CAN-FD 양자내성암호 전환

유튜브 주소 : https://youtu.be/tOsMIL-_3CY

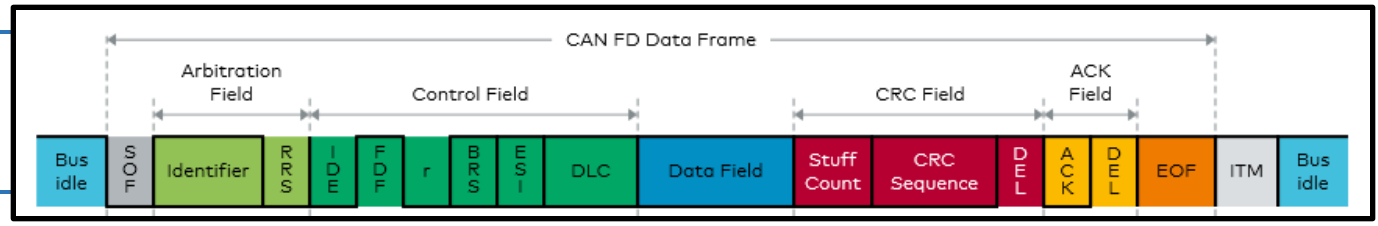
주요 자동차 내부 통신 프로토콜

- 대부분의 내부 통신 BUS는 **실시간성을 위해 프레임 크기가 작음**
  - **대용량 payload가 필요한 PQC는 적용 어려움**

프로토콜	1-프레임 payload	지연 한계	현행 보안	KpqC 적용 가능성	비고	출처
CAN 2.0B	**8 Byte**	**≤ 1 ms**	**X**	**X**	**클래식 CAN**	[1]
CAN-FD	**64 Byte**	**≤ 1 ms**	**X**	**조건부 적용 가능**	**차세대 CAN**	[2]
LIN 2.x	8 Byte	≤ 10 ms	X	X	저속, 저가 네트워크 (창문·시트·조명 등 적용)	[3]
FlexRay (전자식 제동 통신)	254 Byte	≤ 2 ms	MAC(옵션)	조건부 적용 가능	과거 일부 고급 차량 적용 (보급률 추정치 ≈ 10 %)	[4]
100BASE-T1 (이더넷, ADAS)	최대 1,500 Byte	Class A ≤ 2 ms Class CDT ≤ 100 μs	**TLS/DTLS**	**적용 가능**	신차 위주 적용 (보급률 추정치 ≈ 30%)	[5]

[1] https://www.iso.org/standard/86384.html
[2] https://tekeye.uk/downloads/can_fd_spec.pdf
[3] https://www.cs-group.de/wp-content/uploads/2016/11/LIN_Specification_Package_2.2A.pdf
[4] https://www.iso.org/obp/ui/#iso:std:iso:17458:-4:ed-1:v1:en
[5] Abdelgader, Abdeldime MS, and Wu Lenan. "The physical layer of the IEEE 802.11 p WAVE communication standard: the specifications and challenges." Proceedings of the world congress on engineering and computer science. Vol. 2. 2014.

CAN-FD 프로토콜



- CAN: ECU(전자제어장치) 간 실시간 통신 네트워크 표준(ISO 11898)
- **CAN-FD: Classic CAN(2.0B) 확장 버전**
  - **데이터 구간 속도 향상(BRS), 데이터 길이 확장(EDL)**

항목	CAN 2.0B	CAN-FD[1]
최대 데이터 길이	8 Byte	**64 Byte**
비트레이트	단일 속도	**이중 속도** **Nominal 구간(Arbitration + Control + ACK Field): 1 Mbps 이하** **Data 구간(Data + CRC Field): 2, 5, 8 Mbps[2]**
CRC	15/17-bit	**데이터 ≤ 16 byte: 17-bit** **데이터 > 16 byte: 21-bit**
Bit-Stuffing 방식	고정(비트5:1)	**가변(비트0~5: 1)**

<PQC 적용 시 고려 사항>

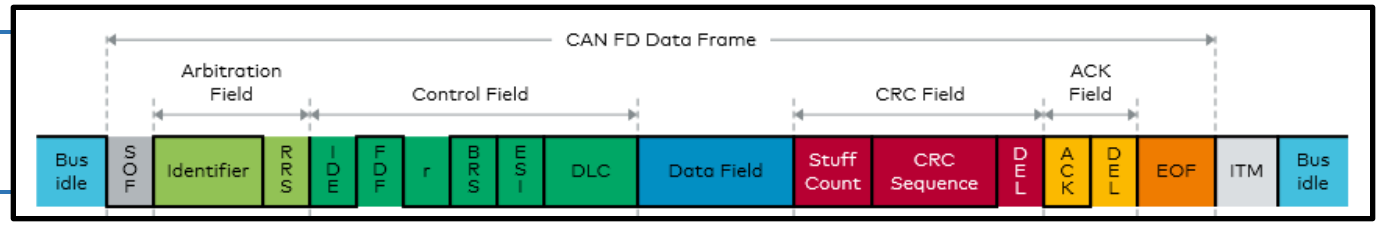
데이터 크기 최대 64 Byte -> PQC 데이터 전송 시 분할 필요(프레임 다량 발생)

가변 Stuff-bit: Worst-case 전송 지연 계산 필요

[1] https://tekeye.uk/downloads/can_fd_spec.pdf

[2] Zeltwanger, Holger. "CAN FD network design hints and recommendations." SAE International Journal of Passenger Cars-Electronic and Electrical Systems 9.2016-01-0060 (2016): 89-92.

CAN-FD 실제 전송 시 패킷 크기



전송하고자 하는 데이터가 20~64 Byte 일 경우의 시나리오(1-프레임 안에 끝날 경우)

필드	길이 (bit)	비고 / 설명
SOF+ Arbitration + Control	**23-bit**	ID(우선순위 선정), FD 모드 플래그, DLC(데이터 길이 코드) 등
CRC + Stuff-counter + FSB	**32-bit**	데이터 ≥ 20 Byte면 CRC-21 사용
ACK + EOF + ITM	**12-bit**	ACK(수신 확인), EOF(프레임 종료 표시), ITM(프레임 간격 비트)
Data Field	**0 ~ 512-bit**	실제 사용자 데이터, DLC 값과 길이 매핑(E.g. DLC 15 -> 64 Byte)
가변 Stuff-bit	**0 ~ 107-bit**	**worst-case: 원본 5-bit당 1-bit(20%)[1] -> 약 107-bit** 원본: CRC 직전(Arbitration + Control ~ Data -> 535-bit)

<실제 전송 시 1-프레임 당 최대 패킷 크기>

고정 오버헤드(67-bits[2]) + 데이터 필드(512-bits) + 최대 Stuff-bit(107-bit)

≈ 86 Byte(686-bit)

(고정 오버헤드: SOF+ Arbitration + Control + CRC + Stuff-counter + FSB + ACK + EOF + ITM)

[1] https://www.can-cia.org/fileadmin/cia/documents/proceedings/2012_oertel.pdf
[2] https://web.archive.org/web/20151211125301/http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can_fd_spec.pdf

CAN-FD 패킷 비교(KEM/DSA)

MTU(64 Byte)를 넘는 데이터 -> 64 Byte씩 분할하여 전송, 프레임당 최대 오버헤드 22 Byte 추가

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**

CAN-FD 전송 지연 산출

<1-프레임 지연 계산(worst case)>

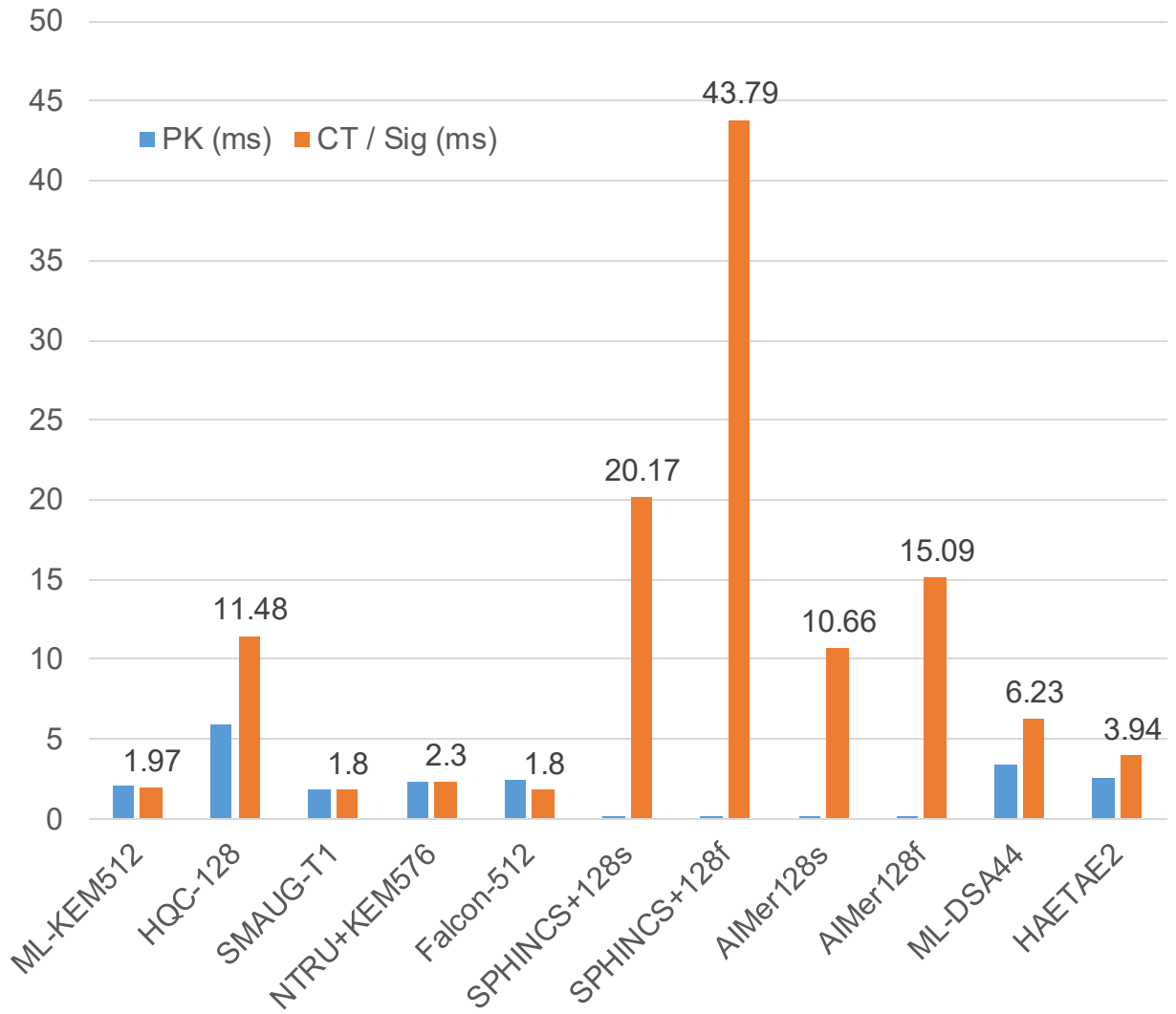
① Nominal 구간 @1 Mbps
- · Arbitration + Control = 22-bit → **22 µs**
- · ACK + EOF + IFS = 12-bit → **12 µs**
- · **22 + 12 = 34 µs**

② Data 구간 @5 Mbps
- · 데이터 64 B = 512-bit
- · CRC + Stuff-counter + FSB = 32-bit
- · 가변 Stuff-bit(≈ 107-bit)

(512 + 32 + 107) bit ÷ 5 Mbps ≈ 130 µs

③ 합계

34 µs + 163 µs = 0.164 ms



알고리즘별 총 전송 지연 (ms)

Hartwich, Florian. "Bit time requirements for can FD." *Proceedings of the 14th International CAN Conference*. 2013.

CAN-FD ECU 도메인 별 실시간성 및 PQC 적용 가능성 평가

- CAN 네트워크 상 ECU 도메인은 ASIL 등급[1]에 따라 구분 가능
  - **ASIL:** Automotive Safety Integrity Level(차량 안전 등급 체계)
  - **A -> B -> C -> D 순으로 위험도 높음(더 엄격한 안전 조치, 검증 요구)**

주요 ECU 도메인	ASIL 등급	지연 한계[2]	ECU 주요 신호	PQC 적용 가능성
Power-train	**D**	**≤ 1 ms**	엔진 ECU, 변속기, 연료분사	**불가능**
Chassis / ADAS	**C~D**	**≤ 2 ms**	ABS(브레이크 잠김 방지), EPS(전자식 조향), 레이더, 카메라	**일부 알고리즘 가능**
Body / Comfort	**A~B**	**≤ 50 ms**	창문, 시트, 조명, 공조	**대부분 알고리즘 가능**
Diagnostics / OTA	**A**	**≤ 100 ms**	서비스 진단, 펌웨어 업데이트	

ASIL C,D 등급 도메인(브레이크,엔진 등)은 μs~ms 단위 실시간성 + 최고 무결성이 필수
PQC처럼 통신 부담이 큰 알고리즘은 사실상 부적합

[1] Gheraibia, Youcef, et al. "An overview of the approaches for automotive safety integrity levels allocation." Journal of failure analysis and prevention 18 (2018): 707-720.
[2] https://www.can-cia.org/fileadmin/cia/documents/publications/cnlm/june_2024/24-2_cnlm.pdf

CAN-FD PQC 적용 가능성

▲: 최적화 시 적용 가능성 있음
(비트레이트 향상, 프레임 재배치 등)

알고리즘	CT / Sig (Byte)	전송 지연 (ms)	Power-train (≤ 1 ms)	Chassis / ADAS (≤ 2 ms)	Body / Diagnostics (≤ 50 ms)
ML-KEM512	768	1.97	X	O	O
HQC-128	4,433	11.48	X	X	O
SMAUG-T1	672	1.8	X	O	O
NTRU+KEM576	864	2.3	X	▲	O
Falcon-512	666	1.8	X	O	O
SPHINCS+128s	7,856	20.17	X	X	O
SPHINCS+128f	17,088	43.79	X	X	O
AIMer128s	4,160	10.66	X	X	O
AIMer128f	5,888	15.09	X	X	O
ML-DSA44	3,256	6.23	X	X	O
HAETAE-2	2,002	3.94	X	▲	O

현행 CAN-FD 버스에 PQC를 **전면 적용**하기에는 지연·대역폭 제약이 크기에 **불가능**
Power-train/Chassis 및 Body·Diagnostics에 PQC 적용을 도입하는 **하이브리드 전략이 현실적**

Q & A