SEMINAR IZ KRIPTOGRAFIJE

Digitalni podpisi
(nadaljevanje)

Tomaž Klobučar

18. maj, 1998

Na zadnjem seminarju

- Digitalni podpisi (na splošno)
- RSA
- El Gamal, DSA
- Enkratni podpisi
- Slepi podpis

Današnji načrt

- Skupinski podpisi
- Fail-stop sheme za podpisovanje
- Podpisi brez možnosti zanikanja

Sistem za digitalno podpisovanje je peterka $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, kjer velja

1. $\mathcal{P}$ je končna množica sporočil;
2. $\mathcal{A}$ je končna množica podpisov;
3. $\mathcal{K}$ je končna množica ključev;
4. Za vsak ključ $K \in \mathcal{K}$ obstaja algoritem za podpisovanje $sig_K \in \mathcal{S}, sig_K : \mathcal{P} \to \mathcal{A}$ in algoritem za preverjanje podpisa $ver_K \in \mathcal{V}, ver_K : \mathcal{P} \times \mathcal{A} \to \{true, false\}$. Funkciji sig_K in ver_K imata to lastnost, da za vsako sporočilo $x \in \mathcal{P}$ in vsak podpis $y \in \mathcal{A}$ velja
$$ver_K(x,y) = \begin{cases} true & \text{če } y = sig_K(x) \\ false & \text{če } y \neq sig_K(x). \end{cases}$$

Skupinski podpisi

- Dokumente lahko podpisujejo le člani določene skupine.
- Kdorkoli lahko preveri, da je dokument podpisal nekdo izmed omenjene skupine, vendar ne more ugotoviti, kdo je to bil.
- V primeru spora je možno podpis odpreti in identificirati podpisnika.

Primer sheme skupinskega podpisa (shema predvideva obstoj razsodnika, kateremu vsi zaupajo):

1. Razsodnik generira $n\,m$ parov ključev, kjer je n število članov skupine.
2. Seznam vseh javnih ključev skupine je javno objavljen, vsak član skupine pa dobi m pripadajočih skritih ključev.
3. Člani skupine podpisujejo s svojimi skritimi ključi, drugi pa preverjajo podpise z javnimi ključi s seznama.
4. V primeru spora razsodnik pove, kdo ima določen skriti ključ.

Chaum, D. (1991) Group Signatures. Zbornik s konference EUROCRYPT'91.

Fail-stop podpisi

Če bi ponarejevalec z metodo grobe sile našel skriti ključ, bi lahko v večini sistemov za digitalne podpise podpis ponaredil. Fail-stop sistemi takšno možnost onemogočijo tako, da vsakemu javnemu ključu priredijo več skritih ključev, ti skriti ključi pa ne dajo istega podpisa.

Podpisov sta se prva spomnila B.Pfitzmann in M.Waidner (Eurocrypt'89).

Primer algoritma (van Heyst - Pedersen)

Generiranje ključa se razdeli med Ano in TTP. TTP izbere praštevili p in q, $q|(p-1)$ (diskretni algoritem težko izračunljiv), element $\alpha \in Z_p^*$ reda q ter skrito naključno število a_0, $1 \leq a_0 \leq q-1$, in izračuna $\beta \equiv \alpha^{a_0} \pmod{p}$.

Nato pošlje Ani (p, q, α, β). Ana izbere naključna števila $a_1, a_2, b_1, b_2 \in Z_q$, ki predstavljajo njen skriti ključ ter določi svoj javni ključ

$$(\gamma_1, \gamma_2, p, q, \alpha, \beta),$$

kjer je

$$\gamma_1 = \alpha^{a_1} \beta^{a_2} \pmod{p}$$

in

$$\gamma_2 = \alpha^{b_1} \beta^{b_2} \pmod{p}.$$

Podpisovanje in preverjanje podpisa:

- **Podpisovanje**: $y = sig_K(x) = (y_1, y_2)$, kjer je

$$y_1 \equiv a_1 + x\, b_1 \pmod{q}$$

in

$$y_2 \equiv a_2 + x\, b_2 \pmod{q}.$$

- **Preverjanje podpisa**: $y = (y_1, y_2)$,

$ver_K(x, y) = true$ natanko tedaj, ko je

$$\gamma_1 \gamma_2^x \equiv \alpha^{y_1} \beta^{y_2} \pmod{p}.$$

Opombe:

1. Natanko q^2 četverk (a'_1, a'_2, b'_1, b'_2), kjer so elementi iz Z_q, da enaki vrednosti (γ_1, γ_2) v javnem ključu (ključa z enakima γ_1 in γ_2 sta ekvivalentna).
2. Teh q^2 četverk da pri istem dokumentu x q različnih podpisov.
3. Naj bo Q_1 množica q četverk, ki da pri x isti podpis. Potem da ta množica pri drugem dokumentu q različnih podpisov.

Primer:

Naj bo $p = 29, q = 7$ in $\alpha = 16$. Izberimo $a_0 = 5$ in izračunajmo $\beta = 23$. Recimo, da je Anin skriti ključ $(2, 3, 5, 2)$. Potem je njen javni ključ $(\gamma_1, \gamma_2) = (7, 16)$. V spodnji tabeli je q^2 skritih ključev, ki dajo isti javni kjuč:

1603	2303	3003	4403	5103	6503	0203
1610	2310	3010	4410	5110	6510	0210
1624	2324	3024	4424	5124	6524	0224
1631	2331	3031	4431	5131	6531	0231
1645	2345	3045	4445	5145	6545	0245
1652	2352	3052	4452	5152	6552	0252
1666	2366	3066	4466	5166	6566	0266

S temi skritimi ključi dobimo pri podpisu sporočila $x = 1$ natanko q različnih podpisov:

(2,6)	(3,3)	(4,0)	(5,4)	(6,1)	(0,5)	(1,2)
1610	1624	1631	1645	1652	1666	1603
2303	2310	2324	2331	2345	2352	2366
3066	3003	3010	3024	3031	3045	3052
4452	4466	4403	4410	4424	4431	4445
5145	5152	5166	5103	5110	5124	5131
6531	6545	6552	6566	6503	6510	6524
0224	0231	0245	0252	0266	0203	0210

Anin podpis sporočila $x = 1$ je $(0, 5)$. Naj bo Q_1 množica skritih ključev, ki da enak podpis. Potem da ta množica pri drugem sporočilu x' q različnih podpisov:

key	x'						
	0	1	2	3	4	5	6
1666	1,6	0,5	6,4	5,3	4,2	3,1	2,0
2352	2,3	0,5	5,0	3,2	1,4	6,6	4,1
3045	3,0	0,5	4,3	1,1	5,6	2,4	6,2
4431	4,4	0,5	3,6	6,0	2,1	5,2	1,3
5124	5,1	0,5	2,2	4,6	6,3	1,0	3,4
6510	6,5	0,5	1,5	2,5	3,5	4,5	5,5
0203	0,2	0,5	0,1	0,4	0,0	0,3	0,6

Varnost sistema

Recimo, da želi nekdo ponarediti Anin podpis za sporočilo x'.

1. Če ponarejevalec pozna le skriti ključ, ki pripada javnemu, je verjenost $\frac{1}{q}$, da je njegov podpis enak Aninemu.
2. Ponarejevalec ima dostop do drugega sporočila x in Aninega podpisa (y_1, y_2). Po tretji opombi je verjetnost spet $\frac{1}{q}$.

Ana lahko z verjetnostjo $\frac{q-1}{q}$ dokaže, da je nek ponarejen podpis sporočila x res ponarejen (čeprav prestane preskus preverjanja) tako, da sama podpiše x in s pomočjo obeh podpisov izračuna skrito število a_0.

Podpisi brez možnosti zanikanja

Podpisa ni mogoče preveriti brez sodelovanja podpisnika, podpisnik pa tudi ne more zanikati, da bi že podpisani dokument res podpisal.

Shemo sestavljajo:

- generiranje ključev
- algoritem za podpisovanje
- algoritem za preverjanje podpisov
- algoritem za preprečevanje zanikanja avtorstva podpisa (*disavowal protocol*)

Primer algoritma (Chaum-van Antwerpen)

Naj bosta q in $p = 2q+1$ praštevili, $\alpha \in Z_p^*$ element reda q, $1 \leq a \leq q-1$ in $\beta \equiv \alpha^a \pmod p$. Grupa G je multiplikativna podgrupa reda q grupe Z_P^* (G sestavljajo kvadratični ostanki modulo p). Naj bo $\mathcal{P} = \mathcal{A} = G$ in

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}.$$

Števila p, α in β so javna, vrednost a pa je skrita.

Podpisovanje in preverjanje podpisa s Chaum-van Antwerpnovim algoritmom:

- **Podpisovanje** (Borut podpiše dokument $x \in G$): $y = sig_K(x) = x^a \pmod p$.
- **Preverjanje podpisa**:
  1. Ana izbere naključni števili $e_1, e_2 \in Z_q^*$. Nato izračuna $c \equiv y^{e_1}\beta^{e_2} \pmod p$ in ga pošlje Borutu.
  2. Borut izračuna $d \equiv c^{a^{-1} \bmod q} \pmod p$ in ga vrne Ani.
  3. Ana sprejme podpis kot veljaven, čee je

$$d \equiv x^{e_1}\alpha^{e_2} \pmod p.$$

Algoritem za preprečevanje zanikanja avtorstva podpisa:

1. Ana izbere naključni števili $e_1, e_2 \in Z_q^*$. Nato izračuna $c \equiv y^{e_1}\beta^{e_2} \pmod{p}$ in ga pošlje Borutu.
2. Borut izračuna $d \equiv c^{a^{-1} \bmod q} \pmod{p}$ in ga vrne Ani.
3. Ana preveri, če je
$$d \not\equiv x^{e_1}\alpha^{e_2} \pmod{p}.$$
4. Ana izbere novi naključni števili $f_1, f_2 \in Z_q^*$. Nato izračuna $C \equiv y^{f_1}\beta^{f_2} \pmod{p}$ in ga pošlje Borutu.
5. Borut izračuna $D \equiv C^{a^{-1} \bmod q} \pmod{p}$ in ga vrne Ani.
6. Ana preveri, če je
$$D \not\equiv x^{f_1}\alpha^{f_2} \pmod{p}.$$
7. Ana ugotovi, da je podpis y ponarejen, čee
$$(d\,\alpha^{-e_2})^{f_1} \equiv (D\,\alpha^{-f_2})^{e_1} \pmod{p}.$$

S protokolom za preprečevanje zanikanja avtorstva lahko Borut

- dokaže, da dokumenta s ponarejenim podpisom res ni podpisal;
- z veliko verjetnostjo ne more prepričati Ane, da bi bil njegov podpis v resnici falsifikat (verjetnost je $\frac{q-1}{q}$).

Primeri podzvrsti:

- *Convertible undeniable signature*: shema vsebuje skrito število. Do razkritja tega števila mora pri preverjanju podpisa sodelovati podpisnik. Po razkritju lahko kdorkoli preveri podpis sam (kot pri običajnem digitalnem podpisu).
- *Entrusted undeniable signature*: protokol za preprečevanje zanikanja avtorstva podpisa lahko izvede le za to določena ustanova, npr. sodišče.
- *Designated confirmer signature*: ob podpisu sami določimo, kdo bo namesto nas sodeloval pri preverjanjih podpisov. Podpis lahko še vedno naredimo le mi.

Spremenljivi podpisi brez možnosti zanikanja (*convertible undeniable signature*)

Naj bosta p in $q, q|(p-1)$ praštevili ter $\alpha \in Z_P^*$ $q-$ti koren enote. Zasebni ključ predstavljata števili x in z, javnega pa stevila p, q, α, y in u, kjer je

$$y = \alpha^x \pmod{p},$$

$$u = \alpha^z \pmod{p}.$$

Podpisovanje sporočila m

Ana izbere naključno število t, $1 \le t \le q-1$ in izračuna

$$T = \alpha^t \pmod p$$

in

$$m' = T\ t\ z\ m \pmod q.$$

Nato izbere še naključno število k in izračuna ElGamalov podpis (γ, δ) na sporočilu m':

$$\gamma = \alpha^k \pmod p,$$

$$\delta = (m' - \gamma x)\ k^{-1}.$$

Celotni podpis sestavljajo γ, δ in T.

Preverjanje podpisa

1. Borut izbere naključni števili a in b in pošlje Ani število $c = T^{Tma}\,\alpha^b \pmod{p}$.
2. Ana izbere naključno število l in pošlje Borutu

$$h_1 = c\,\alpha^l \pmod{p}$$

ter

$$h_2 = h_1^z \pmod{p}.$$

3. Borut pošlje Ani a in b.
4. Ana preveri, če je $c = T^{Tma}\,\alpha^b \pmod{p}$, ter pošlje Borutu l.
5. Borut preveri, če je $h_1 = T^{Tma}\,\alpha^{b+k} \pmod{p}$ in $h_2 = y^{\gamma a}\,\gamma^{\delta a}\,u^{b+l} \pmod{p}$.

Če Ana razkrije število z, lahko njen podpis preveri kdorkoli.