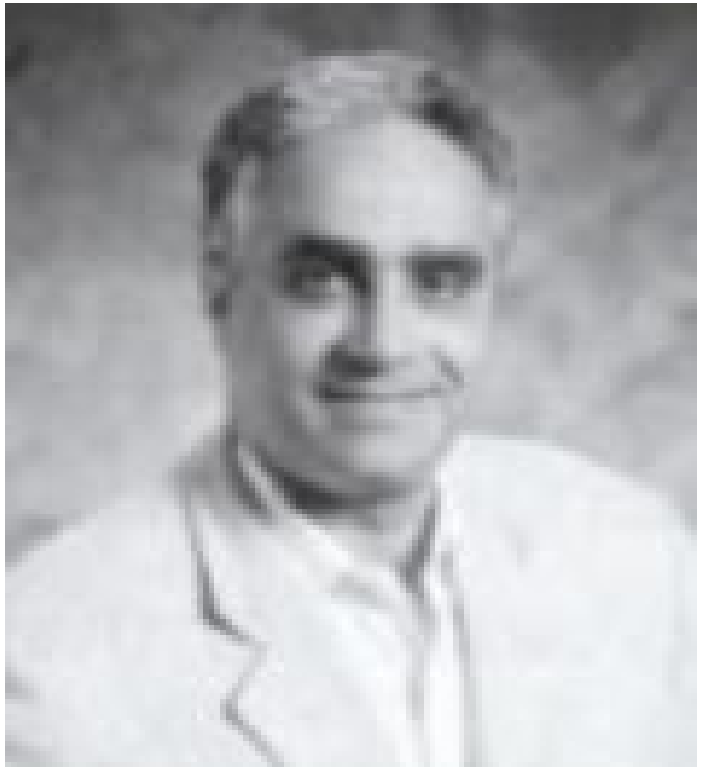
Digitálne podpisy

OBSAH

- Digital signatures
  - ElGamal
  - DSA
- Subliminal channels
- Blind signatures
- Undeniable signatures
- One – Time signatures & Timestamping

ElGamal signature scheme



- schéma digitálneho podpisu
- prvýkrát použitá egyptským kryptografom Dr. Taher El Gamalom v roku 1984

ElGamal signature scheme

- zvolíme prvočíslo p a celé čísla q, x také, že $1 \leq q \leq x \leq p$ kde q je elemet zo Z_p^*
- zrátame $y=q^x \bmod p$
- kľúč K(p,q,x,y)
  - verejná časť k = p,q,y
  - súkromná časť - x

ElGamal signature scheme

- podpísanie správy w:
  - náhodne zvolíme r; $r \in Z_{p-1}^{*}$

    hodnotu uchovávame tajnú
  - sig(w,r) = (a,b)
  - $a = q^r \bmod p$
  - $b = (w - x*a)*r^{-1} \bmod (p-1)$
- overenie podpisu: $y^a a^b \equiv q^w \bmod p$

ElGamal signature scheme - bezpečnosť

Predpokladajme, že sa Eve pokúsi sfalšovať sig (a,b) bez toho aby poznala hodnotu ***x***.

- ak si zvolí hodnotu ***a***, bude k nej musieť nájsť korešpondujúcu hodnotu ***b*** spočítaním diskrétneho logaritmu $\log_a q^w y^{-a}$ pretože platí:

  $a^b \equiv q^{r\,(w - xa)\,r^{(-1)}} \equiv q^{w - xa} \equiv q^w y^{-a}$

- ak si zvolí hodnotu ***b*** a bude chcieť nájsť hodnotu ***a*** musí vyriešiť rovnicu:

  $y^a a^b \equiv q^{xa} q^{rb} \equiv q^w \pmod p$

  Nie je známe, či má predchádzajúca rovnica efektívne riešenie pre ľubovolnú hodnotu ***a***.

ElGamal signature scheme - bezpečnosť

Ak si Eve zvolí obe hodnoty ***a***, ***b*** a bude chcieť určiť správu ***w***, musí zrátať diskrétny logaritmus $\log_q y^a a^b$.

Preto nemôže podpísať náhodnú správu týmto spôsobom.

Digital signature algorithm

- bol navrhnutý v roku 1991 americkým inštitútom NIST a v roku 1994 bol prijatý za štandard
- autor: David W. Kravitz
- algoritmus je založený na probléme výpočtu diskrétneho logaritmu
- modifikácia algoritmu ElGamal.

Návrh algoritmu

1. výber komponentov verejného kľúča:
   - p – náhodne zvolené l-bitové prvočíslo,

     $512 \leq l \leq 1024, \quad l = 64k.$
   - q – náhodne zvolené 160-bitové prvočíslo,

     tak, že p-1 mod q = 0
   - $r = h^{(p-1)/q} \bmod p$, kde h je náhodný element zo Z_p

     $r > 1$
2. výber komponentov privátneho kľúča:
   - x – náhodne zvolené celé číslo, $0 < x < q$
   - y – $r^x \bmod p$
3. Kľúč je $K = (p,q,r,x,y)$

Podpísanie správy a overenie podpisu

Podpísanie 160-bitového nešifrovaného textu w

- náhodne zvolíme $0 < k < q$ tak, aby $\gcd(k, q) = 1$
- vypočítame $a = (r^k \bmod p) \bmod q$
- vypočítame $b = k^{-1}(w + xa) \bmod q$ kde $kk^{-1} \equiv 1 \pmod q$
- podpis: $sig(w, k) = (a, b)$

Overenie podpisu (a,b)

- vypočítame $z = b^{-1} \bmod q$
- vypočítame $u_1 = wz \bmod q$, $u_2 = az \bmod q$

$ver_K(w, a, b) = true \iff (r^{u_1} y^{u_2} \bmod p) \bmod q = a$

ElGamal vs. DSA

ElGamal

- nie je bezpečnejší ako diskrétny logaritmus => nutnosť použiť veľké *p* (min. 512b)
- Podpisy príliš veľké (min 1024b) pre určité aplikácie (čipové karty)

DSA

- redukcia exponentov *r*, *y* a *a* mod *q* bez ovplyvnenia overovacej podmienky
- $y^a a^b = q^w$

DSA - použitie

- široké využitie, napríklad v
  - OpenSSL
  - OpenSSH
  - GnuPG

Subliminal channels

- proces skrývania tajnej správy do inej „nevinne“ vyzerajúcej správy.
- objavil ich v digitálnych podpisoch v roku 1984 Gustavus Simmons.
- broadband channels
- narrow-band channels

Subliminal channels - delenie

- Broadband
  "Hello, how do you do?" - môže reprezentovať tajnú správu
  1
  Dôvod??
- Narrow-band
  - Využiteľné vo všetkých schémach digitálnych podpisov
  - Ong-Schnorr-Shamir subliminal channel

Ong-Schnorr-Shamir

- Najprv sa zvolia n, k tak, že gcd(n,k) = 1
- Spočítame h = $(k^{-1})^2$ mod n
- Verejné kľúče h, n , sukromný kľúč k
- Pre poslanie správy *w'* je potrebné spočítať
  - $S_1 = \frac{1}{2} \cdot \left(\frac{w'}{w} + w \right) \bmod n$
  - $S_2 = \frac{k}{2} \cdot \left(\frac{w'}{w} - w \right) \bmod n$

gcd(w,n) = gcd(w',n) = 1

- Posiela sa **(*w*', *s*$_1$, *s*$_2$)**
- Tretia strana kontroluje, či sa platí **$w' = s_1^2 - h s_2^2 \pmod n$**
- Príjemca získa tajné *w* z nasledujúcej rovnice

$$w = \frac{w'}{\left(S_1 + k^{-1} S_2 \right)} \bmod n.$$

Ong-Schnorr-Shamir - ukážka

Dané n= 4568, k= 3465, h= 913, w´= 15 a w= 9.
Ako prvé potrebujeme spočítať w^{-1}= 3553.

Následne podpisy

$$S_1 = \frac{1}{2}\left(w'w^{-1} + w\right) \bmod n = \frac{1}{2}\left(15 \cdot 3553 + 9\right) \bmod 4568 = 3812$$

$$S_2 = \frac{k}{2}\left(w'w^{-1} - w\right) \bmod n = \frac{3465}{2}\left(15 \cdot 3553 - 9\right) \bmod 4568 = 3283$$

Verifikácia

$$w' = S_1^2 - hS_2^2 \bmod n = 3812^2 - 913 \cdot 3283^2 \bmod 4568 = 15$$

Získanie tajnej správy

$$w = \frac{w'}{S_1 + k^{-1}S_2} \bmod n = 15 \cdot (3812 + 2489 \cdot 3283)^{-1} \bmod 4568$$
$$= 15 \cdot 3655 \bmod 4568 = 9$$

Blind signatures

- David Chaum
- 2 skupiny
- Obsah správy je maskovaný (zaslepený)
- Základný predpoklad: Signer na podnet Sender-a podpíše správu ***m*** bez toho, aby sa Signer dozvedel, čo sa nachádza v správe ***m***
- Možnosť verejného overenia výsledného slepého podpisu

Blind signatures – použitie

- Anonymita správy
- Použitie v protokoloch kde záleží na súkromí
  1. e-commerce
  2. kryptografické volebné systémy
  3. Digitálne platobné systémy
- Nelinkovateľnosť – zabránenie prepojenia u Signer-a medzi maskovanou správou a nemaskovanou správou slúžiacou na overenie
- Príklad – volebná obálka

Blind signatures – použitie

- Aby bolo možné podpísať (Signer vlastní tajný podpisovací ľúč) správu ***m***, Sender vypočíta, s využitím postupu zamaskovania, ***m****, ktoré sa nedá získať z ***m*** bez znalosti tajomstva, a pošle ***m**** Signer-ovi.
- Signer podpíše ***m****, čím sa získa podpis ***sm**** (z ***m****) a pošle ***sm**** Sender-ovi. Podpisovanie sa vykonáva tak, že Sender môže potom vypočítať, s použitím postupu odmaskovania, z podpisu Signer-a ***sm**** z ***m**** - Signer-ov podpis ***sm*** z ***m***.

Blind signatures – Chaumova schéma

- Využitie RSA a vlastnosti maskovania/odmaskovania
  - B (Bob) má verejný kľúč (n,e) a súkromný kľúč $\boldsymbol{d}$
  - Nech $\boldsymbol{m}$ je správa, $0 < m < n$

1. A (Alice) vyberie náhodné $0 < k < n$ s NSD$(n,k)=1$
2. A spočíta $m^* = mk^e \pmod n$ [maskovanie správy] a pošle B
3. B spočíta $s^* = (m^*)^d \pmod n$ a pošle A [podpis maskovanej správy]
4. A spočíta $s = k^{-1}s^* \pmod n$, aby získala B podpis $\boldsymbol{m^d}$ správy $\boldsymbol{m}$ [A vykoná odmaskovanie m^*]

  - Verifikácia je ekvivalentná RSA podpisovej schéme

Blind signatures – riziká

- Podpisovanie – dešifrovanie
- Útočník pošle zašifrovanú správu, ktorú odpozoroval a chce sa dozvedieť jej obsah
  1. Odmaskovanie: $m'' = m'r^e \pmod n = (m^e \pmod n).r^e) \pmod n = (mr)^e \pmod n$ [m' je zašifrovaná správa určená na podpis]
  2. Získanie m: $s' = m''^d \pmod n = ((mr)^e \pmod n))^d \pmod n = (mr)^{ed} \pmod n = m.r \pmod n$
- Útok funguje, pretože Signer podpisuje správu priamo.
- Nemožno použiť hash funkcie na správu,
- Kľuč na podpisovanie – kľúč na dešifrovanie

Undeniable signatures

- Vlastnosti nepopierateľného podpisu:
  - podpis môže byť verifikovaný iba v kooperácii s podpisovateľom
  - podpisovateľ nemôže poprieť korektnosť podpisu
- NP pozostáva z troch komponent:
  - podpisový algoritmus
  - verifikačný algoritmus
  - a tzv. Disawoval protocol

Undeniable signatures - použitie

- Nepopierateľný podpis chráni podpisovateľa pred duplikovaním a distribuovaním dokumentov bez jeho zvolenia

- Chráni podpisovateľa pred popretím toho, čo už v minulosti podpísal

Undeniable signatures - príklady

- Entita A (zákazník) chce získať prístup k chránenej oblasti riadenej entitou B (banka). Pokiaľ A použije nepopierateľný podpis, B nemôže nikomu inému dokázať, že A použila zariadenie bez jeho účasti.

- A vytvorí zásielku, podpíše ju a pošle entite B. B nemôže poslať zásielku C bez účasti entity A vo verifikačnom procese.

Undeniable signatures – CAUSS schéma

Chaum-van Antwerpen undeniable signature scheme

- p, r sú prvočísla, $p = 2r + 1$;
- $q \in Z_p^*$ je rádu r;
- $1 \leq x \leq r - 1$, $y = q^x \mod p$;
- G je podgrupa Z_p^* rádu q s operáciou násobenia(G pozostáva z kvadratických reziduí modulo p);
- Kľúč: $K = \{p, q, x, y\}$, p, q, y sú verejné, $x \in G$ je privátne
- Podpis: $s = sig_K(w) = w^x \mod p$
- Pokiaľ $s \neq w^x \mod p$ potom Alica akceptuje s ako platný podpis s pravdepodobnosťou $\frac{1}{r}$

Undeniable signatures – Disavowal protocol

1. Alica zvolí náhodné e_1, e_2; $e_1, e_2 \in Z_r^*$
2. Alica vypočíta $c = s^{e_1} y^{e_2} \mod p$ a pošle ho Bobovi.
3. Bob vypočíta $d = c^{x^{-1} \mod r} \mod p$ a výsledok pošle Alici.
4. Alica overí, že $d \neq w^{e_1} q^{e_2} \pmod p$
5. Alica zvolí náhodné f_1, f_2; $f_1, f_2 \in Z_r^*$
6. Alica vypočíta $C = s^{f_1} y^{f_2} \mod p$ a pošle ho Bobovi.
7. Bob vypočíta $D = C^{x^{-1} \mod r} \mod p$ a výsledok pošle Alici.
8. Alica overí, že $D \neq w^{f_1} q^{f_2} \pmod p$
9. Alica označí podpis za podvrh vtedy a len vtedy ak

$$(dq^{-e_2})^{f_1} \equiv (Dq^{-f_2})^{e_1} \pmod p$$

Undeniable signatures – dôsledok

- Bob môže presvedčiť Alicu, že neplatný podpis je podvrh
  - stačí dokázať, že pokiaľ $s \neq w^x$

    potom: $(dq^{-e_2})^{f_1} \equiv (Dq^{-f_2})^{e_1} \pmod{p}$

- Bob nemôže Alicu presvedčiť, že platný podpis je podvrh (až na veľmi malú pravdepodobnosť)

One – time signature

- Autor Leslie Lamport
- Koniec '70 rokov minulého storočia
- Každý kľúč môže byť použitý iba raz!

Lamport signature

Nech **k** je kladné celé číslo a $P = \{0,1\}^k$ je množina správ.
Majme jednosmernú funkciu $f : Y \to Z$.
Platí $1 \leq i \leq k, j \in \{0,1\}$.
Osoba, ktorá podpisuje si náhodne zvolí $y_{i,j} \in Y$ a vypočíta $z_{i,j} = f(y_{i,j})$
Privatny kľúč **K**, dĺžky **2k**, sa skladá z hodnôt $y_{i,j}$ a verejný $z_{i,j}$.

Lamport signature

Nech $m = m_1 \dots m_k \in \{0,1\}^k$ je správa potom,
podpis správy je $sig(m_1 \dots m_k) = (y_{1,m_1} \dots y_{k,m_k}) = (s_1 \dots s_k)$.
Na overenie podpisu nám stačí overiť, že platí
$f(s_i) = z_{i,m_i}$ pre všetky $1 \leq i \leq k$.

Lamport signature

Problémy s digitálnymi podpismi

Lamport signature

Problémy s digitálnymi podpismi

- Ako zaručiť, že v daný deň existovala podpisaná správa a neskôr nebola zmenená?
- Strate osobného kľúča $\stackrel{?}{\Rightarrow}$ všetky správy kompromitované

Timestamping

Nech **P** je verejne známa hodnota, ktorá sa ale neda odhadnuť pred dňom podpisu a chceme podpísať správu **w** použítím hashovacej funckie **h** postupujeme nasledovne.

Timestamping

Nech **P** je verejne známa hodnota, ktorá sa ale neda odhadnuť pred dňom podpisu a chceme podpísať správu **w** použítím hashovacej funckie **h** postupujeme nasledovne.

1. $z = h(w)$

Timestamping

Nech **P** je verejne známa hodnota, ktorá sa ale neda odhadnuť pred dňom podpisu a chceme podpísať správu **w** použítím hashovacej funckie **h** postupujeme nasledovne.

1. $z = h(w)$
2. $z^{'} = h(z||P)$

Timestamping

Nech **P** je verejne známa hodnota, ktorá sa ale neda odhadnuť pred dňom podpisu a chceme podpísať správu **w** použítím hashovacej funckie **h** postupujeme nasledovne.

1. $z = h(w)$
2. $z^{'} = h(z||P)$
3. $y = sig(z^{'})$

Potom zverejníme trojicu (z, P, y) a je zrejmé, že podpis nemohol vzniknúť ani pred ani potom čo bolo **P** známe.

Ďakujeme za pozornosť