Newhope의 키 조정 메커니즘을 통한 Apon 등의 프로토콜 구체적 사례 검증[1)]

홍 동 연* 최 락 용** 김 광 조*,**

*카이스트 정보보호대학원 **카이스트 전산학부

Instantiation of Apon *et al.* Protocol using Newhope Key Reconciliation Mechanism

Dongyeon Hong* Rakyong Choi** Kwangjo Kim*,**

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

요 약

안전하지 않은 채널에서 통신 상대방과 안전한 소통을 하기 위해 암호시스템을 사용한다. 암호시스템을 사용하기 전 두 사용자 혹은 그룹 내 비밀키 교환이 우선 수행되어야 한다. 근래 두 명이 아닌 그룹 단위의 작업 환경이 많아짐에 따라 그룹 내 키 교환이 중요해지고 있다. Apon 등은 동일한 라운드의 격자 기반 그룹 키 교환 프로토콜을 최초로 제안하였다. 그러나 프로토콜의 키 조정 메커니즘을 구체적으로 설계하지 않고 제안하였다. 본 논문에서는 해당 부분의 구체적인 설계를 통해 프로토콜을 완성하고 정확성과 안전성을 살펴보도록 한다.

I. 서론

1.1 배경

일반적으로 카카오톡, 라인 등 메신저를 사용하여 다른 사용자와 쉽게 대화를 하거나 문서 파일을 주고받는다. [1]에서 일반적인 카카오톡의 대화를 일부 복구할 수 있는 점을 지적했듯이 일반적인 메신저는 정보 노출에 취약하다. 비밀키 암호를 사용하여 암호화 후 정보를 보낼 경우 정보 노출을 방지할 수 있다. 비밀키 암호를 사용하기 위해 사전에 키 교환 프로토콜을 통해 사용자 간 동일한 키를 공유해야 한다. 최근 페이스북의 그룹 채팅과 스카이프를 통해 둘 이상의 사용자가 동시에 화상 통화를 하거나 정보를 주고받는 사례가 많아지고 있다. 두 사용자인 경우와 마찬가지로 그룹 내 안전한 소통을 위해서는 그룹 단위의 키 교환 프로토콜이 사전에 수행되어야 한다. 이를 그룹 키 교환 프로토콜이라 한다. 그러나 대부분의 그룹 키 교환 프로토콜은 이산 대수 문제, 인수분해 문제에 기반하고 있어 양자컴퓨터를 이용한 공격에 내성을 갖추고 있지 않다. 이를 대비해 NIST(미국 국립표준기술연구소)에서 양자컴퓨터에 내성을 갖춘 키 교환 프로토콜의 표준화 작업을 진행하고 있다. 그러나 그룹 키 교환 프로토콜의 표준화 작업은 진행하고 있지 않다. 두 사용자 간 키 교환 프로토콜을 반복적으로 수행함으로 그룹 내 키 교환을 했다고 할 수 있으나 그룹 내 사용자가 N일 때 각 사용자는 $N-1$번의 키 교환 프로토콜을 수행해야 하므로 효율성이 떨어진다. 그룹 키 교환 프로토콜을 사용하여 더 효율적으로 그룹 내 동일한 키를 공유할 수 있으며 [2-4]가

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

초기 설정: R_q, $a \in R_q$, σ_1, σ_2를 설정한다.

라운드 1: 사용자 P_i는 s_i, e_i를 χ_{σ_1}에서 샘플링하고 $z_i = as_i + e_i$를 모든 사용자에게 전파한다.

라운드 2: 사용자 P_0는 χ_{σ_2}에서 e_0'를 샘플링하고 남은 사용자 P_i는 χ_{σ_1}에서 e_i'를 샘플링한다.
각 사용자 P_i는 $X_i = (z_{i+1} - z_{i-1})s_j + e_j'$을 모든 사용자에게 전파한다.

라운드 3: 사용자 P_{N-1}은 χ_{σ_1}에서 e_{N-1}''을 샘플링하고 $b_{N-1} = z_{N-2}Ns_{N-1} + (N-1)X_{N-1} + (N-2)X_0 + \cdots + X_{N-3} + e_{N-1}''$을 계산한다.
$recMsg(b_{N-1})$을 통해 (rec, k_{N-1})을 구하고 rec을 모든 사용자에게 전파하고 그룹키 sk_{N-1}을 $Hash(k_{N-1})$을 통해 계산한다.

키 계산: P_{N-1}을 제외한 사용자 P_i는 $b_i = z_{i-1}Ns_i + (N-1)X_i + (N-2)X_{i+1} + \cdots + X_{i+N-2}$를 계산하고 $recKey(b_i, rec)$을 통해 k_i를 구한다. 마지막으로 $Hash(k_i)$를 통해 그룹 키 k_i를 계산한다.

그림 1 ADGK19의 프로토콜

그룹키 교환 프로토콜을 제안하였다. 그 중 [2, 3]이 제안한 프로토콜은 Ring Learning with Errors (RLWE) 문제를 기반으로 설계되었다. 그러나 [2]의 프로토콜 중 일부분은 포괄적으로 설계되어있어 구체적인 설계가 추가적으로 필요하다. 본 논문에서는 해당 부분을 더 구체화하여 [2]를 완성하고자 하며 본 프로토콜의 정확성과 안전성을 살펴보고자 한다.

1.2 논문 구성

본 논문의 구성으로 Ⅱ장은 관련 논문을 살펴보며 Ⅲ장에서 제안 프로토콜에 필요한 배경 지식을 간략히 살펴본다. Ⅳ장은 제안 프로토콜을 다룬다. Ⅴ장에서는 Ⅳ장에서 다루었던 프로토콜의 정확성과 안전성에 대해 다룬다. Ⅵ장에서는 결론과 추후 연구에 대한 가능성을 제시한다.

II. 관련 논문

2.1 Apon 등의 프로토콜

Apon 등[2] (이하 ADGK19)은 Burmester와 Desmedt [5]이 제안한 프로토콜 중 방송형 방식에 RLWE 문제를 적용하였다. [5]와 다르게 ADGK19에선 두 개의 이산 가우시안 분포 (discrete Gaussian distribution) χ_{σ_1}과 χ_{σ_2}를 사용하며 군이 아닌 환 $R_q = Z_q[x]/(x^n+1)$에서 연산을 수행하고 $a \in R_q$과 표준편차 σ_1, σ_2를 공개 파라미터로 설정한다. 프로토콜은 그림 1과 같다. 이때 $recMsg$와 $recKey$를 키 조정 메커니즘 (key reconciliation mechanism)이라 하고 그룹 내 사용자가 동일한 키를 공유하기 위해 보조적인 역할을 한다.

2.2 키 조정 메커니즘

키 조정 메커니즘은 Ding 등[3]이 제일 먼저 제안하였으며 뒤이어 [6, 7]이 같은 아이디어를 사용하여 사용자 간 동일한 키를 공유한다는 걸 증명하였다. 이를 프로토콜의 정확성이라 한다. Ding 등[3]과 Peikert [7]는 Z_q에서 $\{0, 1\}$로 가는 함수를 키 조정 메커니즘으로 사용하며 입력값의 범위에 따라 0과 1을 반환한다. 이와 달리 NewHope[6]은 다른 방식의 키 조정 메커니즘을 설계하는데 4장에서 자세히 다룬다.

III. 배경 지식

3.1 Closest vector problem

격자 기반 암호에서 어려운 문제로 알려져 있으며 그림 2와 같이 격자 L과 벡터 w가 주어져 있을 때 w와 가장 가까운 격자점 v를 찾는 것이다.

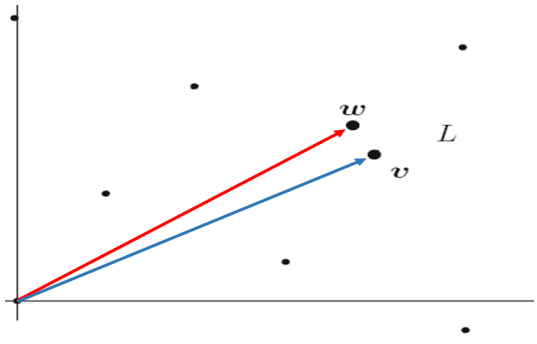

그림 2 Closest Vector Problem[8]

3.2 보로노이 셀

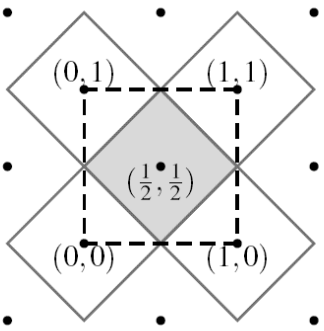

그림 3 보로노이 셀 [2]

보로노이 셀은 격자 L이 주어졌을 때 $V(L)=\{x\in R^n \mid \|x\|<\|x-v\| for\ all\ v\in L\}$로 정의하며 원점과의 거리가 다른 격자점보다 가까운 벡터들의 집합이다. 그림 3에서 원점을 중심으로 한 실선의 사각형이 보로노이 셀이다. 원점 외에 다른 격자점을 중심으로 할 수 있으며 그림 3의 회색 부분은 (1/2, 1/2)을 중심으로 한 보로노이 셀이다.

IV. 제안 알고리즘

본 장에서는 NewHope의 조정 메커니즘을 살펴보고 이를 ADGK19에 적용하여 ADGK19를 구체화한다.

4.1 NewHope의 조정 메커니즘

NewHope의 조정 메커니즘은 두 개의 함수 *HelpRec*과 *Rec*로 나뉘어진다. *HelpRec*은 벡터 $\mathbf{x}\in Z_q^4$와 $b\in\{0,1\}$를 입력을 받아 4차원 격자에서 벡터 $2^r/q\,(\mathbf{x}+b\mathbf{g})$와 가까운 격자점의 계수를 반환한다. 이때 r은 비트수를 나타내며 b는 *HelpRec* 결과값의 편향성을 없애기 위해 사용되며 벡터 $\mathbf{g}$는 $(1/2, 1/2, 1/2, 1/2)^T$이다. 즉, $HelpRec(\mathbf{x}, b)=CVP_{D_4}(2^r/q(\mathbf{x}+b\mathbf{g}))$로 정의할 수 있다. *Decode*는 입력값 벡터 $\mathbf{x_i}\in Z_q^4$와 *HelpRec*의 결과값 $\mathbf{r}\in Z_{2^r}^4$을 사용하여 $(1/2, 1/2, 1/2, 1/2)$의 보로노이 셀 포함 유무에 따라 {0, 1} 중 하나의 값을 반환한다.

4.2 제안 알고리즘

초기설정에서 NewHope과 동일하게 a를 무작위한 값으로 보이도록 하고 프로토콜이 실행될 때마다 새로 설정하여 백도어 공격과 로그잼과 같은 공격을 방지한다. 그림 1의 라운드 3과 키 계산 단계의 *recMsg*와 *recKey*는 NewHope의 *HelpRec*과 *Rec*을 적용하여 rec은 b_{N-1}과 가까운 격자점의 계수이다. 이때 HelpRec과 Rec의 입력 벡터는 4차원이고 b_{N-1}과 b_i는 R_q의 원소로 n차원 벡터이기 때문에 b_{N-1}, b_i를 $n/4$개의 벡터로 나누어 키 조정 메커니즘을 수행한다.

V. 프로토콜의 정확성 및 안전성

그러나 ADGK19과 NewHope에서 서로 다른 분포를 사용하기 때문에 프로토콜의 정확성과 안전성에 문제가 발생할 수 있다. 본 장에서 두 분포의 차이를 최대한 줄일 수 있는 표준편차를 찾아 ADGK19와 NewHope의 정확성과 안전성 증명 모두 적용하고자 한다.

ADGK19는 이산 가우시안 분포를 NewHope은 중앙화된 이항 분포(centered binomial distribution)을 사용한다. 중앙화된 이항 분포는 $\sum_{i=0}^{k-1}(b_i-b_i')$으로 정의한다. 이때 k는 샘플링 횟수로 NewHope과 같이 16으로 설정하며 b_i, b_i'은 1/2의 확률 0과 1의 값을 갖는다. 중앙화된 이항 분포를 다시 정리하면 $\sum_{i=0}^{15}b_i-\sum_{i=0}^{15}b_i'$이며 두 이항 분포의 차이로 볼 수 있다. 각 이항 분포를 기댓값과 분산이 각각 0과 4인 가우시안 분포로 근사한 후 차이를 보면 기댓값이 0이고 분산이 8인 가우시안 분포로 근사할 수 있다. 근사한 가우시안 분포와 중앙화된 이항 분포를 비교하면 그림 4와 같으며 차이가 거의 없음을 알 수 있다. 이산 가우시안 분포는 가우시안 분포를 따르므로 ADGK19와 NewHope에서 보인 정확도와 안전성 증명을 적용할 수 있다.

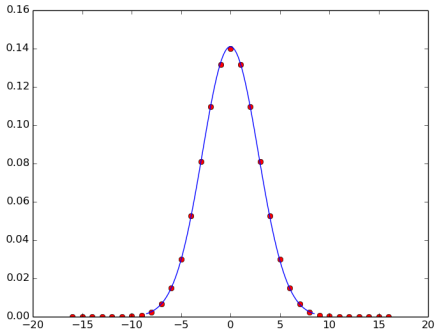

그림 4 가우시안 분포(파란색 선)과 중앙 화된 이항 분포(빨간점) 비교 그래프

VI. 결론 및 향후 과제

본 논문에서는 ADGK19에서 제안한 그룹 키 교환 프로토콜을 NewHope의 키 조정 메커니즘을 적용하여 구체화하였다. 또한 ADGK19과 NewHope은 서로 다른 분포를 사용하여 제안 프로토콜의 정확성과 안전성이 보장되지 않아 ADGK19와 NewHope에서 보인 정확성과 안전성을 동시에 만족하는 표준편차를 제안하였다.

최근 격자 기반 키 교환 프로토콜에 키 재사용 공격 [9-11]이 이루어지고 있으며 특히 [9]는 NewHope에 키 재사용 공격을 제안하였다. 향후 연구 과제로 [9]의 공격을 본 논문에 적용해보고 [13]에서 제안한 pasteurization 기법을 통해 키 재사용 공격 방지를 제안할 예정이다.

[참고문헌]

[1] 이나비, 김광조, 디지털 포렌식을 위한 Android 및 Windows 환경에서 카카오톡 메시지의 아티팩트 분석 (Ⅰ), 2019 정보보호학술발표회논문집 충청지부, 2019.

[2] D.Apon, D.Dachman-Soled, H.Gong, & J.Katz, Constant-round group key exchange from the Ring-LWE assumption, PQCRYPTO 2019, 2019.

[3] J.Ding, X.Xie, & X.Lin, A Simple Provably secure key exchange scheme based on the learning with errors Problem, IACR Cryptology ePrint Archive, 688, 2012.

[4] R. Choi & K. Kim, A novel non-interactive multi-party key exchange from homomorphic encryption, in ProvSec Workshop 2018, 2018.

[5] M.Burmester & Y.Desmedt, A secure and efficient conference key distribution system, In Workshop on the Theory and Application of Cryptographic Techniques (pp.275-286), Springer, 1994.

[6] E.Alkim, L.Ducas, T.Pöppelmann, & P.Schwabe, Post-quantum key exchange—a new hope, In 25th USENIX Security Symposium (pp. 327-343), 2016.

[7] C.Peikert, Lattice cryptography for the internet, In international workshop on post-quantum cryptography (pp. 197-219), Springer, 2014.

[8] J.Hoffstein, J.Pipher, & J.H.Silverman, An introduction to mathematical crypto graphy (Vol. 1), Springer, 2008.

[9] S.R.Fluhrer, Cryptanalysis of ring- LWE based key exchange with key share reuse, IACR Cryptology ePrint Archive, 85, 2016.

[10] J.Ding, S.Alsayigh, R.V.Saraswathy, S.Fluhrer, & X.Lin, Leakage of signal function with reused keys in RLWE key exchange, In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE, 2017

[11] C.Liu, Z.Zheng, & G.Zou, Key reuse attack on newhope key exchange protocol, In International Conference on Information Security and Cryptology (pp. 163-176). Springer, 2018.

[12] J.Ding, P.Branco, & K.Schmitt, Key exchange and authenticated key exchange with reusable keys based on RLWE assumption, IACR Cryptology ePrint Archive, 665, 2019.