RLWE 기반 분산형 그룹키 교환 방식의 성능 분석[1)]

한성호* 최락용** 김광조*,**

* KAIST 정보보호대학원 ** KAIST 전산학부

Performance Analysis of RLWE-based Distributed Group Key Exchange Protocols

Seongho Han* Rakyong Choi** Kwangjo Kim*, **

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

요 약

통신 기술이 발달하면서 한 그룹에서 동일한 키를 공유하는 프로토콜의 수요가 늘고 있다. 그러나 현재 대부분의 그룹키 교환 방식은 이산대수 기반 문제를 사용함으로써 양자 컴퓨터 공격에 취약하다. 양자내성을 갖는 문제 중 하나인 RLWE를 활용하여 다양한 그룹키 교환 방식이 제안되었다. 분산형 그룹키 교환 방식은 모든 노드가 동등한 권한으로 그룹키 형성에 기여하는 방식이다. 본 논문에서는 RLWE 기반 그룹키 교환 방식 중 분산형 방식으로 구현된 프로토콜의 성능을 정량적으로 비교한다. 이를 통해 더 효율적인 RLWE 기반 분산형 그룹키 교환 방식을 파악한다.

I. 서론

통신 기술이 발달하면서 한 그룹에서 같은 키를 공유하는 프로토콜의 수요가 증가하고 있다. Bresson 등[1], Steiner 등[2]과 Dutta, Barua[3] 등이 대표적인 그룹키 교환 방식이다. 그러나 기존 프로토콜 대부분은 이산대수 기반 문제의 어려움에 기반을 두고 있으므로 양자 컴퓨터 공격에 취약하다[4].

양자 컴퓨팅 시대에 대응하여 NIST는 양자 컴퓨터 공격에 안전한 양자내성암호 표준을 채택하기 위해 공모를 시행하고 있다. 격자 기반 키 교환 방식은 양자내성암호에서 가장 유망한 후보 중 하나이다. 초기에는 Regev[5]에 의해 Learning with Error (LWE) 문제를 기반으로 하는 격자 기반 암호가 주목되었다. 그러나 연산량이 많아 효율성이 저하된다는 비판이 제기되었으며 이를 보완하기 위해 Ring Learning with Error (이하 RLWE) 문제[6]가 Lyubashevsky 등에 의해 제안되었다. 대표적으로 구현된 RLWE 기반 키 교환 프로토콜은 NewHope[7], Bos 등[8] 등이 있다.

RLWE 기반 키 교환 방식을 확장한 여러 RLWE 기반 그룹키 교환 방식이 제시되었다. Apon 등[9] (이하 ADGK19), Ding 등[10] (이하 DXL12)은 분산형 RLWE 기반 그룹키 교환 방식을 제안하였다. 분산형 그룹키 교환 방식에서는 모든 노드가 동등한 권한으로 그룹키 형성에 기여한다. 지금까지 알려진 바에 의하면 분산형 RLWE 기반 프로토콜의 효율성을 서로 비교한 적은 없다.

본 논문에서는 RLWE 기반 그룹키 교환 방식 중 분산형 프로토콜인 ADGK19와 DXL12의 효율성을 정량적으로 비교하여 효율적인 RLWE 기반 분산형 그룹키 교환 방식을 분석한다.

1) 본 연구는 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 RLWE 문제 및 분산형 그룹키 교환 방식에 대하여 설명하고, Ⅲ,Ⅳ장에서는 AGDK19과 DXL12의 키 교환 방식을 설명한다. Ⅴ장에서는 ADGK19와 DXL12의 효율성을 정량적으로 분석한다. 끝으로 Ⅵ장에서는 결론과 추후 연구에 대하여 기술한다.

II. 배경지식

이 장에서는 RLWE와 분산형 그룹키 교환 방식에 대해 설명한다.

2.1 RLWE 문제

RLWE 문제에는 search RLWE와 decisional RLWE가 있다. NewHope[7], Ding 키 교환[10] 등에 널리 사용되는 decisional RLWE의 정의는 다음과 같다.

RLWE instance의 차원 n, ring polynomial의 집합 $R=Z[X]/(X^n+1)$, quotient ring을 정의하는 modulus q, R의 q로 quotient한 R_q, R_q에서 error를 추출하는 분포 χ를 정의하자. s를 χ에서 뽑자. 오라클 $O_{\chi,s}$를 다음과 같이 정의하자.

1) $a \leftarrow U(R_q)$, $e \leftarrow \chi$를 추출한다.

2) $(a, as+e) \in R_q \times R_q$를 반환한다.

n, q, χ에 대한 decisional RLWE 문제는 $R_q \times R_q$로부터 균일하게 랜덤 샘플을 반환하는 오라클과 오라클 $O_{\chi,s}$를 구별하는 것이다.

2.2 분산형 그룹키 교환 방식

분산형 그룹키 교환 방식은 키 교환에 참여한 모든 노드가 동등한 권한으로 키 생성에 참여하는 방식을 의미한다. 대표적인 분산형 그룹키 교환 방식은 Steiner 등[2]과 Dutta, Barua[3] 등이 있다. 대부분의 분산형 그룹키 교환 방식은 Diffie-Hellman 문제에 기반을 두고 있으므로, 양자 컴퓨터에 대비한 그룹키 교환 방식의 필요성이 제기되어 왔다.

ADGK19와 DXL12은 RLWE 문제를 기반으로 분산형 그룹키 교환 방식을 제안하였다. ADGK19는 방송형 방식을 이용하며, DXL12은 환 구조와 일방향 통신 방식을 사용한다. 본 논문에서는 두 프로토콜의 효율성을 비교한다.

III. ADGK19의 그룹키 교환 방식

ADGK19는 Dutta, Barua의 그룹키 교환 방식[3]에서 Diffie-Hellman 문제를 RLWE 문제로 변형하여 프로토콜을 설계했다. 노드의 숫자와 관계없이 고정적으로 3 round를 거쳐 키 교환이 이루어지도록 설계하였다. 프로토콜의 진행 과정은 다음과 같다.

(Initialization) 통신할 노드의 수 N, RLWE instance의 차원 n, quotient ring을 정의하는 modulus q, 균일한 값 $a \leftarrow R_q$, R_q에서 error를 추출하는 분포 χ_{σ_1}, χ_{σ_2}, statistical security parameter ρ를 결정한다. 노드의 번호는 0부터 N-1까지이다.

(Round 1) 각 노드 P_i에서 병렬적으로 수행

1. 노드 P_i는 '작은' 비밀 값인 $s_i \leftarrow \chi_{\sigma_1}$를 선택하고 '작은' error $e_i \leftarrow \chi_{\sigma_1}$를 추출한다. 그리고 $z_i = as_i + e_i$를 계산한다.

2. 다른 모든 노드들에게 z_i를 방송한다.

(Round 2) 각 노드 P_i에서 병렬적으로 수행

1. 노드 P_0는 $e'_0 \leftarrow \chi_{\sigma_2}$를 추출한다. 나머지 노드 P_i는 $e'_i \leftarrow \chi_{\sigma_1}$를 추출한다.

2. 각 노드 P_i는 $X_i = (z_{i+1} - z_{i-1})s_i + e'_i$를 계산 후 X_i를 방송한다.

(Round 3)

1. 노드 P_{N-1}는 $e''_{N-1} \leftarrow \chi_{\sigma_1}$를 추출한다.

그리고 $b_{N-1} = z_{N-2}Ns_{N-1} + (N-1) \cdot X_{N-1} + (N-2) \cdot X_0 + \cdots + X_{N-3} + e''_{N-1}$을 계산한다.

2. $(rec,\ k_{N-1}) = recMsg(b_{N-1})$를 계산한다.

3. rec를 방송한다.

4. 세션키 $sk_{N-1} = H(k_{N-1})$을 도출한다.

(Key Computation) 각 노드 P_i (P_{N-1}제외)에서 병렬적으로 수행

1. 노드 P_i는 $b_i = z_{i-1}Ns_i + (N-1) \cdot X_i + (N-2) \cdot X_{i+1} + \cdots + X_{i+N-2}$를 수행한다.

2. $k_i = recKey(b_i, rec)$를 계산한다.

3. 세션키 $sk_i = H(k_i)$를 도출한다.

(Key Computation) 과정이 끝나면 모든 노드 P_i는 1에 가까운 확률로 동일한 세션키를 공유한다.

IV. DXL12의 그룹키 교환 방식

DXL12 방식은 통신에 주로 일방향 통신을 사용한다는 특징이 있다. DXL12는 Bresson 등 [1]의 키 교환 방식에서 Diffie-Hellman 문제를 RLWE 문제로 바꾸어 설계했다. 프로토콜의 진행과정은 다음과 같다.

(Initialization) ADGK19 방식과 유사하다. 통신할 노드의 수 N, RLWE instance의 차원 n, quotient ring을 정의하는 modulus q, 균일한 값 $a \leftarrow R_q$, R_q에서 error를 추출하는 분포 χ_σ를 결정한다. 노드의 번호는 0부터 N-1까지이다.

(Round 1) 각 노드 P_i에서 병렬적으로 수행

1. 노드 P_i는 '작은' 비밀 값인 $s_i \leftarrow \chi_\sigma$를 선택하고 '작은' error $e_i^0 \leftarrow \chi_\sigma$를 추출한다. 그리고 $z_i = as_i + 2e_i^0$를 계산한다.

2. 노드 P_i는 인접한 노드 P_{i+1}에게 z_i를 전송한다.

(Round j (j=2, 3,..., N-1)) 각 노드 P_i에서 병렬적으로 수행

1. 노드 $P_{i+j-1 \pmod N}$는 j번째 Round에 $z_i^{j-1} = s_{i+j-1 \bmod N} \cdot z_i^{j-2} + 2e_i^{j-1}$를 계산한다.

2. 노드 $P_{i+j-1 \pmod N}$는 계산한 z_i^{j-1}를 $P_{i+j \pmod N}$에 전송한다.

(Round N)

1. 노드 P_0는 $e_0^{N-1} \leftarrow \chi_\sigma$을 추출한다.

그리고 $K_0 = s_0 \cdot z_1^{N-2} + 2e_0^{N-1}$을 계산한다.

2. Reconciliation Method S를 사용하여, $\sigma \leftarrow S(K_0)$를 계산한다.

3. 노드 P_0는 세션키 $SK_0 = recKey(K_0, \sigma)$를 얻는다.

4. rec인 σ를 방송한다.

(Key Computation) 각 노드 P_i (P_0 제외)에서 병렬적으로 수행한다.

1. 노드 P_i는 $e_i^{N-1} \leftarrow \chi_\sigma$를 추출한다. 그리고 $K_i = s_i \cdot z_{i+1}^{N-2\ (\bmod N)} + 2e_i^{N-1}$를 계산한다.

2. 각 노드 P_i는 $SK_i = recKey(K_i, \sigma)$를 계산하여 세션키를 도출한다.

(Key Computation) 과정이 끝나면 모든 노드 P_i는 1에 가까운 확률로 동일한 세션키를 공유한다.

V. ADGK19와 DXL12의 그룹키 교환 방식의 효율성 비교

본 논문에서는 ADGK19와 DXL12의 키 교환 방식을 통신 방식, round의 수, ring polynomial addition 연산 횟수, ring polynomial multiplication 연산 횟수, 비밀 값 샘플링 횟수, error 샘플링 횟수의 관점에서 비교하였다. Ring polynomial addition 연산 횟수는 +가 있을 때마다, ring polynomial multiplication 연산 횟수는 •가 있을 때마다 1회로 계산하며 ring polynomial 간의 연산만 고려한다.

비밀 값 샘플링과 error 샘플링은 추출할 때마다 1회로 간주한다.

이 중 ring polynomial multiplication과 각 샘플링 횟수는 프로토콜의 효율성 측정에 가장 중요한 요소이다.

표 1. ADGK19와 DXL12의 그룹키 교환 방식의 성능 비교

	ADGK19[9]	DXL12[10]
통신 방식	방송형	일방향 통신 + 방송형
Round 수	***3***	N
Ring Polynomial Addition 연산 횟수	$(N+1)^2$	N^2
Ring Polynomial Multiplication 연산 횟수	***3N***	N^2
비밀 값 샘플링 횟수	N	N
Error 샘플링 횟수	***2N+1***	N^2

[표 1]은 노드 숫자 N에 따른 ADGK19와 DXL12 키 교환 방식의 연산 횟수이다. Ring polynomial addition 연산을 제외하고 N이 클수록 ADGK19의 연산 횟수가 DXL12보다 더 적음을 알 수 있다. 결론적으로 통신할 노드의 숫자 N이 커질 때, ADGK19 키 교환 방식이 효율성 측면에서 우월함을 도출할 수 있다.

VI. 결론 및 향후 과제

본 논문에서는 두 개의 RLWE 기반 분산형 그룹키 교환 방식인 ADGK19와 DXL12의 효율성을 정량적으로 계산하였다. 그 결과 ADGK19 방식이 효율적임이 확인되었다.

향후 연구에서는 두 프로토콜을 실제 구현한 후 연산 시간을 제시하고 RLWE와 그 외의 양자내성을 가지는 분산형 그룹키 교환 방식의 효율성을 비교한다.

[참고문헌]

[1] E. Bresson, *et al.* “Provably authenticated group Diffie-Hellman key exchange.” ACM CCS 2001, 2001

[2] M. Steiner, G. Tsudik, and M. Waidner. "Key agreement in dynamic peer groups." IEEE Transactions on Parallel and Distributed Systems 11.8: pp. 769-780, 2000.

[3] R. Dutta and R. Barua. "Constant round dynamic group key agreement." ISC 2005, 2005.

[4] P. W. Shor. "Algorithms for quantum computation: Discrete logarithms and factoring." FOCS 1994, 1994.

[5] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography." J. of the ACM 56.6: 34, 2009.

[6] V. Lyubashevsky, C. Peikert, and O. Regev. "On ideal lattices and learning with errors over rings." EUROCRYPT 2010, 2010.

[7] E. Alkim, *et al.* “Post-quantum key exchange - a new hope.” Cryptology ePrint Archive, Report 2015/1092, 2015

[8] J. W. Bos, *et al.* "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem." IEEE S&P 2015, 2015.

[9] D. Apon, *et al.* "Constant-Round Group Key Exchange from the Ring-LWE Assumption." IACR Cryptology ePrint Archive 2019/398, 2019.

[10] 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 2012/688, 2012.