Criptografie - SEMINARUL NR 5 — 28 mai 2019

Partajarea secretelor

$1, 2, \ldots, n$

structură de acces $\mathcal{A} \subseteq \mathcal{P}(\{1,2,\ldots,n\})$

Exemplul 1 $n = 4$

grupuri autorizate ← $\mathcal{A} = \{\{1,2\},\{3,4\},\{1,2,4\},\{1,2,3\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$

grupuri neautorizate ← $\bar{\mathcal{A}} = \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$

$|\mathcal{A} \cup \bar{\mathcal{A}}| = 2^n$

$\mathcal{A}_{min} = \{\{1,2\},\{3,4\}\}$ $\quad \bar{\mathcal{A}}_{max} = \{\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$

grupuri minimale care pot reface construcția (secretul)

grupuri maximale care nu pot reface cont.

Structuri ponderate

$1, 2, \ldots, n$

$\downarrow \quad \downarrow \quad\quad \downarrow$

$w_1 \quad w_2 \quad\quad w_n \in \mathbb{N}^*$

K prag $\quad \mathcal{A} = \{A \subseteq \{1,2,\ldots,n\} \mid \sum_{i \in A} w_i \geq K\}$

Exerciții

(3p) ① Demonstrați că structura de acces de la exemplul precedent (1) nu este ponderată (R.A.)

(4p) ② Dați un exemplu de schemă de partajare pentru structura de la ex (1)
(Cum se împarte S în $\{i_1, i_2, i_3\}$ a.î. $i_1, i_2 \to S$ și $i_1, i_3 \not\to S$)

(3p) ③ P.p. că $\{1,2,\ldots,n\}$ e partiționată în compartimente $\{C_1, C_2, \ldots, C_m\}$. $\exists K$ global
a.î. $K \geq \sum_{i=1}^{m} K_i$, $\quad \mathcal{A} = \{A \subseteq \{1,2,\ldots,n\} \mid |A| \geq K$ și K_i ... $\}$ $\quad$ (↓ $K_1, K_2, \ldots K_m$)

Schema de partajare:

Caz I $K = \sum k_j$ (1p)

Caz II $K > \sum k_j$ (2p)

Rezolvare

① Pp. RA. o structura de acces este ponderată.

fie $1 \rightsquigarrow w_1$, K prag $\in \mathbb{N}$

$2 \rightsquigarrow w_2$

$3 \rightsquigarrow w_3 \in \mathbb{N}^*$

$4 \rightsquigarrow w_4$

$\Rightarrow \forall A \subseteq \mathcal{U}, \sum_{i \in A} w_i \geq K$

$\nexists A \subseteq \bar{A}, \sum_{i \in A} w_i < K$

$\{1,2\} \subseteq A \Rightarrow w_1 + w_2 \geq K$

$\{3,4\} \subseteq A \Rightarrow w_3 + w_4 \geq K$

$\{1,3\} \subseteq \bar{A} \Rightarrow w_1 + w_3 < K$

$\{1,4\} \subseteq \bar{A} \Rightarrow w_1 + w_4 < K$

$\{2,3\} \subseteq \bar{A} \Rightarrow w_2 + w_3 < K$

$\{2,4\} \subseteq \bar{A} \Rightarrow w_2 + w_4 < K$

$\Rightarrow$
$w_1 + w_2 \geq K$
$-w_1 + w_3 > -K$ (+)
$w_2 - w_3 > 0$

$\Rightarrow$
$w_3 + w_4 \geq K$
$-w_2 - w_4 > -K$ (+)
$w_3 - w_2 > 0$

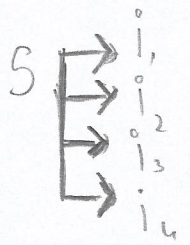
Avem deci că $w_2 - w_3 > 0$

$w_3 - w_2 > 0$ (+)

$0 > 0$ Fals

$\rightarrow$ Pp. făcută e falsă $\rightarrow$ structura nu este ponderată

②



$\mathcal{A}_{min} = \{\{1,2\}, \{3,4\}\}$

$\mathcal{A}_{max} = \{\{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}\}$

$S =$

$i_1 =$ $i_2 = 2$ $i_3 = 0$ $i_4 = 0$

$B =$ $A \subseteq \{1,2,3,4\}$

$\prod_{i \in A} i \bmod 4 = 1 = S$

i_1, i_2 $1 \cdot 1 = 1$

i_3, i_4 $i_3 \cdot i_4 \bmod 4 = 1$

i_1, i_3 i_2, i_4 i_2, i_3 i_1, i_4 $1 \cdot 3 = 3 \neq 1$

$S = 3$

$i_1 = 1$ $i_2 =$ $i_3 =$ $i_4 = 2$

$S =$

$i_1 = 1$ $i_2 = 2$ $i_3 = 3$ $i_4 = 2$

$S = 1$

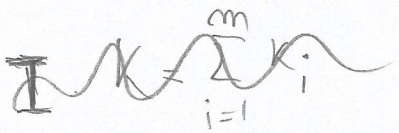
$i_1 = 1$ $i_2 = 1$ $i_3 = 3$ $i_4 = 3$

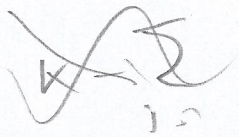
?

$\prod_{i \in A} i \bmod 4$ && $|A| > 1$

(3) $C_1, C_2, \dots C_m \Rightarrow \{1,2,\dots m\}$ — m participanți

$\downarrow K_1 \quad \downarrow K_2 \quad \downarrow K_m$





$S \equiv$

Se generează m polinoame random P_i de grad K_i

$P_i(x) = \sum_{j=0}^{K_i} a_j x_j$, cu $a_0 = S_i$, $i_\ell \in C_i$

$i_\ell = P_i(R_\ell)$ - generarea ca la Shamir pentru componenta

$S = \sum_{i=1}^{m} S_i \bmod m$

reconstrucția se face cu Shamir

Se generează un alt polinom P_{m+1} de grad

$S = \sum_{i=1}^{m+1} S_i \bmod m$

$i_\ell = (P_i(\ell), P_{m+1}(\ell))$

unde $i_\ell \in C_i$

PH reconstrucția lui S se va da S_{m+1}

(4)