9장. 보조자료

디지털 서명

박 종 혁

(jhpark1@snut.ac.kr)

전자서명의 조건

- 위조불가
  :서명자만이 서명문을 생성 가능

- 서명자 인증
  :서명문의 서명자를 확인 가능

- 재사용 불가
  :서명문의 서명은 다른 문서의 서명으로 사용 불가능

- 변경 불가
  :서명된 문서의 내용 변경 불가능

- 부인 불가
  :서명자는 후에 서명한 사실을 부인 불가능

전자서명의 종류

- RSA : (Rivest & Shamir & Adleman 제안, 1978)
- ElGamal : (ElGamal 제안 , 1985)
- DSA : (NIST에서 1991년 미국전자서명 표준으로 제안)
- Schnorr : (1989년 Schnorr가 개인식별방식과 함께 제안)
- GQ : (1998년 Guillou와 Quisquater가 제안)
- ESIGN : (1991년 후지오까, 오까모도, 미야구찌가 제안)
- Fiat Shamir : (Fiat, Shamir, 1987)
- KCDSA : (1999, TTA표준)
- ECDSA : (2000, DSA의 변형, 미국 NIST 전자서명 표준)
- EC-KCDSA : (2001, KC-DSA의 변형, TTA표준)

공개키 전자서명 알고리즘

- 합성수의 소인수분해문제의 어려움에 기초한 RSA 알고리즘
- 유한체의 이산대수문제의 어려움에 기초한 KCDSA, DSA 등 ElGamal 형 알고리즘
- 타원곡선을 이용한 EC-DSA, EC-KCDSA

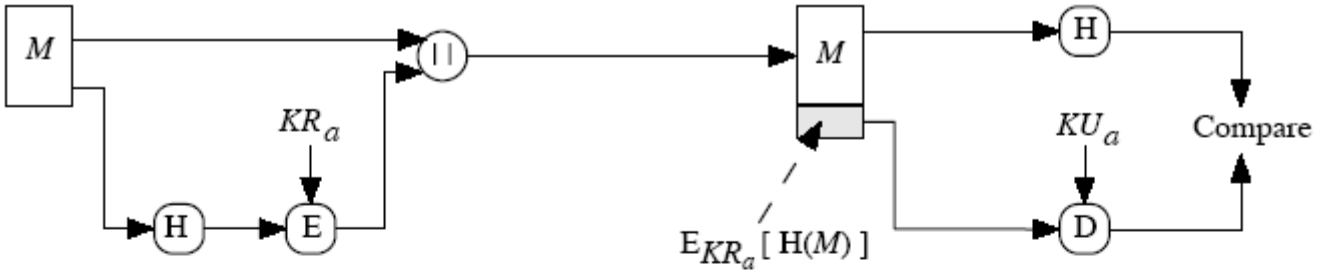
DSA 전자서명

- 1991년 NIST에서는 DSS에서 사용할 DSA을 제안.
  - DSS는 전자서명의 표준이고 이 표준안에서 사용되는 특정 알 고리즘이 DSA. (미국 연방 표준 서명 알고리즘)

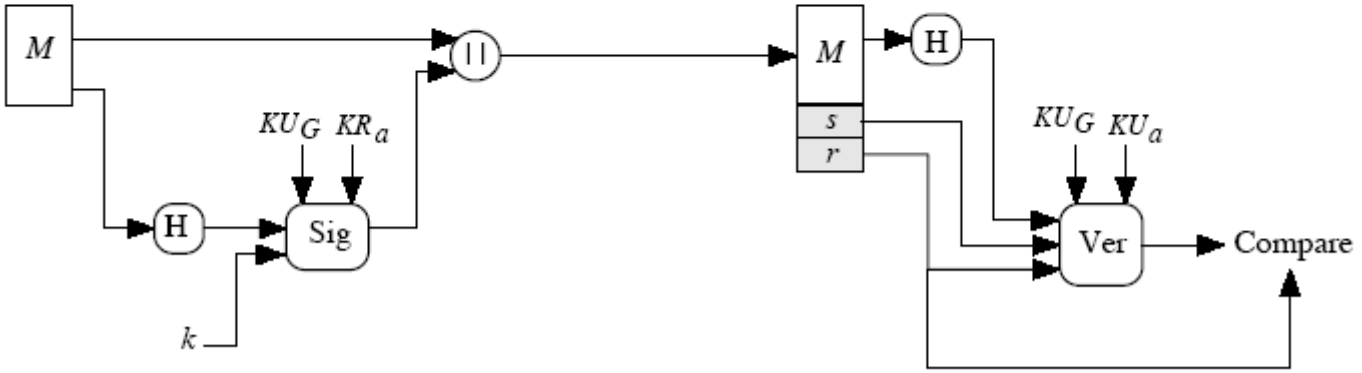
- 이산 대수 문제의 어려움을 안정성의 바탕으로 삼음
  - $Y=g^x \bmod p$ 에서 Y, g, p을 공개하더라도 x를 계산하기 어렵다는 가정

- 해쉬함수로는 SHA-1만을 이용한다.

디지털 서명의 표준 (DSS)



(a) RSA Approach



(b) DSS Approach

❑ RSA 접근 방식

- ❖ M : 메시지
- ❖ H : 해쉬 함수
- ❖ E : 공개키 암호 함수
- ❖ $E_{KRa}[H(M)]$: 메시지 M의 해쉬값을 A의 개인키로 암호화

❑ DSS 접근 방식

- ❖ M : 메시지
- ❖ H : 해쉬 함수
- ❖ s, r : 서명
- ❖ k : 난수
- ❖ KU_G : 전역적 공개키
- ❖ Sig : 서명 함수, Ver : 확인 함수

전자 서명 알고리즘 (DSA)

1) 서명 준비 과정

❖ 사용자 집단에 공통적이며, 공개되는 3개의 매개 변수

- **160** 비트 길이의 소수 **q**
- **512~1024** 비트 사이의 소수 **p**

  ⇒ **(p-1)**이 **q**로 나누어짐
- **h** $^{(p-1)/q}$ **mod p** 형태의 **g(1 < h < (p - 1))**

❖ 각 사용자는 개인키를 선택하고 공개키를 생성

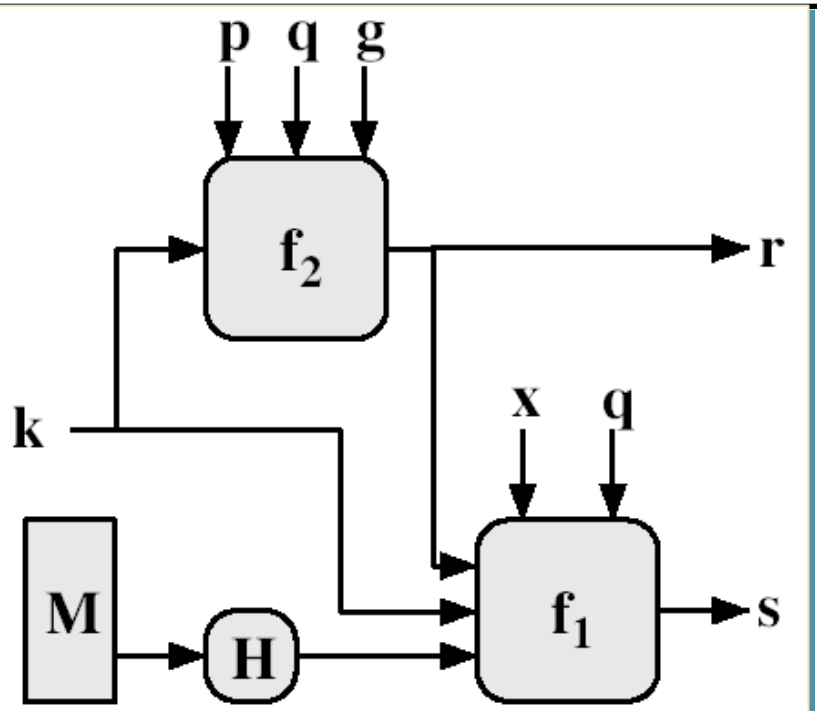
- 랜덤 개인키 **x** 선택 **(1 ≤ x ≤ q-1)**
- 개인키 **x** 로부터 공개키 **y** 계산
  - $y = g^x \bmod p$

1) 서명 생성 과정

- ❖ 메시지별로 고유한 정수 k를 랜덤하게 생성(0 < k < q)
- ❖ 서명
  - ➢ **r = $(g^k \bmod p) \bmod q$:** 메시지의 함수가 아님
  - ➢ **s = $[k^{-1} (H(M)+xr)] \bmod q$**
  - ➢ **Signature = (r, s)**

2) 서명 검증 과정

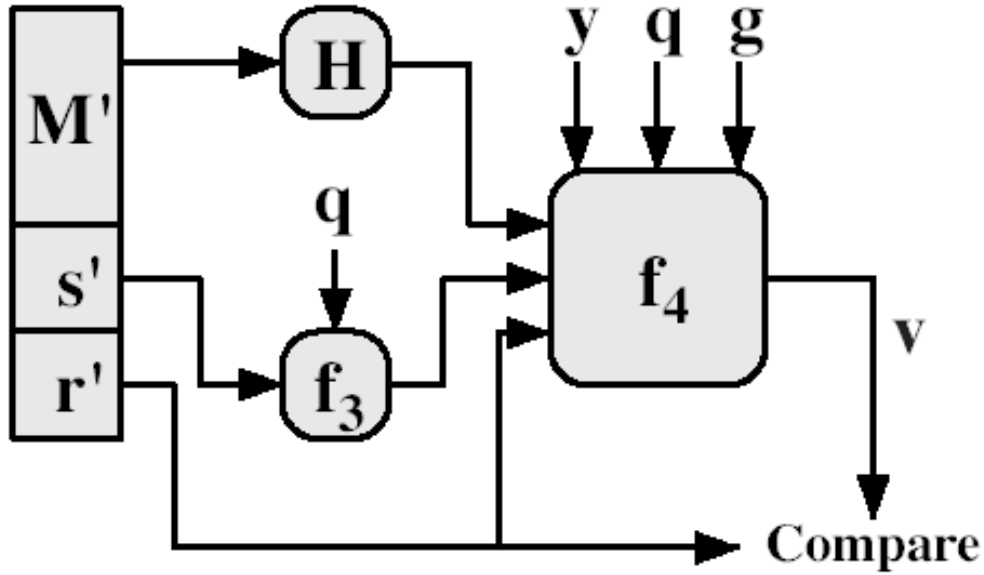
- ❖ 수신한 r'과 s'으로부터 계산한 v를 r'과 비교하여 검증
  - ➢ **w = $s^{-1} \bmod q$**
  - ➢ **u_1 =[(H(M)w)] mod q**
  - ➢ **u_2 = rw mod q**
  - ➢ **v = $[(g^{u1} y^{u2}) \bmod p] \bmod q$, y :** 사용자 공개키



$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing



$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r')$

$= ((g^{(H(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Thanks

Q & A