IITP 정보통신기획평가원

ISSN 1225-6447 (Print)
ISSN 3058-3225 (Online)

2224호
2026. 11. 4.

IITP

주간기술동향

IITP Weekly AI · ICT Trends



- 「주간기술동향」은 과학기술정보통신부 「ICT 동향분석 및 정책지원」 과제의 일환으로 정보통신기획평가원(IITP)에서 발간하고 있습니다.
- 「주간기술동향」은 인터넷(http://www.itfind.or.kr)을 통해 서비스를 이용할 수 있으며, 본 고의 내용은 필자의 주관적인 의견으로 IITP의 공식적인 입장이 아님을 밝힙니다.
- 정보통신기획평가원의 「주간기술동향」 저작물은 공공누리 "출처표시-상업적 이용금지" 조건에 따라 이용할 수 있습니다. 즉, 공공누리의 제2유형에 따라 상업적 이용은 금지하나, "별도의 이용 허락"을 받은 경우에는 가능하오니 이용하실 때 공공누리 출처표시 지침을 참조하시기 바랍니다.
(http://www.kogl.or.kr/info/license.do 참고)

예시) "본 저작물은 'OOO(기관명)'에서 'OO년' 작성하여 공공누리 제O유형으로 개방한 '저작물명(작성자:OOO)'을 이용하였으며, 해당 저작물은 'OOO(기관명), OOO(홈페이지 주소)'에서 무료로 다운받으실 수 있습니다."



2224호
2026-22

IITP

주간기술동향

IITP Weekly AI·ICT Trends

ISSN 1225-6447 (Print)
ISSN 3058-3225 (Online)

기획시리즈: 양자기술

장거리 양자통신의 전송률 한계와 극복 기술

김용수_한국과학기술연구원 양자기술연구단장

서론 2
직접 전송의 전송률 한계 3
양자중계기의 원리와 양자메모리 4
양자메모리 없는 PLOB 한계 극복: 중간 노드 간섭 측정 6
기술적 과제 및 국내 연구개발 동향 10
결론 및 시사점 12

양자안전 네트워크로의 전환

엄상윤_아이디퀀티크 대표

서론 15
양자안전 네트워크와 PQC 전환 16
QKD 네트워크와 하이브리드 기술 19
국내외 실증 및 6계층 검증 프레임 23
국내 전환 전략과 시사점 25

ICT 신기술

이종 로봇 체화 간 지능 전이 공유 기술 동향

장민수_한국전자통신연구원 책임연구원

서론 29
기술 개념과 필요성 30
이종 로봇 체화 간 지능 전이 공유 기술 동향 32
전망 및 결론 39

Chapter 01

장거리 양자통신의 전송률 한계와 극복 기술

- 중간 노드 간섭 측정 기반 양자키분배를 중심으로 -

김용수_한국과학기술연구원 양자기술연구단장

광섬유 기반 양자통신은 광증폭기를 사용할 수 없어, 송수신단을 직접 연결하는 방식의 전송률은 채널 투과율에 비례하는 PLOB 한계의 제한을 받는다. 구간을 나누어 얽힘 교환으로 잇는 양자중계기는 이 한계를 넘는 근본적인 방법이지만, 확률적으로 성공하는 링크들을 동기화하기 위한 양자메모리가 아직 실용 수준에 이르지 못해 실현되지 않았다. 본 고는 양자메모리 없이 이 한계를 넘는 방법으로 중간 노드의 간섭 측정에 주목한다. 단일광자 간섭이나 비동기 이광자 간섭을 이용하면 전송률의 투과율 의존성이 η에서 $\sqrt{\eta}$로 완화되며, 이를 적용한 TF-QKD는 PLOB 한계를 넘어 1,000km급 비밀키 분배를 실증하였다. 다만, 이는 측정 결과의 상관관계만 필요로 하는 QKD이기에 가능한 것으로, 양자얽힘 분배와는 구별해야 한다. 아울러 광원과 위상 기준에 대한 요구조건의 완화, 다자간 네트워크로의 확장을 향후 과제로 제시하고 국내 연구 개발에 대한 시사점을 논의한다.

I. 서론

광섬유를 통해 전송되는 광신호는 거리에 따라 지수적으로 감쇠한다. 표준 단일 모드 광섬유의 손실 계수는 1,550nm 통신 대역에서 약 0.2dB/km로, 100km를 진행할 때마다 100개의 광자 중 99개가 사라지는 수준이다. 고전 광통신은 일정 간격마다 광증폭기를 배치하여 광손실 문제를 해결한다. 그러나 양자통신에는 광증폭기를 이용할 수 없다. 양자역학의 복제 불가정리(no-cloning theorem)에 따르면, 미지의 양자 상태는 완전하게 복제할 수 없고, 증폭 과정도 필연적으로 잡음을 유발한다[1]. 도청자가 신호를 복제할 수 없다는 성질은 양자키분배(Quantum Key Distribution: QKD)[1]가 물리 법칙에 근거한 안전성을 보장하는

* 본 내용은 김용수 단장(☎ 02-958-7266, yong-su.kim@kist.re.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

1) 양자키분배(QKD): 양자 상태에 정보를 실어 주고받음으로써 멀리 떨어진 두 사용자가 동일한 비밀키를 나누어 갖는 기술로, 이렇게 얻은 비밀키는 이후 고전 통신을 암호화하는 데 사용되며, 키를 나누는 과정의 안전성이 계산 복잡도가 아닌 물리 법칙에 근거한다는 점에서 기존 암호 방식과 구별된다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

핵심 원리이지만, 동시에 장거리 양자통신을 어렵게 하는 주된 요인이기도 하다.

그렇다면 양자정보는 광손실이 있을 때 증폭 없이 얼마나 멀리 전송할 수 있을까? 과학자들은 이 질문에 대한 답, 즉 광손실에 따른 근본적인 양자정보 전송 한계를 정확하게 알고 있다. 이 근본적인 전송 한계는 송수신단을 직접 연결하는 방식으로는 광원이나 검출기 성능 향상 등 기술적인 진보로 넘어설 수 있는 종류의 것이 아니다. 따라서 과학자들은 광증폭 없이 장거리 양자통신을 구현하기 위해 송수신부를 직접 연결하지 않는 다양한 방법을 연구해 왔다.

본 고의 구성은 II장에서는 중계 없이 송수신부를 직접 연결하는 직접 전송의 이론적 한계를 정리하고, III장에서는 광증폭을 하지 않으면서도 통신 거리를 늘리는 양자중계기의 원리와 양자메모리가 필요한 이유를 살펴본다. IV장에서는 중간 노드의 간섭 측정을 이용해 양자메모리 없이 직접 전송 한계를 넘는 원리와 이를 적용한 QKD 기술 동향을 살펴보고, V장에서는 기술적 과제와 국내 동향을, VI장에서는 결론과 시사점을 제시한다.

II. 직접 전송의 전송률 한계

QKD를 포함한 대부분의 양자통신은 양자얽힘[2]을 나누어 가짐으로써 시작한다. BB84 프로토콜과 같이 양자얽힘을 사용하지 않는 QKD 프로토콜이 있지만, 이들 역시 등가의 양자얽힘 기반 프로토콜로 기술할 수 있으며, 보안성 증명과 비밀키 생성률 계산도 흔히 이러한 얽힘 기반 등가 프로토콜을 이용하여 이루어진다[2]. 즉, 멀리 떨어진 두 통신자가 양자얽힘을 나누어 가지면 자연스럽게 QKD를 수행할 수 있고, 그 결과 비밀키를 얻을 수 있다.

따라서 양자얽힘은 QKD의 목적인 비밀키보다 일반적인 양자 자원이다. 분산 양자컴퓨팅, 블라인드 양자컴퓨팅, 분산 양자센싱, 원자시계 네트워크의 동기화는 모두 얽힘을 이용해 구현할 수 있으며, 암호키는 이 역할을 대체할 수 없다. 또한, 이러한 양자얽힘-비밀키 관계로 인해 후술하듯 순수한 손실 채널에서는 분배할 수 있는 얽힘의 최대량과 생성할 수 있는 비밀키의 최대량이 정확히 일치한다. 즉, 양자얽힘을 분배하는 것과 암호키를 나누어 가지는

2) 양자얽힘: 두 개 이상의 양자계 사이에 형성되어 각 계의 상태로 분리하여 기술할 수 없는 상관관계. 복제가 불가능하고 제3자가 개입하면 상관관계가 훼손되어 도청을 알아차릴 수 있다.

것은 동일한 물리적 한계 아래 놓여 있다.

중계 장치 없이 순수한 손실 채널에서 전송할 수 있는 양자정보 양의 상한은 2010년대 중반에 규명되었다. 2014년 Takeoka, Guha, Wilde는 손실 채널의 비밀키 전송률이 채널 투과율에 선형으로 비례하는 한계를 넘을 수 없음을 증명하였다[3]. 이어 2017년 Pirandola 등은 상대 엔트로피 기반의 얽힘 척도와 양자 전송 스트레칭 기법을 결합하여 그 정확한 값을 구하였다[4]. 저자들의 머리글자를 따서 PLOB 한계라 불리는 전송 가능한 양자정보의 양은 투과율 η인 순수 손실 채널에서 아래와 같이 쓸 수 있다.

$$K(\eta) = D_2(\eta) = -\log_2(1-\eta)$$

여기서 K는 비밀키 용량[비트/채널 사용], D_2는 양자얽힘 분배 용량[ebit/채널 사용]이다. 한편, 길이 L[km]인 광섬유의 투과율은 감쇠 계수 α[dB/km]를 이용하여 다음과 같이 주어진다.

$$\eta(L) = 10^{-\alpha L/10}$$

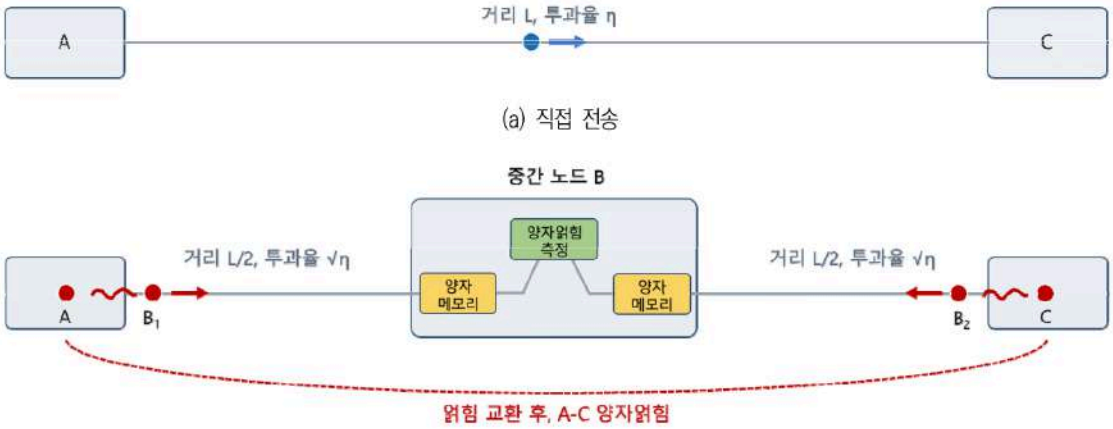
표준 단일 모드 광섬유의 α는 통신 대역에서 약 0.2dB/km이므로 투과율은 거리에 대해 지수적으로 감소하며, 전송률 또한 같은 방식으로 감소한다. 예컨대 L=50km에서 $\eta \approx 0.1$, L=100km에서 $\eta \approx 0.01$이다.

이 PLOB 한계는 광원의 밝기나 검출기 효율을 개선하여 넘어설 수 있는 기술적 제약이 아니라, 송수신단을 직접 연결하는 구성으로는 극복할 수 없는 근본적인 한계이다. 이 결과는 비밀키 용량과 양자얽힘 분배 용량이 동일한 이론적 한계에 묶여 있음을 보여준다.

이 한계가 실질적으로 얼마나 강한 제약인지는 수치로 쉽게 확인할 수 있다. 표준 광섬유 기준 1,000km 구간의 총손실은 200dB에 이르며, 이는 10^{20}개의 광자 중 단 하나의 광자만 무사히 도달하는 수준이다. 실제로 송수신단을 광섬유로 직접 연결하는 방식의 양자통신 실험은 초저손실 광섬유(α = 0.16dB/km)와 초전도 나노선 단일 광자 검출기를 사용하여 최대 400km 수준에 머물러 있다[5].

III. 양자중계기의 원리와 양자메모리

전송률이 거리에 대해 지수적으로 감소하는 이유는 하나의 광자가 전체 구간의 손실을



〈자료〉 한국과학기술연구원 자체 작성

[그림 1] 직접 전송과 양자중계기 기반 구간 분할 전송의 비교

한 번에 감당하기 때문이다. 양자중계기는 이 문제를 N개의 기본 링크로 분할하여 각 링크의 길이를 L/N으로 줄이고, 각 링크에서 독립적으로 생성한 얽힘을 순차적으로 연결하는 방식으로 해결한다[그림 1]. 기본 링크의 투과율은 $\eta^{1/N}$이므로, 얽힘을 순차적으로 연결할 수만 있다면 전체 구간의 전송률은 η에서 $\eta^{1/N}$으로 높일 수 있다. 마치 여러 개의 단일 광자가 구간을 나누어 이어달리기하는 것과 같다.

인접한 두 기본 링크를 연결하기 위해서는 양자얽힘 교환(entanglement swapping)을 수행해야 한다. A-B_1과 B_2-C 두 쌍의 얽힘이 준비된 상태에서 중간 노드 B가 보유한 두 큐비트 B_1과 B_2에 벨 상태 측정(Bell state measurement)을 수행하면, A와 C 사이에 양자얽힘을 생성할 수 있다. 주목할 점은 중간 노드 B가 가지고 있던 두 큐비트 B_1과 B_2는 측정 과정에서 사라지고, 대신 한 번도 직접 상호작용하지 않았던 A와 C 사이에 양자얽힘이 형성되는 것이다. 이와 같이 얽힘 교환을 이용해 원거리 얽힘을 확보하는 장치가 양자중계기이다.

얽힘 교환의 핵심 연산인 벨 상태 측정은 두 기본 링크에서 온 광자를 빔분할기에서 간섭시키는 이광자 간섭을 통해 구현할 수 있다. 따라서 두 광자는 동일한 시점에 측정 지점에 도달해야 하며, 스펙트럼 · 편광 · 시공간 모드 등에서 구별할 수 없어야 한다. 문제는 각 기본 링크의 얽힘 생성이 광자 손실 때문에 확률적으로만 성공한다는 데 있다. 만약, 두 링크가 같은 시도에서 동시에 성공한 경우에만 얽힘 교환을 수행한다면, 그 확률은 각 링크가 성공할

확률의 곱이 된다. 투과율이 η인 전체 구간을 두 개의 링크로 나눈 구성에서 링크당 투과율은 $\sqrt{\eta}$이므로 두 링크가 동시에 성공할 확률은 $\sqrt{\eta} \times \sqrt{\eta} = \eta$가 되어, 결국 전체 구간을 직접 전송하는 경우와 같아진다. 구간을 나누었지만, 이어달리기는 실패한 것이다.

따라서 양자중계기를 이용해 전송 확률을 높이려면 두 링크의 성공이 서로 다른 시점에 일어나더라도 그 결과를 결합할 수 있어야 한다. 먼저, 성공한 링크의 얽힘 상태를 보존하였다가, 나머지 링크가 성공하는 시점에 인출하여 벨 상태 측정을 수행해야 한다. 양자중계기를 구현하기 위해서 양자메모리가 필요한 이유가 여기에 있다. 양자메모리는 확률적으로 발생하는 두 사건을 동기화하는 장치이며, 이 동기화를 통해서 비로소 전송률이 η에서 $\eta^{1/N}$으로 개선되는 것이다. 단순히 양자 상태를 오래 유지하는 것만으로는 부족하며, 지정된 시점에 인출할 수 있는 온디맨드(on-demand) 동작이 가능해야 한다.

현재의 양자메모리 기술 수준은 이러한 요구에 아직 충분히 미치지 못한다. 저장 시간이 늘어날수록 효율과 충실도가 저하되고, 광자와 메모리 큐비트 사이의 결합 효율도 낮다. 또한, 많은 양자메모리가 통신 파장이 아닌 600~800nm 대역에서 동작하여 손실과 잡음을 수반하는 단일광자 파장 변환이 필요하다[6].

이러한 양자메모리의 높은 수준의 요구조건 때문에, 지난 수십 년간의 연구에도 불구하고 양자메모리를 이용하여 PLOB 한계를 극복한 사례는 매우 제한적이다. 2020년 다이아몬드 결함 기반 양자메모리를 이용한 실험에서 PLOB 한계를 넘는 비밀키 생성률이 보고되었으나, 이는 양자광원 대신 단일 레이저의 약한 펄스를 사용하고 광섬유 채널 없이 손실을 등가적으로 구현한 원리 검증 실험이라는 한계가 있다[7]. 실제 장거리 광섬유 링크에서 양자메모리로 PLOB 한계를 넘어선 사례는 아직 보고되지 않았다.

IV. 양자메모리 없는 PLOB 한계 극복: 중간 노드 간섭 측정

이광자 간섭에 기반한 양자중계기가 이점을 가지려면 양자메모리가 필요하다. 양측에서 전송된 두 광자가 모두 중간 노드에서 검출되어야 하므로, 서로 다른 시점에 일어나는 두 링크의 성공 사건을 동기화해야 하기 때문이다.

만약, 중간 노드의 측정을 이광자 간섭이 아닌 단일 광자 간섭으로 구현할 수 있다면, 양측에서 보낸 광자 중 하나만 중간 노드에 도착해도 된다. 두 광자의 도달 사건을 동기화할

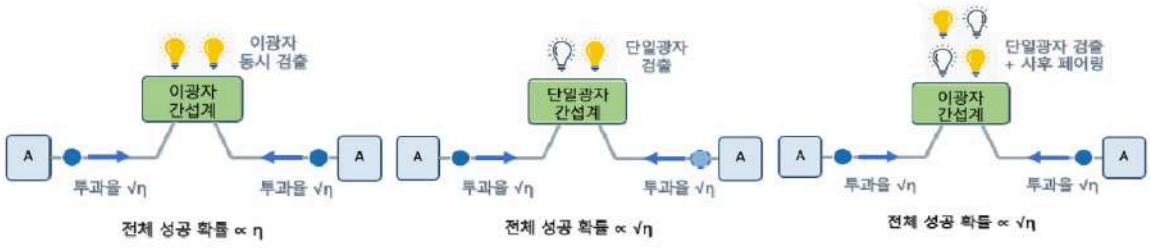
필요가 없으므로 양자메모리도 필요 없다. 이때 중간 노드에서 검출된 광자는 두 경로 중 어느 쪽에서 왔는지 알 수 없는 중첩 상태에 있으며, 이 단일광자 간섭을 통해 양측 사이에 양자얽힘 또는 상관관계를 형성할 수 있다. 전체 구간 L의 투과율을 η라 할 때 각 경로 L/2가 담당하는 투과율은 $\sqrt{\eta}$에 해당하므로, 전송률의 채널 투과율 의존성은 η에서 $\sqrt{\eta}$로 완화된다. 이는 dB 단위로 표현된 손실이 절반으로 줄어드는 것과 같으며, 동일한 전송률을 약 두 배의 거리에서 달성할 수 있음을 뜻한다. 즉, 양자메모리 없이도 손실-전송률 스케일링만 놓고 보면 중간에 노드 하나를 둔 양자중계기와 동등한 효과를 얻는다.

그러나 이러한 단일광자 간섭 기반 벨 상태 측정 방식의 이점에는 대가가 따른다. 이 방식을 구현하려면 검출된 광자의 출처를 원리적으로 구별할 수 없어야 한다. 이는 두 경로의 광학적 위상차가 광파장 수준 이내로 유지되어야 한다. 수백 km 길이의 광섬유에서는 미세한 온도 변화나 주변 진동만으로도 광경로 길이가 크게 변하므로, 정밀한 실시간 위상 추정과 보상 시스템이 필수적이다. 반면, 기존 이광자 간섭 방식은 두 광자의 상대 위상에 무관하므로 이러한 부담이 없다. 즉, 단일 광자 간섭은 높은 성공 확률을 얻는 대신 위상 안정화라는 기술적 부담을 떠안은 것이다.

한편, 양자메모리 없이 광자의 간섭 조건을 완화하여 $\sqrt{\eta}$ 스케일링에 이르는 또 다른 방식이 있다. 실험실에서 수행하는 많은 이광자 간섭은 두 광자가 검출부에 동시에 도달할 때 발생하지만, 이 동시 검출은 사실 이광자 간섭의 필요조건이 아니다. 만약, 이광자 간섭의 동시 검출 조건을 양자통신 실험에서 피할 수 있다면, 중간 노드에서 발생한 단일 검출 사건들을 시간 모드별로 기록해 두었다가, 서로 다른 시각에 발생한 두 사건을 사후에 짝지어 하나의 이광자 간섭으로 취급하는 것을 비동기 이광자 간섭이라 한다.

이러한 비동기 이광자 간섭이 가능한 이유는 두 광자의 시간적 중첩이 이광자 간섭의 필수 조건이 아니기 때문이다. 이광자 간섭은 두 사건의 확률진폭(probability amplitude)을 구별할 수 없을 때 발생하는데, 약한 결맞음 펄스의 경우에는 짝지어지는 두 펄스 사이의 위상 결맞음이 있다면 시간적으로 겹치지 않는 펄스 사이에서도 이광자 간섭이 발생한다[8]. 따라서 비동기 이광자 간섭은 단일 광자 간섭과 달리 광경로 전체의 위상을 실시간으로 보정할 필요 없이 짝지어진 두 시간 모드 사이의 상대 위상만 잘 유지하면, $\sqrt{\eta}$ 스케일링을 얻을 수 있다.

정리하면, 양자메모리 없이 간섭 측정 방식을 이용하여 PLOB 한계를 넘는 방식은 두



(a) 일반적인 이광자 간섭 (b) 단일 광자 간섭 (c) 비동기 이광자 간섭

〈자료〉 한국과학기술연구원 자체 작성

[그림 2] 중간 노드 간섭 측정 방식의 비교

가지가 있다[그림 2]. 두 개의 광자 검출을 하나의 광자 검출로 완화한 단일 광자 간섭 방식과 이광자 간섭의 시간 정합 요건을 완화한 비동기 이광자 간섭이다. 두 방식은 통신 거리 측면에서 동일한 이점을 갖지만, 광경로 전체 위상을 보정할 필요가 없는 비동기 이광자 간섭 방식이 단일 광자 간섭 방식에 비해 구현 측면에서 상대적으로 수월하다. 다만, 후술하듯이 두 방식 모두 비밀키를 분배하는 QKD에 활용할 수 있지만, 양자얽힘 자체를 분배하는 데에는 단일광자 간섭 방식만 활용할 수 있다.

양자메모리 없이 PLOB 한계를 넘을 수 있는 최초의 QKD 프로토콜은 2018년에 제안된, 중간 노드의 단일 광자 간섭을 활용한 TF-QKD(Twin-Field QKD)이다[9]. 송수신자가 각각 위상 무작위화된 약한 결맞음 펄스를 중앙 노드로 전송하고, 중앙 노드는 두 펄스를 간섭시켜 어느 검출기가 반응하였는지만 공표한다. 중앙 노드는 신뢰할 필요가 없으며, 이 점에서 측정 장치 독립(Measurement-Device-Independent: MDI) QKD의 성질을 함께 갖는다[10]. 이후 위상 무작위화 처리와 유한키 보안성 문제를 해결하기 위한 변형들이 잇따라 제안되었다. 위상정합 QKD(phase-matching QKD)는 위상 정보를 직접 부호화하여 보안성 증명을 단순화하였고[11], SNS-TF-QKD(sending-or-not-sending)는 위상 요동에 대한 내성을 강화하여 실환경 적용성을 크게 높였다[12].

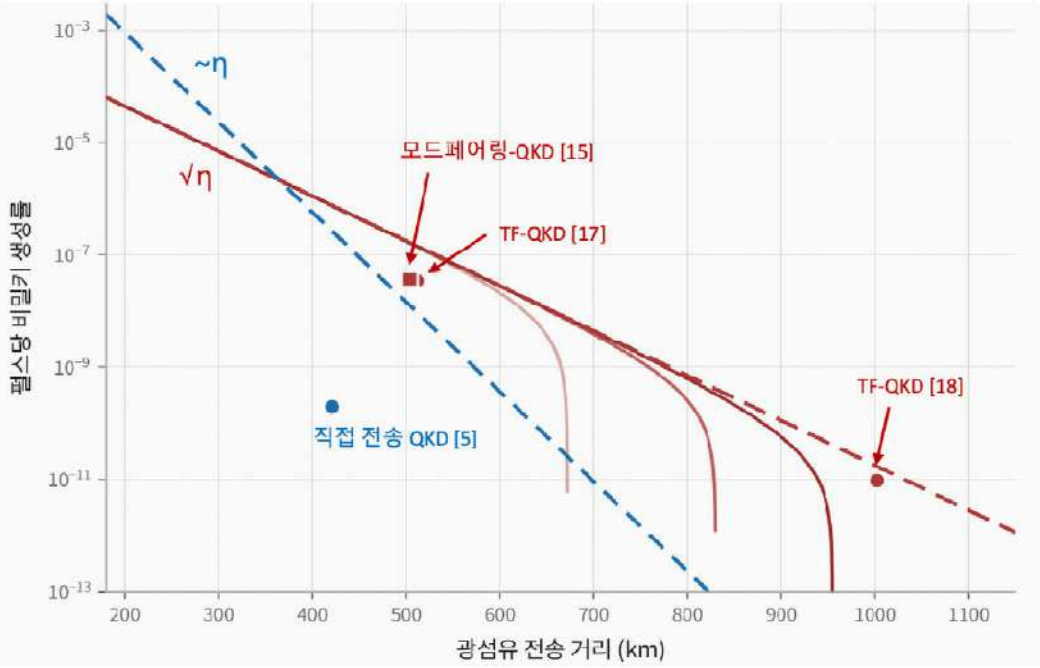
비동기 이광자 간섭을 적용한 프로토콜은 2022년에 모드페어링(mode-pairing) QKD와 비동기(asynchronous) MDI-QKD라는 이름으로 제안되었다[13][14]. 전체 광경로 위상 보정이 필요하지 않아 TF-QKD 계열에 비해 하드웨어 요구조건이 크게 낮아져, 최근의 장거리 QKD는 비동기 이광자 간섭을 활용하는 연구가 늘어나고 있다. 2025년에는 표준 광섬유 403km 구간에서 모드 페어링 QKD로 PLOB 한계의 약 2.9배에 해당하는 비밀키 생성률이

보고되었다[15].

단일 광자 간섭을 이용한 TF-QKD 계열과 비동기 이광자 간섭을 적용한 모드 페어링 QKD 모두 양자메모리 없이 PLOB 한계를 극복하며 수백 km에서 최대 1,000km에 이르는 거리에서 비밀키 분배가 가능함을 실험적으로 검증하였다[15-18]. 또한, 실환경 매설 광케이블에서도 500km 이상의 비밀키 분배에 성공하였다[17].

[그림 3]은 전송 거리에 따른 PLOB 한계와 직접 전송 QKD 그리고 이를 극복한 TF-QKD와 모드 페어링 QKD의 비밀키 생성률을 비교한 것이다. TF-QKD의 점근 곡선과 PLOB 한계는 약 360km 부근에서 교차하며, 이후 거리가 늘어날수록 격차가 급격히 벌어진다. 1,002km 실험에서 보고된 비밀키 생성률은 같은 거리의 PLOB 한계보다 네 자릿수 이상 높다. 다만, 실제 도달 거리는 유한한 데이터 크기에 의한 통계적 효과로 제한되며, 축적한 펄스 수가 많을수록 더 먼 거리까지 비밀키를 생성할 수 있다.

지금까지 우리는 멀리 떨어진 노드 간 비밀키를 분배하는 QKD를 논의하였다. QKD의



* 감쇠 계수 0.16dB/km 가정. 모드페어링 QKD는 표준 광섬유 403km의 총 손실을 0.16dB/km 기준 거리로 환산하여 표시. 세 개의 붉은 실선은 축적 펄스 수가 서로 다른 경우 유한 크기 효과를 반영한 비밀키 생성률로 축적 펄스 수가 증가할수록 더 장거리 통신이 가능하다.
〈자료〉 한국과학기술연구원 자체 작성

[그림 3] 간섭 측정 기반 QKD의 전송 거리별 비밀키 생성률과 PLOB 한계

목표는 송수신자가 얽힘 상태 자체를 나누어 갖는 것이 아니라, 얽힘이 제공하는 상관관계를 확인하고 그로부터 비밀키를 추출하는 것이다. 상관관계는 측정 결과에만 나타나면 충분하므로 측정 이후의 사후 선별을 거쳐도 무방하다. TF-QKD나 모드 페어링 QKD가 양자메모리 없이 PLOB 한계를 넘어설 수 있는 것은 바로 이 완화된 요구조건 덕분이며, 이는 실제로 양자얽힘을 분배하는 양자중계기와는 다르다.

앞서 살펴본 두 간섭 방식 가운데 QKD에서 더 나아가 양자얽힘 분배에 활용할 수 있는 것은 단일 광자 간섭뿐이다. 실제로 단일광자 간섭을 이용한 양자얽힘 분배는 TF-QKD보다 17년 앞서 DLCZ 프로토콜이라는 이름으로 제안되었다[19]. 하지만 얽힘 분배에서 PLOB 한계를 뛰어넘기 위해서는 측정 이후에도 얽힘 상태가 양자메모리에 보존되어야 하며, 이는 양자메모리의 기술적 과제를 그대로 안고 있다. 최근 다양한 물리계에서의 양자메모리 기술이 비약적으로 발전하고 있지만, 최고 수준의 양자메모리 기반 원격 얽힘 분배의 도달 거리는 수십 km 이내에 머물러 있다[20][21].

V. 기술적 과제 및 국내 연구개발 동향

1. 위상 기준과 광원 안정화

단일 광자 간섭 기반 TF-QKD는 두 송신자가 독립적으로 운용하는 레이저의 주파수와 위상을 정합하고, 수백 km 광섬유에서 발생하는 위상 요동을 실시간으로 보상해야 한다. 이를 위해 초안정 레이저, 주파수 전달, 기준 광을 이용한 위상 추적 기법이 사용되며, 이는 시스템의 복잡도와 비용을 높이는 주요 요인이다. 비동기 이광자 간섭 기반 모드 페어링 QKD는 짝지어진 시간 모드 사이의 상대 위상만 요구하므로 이러한 부담을 줄일 수 있다. 2025년에는 상용 레이저와 주파수 추적 기법으로 표준 광섬유 403km에서 PLOB 한계를 넘는 결과가 보고되었다[15].

그러나 모드 페어링 QKD 역시 위상 문제에서 완전히 자유롭지는 않다. 짝지어지는 두 검출 사건 사이에서 두 레이저의 주파수 차이와 광섬유의 위상 요동이 누적되면 상대 위상이 어긋나 오류율이 높아진다. 따라서 짝지을 수 있는 시간 간격은 레이저의 결맞음과 위상 요동 속도에 의해 제한된다. 문제는 거리가 늘어날수록 검출 사건이 드물어져 이 시간 간격

안에서 짝을 찾기가 어려워진다는 점이다. 그 결과 모드 페어링 QKD는 비교적 짧은 거리에서 유리한 반면, 초장거리에서는 위상을 능동적으로 보상하는 TF-QKD가 여전히 우위를 보인다[15]. 또한, 서로 독립적인 두 광원에서 온 펄스가 이광자 간섭을 일으키려면 시간, 편광, 스펙트럼 모드가 정합되어야 하므로 정밀한 시각 동기화와 주파수 오차 추정이 필요하다. 광원과 위상 기준에 대한 요구조건을 낮추면서 장거리 성능을 유지하는 것이 간섭 측정 기반 QKD를 실용망에 적용하기 위한 핵심 과제이다.

2. 다자간 양자암호통신으로의 확장

중간 노드 간섭 측정 기반 QKD는 거리뿐 아니라 참여 사용자 수를 늘리는 데에 유리한 구조를 갖는다. 비밀키는 송신자들이 보낸 광펄스의 간섭 결과로부터 생성되며, 간섭 측정을 수행하는 중앙 노드는 신뢰할 필요가 없다. 따라서 여러 사용자가 하나의 중앙 노드를 공유하는 스타(star) 구조를 자연스럽게 구성할 수 있다. 이 구조에서는 고가의 단일광자 검출기를 중앙 노드에 집중시키고 사용자 단말에는 송신부만 두는 형태로 네트워크를 설계할 수 있다.

나아가 간섭 측정 구조는 두 사용자 사이의 키 분배를 넘어, 셋 이상의 사용자가 하나의 비밀키를 공유하는 양자 회의키 분배(conference key agreement)나 양자 비밀분산(quantum secret sharing)으로도 확장할 수 있다. 여러 사용자가 보낸 펄스를 중앙 노드에서 함께 간섭시키면 단일 검출 사건으로 사용자 전체의 상관관계를 예고할 수 있다. 다만, 단일광자 간섭 방식에서는 참여 사용자 수만큼 광경로의 위상 기준을 동시에 안정화해야 하므로, 규모가 커질수록 구현 부담이 급격히 증가한다. 위상 기준 요구를 완화한 비동기 이광자 간섭 방식을 다자간 구조에 적용하는 것이 대안이 될 수 있다. 사용자 수에 따른 확장성과 중앙 노드 자원의 공유 효율이 다자간 양자암호통신의 핵심 과제가 될 것이다.

3. 국내 연구개발 동향

국내에서도 장거리 양자통신의 각 요소기술에 관한 연구 성과가 축적되고 있다. 간섭 측정 기반 QKD 분야에서는 한국과학기술연구원(KIST)이 편광 · 파장 · 시간 다중화를 결합한 2×N 구성의 TF-QKD 네트워크를 구현하여 50km 광섬유에서 다수 사용자의 동시 접속을 실증하였다[22]. 또한, 광자 수 부호화를 이용하여 양자메모리 없이 얽힘 교환을 수행하는

방안을 제안하였으며, 성공 확률이 채널 투과율에 선형으로 스케일링됨을 보였다[23].

이러한 연구실 수준에서의 괄목할 만한 연구 결과에도 불구하고 실환경에서 양자통신을 실증하는 연구는 더딘 편이다. 가령 국내에서 TF-QKD나 모드페어링 QKD와 같은 장거리 QKD 프로토콜은 아직 실험실 수준에서 연구되고 있으며, 아직 실용망에서의 구현은 보고되지 않았다.

Ⅵ. 결론 및 시사점

순수 손실 채널에서 직접 전송의 전송률은 PLOB 한계를 넘을 수 없으며, 이를 극복하는 근본적인 방법인 양자중계기는 양자메모리 기술의 한계로 아직 실현되지 않았다. 중간 노드의 간섭 측정은 양자메모리 없이 전송률의 투과율 의존성을 $\sqrt{\eta}$로 완화하는 방법으로, 이를 적용한 TF-QKD와 1,000km급, 모드 페어링 QKD는 400km급에서 PLOB 한계를 넘는 비밀키 분배를 실증하였다. 이러한 성과는 측정 결과의 상관관계만 필요로 하는 QKD의 특성에 기반한 것으로, 양자메모리가 필요한 양자얽힘 분배와는 구별하여 이해해야 한다.

암호키 분배만이 목적이라면 간섭 측정 기반 QKD는 이미 국제적으로 1,000km급 실증 단계에 도달해 있으며, 추가적인 메모리 기술 없이도 상용화 경로가 열려 있다. QKD를 넘어 양자얽힘을 분배하는 연구는 암호키로는 대체할 수 없는 기술인 분산형 양자컴퓨팅, 블라인드 양자컴퓨팅, 분산형 양자센싱, 원자시계 네트워크의 동기화 등을 가능하게 할 것이다.

이러한 분석은 국내 연구 개발에 다음과 같은 시사점을 제공한다. 첫째, QKD 분야에서는 거리 경신보다 다자간 통신으로의 확대를 우선순위에 둘 필요가 있다. 간섭 측정 기반 QKD는 중앙 노드를 신뢰하지 않아도 되는 구조이므로 하나의 중앙 노드에 다수의 사용자를 접속시키는 스타(star) 구성이 자연스럽고, 국내에서 이미 2×N 형태의 네트워크가 실증된 바 있다[22]. 이를 확장하여 양자 회의키 분배, 양자 비밀분산, 다자간 인증 등으로 응용 범위를 넓히는 편이 거리 지표를 경신하는 것보다는 실용적 가치가 크다. 이는 양자중계기 기술이 성숙하기 전까지 QKD 인프라의 활용도를 높이는 현실적 경로이기도 하다.

둘째, 간섭 측정 기반 QKD의 실용화를 위해서는 거리 기록보다 광원 요구조건의 완화와 실환경 운용 안정성이 중요하다. 모드페어링 QKD와 같이 위상 기준에 대한 요구를 낮춘 방식을 중심으로 상용 부품 기반 시스템을 개발하고 실용망 시험을 추진할 필요가 있다.

셋째, $\sqrt{\eta}$ 스케일링 이상의 확장과 양자얽힘 분배를 위해서는 결국 양자메모리 기반 양자중계기가 필요하다. QKD 기술의 실용화를 병행하여 양자메모리와 광자-물질 인터페이스 등 원천기술을 장기적으로 확보하는 것이 양자통신 기술의 경쟁력을 확보하는 길이 될 것이다.

참고문헌

[1] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature, Vol.299, 1982, pp.802-803.

[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Physical Review Letters, Vol.85, No.2, 2000, pp.441-444.

[3] M. Takeoka, S. Guha and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution", Nature Communications, Vol.5, 2014, art. No.5235.

[4] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, "Fundamental limits of repeaterless quantum communications", Nature Communications, Vol.8, 2017, art. No.15043.

[5] A. Boaron et al., "Secure quantum key distribution over 421 km of optical fiber", Physical Review Letters, Vol.121, No.19, 2018, art. No.190502.

[6] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet", Reviews of Modern Physics, Vol.95, No.4, 2023, art. No.045006.

[7] M. K. Bhaskar et al., "Experimental demonstration of memory-enhanced quantum communication", Nature, Vol.580, 2020, pp.60-64.

[8] Y.-S. Kim, O. Slattery, P. S. Kuo and X. Tang, "Conditions for two-photon interference with coherent pulses", Physical Review A, Vol.87, No.6, 2013, art. No.063843.

[9] M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters", Nature, Vol.557, 2018, pp.400-403.

[10] H.-K. Lo, M. Curty and B. Qi, "Measurement-device-independent quantum key distribution", Physical Review Letters, Vol.108, No.13, 2012, art. No.130503.

[11] X. Ma, P. Zeng and H. Zhou, "Phase-matching quantum key distribution", Physical Review X, Vol.8, No.3, 2018, art. No.031043.

[12] X.-B. Wang, Z.-W. Yu and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error", Physical Review A, Vol.98, No.6, 2018, art. No.062323.

[13] P. Zeng, H. Zhou, W. Wu and X. Ma, "Mode-pairing quantum key distribution", Nature Communications, Vol.13, 2022, art. No.3903.

[14] Y.-M. Xie et al., "Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference", PRX Quantum, Vol.3, No.2, 2022, art. No.020315.

[15] L. Zhang, W. Li, J. Pan, Y. Lu, W. Li, Z.-P. Li, Y. Huang, X. Ma, F. Xu and J.-W. Pan,

"Experimental mode-pairing quantum key distribution surpassing the repeaterless bound", Physical Review X, Vol.15, No.2, 2025, art. No.021037.

[16] M. Minder et al., "Experimental quantum key distribution beyond the repeaterless secret key capacity", Nature Photonics, Vol.13, No.5, 2019, pp.334-338.

[17] J.-P. Chen et al., "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas", Nature Photonics, Vol.15, No.8, 2021, pp.570-575.

[18] Y. Liu et al., "Experimental twin-field quantum key distribution over 1000 km fiber distance", Physical Review Letters, Vol.130, No.21, 2023, art. No.210801.

[19] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics", Nature, Vol.414, 2001, pp.413-418.

[20] W.-Z. Liu et al., "Long-lived remote ion-ion entanglement for scalable quantum repeaters", Nature, Vol.652, 2026, pp.51-57.

[21] T.-X. Zhu, C. Zhang, Z.-W. Ou, X. Liu, P.-J. Liang, X.-M. Hu, Y.-F. Huang, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, "A metropolitan-scale multiplexed quantum repeater with Bell non-locality", Nature Photonics, Vol.20, No.7, 2026, pp.812-817.

[22] C. H. Park et al., "2×N twin-field quantum key distribution network configuration based on polarization, wavelength and time division multiplexing", npj Quantum Information, Vol.8, 2022, art. No.48.

[23] W. Zo, B. Bilash, D. Lee, Y. Kim, H.-T. Lim, K. Oh, S. M. Assad and Y.-S. Kim, "Entanglement swapping via lossy channels using photon-number-encoded states", Physical Review A, Vol.110, No.5, 2024, art. No.052603.

Chapter
02

양자안전 네트워크로의 전환
- PQC · QKD 하이브리드 기술, 검증 및 표준화 -

엄상윤_아이디퀀티크 대표

양자컴퓨터의 실용화 시점은 불확실하지만, 장기 보존 데이터와 교체 주기가 긴 네트워크에서는 전환 지연 자체가 위험 요인이다[9][19]. 본 고에서는 양자내성암호(Post-Quantum Cryptography: PQC)를 범용 전환의 기본 계층으로 보고, 양자키분배(Quantum Key Distribution: QKD)는 고가치 고정 구간의 독립 키 출처로 배치한다. 그리고 암호 정확성, 상호운용, 구현 안전성, 성능 · 용량, 복원력, 거버넌스의 여섯 계층으로 검증 틀을 구성한다[1]-[3][11].

I. 서론

양자안전 전환은 상용화 연도 예측보다 데이터 보호기간 X와 전환 기간 Y의 합이 양자 위협까지 남은 시간 Z보다 긴지를 판단하는 일에서 시작한다[9]. 선수집 · 후해독(Harvest Now, Decrypt Later: HNDL) 위험을 고려하면 기밀 수명이 긴 자산부터 보호 방식과 교체 일정을 정해야 한다[19]-[21].

병목은 시스템 곳곳에 얽힌 암호 의존성이다. 전송 계층 보안(Transport Layer Security: TLS) 라이브러리, 인증서, 하드웨어 보안 모듈(Hardware Security Module: HSM), 가상 사설망(Virtual Private Network: VPN), 펌웨어 서명과 조달 주기가 서로 맞물린다. 미국 국립표준기술연구소(National Institute of Standards and Technology: NIST)가 정의한 암호민첩성은 이러한 구성요소를 교체하면서도 보안과 운영을 유지하는 능력이다[4]. 따라서 자산 목록에는 사용 위치, 호출 주체와 교체 책임도 기록되어야 한다.

* 본 내용은 엄상윤 대표(☎ 031-608-3018, sangyun.uhm@idquantique.com)에게 문의하시기 바랍니다.
** 본 원고는 2026년 10월 18일까지 공개된 표준 · 정책 · 연구 자료를 기준으로 작성
***본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

NIST는 2024년 8월 모듈 격자 기반 키 캡슐화 메커니즘(Module-Lattice-Based Key-Encapsulation Mechanism: ML-KEM), 모듈 격자 기반 전자서명 알고리즘(Module-Lattice-Based Digital Signature Algorithm: ML-DSA), 상태 비저장 해시 기반 전자서명 알고리즘(Stateless Hash-Based Digital Signature Algorithm: SLH-DSA)을 미국 연방 정보처리 표준(Federal Information Processing Standards: FIPS) 203 · 204 · 205로 확정했다[1]-[3]. 인터넷기술표준화기구(Internet Engineering Task Force: IETF)는 2026년 RFC 9954와 RFC 10024를, 유럽전기통신표준협회(European Telecommunications Standards Institute: ETSI)는 PQC · QKD 결합 규격 TS 104 146을 발간했다[7][8][11]. 논의의 초점은 알고리즘 선정에서 안전한 배치와 검증으로 옮겨갔다.

본 고는 두 기술의 우열보다 배치 조건에 초점을 맞춰, II장은 PQC 전환, III장은 QKD와 하이브리드, IV장은 실증과 여섯 계층 검증, V장은 국내 배치 원칙을 다룬다.

II. 양자안전 네트워크와 PQC 전환

1. PQC와 QKD가 보호하는 대상

PQC는 격자 · 해시 등 양자 공격에 견딜 것으로 평가되는 수학 문제로 키 캡슐화 메커니즘(Key-Encapsulation Mechanism: KEM)과 전자서명을 제공하며 기존 인터넷 프로토콜(Internet Protocol: IP)망과 공개키 기반 구조(Public Key Infrastructure: PKI)에 단계적으로 배치할 수 있다. QKD는 양자 상태가 측정될 때 생기는 교란을 통계적으로 확인하여 도청 가능성을 판정하고 대칭키 재료를 공급한다. [표 1]은 두 기술의 보안 근거, 배치 범위와 검증 초점을 비교하지만, QKD가 데이터 암호화, 상대 인증, 단말 보안과 키 관리 전체를 보장하지는 않는다[11][15][16].

[표 1]의 하이브리드 설계는 서로 다른 키 재료를 한 세션에 결속하고 인증·키 동기화 · 장애 정책을 함께 검증하며, PQC는 범용 경로의 기본 수단으로, QKD는 고가치 고정 구간의 보완 수단으로 배치하는 방식이다[11][22].

[표 1] PQC와 QKD의 역할 비교

구분	PQC	QKD	하이브리드 설계의 의미
보안 근거	계산 복잡도와 표준화된 알고리즘	양자 상태 측정과 물리적 교란	서로 다른 실패 원인을 가진 키 출처 구성
주요 기능	키 캡슐화, 서명, 인증서, 프로토콜 보호	대칭키 재료의 생성 · 분배	세션 키와 인증을 하나의 문맥에 결속
배치 범위	인터넷, 클라우드, 단말, 임베디드까지 확장 가능	광 경로와 키 관리가 가능한 제한 구간	PQC 기본, QKD 선별의 위험 기반 배치
대표 제약	키 · 서명 크기, 연산량 · 메모리, 구현 공격, 교체 복잡도	거리 · 손실, 신뢰 노드, 장비 비용, 가용성	강등, 키 비동기, 공통 구현 결함, 장애 정책
검증 초점	알고리즘 적합성, 프로토콜, 성능, 부채널	양자 광학, 키 관리, API, 물리 보호	결합 함수, 독립성, 인증, 추적성, 복구

〈자료〉 [1]-[3], [11], [13]-[17], [22] 재구성

2. 계층형 기준 구조

[그림 1]은 양자안전 네트워크를 세 층으로 나누며, PQC 신뢰 체계와 QKD 키 서비스가 독립 키 출처를 이루고, 조정 · 통합 층은 키 유도 함수(Key Derivation Function: KDF), 키 식별자와 장애 전환을 관리한다. 서비스 층은 TLS, 인터넷 프로토콜 보안(Internet Protocol Security: IPsec), 매체 접근 제어 보안(Media Access Control Security: MACsec)과 응용



* 원칙: PQC는 기본 계층, QKD는 선별 계층, 정책과 검증은 공통 계층
〈자료〉 [1]-[5], [11], [13]-[17] 재구성

[그림 1] 위험 등급에 따른 양자안전 네트워크 기준 구조

프로그램 암호화에 키를 전달한다.

조정 · 통합 층은 장비나 알고리즘이 바뀌어도 장애 정책과 감사 항목을 유지해야 한다. 또한, 알고리즘 묶음, 키 출처, 상대 신원과 프로토콜 대화록을 같은 세션 식별자에 결속해 장애 뒤 보안 등급의 유지 여부를 판정해야 한다.

3. PQC 표준 확정 이후의 네트워크 전환

가. 알고리즘 선택에서 암호민첩성

FIPS 203은 ML-KEM의 세 매개변수 집합을, FIPS 204와 205는 ML-DSA와 SLH-DSA를 정의한다[1]-[3]. RFC 10024의 세 TLS 그룹 가운데 두 그룹은 ML-KEM-768을 사용한다[8]. NIST는 해밍 준순환(Hamming Quasi-Cyclic: HQC) 부호 기반 KEM을 추가 표준화 대상으로 선정했다[6]. 제품에서는 알고리즘과 인증서 프로파일이 교체가 가능한 정책 객체로 관리되어야 한다.

NIST SP 800-227과 암호민첩성 지침은 KEM 통합, 난수, 디캡슐레이션 실패, 키 삭제와 부채널 대응을 각각 점검할 항목으로 제시한다[4][5]. 암호자산 목록에는 라이브러리 · 버전, 인증서 체계, HSM 의존성, 상대 시스템, 보호기간과 담당자를 기록하고 시험 벡터와 상호운용 증거를 남겨야 한다.

나. TLS 1.3 하이브리드 키 교환의 표준화

RFC 9954는 TLS 1.3에서 복수 키 교환 결과를 결합하는 일반 구조를 설명하는 정보 제공 문서다[7]. RFC 10024는 임시 타원곡선 디피-헬먼(Elliptic Curve Diffie-Hellman Ephemeral: ECDHE)과 ML-KEM을 결합한 세 그룹의 상호운용 규칙을 정한 제안 표준이다[8].

[표 2]는 알고리즘 적합성부터 KEM 통합, TLS 그룹, QKD 평가와 네트워크 구조까지 주요 문서의 지위 · 발간 시점과 담당 범위를 비교하며, 각 문서는 서로 다른 검증 단위를 다루므로 어느 하나가 다른 문서를 대신하지 않는다. NIST는 알고리즘과 KEM 통합, IETF는 TLS 결합, ETSI는 하이브리드 키 설정, ISO/IEC와 ITU-T는 QKD 평가와 망 구조를 담당한다[1]-[5][7][8][10]-[17]. 따라서 제품 검증에서는 지원 조합, 실패 코드와 지연이 따로 측정되어야 한다.

[표 2] 2026년 10월 기준 주요 표준과 전환 의미

영역	문서	문서 지위 · 발간 시점	실무적 의미
PQC 알고리즘	NIST FIPS 203 · 204 · 205	최종 표준(2024. 8.)	KEM과 서명의 조달 · 시험 기준 확정
KEM 사용	NIST SP 800-227	최종 권고(2025. 9.)	KEM 통합과 구현 안전성 지침
TLS 결합	IETF RFC 9954	정보 제공 RFC(2026. 7.)	TLS 1.3 하이브리드 키 교환 일반 구조
TLS 그룹	IETF RFC 10024	제안 표준 RFC(2026. 8.)	ECDHE와 ML-KEM 결합 그룹의 상호운용 기준
전통+PQC	ETSI TS 103 744 V1.2.2	기술규격(2026. 2.)	ECDH와 ML-KEM 기반 하이브리드 키 설정
PQC+QKD	ETSI TS 104 146 V1.1.1	기술규격(2026. 8.)	PQC · QKD · 선택적 전통 키와 양자안전 인증 결합
QKD 평가	ISO/IEC 23837-1·2	국제표준(2023. 8. · 9.)	QKD 구성요소 · 프로토콜의 보안 요구와 시험 방법
QKD 네트워크	ITU-T Y.3800 계열	권고 · 보충서(지속 개정)	요구사항, 기능 구조, 키 관리, 제어 · 관리 기준

〈자료〉 [1]-[5], [7], [8], [10]-[17] 재구성

다. 배치 공학의 핵심 점검 항목

PQC 전환은 인증서뿐 아니라 상태 확인, 폐기 목록, 코드 서명, 타임스탬프, HSM, 장비의 인증서 길이와 로그 규칙을 함께 시험해야 한다[4][5]. 암호 구성명세서(Cryptographic Bill of Materials: CBOM)에는 라이브러리 버전, 서비스 · 공급사 의존성, 교체 담당자와 기한을 기록한다[4][32].

긴 인증서 체인과 하이브리드 키 공유가 최대 전송 단위(Maximum Transmission Unit: MTU)를 넘으면 단편화, 전송 제어 프로토콜(Transmission Control Protocol: TCP) 분할, QUIC 재조립과 프록시 버퍼 문제가 생길 수 있다. 정상 연결과 함께 잘못된 암호문, 미지원 그룹, 인증서 검증 실패와 재전송 폭주를 시험하고 지연 · 메모리 · 복구 시간을 기록해야 한다[5][8].

III. QKD 네트워크와 하이브리드 기술

1. 링크가 아니라 키 서비스로 평가

QKD는 전송 거리, 양자비트 오류율(Quantum Bit Error Rate: QBER)과 비밀키율만으로 평가할 수 없다. 양자 · 고전 채널, QKD 장비, 키 관리 시스템(Key Management System:

KMS), 신뢰 노드와 응용 프로그램 인터페이스가 하나의 키 공급망을 이룬다[표 3].

ETSI GS QKD 004와 014는 키 요청 및 표현 상태 전송(Representational State Transfer: REST) 방식 응용 프로그램 인터페이스(Application Programming Interface: API)를 정의한다[13][14]. 키 ID는 한 번만 소비되어야 하며, API 채널도 상호 인증과 기밀성·무결성 보호가 필요하다[11]. 운영자는 생성률, 소비율, 버퍼 수위, 키 나이와 동기화 상태를 추적하고 다중 경로의 우회가 정책과 맞는지 확인해야 한다[17].

2. 보안 평가와 인증의 경계

ISO/IEC 23837-1·2는 QKD의 전통적 구성요소, 양자 광학 구성요소와 전체 프로토콜에 대한 보안 요구 및 시험 방법을 규정한다[15][16]. 평가는 광원·검출기, 후처리, 난수, 인증, 펌웨어와 키 출력 경계를 포함해야 하며, 장비 인증을 다중 공급사 KMS와 응용 프로그램까지 자동 확대해서는 안 된다.

미국 국가안보국(National Security Agency: NSA)은 국가 안보 시스템에서 인증, 전용 장비·광 구간, 신뢰 릴레이, 구현 검증과 서비스 거부 대응의 제약을 들어 QKD를 권고하지 않는다[22]. 이 입장은 민간망 전체를 배제하는 근거가 아니라, 도입 전에 인증·가용성·운영 비용을 먼저 점검해야 한다는 경고로 해석되어야 한다. QBER 상승 시 중단·폐기·우회·조사 기준도 미리 정해야 한다.

[표 3]은 링크 상태를 키 관리·인터페이스·서비스 증거와 연결한다. QBER가 정상이어도

[표 3] QKD 실증에서 측정해야 할 서비스 지표

계층	대표 지표	시험 질문	필요 증거
양자 링크	QBER, 비밀키율, 광 손실, 거리	환경 변화와 공격 모사에서 임계치가 일관적인가	원시 측정값, 교정 기록, 시간 동기 로그
키 관리	버퍼 수위, 키 나이, 폐기량, ID 중복	키가 한 번만 소비되고 양 끝 상태가 맞는가	KMS 감사 로그, 키 생애주기 기록
인터페이스	API 성공률, 인증 실패, 응답 지연	ETSI API와 다중 공급사 조합이 연동되는가	상호운용 시험표, 오류 코드, 패킷 추적
서비스	재키잉 간격, 암호화 가용성, 복구 시간	키 고갈·링크 중단 시 사전 정책대로 동작하는가	장애 주입 결과, 서비스 수준 협약(Service Level Agreement: SLA) 보고서
보안	부채널, 설정 변경, 물리 침입, 강등	관리자·공급망·단말 위협이 통제되는가	평가서, 설정 기준선, 침투시험 결과

〈자료〉 [11], [13]-[17] 재구성

키 ID 중복이나 API 인증 실패가 있으면 서비스는 통과할 수 없다. 원시 측정값과 KMS 로그, 패킷 추적, 복구 시간을 같은 사건 식별자로 묶어야 한다[11][13]-[17].

3. PQC · QKD 하이브리드 기술

가. 세 가지 하이브리드의 구분

'하이브리드'는 전통 키 교환과 PQC를 결합하는 알고리즘 방식, PQC와 QKD 재료를 결합하는 키 출처 방식, 장애 때 전환 · 거부를 정하는 운영 방식으로 구분된다[8][11].

ETSI TS 104 146은 전통 키 교환, PQC와 QKD 재료를 양자안전 인증 및 KDF와 결합한다[11]. Buruaga 등은 MACsec에 적용되는 결합 방식을 제시했으나 QKD 키 모의기를 사용했으므로 실장비의 지연과 키 고갈은 별도로 시험되어야 한다[18].

키 재료는 길이와 순서를 구분하고 세션 · 용도 값을 KDF에 넣어야 한다. [식 1]은 해시 기반 메시지 인증 코드 기반 추출 · 확장 키 유도 함수(HMAC-based Extract-and-Expand Key Derivation Function: HKDF)를 적용한 개념 식이다[34]. 구현 시 공통 난수원 · 라이브러리 · 관리자 계정이 두 경로를 함께 손상시킬 가능성도 점검해야 한다[11][18].

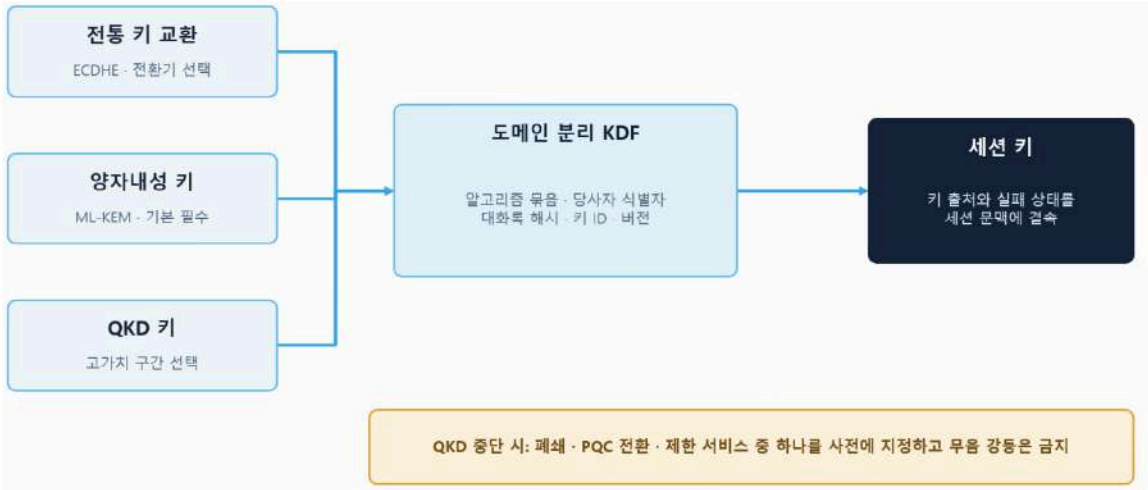
K_session = HKDF-Expand(HKDF-Extract(salt, Z_cl ‖ Z_pq ‖ K_qkd), "QSN-v1" ‖ context, L) [식 1]

※ [식 1]은 RFC 5869의 HKDF 추출 · 확장 구조를 하이브리드 키 출처에 적용한 필자 구성임[11][18][34]

[식 1]에서 Z_cl은 전통 키 교환 비밀, Z_pq는 PQC KEM 비밀, K_qkd는 QKD 키이며 K_session은 최종 세션 키이다. 솔트(salt)는 추출 단계에 선택적으로 입력되는 비밀이 아닌 값이고, L은 출력 길이(바이트)다. HKDF-Extract는 솔트와 결합 재료로 의사난수 키를 만들고, HKDF-Expand는 'QSN-v1'과 문맥 정보(context)를 반영해 최종 키를 확장한다[34]. 문맥 정보에는 알고리즘 묶음, 양 끝 식별자, 대화록 해시, 키 출처 ID, 규격 버전과 용도가 포함된다[11].

나. 인증, 키 추적성, 장애 전환

QKD 자체는 상대 신원을 보장하지 않으므로, 최초 세션은 양자내성 서명 인증서, 양자안전 사전 공유키 또는 승인된 수단으로 인증하고, QKD 키 사용과 양자안전 인증은 별도 통제로



〈자료〉 ETSI, "Authenticated Quantum Safe Hybrid Key Establishment", ETSI TS 104 146 V1.1.1, 2026. 8, pp.1-17. J. S. Buruaga et al., "Versatile quantum-safe hybrid key exchange and its application to MACsec", EPJ Quantum Technology, Vol.12, Article 84, 2025. 7. 4, pp.1-27.재구성

[그림 2] 키 출처 결합과 장애 전환 정책의 관계

기록한다[11][18].

키 추적성은 키 값이 아니라 PQC 매개변수, QKD 키 ID, KDF 프로파일, 생성·소비 시각, 통신 상대·경로·정책 버전의 메타데이터를 관리하는 일이다. 키 값은 로그에서 제외하고 ID가 일치하지 않으면 격리·재동기화한다[11].

장애 전환 정책은 세 가지로 구분된다. QKD 공급이 끊기면 새 세션을 거부하는 폐쇄 정책, 경보와 시간제한을 두고 PQC 단독으로 바꾸는 전환 정책, 제한된 명령만 허용하는

[표 4] 하이브리드 구현 프로파일 예시

프로파일	키 구성	인증	장애 시 정책	적합 구간
H1 전환	ECDHE + ML-KEM	기존 또는 PQ 인증	PQC 필수, 전통 구성은 단계적 제거	인터넷·클라우드 전반
H2 고가치	ML-KEM + QKD	양자내성 서명 또는 양자안전 사전 공유키 (Pre-Shared Key: PSK)	QKD 중단 시 PQC 전환과 즉시 경보	금융·정부·데이터센터 백본
H3 최고 등급	ECDHE + ML-KEM + QKD	양자내성 서명과 엄격한 장비 인증	QKD 중단 시 폐쇄 또는 승인된 제한 서비스	장기기밀 핵심 고정 구간
H4 복원력	복수 PQC + 복수 QKD 경로	양자내성 인증과 분리된 운영 권한	경로 재선정 후 정책 기준 재검증	다중 도메인 중요 기반 설비

〈자료〉 [8], [11], [18], [22] 재구성

축소 서비스 정책이다. [그림 2]는 전통 키, PQC 키와 QKD 키가 도메인 분리 KDF를 거쳐 결합하고 장애 정책이 빠진 출처를 판정하는 흐름을 보여준다.

[표 4]는 전환기 호환(H1), QKD 중단 시 PQC 전환(H2), 폐쇄 또는 제한 서비스(H3), 복수 경로 재검증(H4)을 구분한다. 데이터 등급, 허용 중단시간, 대체 경로와 키 버퍼에 따라 프로파일이 선택되며, 무음 강등은 허용되지 않는다.

IV. 국내외 실증 및 여섯 계층 검증 프레임

1. 국가 로드맵의 자산 식별 · 우선순위 · 완료 시점

영국은 2028년 계획, 2031년 우선 전환, 2035년 전면 전환을 제시했고[19], 캐나다도 2031년 우선 시스템과 2035년 나머지 시스템 전환을 목표로 한다[21]. 유럽연합은 2026년 말 전환 착수와 2030년 말 핵심 기반 시설의 PQC 전환을 권고했다[20]. 구속력은 달라도 자산 식별, 위험 분류, 시험, 조달과 단계적 배치라는 순서는 같다.

미국 행정명령 14412호는 전환 책임자 지정과 고가치 · 고영향 시스템의 키 설정 및 전자서명 전환 지침을 요구한다[32]. 목표 시점은 각각 2030년 말과 2031년 말이며, NIST 시범 전환은 2027년 말이다. 행정명령 14413호는 양자 연구 · 상용화 · 공급망 정책을 갱신했다[33].

통신 분야에서는 3세대이동통신표준화협력기구(3rd Generation Partnership Project: 3GPP) TR 33.703이 5G 시스템의 PQC 전환 영향을 다루고[28], 세계이동통신사업자협회(GSMA) PQ.03은 단말 · 망 · 로밍 · 인증별 전환 지침을 제시한다[29].

2. QKD 실증의 다중 공급사·서비스 검증

유럽 양자통신 기반 설비(European Quantum Communication Infrastructure: Euro QCI)는 27개 회원국의 지상 · 위성 구간과 시험 · 평가 기반을 연결한다[23]. 싱가포르 국가 양자안전망 플러스(National Quantum-Safe Network Plus: NQSN+)는 통신사업자와 기업의 상호운용 시험을 지원한다[24]. 다만, 영국의 2026년 독립 연구는 QKD가 대체로 시험망과 시범 배치에 머문다고 평가했다[25].

3. 국내: 알고리즘, 전환, 시험망의 연결

국내에서는 2025년 한국형 양자내성암호(KpqC)의 KEM 분야 NTRU+ · SMAUG-T와 전자서명 분야 HAETAE · AIMer가 표준 대상 알고리즘으로 선정되었고[26], 지식재산정보 분석 플랫폼(IP One Portal: IPOP)에 실증 적용이 추진되었다[27]. 과학기술정보통신부는 PQC 시범 전환과 PQC · QKD 결합 기술개발을 추진하고 있으며, 서울 · 판교 · 대전 구간의 개방형 양자 시험망에서는 수요기관 참여형 검증이 확대되고 있다[30][31]. 성과는 구매 명세와 검증 보고서에 기록된 시험 결과를 기준으로 평가되어야 한다.

4. 실증에서 검증으로: 여섯 계층 평가 프레임

실증은 정해진 조건에서 시스템이 정상 작동하는지를 확인하는 과정이며, 검증은 오류 · 공격 · 복구 상황에서도 보안 속성이 유지되는지까지 확인해야 한다. [표 5]는 암호 정확성부터 거버넌스까지 여섯 계층을 시험과 산출물에 연결한 제안으로[4][5][11][13]-[17][22], 같은 빌드 · 설정 · 망 구조 식별자로 묶어 회귀 시험에 다시 사용한다.

[표 5] 양자안전 네트워크 검증 프레임과 최소 산출물

검증 층	핵심 시험	권장 지표 · 판정 기준	최소 산출물
1. 암호 정확성	알고리즘 시험 벡터, KEM 실패 처리, 서명 검증	승인 매개변수 전부 통과, 오류가 비밀을 누설하지 않음	시험 벡터 결과, 라이브러리 · 빌드 해시
2. 상호운용	RFC · ETSI 프로파일, 다중 공급사, 버전 협상	지원 조합별 성공 · 실패 코드 일치, 모호한 협상 없음	조합 행렬, 패킷 추적, API 로그
3. 구현 안전성	난수, 키 삭제, 부채널, 권한, 공급망	위협 모형별 허용 기준 충족, 중대 취약점 미해결 0건	코드 · 구성 검토서, 침투 · 부채널 시험
4. 성능 · 용량	정상 · 폭주 · 장거리 · 키 고갈 부하	95 · 99백분위 지연, 연산량 · 메모리, 키율, 버퍼가 서비스 수준 협약 범위 내	기준선 대비 보고서, 용량 모형
5. 복원력	광 단절, KMS 이중화, 패킷 손실, 잘못된 암호문, 강등	정책대로 폐쇄 · 전환 · 축소, 복구목표시간 · 복구목표시점 충족	장애 주입 기록, 복구 경과 기록
6. 거버넌스	CBOM, 인증서 · 키 수명, 패치 · 조달 · 폐기	소유자 · 교체 기한 · 예외 승인 추적 가능	CBOM, 위험등록부, 예외 · 감사 기록

〈자료〉 [4], [5], [11], [13]-[17], [22] 재구성

가. 필수 장애 주입 시나리오

- PQC · QKD: 미지원 매개변수, 잘못된 KEM 암호문, 인증서 팽창 · MTU 초과, 광 손실, QBER 상승, 키 버퍼 고갈과 KMS 전환을 주입한다.
- 하이브리드 · 운영: 인증 실패, KDF 문맥 불일치, 버전 롤백, 무음 강등, 인증서 철회와 공급사 패치 뒤 세션 결과 · 경보 · 추적성을 확인한다.

나. 성능 수치보다 정책 준수율

성능 최고값보다 정책 준수율이 중요하다. QKD 키가 부족할 때 H2 세션은 PQC로 전환되고 H3 세션은 닫혀야 한다. 검증 보고서에는 날짜, 장비 · 펌웨어, 라이브러리, KMS, 광 경로, 트래픽과 정책 버전을 기록하고, 재현 가능한 입력 · 관측값 · 판정 근거 · 제한을 남겨야 한다.

V. 국내 전환 전략과 시사점

1. 전 구간 PQC, 전환기 이중화, 선별 QKD

배치는 세 단계로 나뉜다. 1단계에서는 신규 조달 시 암호자산 목록, 알고리즘 교체 인터페이스, 패킷 · 인증서 크기와 시험 가능한 오류 처리가 요구된다. 2단계에서는 인터넷 경계, 원격접속, 데이터센터 트래픽과 코드 · 펌웨어 서명에 전통 공개키와 PQC가 함께 배치되고 제거 기한이 정해져야 한다.

3단계에서는 장기 기밀 · 고가치 · 고정 경로 · 물리 관리 조건을 충족하는 구간에 PQC · QKD가 결합된다. 위험 분류에는 기밀 수명, 중단 영향, 단말 수, 광 경로 통제, 규제와 교체 주기를 반영하고 등급별 프로파일과 예외 승인 절차를 둔다.

2. 정책 · 표준 · 산업 과제

- 공통 기준과 증거: 부문별 공통 용어와 키 결합 프로파일을 쓰고, 알고리즘 · 장비 · API · 종단 간 장애 시험의 경계와 결과 재사용 조건을 정한다.

- 조달과 암호민첩성: 교체 시간, 지원 프로파일, CBOM, 회귀 시험과 공급 종료 뒤 패치 의무를 계약에 넣는다.
- 국산 · 국제 연계: KpqC 적용성과 NIST · IETF · ETSI 프로파일의 이중 지원 비용을 검증하고, 민감 정보를 제외한 시험 조건 · 실패 유형 · 성능 분포를 공유한다.

국내 시험망은 단일 장비의 최고 성능보다 재현 가능한 프로파일을 남겨야 한다. 알고리즘, API, 장비와 서비스의 경계를 나누고 어떤 변경이 재시험을 요구하는지 밝혀야 한다. 하지만 오래된 장비와 승인 절차가 병목이 될 수 있으므로 1년 안에는 자산 목록을, 2년 안에는 조달 규격을, 3년 안에는 우선 서비스 검증을 완료 기준으로 두어야 한다.

3. 맺음말

양자안전 전환의 성패는 가장 강한 알고리즘보다 교체 가능한 운영 구조에 달려 있다. 범용 경로에는 PQC를 먼저 적용하고, 장기 기밀성과 높은 자산 가치가 있으며, 광 경로를 물리적으로 통제할 수 있는 고정 구간에는 QKD를 독립 키 출처로 추가하는 것을 기본 원칙으로 제안한다.

기밀 수명이 짧고 단말이 많은 서비스에서는 PQC와 암호민첩성이 우선이다. 수십 년간 보호할 데이터가 소수의 고정 거점을 오가고 광 전송 경로가 관리될 때 QKD 도입 비용을 검토할 근거가 생긴다[11][19]-[22].

표준을 준수했다는 사실만으로 서비스 검증이 끝나지는 않는다. 표 5의 여섯 계층에 따라 알고리즘 적합성 · 장비 평가 · API 상호운용을 확인한 뒤, 실제 트래픽과 장애에서도 서비스 정책이 지켜지는지 다시 시험해야 한다. QKD 키 고갈 때 H3 세션이 열리거나 협상 실패 뒤 전통 암호로 무음 강등되면 불합격이다. 잘못된 암호문, 인증 실패, 키 ID 불일치, 광 단절과 패치 뒤 회귀 시험도 같은 승인 절차에 포함되어야 한다[표 5].

국내 정책은 암호자산과 기밀 수명의 분류에서 시작해야 한다. 신규 조달 계약에는 교체 인터페이스, CBOM, 회귀 시험과 공급 종료 뒤 패치 의무가 포함되어야 한다[19]-[21][32]. 필자는 첫해에 자산 목록과 보호기간을 정리하고, 둘째 해에 공통 조달 문구와 최소 시험표를 확정하며, 셋째 해에 금융 · 통신 · 공공 대표 서비스를 교차 검증할 것을 제안한다. 중앙 정책에서는 증거 형식과 상호 인정 조건을 정하고, 부문 기관에서는 위험 등급과 장애 정책을 관리하는 책임을 맡아야 한다.

참고문헌

[1] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", U.S. Department of Commerce, FIPS 203, 2024. 8. 13, pp.1-56.

[2] NIST, "Module-Lattice-Based Digital Signature Standard", U.S. Department of Commerce, FIPS 204, 2024. 8. 13, pp.1-65.

[3] NIST, "Stateless Hash-Based Digital Signature Standard", U.S. Department of Commerce, FIPS 205, 2024. 8. 13, pp.1-61.

[4] E. Barker et al., "Considerations for Achieving Crypto Agility: Strategies and Practices", NIST CSWP 39upd1, 2026. 6. 29, pp.1-47.

[5] G. Alagic et al., "Recommendations for Key-Encapsulation Mechanisms", NIST SP 800-227, 2025. 9. 18, pp.1-64.

[6] NIST, "Post-Quantum Cryptography Standardization", PQC Project, 2026. 10. 18.

[7] D. Stebila, S. Fluhrer, S. Gueron, "Hybrid Key Exchange in TLS 1.3", IETF, RFC 9954, 2026. 7, pp.1-18.

[8] K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, D. Stebila, "Post-Quantum Traditional(PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3", IETF, RFC 10024, 2026. 8, pp.1-9.

[9] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?", IEEE Security & Privacy, Vol.16, No.5, 2018. 9.-10, pp.38-41.

[10] ETSI, "Quantum-safe Hybrid Key Establishment", ETSI TS 103 744 V1.2.2, 2026. 2, pp.1-36.

[11] ETSI, "Authenticated Quantum Safe Hybrid Key Establishment", ETSI TS 104 146 V1.1.1, 2026. 8, pp.1-17.

[12] ETSI, "Quantum Safe Enterprise Transport Security", ETSI TS 104 145 V1.2.1, 2026. 8, pp.1-32.

[13] ETSI, "Quantum Key Distribution(QKD); Application Interface", ETSI GS QKD 004 V2.1.1, 2020. 8, pp.1-22.

[14] ETSI, "Quantum Key Distribution(QKD); Protocol and Data Format of REST-based Key Delivery API", ETSI GS QKD 014 V1.1.1, 2019. 2, pp.1-22.

[15] ISO/IEC, "Information Security, Cybersecurity and Privacy Protection-Security Requirements, Test and Evaluation Methods for Quantum Key Distribution-Part 1: Requirements", ISO/IEC 23837-1:2023, 2023. 8, pp.1-52.

[16] ISO/IEC, "Information Security, Cybersecurity and Privacy Protection-Security Requirements, Test and Evaluation Methods for Quantum Key Distribution-Part 2: Evaluation and Testing Methods", ISO/IEC 23837-2:2023, 2023. 9, pp.1-106.

[17] ITU-T, "Standardization Roadmap on Quantum Key Distribution Networks", Supplement 74 to ITU-T Y-series, 2023. 3, pp.1-25.

[18] J. S. Buruaga et al., "Versatile quantum-safe hybrid key exchange and its application to MACsec", EPJ Quantum Technology, Vol.12, Article 84, 2025. 7. 4, pp.1-27.

[19] UK NCSC, "Timelines for Migration to Post-Quantum Cryptography", NCSC Guidance, 2025. 3. 20.
[20] European Commission, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography", Shaping Europe's Digital Future, 2025. 6. 23.
[21] Canadian Centre for Cyber Security, "Roadmap for the migration to post-quantum cryptography for the Government of Canada", Government of Canada, ITSM.40.001, 2025. 6. 23.
[22] NSA, "Quantum Key Distribution and Quantum Cryptography", NSA Cybersecurity Information, 2026. 10. 18.
[23] European Commission, "European Quantum Communication Infrastructure(EuroQCI)", Shaping Europe's Digital Future, 2026. 10. 18.
[24] IMDA, "Singapore Launches Southeast Asia's First Quantum-Safe Network Infrastructure", IMDA 보도자료, 2023. 6. 6.
[25] Technopolis, "Quantum Key Distribution Research Report", UK DSIT, DSIT 2026/010, 2026. 6. 10.
[26] 한국인터넷진흥원, "양자내성암호 개요 및 KpqC 추진 현황", 암호이용활성화, 2026. 10. 18.
[27] 지식재산처, "정부 최초로 온라인시스템에 한국형 양자내성암호 실증적용 추진", 보도자료, 2026. 2. 3.
[28] 3GPP, "Study on transitioning to Post Quantum Cryptography(PQC) in 3GPP", TR 33.703 V20.1.0, Release 20, 2026. 9. 28.
[29] GSMA, "Post Quantum Cryptography: Guidelines for Telecom Use Cases", PQ.03 Version 2.0, 2024. 10. 4, pp.1-146.
[30] 과학기술정보통신부, "양자 보안, 더 이상 선택이 아닌 필수, 양자내성암호 실증 확대 및 핵심기술 개발 본격 착수", 보도자료, 2026. 5. 6.
[31] 과학기술정보통신부, "양자암호통신 기술 실증으로 산업 활용 앞당긴다", 보도자료, 2026. 5. 6, p.1.
[32] The White House, "Securing the Nation Against Advanced Cryptographic Attacks", Executive Order 14412, Federal Register, Vol.91, 2026. 6. 25, pp.38483-38486.
[33] The White House, "Ushering in the Next Frontier of Quantum Innovation", Executive Order 14413, Federal Register, Vol.91, 2026. 6. 25, pp.38487-38491.
[34] H. Krawczyk, P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function(HKDF)", IETF, RFC 5869, 2010. 5, pp.1-14.

Chapter 03

이종 로봇 체화 간 지능 전이 공유 기술 동향

- 휴머노이드 로봇을 중심으로 -

장민수_한국전자통신연구원 책임연구원

이종 로봇 체화 간 지능 전이는 한 로봇에서 학습한 작업 능력을 기능과 형태가 다른 이종 로봇으로 전이 공유하는 기술이다. 로봇 파운데이션 모델(Robot Foundation Model: RFM)과 대규모 로봇 데이터셋의 등장과 함께 단일 로봇에 종속되던 로봇 지능 모델이 다중 체화 공유 지능으로 확장되고 있으나 이종 로봇에 지능을 전이할 때 발생하는 심각한 성능 저하 문제는 여전히 존재한다. 본 고는 체화 간 지능 전이 기술을 체화 간 지능 전이 학습용 데이터셋, 체화 교체 영상 생성, 체화 독립적 잠재 행동 표현 학습, 월드 액션 모델(World Action Model), 기구학 기반 스킬 전이의 다섯 유형으로 분류하고 국내외 동향을 소개한다.

I. 서론

인공지능(Artificial Intelligence: AI)은 언어와 시각 인지 능력을 넘어 실세계 환경을 이해하고 물리적인 작업을 수행하는 피지컬 AI(Physical AI)로 확장되고 있으며, 그 핵심 응용 플랫폼으로 휴머노이드 로봇이 부상하고 있다[1]. 휴머노이드 로봇은 인간과 동일한 환경 조건에서 다양한 작업을 수행할 수 있다는 잠재력을 인정받으며 형태가 서로 다른 다수 플랫폼이 동시에 등장하고 있다. 미국 보스턴다이나믹스(Boston Dynamics)와 현대자동차의 Atlas, 미국 피규어 AI(Figure AI)의 Figure, 노르웨이 1X 테크놀로지스(1X Technologies)의 NEO, 중국 유니트리(Unitree)의 G1과 H1, 한국 로보티즈(ROBOTIS)의 AI Worker, 한국 레인보우로보틱스(Rainbow Robotics)의 RB-Y1 등이 대표적이다.

* 본 내용은 장민수 책임연구원(☎ 042-860-1250, minsu@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
*** 본 고는 관련 논문과 보고서 리뷰, 심층분석, 초안 작성 등 핵심 분석 활동은 저자들이 수행하였으며, 문장 표현의 개선을 위해 생성형 AI인 클로드 Sonnet 4.6 버전을 활용하였다.
****본 고는 2026년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (IRIS 연구개발과제번호: RS-2026-25550793, 연구개발과제명: 다양한 형태의 휴머노이드 간 작업 지능 공유를 위한 체화 인지 기반 행동 생성과 작업 계획 기술 개발)

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

휴머노이드 로봇은 다른 유형의 로봇에 비해 모델별로 구조와 기능의 차이가 크다. 크기, 전신 자유도, 가반하중(payload), 촉각 센서 유무 등이 모델마다 상이하다. 중국 유니트리 G1과 한국 로보티즈 AI Worker를 비교하면 체화 구조의 차이가 뚜렷하게 드러난다. G1은 키 1.3m, 무게 35㎏, 양팔 자유도 10인 이족 보행 로봇이고, AI Worker는 키 1.6m, 무게 90㎏, 양팔 자유도 14인 휠형 이동 로봇이다. 이처럼 구조와 기능이 다른 두 로봇은 동일 작업을 수행하더라도 요구되는 관절 제어와 동작 계획 방법이 서로 다르다.

로봇 학습에서 체화(embodiment)는 로봇이 물리 세계와 상호작용하는 신체 형태와 기능 전체를 가리킨다. 관절의 개수와 배치, 링크 길이, 엔드이펙터(end-effector) 형태, 센서 구성, 이동 방식 등이 로봇의 체화를 규정한다. 일반적으로 로봇의 작업 지능은 주어진 로봇 체화의 관절 공간과 지각 정보 구조에 종속적으로 학습된다. 따라서 센서 구성과 관절 구조가 다른 로봇들은 센서 데이터와 행동을 표현하는 값의 범위와 차원이 서로 일치하지 않는다. 물리적으로도 로봇 크기에 따라 팔 도달 범위나 보폭이 다르면 같은 물체를 잡는 작업이라도 요구되는 관절 움직임이 달라진다.

이러한 휴머노이드 로봇 간 체화 구조의 차이는 로봇 작업 지능을 구현하고 활용하는 것에 심각한 장벽으로 작용한다. 로봇 A에서 학습한 정책을 형태가 다른 로봇 B에 그대로 적용하면 성능이 급격히 저하되기 때문이다. 새 로봇마다 데이터 수집과 재학습을 반복해야 하는 부담은 휴머노이드 로봇의 보급과 실용화에 핵심 병목으로 작용한다. 이종 로봇 체화 간 지능 전이는 이 병목을 해소하기 위한 기술로서 형태가 다른 로봇 간에 작업 지능을 공유하고 전이하는 것을 목표로 한다. 즉, 한 로봇이 학습한 작업 능력을 다른 로봇이 재학습 없이 또는 소량의 추가 데이터만으로 전달받아 즉시 활용하도록 하는 것이 목표이며 신규 체화에 대한 제로샷(Zero-Shot) 또는 퓨샷(Few-Shot) 전이 효율을 핵심 지표로 삼는다.

이후 II장에서 이종 로봇 체화 간 지능 공유와 전이의 개념과 필요성을 살펴보고, III장에서 국내외 기술 동향을 다섯 개의 하위 기술 분야에 걸쳐 소개한 후, IV장에서 전체 내용을 요약하고 전망을 다룬다.

II. 기술 개념과 필요성

이종 로봇 체화 간 지능 전이 공유는 대체적으로 세 가지 문제로 귀결된다. 첫째는 체화의

경계를 가로지르는 학습 데이터 확보 문제, 둘째는 로봇 간에 공유 가능한 행동 표현의 문제, 셋째는 각 로봇 체화에 지능을 특화하는 문제이다.

첫째, 문제인 데이터 확보에 대해서는 실세계 데이터 수집과 가상 데이터 합성이 모두 시도되고 있다. 실세계 수집에서는 이종 로봇이 유사한 환경에서 동일한 작업을 수행하는 로봇 쌍(pair) 데이터 수집이 대표적이다. 가상 합성에서는 원본 로봇 작업 영상에서 로봇 체화만 다른 로봇으로 교체하여, 실물 수집 없이 이종 체화 쌍 데이터를 확보하는 체화 교체 영상 생성이 대표적이다.

둘째, 문제인 체화 간 공유 가능한 행동 표현에 대한 해결책은 체화 독립적 잠재 행동 표현 학습이다. 행동 제어 명령은 관절의 구조와 배치가 다른 로봇에 그대로 적용할 수 없다. 따라서 서로 다른 로봇들의 동작을 잠재 공간(latent space)에 정렬하여 체화가 달라도 유사한 동작을 동일한 표현으로 기술할 수 있는 공통 행동 표현 체계를 구축한다. 로봇 지능이 이 공통 어휘로 행동 명령을 내리면, 각 로봇의 체화 정보를 기반으로 이를 목표 로봇에 특화된 제어 명령으로 번역함으로써 체화 간 차이를 극복할 수 있다. 엔비디아(NVIDIA)의 GR00T를 비롯한 최근의 로봇 파운데이션 모델들이 유사한 방식을 채택하고 있다.

표현의 문제를 한층 더 밀고 나간 접근이 비디오 월드 모델(video world model)에 기반한 월드 액션 모델(world action model)이다. 이 접근은 로봇의 행동 자체가 아니라 행동이 일으키는 세계의 변화를 공유 표현으로 삼는다. 물리 동역학에 따른 조작의 결과는 어떤 로봇이 수행하든 동일하므로, 비디오 월드 모델이 갖춘 미래 상황 예측과 장면 생성 능력은 그 자체로 체화 중립적인 지식이 된다. 월드 액션 모델은 모든 체화가 공유하는 시각 공간에서 로봇의 작업 장면을 먼저 생성하고, 생성된 영상으로부터 목표 로봇에 특화된 제어 명령을 추출한다. 이러한 특성 덕분에 월드 액션 모델은 신규 체화에 대한 제로샷(Zero-Shot) 전이를 실현할 유력한 경로로 부상하고 있다.

셋째, 문제인 로봇 지능의 체화 특화에 대응하는 대표적인 기술은 기구학 기반 스킬 전이이다. 공유 표현으로 계획된 행동은 최종적으로 목표 로봇의 관절 한계와 도달 범위, 동역학 제약 안에서 실행되어야 한다. 기구학 기반 스킬 전이는 URDF와 관절 구조 등 이미 알려진 로봇 설계 정보를 활용하여 동작을 목표 체화에 분석적으로 최적화하는 방법으로, 학습 기반 로봇 제어 모델의 뒷단에 결합하여 활용할 수 있다.

III장에서 이상의 기술들을 체화 간 지능 전이 학습용 데이터셋, 체화 교체 영상 생성,

체화 독립적 잠재 행동 표현 학습, 월드 액션 모델, 기구학 기반 스킬 전이의 다섯 분야로 나누어 대표적인 연구 사례를 중심으로 설명한다.

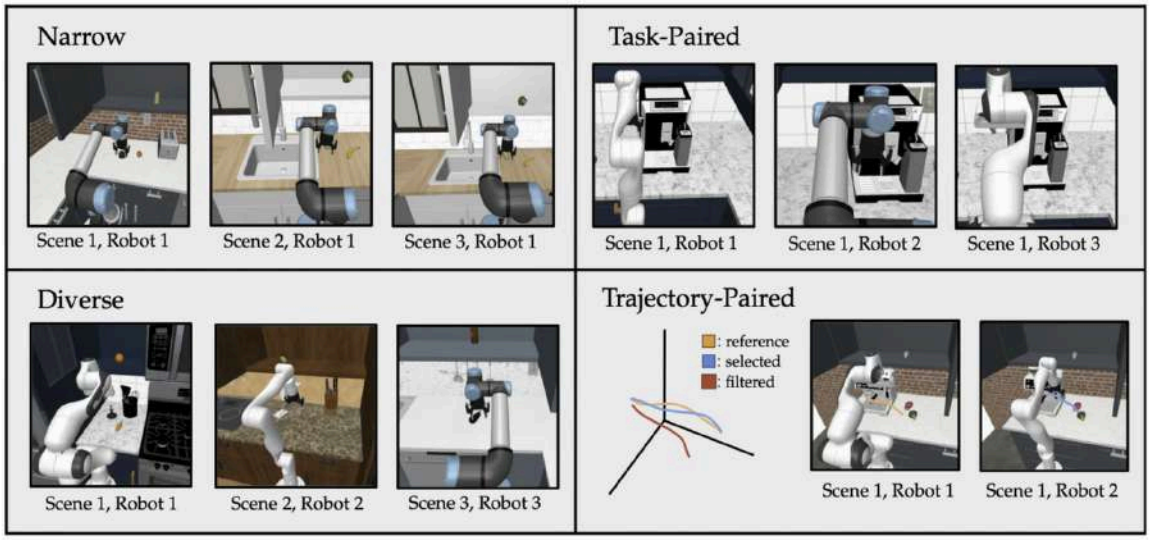
III. 이종 로봇 체화 간 지능 전이 공유 기술 동향

1. 체화 간 지능 전이 학습용 데이터셋

로봇 제어 정책 모델의 이종 체화 간 전이는 정책 모델을 훈련한 데이터의 규모와 다양성, 정렬 품질에 직접 의존하므로 적절한 데이터셋 구축은 모든 전이 학습의 출발점이다. 단순히 대규모 데이터를 축적하는 것을 넘어 보다 전략적인 접근이 필요하다. 로봇 체화의 다양성이 크고 로봇 간 대응 관계 학습에 유리한 데이터가 체화 격차 극복의 관건임이 여러 연구를 통해 드러나고 있다.

구글 딥마인드의 Open X-Embodiment 데이터는 22종의 서로 다른 로봇과 100만 개 이상의 시연 궤적을 통합한 최초의 대규모 이종 로봇 데이터셋으로 통합 학습 시 단일 로봇 데이터 대비 평균 50% 이상 작업 성능이 향상됨을 보여 체화 다양성이 작업 지능의 성능과 일반화 능력 향상에 중요함을 보였다[3].

미국 스탠퍼드대(Stanford University)의 데이터 아날로지(data analogies)는 이종 로봇이 유사 환경에서 동일 작업을 수행한 로봇 쌍 데이터를 로봇 지능 훈련에 활용하면 일반적인 로봇 데이터 대비 실환경 이종 로봇 전이 작업 성공률이 평균 22.5% 향상됨을 보여 체화 간 전이에 특화된 전략적 로봇 데이터 수집의 중요성을 증명했다[그림 1][4]. 중국 엑스휴머노이드(X-Humanoid)의 RoboMIND는 체화 간 전이를 본격적으로 데이터 수집 방법에 반영한 데이터셋이다[5]. 단일팔, 양팔, 휴머노이드를 포함한 4종의 로봇을 활용하여 공통의 환경 하에서 동일 작업과 물체들을 대상으로 479종의 작업 시연 궤적 10만 개를 수집했다. 서로 다른 체화가 같은 작업을 같은 조건에서 수행한 기록이므로 성능 차이가 관측되면 그 원인을 환경이나 작업이 아닌 체화의 차이로 귀속할 수 있고 로봇 간 행동을 정렬하는 기준으로도 쓸 수 있다. 기존 대규모 데이터셋이 기관마다 다른 환경에서 수집된 데이터를 사후에 통합하여 이러한 비교 기준을 제공하지 못하는 것과 대비된다.



* Data Analogies: 환경, 사물, 작업, 로봇 체화의 다양한 조합을 통해 체화 간 지능 전이에 유리한 데이터셋 구축 전략을 도출
〈자료〉 J. Yang et al., "Data analogies enable efficient cross-embodiment transfer", arXiv:2603.06450, 2026.

[그림 1] 스탠포드대학의 데이터 아날로지에 따른 로봇 쌍 데이터 개념

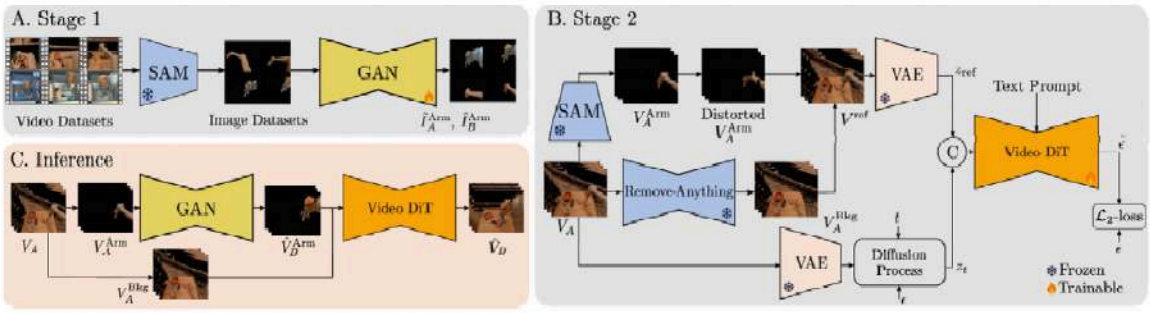
최근 휴머노이드 로봇 데이터셋 구축이 활발하나 대체로 체화 간 전이를 겨냥한 데이터 수집 전략은 적용되지 않고 있다. 중국 AgiBot의 AgiBot World는 로봇 100대로 217종 작업의 궤적을 약 100만 개 수집한 현존 최대 규모의 휴머노이드 데이터셋이나 데이터셋에 자사의 휴머노이드 로봇 단일 기종만 포함하고 있다[6]. 미국 서던캘리포니아대(USC)의 Humanoid Everyday는 작업 260종을 대상으로 10,300개의 궤적을 수집했으나 역시 단일 플랫폼에서 수집되었다[7]. 엔비디아의 GR00T N1 데이터셋은 인터넷 영상, 시뮬레이션 합성, 로봇 원격조작의 3단계 구성으로 32만 개의 시연 궤적과 78만 개의 합성 궤적을 제공하며 합성 데이터와 실 데이터의 혼합 학습으로 작업 성공률을 40% 향상했으나 데이터 규모와 품질에 집중할 뿐 이종 휴머노이드 간 정렬은 다루지 않는다[8]. 엔비디아의 SONIC 데이터셋은 700시간 이상 규모의 모션 캡처 데이터로 Unitree G1의 동작 50종을 100% 성공률로 재현했으나 다른 휴머노이드로의 전이 결과는 보고된 바 없다[9]. 요컨대 데이터의 규모와 모달리티는 빠르게 확장되고 있으나 체화 다양성을 확장하고 로봇 간 대응관계를 포함하는 등 체화 간 전이를 위한 전략은 부재하다. 한국전자통신연구원(ETRI)은 이러한 공백을 메우기 위해 형태가 다른 휴머노이드 로봇들을 활용한 동일 작업 쌍 데이터를 구축하는 시도를 진행 중이다.

2. 체화 교체 영상 생성

체화 교체 영상 생성은 영상 내 로봇을 여러 종류의 서로 다른 로봇으로 교체 합성하여 다중 체화 훈련용 로봇 시연 데이터를 확보하거나 원본 영상으로 학습한 로봇 지능을 속이는 접근 방법이다. 하나의 지능 모델을 그대로 목표 로봇에 적용 활용하거나, 목표 로봇으로 시연 데이터를 수집하지 않고도 목표 로봇용 지능 모델 훈련 데이터를 확보할 수 있다.

독일 뮌헨대학의 RoboSwap[10]은 이러한 접근의 대표적 기술이다. RoboSwap은 생성적 적대 신경망(generative adversarial network)과 비디오 확산 모델(video diffusion model)을 결합한 이중 구조로 영상 내 로봇 팔 모델을 교체한다[그림 2]. 1단계에서 GAN으로 영상 내 원본 로봇 팔을 목표 로봇 팔로 교체하고, 2단계에서 비디오 확산 모델을 이용하여 배경과 동작, 물체 상호작용 등의 전체적 정합성을 보정한다. 관련 대표 연구로 동영상 생성 모델을 기반으로 모션 전이와 체화 적응을 분리하여 새로운 휴머노이드 체화의 시연 영상을 합성하는 싱가포르국립대의 OmniHumanoid[11]와 로봇 궤적 데이터를 기반으로 Open X-Embodiment 내 16개 데이터셋을 최대 9개의 로봇 체화로 합성 확장하여 400만 개 규모의 시연 데이터셋을 구축한 미국 UC 버클리의 OXE-AugE[12]가 있다.

로봇 시각 센서에 입력되는 영상 내 로봇 형상을 실시간 교체 합성하여 로봇 지능을 속이는 방식도 시도되고 있다. 로봇 A의 시연 데이터로 훈련한 지능 모델을 로봇 B에 탑재하고 시각 센서에 입력되는 로봇 B의 형상을 로봇 A의 형상으로 실시간 교체하는 방식이다. 지능 모델은 로봇 A가 작업하는 영상을 입력받는 셈이므로 지능 모델을 로봇 B 데이터로 추가



* GAN을 통한 로봇 팔 변환(1단계)과 비디오 확산 모델 기반 배경 · 동작 정합성 보정(2단계)
〈자료〉 Y. Bai et al., "RoboSwap: A GAN-driven Video Diffusion Framework for Unsupervised Robot Arm Swapping", LMU Munich, arXiv:2506.08632, 2025.

[그림 2] RoboSwap의 2단계 체화 교체 구조

훈련하지 않고도 바로 로봇 B에 전이 공유할 수 있다는 장점이 있다. 이런 방식의 대표 기술로 미국 UC 버클리의 미라지(Mirage)가 있다[13]. 영상 안의 목표 로봇을 영상 분할과 마스킹을 통해 도려내고 인페인팅(inpainting) 기법과 리타게팅(retargetting)을 통해 원본 로봇 형상으로 교체한다. 이러한 크로스페인팅(cross-painting) 기법을 통해 미라지는 원본 로봇에서 실행한 작업 성능 대비 목표 로봇에서 재학습 없이 75% 이상의 성능을 달성했다. 다만, 원본 로봇과 목표 로봇이 동일한 그리퍼를 장착해야 하고 원본 로봇의 모델과 렌더러가 확보되어야 한다는 전제가 있다.

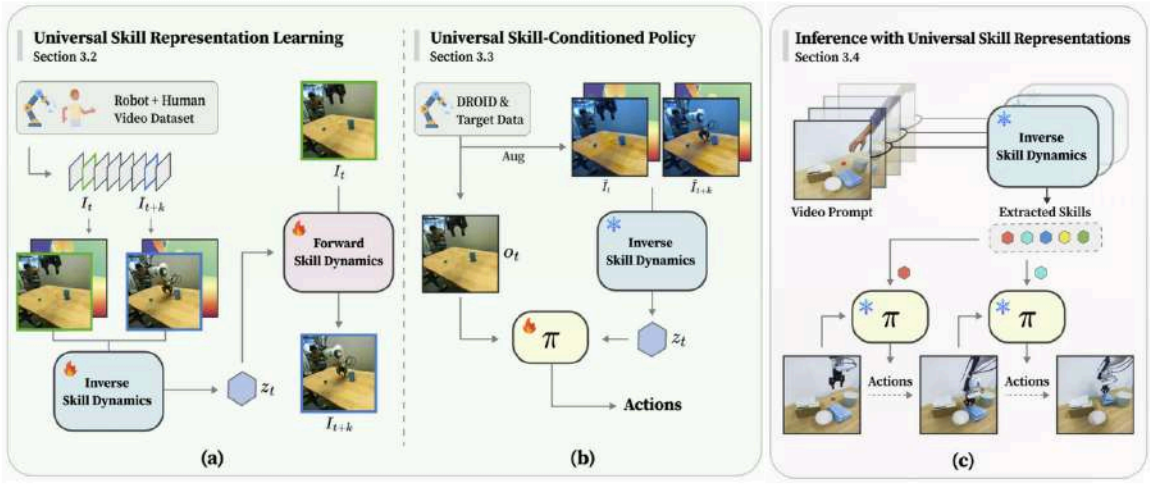
체화 교체 영상 생성은 생성형 AI 기술을 활용하여 비교적 적은 비용으로 로봇 체화 간 차이를 극복할 수 있다는 장점이 있으나 생성 결과의 물리적 정확도와 품질 저하, 체화 간 차이가 큰 로봇 간 체화 교체의 어려움이 난제이다.

3. 체화 독립적 잠재 행동 표현 학습

체화 독립적 잠재 행동 표현 학습은 서로 다른 로봇들의 동작을 하나의 잠재 공간에 정렬하여 체화에 무관한 공통 행동 표현을 학습하는 접근 방법이다. 로봇 지능이 직접 관절을 제어하는 명령이 아니라 잠재 행동을 매개로 동작을 제어하는 명령을 기술하므로 특정 로봇 체화에 특화된 행동 디코더(action decoder)의 교체만으로 공통 표현 수준에서 학습한 작업 지능을 다른 체화에 전이 공유할 수 있다.

사물 조작 분야의 대표적인 잠재 행동 표현 기술로 스위스 취리히연방공대(ETH Zurich)의 LAD(Latent Action Diffusion)[14]가 있다. LAD는 대조학습(contrastive learning)으로 구조가 서로 다른 로봇 손들의 행동을 공통 잠재 공간에 정렬한 뒤 이 잠재 공간 위에서 동작을 생성하는 확산(diffusion) 정책을 학습한다. 정책이 잠재 행동을 출력하면 체화별 디코더가 이를 각 로봇 손에 특화된 제어 명령으로 번역한다. 다양한 이종 로봇 손의 데이터를 더 많이 학습할수록 작업 수행 성능이 향상되는 긍정 효과를 실세계 로봇 실험을 통해 보였다.

한국 연세대학교의 UniSkill[15]은 정답 레이블 없는 대규모 사람 · 로봇 시연 영상만으로 체화 독립적 동작 표현을 학습한다. 시간적으로 떨어진 두 영상 프레임 사이의 동적 변화를 해석하여 스킬 표현을 생성하는 역스킬동역학(inverse skill dynamics) 모델과 스킬 표현으로부터 미래 장면을 예측하는 순스킬동역학(forward skill dynamics) 모델을 공동 학습함으로써 체화의 외형과 구조에 독립적인 잠재 스킬 표현 체계를 학습한다[그림 3]. 이렇게



[역스킬동역학 모델의 스킬 추출과 순스킬동역학 모델의 미래 프레임 예측 공동 학습]

[인간 시연 영상 프롬프트 기반 로봇 정책 실행]

〈자료〉 H. Kim et al., "UniSkill: Imitating Human Videos via Cross-Embodiment Skill Representations", Yonsei University, arXiv:2505.08787, 2025.

[그림 3] UniSkill의 체화 독립적 스킬 표현 학습 구조

학습한 잠재 스킬 표현 체계를 기반으로 로봇 데이터만으로 학습한 로봇 제어 정책 모델이 처음 보는 인간 시연 영상에서 스킬을 추출하고 로봇에 작업 스킬을 전이할 수 있음을 시뮬레이션과 실세계 환경에서 실증했다.

행동 표현을 로봇의 신체가 아니라 조작 대상 물체의 움직임에서 구하는 시도도 있다. 중국 화남이공대(South China University of Technology)와 텐센트 로보틱스 X(Tencent Robotics X)의 3DFlowAction[16]은 물체의 3차원 옵티컬 플로우(3D Optical Flow)를 체화 중립적 행동 표현으로 삼는다. 이 방법은 인간과 로봇의 조작 영상에서 자동 구축한 시연 에피소드 11만 개 규모의 ManiFlow-110k 데이터셋으로 3D 플로우 월드모델을 학습하여 초기 장면과 작업 지시로부터 물체 이동 흐름을 예측하고 이 흐름을 유도할 수 있는 로봇 제어 명령을 생성할 수 있어 재학습 없이도 다양한 로봇 체화에 적용 가능하다.

로봇 주행·보행 분야의 통합 행동 표현 연구로는 독일 다름슈타트공대(TU Darmstadt)와 미국 UC 샌디에이고(UC San Diego)의 URMA[2]가 있다. 어텐션 모듈을 이용해 로봇 체화를 공통 표현으로 인코딩하고 이동 제어 정책을 훈련함으로써 하나의 정책 모델로 시뮬레이션 상에서 이족, 사족, 육족 등 다양한 구조의 로봇 이동을 제어하였고, 실제 로봇을

이용한 이동 지능 전이도 성공적으로 보였다. 후속 연구인 UC 샌디에이고의 체화 스케일링 법칙(embodiment scaling law) 연구[17]는 URMA를 확장한 아키텍처로 가상으로 생성한 1,012종의 로봇(GenBot-1K)을 체화 인코딩 학습에 적용함으로써 학습에 참여하는 서로 다른 로봇 체화의 개수가 늘어날수록 신규 체화에 대한 전이 공유 성능이 향상되는 현상을 실증했다. 소수의 체화에서 데이터 양을 늘리는 것보다 체화의 종류를 늘리는 것이 체화 간 전이 공유에 더 효과적이라는 것이다. 이와 같은 방식으로 훈련한 이동 제어 정책은 학습하지 않은 실세계 Unitree Go2와 H1 로봇에도 성공적으로 제로샷 전이되었다.

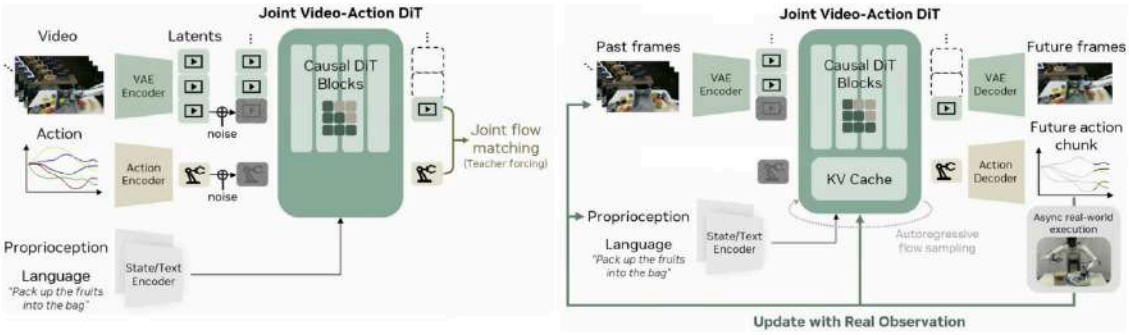
체화 독립적 잠재 행동 표현 학습은 이종 체화 데이터가 늘수록 성능이 향상되는 긍정 전이의 토대이자 인간 영상을 로봇 학습 자원으로 끌어들이는 관문이라는 점에서 체화 간 지능 전이 공유의 중심 기술이다. 다만, 휴머노이드 로봇의 상반신 또는 전신 작업을 대상으로 한 지능 전이 연구는 아직 부족한 상태로 추가 연구가 필요하고, 잠재 표현 체계의 품질이 학습 데이터에 포함된 체화의 다양성에 좌우되며, 잠재 공간에서 생성되는 행동 제어 명령의 안전 검증이 어렵다는 문제가 있다.

4. 월드 액션 모델

월드 액션 모델(World Action Model: WAM)은 비디오 월드 모델에 내재된 동역학 사전 지식을 기반으로 지시된 작업이 실행되는 장면을 동영상으로 예측하고, 이로부터 로봇 행동을 계획하는 로봇 파운데이션 모델이다. 동영상 생성이 모든 체화가 공유하는 시각 공간에서의 암묵적 작업 계획에 해당하고 행동 예측이 체화별 역동역학(inverse dynamics)에 대응하므로, 다른 유형의 로봇 파운데이션 모델에 비해 체화 독립적 행동 생성 능력이 뛰어나다.

엔비디아의 DreamZero는 이 분야의 대표 기술로, DreamZero는 사전학습 비디오 확산 모델을 기반으로 미래 비디오와 행동을 동시 예측하며, 신규 작업과 환경에서 기존 VLA 대비 2배 이상의 작업 수행 성능을 보였다[18]. 또한, 행동 레이블 없는 비디오만으로 이종 체화 전이 성능을 42% 이상 높였고, 30분 분량의 짧은 로봇 동작 영상을 이용한 퓨샷 파인튜닝(Fine-Tuning)으로 작업 지능 모델을 새로운 로봇에 전이할 수 있다[그림 4].

이 분야 최초 기술은 구글 딥마인드(Google DeepMind)의 UniSim이다[19]. UniSim은 인터넷 동영상, 로봇 시연, 인간 활동 기록처럼 성격이 서로 다른 데이터가 각각 세계의 다른 단면, 즉 다양한 물체와 장면, 사람의 움직임, 로봇의 행동을 담고 있다는 점에 착안하여



[비디오와 행동의 공동 플로 매칭 학습] [실세계 폐루프 실행 시 미래 비디오·행동 청크 동시 생성]

〈자료〉 NVIDIA GEAR Lab, "World Action Models are Zero-shot Policies", arXiv, 2026.

[그림 4] DreamZero의 구조

이들을 하나의 비디오 확산 모델로 통합 학습했다.

그 결과 현재 장면과 행동을 입력하면 그 행동이 일으킬 다음 장면을 생성하는 범용 실세계 시뮬레이터가 만들어졌고, 이 가상 세계 안에서 로봇 정책을 훈련한 뒤 실세계로 옮기는 활용 방식을 제시하였다. 엔비디아 코스모스(Cosmos)는 이 개념을 파운데이션 모델 수준으로 확장한 사례이다[1]. 코스모스는 방대한 영상으로부터 중력, 충돌, 물체 영속성 같은 물리 법칙을 따르는 장면 생성 능력을 학습한 7B, 14B 규모의 비디오 생성 파운데이션 모델로 로봇 특화 후속 모델들의 토대가 되고 있다. 중국 알리바바(Alibaba)의 WorldVLA는 장면 예측과 행동 생성을 한 모델에 통합한 구조이다[20]. 하나의 자기회귀(autoregressive) 생성 모델을 기반으로 영상과 행동을 동일한 토큰 어휘로 표현하기 때문에 행동이 주어지면 그 결과 장면을 예측하고 장면이 주어지면 다음 행동을 생성한다. 행동이 일으킬 결과를 미리 내다보는 물리 이해가 행동 생성의 근거로 작동하여 예측과 생성 두 능력이 서로를 강화한다.

5. 기구학 기반 스킬 전이

기구학 기반 스킬 전이는 데이터를 학습하는 대신 URDF 등 로봇 설계 명세에 담겨 있는 로봇 구조 정보를 기반으로 작업 시연을 분석적으로 다양한 로봇에 전이하는 방법이다.

대표 사례로 스위스 로잔공대(EPFL)의 기구학 지능(kinematic intelligence)을 들 수 있다[21]. 핵심 아이디어는 시연 데이터에서 동작 정보를 지우고 작업의 목표 정보만 남기는

것이다. 이 기술은 모션 캡처로 수집한 사람의 시연 데이터를 입력받으면 물체의 출발과 목표 위치, 이동 속도와 방향 정보를 추출한 운동 전략(movement strategy) 표현을 생성한다. 이 전략을 목표 로봇의 관절 한계와 도달 범위에 맞춰 동작 데이터로 변환하면 재프로그래밍 없이 해당 로봇에 적합하고 안전한 동작으로 작업을 수행할 수 있다. 조립 작업 환경을 대상으로 한 실험에서 인간의 1회 시연만으로 상용 협동 로봇 3종이 나무 블록을 컨베이어에서 밀어내고 옮긴 뒤 바구니에 던지는 동작을 성공적으로 재현했다.

리타게팅(Retargeting)은 사람이나 로봇의 동작을 구조가 다른 로봇의 관절 움직임으로 변환하는 기법으로서 기구학 기반 지능 전이의 또 다른 접근 방법이다. 미국 CMU의 Omni H2O는 인간 동작 리타게팅을 기반으로 휴머노이드 로봇의 전신 원격조작을 가능하게 했고[22], 독일 뮌헨공대(TUM)의 DynaRetarget은 샘플링 기반 궤적 최적화(sampling-based trajectory optimization)로 리타게팅 결과를 정제하여 몸체 균형과 접촉 등 동역학을 고려한 동작 궤적을 생성한다[23]. DynaRetarget은 인간 시연으로부터 서로 다른 로봇 체화에 적합한 동작 궤적을 반복 생성할 수 있어 이종 로봇 쌍 데이터를 생성 증강하는 용도로도 활용할 수 있다.

IV. 전망 및 결론

이종 로봇 체화 간 지능 전이 공유는 특정 로봇에 종속되어 학습되던 작업 지능을 형태가 다른 로봇들이 공유하고 재사용할 수 있도록 하는 기술로서 새 로봇마다 데이터 수집과 재학습을 반복해야 하는 병목을 해소하여 휴머노이드 로봇의 보급과 실용화를 앞당길 핵심 기술로 부상하고 있다. 본 고는 관련 기술을 체화 간 지능 전이 학습용 데이터셋, 체화 교체 영상 생성, 체화 독립적 잠재 행동 표현 학습, 월드 액션 모델, 기구학 기반 스킬 전이의 다섯 분야로 나누어 국내외 동향을 살펴보았다. 향후 발전 방향을 전망해 보면, 첫째, 공통 잠재 행동 표현과 월드 모델을 결합하여 이종 체화 간 지능 전이 성능을 최적화하는 로봇 지능 아키텍처 개발, 둘째, 이종 휴머노이드 쌍 데이터의 구축과 합성 데이터의 결합을 통한 체화 간 지능 전이 데이터 병목의 해소, 셋째, 체화 간 전이 성능을 단일 기준으로 측정하고 비교할 수 있는 공개 벤치마크와 메타데이터 표준의 정립이다. 이 세 방면의 기술 발전이 성숙한다면 단일 로봇에 종속되던 작업 지능이 형태가 다른 다수 로봇으로 자유롭게 전이 공유되는 또

다른 의미의 범용 피지컬 AI의 기반이 마련될 것으로 기대한다.

참고문헌

[1] NVIDIA(N. Agarwal et al.), "Cosmos World Foundation Model Platform for Physical AI", arXiv:2501.03575, 2025.

[2] N. Bohlinger, G. Czechmanowski, M. Krupka, P. Kicki, K. Walas, J. Peters, D. Tateo, "One Policy to Run Them All: An End-to-End Learning Approach to Multi-Embodiment Locomotion", CoRL 2024, PMLR vol. 270, 2024, pp.3356-3378.

[3] A. Padalkar et al.(Open X-Embodiment Collaboration), "Open X-Embodiment: Robotic Learning Datasets and RT-X Models", ICRA, 2024.

[4] J. Yang, C. Finn, D. Sadigh, "Data Analogies Enable Efficient Cross-Embodiment Transfer", arXiv:2603.06450, 2026.

[5] K. Wu et al., "RoboMIND: Benchmark on Multi-embodiment Intelligence Normative Data for Robot Manipulation", arXiv:2412.13877, 2024.

[6] Q. Bu et al.(AgiBot-World-Contributors), "AgiBot World Colosseo: A Large-scale Manipulation Platform for Scalable and Intelligent Embodied Systems", arXiv:2503.06669, 2025.

[7] Z. Zhao et al., "Humanoid Everyday: A Comprehensive Robotic Dataset for Open-World Humanoid Manipulation", arXiv:2510.08807, 2025.

[8] NVIDIA, "GR00T N1 Dataset", Hugging Face, 2025.

[9] NVIDIA, "SONIC Dataset", nvlabs.github.io/GEAR-SONIC, 2025.

[10] Y. Bai, L. Yang, G. Eskandar, F. Shen, D. Chen, M. Altillawi, Z. Liu, G. Kutyniok, "RoboSwap: A GAN-driven Video Diffusion Framework for Unsupervised Robot Arm Swapping", arXiv:2506.08632, 2025.

[11] Y. Song et al., "OmniHumanoid: Streaming Cross-Embodiment Video Generation with Paired-Free Adaptation", arXiv:2605.12038, 2026.

[12] G. Ji, H. Polavaram, L. Y. Chen, S. Bajamahal, Z. Ma, S. Adebola, C. Xu, K. Goldberg, "OXE-AugE: A Large-Scale Robot Augmentation of OXE for Scaling Cross-Embodiment Policy Learning", arXiv:2512.13100, 2025.

[13] L. Y. Chen, K. Hari, K. Dharmarajan, C. Xu, Q. Vuong, K. Goldberg, "Mirage: Cross-Embodiment Zero-Shot Policy Transfer with Cross-Painting", RSS, 2024.

[14] E. Bauer, E. Nava, R. K. Katzschmann, "Latent Action Diffusion for Cross-Embodiment Manipulation", arXiv:2506.14608, 2025.

[15] H. Kim et al., "UniSkill: Imitating Human Videos via Cross-Embodiment Skill Representations", Yonsei University, arXiv:2505.08787, 2025.

[16] H. Zhi, P. Chen, S. Zhou, Y. Dong, Q. Wu, L. Han, M. Tan, "3DFlowAction: Learning Cross-Embodiment Manipulation from 3D Flow World Model", arXiv:2506.06199, 2025.

[17] B. Ai, L. Dai, N. Bohlinger, D. Li, T. Mu, Z. Wu, K. Fay, H. I. Christensen, J. Peters, H. Su, "Towards Embodiment Scaling Laws in Robot Locomotion", CoRL, arXiv:2505.05753, 2025.
[18] S. Ye et al., "World Action Models are Zero-shot Policies(DreamZero)", arXiv:2602.15922, 2026.
[19] S. Yang, Y. Du, K. Ghasemipour, J. Tompson, L. Kaelbling, D. Schuurmans, P. Abbeel, "UniSim: Learning Interactive Real-World Simulators", ICLR, 2024.
[20] J. Cen et al., "WorldVLA: Towards Autoregressive Action World Model", arXiv:2506.21539, 2025.
[21] S. Gupta, D. H. Salunkhe, A. Billard, "Demonstrate Once, Execute on Many: Kinematic Intelligence for Cross-Robot Skill Transfer", Science Robotics, Vol.11, eaea1995, 2026.
[22] T. He et al., "OmniH2O: Universal and Dexterous Human-to-Humanoid Whole-Body Teleoperation and Learning", CoRL, 2024.
[23] V. Dhedin, I. Taouil, S. Omar, D. Yu, K. Tao, A. Dai, M. Khadiv, "DynaRetarget: Dynamically -Feasible Retargeting using Sampling-Based Trajectory Optimization", arXiv:2602.06827, 2026.

주간기술동향 원고 공모

정보통신기획평가원은 주간기술동향에 게재할 기술 · 시장 · 정책 동향의 각 분야 원고를 모집하고 있습니다. 관심 있는 전문가 분들의 많은 참여를 바랍니다.

❑ 원고 주제

- 통신 · 전파 · 방송(이동통신, 네트워크, 전파, 위성, IoT, 방송 등)
- AI · SW · 컴퓨팅(AI · 빅데이터 · 자율주행, SW · 클라우드 · 디지털콘텐츠, 보안 · 블록체인 등)
- 반도체 · 양자 · 디바이스(AI반도체, 양자컴퓨터/통신, 디바이스, 소재 · 부품 등)
- ICT융합(스마트헬스, 스마트시티, 스마트제조, 스마트농업, 스마트국방, 스마트재난안전, 탄소중립, 사회문제해결 등)
- ICT 산업/기술 정책

※ 제목과 목차는 저자가 자율적으로 결정

❑ 제출 자격 : 원고 모집 분야의 전문가

❑ 접수 기간 : **수시 접수**

❑ 제 출 처 : 주간기술동향 원고접수메일(wttrends@iitp.kr)로 제출

❑ 원고 양식 : 파일참조(원고양식)

❑ 원고 분량 : 12페이지 내외

❑ 기타

- 원고 심의절차를 통과한 원고만 게재되므로 원고제출 시 반드시 원고심의의뢰서(첨부파일참조)를 함께 제출하여 주시기 바랍니다.

  ※ 카피킬러라이트 표절 검사 확인서 제출(표절률 10% 이하)
- 게재된 원고에 대하여 소정의 원고료 지급(200자 원고지 10,000원/1매, 최고 40만 원)
- 게재된 원고로 인해 지적재산권 침해문제가 발생할 경우, 원고저자는 원고료 반환, 게시물 삭제 및 정보통신기획평가원이 입게 될 손실·비용에 대한 배상 등의 불이익을 받을 수 있습니다.

❑ 제출 및 문의처

- (34054) 대전광역시 유성구 유성대로 1548 정보통신기획평가원
  디지털미래정책단 동향분석팀 주간기술동향 담당
- Tel : 042-612-8296, 8246 / Fax : 042-612-8209 / E-mail : wttrends@iitp.kr

➢ 사업책임자: 이현재(디지털미래정책단 동향분석팀장)

➢ 참여연구원: 도승희, 허창회, 유영신, 김도현, 김지훈, 김형석, 장미래, 박진아

IITP 주간기술동향

통권 2224호(2026-22)

발 행 년 월 일 : 2026년 11월 4일
발 행 소 : 정보통신기획평가원
편집인겸 발행인 : 홍진배
등 록 번 호 : 대전 다-01003
등 록 년 월 일 : 1985년 11월 4일
인 쇄 인 : 위고디자인

IITP 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)
전화 : (042) 612-8246, 8296 팩스 : (042) 612-8209

청렴韓세상

깨끗한 IITP, 신뢰받는 IITP

IITP 정보통신기획평가원

http://www.iitp.kr