘플 (a_i, b_i)을 구별하는 것이다.

III. Open Quantum Safe 프로젝트

OQS는 포스트 양자 암호 중 키 교환 프로토콜에 대하여 오픈소스로 진행하고 있는 프로젝트이다. 현재 Stebila 등에 의하여 OpenSSL에 PQC 프로토콜을 추가할 예정이다. OQS 프로젝트에 총 9 종류의 키 교환 프로토콜이 있으며, 이 중 코드 기반 1 종류, 래티스 기반 5 종류, SIDH (Supersingular Isogeny Diffie-Hellman) 기반 2 종류, NTRU로 구성되어 있다. 본 논문에서는 5 종류의 래티스 기반 키 교환 프로토콜에 대하여 분석하였다.

3.1 Frodo[5]

Frodo는 Bos 등이 설계하고 구현한 프로토콜로 LWE 문제를 기반으로 설계하였다. 파라미터는 $n = 752$, $q = 2^{15}$이다. 타 프로토콜과 비교하여 NTT(Number Theoretic Transform)나 FFT(Fast Fourier Transform)를 쓰지 않은 것이 특징이다.

3.2 BCNS[6]

Bos 등에 의해 2015년 발표된 프로토콜로 Ring-LWE 문제를 기반으로 한다. 파라미터 $q = 2^{32} - 1$로 비교적 큰 편이다. 연산과정에서 FFT 알고리즘을 사용한다.

3.3 NewHope[7]

NewHope 프로토콜은 Alkim 등에 의해 BCNS 프로토콜의 단점을 보완하여 설계 및 구현하였다. $n = 1024$, $q = 12289 < 2^{14}$까지 파라미터의 크기를 줄인 것이 특징이다. NTT 연산에서 AVX2(Advanced Vector Extensions)을 사용하기 때문에 프로토콜의 속도가 증가하였다. NewHope 프로토콜에서는 BCNS의 에러 샘플링 분포를 이산 가우시안 분포에서 이항분포로 변경하였다.

3.4 MSrln[8]

Longa 등에 의해 제안된 Ring-LWE 기반 프로토콜이며, NTT 연산을 사용하여 연산속도가 증가하였다. 또한 새로운 모듈러 감쇄 알고리즘을 제안하였다. 수정된 NTT 알고리즘은 전체적

[표 1] OQS 오픈소스 프로젝트의 비교

항목	Frodo	BCNS	MSrln	NewHope	Kyber
기반 문제	LWE	Ring-LWE	Ring-LWE	Ring-LWE	Module-LWE
연산 알고리즘	-	FFT[1]	NTT[2]	NTT[2]	NTT[2]
에러 샘플링	연속 가우시안 분포	이산 가우시안 분포	이산 가우시안 분포	이항 분포	이항 분포

1) FFT(Fast Fourier Transform)
2) NTT(Number Theoretic Transform)

인 NTT의 연산 속도를 증가하여 프로토콜의 전체적인 부분에서 속도를 향상 시킬 수 있다. 연산속도가 동일한 C 환경에서 약 1.44배, AVX2 환경에서는 약 1.21배로 증가한다.

3.5 Kyber[9]

Kyber는 Bos 등에 의해 2017년 발표된 Module-LWE를 기반으로 한 KEM(Key Encapsulation Mechanism)에 프로토콜로 CCA(Chosen Plaintext Attack)에 대해 안전하며 NewHope 프로토콜과 같이 NTT 알고리즘과 AVX2 사용하기 때문에 빠른 NTT 연산 속도를 보여준다. 다만, 파라미터 n과 q의 값이 각각 $n=256$, $q=7681$로 구현상의 효율성을 위해 API를 통합적으로 사용한다.

IV. 타이밍과 오류주입공격

이번 장에서는 OQS 프로젝트의 래티스 기반 키 교환 프로토콜의 부채널공격 측면에서 분석한다. [표 1]에서 본 논문에서 분석한 OQS 프로젝트 프로토콜을 간단히 비교하였다.

4.1 연산 알고리즘

각 프로토콜은 안전한 연산과 빠른 연산 속도를 위하여 효율적인 연산 알고리즘을 사용한다. BCNS는 FFT를 사용하고 MSrln, NewHope. Kyber는 NTT를 사용한다. FFT 및 NTT에서의 연산은 입력값과 출력값이 달라짐에 따라 연산 시간의 차이가 생기지 않기 때문에 타이밍공격이 어렵다. LWE 및 Ring-LWE를 기반으로 하는 키 교환 프로토콜 연산과정 중, $b=as+e$ 에서 s와 e가 달라져도 전체 연산시간은 동일하기 때문에 타이밍공격을 시도하기 어렵다.

한편, 부채널공격 중 오류주입공격에는 모든 프로토콜이 취약하다. MSrln 프로토콜의 경우, $b=as+e$를 계산하는 과정이 as를 계산한 이후에 e를 더한다. 이 과정에서 e를 더하는 과정을 건너뛰거나 공격자가 주입하는 e를 임의로 바꾼다면 개인키 s를 가우스 소거법(Gaussian elimination)에 의하여 쉽게 구할 수 있다. 그러나 SW 상으로 구현되었을 경우 연산 과정이 분리되어 있을지라도 오류를 주입하는 것은 어려우나, HW로 구현된 경우에는 앞서 설명한 바와 같이 오류를 주입하여 개인키를 쉽게 얻을 수 있다.

$b=as+e$과정에서 [그림 1]과 같이 곱셈과 덧셈으로 이루어진 연산을 하기 위하여 2가지의 FFT API를 사용한다. [그림 2]에서는 이것을 하나로 통합하여 1개의 API로 구현하였다. 제안하는 API를 사용한다면, 오류주입공격에 대하여 안전하다.

NTT에서도 위와 같은 통합 API 구현으로 오류주입공격에도 안전한 래티스 기반 키 교환 프로토콜을 구현할 수 있다.

```
void oqs_kex_rlwe_bcns15_fft_mul(uint32_t z[1024], const uint32_t x[1024],
const uint32_t y[1024], struct oqs_kex_rlwe_bcns15_fft_ctx *ctx) {
        nussbaumer_fft(z, x, y, ctx);
}

void oqs_kex_rlwe_bcns15_fft_add(uint32_t z[1024], const uint32_t x[1024],
const uint32_t y[1024]) {
        int i;
        for (i = 0; i < 1024; i++) {
                add(z[i], x[i], y[i]);
        }
}
```

[그림 1] BCNS의 FFT 곱셈 및 덧셈 API

```
void oqs_kex_rlwe_bcns15_fft_muladd(uint32_t z[1024], const uint32_t x
[1024], const uint32_t y[1024], const uint32_t w[1024], struct
oqs_kex_rlwe_bcns15_fft_ctx *ctx) {
        int i;
        const uint32_t c[1024];

        nussbaumer_fft(c, x, y, ctx);

        for (i = 0; i < 1024; i++) {
                add(z[i], c[i], w[i]);
        }
}
```

[그림 2] 개선된 통합 FFT 연산 API

4.2 에러 샘플링

LWE 및 Ring-LWE 기반 키 교환 프로토콜은 충분히 랜덤한 에러를 추출하여 더하기 때문에 안전성이 확보된다. Frodo는 연속 가우시안 분포, BCNS, MSrln은 이산 가우시안 분포, NewHope와 Kyber는 이항분포를 사용한다.

에러 추출시 난수는 ChaCha20[11], AES의 CTR모드를 사용하여 생성한다. 이는 현재 OpenSSL에서 사용하고 있는 난수 생성과정과 일치한다. 5 종류의 프로토콜을 확인해 본 결과, 모든 프로토콜은 위와 동일하게 난수 생성을 하고 있으며, 실제 구현상의 문제도 존재하지 않았다. 따라서 에러 샘플링 과정은 안전하다는 것을 확인할 수 있었다.

V. 결론 및 향후 연구

본 논문에서는 NIST의 PQC 공모사업의 일환으로 오픈소스로 구현된 OQS 프로젝트에 대하여 소개하였다. OQS 프로젝트는 Frodo, BCNS, MSrln, NewHope, Kyber의 래티스 기반 키 교환 프로토콜이 있으며, 연산 알고리즘과 에러 샘플링 과정에서의 부채널공격에 대하여 분석하였다. 결과적으로 FFT와 NTT 과정에서 오류주입 공격이 가능한 것을 확인하였다. 이에 대한 개선책으로 FFT 연산시 덧셈과 곱셈으로 분리된 API를 통합된 API로 구현하였다.

향후 연구 과제로는 OQS 프로젝트에 포함되지 않은 Lizard[12]에 대한 부채널공격 가능성과 메모리관련 취약점도 확인하여 오류주입 없이 개인키를 추출하는 공격 등을 검증할 예정이다.

[참고문헌]

[1] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in Proceedings of the Foundations of Computer Science, 35th Annual Symposium on IEEE, 1994, pp. 124-134.

[2] https://csrc.nist.gov/Projects/Post - Quantum-Cryptography

[3] D. Stebila and M. Mosca, “Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project”, Cryptology ePrint Archive, Report 2016/1017, 2016.

[4] https://github.com/open-quantum-safe/

[5] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, and V. Nikolaenko. “Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE.” In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1006-1018.

[6] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, M. Schanck, and D. Stehlé, “CRYSTALS - Kyber: a CCA- secure module-lattice-based KEM”, Cryptology ePrint Archive, Report 2017/634, 2017.

[7] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem.” Security and Privacy (S&P), 2015 IEEE Symposium on. IEEE, 2016, pp.553-570.

[8] P. Longa and M. Naehrig. "Speeding up the number theoretic transform for faster ideal lattice-based cryptography", in International Conference on Cryptology and Network Security 2016, pp. 124-139.

[9] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe, “Post-quantum Key Exchange - A New Hope”, In USENIX Security Symposium 2016, pp. 327-343.

[10] M. Albrecht and A. Deo, “Large Modulus Ring-LWE ≥ Module-LWE”, Cryptology ePrint Archive, Report 2017/612, 2017.

[11] Y. Nir and A. Langley. “ChaCha20 and Poly1305 for IETF Protocols”, No. RFC 7539. 2015.

[12] J. Cheon, D. Kim, J. Lee, and Y. Song, “Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR”, Cryptology ePrint Archive, Report 2016/1126, 2016.