래티스 기반 키 교환 프로토콜의 비교[1)]

안형철* 최락용** 이지은** 김광조*,**

*카이스트 정보보호대학원/ **전산학부

Comparison of Lattice-based Key Exchange Protocols

Hyeongcheol An* Rakyong Choi** Jeeun Lee** Kwangjo Kim*,**

*Graduate School of Information Security/ *School of Computing, KAIST.

요 약

래티스 기반 키 교환 프로토콜은 양자컴퓨터의 공격에도 안전한 포스트 양자 암호(Post Quantum Cryptography, PQC)이며, 최근 각광받고 있는 분야이다. 기존에 사용하고 있는 DH방식의 키 교환 프로토콜은 양자컴퓨터의 공격에 의해 쉽게 해독되기 때문에 래티스 기반 키 교환 프로토콜의 필요성이 제기되고 있다. 그 중, 총 5 가지의 DXL, BCNS, NewHope, Frodo 키 교환 프로토콜, 그리고 ZZD+ 인증 키 교환 프로토콜에 대하여 분석하였다. 이에, 본 논문에서는 키 교환 프로토콜을 구현 효율성, 기반 문제, 샘플링 과정에서 쓰는 확률분포, 디지털 컴퓨터와 양자 컴퓨터에 대한 보안도 측면에서 비교하였다.

I. 서론

기존 키 교환(Key Exchange, KE) 프로토콜 및 인증 키 교환(Authenticated Key Exchange, AKE) 프로토콜은 이산 대수 문제, 소인수 분해 문제의 어려움에 기반하기 때문에 Shor 알고리즘[1]에 따라 양자컴퓨터의 공격에 깨지게 된다. 따라서 양자컴퓨터의 공격에도 안전한 KE가 필요하다. 포스트 양자 암호(Post-Quantum Cryptography)의 필요성이 제기되고 있으며, 그 중 하나로 래티스(Lattice) 기반 KE 프로토콜이 알려져 있다. 또한 인증과정이 추가된 AKE 프로토콜은 기존의 KE 프로토콜에 비하여 상호간의 인증 정보를 교환하여 중간자 공격(Man-in-the-Middle Attack)에 안전하다.

본 논문에서 분석한 래티스 기반 KE 및 AKE 프로토콜은 총 5 가지로 DXL[2], BCNS[3], NewHope[4], Frodo[5], ZZD+[6]이다. 위의 프로토콜에 대하여 소개하고 각각의 프로토콜을 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘에 대하여 비교한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. Ⅱ장에서 KE와 AKE 프로토콜에 대하여 간략히 설명한다. 이후 Ⅲ장은 5 가지의 래티스 기반 KE 및 AKE 프로토콜 대하여 소개하고, Ⅳ장에서는 앞서 설명한 프로토콜에 대하여 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘, 디지털컴퓨터와 양자컴퓨터에 대한 보안도에 대하여 비교하고 표로 정리하였다. 마지막으로 Ⅴ장에서는 향후 래티스 기반 키 교환 프로토콜을 활용한 연구과제에 대하여 논의하고 결론을 내린다.

1) 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2015R1A2A2A01006812).

[표 1]. 래티스 기반 키 교환 프로토콜의 파라미터 비교

항목	DXL	BCNS	NewHope	Frodo	ZZD+
n	1024	1024	1024	752	1024 or 2048
q	$2^{32}-1$	$2^{32}-1$	12289	2^{15}	$2^{45}\sim 2^{50}$
λ	128	86	229	144	75-230

n: 행렬 및 벡터의 차원, q: modulus value, λ: 보안변수

II. 배경지식

2.1 키 교환 프로토콜

KE는 공개된 채널에서 공통의 비밀 키를 공유할 수 있는 방법으로 DH(Diffie-Hellman)[7] KE 프로토콜이 널리 알려져 있다. 그러나 인증 과정이 없으면 중간자 공격에 취약하기 때문에 AKE 프로토콜이 필요하다.

2.2 인증 키 교환 프로토콜

앞서 설명한 일반적인 KE와 달리 AKE는 상호 간의 인증과정이 추가되어 중간자 공격에 안전한 프로토콜이다. 일반적으로 AKE를 달성하기 위하여 KE 프로토콜에서 해시함수나 공개키 암호화를 활용하여 인증 과정을 추가한다.

III. 키 교환 프로토콜

이번 장에서는 총 5 가지의 래티스 기반 KE 및 AKE에 대하여 설명한다. 각 프로토콜의 파라미터 크기는 [표 1]에 정리하였다.

3.1 DXL

DXL은 Ding 등이 2012년에 발표한 프로토콜로 래티스 기반 KE 프로토콜 중에서 가장 먼저 발표되었다. 이후 이 프로토콜은 Peikert[8]에 의해 발전되었다. Ring-LWE 기반 문제로 설계되어 효율성이 증가하였다. 그러나 실제 구현은 이루어지지 않았다는 단점이 있다. 또한 파라미터 크기가 $q=2^{32}-1$로 크기 때문에 Ring-LWE를 사용했음에도 LWE문제를 사용한 프로토콜에 비하여 효율성이 크게 증가하지는 않는다.

3.2 BCNS

Bos 등에 의해 2015년 발표된 프로토콜로 DXL 프로토콜을 실제 최적화 하여 구현하였다. 이 프로토콜에서 사용하는 이산 가우시안 분포는 타이밍 공격(Timing Attack)[9]에 취약하다. 또한 CPU의 캐시 메모리를 활용한 캐시 공격(Cache Attack)[10]의 가능성이 있다. 그러나 래티스 기반 KE에서 OpenSSL[11]에 추가되어 상용화를 시도하였고, TLS/SSL 프로토콜에서 추가하여 사용하고 있다.

3.3 NewHope

NewHope 프로토콜은 Alkim 등에 의해 BCNS 프로토콜의 단점을 보완하여 설계 및 구현하였다. BCNS 프로토콜은 파라미터 중 $q=2^{32}-1$로 다른 KE 프로토콜에 비하여 크기 때문에 안전하지 않으며 효율성이 떨어진다. 그러나 NewHope에서는 $q=12289<2^{14}$까지 줄여서 취약점을 보완하였고, 효율성이 증가하였다. 또한 NTT(Number Theoretic Transform) 연산에서 Intel CPU에서 지원하는 AVX2(Advanced Vector Extensions)을 사용하기 때문에 프로토콜의 속도가 증가하였다.

현재 Google Chrome Canary 브라우저[12]와 서버 간의 통신과정에서 KE 프로토콜로 NewHope을 사용하고 있다는 것이 특징이다. 앞서 설명한 BCNS의 에러 샘플링 알고리즘을 이산 가우시안 분포에서 이항분포로 바꾸어 타이밍 공격에 대하여 안전하다.

표 2. 래티스 기반 키 교환 프로토콜 비교

항목	DXL	BCNS	NewHope	Frodo	ZZD+
발표년도	2012	2015	2015	2016	2015
프로토콜	KE	KE	KE	KE	AKE
기반 문제	LWE/ Ring-LWE	Ring-LWE	Ring-LWE	LWE	Ring-LWE
실행시간(ms)	-	2.8	0.3	2.6	37.8-119.5
데이터 전송량(KB)	-	8	4	23	12-25
에러 샘플링	이산 가우시안 분포	이산 가우시안 분포	이항 분포	연속 가우시안 분포	이산 가우시안 분포
종래 보안도(bit)	128	86	229	144	75-230
양자 보안도(bit)	-	78	206	130	-
증명방법(ROM[1])	X	X	X	X	O

1) ROM(Random Oracle Model)

3.4 Frodo

Frodo 프로토콜은 Bos 등이 설계하고 구현한 프로토콜로 Ring-LWE 문제를 사용한 NewHope의 위험성을 가정하고, LWE 문제를 기반으로 하는 것이 가장 큰 특징이다. 파라미터의 크기는 $n=752$이며, $q=2^{15}$이다. Ring-LWE 문제를 기반으로 설계한 BCNS 프로토콜과 비교하여 실행시간의 차이가 크게 나지 않는 것은 $q=2^{15}<2^{32}-1$로 파라미터의 크기가 크게 줄었기 때문에 LWE 문제를 기반으로 했음에도 불구하고 오히려 HTTP 환경[5]에서는 더 빠른 것을 알 수 있다.

3.5 ZZD+

앞서 설명한 KE 프로토콜들과 ZZD+ 프로토콜의 가장 큰 차이는 인증과정이 있다는 것이다. 이전의 KE 프로토콜은 파라미터의 크기가 고정되어 있지만, 파라미터의 크기가 가변적으로 설정할 수 있다. n의 크기를 1024-bit와 2048-bit로 설정하여 각각의 파라미터 크기에 대하여 보안도를 가변적으로 조절할 수 있다.

인증과정에서는 공격자가 세션 키를 바꿀 수 없는 HMQV[13] 프로토콜을 사용하였다. 해시함수를 추가한 방법으로 효율성이 증가하였다.

IV. 키 교환 프로토콜 비교

이번 장에서는 기반문제, 실행시간, 데이터 전송량, 에러 샘플링, 그리고 보안도를 중심으로 각 프로토콜을 비교한다. 각 프로토콜의 비교는 [표 2]에 정리하였다. 실험은 Intel CPU 3.4GHz에서 실행시간을 측정하였다.

4.1 기반 문제

앞서 설명한 5 종류의 프로토콜은 래티스 기반 문제로 설계되었으며, Frodo는 LWE 문제를 사용하여 설계하였으며, DXL, BCNS, NewHope, ZZD+ 프로토콜은 Ring-LWE를 사용하였다. LWE 문제는 행렬 A와 벡터 $b=As+e$가 주어졌을 임의의 쌍 (A,b')을 구분하는 문제이고, Ring-LWE 문제는 다항식 쌍 $\{a_i, b_i = a_i \bullet s + e_i\}_{i=1}^{m}$가 주어졌을 때, 임의의 쌍 $\{a_i, b_i'\}_{i=1}^{m}$을 구분하는 문제이다. LWE 기반 문제보다 Ring-LWE 기반 문제가 구현 효율성이 증가하고, 파라미터의 크기가 작아지기 때문에 프로토콜 과정의 고속화에 기여할 수 있다는 장점이 있다.

4.2 실행시간

비교한 5 가지의 프로토콜 중 가장 빠른 프로토콜은 NewHope이며 약 0.3ms의 실행시간이 걸린다는 것을 확인할 수 있다. 이는 기반문제가 Ring-LWE를 사용하여 프로토콜 과정의 고속화에 기여한 것으로 분석할 수 있다. 또한 LWE 문제를 사용한 Frodo의 경우 2.6ms가 걸렸고, 이것은 BCNS의 2.8ms와 비슷한 실행시간을 가진다는 것을 알 수 있다.

4.3 데이터 전송량

데이터 전송량에서는 NewHope 프로토콜이 4KB로 5 가지의 프로토콜 중 가장 적은 양을 사용한다. 반면에 Frodo는 대략 6배의 23KB의 데이터를 전송한다. 이것은 앞서 설명한 기반문제의 차이로 분석할 수 있다. LWE 문제를 사용하면 데이터의 전송량이 커진다는 단점이 존재한다. NewHope 프로토콜의 경우 Ring-LWE를 사용하였지만, Frodo는 LWE 문제를 사용하여 데이터 전송량에서 단점을 가지고 있다. BCNS는 약 8KB의 데이터가 전송되며 Frodo 보다 적은 것을 알 수 있다. ZZD+는 다른 프로토콜과는 달리 인증과정이 추가되어 최대 25KB의 데이터가 전송된 다는 것을 확인할 수 있다.

4.4 에러 샘플링

DXL, BCNS, ZZD+ 프로토콜은 이산 가우시안 분포(Discrete Gaussian Distribution)을 에러 샘플링 알고리즘으로 사용하였다. 반면에 NewHope 프로토콜은 이항 분포(Binomial Distribution)을 사용하였고, Frodo 프로토콜은 Rounded 연속 가우시안(Rounded Continuous Gaussian Distribution) 분포를 사용하였다.

4.5 보안도(Security Level)

5 가지의 KE 및 AKE 프로토콜은 래티스 기반의 프로토콜로 양자컴퓨터의 공격에 안전하다. 따라서 디지털 컴퓨터의 보안도와 양자 컴퓨터의 보안도로 구분된다. DH KE 프로토콜의 경우 1024-bit의 파라미터를 사용하면 80-bit의 보안도를 가진다. 기존 디지털 컴퓨터에서 5 가지의 KE 및 AKE 프로토콜의 보안도는 86-bit에서 230-bit까지 나타나 있다. 따라서 분석한 프로토콜 모두 실제 환경에서 안전성에 문제없이 사용할 수 있다는 것을 알 수 있다.

양자 보안도의 경우 공격 모델이 현재 사용하고 있는 디지털 컴퓨터가 아닌 양자컴퓨터를 활용한 공격에서의 안전성을 뜻한다. DXL과 ZZD+ 프로토콜의 양자 보안도는 공개되지 않았고, NewHope 프로토콜이 206-bit인 것을 확인할 수 있다. 이것은 양자컴퓨터가 상용화되어도 KE 프로토콜의 안전성을 보장한다고 할 수 있다.

V. 결론 및 향후 연구

본 논문에서는 래티스 기반 KE 및 AKE 프로토콜인 DXL, BCNS, NewHope, Frodo, ZZD+ 프로토콜에 대하여 특징 및 구현 효율성 측면에서 비교 분석하고 분류하였다.

앞서 분석한 프로토콜은 모두 양자간에 사용할 수 있으며, 다자간(Multi-Party)에는 사용할 수 없다. 따라서 향후 래티스 기반 AKE 프로토콜을 다자간 통신 환경에서 사용할 수 있도록 확장하는 연구를 진행할 예정이다. 또한 구현 효율성 측면에서 AKE 프로토콜의 실행시간 및 데이터 전송량을 KE 프로토콜 정도로 줄이는 연구도 병행하여 진행할 것이다. 래티스 기반 KE 및 AKE 프로토콜은 양자컴퓨터의 공격에도 안전하지만 실제 QROM(Quantum Random Oracle Model)에서 증명을 하지 않았다. QROM은 임의의 질의에 대한 응답을 가진 가상 암호학적 기능을 모델링한 것이다. 특히 해시 함수를 이용한 프로토콜의 증명 가능한 안전성 분석에 널리 사용된다. 따라서 QROM에서 증명을 통하여 실제 이론적으로 양자컴퓨터의 공격에 안전한지 확인할 것이다.

[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] J. Ding, X. Xie, and X. Lin. “A simple provably secure key exchange scheme based on the learning with errors problem.” IACR Cryptology ePrint Archive, Report 2012/688. 2012.

[3] 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, pp.553-570. 2015.

[4] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. “Post-quantum key exchange - a new hope.” Cryptology ePrint Archive, Report 2015/1092, 2015.

[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, pp. 1006-1018. 2016.

[6] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö Dagdelen. “Authenticated key exchange from ideal lattices. ”Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015, pp.719-751. 2015.

[7] W. Diffie and M. Hellman. “New directions in cryptography.” IEEE Transactions on Information Theory 22.6, pp. 644-654. 1976.

[8] C. Peikert. "Lattice cryptography for the Internet." International Workshop on Post-Quantum Cryptography, pp. 197-219. 2014.

[9] 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, pp.553-570. 2015.

[10] D. Osvik, A. Shamir, and E. Tromer, “Cache attacks and countermeasures: The case of AES”, In David Pointcheval, editor, CT-RSA 2006, pp.1 - 20, 2006.

[11] OpenSSL, https://www.openssl.org/

[12] Google Canary, https://www.google.co.kr /chrome/ browser/canary.html

[13] H. Krawczyk, “HMQV: A high - performance secure Diffie-Hellman protocol”, In Annual International Cryptology Conference, CRYPTO 2005, pp.546-566, 2005.