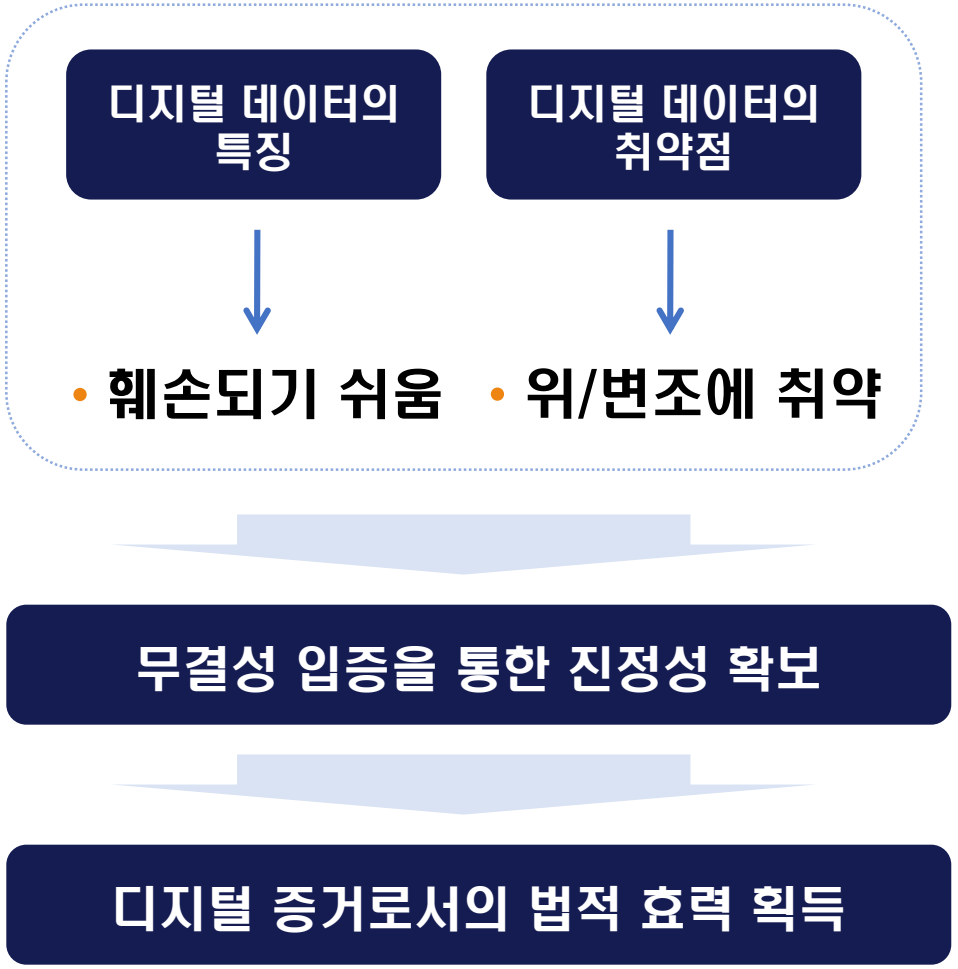
디지털 증거의 무결성 유지 및 검증

김 종 성

국민대학교

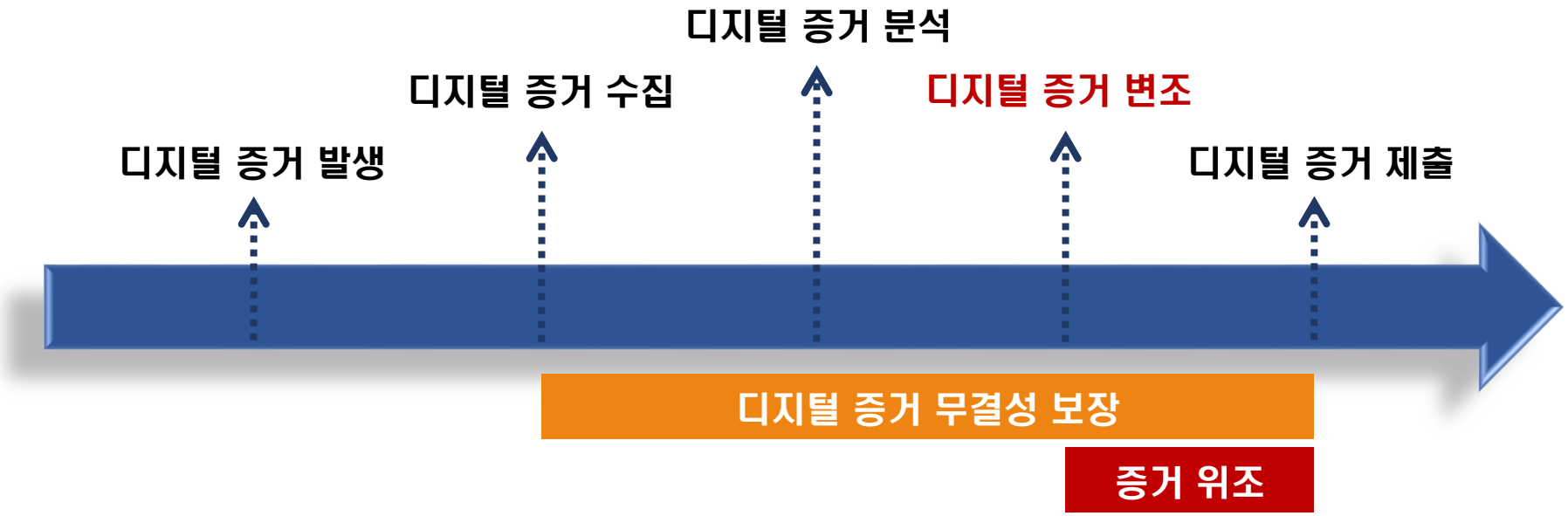
1. 디지털 증거의 무결성

- 디지털 데이터의 무결성 유지



1. 디지털 증거의 무결성

- 디지털 데이터의 무결성 유지
  - 디지털 증거의 신뢰성
    - 디지털 증거가 위조되어 법정에 제출되는 경우
    - 디지털 증거가 위조되지 않았음에도 불구하고, 용의자 또는 피고소인이 디지털 증거가 위조되었을 가능성을 이유로 증거 효력을 무력화시키려 하는 경우



1. 디지털 증거의 무결성

- 디지털 증거의 무결성
  - 증거 수집 과정과 내용에 대한 인증
    - 법원에서 증거 수집 과정이 무결성을 보장하고 적법 절차를 거쳐 이루어졌음을 입증할 수 있어야 함

수집 도구

- **법원에서 인정한 도구**
- **기능에 대한 명세가 명확한 도구**

수집 과정

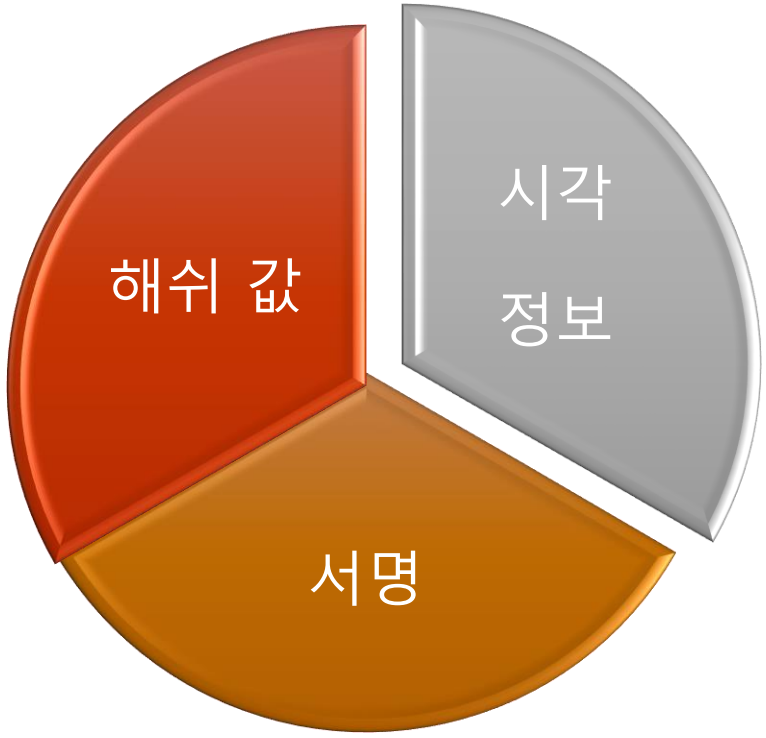
- **비디오 카메라로 전 과정 기록**
- **아날로그 or 디지털(w/전자서명)**

제 3자에 의한 무결성 인증

- **공식적으로 인증된 단체나 기관 존재하지 않음**
- **현재는 전문가를 초빙하여 참관**
- **법정, 검/경찰, 민간이 인정할 수 있는 인증기관 요구**

1. 디지털 증거의 무결성

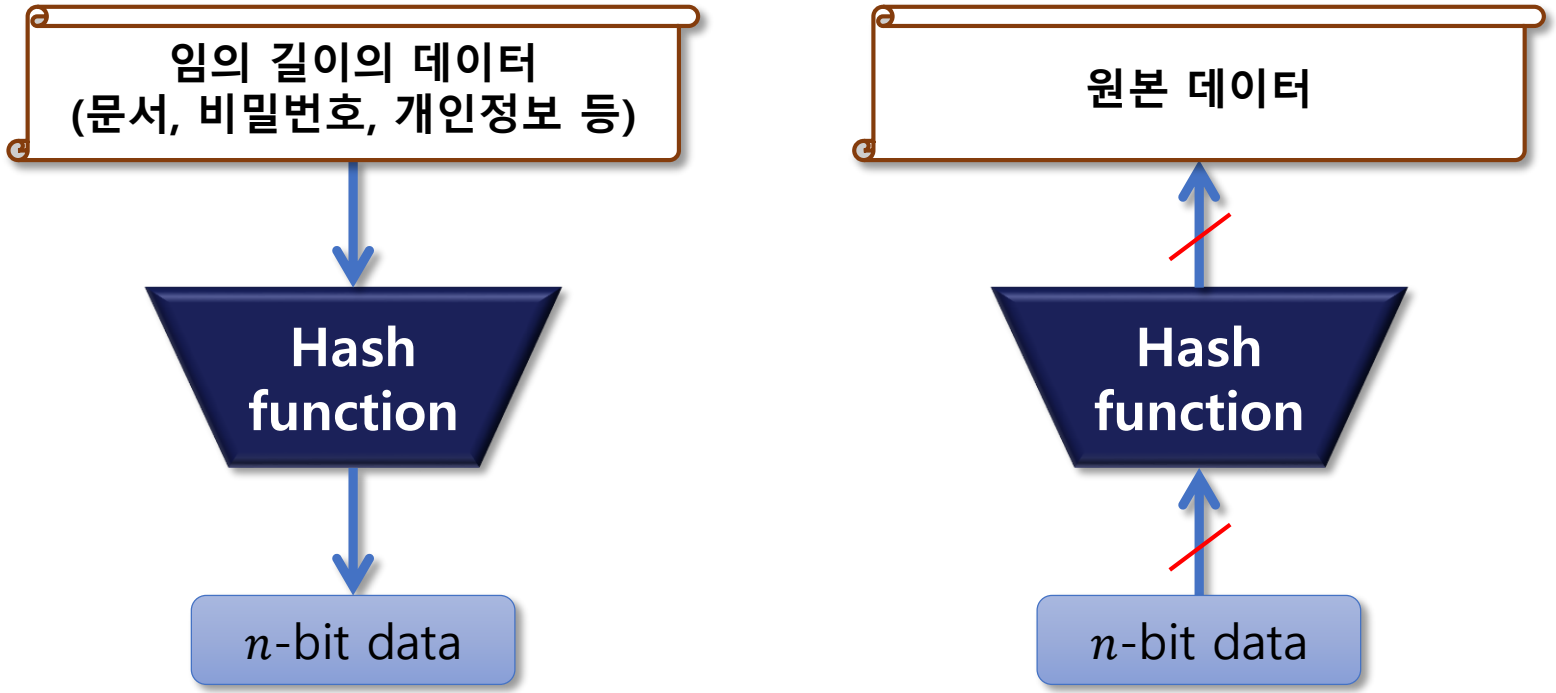
- 디지털 증거의 무결성
  - 무결성 입증을 위한 3가지 요소



2. 해쉬함수

- 해쉬함수(Hash function)
  - 임의의 길이의 데이터를 고정된 길이(n비트)의 데이터로 매핑하는 함수

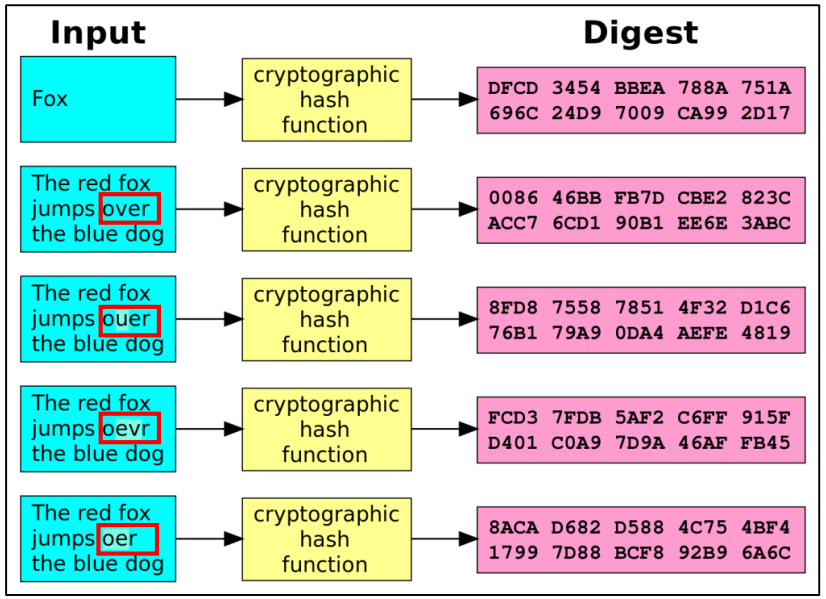
$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$



2. 해쉬함수

- 해쉬함수(Hash function)
  - 해쉬 값이 중복되는 데이터 쌍을 찾는 것이 현실적으로 불가능하다.
  - 무결성 제공, 전자서명, 파일식별 등에 사용함
  - 쉐도효과(Avalanche effect) : 입력의 작은 변화에도 출력에서는 큰 변화
  - MD5, SHA-1, SHA-32, SHA-3 등
  - 비암호학적 해쉬함수에는 CRC32 등이 있음

암호학적 해시함수의 입·출력 (SHA-1)



(그림출처: Wikipedia)

2. 해쉬함수

- 해쉬함수의 응용

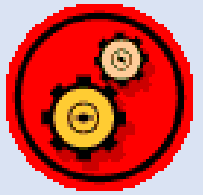
데이터 무결성검사

전자 서명

해쉬 함수

인증

난수 생성기



2. 해쉬함수

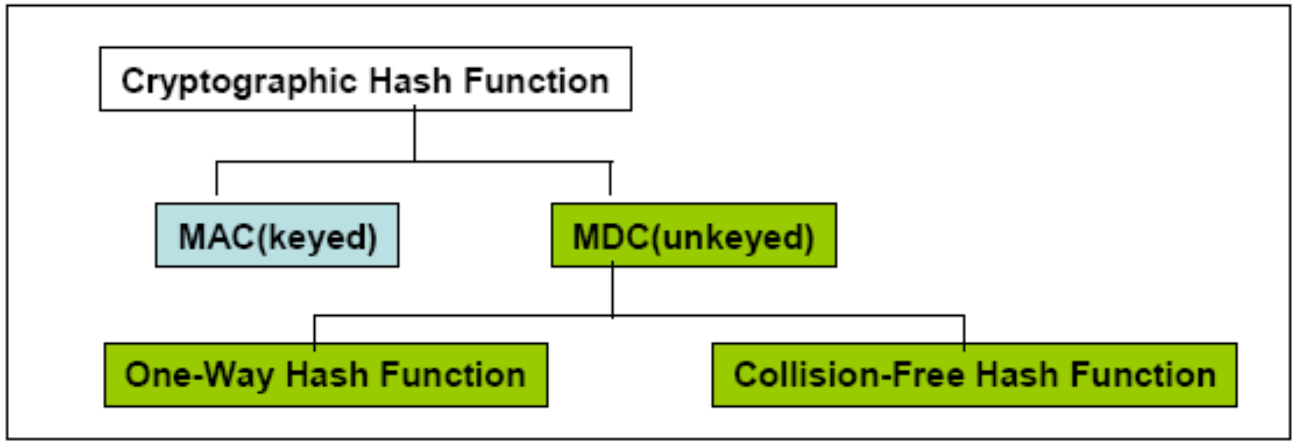
- 해쉬함수의 필요성

무결성	• 악의적인 사용자에 의한 데이터 위/변조 확인
효율성	• 데이터의 거대화 방지 • 전자 서명 시 연산의 효율성을 증대 시킴

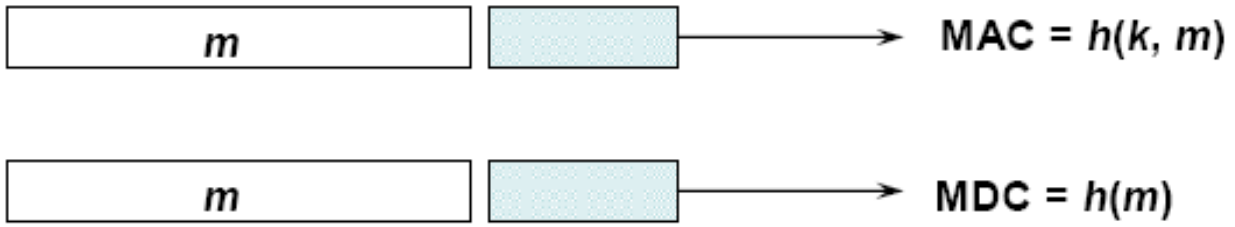
- 입력 값과 해쉬 값에 대해서, 해시 값을 망가뜨리지 않으면서 입력 값을 수정하는 공격에 안전해야 함
- 이런 성질을 가지는 **해쉬 값은 의도적으로 손상시키지 않았는지에 대한 검증 장치로 사용할 수 있어 디지털 포렌식의 무결성 검증에 많이 활용됨**

2. 해쉬함수

- 해쉬함수의 분류
  - 키 사용 유무에 따른 해쉬 함수의 분류



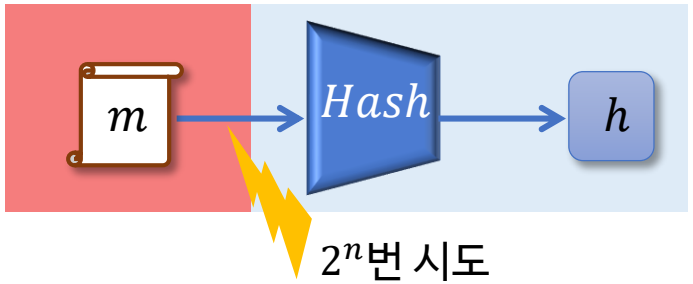
–



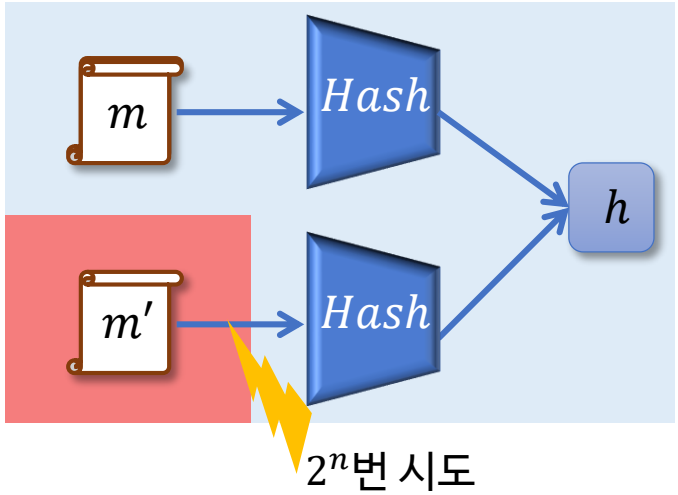
2. 해쉬함수

: 주어진 정보 : 알아내는 정보

- 해쉬함수의 성질
  - 해쉬함수(Hash function)
    - 역상(preimage), 제2역상(2nd preimage), 충돌쌍(collision) 공격에 안전성을 가져야 함
  - 역상 공격
    - 주어진 해쉬 값 h 를 갖는 메시지 m을 2^n보다 적은 복잡도로 찾는 공격



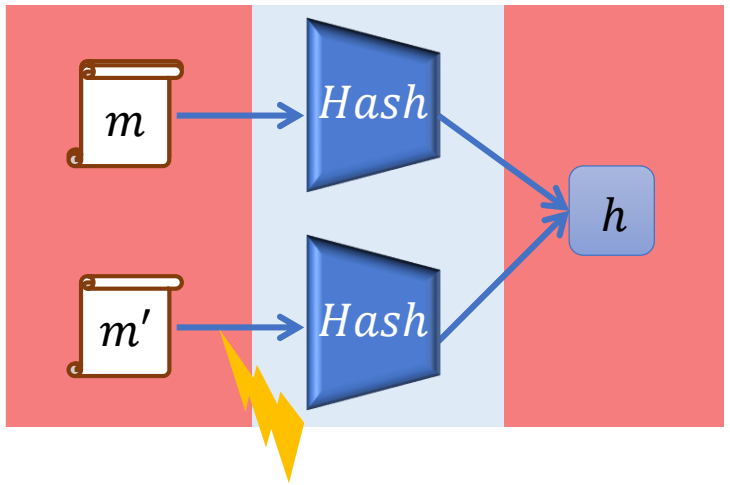
  - 제2역상 공격
    - 주어진 메시지 m과 같은 해쉬 값 h을 가지는 메시지 m'을 2^n보다 적은 복잡도로 찾는 공격



2. 해쉬함수

: 주어진 정보 : 알아내는 정보

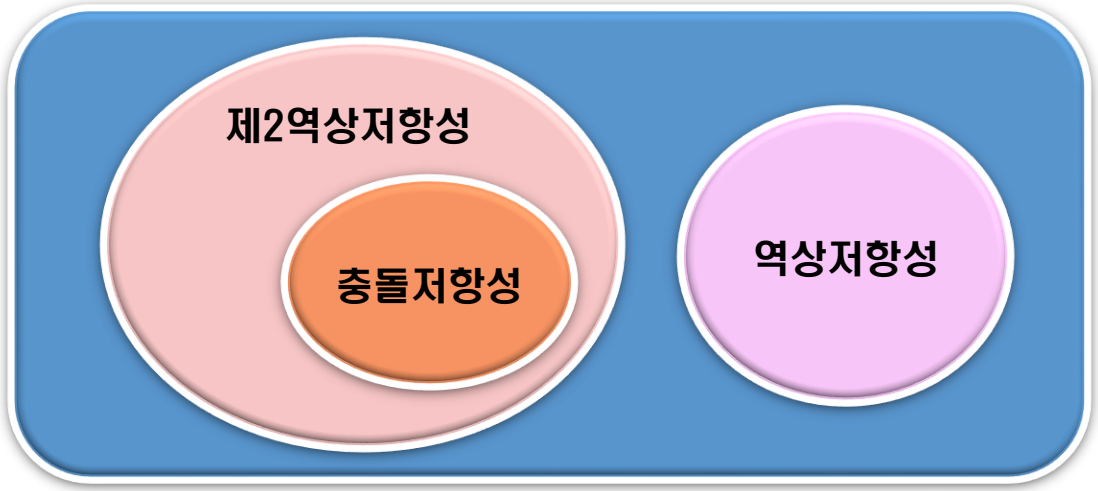
- 해쉬함수의 성질
  - 해쉬함수(Hash function)
    - 역상(preimage), 제2역상(2^{nd} preimage), 충돌쌍(collision) 공격에 안전성을 가져야 함
  - 충돌쌍 공격
    - 같은 해쉬 값 h를 가지는 서로 다른 메시지 쌍을 $2^{n/2}$보다 적은 복잡도로 찾는 공격



$2^{n/2}$개의 서로 다른 메시지에 대해 해시값 충돌 여부를 확인
[생일역설에 의함]

2. 해쉬함수

- 해쉬함수의 성질
  - 해쉬함수의 안전성 성질들 간의 관계



2. 해쉬함수

▪ 생일 역설

- 생일 역설(Birthday Paradox)과 해쉬함수의 안전성

생일 역설

- 가능한 데이터의 개수가 n일 때, $2^{n/2}$정도의 데이터가 있으면 일치하는 데이터가 존재할 확률이 ½보다 크다.

- 어느 집단에서 생일이 같은 한 쌍 이상의 학생이 존재할 확률(p)이 0.5이상이 되기 위한 학생수(r) ?
- $p = 1 - 1(1-1/n)(1-2/n) \ldots (1-\{r-1\}/n)$
- When $n=365$ and $r \geq 23$, $p \geq 0.5$

2. 해쉬함수

▪ 생일 역설

- 생일 역설(Birthday Paradox)과 해쉬함수의 안전성

해쉬함수의 안전성

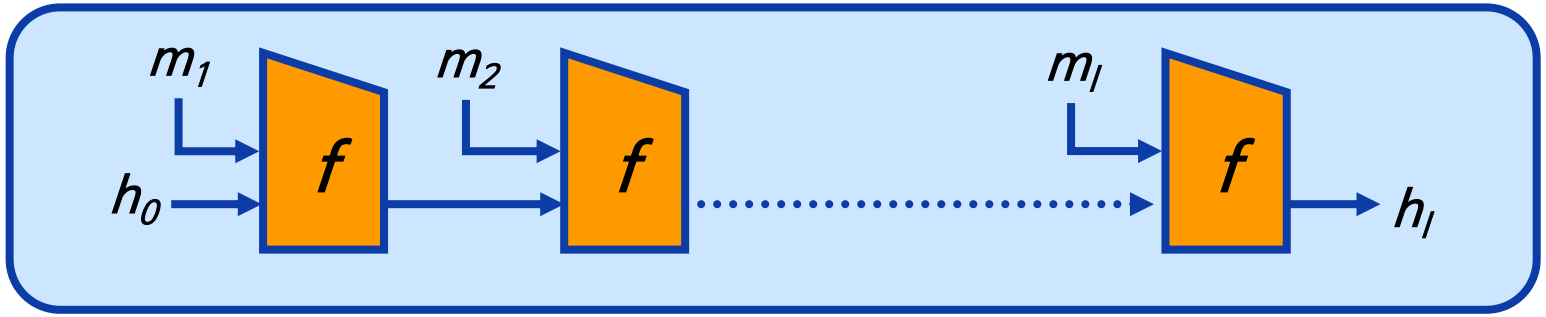
- 해쉬함수의 출력길이가 n비트이면, 생일 역설에 의해 그 해쉬함수의 안전성은 $2^{n/2}$ 를 넘을 수 없음

	해쉬 함수의 출력 길이	해쉬 함수의 안전성
MD4, MD5	128	2^{64}
HAS-160, SHA1	160	2^{80}
SHA-256	256	2^{128}

2. 해쉬함수

- MD 구성방법
  - 1989년 CRYPTO에서 Merkle과 Damgard에 의해 제안됨

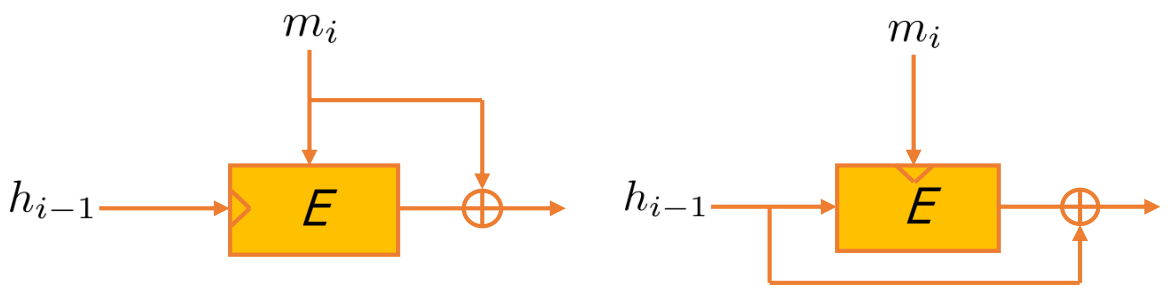
설계논리	•고정된 입출력 크기를 갖는 함수를 이용하여 임의의 길이의 입력 값을 다루는 해쉬함수를 구성하는 방법
압축함수(f)	•고정된 입출력 크기를 갖는 함수 : 압축함수 (Compression Function)



2. 해쉬함수

- 압축함수 설계 논리
  - 해쉬함수의 기반이 되는 압축 함수의 설계논리에 따른 분류

전용 해쉬함수	•MD4, MD5, SHA-1, SHA-2, HAS-160 등과 같이 순수하게 해쉬함수로서 이용되기 위하여 설계
블록암호(E) 기반 해쉬함수	•블록암호를 기반으로 역상저항성을 만족하도록 변형하여 설계됨(MDC-2, MDC-4, PGV 모델)



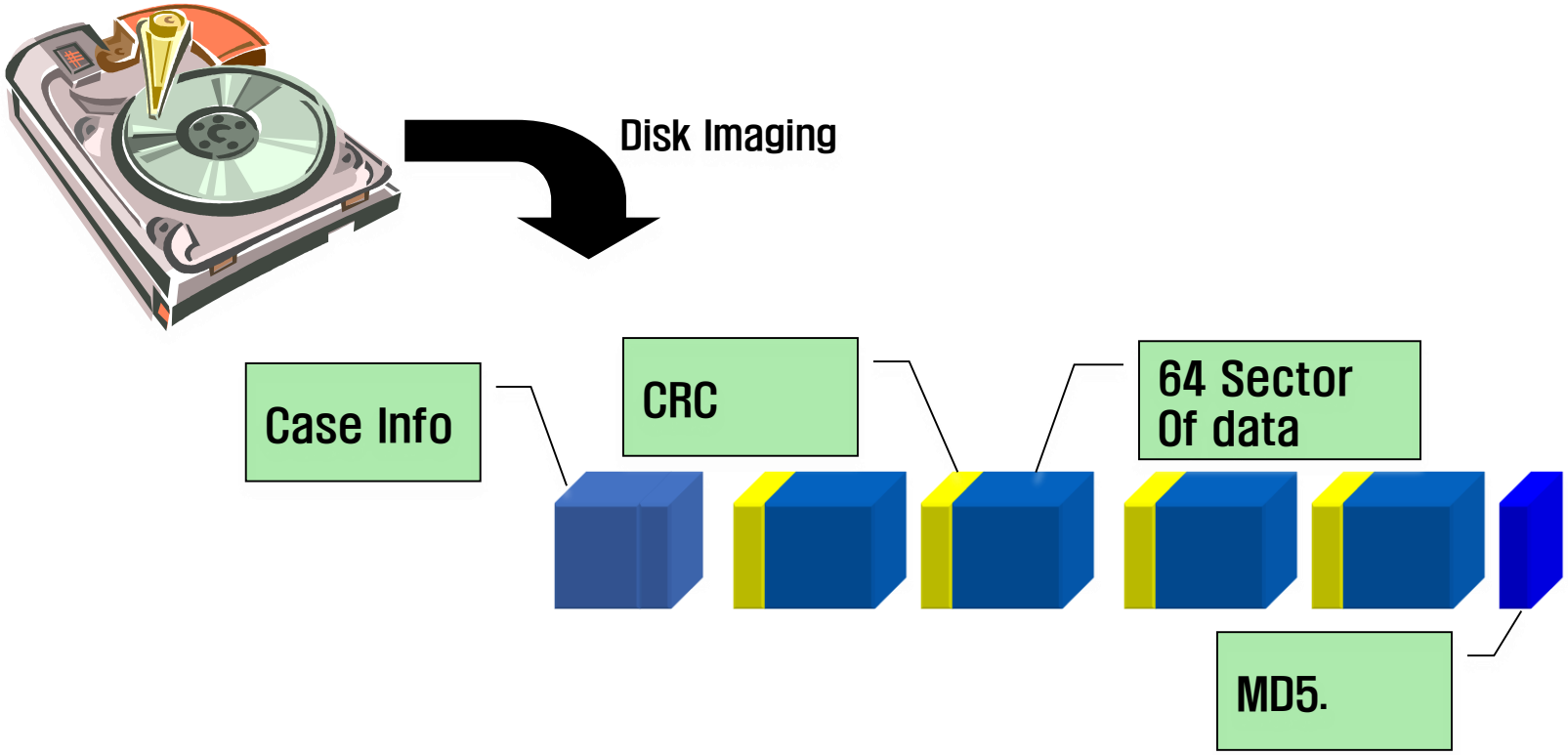
2. 해쉬함수

- 무결성과 해쉬함수
  - 해쉬함수를 이용한 증거 위/변조 방지
    - 비트 스트림 복제(Bit Stream Clone) 방식으로 저장매체를 전체 복사하여 하드 디스크 드라이브 이미지를 생성한 후, 해쉬함수를 적용
    - 해쉬 및 오류 검증 알고리즘을 저장매체와 이미지에 적용
  - 해쉬 알고리즘의 특성
    - 원본 데이터를 1비트만 바꿔도 해쉬 함수의 결과 값은 전혀 다른 출력 값을 생성하기 때문에 증거 무결성에 활용되고 있음
  - 오류 검증 알고리즘의 특성
    - CRC(Cyclic Redundancy Check) : 전송 데이터 내에 에러가 있는지 확인하기 위한 방법 중의 하나

해쉬 및 오류 검증 알고리즘을 원본 Disk와 Disk Image에 적용하여 보관한 뒤, 법정 증거 제출 시 무결성을 주장

2. 해쉬함수

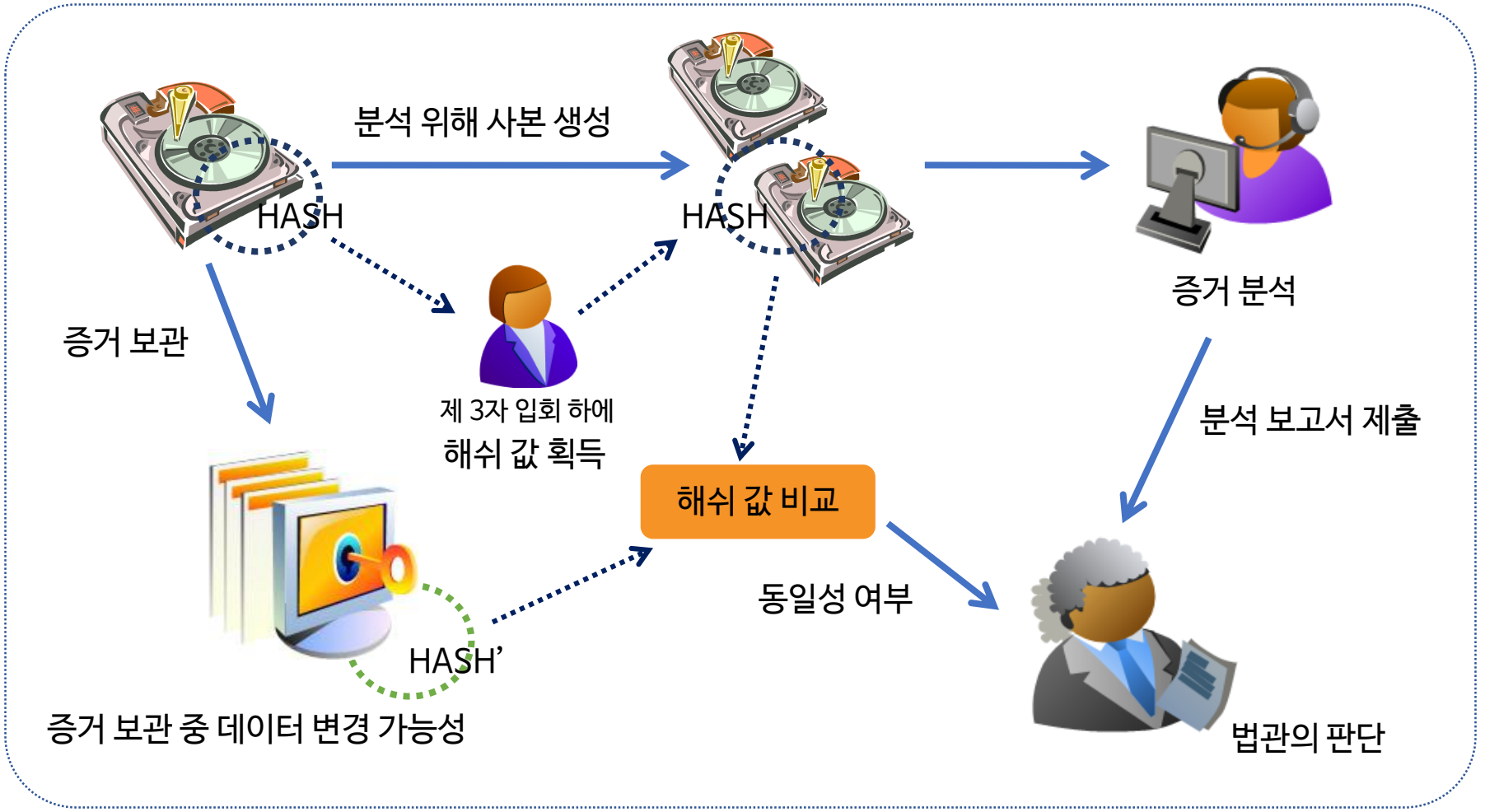
- 무결성과 해쉬함수
  - EnCase의 디지털 증거 무결성 확보 방법



$$V = h(H) = h(I)$$

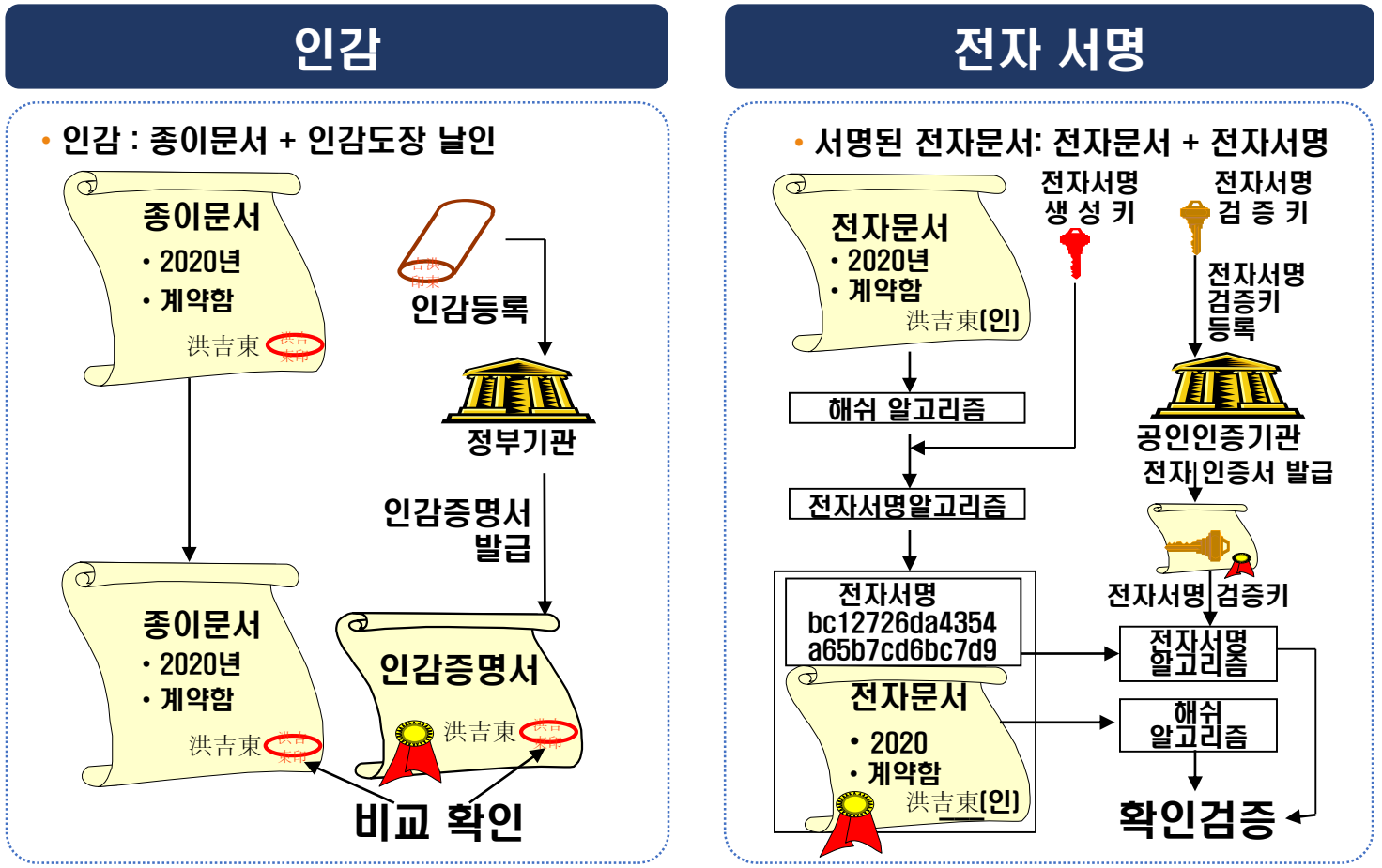
2. 해쉬함수

- 디지털 증거의 무결성 확보 및 판단



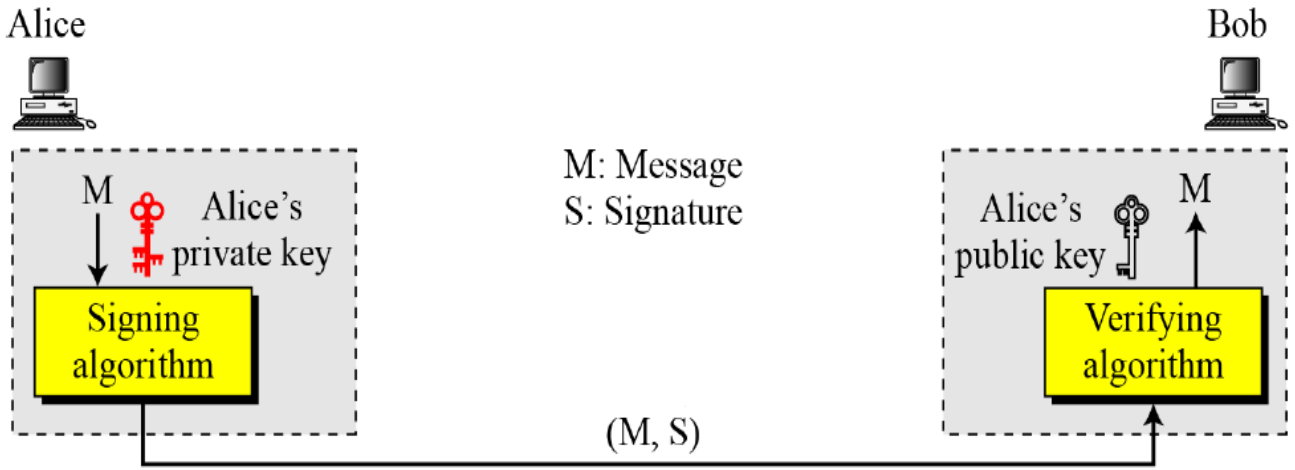
3. 전자서명

- 전자서명
  - 현재 사용되고 있는 도장이나 서명을 디지털로 실현한 것



3. 전자서명

- 전자서명-동작 원리



- 서명 생성: 개인키를 가지고 있는 사람만이 가능
- 서명 확인: 공개키를 기반으로 누구나 확인 가능
  - 인감-소유자: 국가기관에서 인감 등록, 증명서 발급
  - 공개키-소유자: 공인인증기관(CA)에서 공개키 등록, 인증서 발급

3. 전자서명

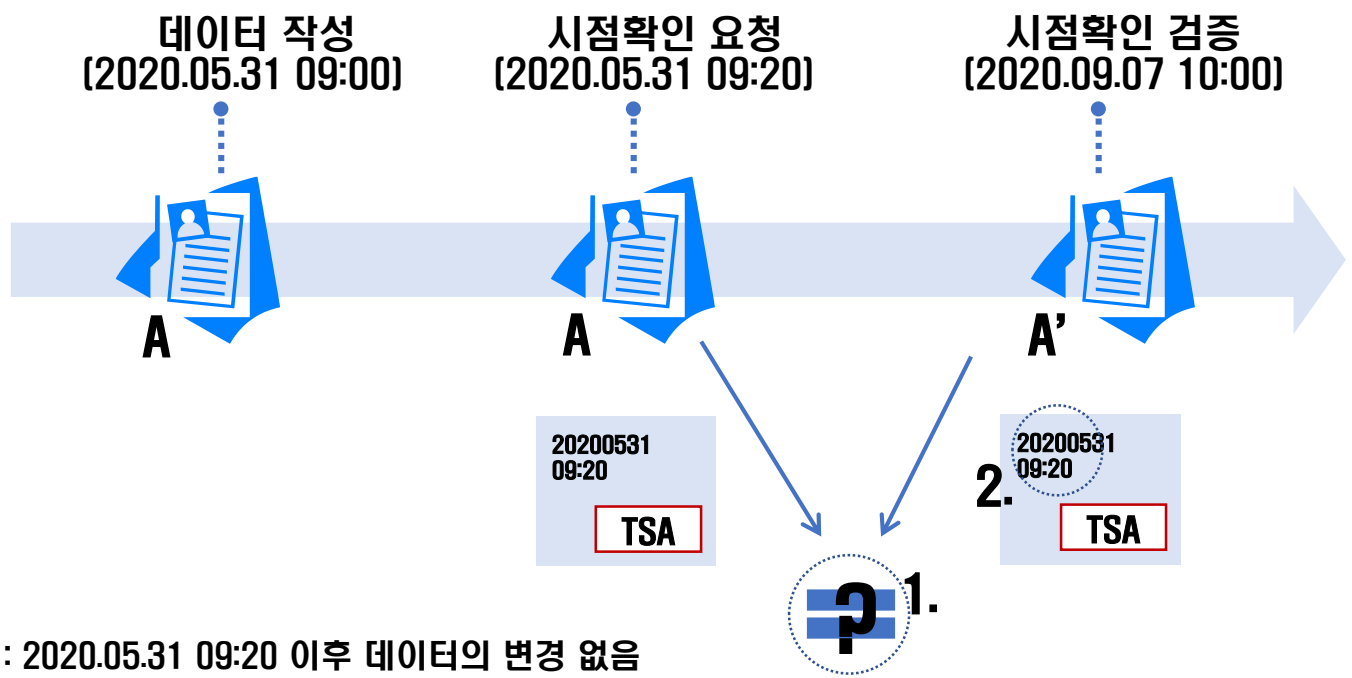
- 시점 확인 서비스(Time Stamping Service)
  - 임의의 디지털 데이터가 특정한 시점에 존재하였으며, 특정 시점 이후에는 데이터의 내용이 변경되지 않았음을 증명해주는 서비스
  - 디지털 데이터와 객관적인 시각 정보를 결합한 뒤 제 3자의 전자 서명을 거쳐 시점 확인 토큰(Time Stamping Token) 생성
  - 전자 서명과의 비교
    - 공통점: 디지털 데이터의 무결성을 입증하기 위해 사용
    - 차이점

      전자서명: “누가” 서명을 하였는가에 초점

      시점 확인 서비스 : “언제” 서명을 하였는가에 초점

3. 전자서명

- 시점 확인 서비스(Time Stamping Service)
  - 무결성 입증 원리



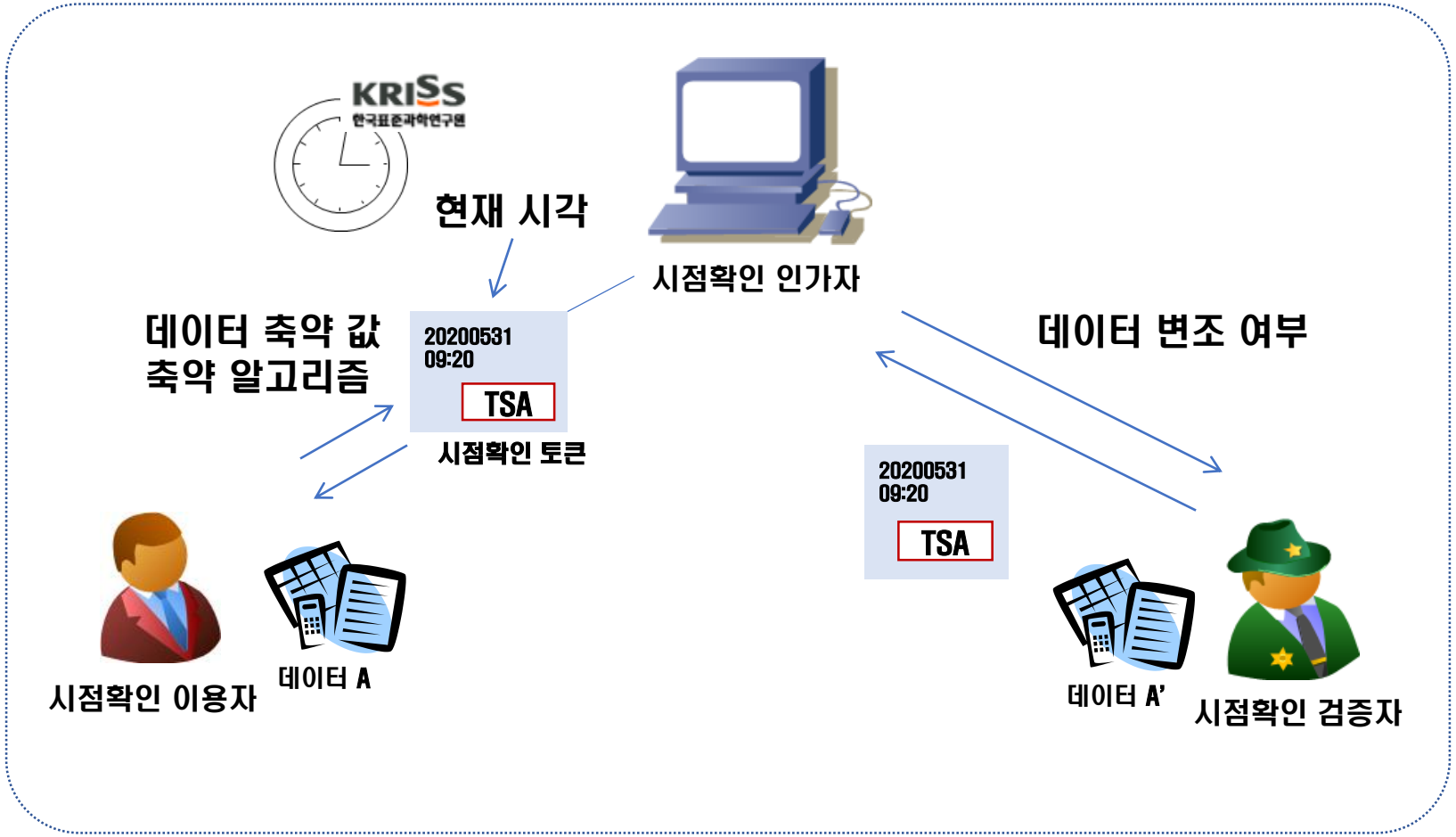
1 : 2020.05.31 09:20 이후 데이터의 변경 없음

2 : 2020.05.31 09:20 이전에 작성

TSA : Time Stamping Authority, 시점확인인가자

3. 전자서명

- 시점 확인 서비스(Time Stamping Service)
  - 동작 원리



3. 전자서명

- 시점확인 토큰의 법적 효력
  - 시점확인 토큰의 무결성을 추정하기 위해서는 시점확인 인가자가 신뢰할 수 있는 제 3의 기관(TTP, Third Trust Party)이어야 함
    - 국내 시점 확인 서비스 제공 기관: 한국정보인증, 코스콤 공인인증센터, 금융결제원 전자인증센터