Merkle-Hellmanov sistem z nahrbtnikom

Merkle in Hellman sta leta 1978 predlagala ta sistem, že leta 1980 pa ga je razbil Shamir s pomočjo Lenstrinega algoritma za celoštevilčno programiranje (angl. integer programming).

Njegovo iterativno varianto pa je razbil malo kasneje Brickell.

Drugačen sistem z nahrbtnikom je predlagal Chor, razbil pa ga je Rivest.

Problem "podmnožica za vsoto"

Podatki: $I = (s_1, \dots, s_n, T)$, *T je* **ciljna vsota**, *naravna števila s_i pa so* **velikosti**.

Vprašanje: *Ali obstaja tak binarni vektor $\underline{x} = (x_1, \dots, x_n)$, za katerega velja $\sum_{i=1}^{n} x_i s_i = T$?*

Ta odločitveni problem je NP-poln:

– polinomski algoritem ni znan,
– isto velja tudi za ustrezen iskalni problem.

Ali za kakšno podmnožico problemov morda obstaja polinomskim algoritem?

Zaporedje $(s_1, \dots, s_n)$ je **super naraščajoče**, če velja

$$s_j > \sum_{i=1}^{j-1} s_i \qquad \text{za } 2 \leq j \leq n.$$

Če je seznam velikosti super naraščajoč, potem lahko iskalno varianto zgornjega problema rešimo v času $O(n)$, rešitev $\underline{x}$ (če obstaja) pa je enolična.

Opišimo tak algoritem:

1. **for** $i = n$ **downto** 1 **do**
2. **if** $T \geq s_i$ **then**
3. $T = T - s_i$, $x_i = 1$
4. **else** $x_i = 0$
5. **if** $T = 0$ **then** $\underline{x} = (x_1, \dots, x_n)$ je rešitev
6. **else** ni rešitve.

Naj bo $\underline{s} = (s_1, \dots, s_n)$ super naraščajoč in

$$e_{\underline{s}} : \{0,1\}^n \longrightarrow \left\{0, \dots, \sum_{i=1}^{n} s_i\right\}$$

funkcija, definirana s pravilom

$$e_{\underline{s}}(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i s_i.$$

Ali lahko to funkcijo uporabimo za enkripcijo?

Ker je $\underline{s}$ super naraščajoče zaporedje, je $e_{\underline{s}}$ injekcija, zgoraj opisani algoritem pa lahko uporabimo za dekripcijo.

Sistem **ni varen**, saj dekripcijo lahko opravi prav vsak.

Morda pa lahko transformiramo super naraščajoče zaporedje tako, da izgubi to lastnost in edino Bojan lahko opravi inverzno operacijo, da dobi super naraščajoče zaporedje.

Če napadalec Oskar ne pozna te transformacije, ima pred seboj primer (na videz) splošnega problema, ki ga mora rešiti, če hoče opraviti dekripcijo.

En tip takih transformacij se imenuje **modularna transformacija**. Izberemo si tak praštevilski modul p, da je

$$p > \sum_{i=1}^{n} s_i$$

ter število a, $1 \leq a \leq p-1$. Naj bo

$$t_i = \ a s_i \bmod p, \qquad \text{za } 1 \leq i \leq n.$$

Seznam $\underline{t} = (t_1, \dots, t_n)$ je javni ključ, ki ga uporabimo za enkripcijo, vrednosti a in p, ki definirata modularno transformacijo, pa sta tajni.

Zakaj smo si izbrali za p praštevilo?

Zakaj je bil ta sistem sploh zanimiv?

Primer: Naj bo

$$s = (2, 5, 9, 21, 45, 103, 215, 450, 946)$$

tajni super naraščajoči seznam velikosti.

Za $p = 2003$ in $a = 1289$ dobimo javni seznam velikosti

$$\underline{t} = (575, 436, 1586, 1030, 1921, 569, 721, 1183, 1570).$$

Anita zašifrira sporočilo $\underline{x} = (1, 0, 1, 1, 0, 0, 1, 1, 1)$:

$$y = 575 + 1586 + 1030 + 721 + 1183 + 1570 = 6665$$

ter ga pošlje Bojanu, ki najprej izračuna $z = a^{-1} y \bmod p = 1643$ in nato reši problem podmnožice zaporedja $\underline{s}$ za vsoto z.

6. poglavje

Sheme za digitalne podpise

- uvod (podpis z RSA sistemom)
- ElGamalov sistem za digitalno podpisovanje
- Digital Signature Standard
- napadi
- enkratni podpis
- podpisi brez možnosti zanikanja
- Fail-stop podpisi

Digitalni podpis je nadomestek za lastnoročni podpis pri elektronski izmenjavi in digitalnemu hranjeju podatkov.

Konceptualno se način zapisovanja informacij ni dramatično spremenil.

Medtem ko smo prej shranjevali in prenašali informacije na papirju, jih sedaj hranimo na magnetnih in drugih medijih ter jih prenašamo preko telekomunikacijskih sistemov (tudi brezžičnih).

Bistveno pa se je spremenila možnost kopiranja in spreminjanja informacij.

Zlahka naredimo na tisoče kopij neke informacije, ki je shranjena digitalno, pri tem pa se nobena ne razlikuje od originala.

Z informacijo na papirju je to precej težje.

Družba, v kateri so informacije spravljene in prenašane v digitalni obliki, mora poskrbeti za to, da ne bo varnost informacij odvisna od fizičnega medija, ki jih je zapisal ali prenesel.

Varnost informacij mora temeljiti izključno na digitalni informaciji.

Eno izmed osrednjih orodij pri zaščiti informacij je **podpis**. Le-ta preprečuje poneverjanje, je dokaz o izvoru, identifikaciji, pričanju.

Podpis naj bi bil unikat vsakega posameznika, z njim se predstavimo, potrdimo, pooblastimo.

Z razvojem digitalne informacije moramo ponovno obdelati tudi koncept podpisa.

Ni več unikat, ki enolično določa podpisnika, kajti elektronsko kopiranje podpisa je tako lahko, da je skoraj trivialno na nepodpisan dokument pripeti poljuben podpis.

Potrebujemo protokole, ki imajo podobne lastnosti kot trenutni "papirni protokoli".

Družba ima enkratno priložnost, da vpelje nove in učinkovitejše načine, ki nam bodo zagotovili varnost informacij.

Veliko se lahko naučimo iz dosedanjih sistemov, obenem pa moramo odpraviti tudi številne pomanjkljivosti.

Primerjava digitalnega in navadnega (lastnoročnega) podpisa:

- navadni podpis je fizično del podpisanega dokumenta;
- navadni podpis preverjamo s primerjanjem, digitalnega z algoritmom, katerega rezultat je odvisen od ključa in dokumenta;
- kopija digitalnega podpisa je identična originalu;
- digitalni podpis je odvisen od dokumenta, ki ga podpisujemo.

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

1. $\mathcal{P}$ je končna množica sporočil,
2. $\mathcal{A}$ je končna množica podpisov,
3. $\mathcal{K}$ je končna množica ključev,
4. $\forall$ ključ $K \in \mathcal{K}$ obstaja algoritem za podpisovanje
$$\mathrm{sig}_K \in \mathcal{S}, \quad \mathrm{sig}_K : \mathcal{P} \to \mathcal{A}$$
in algoritem za preverjanje podpisa
$$\mathrm{ver}_K \in \mathcal{V}, \quad \mathrm{ver}_K : \mathcal{P} \times \mathcal{A} \to \{\mathrm{true}, \mathrm{false}\}.$$

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

$$\mathrm{ver}_K(x, y) = \begin{cases} \mathrm{true}, & \text{če } y = \mathrm{sig}_K(x) \\ \mathrm{false}, & \text{če } y \neq \mathrm{sig}_K(x) \end{cases}$$

Zahteve:

- algoritma sig_K in ver_K imata polinomsko časovno zahtevnost
- sig_K je znan le podpisniku
- ver_K je splošno znan
- računsko mora biti nemogoče ponarediti podpis

Primer: Algoritem RSA lahko uporabimo tudi za podpisovanje. Naj bo $n = pq$, kjer sta p in q praštevili.

Če je (n, d) skriti ključ, (n, e) pa javni, pri čemer je $de \equiv 1 \pmod{\varphi(n)}$, potem definiramo:

$$\mathrm{sig}_K(x) = d_K(x) = x^d \bmod n$$

$$\mathrm{ver}_K(x, y) = \text{true} \iff x = e_K(y) = y^e \bmod n$$

za $x, y \in \mathbb{Z}_n$.

Z zgornjim algoritmom je mogoče ponarediti podpis naključnih sporočil.

Ponarejevalec najprej izbere podpis y in nato izračuna

$$x \equiv y^e \pmod{n}.$$

Možnosti takega ponarejanja se izognemo z

- enosmernimi zgoščevalnimi funkcijami ali
- zahtevo, da ima sporočilo x določen pomen.

Pošiljanje podpisanih tajnih sporočil

Vrstni red šifriranja in digitalnega podpisovanja je pomemben.

1. Najprej podpisovanje:
$$x, \mathrm{sig}_{\mathrm{Anita}}(x) \rightarrow e_{\mathrm{Bojan}}((x, \mathrm{sig}_{\mathrm{Anita}}(x))).$$
2. Najprej šifriranje $z = e_{\mathrm{Bojan}}(x)$,
   potem podpis $y = \mathrm{sig}_{\mathrm{Anita}}(z)$:
   Bojan prejme (z, y), odšifrira tajnopis
   $x = d_{\mathrm{Bojan}}(z)$ ter preveri podpis $\mathrm{ver}_{\mathrm{Anita}}(z, y)$.

V drugem primeru lahko napadalec Cene zamenja Anitin podpis s svojim:

$$y' = \mathrm{sig}_{\mathrm{Cene}}(z) \rightarrow (z, y') \rightarrow x = d_{\mathrm{Bojan}}(z),$$
$$\mathrm{ver}_{\mathrm{Cene}}(z, y')$$

in Bojan bo mislil, da je sporočilo prišlo od Ceneta.

Zato se priporoča najprej podpisovanje in nato šifriranje.

V primeru algoritma RSA je potrebno pri zaporednem podpisovanju in šifriranju paziti na velikosti modulov (*reblocking problem*).

Če je $n_{\mathrm{Anita}} > n_{\mathrm{Bojan}}$, se lahko zgodi, da Bojan ne bo mogel razvozlati sporočila. Naj bo

$$(n_{\mathrm{Anita}}, e_{\mathrm{Anita}}, d_{\mathrm{Anita}}) = (62894113, 5, 37726937),$$
$$(n_{\mathrm{Bojan}}, e_{\mathrm{Bojan}}, d_{\mathrm{Bojan}}) = (55465219, 5, 44360237).$$

Anita podpiše sporočilo $x = 1368797$ in podpis zašifrira:

1. $s = x^{d_{\mathrm{Anita}}} \bmod n_{\mathrm{Anita}} = 59847900$,
2. $y = s^{e_{\mathrm{Bojan}}} \bmod n_{\mathrm{Bojan}} = 38842235$.

Bojan izračuna

1. $\widehat{s} = y^{d_{\mathrm{Bojan}}} \bmod n_{\mathrm{Bojan}} = 4382681$,
2. $\widehat{x} = \widehat{s}^{e_{\mathrm{Anita}}} \bmod n_{\mathrm{Anita}} = 54383568$.

Ker je $s > n_{\mathrm{Bojan}}$, je $\widehat{x} \neq x = 1368797$.

Verjetnost tega dogodka je

$$\frac{n_{\mathrm{Anita}} - n_{\mathrm{Bojan}}}{n_{\mathrm{Anita}}}.$$

Delitev shem za digitalno podpisovanje

1. Podpis je dodatek (ElGamal, DSA) sporočilu - sporočilo je možno rekonstruirati iz podpisa (RSA),
2. deterministični - nedeterministični,
3. enkratni - večkratni.

Različni sistemi za digitalno podpisovanje

- RSA
- ElGamal, DSS (*Digital Signature Standard*)
- Enkratni podpisi (*one-time signatures*)
- Slepi podpisi (*blind signatures*)
- Podpisi brez možnosti zanikanja (*undeniable signatures*)
- Skupinski podpisi (*group signatures*)
- Fail-Stop podpisi

ElGamalov sistem za digitalno podpisovanje

Za razliko od algoritma RSA je ElGamalov sistem namenjen predvsem digitalnemu podpisovanju, čeprav se ga da v posebnih primerih uporabiti tudi za šifriranje.

Podpis je nedeterminističen (odvisen od naključnega števila), torej sploh ni natanko določen.

Algoritem

Naj bo p takšno praštevilo, da je v $\mathbb{Z}_p$ težko izračunati diskretni logaritem in $\alpha \in \mathbb{Z}_p^*$ primitivni element.

Naj bo še $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$ in

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

Število a je skrito (zasebno),

števila p, α in β pa so javno znana.

Podpisovanje: podpisnik s ključem $K = (p, \alpha, a, \beta)$ izbere naključno skrito število $k \in \mathbb{Z}_{p-1}^*$ in določi

$$\mathrm{sig}_K(x, k) = (\gamma, \delta),$$

kjer je

$$\gamma \equiv \alpha^k \bmod p$$

in

$$\delta \equiv (x - a\gamma)k^{-1} \bmod (p-1).$$

Preverjanje podpisa: (samo z javnimi p, α in β)

$$\mathrm{ver}_K(x, \gamma, \delta) = \mathrm{true} \iff \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}.$$

Primer: Naj bo $p = 467, \alpha = 2$ in $a = 127$. Potem je $\beta \equiv \alpha^a \bmod p = 132$. Recimo, da želimo podpisati $x = 100$, izbrali pa smo si tudi $k = 213$. Podpis je enak (γ, δ), kjer je

$$\gamma \equiv 2^{213} \bmod 467 = 29$$

in

$$\delta \equiv (100 - 127 \cdot 29)\ 431 \bmod 466 = 51.$$

Pri preverjanju izračunamo

$$132^{29}\ 29^{51} \equiv 189 \bmod 467 \quad \text{in}$$

$$2^{100} \equiv 189 \bmod 467.$$

Zadnji vrednosti se ujemata, zato je podpis pravi.

Varnost ElGamalovega sistema za podpisovanje

Kako bi lahko ponaredili podpis, ne da bi vedeli za vrednost skritega števila a?

1. Za dano sporočilo x je potrebno najti tak par (γ, δ), da bo veljalo $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$, torej
   - če izberemo γ: rabimo $\delta = \log_\gamma \alpha^x \beta^{-\gamma} \pmod{p}$,
   - če izberemo δ: glede na γ je potrebno rešiti enačbo $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$,
   - hkrati računamo γ in δ (zaenkrat ni še nihče odkril hitrega postopka za reševanje zgornje enačbe).

2. Za podpis (γ, δ) je potrebno najti ustrezno sporočilo x:
$$x = \log_\alpha \beta^\gamma \gamma^\delta \pmod{p}.$$

3. Hkratno računanje x, γ in δ: naj bosta i in j takšni števili, da velja $0 \leq i, j \leq p-2$ in $D(j, p-1) = 1$. Potem števila
$$\begin{aligned} \gamma &\equiv \alpha^i \beta^j \pmod{p}, \\ \delta &\equiv -\gamma j^{-1} \pmod{(p-1)}, \\ x &\equiv -\gamma i j^{-1} \pmod{(p-1)} \end{aligned}$$
zadoščajo enačbi $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$.

Primer: Če je $p = 467, \alpha = 2$ in $\beta = 132$, lahko z izbiro $i = 99$ in $j = 179$, dobimo veljaven podpis $(117, 41)$ za sporočilo 331.

4. Ali lahko pri veljavnem podpisu (γ, δ) za x najdemo še kakšen podpis za neko drugo sporočilo x'? Odgovor je "DA".

   Naj bodo h, i in j takšna števila, da zanje velja $0 \leq h, i, j \leq p-2$ in $D(h\gamma - j\delta, p-1) = 1$. Potem je par (λ, μ) veljaven podpis za x', kjer je
$$\begin{aligned} \lambda &= \gamma^h \alpha^i \beta^j \bmod p, \\ \mu &= \delta\lambda(h\gamma - j\delta)^{-1} \bmod (p-1), \\ x' &= \lambda(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod (p-1). \end{aligned}$$