정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

양자 키 분배 기술을 활용한 하이브리드 키 교환 방법

심 동 희*

요 약

본 논문에서는 표준화 기구에서 개발되었거나 아직 개발 중인, 양자 컴퓨팅에 의한 공격에 대해 안전한 양자 내성 보안 체계로의 전환을 위해 양자 키 분배 (Quantum Key Distribution - QKD) 기술을 암호키 교환에 활용하는 다양한 하이브리드 접근 방식 들을 살펴보았다. 이러한 방법들은 두 가지 이상의 서로 다른 키 교환 방법을 결합하는 '키 교환을 위한 하이브리드 접근 방식'들을 의미한다. 양자 키 분배(QKD) 네트워크에서 생성하는 대칭 키를 활용하여 다른 방식으로 생성된 암호키와의 다양한 방식의 결합을 통한 하이브리드 접근 방식의 호환성에 대해서 살펴보았고, 아울러 다양한 네트워크 계층의 보안 통신 프로토콜과 함께 QKD를 함께 사용할 수 있도록 하는 표준들을 함께 분석하였으며, 이러한 표준들에서 추가적으로 개발이 필요한 영역들을 함께 살펴보았다.

Ⅰ. 서 론

양자 컴퓨팅은 기존 및 미래 통신 네트워크의 보안에 심각한 위협으로 인식되고 있다. 양자 컴퓨터는 정수 인수분해(RSA 암호화 기반) 및 이산 로그(DH 키 공유 기반)와 같은 특정 계산 문제를 기존 컴퓨터보다 훨씬 빠르게 해결할 수 있어, 기존 암호체계에 심각한 위협이 되고 있다. 이에 대비해 기존 네트워크를 양자 내성(즉, 양자 컴퓨팅과 관련 알고리즘에 의한 공격에 대해 안전한 성질) 네트워크로 전환하는 것을 잘 준비해야 하는데 이는 상당한 노력이 필요한 복잡한 작업이다. 이러한 맥락에서 여러 표준화 기구가 양자 내성 보안 주제에 대한 표준을 개발했거나 개발 중에 있다. 특히 양자 내성 암호 알고리즘을 표준화 하고 있는 미국의 NIST는 PQC(Post Quantum Cryptography – 양자 내성 암호) 표준화 프로세스에 따라 2017년부터 양자 내성 공개 키 암호화 알고리즘을 평가하고 표준화하기 위한 표준화 활동을 진행 중에 있다.

ITU-T에서 보안 영역에 대한 표준화를 담당하고 있는 SG17(Study Group 17)은 QKDN(Quantum Key Distribution Network – 양자 키 분배 네트워크)에 대한 보안 요구 사항 및 관련 조치에 대한 표준화를 진행해 왔으며 X.1710 (19) 및 X.1714 [5]가 이를 통해 발간되었다. X.1710은 QKDN에 대한 보안 프레임워크(Framework)이며 QKDN에 대한 전반적인 요구 사항을 정의하였다. X.1714는 QKDN에서 암호화 응용 프로그램으로 키를 공급할 때 키를 조합하여 공급하는 방법과 이에 대한 보안 요구 사항을 정의하였다.

그러나 다음과 같이 몇 가지 보완 사항(gap)이 여전히 남아있다.

하이브리드 키 교환 방식에 대한 대부분의 표준화 활동은 PQC(Post Quantum Cryptography) 즉 양자 내성 암호 전문가에 의해 구상되고 진행되었다. 그 결과 표준이 이미 개발되었거나 또 개발 중인 표준이 QKD (Quantum Key Distribution – 양자 키 분배)와 호환되는지 여부가 QKD 프로토콜이 키 교환 프로토콜이라는 사실에도 불구하고 양자 내성 암호화 표준화 작업에 반영되지 않았다. 따라서, 키 교환을 위한 하이브리드 접근 방식은 적어도 QKD를 포함한 두 가지 다른 키 교환 방법을 결합하여 키 교환 기능을 수행하는 것을 고려할 수 있다. 그럼에도 불구하고 이러한 키 교환을 위한 하이브리드 접근 방식은 기존 표준을 기반으로 하는 QKD에 바로 적용되지 않을 수는 있을 것이다. 이에 대해 현재 진행되고 있는 다양한 표준화 활동과 더 추가되어야 할 요소들을 이 논문에서 분석해 본 것이다.

이러한 격차를 극복하기 위해 기존 통신 네트워크에서 QKD를 활용하여 보안을 향상시키려는 다양한 노력

* SK텔레콤 혁신사업TF (팀장, donghee.shim@sk.com)

이 이루어져 왔다. 많은 연구에서 다음과 같이 QKD를 OSI 모델의 다양한 계층에서 작동하는 프로토콜과 통합하고자는 노력들이 진행되어 왔다.

광통신망에서 QKD의 사용은 최근 몇 년 동안 크게 발전했지만 다른 OSI 계층 내에서 QKD를 적용하는 연구 및 개발은 아직 초기 단계에 있다. QKD는 공유 비밀 키를 설정하므로 적절한 사용 사례에서 다른 대칭 키 프리미티브(primitive)를 잠재적으로 대체할 수 있다. OTN(Optical Transport Network - 광 전송 네트워크)과 같은 물리적 계층에서의 구현과 비교할 때 상위 계층의 프로토콜은 암호화 프리미티브(primitive)의 교체를 허용하도록 설계되었을 가능성이 더 크기 때문이다.

이러한 연구 노력의 예로는 링크 계층(즉, OSI 2계층)에서 QKD 점대점 프로토콜(PPP – Point to Point)[2] 및 MACsec[1]과 QKD의 통합 사례가 있다. 네트워크 계층(즉, OSI 3계층)에서는 IPsec[3]에서 QKD를 사용하는 것을 연구하였다. 또한 SSL/TLS[4]와 전송 계층(즉, OSI 4계층)에서 QKD와의 통합이 시도되었다.

좀 더 자세히 살펴보면, 데이터 링크 계층에서 QKD는 두 노드를 연결하는 데이터 링크 프로토콜인 PPP의 키 교환 프로토콜로 사용할 수 있다[2].

MACsec(Medium Access Control security)은 이더넷 링크의 보안 통신을 위한 IEEE 802.1AE 표준[18]이다. MACsec은 근거리 통신망에서 이더넷 프레임의 기밀성, 무결성 및 원본 신뢰성을 보장한다. MACsec의 비밀성은 사전 공유 키로 구성되거나 상호 인증 프로토콜에서 파생된 루트 키에서 비롯된다. QKD는 보안 이더넷 네트워크를 위한 MACsec에서 사용할 수 있다[1].

네트워크 및 전송 계층의 경우 IPsec(인터넷 프로토콜 보안) 및 TLS(전송 계층 보안) 모두 Shared Secret을 계산한 다음 이를 사용하여 암호화 및 무결성 보호를 위한 키를 계산한다.

IPsec은 IP 데이터 패킷을 인증 및 암호화하여 네트워크 계층에서 IP 통신에 보안을 제공하는 프로토콜 들의 세트이다. IPsec은 두 위치 간에 또는 원격 장치와 기업 네트워크 간에 VPN(가상 사설망)을 제공하는 데 자주 사용된다. IPsec은 종단 간 보안도 제공할 수 있다. IKE(인터넷 키 교환)는 IPsec 프로토콜 제품군에서 보안 연결을 설정하는 데 사용되는 프로토콜이다. IKE는 DH(Diffie-Hellman) 공개 키 교환을 사용하여 암호화 키가 파생되는 공유 세션 secret을 설정한다. 공개 키 기술 또는 사전 공유 키 (pre-shared key)는 통신 당사자들을 상호 인증하는 데 사용된다.

TLS(전송 계층 보안)는 네트워크 통신 서비스에 종단 간 보안을 제공하는 전송 계층 프로토콜이다. TLS는 이전 SSL(Secure Sessions Layer) 프로토콜을 기반으로 하며 애플리케이션에서 호출한다. 다양한 응용 프로그램에서 널리 사용되지만 가장 일반적인 용도는 웹 서버와 브라우저 간의 트래픽을 암호화하는 것이다. QKD 키는 TLS 세션의 Shared Secret로도 사용할 수 있다. 이 경우 QKD 키는 DH(Diffie-Hellman) Shared Secret을 대체하므로 DH Shared Secret을 계산할 필요가 없다[4].

본 논문에서는 표준화 기구에서 개발되었거나 아직 개발 중인, 양자 컴퓨팅에 의한 공격에 대해 안전한 양자 내성 보안체계로의 전환을 위해 양자 키 분배(Quantum Key Distribution - QKD) 기술을 암호키 교환에 활용하는 다양한 하이브리드 접근 방식 들을 살펴보았다. 이러한 방법들은 두 가지 이상의 서로 다른 키 교환 방법을 결합하는 '키 교환을 위한 하이브리드 접근 방식'들을 의미한다. 양자 키 분배(QKD) 네트워크에서 생성하는 대칭 키를 활용하여 다른 방식으로 생성된 암호키와의 다양한 방식의 결합을 통한 하이브리드 접근 방식의 호환성에 대해서 살펴보았고, 아울러 다양한 네트워크 계층의 보안 통신 프로토콜과 함께 QKD를 함께 사용할 수 있도록 하는 표준들을 함께 분석하였으며, 이러한 표준들에서 추가적으로 개발이 필요한 영역들을 함께 살펴보았다.

Ⅱ. 키 교환 방법을 위한 하이브리드 접근 방식표준화 활동 개요

이 절은 키 교환 메커니즘에 대한 하이브리드 접근 방식에 대한 다양한 표준화 기구의 활동을 살펴보았다.

2.1. 키 교환을 위한 하이브리드 접근 방식을 다루는 표준

'키 교환을 위한 하이브리드 접근 방식'은 표준에 명시된 암호화 메커니즘으로 이해해야 하며 둘 이상의 키 교환 방법으로 인해 암호화 키를 설정할 수 있다.

2.1.1. ITU-T X.1714

ITU-T X.1714 [5]는 QKDN에 대한 키 조합 방법을 설명하고 키 조합과 QKDN에서 암호화 응용 프로그램으로의 키 공급에 대한 보안 요구 사항을 정의한다. 특히 이 권고안(Recommendation)는 다음 사항을 다룬다.

- QKDN을 통해 교환된 키와 다른 키 교환 방법을 통해 교환된 키 조합에 대한 보안
- QKDN에서 암호화 애플리케이션으로의 키 공급 보안

2.1.2. ETSI TS 103 744 양자 내성을 지닌 하이브리드 키 교환

유럽 표준화 기구에는 CEN, CENELEC 및 ETSI 등의 세 기구가 있으나, 본 논문 작성 시점에 ETSI Technical Committee 중의 하나인 CYBER QSC에서만 하이브리드 접근 방식에 대한 표준화 활동을 확인할 수 있었다.

ETSI TC CYBER QSC는 2020년 12월 양자 내성 하이브리드 키 교환에 대한 Technical Specification(기술 규격)인 TS 103 744[6]을 발표했다. 이 기술 규격은 여러 Shared Secret에서 암호화 키를 유도하는 두 가지 방법을 지정하여 키 교환에 대한 하이브리드 접근 방식의 개념을 다루고 있다. 이러한 Shared Secret은 양자 내성 또는 비 양자 내성 암호화 방법 또는 pre-shared Secret을 설정하는 다른 방법을 사용하여 설정할 수 있다.

TS 103 744 [6]는 키 합의 방식 중 하나가 NIST SP 800-56Ar3[7]의 5.7.1.2절에 정의된 타원 곡선 Diffie-Hellman이어야 한다고 지정하였다. 이 표준은 예를 들어, 해시 함수, 의사 난수 함수 또는 키 파생 함수 등의 몇 가지 암호 primitive 알고리즘을 정의하고 있다.

TS 103 744에서는 두 가지 유형의 하이브리드 키 합의 방식을 지정하고 있다. 첫 번째 방식은 '연결 하이브리드 키 합의 방식 (concatenate hybrid key agreement scheme)'이고 다른 하나는 '캐스케이드 하이브리드 키 합의 방식(cascade hybrid key agreement scheme)'이다.

첫 번째 방법은 모든 주요 합의 방법을 병렬로 실행하는 것으로 구성된다. 개시자(initiator)와 응답자(responder) 사이에 교환되는 메시지는 하이브리드 키 합의 방식의 각 단계에서 각 키 합의 방식에 의해 생성된 메시지를 연결한 결과이다. 또한, 키 유도 기능의 입력으로 사용되는 shared secret은 각 키 합의 방식으로 설정된 secret과 하나의 선택적 사전 공유 키(pre-shared key)를 연결한 결과이다.

두 번째 방식은 키 합의 방식을 순차적으로 실행하는 방식이다. 이 경우 개시자(initiator)와 응답자(responder) 사이에 교환되는 각 메시지는 주요 합의 방식 중 하나의 특정 단계와 관련된다. 최종 키 재료(key material)는 하이브리드 키 합의 방식을 구성하는 키 합의 방식의 수만큼 키 유도 함수를 반복하여 적용해서 계산된다. 키 유도 함수(key derivation function)의 각 반복 결과는 secret과 일부 키 재료(key material)이다. i번째 반복의 입력 secret은 i번째 키 합의 방식에 의해 교환된 secret과 (i-1)번째 반복에서 계산된 secret로 얻어진다. 첫 번째 계산에서 입력 secret은 첫 번째 키 합의 방식에 의해 교환된 secret과 pre-shared secret에서 얻을 수 있다.

TS 103 744는 첫 번째 방식(concatenate hybrid key agreement scheme) 및 두 번째 방식(cascade hybrid key agreement 방식)에 대한 pre-shared secret으로 QKD를 이용한 이전 세션 (previous session) 또는 대체 키 설정 방법으로 생성된 키를 사용할 수 있음을 나타내고 있다.

참고로, ETSI TS 103 744를 개정하기 위해 2021년 6월 TC CYBER QSC에서 새 표준화 과제를 시작한 바 있다.

2.1.3. NIST SP800-133r2

NIST에는 하이브리드 키 교환 전용 표준이 현재 없는 상태이다. 그러나 NIST는 여러 대칭 키 또는 값(value)(NIST SP800-133r2[8])에서 대칭 키를 안전하게 생성하기 위한 다양한 옵션과, 다양한 키 교환 방식에 의해 설정된 여러 secret을 결합하는 한 가지 방법에 대한 권장 사항을 제공하고 있다[9].

NIST SP800-133r2[8]는 암호화 키 생성을 위한 권장 사항이다. 이 권장 사항의 두 번째 개정은 2020년 6월에 완료되었다. 이 문서의 6.3절은 (다중) 키와 기타 데이터를 결합하여 생성된 대칭 키 규격으로, 이 6.3절에 설명된 조합 방식은 여러 키 교환에 의해 설정된 키에서 대칭 키를 생성하는 역할을 할 수 있다.

NIST SP800-133r2[8]의 맥락에서 ‘키’는 NIST에서 승인한 키 교환 체계에 의해 설정된 암호화 키를 의미한다. 반면에 ‘기타 데이터’는 secret일 수도 있고 아닐 수도 있는 문자열이다. 특히 ‘기타 데이터’는 모든 양자 내성 암호화 알고리즘 또는 QKD를 기반으로 하는 것과 같이 NIST에서 승인하지 않은 키 교환 방식으로 설정된 키일 수 있다.

NIST에서는 키와 기타 데이터의 조합에서 대칭 키를 생성하기 위해 세 가지 방법을 권장한다. 결합된 키 및 기타 데이터에 대한 중요한 요구 사항은 이들이 서로 독립적이라는 것이다.

1. 첫 번째 방법은 두 개 이상의 키를 연결하는 것이다. 생성된 키의 길이는 연결된 키의 길이의 합과 같다. 참고로, 이 방법은 다른 데이터(예: 승인되지 않은 키 교환 방법으로 교환된 키)의 사용을 허용하지 않는다.

2. 두 번째 방법은 배타적 논리합(XOR)으로 생성된 키와 데이터 항목으로 구성된다. 입력으로 사용되는 각 키 또는 항목의 길이는 배타적 논리합으로 생성되는 대칭 키에서 필요한 길이와 동일해야 한다.

3. 세 번째 방법은 키 추출 프로세스로 구성된다. 최종 대칭 키는 (다중) 키와 다른 데이터의 연결에 HMAC 함수를 적용한 결과이다. 해시 결과는 필요한 키 길이와 동일한 길이로 최종 키를 생성하기 위해 잘려질(truncated) 수 있다.

2.1.4. NIST SP800-56Cr2

NIST SP800-56Cr2[9]는 키 설정 체계에서 키 파생 방법에 대한 권장 사항이다. 이 권고의 2차 개정은 2020년 8월에 완성되었다. 2절은 문서의 범위와 목적에 관한 것이다. 2절의 한 단락은 키 파생 방법에 대한 입력으로 사용할 수 있는 하이브리드 shared secret의 구조를 소개한다.

이 표준은 NIST가 승인한 secret 생성 체계를 사용하여 설정한 Z라고 하는 shared secret과 다른 방법을 사용하여 설정한 T라고 하는 보조 shared secret을 연결한 결과인 Z’라고 하는 하이브리드 shared secret의 사용을 허용한다. SP800-56Cr2 프로세스 Z’에 지정된 키 파생 방법은 Z와 동일한 방식으로 처리된다. 이는 두 가지 다른 secret 생성 방법을 사용하여 만들어진 secret에서 암호 키를 파생할 수 있음을 의미한다. 참고로, NIST SP800-56Cr2[9]에서는 보조 shared secret T를 생성하는 데 사용할 수 있는 방법에 제한이 없다.

2.1.5. BSI TR-02102-1 표준 (독일)

BSI는 하이브리드 키 교환을 위한 표준을 제정한 바 없다. 그러나 BSI는 양자 내성 암호화 키 교환(BSI TR-02102-1[10]) 사용을 위한 한 가지 옵션에 대한 권장 사항을 제공한다.

BSI TR-02102-1[10]은 BSI가 선택한 암호화 메커니즘에 대한 보안 및 장기 지향성 (long-term orientation)을 평가하는 기술 가이드라인이다. 이 가이드라인의 버전 2022-01은 2022년 1월에 완료되었다. 3.2절은 양자 내성 암호화에 대한 기술 설명 및 권장 사항을 제공한다. 또한 기존 보안과 PQC(Post Quantum Cryptography – 양자 내성 암호) 보안의 조합에 대해 설명하고 있다.

BSI TR-02102-1에서는 고전적인 ECC 또는 RSA 기반 키 교환 또는 키 전송과 결합된 경우에만 양자 내성 암호화 알고리즘을 사용할 것을 권장한다. 하나의 고전적인 키 생성 방법으로 생성된 secret은 동일한 문서의 섹션 B.1.1에 지정된 키 유도 방법을 사용하여 하나의 양자 내성 키 생성 방법으로 생성된 secret과 결합되어야 한다.

2.2. 프로토콜에서 키 교환을 위한 하이브리드 접근 방식을 허용하는 표준

‘프로토콜에서 키 교환을 위한 하이브리드 접근 방식’은 표준에 지정된 특정 프로토콜의 변형으로 이해해야 하며 둘 이상의 키 교환 방법으로 암호화 키를 설정할 수 있다.

하이브리드 접근 방식의 개념을 도입하는 ISO, IEC 또는 ITU 내에서 제정되었거나 연구 중인 표준은 아직 없는 상태이다.

2.2.1. IETF RFC 8784

IETF RFC 8784[11]는 양자 내성 보안을 위해 인터넷 교환 프로토콜 버전 2(IKEv2)에서 사전 공유 키를 혼합하기 위한 IETF 표준이다. 이 IETF 표준은 2020년 6월에 제정되었다. 이 문서는 IKEv2가 사전 공유 키를 사용하여 대체 키 교환 메커니즘을 활용할 수 있도록

하는 확장에 대해 설명하고 있다.

IETF RFC 8784[11]는 각 IKE peer가 양자 내성을 지닌 양자 키 교환 방법을 사용하여 공유된 키들의 목록과 이를 구분할 수 있는 관련 식별자들을 가지고 있다는 가정 하에 작성되었다. 그런 다음 IETF RFC 8784는 개시자(initiator)와 응답자(responder)가 IKEv2 transaction에서 사전 공유 키를 사용하거나 사용하지 않도록 허용하는 알림을 도입한다. 사전 공유 키를 사용하지 않기로 하는 결정은 프로토콜의 여러 단계에서 두 당사자 중 하나가 내릴 수 있다. 이 경우 개시자(initiator)와 응답자(responder)는 기존의 IKEv2 프로토콜을 사용한다. 미리 공유한 키를 사용하는 경우 IETF RFC 7296[12]에 지정된 기존 IKEv2 프로토콜에서 생성된 3개의 하위 키와 결합된다. 사전 공유 키와 하위 키의 조합은 의사 난수 함수로 수행된다. 참고로 IETF RFC 8784[11]는 pre-shared secret을 교환하는 데 사용할 수 있는 키 교환 방법을 지정하지 않고 있다.

2.2.2. IETF draft-ietf-ipsecme-ikev2-multiple-ke-05

draft-ietf-ipsecme-ikev2-multiple-ke-05[13]는 IKEv2의 다중 키 교환을 위한 IETF 초안으로, 이 논문을 작성할 시점에, 해당 IETF draft의 다섯 번째 초안은 2022년 9월에 만료될 예정이다. 이 문서에서는 보안 연결 설정 중에 shared secret을 계산하는 동안 다중 키 교환을 허용하는 IKEv2의 확장에 대해 설명하고 있다.

draft-ietf-ipsecme-ikev2-multiple-ke-05[13]은 IETF RFC 7296[12]에 명시된 Diffie-Hellman 키 교환 방법 외에 대체 키 교환 방법을 사용할 수 있는 가능성을 제공하도록 IETF RFC 7296를 업데이트하는 것을 목표로 한다. 서로 다른 키 교환 방법이 연속적으로 수행되는데, 각 키 교환에서 설정된 secret은 Diffie-Hellman 키 교환으로 설정된 shared secret이 IETF RFC 7296에서 사용되는 방식과 동일한 방식으로 사용될 shared secret을 생성하기 위해 결합된다. n번째 키 교환으로 생성된 secret은 의사 난수 함수를 사용하여 (n-1)번째 키 교환에서 생성된 중간 키와 결합된다.

2.2.3. IETF draft-campagna-tls-bike-sike-hybrid-07

draft-campagna-tls-bike-sike-hybrid-07[14]은 TLS (전송 계층 보안 1.2)용 하이브리드 PQ KEM(양자 내성 키 캡슐화(encaptulation) 방법)을 위한 IETF 초안이다. 이 문서는 독립적인 실험이 상호 운용될 수 있도록 충분한 세부 사항을 하이브리드 키 교환에서 정의하기 위한 것이다.

draft-campagna-tls-bike-sike-hybrid-07[14]은 TLS 버전 1.2 (IETF RFC 5246[15])에 적용 가능한 양자내성을 지닌 하이브리드 키 교환을 지원하기 위한 TLS 추가 사항에 대해 설명하고 있다. 정의된 하이브리드 키 교환은 두 가지 키 교환 방법에 의해 설정된 shared secret을 결합한다. 키 교환 방법 중 하나는 ECDHE(Elliptic-Curve Diffie-Hellman Ephemeral)를 기반으로 한다. 다른 하나는 BIKE, Kyber 또는 SIKE를 기반으로 할 수 있다. 이 세 가지 알고리즘은 양자 컴퓨터 공격에 강한 NIST 키 교환 알고리즘의 3차 표준화 프로세스의 일부이다. TLS 1.2 [14] premaster secret의 역할을 하는 하이브리드 premaster secret은 두 개의 shared secret을 연결한 결과이다.

Ⅲ. 양자 키 분배 네트워크에서 제공하는 키와 하이브리드 키 교환 방식의 호환성 분석

이 절은 QKD 네트워크에서 제공하는 키와 2절에서 식별된 키 교환에 대한 하이브리드 접근 방식의 호환성 및 갭 분석을 다루었다.

3.1. 키 교환을 위한 하이브리드 접근 방식의 개념을 다루는 표준

3.1.1. 개요

하이브리드 키 교환 구현을 위한 암호화 메커니즘을 지정하는 여러 표준이 최근에 발표되었거나 아직 연구 중이다. 이러한 표준은 주로 현재 사용되는 암호화 알고리즘(예: Diffie-Hellman)을 양자 컴퓨팅에 대해 강력한 것으로 간주되는 새로운 암호화 알고리즘과 결합하기 위한 목적으로 작성된 것이다. QKD 기술은 양자 컴퓨팅 위협에서 안전한 방식으로 키를 교환하는 훌륭한 대안이나, 키 교환 암호화 알고리즘과 QKD 기술의 조합은 이전에 설명한 키 교환에 대한 하이브리드 접근 방식의 개념을 다루는 표준에서 항상 언급되는 것은 아니다.

아래에서 QKD 키 및 해당 표준과 기술의 호환성을 분석한다. 일부 비호환성이 있는 경우 호환성을 위해 어

떠한 추가적인 표준화가 필요한지 함께 분석해 보았다.

3.1.2. ETSI TS 103 744, 양자 내성 하이브리드 키 교환

ETSI TS 103 744[6]는 양자 내성 키 교환과 관련하여, 가능한 키 설정 방법 중 하나로 QKD를 언급하는 국제 표준이다. 하이브리드 키 합의 체계는 공개 키를 사용하는 키 교환 메커니즘을 사용하고 QKD는 이러한 종류의 암호화 메커니즘에 속하지 않는다고 가정한다. 그러나 키 유도 함수(key derivation function)는 선택적인 pre-shared secret을 사용하며, pre-shared secret 키를 위한 키 생성 방법으로 QKD가 언급되고 있다.

QKD는 하이브리드 키 생성 체계 내에서 지정된 통신의 일부로 개시자(initiator)와 응답자(responder) 간에 shared secret을 설정하는 데 사용할 수 없다. 그러나 QKD 키를 pre-shared secret 키로 사용하여 ETSI TS 013 744에 따른 공개 키 방법의 키와 결합할 수 있다. 이 제한은 QKD 키를 사용하는 응용 프로그램과 QKD 네트워크 간의 상호 운용성에 큰 영향을 미치지는 않는다. 실제로 QKD는 일반적으로 기존 통신 채널 외에 양자 채널을 사용하여 보안 응용 프로그램에서 대역 외 키를 설정하는 양자 내성 키 설정 메커니즘이기 때문이다.

요약하면, ETSI TS 103 744는 주로 양자 내성을 지니는 공개 키 교환 메커니즘을 위해 설계되었다. 그러나 하이브리드 키 합의 체계에서 사용하기 위해 pre-shared secret 키를 설정하는 하나의 옵션으로 QKD를 사용할 수 있다.

3.1.3. NIST SP800-133r2

NIST SP800-133r2[8]는 승인되지 않은 (not-approved) 키 교환 메커니즘으로 계산된 비밀 키의 사용을 허용하는 방식으로 작성된 미국 표준이다. 이 경우 이러한 비밀 키를 '기타 데이터'라고 한다. NIST는 이 '기타 데이터'가 secret일 수도 있고 아닐 수도 있다고 간주한다. 승인된 키 교환 메커니즘으로 설정된 비밀 키를 NIST 표준에서 '키'라고 불린다. QKD 기술은 NIST에서 승인되지 않은 (not-approved) 키 교환 메커니즘으로 간주될 수 있다. 따라서 QKD 키는 NIST SP800-133r2를 구현할 때 '기타 데이터' 역할만 할 수 있다.

참고로 NIST 표준의 맥락에서 '승인된(approved)' 알고리즘 또는 기술은 1) FIPS(연방 정보 처리 표준) 또는 NIST 권장 사항에 지정되거나 2) FIPS 또는 NIST 권장 사항에 채택된 알고리즘 또는 기법을 의미한다.

NIST SP800-133r2의 6.3절에 명시된 두 번째 및 세 번째 방법만이 '기타 데이터'의 사용을 허용한다. 두 번째 방법은 결과 키를 생성하기 위해 모든 키와 기타 데이터를 배타적 논리합으로 구성하는 것이다. 세 번째 방법은 모든 키와 기타 데이터의 연결로 구성된 secret에서 결과 키를 추출하는 것으로 구성된다. 두 경우 모두 키와 기타 데이터가 동일한 방식으로 사용된다.

요약하면 NIST SP800-133r2에 지정된 두 가지 방법을 통해 QKD 기술을 사용하여 최소한 하나의 승인된(approved) 키 교환 메커니즘과 함께 양자 내성 하이브리드 키 교환을 구현할 수 있다.

3.1.4. NIST SP800-56Cr2

NIST SP800-56Cr2[9]는 두 가지 주요 파생 방법을 지정하는 미국 표준이다. 이러한 방법은 여러 shared secret을 연결한 shared secret에 적용할 수 있다. 이 NIST 표준은 승인되지(approved) 않은 방법으로 설정된 '보조 비밀(auxiliary secret)'이라는 shared secret의 사용을 허용하는 방식으로 작성되었다. NIST에서 승인한(approved) shared secret 설정 방법은 NIST SP800-56A 및 SP 800-56B에 지정되어 있다.

QKD 기술은 NIST SP800-56A 및 SP800-56B에서 제공하는 사양과 일치하지 않는다. 따라서 QKD 키는 '보조 비밀(auxiliary secret)'로만 사용할 수 있다. '보조 비밀(auxiliary secret)'은 NIST SP800-56Cr2의 'shared secret'과 같은 방식으로 취급된다.

요약하면 NIST SP800-56Cr2를 구현하면 QKD 키를 '보조 비밀(auxiliary secret)'로 사용할 수 있다. 이를 통해 shared secret 설정에 대해 승인된(approved) 방법이 하나 이상 사용되는 한 QKD 기술을 사용하여 양자 내성 하이브리드 키 교환을 구현할 수 있다.

3.1.5. BSI TR-02102-1 표준 (독일)

BSI TR-02102-1[10]은 BSI가 승인한 하이브리드 키 교환 메커니즘 및 양자 내성을 포함한 키 교환 메커니즘을 지정하는 독일 기술 가이드라인이다. QKD 기

술은 현재 버전에서 승인된 양자 내성 키 교환 메커니즘의 일부가 아니지만 BSI는 필요한 전제 조건이 충족되면 중기적으로 프로토콜, 인증 및 QKD 사용에 대한 권장 사항을 만들 계획이라고 언급하고 있다. 또한, 이 기술 가이드라인은 승인된 키 교환 메커니즘을 통해 교환된 키와 승인되지 않은 키 교환 메커니즘을 통해 교환된 다른 키를 결합하는 옵션을 제공하지 않는다.

요약하면, BSI TR-02102-1은 QKD 기술을 사용한 양자 내성 하이브리드 키 교환의 구현을 아직 허용하지 않고 있다. 이 상황은 BSI가 QKD 기술을 키 교환 메커니즘에 대한 하나의 옵션으로 승인하지 않는 한 달라지지 않을 가능성이 있다.

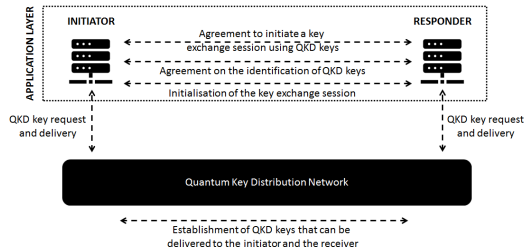
3.2. 프로토콜에서 키 교환을 위한 하이브리드 접근 방식을 허용하는 표준

3.2.1. 개요

QKD 기술과 키 교환 프로토콜의 호환성은 QKD 키가 대역 외 방식으로 응용 프로그램 간에 설정되기 때문에 연구하기가 더 복잡하다. 실제로 QKD 키는 QKDN 내에서 교환된 다음 이 QKDN에서 응용 프로그램으로 네트워크 노드들에 의해 전달된다.

키 교환 프로토콜 내에서 QKD 키 사용을 허용할 때 고려해야 하는 일반적인 단계를 그림 1에 도시하였다.

그림 1에 표시된 응용 프로그램 계층에서 개시자(initiator)는 키 교환 프로토콜을 통해 응답자(responder)와 키를 교환하는 것을 목표로 한다. 개시자(initiator)와 응답자(responder)가 프로토콜에서 QKD 키를 사용하려면 키 교환 세션을 시작하기 전에 QKD 키 사용 및 이러한 QKD 키 식별에 동의해야 한다. QKDN은 애플리케이션의 요청과 일치하는 QKD 키를



〔그림 1〕 키 교환 프로토콜 내에서 QKD 키 사용을 허용할 때 고려해야 할 일반적인 단계

설정하고 이러한 키를 애플리케이션에 전달하는 역할을 한다. 다음의 호환성 평가는 그림 1에서 식별된 프로토콜 단계를 기반으로 수행되었다.

3.2.2. IETF RFC 8784

IETF RFC 8784[11]는 양자 내성을 가진 보안을 위해 인터넷 교환 프로토콜 버전 2(IKEv2)에서 pre-shared 키를 혼합하기 위한 IETF 표준이다. IETF RFC 8784의 3절은 양자 내성을 지닌 pre-shared키 사용에 대한 알림을 지정한다. 이러한 알림은 개시자(initiator)와 응답자(responder) 간에 교환된다. 응답자(responder)의 알림에 따라 애플리케이션은 표준 IKEv2 프로토콜을 사용하거나 양자 내성을 지닌 pre-shared 키와 함께 IKEv2의 변형을 사용하기로 결정할 수 있다. 후자의 경우 개시자(initiator)는 양자 내성을 지닌 pre-shared 키의 식별자에 대한 알림을 응답자(responder)에게 보낸다. 양자 내성을 지닌 pre-shared 키를 Diffie-Hellman 교환(IETF RFC 7296[12]에 지정된 대로)으로 교환된 secret과 혼합하는 방법도 3절에 지정되어 있다.

그러나, 사전 공유 키를 교환하는 방법은 정의되어 있지 않다. 따라서 QKD는 이 표준에서 지원하는 하나의 옵션일 것이다. 그러나 IETF RFC 8784에서 제안하는 방법은 미리 공유된 키와 미리 공유한 키 식별자의 고정 목록으로 구성된 개시자(initiator) 및 응답자(responder)에 국한된다. 이 표준은 사전 공유 키의 동적 변경을 다루지 않고 있다.

요약하면 IETF RFC 8784를 사용하면 IKEv2 프로토콜에서 QKD 기술을 사용할 수 있다. 그럼에도 불구하고 QKD 기술은 응용 프로그램 간에 양자 내성을 지닌 사전 공유 키 및 키 식별자의 고정 목록을 생성하는 한 가지 방법으로만 사용할 수 있다.

3.2.3. IETF draft-ietf-ipsecme-ikev2-multiple-ke-05

draft-ietf-ipsecme-ikev2-multiple-ke-05[13]는 IKEv2의 다중 키 교환을 위한 IETF 초안 (IETF draft)이다. 특히 3.2.1절에는 개시자(initiator)와 응답자(responder)가 지원하는 대체 키 교환 방법을 알리는 알림을 지정한다. 이러한 알림은 개시자와 응답자 간에 교환된다. 개시자와 응답자가 하나 이상의 대체 키 교환 방법에 동의하면 3.2.2절에 지정된 대로 이러한 대체 키

교환 방법이 Diffie-Hellman 교환(IETF RFC 7296[12]에 지정된 대로)과 혼합된다.

대체 키 교환 방법은 [IETF draft-ietf-ipsecme-ikev2-multiple-ke-05]에 지정되어 있지 않으며 다른 표준에 의해 지정되어야 한다. 이는 QKD 기술을 IETF RFC 7296(즉, 표준 IKEv2)의 잠재적 업데이트에서 대체 키 교환 방법에 대한 가능한 옵션 중 하나로 간주할 수 있다. 이 가능성을 구체화하려면 응용 프로그램이 QKDN에 QKD 키를 요청하고 수신하는 방법에 대한 표준에 따라야 한다. 이러한 표준으로는 애플리케이션과 QKDN 간의 QKD 키 인터페이스를 지정하는 공개된 표준 중 하나인 ETSI GS QKD 014[16] 및 ETSI GS QKD 004[17]가 있다.

3.2.4. IETF draft-campagna-tls-bike-sike-hybrid-07

draft-campagna-tls-bike-sike-hybrid-07[14]은 TLS (전송 계층 보안 1.2)(IETF RFC 5246[15])에 대한 하이브리드 PQ KEM(양자 내성 키 캡슐화(encaptulation) 방법)을 설명하는 IETF 초안(IETF draft)이다. 이 IETF 초안은 표준 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘과 함께 세 가지 양자 내성 키 캡슐화 메커니즘 BIKE, Kyber 및 SIKE 중 하나를 사용할 수 있는 TLS 1.2 확장을 제안한다. 하이브리드 접근 방식은 ECDH와 교환된 secret의 연결(concatenation)과 선택한 양자 내성 키 캡슐화 메커니즘과의 키 교환으로 구성된다.

draft-campagna-tls-bike-sike-hybrid-07[14]의 목적은 서로 다른 실험 간의 상호 운용성을 제공하는 것이므로 제안된 확장의 모든 세부 사항이 잘 지정되어 있다. QKD 기술은 선택되어진 양자 내성 키 교환 방법의 일부가 아니므로 IETF draft-campagna-tls-bike-sike-hybrid-07은 QKD 키와 호환되지 않는다. 그럼에도 불구하고 이 IETF 초안은 QKD 키를 사용할 수 있는 가능성을 제공할 수 있는 향후 TLS 확장 개발의 예가 될 수 있다. 한 가지 방법은 IETF draft-campagna-tls-bike-sike-hybrid-07[14]에서 지원되는 양자 내성 키 교환 중 하나로 QKD 기술을 도입하는 것이다. 이를 위해 응용 프로그램이 QKDN에 QKD 키를 요청하고 수신하는 방법에 대한 표준을 준용하는 개발이 선행되어야 한다.

Ⅳ. 결 론

양자암호기술은 본격적으로 생태계가 형성되어 가고 있으며, 그 기술의 상용화가 빠르게 진행되어 한국의 SK텔레콤을 필두로 유럽, 미국의 다수 사업자가 실제 통신망에 적용하고 있다. 보다 많은 장비업체들 그리고 서비스업체들이 양자암호기술을 적용하고 상호보완성을 보장하기 위해 표준화가 함께 진행되고 있으며, 기존의 암호체계와의 연동이 중요한 이슈로 부각되고 있다. 본 논문에서는 표준화 기구에서 개발되었거나 아직 개발 중인, 양자 컴퓨팅에 의한 공격에 대해 안전한 양자 내성 보안체계로의 전환을 위해 양자 키 분배 (Quantum Key Distribution - QKD) 기술을 암호키 교환에 활용하는 다양한 하이브리드 접근 방식 들을 살펴보았다. 이러한 다양한 표준화 활동을 통해 양자암호통신 업계가 보다 성숙해 지고 보다 다양한 서비스들이 도출될 것으로 기대된다.

참 고 문 헌

[1] Joo Yeon Cho, ‘Using QKD in MACsec for secure Ethernet networks’, IET Quantum Communication, 2021

[2] Solange Ghernaouti-Hélie, Mohamed Ali Sfaxi, ‘Upgrading PPP security by Quantum Key Distribution’, International Conference on Network Control and Engineering for QoS, Security and Mobility Netcon 2005, Lannion, France

[3], Solange Ghernaouti-Hélie et al, “Using Quantum Key Distribution within IPSEC to secure MAN communications”. MAN 2005 conference

[4] Alan Mink et al., ‘Quantum Key Distribution and Commodity Security Protocols: Introduction and Integration’, International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009

[5] [ITU-T X.1714], ITU-T Recommendation X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks*.

[6] ETSI TS 103 744, Technical Specification TS 103 744 (2020), *CYBER; Quantum-safe Hybrid Key*

Exchanges (2020)

[7] NIST SP 800-56Ar3, NIST Special Publication 800-56A Revision 3(2018), *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.*

[8] NIST SP800-133r2, NIST Special Publication 800-133 Revision 2 (2020), *Recommendation for Cryptographic Key Generation*.

[9] NIST SP800-56Cr2, NIST Special Publication 800-56C Revision 2 (2020), *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.

[10] BSI TR-02102-1, BSI Technical Guideline TR-02102-1 (2022), *Cryptographic Mechanisms: Recommendations and Key Lengths*.

[11] IETF RFC 8784, IETF Standard RFC8784 (2020), *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*.

[12] IETF RFC 7296, IETF Standard RFC7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2)*.

[13] IETF draft-ietf-ipsecme-ikev2-multiple-ke-05, IETF draft standard draft-ietf-ipsecme-ikev2-multiple-ke-05 (2021), *Multiple Key Exchanges in IKEv2 draft-ietf-ipsecme-ikev2-multiple-ke-05*.

[14] IETF draft-campagna-tls-bike-sike-hybrid-07, IETF draft experimental draft-campagna-tls-bike-sike-hybrid-07, *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)*.

[15] IETF RFC 5246, IETF Standard RFC5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[16] ETSI GS QKD 014, ETSI Group Specification GS QKD 014 (2019), *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API (2019)*

[17] ETSI GS QKD 004, ETSI group Specification GS QKD 004 (2020), *Quantum Key Distribution (QKD); Application Interface (2020)*

[18] IEEE 802.1AE, IEEE std 802.1AE-2018 (2018), *802.1AE MAC Security (MACsec)*

[19] [ITU-T X.1710], ITU-T Recommendation X.1710 (2020), *Security framework for quantum key distribution networks.*

〈저자소개〉

심 동 희 (Dong-Hi SIM)

1999년 2월~2007년 5월 : LG전자 차세대통신연구소, 책임연구원
2007년 6월~2009년 6월 : SK텔레콤 기술전략팀, 매니저
2009년 7월~2012년 6월 : European Telecommunication Standards Institute, Technical Officer
2012년 7월~2018년 6월 : SK경영경제연구소 미래연구실, 수석연구원
2018년 7월~현재 : SK텔레콤 혁신사업TF, 팀장
2019년 12월~2021년 6월 : HEC Paris, MBA
<관심분야> 5G, 통신공학, 정보보호, 기술표준화, 양자암호, 양자키분배, 양자난수생성기