TLS 1.3 환경에서 Hybrid PQC 인증서의 전송 최적화 : Signature-Only 압축 기법 실험 사례

이올미*, 장우현, 김사연

엘아이지넥스원

*olmi.lee@lignex1.com, woohyun.jang2@lignex1.com, sayeon.kim@lignex1.com

Transmission Optimization of Hybrid PQC Certificates in TLS 1.3 : A Signature-Only Compression Approach

Lee Ol Mi, Jang Woo Hyun, Kim Sa Yeon

LIG NEX1

요 약

현대 통신에서 널리 사용되는 TLS 1.3은 전통적으로 공개키 서명 방식을 사용하고 있다. 그러나 양자 컴퓨팅 기술의 발전으로 인하여 기존 공개키 기반 암호인 ECDSA와 RSA 등은 안전성을 위협받고 있다. 이에 따라 양자내성암호 기술들을 TLS 1.3에 적용하려는 연구가 활발히 이어지고 있다. 이러한 흐름에 따라 본 연구는 기존 서명 방식인 ECDSA와 Dilithium3 서명 방식을 통합한 하이브리드 인증서를 구현하고 이를 TLS 1.3 통신에 적용할 수 있도록 전송 최적화를 시도하였다. selective encoding 방식은 TBS 해시 불일치 문제로 인하여 인증서 검증에 실패하였으며, 이에 따라 일반 압축 알고리즘인 zlib를 적용하도록 하였다. 인증서 전체 압축 방식과 서명 필드만 압축하는 방식에 대한 실험을 수행한 결과 압축률은 낮았으나, 인증서의 구조적 무결성과 해시를 일치시킨 채로 전송이 가능한 것을 확인하였다. 본 연구는 PQC 적용에 따른 인증서 구조의 제약을 분석하고 전송 최적화에 대해 검토한 사례로 의의를 가진다.

Ⅰ. 서 론

양자 컴퓨팅 기술의 발전으로 인해 기존 공개키 기반 암호의 안정성이 위협받고 있으며, 이에 따라서 양자 내성 암호의 표준화와 실제 적용에 대한 연구가 활발히 진행되고 있다. 이에 따라 현대 인터넷 통신의 표준 프로토콜인 TLS 1.3에 PQC 적용 필요성이 논의되고 있다.

TLS 1.3에 사용되는 X.509 인증서는 국제 표준에 따라 정의된 디지털 인증서 형식이다. 인증서 소유자의 공개키, 인증서의 유효기간 등 인증서와 관련한 정보와 더불어 서명 알고리즘과 서명값을 포함하고 있다. 특히 서명 알고리즘을 나타내는 signatureAlgorithm 필드와 서명값을 나타내는 signatureValue 필드는 TLS 핸드셰이크 과정에서 인증서의 무결성을 검증할 때 사용된다.

이러한 X.509 인증서에 PQC를 적용하기 위한 방안 중 하나인 하이브리드 인증서는 기존 서명방식과 양자 내성 암호를 병합한 형태로 호환성과 보안성을 모두 확보할 수 있는 대안으로 주목받고 있다.

그러나 양자 내성 암호는 기존 공개키 기반 암호에 비해 서명 및 키의 크기가 크기 때문에 TLS 1.3에 적용 시 부하가 커진다는 단점이 있다. 하이브리드 인증서를 TLS 1.3에 적용한 기존 연구에서는 성능 측정과 핸드셰이크 비용 처리를 중심으로 분석하였으나[1], 전송 효율을 개선하기 위한 방안은 시도되지 않았다.

또 다른 연구에서는 양자 내성 암호 인증서에 다양한 압축 알고리즘을 적용하여 평균 24%에 달하는 압축률을 보고하기도 하였으나, 이는 양자 내성 암호에만 적용한 내용으로 하이브리드 인증서에 대한 언급은 없다.[2]

본 연구는 호환성과 보안성을 동시에 확보할 수 있는 하이브리드 서명 X.509 인증서를 채택하고, TLS 1.3의 성능 개선을 위해 signatureValue 및 인증서 전체에 대한 압축 방안을 실험하였다.

Ⅱ. 본론

1. 구현 및 실험

1.1 양자 내성 암호 선정

양자 내성 암호는 NIST 표준으로 선정된 Dilithium을 선정하였다.[4] Dilithium 알고리즘은 격자 기반 구조를 바탕으로 구현된 암호 알고리즘의 하나이다. Falcon 알고리즘의 경우 서명 크기가 작지만 구현이 복잡하다. SPINCS+ 알고리즘은 공개키 사이즈는 32 바이트로 매우 작지만, 서명의 크기는 7,856 바이트로 Dilithium3에 비해 약 2배 크다. 또한 openSSL 암호 라이브러리에서도 Dilthium의 실험적 통합이 진행되는 것을 고려하여, Dilithium 중에서도 너무 크지 않은 서명 크기를 가진 Dilithium3 알고리즘을 선정하였다.

	키 크기(bytes)	서명 크기(bytes)
CRYSTALS-Dilithium	1,312	2,420
Falcon	897	666
SPHINCS+	32	7,856

표 1 NIST 표준 PQC 알고리즘 비교

	NIST 보안 등급	키 크기 (bytes)	서명 크기 (bytes)
Dilithium2	level 2	1,312	2,420
Dilithium3	level 3	1,952	3,293

Dilithium5	level 5	2,528	4,564

표 2 Dilithium 알고리즘 비교

1.2 하이브리드 인증서 구조 구현

본 연구에서 구현한 하이브리드 인증서의 구조는 X.509 인증서의 signatureValue 필드에 ECDSA 서명과 Dilithium3 서명을 병합한 하이브리드 서명을 삽입하는 방식이다. 인증서의 signatureAlgorithm 필드는 ECDSA 기반을 유지하였으며, 필요시 클라이언트가 선택한 서명 방식만 검증할 수 있으므로 통신 환경이나 보안 정책에 따라 유연하게 대응 할 수 있다.

위와 같이 구현한 인증서의 전체 크기는 약 3,950 바이트로 이 중 Dilithium3 서명의 크기는 3,293 바이트, ECDSA 서명은 약 70 바이트를 차지한다. 즉 구조적으로 signatureValue 필드가 전체 인증서의 약 85%를 차지하고 있음을 확인할 수 있고, 전송 최적화를 하기 위해 해당 필드를 줄여야 함을 알 수 있다.

1.3 Selective Encoding 실험

먼저 최적화를 위해 인증서 signatureValue 필드의 태그 및 NULL 값, unused bits 등을 제거하여 ASN.1 DER 구조를 최적화하는 selective encodign 기법을 적용하였다. 그러나 해당 방식은 인증서의 TBS 영역 구조를 변경시켜 결과적으로 해시 불일치를 초래하였다. 이에 따라 mbedtls 및 openSSL 기반 서명 검증을 실패하였고, 이는 실용성이 없으며 다른 최적화 방안이 필요함을 알 수 있다.

1.4 Signature-Only 압축 기법 설계

1.3의 방식이 실패한 이후 TBS 구조를 변경하지 않으면서 signatureValue에 일반 압축 알고리즘인 zlib을 적용하는 방식을 실험하였다.

signatureValue 필드만 추출한 후 zlib.compress()를 활용하여 압축을 진행한 결과, ASN.1 BIT STRING 구조는 유지하였으며 복원 및 검증에도 성공했지만 압축 전 인증서의 크기가 약 3,364 바이트, 압축 후 인증서의 크기가 약 3,350 바이트로 압축률은 매우 미미함을 확인하였다.

1.5 전체 압축 실험과 비교

또한 인증서 전체를 zlib으로 압축하고 이를 전송 및 복원하는 실험을 수행하였다. 그러나 그 결과 압축 전 인증서의 크기는 약 3,950 바이트, 압축 후 인증서의 크기는 약 3,895 바이트 정도로, 1.3의 실험과 크게 다르지 않은 결과를 보였다. 이는 하이브리드 인증서의 구조 특성상 인증서의 signatureValue가 인증서 전체 비중에서 약 85% 이상을 차지하고 있으며, 따라서 압축 가능한 필드가 매우 제한적이었음을 알 수 있다.

2. 결과 분석 및 논의

1.3~1.5의 실험 결과, signaureValue 필드만을 압축하는 방식과 하이브리드 인증서 전체를 압축하는 방식 모두 해시 일치와 복원 및 검증은 성공할 수 있었으나, 실제 인증서의 크기 감소 효과는 크지 않았다. signatureValue 필드만을 압축하는 방식은 ASN.1 포맷을 유지할 수 있다는 점에서 TLS 환경과의 호환성에서는 긍정적으로 평가할 수 있다. 두 방식 모두에서 압축률은 1% 이하로 매우 낮았으나, 본 연구에서는 압축률 자체보다는 구조를 유지한 채 서명 필드만 선택적으로 압축하는 실험을 수행하여 서명 필드에 대한 압축 가능성을 실험적으로 검토했다는 기여점을 가진다.

Ⅲ. 결론

본 연구는 TLS 1.3 환경에서 기존 서명과 양자 내성 암호를 병합한 하이브리드 인증서의 전송 최적화를 위한 압축 기법으로 signatureValue 압축 방식을 실험했다. 그러나 실험 결과 인증서 압축률은 미미했다. 이러한 현상의 원인으로는 PQC 서명의 구조적 특성인 높은 엔트로피를 꼽을 수 있다. 이는 실험에서 사용된 zlib와 같은 압축 알고리즘이 탐지할 수 있는 중복성이 거의 없음을 의미하며, zlib의 경우 zlib의 포맷이 요구하는 헤더나 블록 메타데이터 등이 오히려 오버헤드를 일으킬 수 있을 것으로 보인다. 하지만 실험에서 ASN.1 포맷을 유지하고 해시 무결성을 확보하였으며, 구조적 일관성 및 검증 가능성을 확보했다. 또한 기존 연구와 달리 하이브리드 구조 특유의 제약 조건에서 압축 실험을 진행하였다. 향후 연구에서는 구조적 압축이 가능한 서명 포맷의 탐색 혹은 새로운 압축 전략에 대한 탐색을 진행할 수 있다.

참 고 문 헌

[1] Marchsreiter, D., & Sepúlveda, J. (2022, August). Hybrid post-quantum enhanced tls 1.3 on embedded devices. In 2022 25th Euromicro Conference on Digital System Design (DSD) (pp. 905-912). IEEE.

[2] 강정훈, 김제인, 서승현. (2023). 효율적인 PQC TLS 통신을 위한 인증서 압축 알고리즘 분석. 한국정보처리학회 학술대회논문집, 30(2), 1193-1195.

[3] 이현우, 김영현, 조은상, 권태경. (2018-01-17). 인증서 압축을 활용한 TLS 확장 프로토콜의 적용 및 분석. 한국통신학회 학술대회논문집, 강원.

[4] NIST, “Post-Quantum Cryptography Standardization,” National Institute of Standards and Technology. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography. [Accessed: May 7, 2025].

[5] Astrizi , T. L., & Custódio , R. (2024). Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption. Sensors, 24(22), 7300. https://doi.org/10.3390/s24227300