2010-1학기 현대암호학

제 8장 메시지 인증 코드

박 종 혁

Tel: 970-6702
Email: jhpark1@snut.ac.kr

목차

8.1 주요 내용

- 이 장에서는 메시지 인증 코드에 대해 설명하도록 한다.
- 메시지 인증 코드를 사용하면 자신에게 도착한 메시지가 송신자가 보낸 그대로 인지를 확인할 수 있다.

메시지 인증으로 막을 수 있는 두 가지 위협

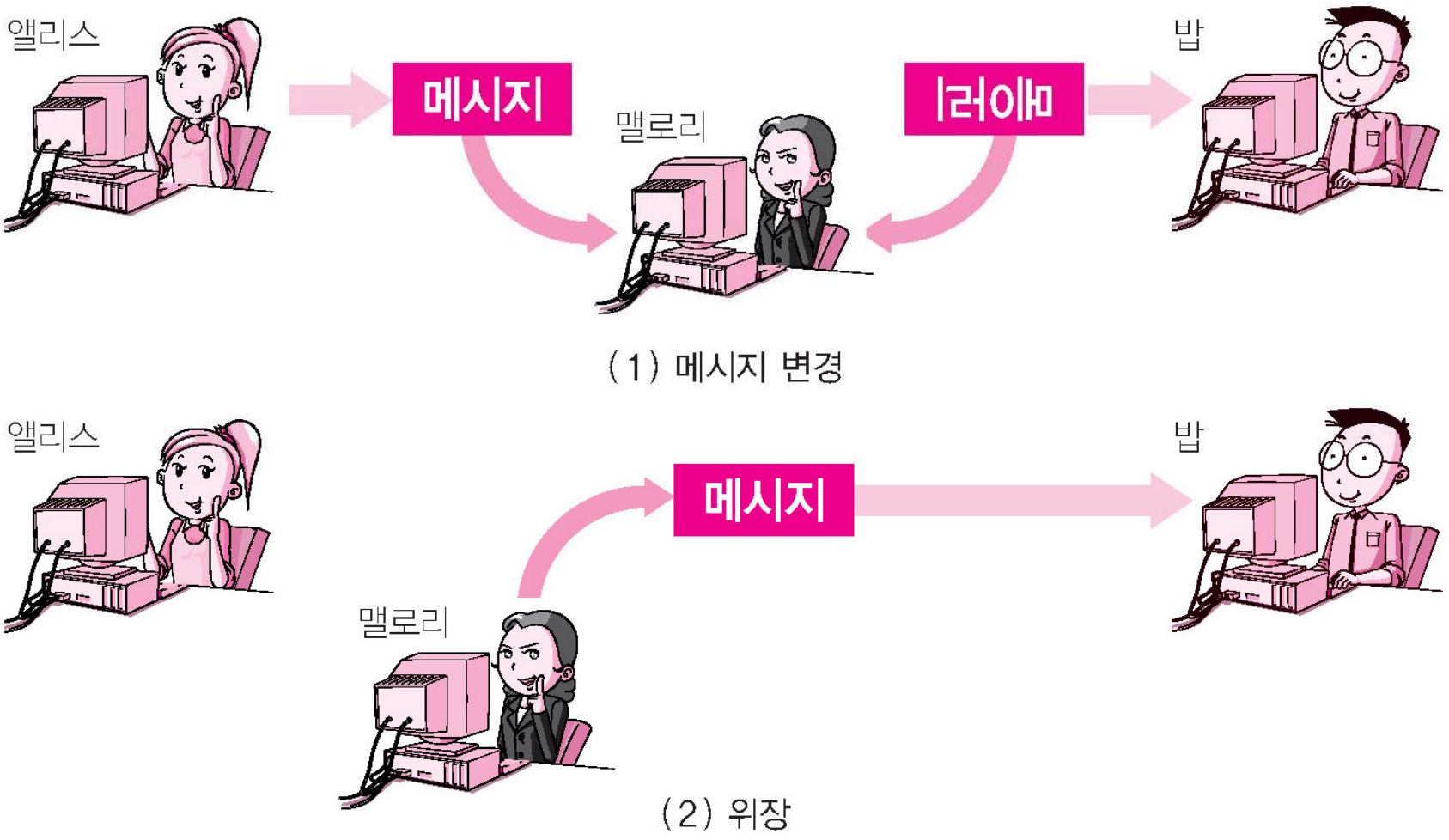


그림 8-1 메시지 인증으로 막을 수 있는 두 가지 위협

8.2 메시지 인증 코드

8.2.1 올바른 송금 의뢰

- 앨리스와 밥은 사람이 아니라 양쪽 모두가 은행이라고 해보자. 즉, 은행 이름이 하나는 앨리스이고 다른 한 은행의 이름은 밥이다.
- 어느 날 앨리스 은행으로부터 밥 은행에 네트워크를 통해서 송금 의뢰가 도착했다.
- 밥 은행이 읽어 보니,

계좌 Alice-7317에서 계좌 Bob-8282로
1000만 원을 송금할 것

이라는 내용이었다.

믿을 수 있는가?

- 이 송금 의뢰는 정말로 앨리스 은행이 보낸 것일까?
- 앨리스 은행은 송금 의뢰 같은 것은 하지도 않았는데, 적극적 공격자 맬로리가 앨리스 은행인 것처럼 거짓 행세를 하며 송금 의뢰를 한 것인지도 모른다.

메시지의 무결성과 인증

- 지금 필요한 것은 송금 의뢰(메시지)의 「무결성」과 「인증」이라는 2개의 성질이다.

- 메시지의 **무결성**(integrity)
  - 「메시지가 변경되지 않았다」는 성질

- 메시지 **인증**(authentication)
  - 「메시지가 올바른 송신자로부터 온 것이다」라는 성질

8.2.2 메시지 인증 코드란

- 메시지에 붙여지는 작은 데이터 블록을 생성하기 위해 비밀키를 이용하는 방법
- 이 기술을 이용하면 전송되는 메시지의 무결성을 확인하여, 메시지에 대한 인증을 할 수 있음
- 코드를 보통 첫 글자를 따서 MAC이라 부름

메시지 인증코드 MAC

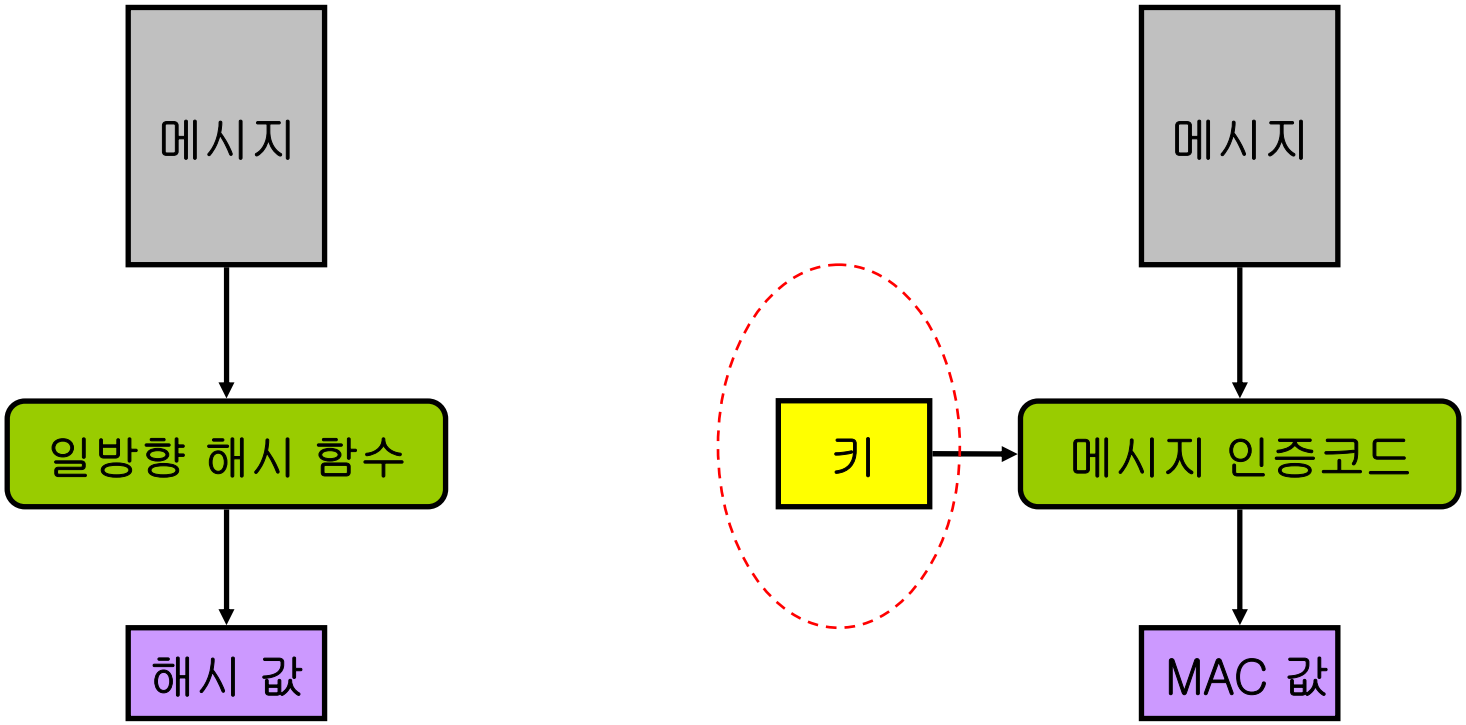
- 메시지 인증 코드는,
  - 입력
    - 임의 길이의 **메시지**
    - 송신자와 수신자가 **공유하는 키**
  - 고정 비트 길이의 출력을 계산하는 함수

- 이 출력 ➔ **MAC 값**

일방향 함수와 메시지 인증코드

- 일방향 해시 함수로 해시 값을 계산할 때 키를 사용하지 않음
- 메시지 인증 코드에서는 송신자와 수신자가 공유하는 키를 사용함

일방향 해시 함수와 메시지 인증 코드의 비교



8.2.3 메시지 인증 코드를 이용한 인증 순서

(1) 송신자 앨리스와 수신자 밥은 사전에 키를 공유해 둔다.

(2) 송신자 앨리스는 송금 의뢰 메시지를 기초로 해서 MAC 값을 계산한다(공유 키를 사용).

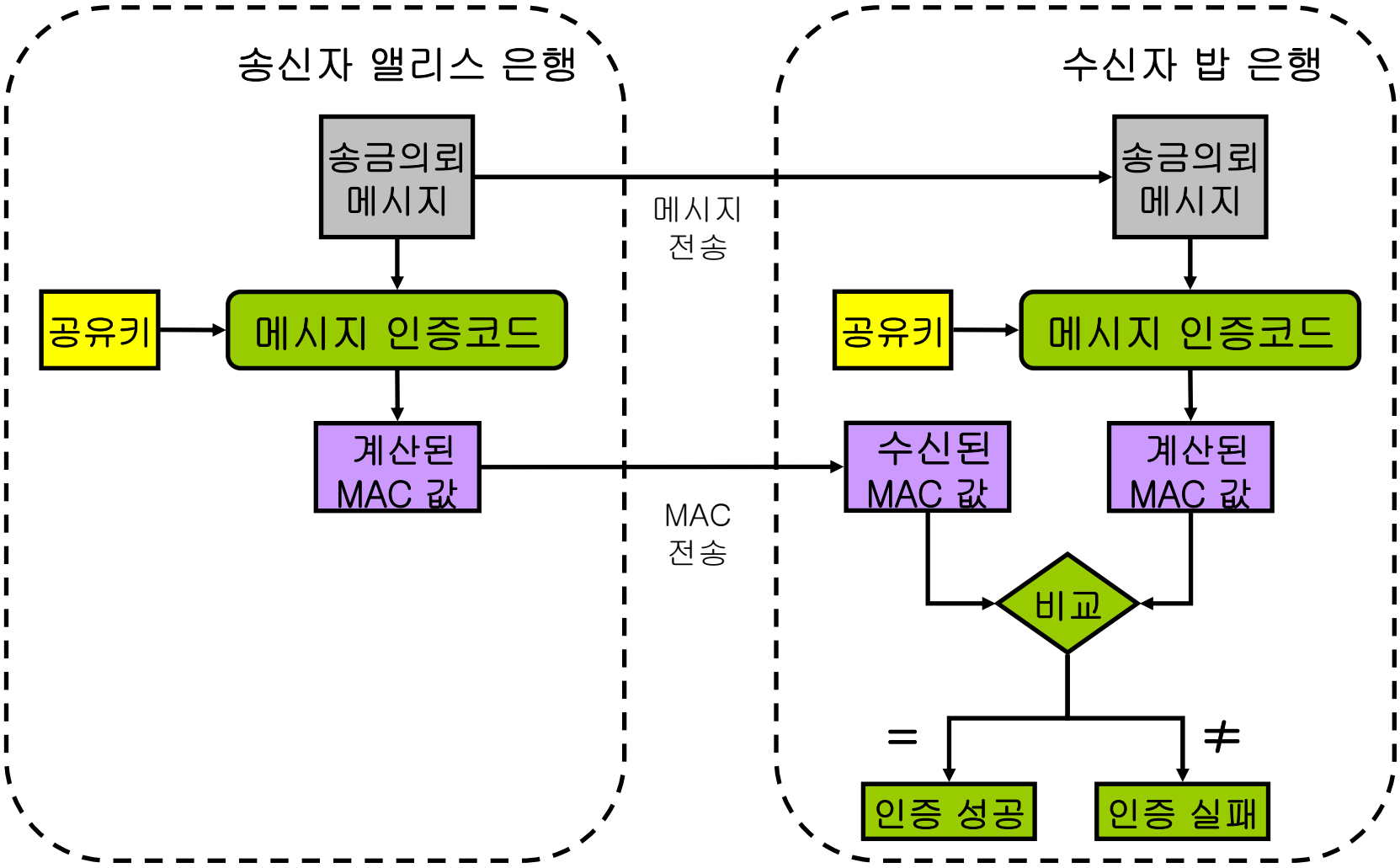
(3) 송신자 앨리스는 수신자 밥에게 송금 의뢰 메시지와 MAC 값을 보낸다.

(4) 수신자 밥은 수신한 송금 의뢰 메시지를 기초로 해서 MAC 값을 계산한다(공유 키를 사용).

(5) 수신자 밥은 앨리스로부터 수신한 MAC 값과 계산으로 얻어진 MAC 값을 비교한다.

(6) 수신자 밥은 2개의 MAC 값이 동일하면 송금 의뢰가 틀림없이 앨리스로부터 온 것이라고 판단한다(인증 성공). 동일하지 않다면 앨리스로부터 온 것이 아니라고 판단한다(인증 실패).

메시지 인증 코드의 이용 순서



8.2.4 메시지 인증 코드의 키 배송 문제

- 메시지 인증 코드에서는 송신자와 수신자가 키를 공유할 필요가 있음
  - 이 키는 적극적 공격자 맬로리에게 넘어가서는 안 된다.
- 만약 이 키가 맬로리의 손에 들어간다면,
  - 맬로리도 MAC 값을 계산할 수 있기 때문에, 자유롭게 변경이나 거짓 행세를 하는 것이 가능
- 실제로 대칭 암호 때의 「**키 배송 문제**」와 같은 문제가 메시지 인증 코드에도 일어남

8.3 메시지 인증 코드 이용 예

8.3.1 SWIFT

- SWIFT는 Society for Worldwide Internet Financial Telecommunication(국제은행간 통신협회)의 약자
- 국제적인 은행 간의 송금을 안전하게 행하기 위해 1973년에 설립된 단체
- SWIFT에서는 무결성을 확인하고 메시지를 인증하기 위해서, 메시지 인증 코드를 사용하고 있음

8.3.2 IPsec

- IPsec은 인터넷 기반의 통신 프로토콜인 IP(Internet Protocol)에 보안 기능을 첨가한 것

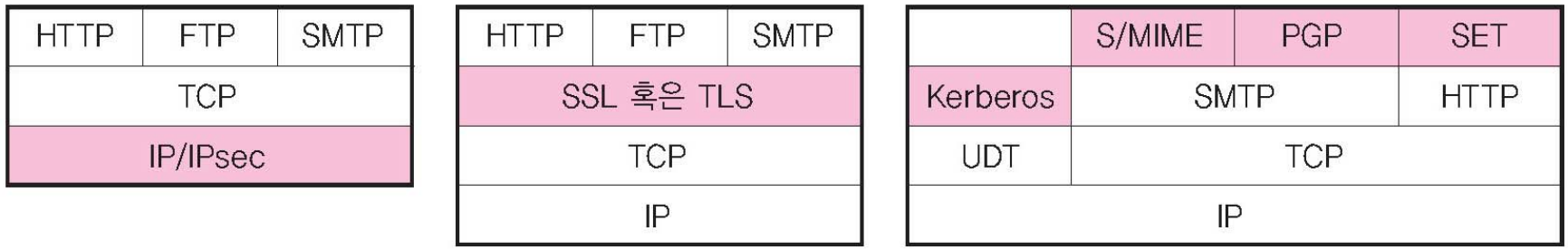
- IPsec에서는 통신 내용의 인증과 무결성을 확인하기 위해 메시지 인증 코드를 이용하고 있음

8.3.3 SSL/TLS

- SSL/TLS는 우리가 웹에서 온라인 쇼핑을 할 때 사용되는 통신 프로토콜

- SSL/TLS에서도 통신 내용의 인증과 무결성 확인을 위해 메시지 인증 코드를 이용하고 있음

TCP/IP 프로토콜 계층에서 보안장치의 상대적 위치



(a) 네트워크 층 (b) 전송 층 (c) 응용 층

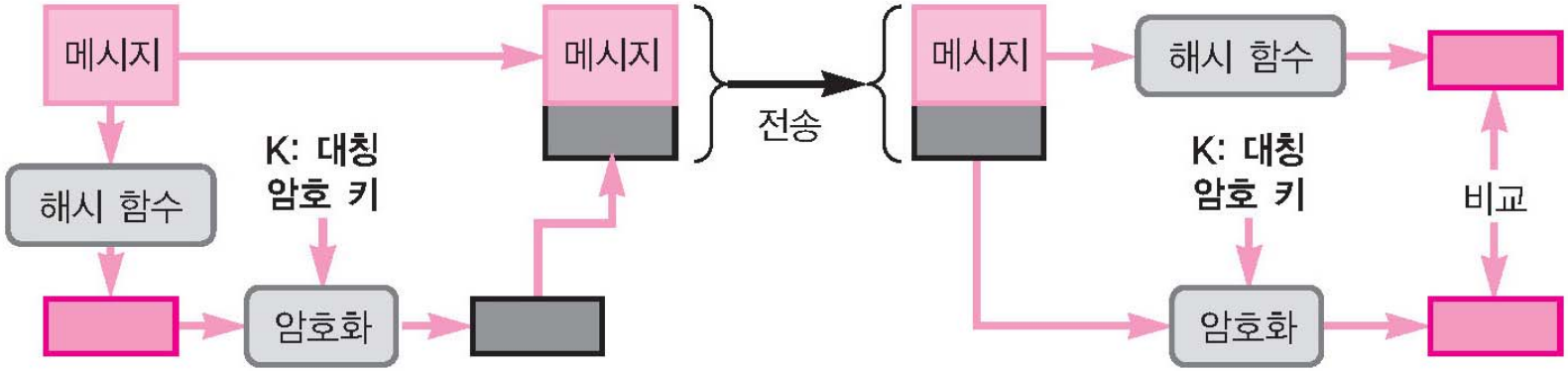
그림 8-4 TCP/IP 프로토콜 계층에서 보안장치의 상대적 위치

8.4 메시지 인증 코드의 실현 방법

8.4.1 일방향 해시 함수를 써서 실현

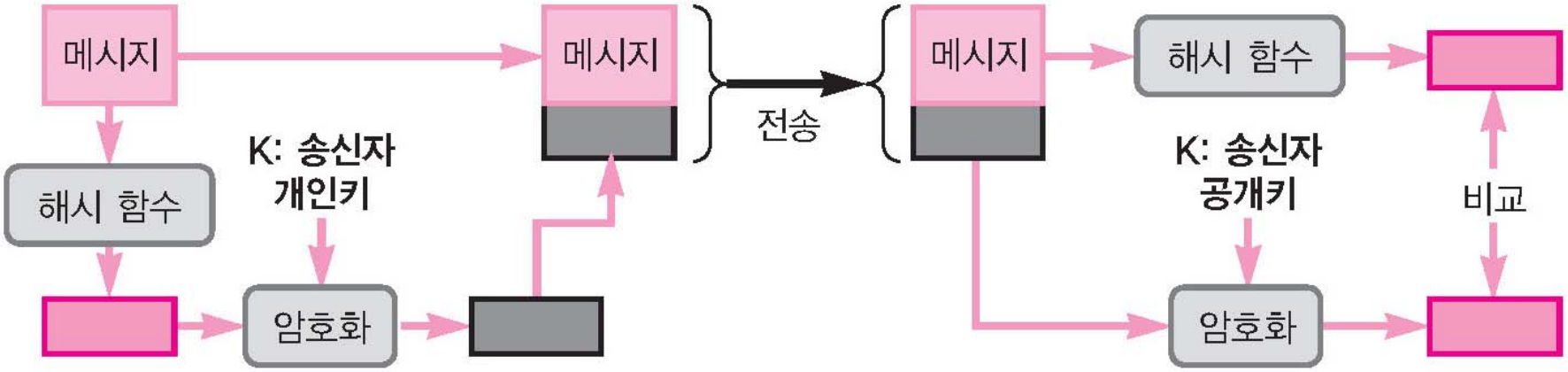
- 메시지 다이제스트는 대칭 암호를 이용해서 암호화
  - 비밀 값을 이용하여 메시지 다이제스트를 생성하는 경우도 있음
- 메시지는 공개키를 이용하여 암호화

일방향 해시 함수를 이용한 메시지 인증



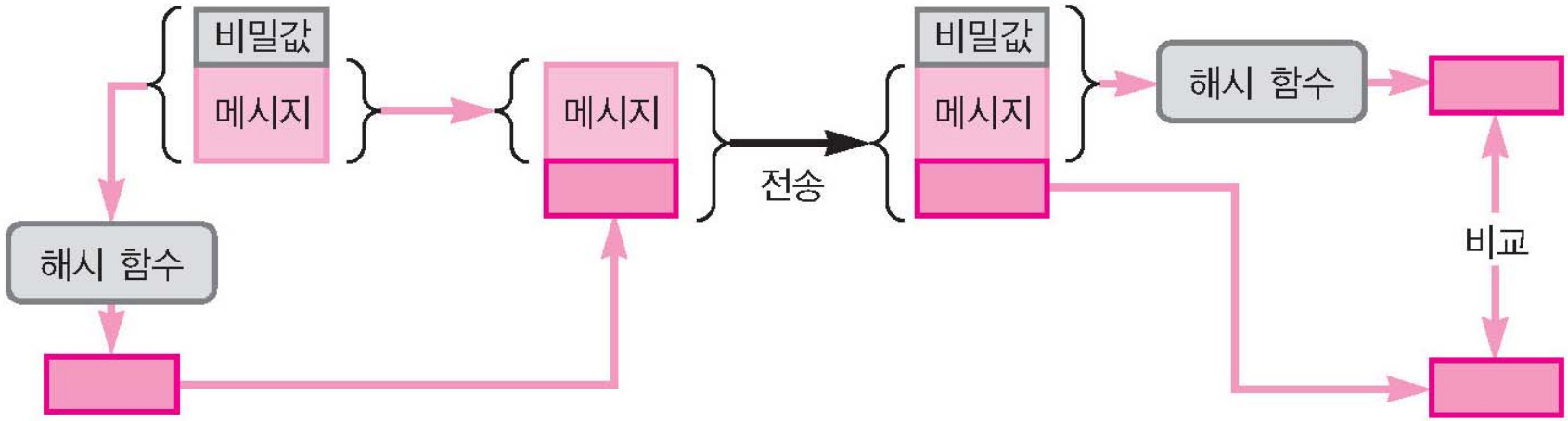
(a) 대칭 암호 사용

일방향 해시 함수를 이용한 메시지 인증



(b) 공개키 암호 사용

일방향 해시 함수를 이용한 메시지 인증



(c) 비밀 값 사용

8.4.2 블록 암호를 이용한 인증코드

- 트리플 DES나 AES와 같은 블록 암호를 사용해서 메시지 인증 코드를 실현할 수 있음
- 블록 암호의 키: 메시지 인증 코드의 공유 키로 사용하고, CBC 모드를 써서 메시지 전체를 암호화함
- 메시지 인증 코드에서는 복호화를 할 필요가 없으므로 마지막 블록만 제외하고 나머지 블록들은 모두 폐기함
- 이렇게 얻어진 마지막 블록을 MAC 값으로 이용함

블록 암호를 이용한 인증코드

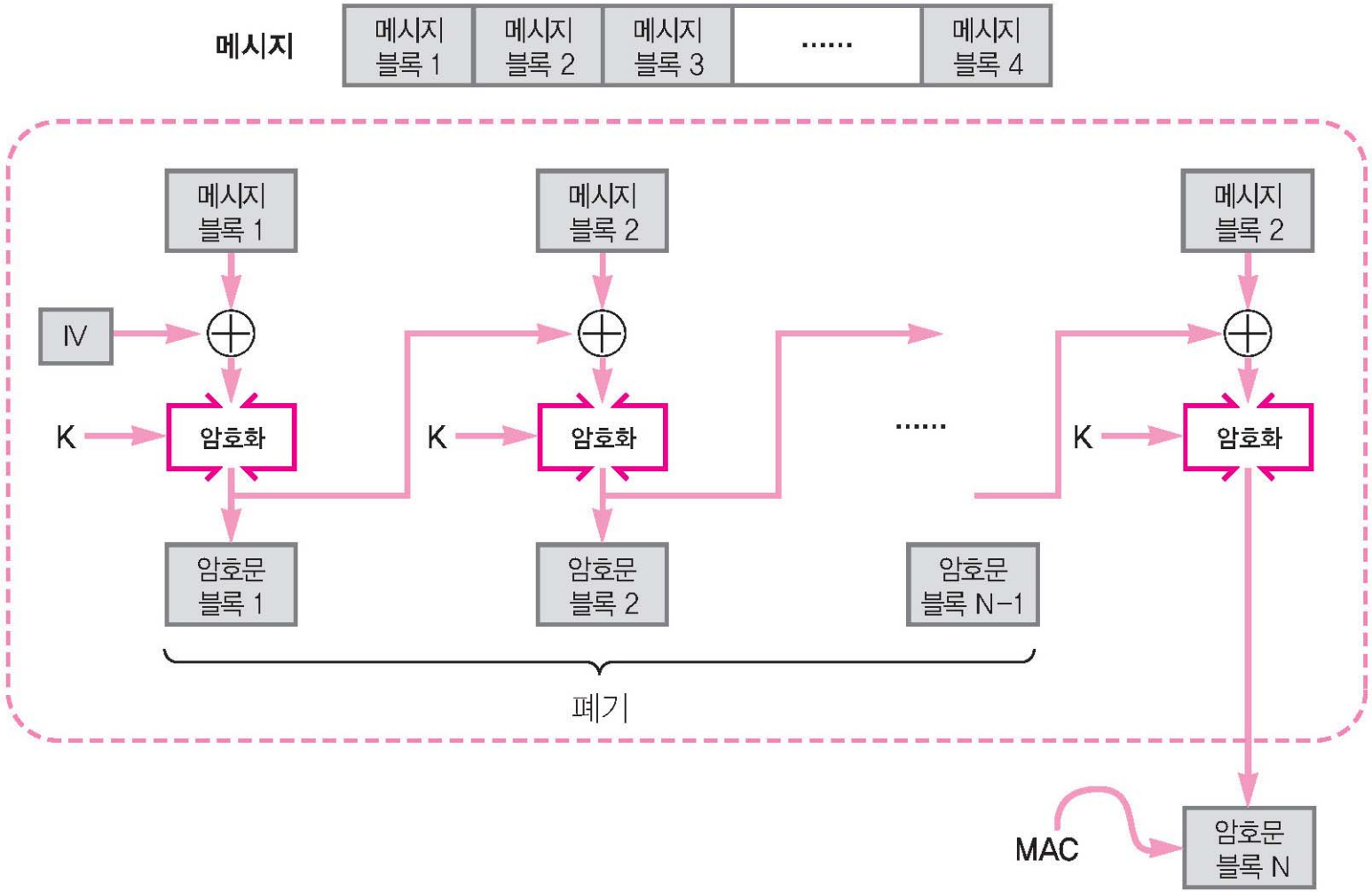


그림 8-6 일방향 해시 함수를 이용한 메시지 인증

8.4.3 기타 인증코드 만들기

- 스트림 암호나 공개 키 암호 등을 사용해서 메시지 인증 코드를 실현할 수 있음
- 코드를 생성하는 알고리즘에는 여러 가지가 있음
- NIST 명세 FIPS PUB 113 에서는 DES 사용을 권장
  - DES 를 이용해서 메시지를 암호화 하고 암호문의 끝부분에 있는 여러 비트들을 코드로 사용
- 16 비트 혹은 32 비트 코드가 전형적인 크기이임

8.5 HMAC

8.5.1 HMAC란

- SHA-1 같은 암호알고리즘을 이용하여 출력한 해시 값으로부터 MAC 을 만드는 기술에 관심이 집중

관심을 가지게 된 이유

- 암호기술이 첨가된 해시 함수는
  - 일반적으로 대칭 암호 알고리즘인 DES보다 소프트웨적으로 속도가 빠르름
- 암호기술이 포함된 해시 함수에 대한 코드들을 쉽게 구할 수 있음
- 대칭 암호 알고리즘이나 MAC 에서 사용하는 대칭 암호 알고리즘까지 수출 규제를 받고 있는 데 반해
  - 암호적 해시함수에 대해서는 미국이나 다른 나라들이 수출 규제를 하고 있지 않음

HMAC(Hashed MAC)

- 일방향 해시 함수를 이용해서 메시지 인증 코드를 구성하는 방법
  - HMAC에서는 사용하는 일방향 해시 함수를 단 한 종류로 정해 놓고 있는 것은 아님
- 강한 일방향 해시 함수라면 뭐든지 HMAC에 이용할 수 있음
- 새로운 일방향 해시 함수가 고안된다면 그것을 사용할 수도 있음
- 이와 같은 형태로 만들어진 알고리즘을 모듈형 알고리즘이라함

8.5.2 HMAC 설계 목표

- 수정하지 않고 쓸 수 있는 해시 함수들을 만든다.
  - 소프트웨어에서 잘 돌아가고 코드를 무료로 제공하고 널리 쓰일 수 있도록 함
- 더 빠르고 안전한 해시함수가 있거나 필요하다면 기존의 해시함수를 쉽게 교환할 수 있도록 한다.
- 심각하게 기능저하를 유발하지 않고 해시함수의 원래 성능을 유지하도록 한다.
- 키를 보다 쉽게 다루고자 한다.
- 내장된 해시 함수가 충분히 강하다면
  인증 메커니즘의 강도에 대한 암호해독의 정도를 확실히 파악할 수 있도록 한다.

8.5.3 HMAC의 순서

- HMAC에서는 다음 순서로 MAC 값을 계산한다

일방향 해시 함수를 사용한 메시지 인증 코드의 예 (HMAC)

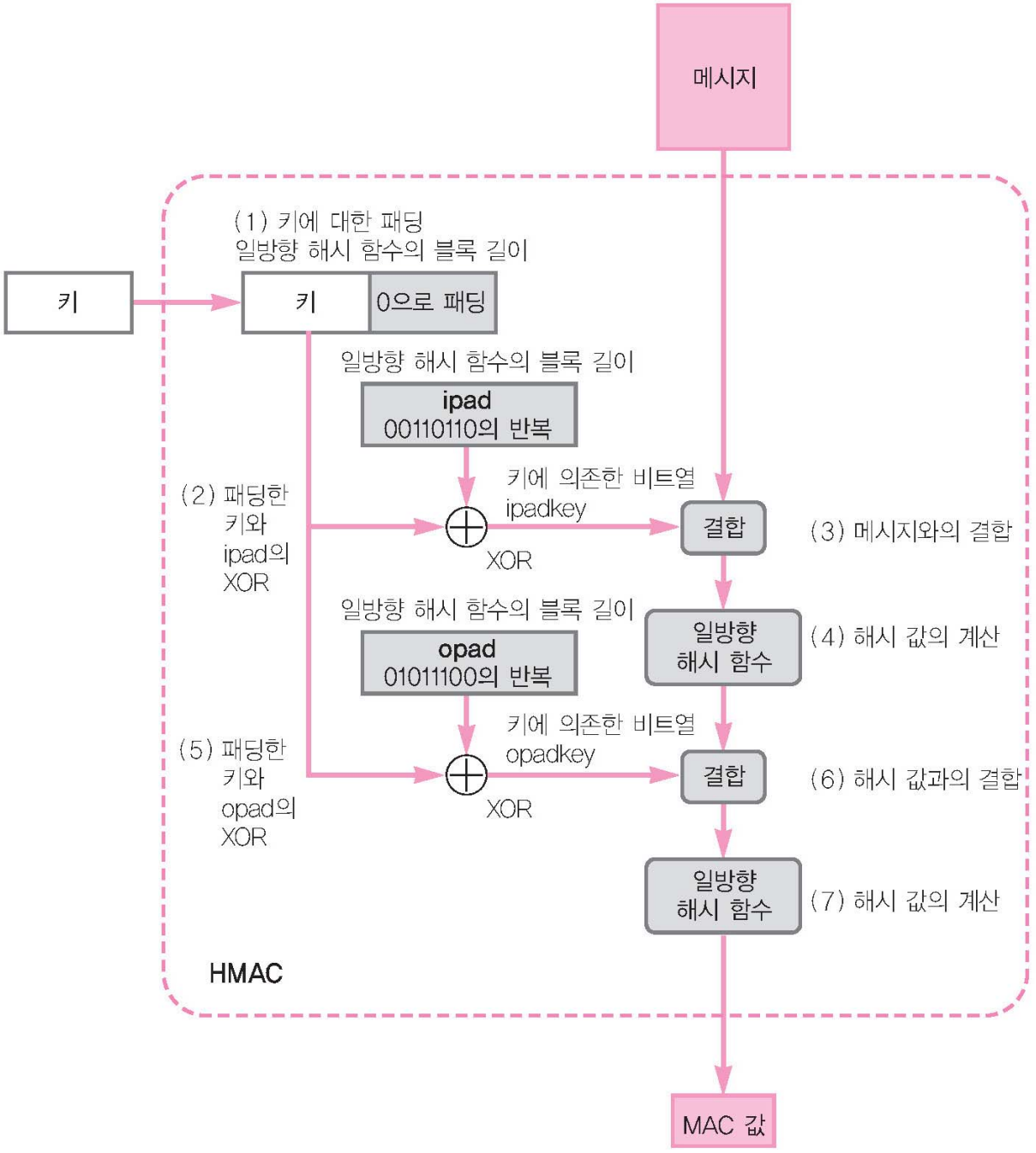
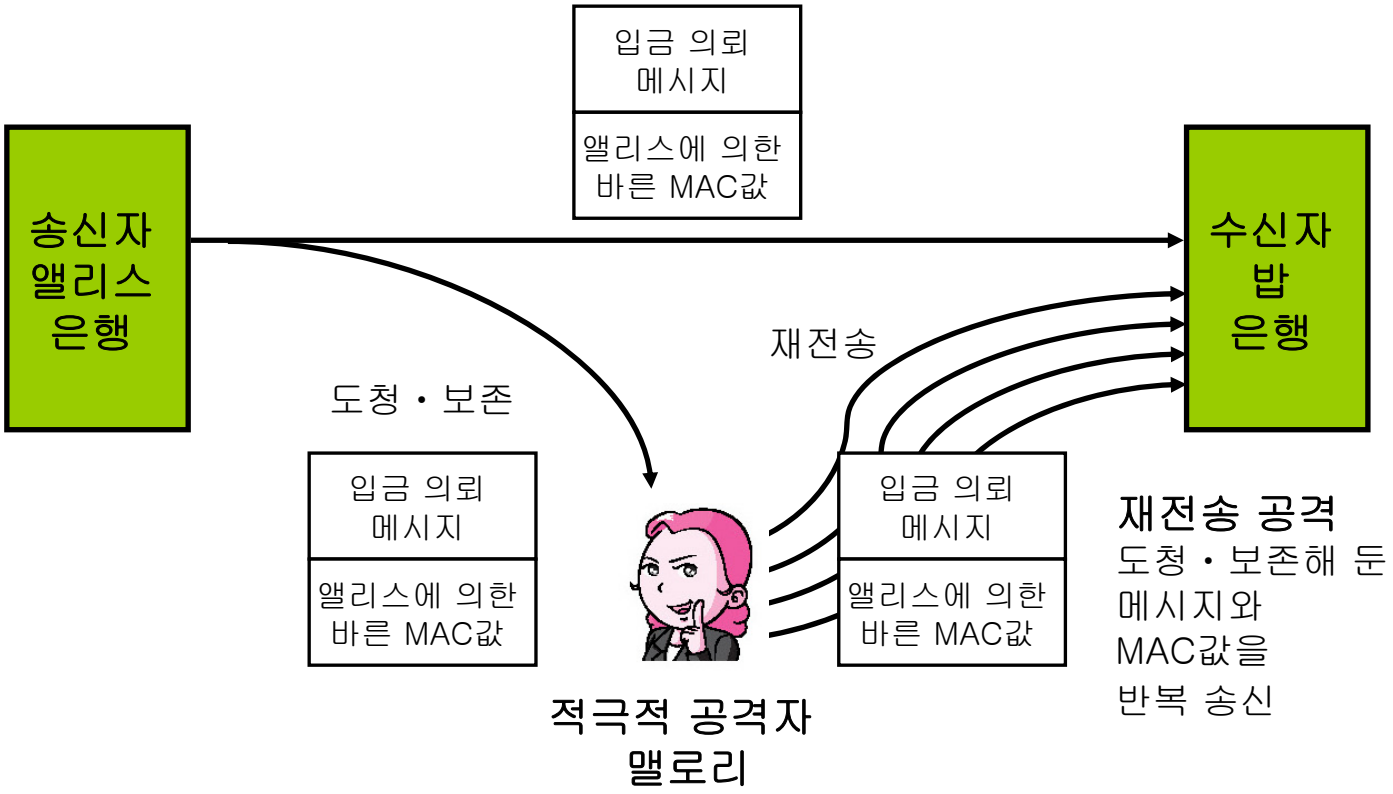


그림 8-7 일방향 해시 함수를 이용한 메시지 인증 코드의 예(HMAC)

8.6 메시지 인증 코드에 대한 공격

8.6.1 재전송 공격


입금 의뢰
메시지
앨리스에 의한
바른 MAC값
송신자
앨리스
은행
수신자
밥
은행
재전송
도청・보존
입금 의뢰
메시지
앨리스에 의한
바른 MAC값
입금 의뢰
메시지
앨리스에 의한
바른 MAC값
재전송 공격
도청・보존해 둔
메시지와
MAC값을
반복 송신
적극적 공격자
맬로리

재전송 공격을 막을 수 있는 방법

- 순서 번호(sequence number)
  - 송신 메시지에 매회 1씩 증가하는 번호
- 타임스탬프(timestamp)
  - 송신 메시지에 현재 시각을 넣는다
- 비표(nonce)
  - 메시지를 수신하기에 앞서 수신자는 송신자에게 일회용의 랜덤한 값(비표)을 건네준다.

8.6.2 키의 추측에 의한 공격

- 메시지 인증 코드에 대해서도 **전사공격**과 **생일 공격**이 가능하다.
- 공격자에 의해 송수신에서 사용된 **키를 추측당해서는 안 된다.**
- 메시지 인증 코드에서 사용하는 키를 생성할 때에는 암호학적으로 안전하고 강한 의사난수 생성기를 사용해야 한다.

8.7 메시지 인증 코드로 해결할 수 없는 문제

- 메시지 인증 코드로는 해결할 수 없는 사항
  - 제3자에게 증명하기
  - 부인 방지

8.7.1 제삼자에 대한 증명

- 앨리스로부터 메시지를 받은 밥이 「이 메시지는 앨리스가 보낸 것이다」라는 것을 제삼자인 검증자 빅터에게 증명하고 싶다고 하자.
- 그러나 메시지 인증 코드로 그 증명을 행할 수는 없다.

8.7.2 부인 방지

- 밥이 MAC 값이 딸린 메시지를 받았다고 하자.
- 이 MAC 값은 앨리스와 밥이 공유하고 있는 키를 사용해서 계산한 것이다.
- 밥은 「이 메시지는 앨리스로부터 온 것이다」라고 알 수 있다.
- 그러나 위에서 말한 것처럼 그것을 검증자 빅터에게 증명할 수는 없다.

8.7.2 부인 방지

- 즉, 송신자 앨리스는 의도적으로 혹은 자신이 불리하게 될 가능성 등을 고려하여
  - 「나는 밥에게 그런 메시지를 보내지 않았어」라고 빅터에게 주장할 수도 있다는 것이다.

- 이와 같은 주장을 **부인**(repudiation)이라고 한다.