9장 전자 서명(Digital Signature)

정보보호이론

Spring 2015

고려대학교
KOREA UNIVERSITY

9.1 개요

- 전자서명 vs 종이서명

	종이 서명	전자 서명
작성 형태	문서 내에 서명이 포함	문서와 서명이 분리
검증 방법	서명 파일의 서명과 대조, 비교	별도의 검증기술을 적용
서명과 문서의 관계	One-to-Many	One-to-One
서명 검증	서명 파일이 필요	공개 검증

9.2 전자 서명의 기본 원리

전자 서명 과정

- 공개키 암호시스템과 유사
  - (공개키 pk, 개인키 sk) → (검증키 pk, 서명키 sk)
  - $Sig_{sk}(\cdot)$ = 서명 생성 알고리즘, $Ver_{pk}(\cdot)$= 검증 알고리즘

1. Alice → Bob : 메시지 m에 대한 서명 $s = Sig_{sk}(m)$
2. Bob : $Ver_{pk}(m, s)$로 검증

9.2.2 해쉬 함수를 이용한 전자 서명

- 해쉬 후 서명 : $s = Sig_{sk}(h(m))$
  - 효율적
  - 서명의 순서 변경이나 삭제를 방지
  - 서명 위조 방지 (9.4 절 참조)

9.3 전자 서명이 제공하는 보안 서비스

- 무결성(message integrity)
  - $Sig_{sk}(h(m)) \neq Sig_{sk}\left(h(m')\right)$ $if\ m \neq m'$$\{h$는 충돌저항성$\}$
- 메시지 인증(message authentication)
  - 정당한 sk를 이용한 서명만이 $Ver_{pk}(m, Sig_{sk}(h(m)))$을 통과
- 부인방지(non-repudiation)
  - $Sig_{sk}(h(m))$을 생성할 수 있는 사람은 sk 의 소지자

9.3.1 MAC vs 전자 서명

- MAC과 전자서명은 모두 무결성과 메시지 인증 제공
- 차이점

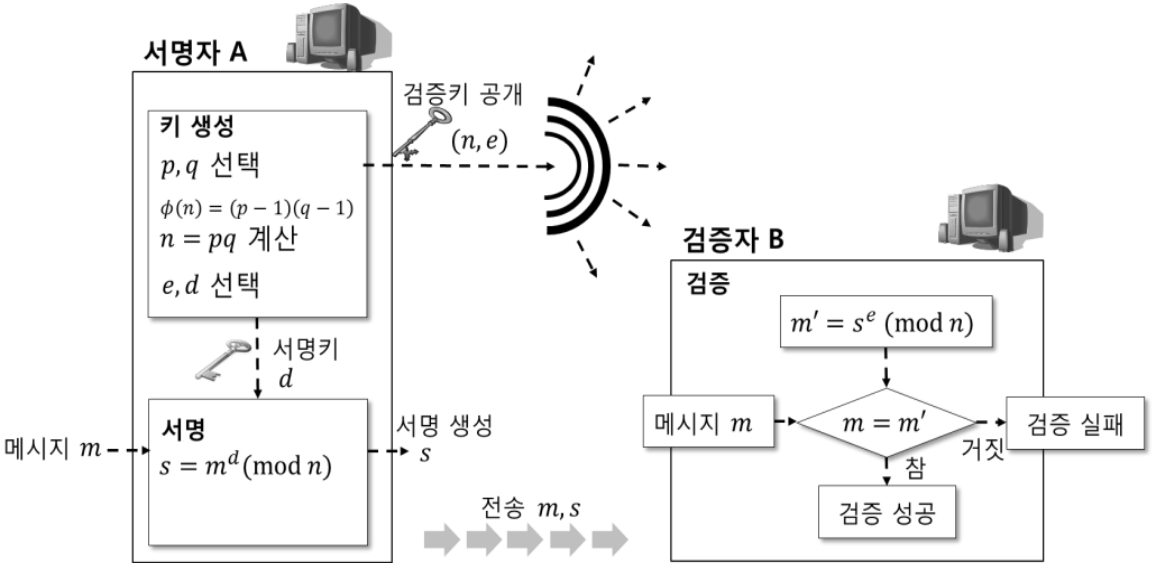
1. 공개 검증(public verifiability)
   - pk는 공개된 정보
2. 키 관리
   - MAC의 겨우, MAC key를 공유해야
3. 부인방지(non-repudiation)
   - $Sig_{sk}(h(m))$을 생성할 수 있는 사람은 sk 의 소지자
4. Transferability
5. MAC은 전자서명보다 2~3배 효율적

9.4 전자 서명의 안전성

- 공격 방법
  - 키만 주어진 공격(key-only attack)
  - 알려진 메시지 공격(known message attack)
  - 선택 메시지 공격(chosen message attack)
- 공격목적
  - 선택적 위조(selective forgery)
    - 원하는 메시지에 대하여 서명자의 서명을 생성하는 것이 목적
  - 존재적 위조(existential forgery)
    - 적어도 하나의 메시지와 이 메시지에 대응되는 서명자의 유효한 서명 값을 생성하는 것이 목적

9.5 다양한 전자 서명 기법

- RSA 전자 서명
  - 키 생성 : RSA 암호와 동일
  - 서명 생성 :
    - $Sig_{sk}(m) \equiv m^d \equiv s \pmod n$
  - 서명 검증 :
    1. $s^e \pmod n = m', \quad m' =? \, m$



9.5 다양한 전자 서명 기법

- RSA 전자 서명의 안전성
  - 키만 주어진 공격자에 의한 존재적 위조
    - 임의의 서명 값 s를 선택하여 메시지 $m \equiv (s)^e (\bmod n)$를 계산
    - $m \equiv (s)^e (\bmod n)$에 대한 서명이 s 라 주장

    →검증식 $Ver_{pk}(m, s) \equiv (s)^e (\bmod n)$을 통과

  - 알려진 메시지 공격자에 의한 존재적 위조
    - 알려진 서명 $s_1 \equiv m_1^d (\bmod n)$ & $s_2 \equiv m_2^d (\bmod n)$

    →$s_1 s_2 \equiv m_1^d \times m_2^d \equiv (m_1 \times m_2)^d \ (\bmod n)$

9.5 다양한 전자 서명 기법

- RSA 전자 서명의 안전성
  - 선택 메시지 공격자에 의한 선택적 위조
    1. 원하는 m을 선택하고, $m \equiv m_1 \times m_2 \pmod{n}$인 m_1과 m_2을 획득
    2. m_1과 m_2에 대한 정당한 서명값 s_1과 s_2를 각각 얻음
    3. $s_1 s_2 \equiv m_1^d \times m_2^d \equiv (m_1 \times m_2)^d \pmod{n}$
    - $m_1 \times m_2$ 에 대한 정당한 서명 $s_1 s_2$
    - m이 두 개의 큰 소수로 이루어졌다면, m_1과 m_2을 찾는 것이 매우 어렵다. 반대로 m이 작은 소수를 포함한다면 m_1과 m_2을 찾는 것은 어렵지 않다.

9.5 다양한 전자 서명 기법

- 해쉬를 이용한 RSA 전자 서명
  - $Sig_{sk}(m) \equiv h(m)^d \equiv s \pmod n$
  - 키만 주어진 공격자에 의한 존재적 위조
    - 임의의 서명 값 s를 선택하여 메시지 $m \equiv (s)^e \pmod n$를 계산

      →$(s)^e = h(m)$ → $h(\cdot)$의 역상 저항성(preimage resistance) 때문에 m을 찾는 것은 매우 어려움
  - 알려진 메시지 공격자에 의한 존재적 위조
    - 알려진 서명 $s_1 \equiv h(m_1)^d \pmod n$ & $s_2 \equiv h(m_2)^d \pmod n$

      →$s_1 \times s_2 \equiv h(m_1)^d \times h(m_2)^d \equiv (h(m_1) \times h(m_2))^d$

      $\not\equiv h(m_1 \times m_2)^d \pmod n$

      →$(h(m_1) \times h(m_2)) = h(m)$인 메시지 m을 발견해야 함

      →$h(\cdot)$의 역상 저항성(preimage resistance) 때문에 불가능

9.5 다양한 전자 서명 기법

- 해쉬를 이용한 RSA 전자 서명
  - $Sig_{sk}(m) \equiv h(m)^d \equiv s \pmod{n}$

  - 선택 메시지 공격자에 의한 존재적 위조
    1. 원하는 m을 선택하고, $m \equiv m_1 \times m_2 \pmod{n}$인 m_1과 m_2
    2. m_1과 m_2에 대한 서명값 s_1과 s_2를 각각 얻음
    3. $h(m_1)^d \times h(m_2)^d \equiv h(m)^d \pmod{n}$ 인 m을 찾는 것은 암호학적 해쉬 함수 $h(\cdot)$의 역상 저항성(preimage resistance) 때문에 어려움

9.5 다양한 전자 서명 기법

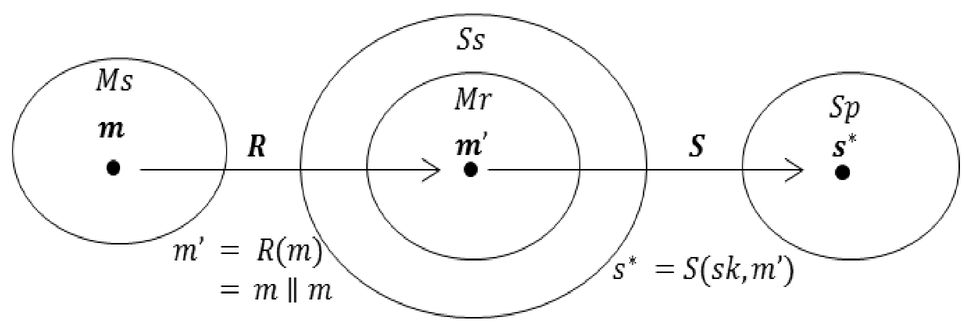
- 전자 서명의 종류
  - 메시지 부가형 전자 서명(Digital Signature with Appendix)
    - Ver_{pk}에 입력으로 메시지 m과 서명 s가 필요
  - 메시지 복원형 전자 서명(Digital Signature with Message Recovery)
    - Ver_{pk}에 입력으로 서명 s만 필요하며 검증과정에서 m 복원

9.5 다양한 전자 서명 기법

- 중복 함수를 이용한 RSA 전자 서명
  - 서명 생성
    - 중복 함수 $R(\cdot)$을 사용하여 $R(m)$을 계산
    - 서명키 d로 $R(m)$에 대한 서명 $Sig_{sk}(R(m)) \equiv \left(R(m)\right)^d \equiv s \pmod n$를 생성

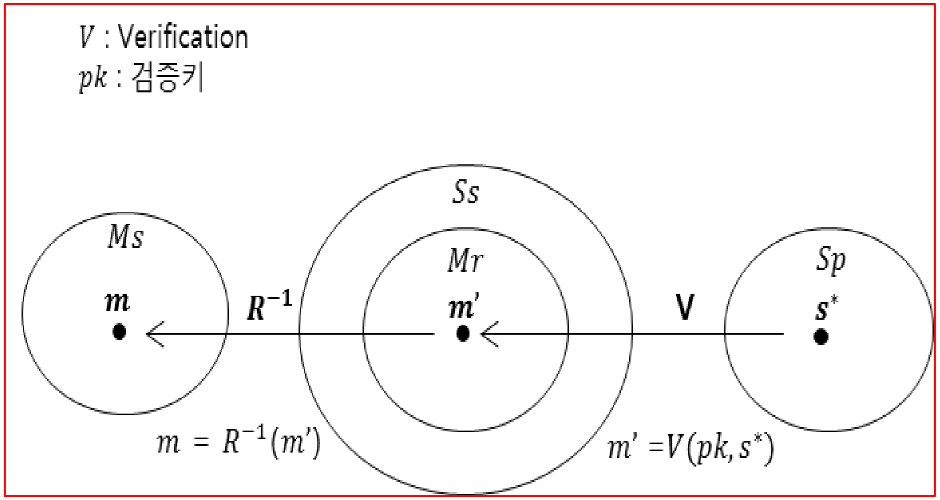
sk : 개인키
m : 메시지
Ms : 메시지 공간
$R(\cdot)$: 중복 함수

Ss : Signing 공간
Mr : Redundancy Image
Sp : Signature 공간
S : Signing Transformation



9.5 다양한 전자 서명 기법

- 중복 함수를 이용한 RSA 전자 서명
  - 서명 검증
    1. 서명 값 s와 공개키 (e, n)을 이용하여 $s^e \equiv m' \pmod n$을 계산
    2. m'이 올바른 형태이면 $R^{-1}(m')$을 계산하여 m을 얻고, 그렇지 않으면 유효한 서명이 아님
    - $R(m) = m \parallel m$인 경우,
      - 존재적 위조 : s를 선택, $m' \equiv (s)^e \pmod n$은 $m||m$의 형태이어야 함
      - Mr에 속할 확률은 $\frac{1}{2^{|m|}}$이며, m이 1024 비트인 경우 이 확률은 $\frac{2^{1024}}{2^{2048}} = \frac{1}{2^{1024}}$



9.5 다양한 전자 서명 기법

- The most commonly used method is adding randomness+hash : PSS (Probabilistic Signature Scheme)
  - a provably secure way of creating signatures with RSA due to Bellare and Rogaway [1996].
  - The method for creating digital signatures with RSA that is described in PKCS #1 has not been proven secure even if the underlying RSA primitive is secure; in contrast, PSS uses hashing in a sophisticated way to tie the security of the signature scheme to the security of RSA.
  - PSS-R is a message recovery variant of PSS with provable security.

9.5 다양한 전자 서명 기법

ElGamal 전자 서명

- 키 생성 :
  - $y = g^x (\mathrm{mod\ p})$, (y, g, p)는 검증키, x를 서명키
- 서명 생성 :
  1. $1 \le k \le p-2$ 의 범위에서 $p-1$과 서로소인 정수 k를 임의로 선택
  2. $\gamma \equiv g^k (\mathrm{mod}\ p)$와 $\delta \equiv (m - x\gamma)k^{-1} (\mathrm{mod}\ p-1)$를 계산
  3. 서명 값 $s = (\gamma, \delta)$
- 서명 검증 :
  1. 서명 값 $s = (\gamma, \delta)$와 서명한 메시지 m, 검증키 (y, g, p)
  2. $g^m (\mathrm{mod}\ p)\ =?\ y^\gamma \gamma^\delta (\mathrm{mod}\ p)$

→

$$y^\gamma \gamma^\delta \equiv g^{x\gamma} g^{k\delta} \equiv g^{x\gamma + k\delta} \equiv g^{x\gamma + k(m - x\gamma)k^{-1}} \equiv g^{x\gamma + (m - x\gamma)} = g^m (\mathrm{mod}\ p)$$

9.5 다양한 전자 서명 기법

ElGamal 전자 서명

- 키 생성 : $p = 113, g = 3$
  - 서명키 $x = 42$로 선택, $y \equiv g^x \equiv 3^{42} \equiv 69 \ (\mathrm{mod}\ 113)$
  - $(y, g, p) = (69,3,113)$
- 서명 생성 :
  1. $\mathrm{m} = 26, k = 23,$
  2. $\gamma \equiv g^k \equiv 3^{23} \equiv 39 \ (\mathrm{mod}\ 113),\ \delta \equiv (m - x\gamma)k^{-1} \equiv (26 - 42 \times 39) \times 39 \equiv 76 \ (\mathrm{mod}\ 112)$
  3. 메시지 $m = 26$에 대한 서명 값 $s = (\gamma, \delta) = (39,76)$
- 서명 검증 :
  1. $y^\gamma \gamma^\delta \equiv g^m \ (mod\ p)$
  2. $y^\gamma \gamma^\delta \equiv 69^{39}39^{76} \equiv 36 \ (\mathrm{mod}\ 113)$
  3. $g^m \equiv 3^{26} \equiv 36 \ (\mathrm{mod}\ 113)$

9.5 다양한 전자 서명 기법

ElGamal 전자 서명의 안전성

- 난수 k가 같을 때 알려진 메시지 공격 모델에서 키 획득 :

1. 두 개의 메시지 m_1과 m_2에 대하여 같은 k를 사용한 서명 s_1과 s_2을 가지고 있다고 가정

$$s_1 \equiv (\gamma_1, \delta_1) \equiv (g^k \pmod p), (m_1 - x\gamma_1)k^{-1} \pmod{p-1})$$
$$s_2 \equiv (\gamma_2, \delta_2) \equiv (g^k \pmod p), (m_2 - x\gamma_2)k^{-1} \pmod{p-1})$$

2. $\delta_1 - \delta_2 = (m_1 - x\gamma_1)k^{-1} - (m_2 - x\gamma_2)k^{-1} = (m_1 - x\gamma_1 - m_2 + x\gamma_2)k^{-1}$

3. $\delta_1 - \delta_2$ 값이 0이 아니라면 공격자는 k^{-1}을 계산

$$k^{-1} = \frac{\delta_1 - \delta_2}{(m_1 - m_2)}$$

4. $x = -(\delta_1 k - m_1)/\gamma_1 = -(\delta_2 k - m_2)/\gamma_2 \pmod{p-1}$

9.5 다양한 전자 서명 기법

- ElGamal 전자 서명의 안전성
  - (해쉬 함수를 사용하지 않을 때) 키만 주어진 공격 모델에서 존재적 위조
    1. 공격자는 $1 \le i, j \le p-2$인 정수 i와 j를 선택

    2. $\gamma = g^i y^j \pmod{p}$로 설정한다면 검증식
    $g^m \equiv y^\gamma \gamma^\delta \equiv y^\gamma (g^i y^j)^\delta \pmod{p} \quad \rightarrow \quad g^{m-i\delta} \equiv y^{\gamma+j\delta} \pmod{p}$

    3. 위조할 메시지 m과 이에 대한 서명
    $S(m) \equiv (\gamma, \delta) \equiv \left(g^i y^j \pmod{p}, \quad -\gamma j^{-1} \pmod{p-1}\right)$와
    $m \equiv -\gamma i j^{-1} \pmod{p-1}$로 설정
    $\rightarrow y^\gamma \gamma^\delta = g^{x\gamma}(g^i y^j)^{-\gamma j^{-1}} = g^{x\gamma}(g^i g^{xj})^{-\gamma j^{-1}} = g^{x\gamma - \gamma i j^{-1} - xj\gamma j^{-1}}$
    $= g^{x\gamma - \gamma i j^{-1} - x\gamma} = g^{-\gamma i j^{-1}} = g^m$

9.5 다양한 전자 서명 기법

- Schnorr 서명
  - Schnorr 전자 서명 : 소수 p의 크기가 1024비트일 때, γ 는 160비트 → 서명의 길이는 1184비트
    - ElGamal 서명 : 1024비트의 안전성을 보장하기 위해서는 사용되는 소수 p의 크기가 1024비트 → 서명 (γ, δ)의 길이는 $1024 \times 2 = 2048$비트
    - 스마트 카드와 같은 메모리 크기가 제한된 응용 환경에서는 짧은 길이의 서명이 요구
  - 키 생성 :
    1. 큰 소수 p와 $q|p-1$를 만족하는 소수인 q를 선택
    2. 위수가 q (in Z_p^*)인 생성원 g (즉 g는 q개의 원소를 갖는 subgroup을 생성)와 $1 \leq x \leq q$ −1인 정수 x를 임의로 선택
    3. $y \equiv g^x (\mathrm{mod}\, p)$
    4. (y, g, p, q)는 검증키로 사용하고, x를 서명키로 사용
    5. 안전한 해쉬 함수 $h\colon \{0,1\}^* \to \mathbb{Z}_q$ 를 선택

9.5 다양한 전자 서명 기법

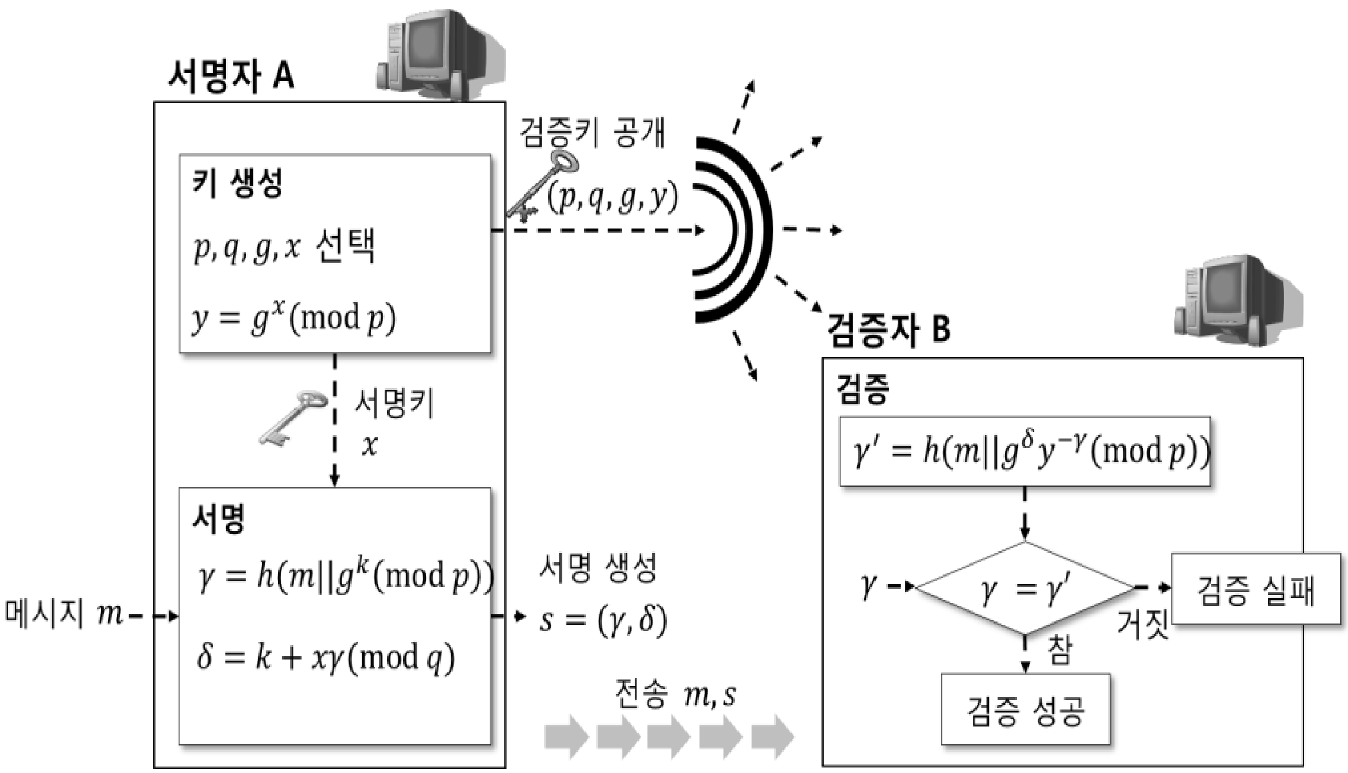
Schnorr 서명

- 서명 생성 :
  - 메시지 m과 서명키 x를 입력 받고 $1 \le k \le q-1$인 정수 k를 선택
  - $\gamma \equiv h(m||g^k \pmod p)$와 $\delta \equiv k + x\gamma \pmod q$를 계산
  - 서명 값 $s = (\gamma, \delta)$를 출력
- 서명 검증 :
  - 서명값 $s = (\gamma, \delta)$과 서명한 메시지 m, 검증키 (y, g, p, q)를 입력
  - $\gamma' \equiv h(m \parallel g^\delta y^{-\gamma} \pmod p)$계산
  - $\gamma \ =?\ \gamma'$

→ If $g^\delta y^{-\gamma} \equiv g^{k+x\gamma} g^{-x\gamma} \equiv g^{k+x\gamma-x\gamma} \equiv g^k \pmod p$, then $\gamma = \gamma'$

9.5 다양한 전자 서명 기법

- Schnorr 서명



9.5 다양한 전자 서명 기법

- Schnorr 서명
  - 키 생성
    - 소수 $p = 23, q = 11$, 생성원 $g = 7$, 비밀키 $x = 6$ 선택
    - $y = 7^6 = 4\ (mod\ 23)$ 계산
    - 서명키 $x = 6$, 검증키 $(p = 23, g = 7, y = 4)$
  - $m = 10$에 대한 서명 생성 :
    - $k = 7$ 선택, $g^k(\mathrm{mod}\, p) \equiv 7^7 \equiv 5\ (\mathrm{mod}\ 23)$
    - $\gamma = h(m||g^k(\mathrm{mod}\, p)) = h(10||5) = 6$ 라 가정.
    - $\delta \equiv (k + x\gamma) \equiv (7 + 6 \times 6) \equiv 43 \equiv 10(mod\ 11)$

    $\Rightarrow \ s = (\gamma, \delta) = (6{,}10)$
  - 서명 검증 :
    - $\gamma' = h(m||g^\delta y^{-\gamma}(mod\ p)) = h(10||7^{10}4^{-6}(mod\ 23)) = 6$
    - $\gamma = \gamma'$

9.5 다양한 전자 서명 기법

- DSA 서명
  - 1991년 NIST에 의해서 제안되었으며 1994년 12월에 미국의 전자 서명 기법 표준으로 제정
    - ElGamal 서명, Schnorr 서명, DSA는 각각 2048, 1184, 320비트
  - 키 생성 : Schnorr와 동일
  - 서명 생성 :
    - $1 \le k \le q-1$ 인 정수 k를 선택, $\gamma \equiv (g^k (\mathrm{mod}\ p))(\mathrm{mod}\ q)$와 $\delta \equiv (h(m)+x\gamma)k^{-1}(\mathrm{mod}\ q)$를 계산
    - 서명 값 $s = (\gamma, \delta)$
  - 서명 검증 :
    - $e_1 = h(m) \cdot \delta^{-1}(\mathrm{mod}\ q)$, $e_2 = \gamma\delta^{-1}(\mathrm{mod}\ q), \gamma' = (g^{e_1}y^{e_2}(\mathrm{mod}\ p))(\mathrm{mod}\ q)$
    - $\gamma = \gamma'$

$\rightarrow g^{e_1}y^{e_2} \equiv g^{h(m)\cdot\delta^{-1}} g^{x\gamma\delta^{-1}} \equiv g^{h(m)\cdot\delta^{-1}+x\gamma\delta^{-1}} \equiv g^{(h(m)+x\gamma)\delta^{-1}} \equiv g^{(h(m)+x\gamma)\left((h(m)+x\gamma)k^{-1}\right)^{-1}} \equiv g^{(h(m)+x\gamma)(h(m)+x\gamma)^{-1}k} \equiv g^k(\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$

9.5 다양한 전자 서명 기법

- DSA 서명
  - 키 생성 : Schnorr와 동일
    - 소수 $p = 23, q = 11$, 생성자 $g = 7$, 비밀키 $x = 6$ 선택
    - $y = 7^6 = 4\ (mod\ 23)$ 계산
    - *서명키* $x = 6$, *검증키* $(p = 23, g = 7, y = 4)$
  - 서명 생성 : $m = 10$
    - $k = 7$ 선택, $\gamma \equiv 7^7 \equiv \big(5\ \ (\mathrm{mod}\ 23)\big)(\mathrm{mod}\ 11) = 5$
    - $\delta \equiv (h(m) + x\gamma)\ k^{-1}\ (mod\ q) \equiv (4 + 6 \times 5)8\ (mod\ 11) \equiv 8\ (mod\ 11)$

    $\Rightarrow\ \ s = (\gamma, \delta) = (5{,}8)$
  - 서명 검증 :
    - $e_1 \equiv h(m)\delta^{-1}\ (mod\ q) = 4 \times 7(mod\ 11) = 6$
    - $e_2 \equiv \gamma\delta^{-1}(mod\ q) = 5 \times 7\ (mod\ 11) = 2$
    - $\gamma' \equiv g^{e_1}y^{e_2}(mod\ p)(mod\ q) = 7^6 4^2(mod\ 23)(mod\ 11) \equiv 5$

9.5 다양한 전자 서명 기법

- Easy for the signer
  - 키 생성 : DSA와 동일
  - 서명 생성 :
    - $1 \le k \le q$와 $1 \le d \le q$ 인 정수 k와 d를 임의로 선택
    - $\gamma \equiv (g^k (\bmod p))(\bmod q)$, $\delta \equiv (h(m) + x\gamma) \cdot d \ (\bmod q)$와 $t \equiv kd \ (\bmod q)$를 계산
    - 서명 값 $s = (\gamma, \delta, t)$
  - 서명 검증 :
    - $w \equiv t/\delta (\bmod q)$, $e_1 \equiv h(m) \cdot w \ (\bmod q)$, $e_2 \equiv \gamma w (\bmod q)$
    - $\gamma' \equiv (g^{e_1} y^{e_2} (\bmod p))(\bmod q)$
    - $\gamma \ =? \ \gamma'$

$$\rightarrow g^{e_1} y^{e_2} \equiv g^{h(m)\cdot w} g^{x\gamma w} \equiv g^{h(m)\cdot w + x\gamma w} \equiv g^{(h(m)+x\gamma)w}$$

$$\equiv g^{\frac{(h(m)+x\gamma)kd}{(h(m)+x\gamma)d}} \equiv g^k (\bmod p)(\bmod q)$$

9.5 다양한 전자 서명 기법

- Easy for the verifier
  - 키 생성 : DSA와 동일
  - 서명 생성 :
    - $1 \leq k \leq q$인 정수 k를 임의로 선택
    - $\gamma \equiv (g^k (\mathrm{mod}\, p))(\mathrm{mod}\, q)$와 $\delta \equiv k(h(m) + x\gamma)^{-1} (\mathrm{mod}\, q)$를 계산
    - 서명 값 $s = (\gamma, \delta)$
  - 서명 검증 :
    - $e_1 \equiv h(m) \cdot \delta (\mathrm{mod}\, q)$, $e_2 \equiv \gamma\delta (\mathrm{mod}\, q)$
    - $\gamma' \equiv (g^{e_1} y^{e_2} (\mathrm{mod}\, p))(\mathrm{mod}\, q)$
    - $\gamma \ =?\ \gamma'$

    → $g^{e_1} y^{e_2} \equiv g^{h(m)\cdot\delta} g^{x\gamma\delta} \equiv g^{h(m)\cdot\delta + x\gamma\delta} \equiv g^{(h(m)+x\gamma)\delta}$

    $\equiv g^{(h(m)+x\gamma)(h(m)+x\gamma)^{-1}k} \equiv g^k (\mathrm{mod}\, p)\ (\mathrm{mod}\, q)$

9.5 다양한 전자 서명 기법

- ECDSA
  - 2000년에 미국 표준으로 제정, DSA 전자 서명을 타원 곡선에 적용
  - 키 생성
    - 소수 p, 타원 곡선 E를 선택
    - 소수 q와 $1 \leq x \leq q-1$인 정수 x를 임의로 선택
    - 타원 곡선 E에서 위수가 q인 점 $A \in Z_q \times Z_q$를 선택하고, 다른 점 $B = xA$
    - (E, A, B, p, q)는 검증키, x를 서명키

9.5 다양한 전자 서명 기법

- ECDSA
  - 서명 생성 :
    - $1 \le k \le q$인 정수 k를 임의로 선택
    - 타원 곡선 E 위의 점 $P(u, v) = kA$ 계산
    - $\gamma \equiv u (\mathrm{mod}\ q)$와 $\delta \equiv (h(m) + x\gamma)k^{-1} (\mathrm{mod}\ q)$를 계산
    - 서명 값 $s = (\gamma, \delta)$
  - 서명 검증 :
    - $e_1 \equiv h(m) \cdot \delta^{-1} (\mathrm{mod}\ q)$, $e_2 \equiv \gamma\delta^{-1} (\mathrm{mod}\ q)$
    - $P'(u', v') = e_1 A + e_2 B$과 $\gamma' \equiv u' (\mathrm{mod}\ q)$계산
    - $\gamma \ =?\ \gamma'$

    → $e_1 A + e_2 B = e_1 A + e_2 x A = h(m) \cdot \delta^{-1} A + \gamma\delta^{-1} x A =$
    $(h(m) \cdot \delta^{-1} + \gamma\delta^{-1} x) A$
    $= (h(m) + \gamma x)\delta^{-1} A = (h(m) + \gamma x)(h(m) + \gamma x)^{-1} kA = kA$

9.5 다양한 전자 서명 기법

- ECDSA simulating DSA

Point on the curve

	DSA	ECDSA
Public Key Private Key	$\{y \equiv g^x (\mathrm{mod}\ p), g, p, q\}$ { d }	$\{E, A, B = xA, p, q\}$ $\{x\}$
Signing	$[\gamma, \delta] = [(g^k (\mathrm{mod}\ p))(\mathrm{mod}\ q),$ $(h(m) + x\gamma)k^{-1}(\mathrm{mod}\ q)]$	P(u,v) = kA $[\gamma, \delta]$ = [u mod q, $\delta \equiv (h(m) + x\gamma)k^{-1}(\mathrm{mod}\ q)]$
Veri.	$e_1 = h(m) \cdot \delta^{-1}(\mathrm{mod}\ q)$ $e_2 = \gamma\delta^{-1}(\mathrm{mod}\ q),$ $\gamma' = (g^{e_1} y^{e_2} (\mathrm{mod}\ p))(\mathrm{mod}\ q)$ $\gamma =? \gamma'$	$P'(u', v') = e_1 A + e_2 B$ $\gamma' \equiv u'(\mathrm{mod}\ q)$ $\gamma =? \gamma'$

9.6 전자 서명의 활용

- Time-stamped 전자 서명
  - To prevent repudiation → S(M||time)
  - Need synchronization →Use nonce (a one-time random number), i.e., S(M||nonce)
    - Nonce needs to be recorded to detect any reuse

9.6 전자 서명의 활용

- Secret Sharing
  - Split M into shares $m_1, m_2, \ldots.$
    - Each share has no information of M
    - M can be reconstructed using all shares
  - Example

    (1) Trent generates One-Time Pad R and compute S = M XOR R.

    (2) Trent --> Alice : R

    (3) Trent --> Bob : S

    (4) Bob and Alice reconstruct M = S XOR R.

9.6 전자 서명의 활용

- Secret Sharing : LaGrange Interpolating Polynomial Scheme
  - For (m, n)-threshold scheme,
    - choose p and generate a random polynomial of degree m-1.
    - Example : (3,5)-scheme and secret S= 11

    (1) Generate $F(x) = ax^2 + bx + S = 7x^2 + 8x + 11 \bmod 13$

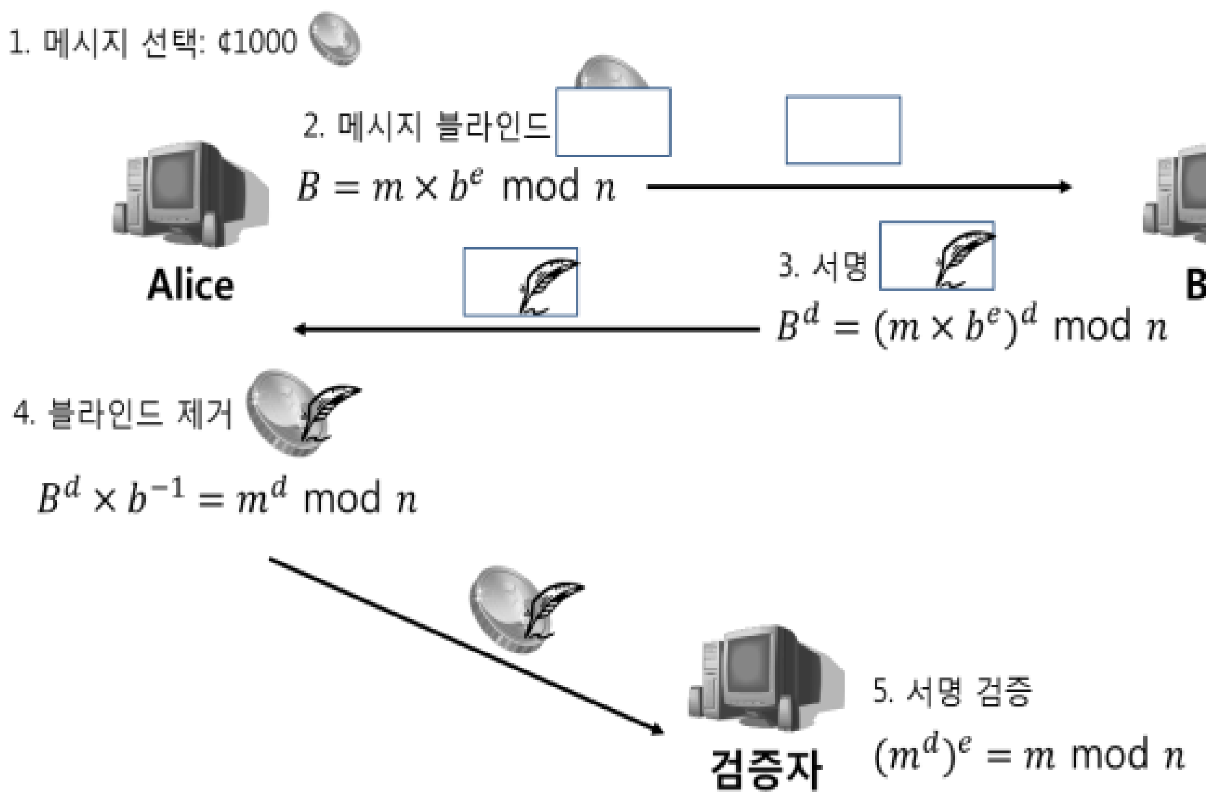
    (2) Generate the five shadows F(1) . . . F(5) and distribute them secretly.

    (3) Any three can construct S.

    $F(2) = a2^2 + b2 + S = 3 \pmod{13}$
    $F(3) = a3^2 + b3 + S = 7 \pmod{13}$
    $F(4) = a4^2 + b4 + S = 12 \pmod{13}$

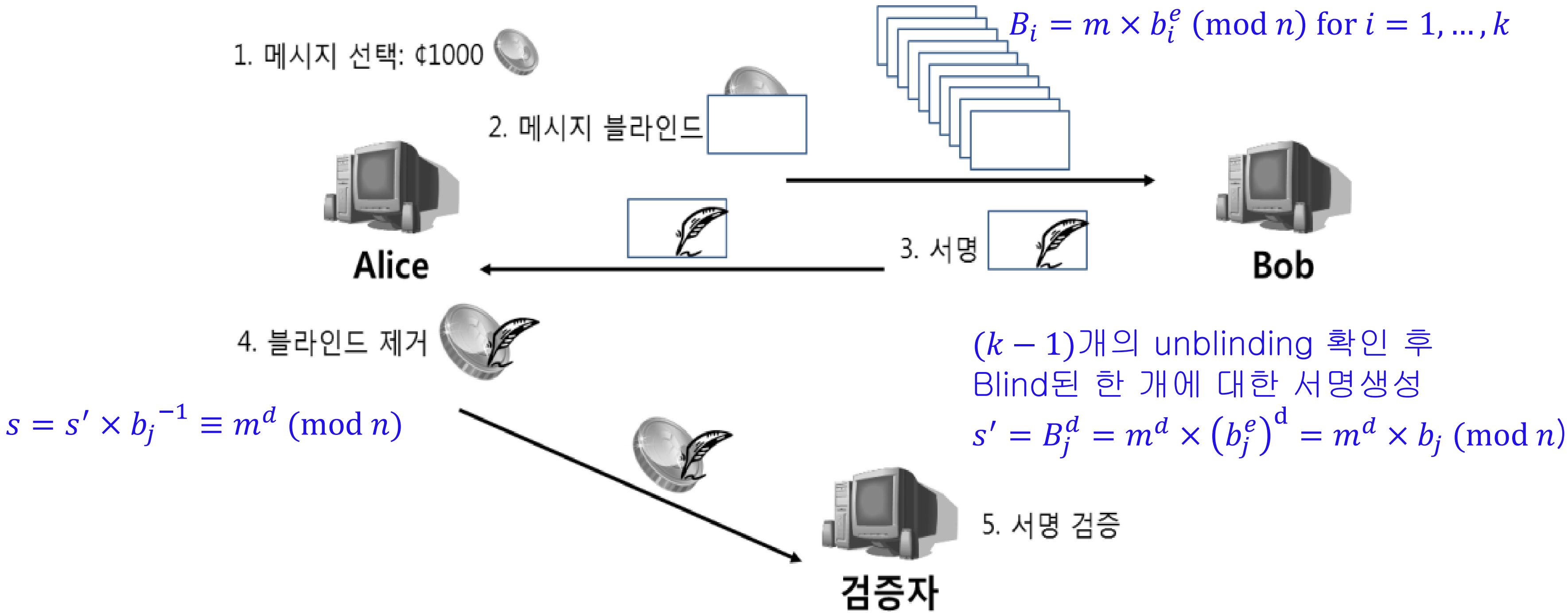
9.6 전자 서명의 활용

- 블라인드 전자 서명 (Blind Digital Signature)



9.6 전자 서명의 활용

- Self-enforced 블라인드 전자 서명



9.6 전자 서명의 활용

- Traceable 블라인드 전자 서명

$Id = P, Id' = P \oplus ID$

$f(Id \parallel G, K_0), f(Id' \parallel G, K_1)$

- *Id* 와 *Id'* 이 노출되면 *ID* 확인
- 상점(검증자) A는 *Id* 와 *Id'* 중 하나를 복호화
  - K_0 혹은 K_1 요구 : 정당한 키를 확인하기 위하여 "G" (recognizable string) 삽입
  - 동일한 화폐를 상점 B에 사용하는 경우 *Id* 와 *Id'* 중 하나를 복호화

→double spending이 탐지되지 않을 확률 50%

→동일한 ID에 대하여 다수의 secret sharing 적용

→ 탐지되지 않을 확률 $(1/n)^2$로 감소

9.6 전자 서명의 활용

■ Traceable 블라인드 전자 서명