Aplicacions (II)

lunes, 9 de noviembre de 2020 11:08

Criptosistema d'Elgamal

Triem un cos finit $\mathbb{F}_q$ amb $q >> 0$; $g \in \mathbb{F}_q^*$ t.q. $\mathbb{F}_q^* = \langle g \rangle$

Identifiquem cada missatge natural amb un element de $\mathbb{F}_q^*$

Xifrar missatges: transformar $m \in \mathbb{F}_q^*$ en $\tilde{m} \in \mathbb{F}_q^*$

de forma que

- m es pugui recuperar a partir de $\tilde{m}$
- però només si se sap una clau secreta
- el xifrat ($m \to \tilde{m}$) i el desxifrat ($\tilde{m} \to m$) han de ser eficients

Cada usuari A_i tria una clau secreta $xs_i \in \{1, \dots, q-1\}$ (catxa preferentment a l'atzar), i fa pública

$$xp_i = g^{xs_i}$$

Si algú li vol enviar el missatge m a aquest usuari tria $x \in \{1, \dots, q-1\}$ a l'atzar i li envia el parell

$$\tilde{m} = (g^x, g^{xs_i \cdot x} m)$$

$(g^{k_{s_i}})^{k}$ → tothom ho pot calcular (encara que no sàpiga k_{s_i})

L'usuari A_i pot desxifrar el missatge

$$m = \frac{g^{k_{s_i} k} \cdot m}{(g^k)^{k_{s_i}}}$$

A_i no sap k però sap k_{s_i}

Un espia no pot desxifrar el missatge si no sap $(g^k)^{k_{s_i}}$ encara que sàpiga $g^{k_{s_i}}$: hauria de trobar

$$k = \log_g (g^k) = \log_{g^{k_{s_i}}} (g^{k \cdot k_{s_i}})$$

log. discret

La seguretat del criptosistema d'ElGamal es basa en la dificultat computacional del "problema del logaritme discret" en $\mathbb{F}_q^*$ $q >> 0$

De fet, la seguretat d'aquest criptosistema es pot reduir a la del protocol de Diffie-Hellman

Codis correctors d'errors

Suposarem que tenim un conjunt finit de missatges (per exemple, paraules de 8 lletres)

$256 = 2^8$ lletres possibles (codi ASCII)

$(2^8)^8 = 2^{64}$ missatges possibles

Identifiquem cada paraula amb un element de $\mathbb{F}_{2^{64}}$

Triem $n > 0$ i ens l'espai vectorial $\mathbb{F}_2^n$ triem un subespai V de dimensió 64, de forma que $\#V = 2^{64}$

Triem una base de V tal que

$$\mathbb{F}_{2^{64}} \xrightarrow{\sim} V$$

Pensarem els missatges com elements de V

Trobem equacions de V

$V = \{\text{sols. d'un sist. lineal homogeni}\}$

Els missatges originals seran elements de V

Determinem si $x \in \mathbb{F}_2^n$ és un missatge original o no?

és mirar si x satisfà les equacions de V

Exemple: $\mathbb{F}_{2^3}$ primera prueba

Exemple En $\mathbb{F}_{2^6}^3$ podríem prendre

$$V=\{(x,y,z)\in\mathbb{F}_{2^6}^3 : x-y=z\}=\{(w,w,w): w\in\mathbb{F}_{2^6}\}$$

En aquest cas codifiquem un missatge repetint-lo tres cops. Aquesta codificació és "bastant" segura però és cara

n = longitud del codi

k = dimensió del codi

k/n = ratio del codi ← interessa que això sigui petit

Pes de Hamming

$$w:\mathbb{F}_2^n \longrightarrow \mathbb{N}$$

$$v=(a_1,\dots,a_n) \qquad w(v)=\#\{i : a_i\neq 0\}$$

$d(V)=\min\{w(v): v\in V\setminus\{0\}\}$ distància mínima en V

Si s'ha enviat un missatge w, però hem rebut $r\notin V$ convé r per $c\in V$ tq $w(r-c)$ mínima

si $w(r-w)\leq d(V)/2$ (i té com a molt $d(V)/2$ (t incorrectes)

si $w(r-m) \leq d-1/2$ (r conté a molt $d-1/2$ bits incorrectes)

llavors ha de ser $c=m$, i per tant, hem pogut corregir els errors de transmissió

Esquema per compartir secrets de Shamir

Volem compartir un secret $s \in \mathbb{F}_p$ entre n persones de forma que calguin al menys t persones per reconstruir-lo.

Triem $p \gg n$

Construim a l'atzar $H(x) \in \mathbb{F}_p[x]$ tq

- $\deg H(x) \leq t-1$
- $H(0) = s$

Triem $x_1, \ldots, x_n \in \mathbb{F}_p$ a l'atzar i calculem $s_i = H(x_i)$

A cada participant li enviem un parell (x_i, s_i)

Recuperar $s \longleftrightarrow$ trobar $H(x) \longleftrightarrow$ interpolar els pts $\{(x_i, s_i)\}_i$

$\deg H \leq t-1$

necessitem

depth ≤ t-1

necessary

t- doesn't