차량 내부 통신 프로토콜의 KpqC 알고리즘 적용 가능성 평가

이민우[1], 심민주[1], 송경주[1], 윤세영[2], 서화정[3]
[1]한성대학교 정보컴퓨터공학과 박사과정
[2]한성대학교 융합보안학과 석사과정
[3]한성대학교 융합보안학과 부교수
minunejip@gmail.com, minjoos9797@gmail.com, thdrudwn98@gmail.com,
sebbang99@gmail.com, hwajeong84@gmail.com

KpqC on CAN-FD: A Feasibility Assessment

Min-Woo Lee[1], Min-Joo Sim[1], Gyeong-Ju Song[1], Se-Young Yoon[2],
Hwa-Jeong Seo[2]
[1]Dept. of Information Computer Engineering, Hansung University
[2]Dept. of Convergence Security, Hansung University

요 약

본 연구는 CAN-FD에서 국내 KpqC 최종군(DSA: HAETAE/AIMer, KEM: SMAUG-T/NTRU+)의 통신 관점에서의 적용 가능성에 대해 평가하였다. KpqC 알고리즘들의 데이터 크기를 64바이트 페이로드 기준으로 프레임 수에 매핑하고, ISO-TP 분할과 BRS를 반영하여 프레임당 0.164 ms로 지연 시간을 산출하였다. 결과적으로 KEM(SMAUG-T/NTRU+)은 ECU 1대당 수 ms 미만, 도메인 시동 여유 내 수용 가능했고, 서명(HAETAE/AIMer) 전송도 진단/OTA 응답 창구 대비 충분히 작음을 확인하였다. 종합적으로 KpqC 알고리즘의 CAN-FD 각 도메인 상에서의 통신 지연 측면에서의 적용 가능성에 대해 확인하였다.

1. 서론

양자 컴퓨팅의 발전으로 인해 기존 보안체계가 붕괴될 위험이 생기며, 차량 내부 네트워크에서도 공개키 기반 보안에 대한 PQC(양자내성암호) 적용이 논의되고 있다[1]. NIST는 2024년부터 KEM(키 캡슐화 매커니즘)과 DSA(전자서명) 표준화를 진행중이며[2], 국내에서도 국가 주도의 KpqC 공모전을 통해 KEM 및 DSA 후보군을 선정했으며, 표준화 진행중에 있다[3]. 자동차 분야 역시 이 흐름에 맞춰 PQC의 적용 가능성과 조건을 조기에 점검할 필요가 있다.

차량 내부 통신 프로토콜인 CAN-FD는 기존 클래식 CAN에서 데이터 필드가 최대 64바이트로 확장되고, 데이터 구간에서 BRS(비트 전송률 가변 스위칭)를 지원해 전송 한계를 늘렸다[4]. 그럼에도 PQC의 공개키, 서명처럼 상대적으로 큰 데이터를 보낼 때에는 실제 시스템에서의 전송 지연 한계와 통신 오버헤드를 고려할 필요가 있다. 이 경우, 대용량 데이터는 표준화된 분할 및 재조립 전송 절차(ISO 15765-2)에 따라 여러 프레임으로 나누어 전송되고[5], 수신 측에서 순서와 흐름을 제어하며 원본 데이터로 복원한다. 즉, 큰 데이터를 안전하게 나눠 보내고 받는 방식이 규격 차원에서 정의되어 있으며, 본 연구에서 다루는 데이터도 이를 따르는 것을 전제로 한다.

평상시 주행 데이터 보호는 대체로 대칭키 기반(AEAD/MAC)으로 처리되고, 공개키 연산은 빈도가 낮은 절차에 집중되는 것이 일반적이다[6]. AES 등 현재 사용중인 대칭키 암호는 양자컴퓨터의 위협으로부터 안전할 것으로 평가되기에[7], 평상시 주행 데이터 패킷의 보안성은 대칭키 암호 적용을 통해 확보할 수 있을 것으로 사료된다. PQC는 차량 시동 시 도메인 게이트웨이와 각 ECU(전자제어장치) 사이의 초기 세션키 합의를 담당하는 KEM과, 진단 및 OTA(펌웨어 업데이트)와 같은 절차에서 메타데이터, 이미지 등의 진위를 확인하는 용도로 사용되는 DSA에 적용할 수 있다[8]. 본 연구에서는 이와 같은 상황에서 KEM 및 DSA에 PQC를 적용하는 것을 전제로 한다.

본 연구는 CAN-FD 프로토콜을 대상으로 KpqC 알고리즘의 적용 가능성을 이론적으로 평가하는 데 초점을 맞춘다. 구체적으로, KpqC 알고리즘의 키, 서명 등의 데이터 크기를 CAN-FD 프레임 수로 환산하고, 프레임당 총 전송 지연을 산출한다. 이후 KEM은 게이트웨이 공개키를 한 번 브로드캐스트하고, ECU별 암호문을 한 번 전송하는 절차를 가정해 도메인별 전송 지연 한계 내에 통신을 할 수 있는지의 가능성을 평가한다. DSA는 진단/OTA ECU 도메인에서의 1회성 통신을 가정하며, KEM과 마찬가지로 통신 가능성을 평가한다.

2. 관련 연구

2.1 CAN-FD 프로토콜

CAN은 ECU 간 실시간 네트워크 표준(ISO-11898)이다. 클래식 CAN(CAN 2.0A/B)은 프레임당 최대 8바이트 프레임 페이로드와 최대 1 Mbps급 비트레이트를 사용하고, 오류 검출을 위해 CRC-15를 적용한다. CAN-FD는 같은 표준에 통합된 확장 프레임 형식으로, 프레임 페이로드를 최대 64바이트까지 확대하고 BRS를 통해 프레임 내부에서 노미널 구간(Arbitration/Control/ACK)과 데이터 구간(Data/CRC)의 비트레이트를 다르게 설정할 수 있다. 실무적으로 노미널 구간은 클래식 CAN과의 호환성 때문에 약 ≤1 Mbit/s, 데이터 구간은 5 Mbps(2,5,8 Mbps 지원) 수준으로 설정되는 구성이 일반적이다[9]. 그림[1]은 CAN-FD 프레임 구조를 나타낸다.

오류 검출 측면에서 CAN-FD는 프레임이 16B 이하일 때 CRC-17, 프레임이 16B보다 클 때 CRC-21을 사용하며, 동적 비트스터핑을 CRC 계산에 포함하고 SBC(스터프 비트 카운터)와 FSB(고정 스터프비트)를 추가해 검출 능력을 강화한다. 클래식 CAN의 5연속 동일 비트 후 보정 1비트 삽입 규칙은 CAN-FD에서도 유지되지만, FD는 스터프 개수 정보와 고정 스터프비트를 CRC 필드에 추가한다. 식별자 길이(11/29비트), FDF(FD 포맷 식별), BRS 비트(비트레이트 설정)등 제어 필드의 확장은 ISO 11898-1의 FD 프레임 정의에 포함된다. 이로써 클래식 CAN을 사용하는 단말과의 호환성을 유지하면서도 데이터 처리량을 향상시킬 수 있게 되었다.

(그림 1) CAN-FD 프레임 구조

CAN-FD의 PQC 적용 시 고려사항은 다음과 같다. CAN-FD의 프레임당 페이로드 한계(64 B) 때문에 공개키, 암호문, 서명과 같은 대용량 데이터는 ISO 15765-2(통칭 ISO-TP)의 분할 절차로 운반하는 것이 일반적이다. 이 경우 프레임 수 증가가 네트워크 점유율을 좌우하므로, 본 연구에서는 보수적 상한을 잡기 위해 최악의 스터핑(최대 5:1 동적 스터핑) 및 ISO-TP 오버헤드를 포함하여 프레임 당 전송 지연을 평가한다.

2.2 KpqC 공모전

KpqC 공모전은 2022년 공고 후 2023년 12월에 라운드 2를 거쳐, 2025년 1월 16일 최종 표준화 대상 알고리즘을 선정하였다. DSA는 AIMer, HAETAE가 선정되었으며, KEM은 NTRU+, SMAUG-T가 선정되었다[10]. AIMer는 BN++/MPC-in-the-Head 기반으로, 자체 제안 대칭 프리미티브인 AIM2의 안정성에 의존한다. HAETAE는 모듈 격자(MLWE/MISIS) 기반의 Fiat-Shamir with Aborts 계열 서명으로, 하이퍼볼 샘플링 등으로 서명/키 크기를 줄이는 설계를 채택하며 동급 보안수준에서 Dilithium 대비 서명 및 검증키가 30 - 40% 작다고 보고된다. NTRU+는 고전적 NTRU 격자 문제에 기반한 KEM으로, ACWC2 및 Fujisaki - Okamoto 변환을 도입해 간결한 인코딩과 IND-CCA2 안전성을 달성하도록 설계되었다. SMAUG-T는 MLWE/MLWR 난제에 기반하며, NTRU+와 마찬가지로 Fujisaki - Okamoto 변환으로 IND-CCA2를 보장하는 KEM이다.

3. CAN-FD 전송 지연 산출

본 장은 KpqC 알고리즘의 공개키, 암호문, 서명을 CAN-FD로 보낼 때의 프레임 수와 총 전송 지연을 최악으로 상정하여 계산하는 절차를 정리한다. 프레임 구성은 노미널 구간과 데이터 구간으로 나뉘며, 비트레이트는 노미널 1 Mbps, 데이터 5 Mbps로 둔다. 64 B 페이로드를 꽉 채운 한 프레임을 보낼 때, 헤더, CRC(17/21), Stuff-counter, FSB, ACK, EOF, ITM 및 최악의 스터핑(5:1)을 모두 반영하면

<표 1> CAN-FD 패킷 비교(KEM/DSA)

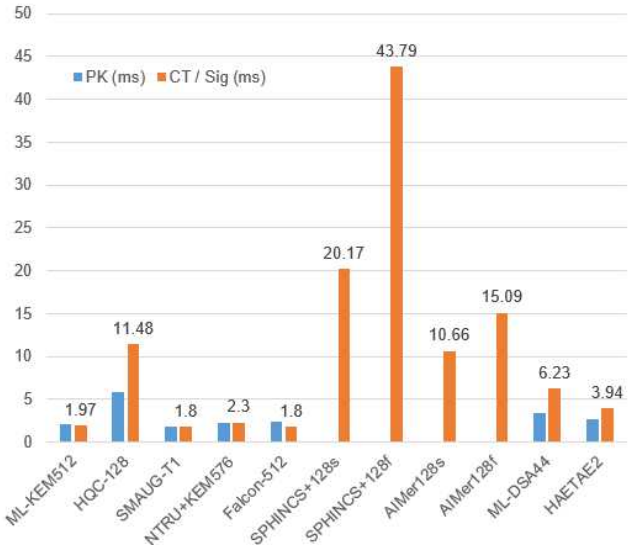
알고리즘	보안 레벨	공개키/PK (Byte)	암호문/서명 (Byte)	CAN 패킷 최대 크기 (Byte) (PK / CT, PK / Sig)	프레임 수 (PK / CT, PK / Sig)
ML-KEM512	1	800	768	1,086 / 1,032	13 / 12
HQC-128	1	2,249	4,433	3,041 / 5,973	36 / 70
SMAUG-T1	1	672	672	914 / 914	11 / 11
NTRU+KEM576	1	864	864	1,172 / 1,172	14 / 14
Falcon-512	1	897	666	1,227 / 908	15 / 11
SPHINCS+128s	1	32	7,856	54 / 10,562	1 / 123
SPHINCS+128f	1	32	17,088	54 / 22,962	1 / 267
AIMer128s	1	32	4,160	54 / 5,590	1 / 65
AIMer128f	1	32	5,888	54 / 7,912	1 / 92
ML-DSA44	2	1,312	2,420	1,774 / 3,256	21 / 38
HAETAE2	2	992	1,474	1,344 / 2,002	16 / 24

실제 전선에 흐르는 길이는 약 86 B(64 B 데이터 + ≈22 B 오버헤드)가 된다. 세부적으로는, 고정 오버헤드 67-bit, 데이터 필드 512-bit, 최대 스터프 비트 107-bit로, 이를 모두 더하면 686-bit이다. 이는 86 B에 근사한다. 표[1]은 PQC 및 KpqC 알고리즘 별 패킷 최대 크기 및 프레임 수를 나타낸다.

이 조건에서 1프레임 전송 시간 계산은 다음과 같다. 노미널 구간은 Arbitration + Control 필드가 22-bit, ACK + EOF + IFS 필드가 12-bit로, 이를 노미널 구간의 비트레이트인 1로 곱해주면 총 34ms의 지연이 됨을 계산할 수 있다. 데이터 구간은 데이터 512-bit, CRC + 스터프 카운터 + FSB 32-bit, 가변 스터프 비트 107-bit로, 이를 모두 더한 656-bit에 데이터 구간의 비트레이트인 5로 곱해주면 약 130ms의 지연이 됨을 계산할 수 있다. 노미널 구간과 데이터 구간의 전송 지연을 더하면 1프레임 당 지연 시간이 계산되며, 이는 약 0.164 ms로 잡는다.

아티팩트가 64 B를 넘으면 ISO-TP로 분할 및 재조립하며, 프레임 수는 데이터 크기를 64로 나눈 뒤 올림으로 정한다. 프레임마다 약 22 B의 오버헤드가 누적되므로 총 데이터 프레임 크기는 대략 데이터 크기 + 22 B × 프레임 수이다. 총 전송 지연은 프레임 수 × 0.164 ms로 근사한다.

KEM의 경우 SMAUG-T1 은 공개키, 암호문이 각각 672 B로 프레임 11개, 약 1.80 ms가 걸린다. NTRU+KEM576은 공개키, 암호문이 864 B로 프레임 14개, 약 2.30 ms가 소요된다. DSA는 진단/OTA와 같은 비정기 절차에서 한 번씩 전송된다. HAETAE-2의 서명 크기는 1,474 B로, 프레임 24개로 분할된다. 이는 약 3.94 ms가 소요된다. AIMer-128s의 서명 크기는 4,160 B로, 프레임 65개로 분할된다. 이는 약 10.66 ms가 소요된다. 그림[2]는 KpqC 및 NIST PQC의 알고리즘 별 총 전송 지연을 나타낸다.



(그림 2) 알고리즘 별 총 전송 지연

4. KpqC 적용 시나리오 및 적용 가능성 평가

4-1. CAN-FD ECU 도메인 별 적용 시나리오

Power-train 도메인의 엔진/변속제어 신호는 일반적으로 5 - 10 ms 주기를 목표로 설계된다. 실제 측정 및 사례에서는 엔진/변속 관련 CAN 신호의 평균 주기 10 ms가 보고되고, 제어 실험 환경에서도 5 ms 또는 10 ms 주기가 사용된다[11]. 즉, 파워트레인의 런타임 주기 프레임은 대칭키(AEAD/MAC)로 보호한다는 전제를 유지하고, PQC(KEM) 은 시동 시 1회 수행으로 한정한다. 3장의 결과로 보면, SMAUG, NTRU+는 수ms 내에서 마무리되므로,

KpqC 적용 가능성이 높다.

Chassis/ADAS 도메인의 차체 제어(제동/조향/차량안전)와 ADAS 보조 제어는 10 - 20 ms급 주기가 흔하며, 실제 트레이스 예시에서도 10/20/40/100 ms 주기가 혼재한다. 고급 ADAS의 엔드-투-엔드 반응 지연은 100 ms 미만이 바람직하다는 시스템 연구가 있다[12]. 즉, 여기서도 런타임 주기 프레임은 대칭키로 처리하고, PQC는 이벤트성(시동, 진단/업데이트)으로만 배치하는 것이 현실적이다. 해당 도메인에서도 파워트레인과 마찬가지로 전송 지연 내 통신이 가능하므로, KpqC 적용 가능성이 높다.

Body/Comfort 도메인은 상대적으로 완화된 주기를 사용한다. LIN/Body 계열에서는 10 - 100 ms가 전형적이고, CAN에서도 100 ms 주기 신호 예시가 다수 존재한다. 즉, 진단/온보딩 혹은 시동 초기화 시점의 PQC 트래픽은 버스 점유율 측면에서 여유가 크다고 볼 수 있다. KEM 1회와 DSA 1회의 통신 지연은 각각 수 ms - 수십 ms 범위로 계산되며, 도메인 동작에 영향이 매우 제한적이다.

진단/OTA 도메인은 응답 대기 시간을 표준 응답과 연장 응답으로 구분하며, 문헌 및 사례에서 표준 응답 ≈ 10 - 50 ms, 연장 응답 ≈ 수 초(E.g. 5 s) 설정이 널리 보인다. 표준은 파라미터 정의와 적용 맥락을 규정하고, 실제 값은 세션/서비스에 따라 OEM이 정한다. 또한 OTA의 절차 및 보안 프레임워크는 실시간 제어와 분리된 비실시간 서비스로 분류된다[13]. 즉, DSA 서명 전송 및 검증은 서비스 시간 창구(수백 ms~수 s) 안에서 처리되므로, 본 논문의 전송 지연(E.g. HAETAE2 서명 ≈4 ms, AIMer-128s ≈11 ms)은 통신 측면에서 충분히 여유가 있다.

4-2. CAN-FD에서의 KpqC 적용 가능성 평가

본 절은 3장에서 정의한 프레임당 지연(≈0.164 ms) 과 사용자가 제시한 KpqC 전송 데이터 크기 당 전송 지연 값을 그대로 대입해, 각 도메인에서 시동 시 KEM과 진단/OTA에서 DSA를 운용할 수 있는지를 판단한다. 비교 기준으로는 도메인별 지연 허용 시간을 대상으로 한다.

먼저 KEM 부문이다. SMAUG-T1(672 B, 1.8 ms/회)과 NTRU+KEM576(864 B, 2.3 ms/회)은 ECU 1대당 통신 지연이 수 ms 이내이며, “게이트웨이 공개키 1회 + ECU별 암호문 1회” 모델을 적용해도 ECU 수가 8, 16, 32대로 늘어날 때 총 지연이 대략 16→31→60 ms(SMAUG-T1), 20→39→76 ms(NTRU+KEM576) 수준에 그친다. 파워트레인 및 Chassis/ADAS 도메인의 시동 시 여유(수십~100 ms+)를 고려하면 충분히 수용 가능하다. ML-KEM-512(768 B, 1.97 ms/회) 역시 동급 수준으로 무난하다. 다만 HQC-128(4,433 B, 11.48 ms/회)은 ECU 수가 많을수록 총 지연이 빠르게 커져(예: N=8일 때 이미 약 98 ms 수준) 여유가 작은 시스템에서는 보수적으로 재검토가 필요하다. 결론적으로 KpqC KEM(SMAUG-T, NTRU+)은 모든 도메인 시동에서 실무적으로 적용 가능, NIST의 HQC는 구성에 따라 경계선에 놓인다.

다음은 DSA(진단/OTA) 부문이다. HAETAE-2(서명 2,002 B, 3.94 ms), ML-DSA-44(3,256 B, 6.23 ms), AIMer-128s/f(4,160/5,888 B, 10.66/15.09 ms)의 전송 지연은 모두 한 자릿수~십여 ms에 머문다. 진단/OTA는 수백 ms~수 s의 응답 창구를 운용하므로, 통신 측면에서 제약 요인은 사실상 없음에 가깝다. 실제 병목은 검증 연산 시간과 스토리지/전력 제약일 가능성이 크며, 통신은 충분한 여유를 가진다. 추가로 NIST의 Falcon-512는 666 B/1.8 ms로 통신 관점에서 가장 여유가 크다.

5. 결론

본 연구는 CAN-FD 환경에서 KpqC를 어디에, 어떻게 올릴 때 통신 측면에서 실현 가능한지 최악을 가정으로 검토하였다. 64B 페이로드, BRS 구성과 ISO-TP 분할을 전제로, 아티팩트 크기를 프레임 수와 전송 지연으로 단순 환산해 도메인별 허용 전송 지연 한계와 비교하였다.

요약하면, 국내 KpqC 최종군 전부 CAN-FD에 적용 가능하다. 런타임은 대칭키, 이벤트는 PQC라는 운용 전제를 유지할 때, KpqC의 도입은 통신 지연 관점에서 모든 도메인에서 수용 가능하다.

향후 연구로는, CAN-FD 패킷 시뮬레이터 기반의 구현 검증을 수행할 계획이다. ISO-TP 분할, BRS(데이터 구간 비트율), 우선순위 경쟁과 버스 부하를 모델링하여 프레임당 지연 0.164 ms 가정의 보수성을 실측치로 교정하고, 도메인 동시 초기화 및 재 키합의 주기, 게이트웨이 병렬화 등 운영 시나리오별 버스 점유율과 시동 총지연을 재평가할 것이다. 아울러 ECU환경에서의 서명 검증 시간을 계측해 통신과 연산을 합친 최종 단말 지연을 제시함으로써, KpqC의 실차 적용 가이드로 확장할 예정이다.

6. Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 20%) and this work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2025-02306395, Development and Demonstration of PQC-Based Joint Certificate PKI Technology, 40%) and this work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No. RS-2025-25394739, Development of Security Enhancement Technology for Industrial Control Systems Based on S/HBOM Supply Chain Protection, 40%).

참고문헌

[1] Cultice, Tyler, and Himanshu Thapliyal. "PUF-based post-quantum CAN-FD framework for vehicular security." Information 13.8 (2022): 382.

[2] Alagic, Gorjan, et al. Status report on the fourth round of the nist post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology, 2025.

[3] Bernstein, Daniel J., et al. "Report on evaluation of KpqC Round-2 candidates." Cryptology ePrint Archive (2024).

[4] Wang, Xu, et al. "Intrusion detection system for in-vehicle can-fd bus id based on gan model." IEEE Access 12 (2024): 82402-82412.

[5] ISO 15765-2, Road vehicles — Diagnostic communication over Controller Area Network (DoCAN) — Part 2: Transport protocol and network layer services, 2016.

[6] T. Rosenstatter et al., “Extending AUTOSAR’s Counter-based Solution for Freshness in SecOC,” PRDC 2019, 2019.

[7] Baksi, Anubhab, and Kyungbae Jang. "Quantum Analysis of AES." Implementation and Analysis of Ciphers in Quantum Computing. Singapore: Springer Nature Singapore, 2024. 51-90.

[8] Bazzi, Abir, Adnan Shaout, and Di Ma. "A novel variability-rich scheme for software updates of automotive systems." IEEE Access 12 (2024): 79530-79548.

[9] Schreiner, M., et al. "CAN FD from an OEM point of view." 14th International CAN Conference. 2013.

[10] KpqC Competition. 2025. Available online: https://kpqc.or.kr/competition.html (accessed on 17 September 2025).

[11] Reinsel, Samuel Joseph. Drive Quality Improvement and Calibration of a Post-Transmission Parallel Hybrid Electric Vehicle. Diss. Virginia Tech, 2018.

[12] Jichici, Camil, Bogdan Groza, and Pal-Stefan Murvay. "Integrating adversary models and intrusion detection systems for in-vehicle networks in CANoe." International Conference on Information Technology and Communications Security. Cham: Springer International Publishing, 2019.

[13] ISO, ISO. "14229: Road Vehicles-Unified Diagnostic Services (UDS)." Switzerland: ISO copyright office.