Seminar 9 - 24.04.2024

Ex#1 Arătați că polinomul x^3+x^2+1 este ireductibil peste $\mathbb{F}_2$. Fie ω o rădăcină a polinomului. Calculați elementul $(\omega^2+\omega+1)^{-1}$ în $\mathbb{F}_8=\mathbb{F}_2[\omega]$.

Deci

Dacă nu ar fi, atunci ar trebui să putea avea un factor de grad 1 și un factor de grad 2.

Dacă notăm $P(x)=x^3+x^2+1$, observăm că

$$P(0)=0+0+1 \Rightarrow P(0)=1$$
$$P(1)=1+1+1 \to P(1)=1.$$

Așadar, P nu are factori de grad 1 (singurele polinoame de grad 1 sunt x și $x+1$ care, în $\mathbb{F}_2$, au rădăcinile 0 și, respectiv, 1), deci P este ireductibil.

Fie, acum, ω o rădăcină a lui P. Regula de calcul din $\mathbb{F}_8=\mathbb{F}_2[\omega]$ este

$$\omega^3=\omega^2+1$$

iar elementele lui $\mathbb{F}_8$ sunt de forma $\alpha+\beta\omega+\gamma\omega^2$ cu $\alpha,\beta,\gamma\in\mathbb{F}_2$. Căutăm un astfel de element care să satisfacă

$$(1+\omega+\omega^2)(\alpha+\beta\omega+\gamma\omega^2)=1.$$

Calculăm

$$(1+\omega+\omega^2)(\alpha+\beta\omega+\gamma\omega^2)=1 \iff$$
$$\alpha+\beta\omega+\gamma\omega^2+\alpha\omega+\beta\omega^2+\gamma\omega^3+\alpha\omega^2+\beta\omega^3+\gamma\omega^4=1$$

Observăm că dacă $\omega^3=\omega^2+1$, atunci

$$\omega^4=\omega^3+\omega=\omega^2+1+\omega \to \omega^4=1+\omega+\omega^2$$

Continuăm calculele și avem

$$\alpha+(\alpha+\beta)\omega+(\alpha+\beta+\gamma)\omega^2+(\beta+\gamma)\omega^3+\gamma\omega^4=1 \iff$$
$$\alpha+(\alpha+\beta)\omega+(\alpha+\beta+\gamma)\omega^2+(\beta+\gamma)(\omega^2+1)+\gamma(1+\omega+\omega^2)=1 \iff$$
$$(\alpha+\beta+\gamma+\gamma)+(\alpha+\beta+\gamma)\omega+(\alpha+\beta+\gamma+\beta+\gamma+\gamma)\omega^2=1 \iff$$
$$(\alpha+\beta)+(\alpha+\beta+\gamma)\omega+(\alpha+\gamma)\omega^2=1$$

$$\begin{cases}\alpha+\beta=1\\ \alpha+\beta+\gamma=0\\ \alpha+\gamma=0\end{cases}$$

Dar ultima egalitate avem $\alpha = 8$. Înlocuim în a doua și găsim $\beta = 0$ și dacă mergem cu β în prima, găsim $\alpha = 1$. Așadar $(\alpha, \beta, \gamma^2) = (1, 0, 1)$. Cu alte cuvinte,

$$(1+\omega+\omega^2)^{-1} = 1 + \omega^2$$

Dacă facem verificarea, avem

$$\begin{aligned}(1+\omega+\omega^2)(1+\omega^2) &= 1+\omega+\omega^2+\omega^2+\omega^3+\omega^4 = \\ &= 1+\omega+\omega^3+\omega^4 = \\ &= 1+\omega+\omega^2+1+1+\omega+\omega^2 = \\ &= 1.\end{aligned}$$

□

Ex#2 Găsiți o valoare pentru expresia $\sqrt[7]{23} \bmod 77$.

Deci

Teorema lui Euler

Dacă a și n sunt prime între ele, atunci

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

OBS Dacă n este prim avem Mica teoremă a lui Fermat

Să observăm că $23 \in \mathbb{Z}_{77}^*$ și $\gcd(77, 23) = 1$.

Știm că $\#\mathbb{Z}_{77}^* = \varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$.

Calculăm $\sqrt[7]{23} \bmod 77$ astfel

$$\sqrt[7]{23} \bmod 77 = 23^{\frac{1}{7}} \bmod 77 = 23^{(7^{-1} \bmod \varphi(77))} \bmod 77 = 23^{(7^{-1} \bmod 60)} \bmod 77.$$

Folosind algoritmul lui Euclid, calculăm $7^{-1} \bmod 60$:

$$\left.\begin{aligned} 60 &= 7 \cdot 8 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}\right\} = 7$$

$$\begin{aligned}\Rightarrow 1 &= 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = \\ &= (60 - 7 \cdot 8) \cdot 2 - 7 = \\ &= 60 \cdot 2 - 7 \cdot 17.\end{aligned}$$

Modulo 60 avem $1 = -7 \cdot 17 \pmod{60}$

Adică avem $7 \cdot (-17) = 1 \pmod{60}$

$7 \cdot 43 = 1 \pmod{60}$

$7^{-1} = 43 \pmod{60}$

Prin urmare $\sqrt[7]{23} = 23^{43} \bmod 77$.

Observăm că $43 = 1+2+8+32$. Aplicăm algoritmul de exponențiere rapidă și avem

$23^1 = 23 \pmod{77}$

$23^2 = -10 \pmod{77}$

$23^4 = 23 \pmod{77}$

$23^8 = -10 \pmod{77}$

$23^{16} = 23 \pmod{77}$

$23^{32} = -10 \pmod{77}$.

Așadar $23^{43} = 23^1 \cdot 23^2 \cdot 23^8 \cdot 23^{32} =$

$= 23 \cdot (-10) \cdot (-10) \cdot (-10) =$

$= 23 \cdot 23 \cdot (-10) =$

$= (-10) \cdot (-10) =$

$= 23 \pmod{77}$

Într-o concluzie $\sqrt[7]{23} \bmod 77 = 23 \bmod 77$.

□

EX#3 Examenul restanței 25 mai 2022

Secure Multiparty Computation peste $\mathbb{Z}$. Valoarea secretă a lui Alice este $x_1 = 1$, valoarea secretă a lui Bob este $x_2 = 2$ și valoarea secretă a lui Cezar este $x_3 = 3$. Ei vor să calculeze împreună cantitatea $x_1 x_2 + x_3$ fără a-și dezvălui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajările inițiale, Alice folosește $4X+1$, Bob folosește $5X+2$, iar Cezar folosește $6X+3$. Pentru a partaja înmulțirile locale, Alice folosește $X+a$, Bob folosește $2X+b$, iar Cezar folosește $3X+c$. Efectuați protocolul pas cu pas.

Dem
ow

Vrem $x_1x_2+x_3$ fără a face cunoscute x_1, x_2 și respectiv x_3.

PAS 1 Multiplicative gate

PAS 2 Additive gate

Considerăm Alice = Utilizatorul 1
Bob = Utilizatorul 2
Cesar = Utilizatorul 3

PAS 1 Facem construcția pentru poarta multiplicativă

Partajarea datelor inițiale

	A	B	C
$4X+1$	5	9	13
$5X+2$	7	12	17
$6X+3$	9	15	21

- Evaluarea înmulțirilor locale

A: $5 \cdot 7 = 35$
B: $9 \cdot 12 = 108$
C: $13 \cdot 17 = 221$

- Partajarea înmulțirilor locale

	A	B	C
$X+35$	36	37	38
$2X+108$	110	112	114
$3X+221$	224	227	230

- Aplicăm vectorul de recombinare $(3,-3,1)$

A: $3 \cdot 36 - 3 \cdot 110 + 224 = 2$
B: $3 \cdot 37 - 3 \cdot 112 + 227 = 2$
C: $3 \cdot 38 - 3 \cdot 114 + 230 = 2$

PAS 2 Construcția pentru poarta additivă

A: $9 + 2 = 11$
B: $15 + 2 = 17$
C: $21 + 2 = 23$

Dișecția publică ~ se aplică vectorul de recombinare $(3,-3,1)$

$3 \cdot 11 - 3 \cdot 17 + 23 = 5$

Verificare: $x_1 x_2 + x_3 = 1 \cdot 2 + 3 = 5$.

□

Ex #4 Goldwasser-Micali din seminarul 8 (ex #4)

Ex #5 Cipolla din seminarul 8 (ex #7)

Ex #6 Secret Multiparty Computation

- Valorile secrete

Alice	$x = 6$
Bob	$y = 11$
Cesar	$z = 13$

- Vor să calculeze $2 \cdot (x + y)$
- Pentru partajarea valorilor inițiale

Alice	$3X + 6$
Bob	$5X + 11$
Cesar	$9X + 13$

- Partajarea înmulțirii

Alice	$X + a$
Bob	$3X + b$
Cesar	$6X + c$

Relați protocolul.

Deu
ans

PAS 1 Adunarea

PAS 2 Înmulțirea

PAS 1

a) Partajarea valorilor inițiale

	A	B	C
$3X + 6$	9	12	15
$5X + 11$	16	21	26
$9X + 13$	22	31	40

b) Adunarea locală

A: $9+16=25$

B: $12+21=33$

C: $15+26=41$

c) Realizarea locală a înmulțirii

A: $25 \cdot 22 = 550$

B: $33 \cdot 31 = 1023$

C: $41 \cdot 40 = 1640$

d) Partajarea înmulțirii

	A	B	C
$X+550$	551	552	553
$3X+1023$	1026	1029	1032
$6X+1640$	1646	1652	1658

e) Recombinarea locală.

A: $3 \cdot 551 - 3 \cdot 1026 + 1646 = 221$

B: $3 \cdot 552 - 3 \cdot 1029 + 1652 = 221$

C: $3 \cdot 553 - 3 \cdot 1032 + 1658 = 221$

f) Recombinarea finală

$3 \cdot 221 - 3 \cdot 221 + 221 = 221$

Verificare: $2(x+y) = 13 \cdot (6+11) = 13 \cdot 17 = 221$.

□

Secure circuit evaluation III

- Pp că avem $n \geq 3$ utilizatori, $A_1, A_2, \dots, A_n$
- Vor să calculeze o funcție aritmetică $f(x_1, \dots, x_n)$, unde fiecare x_i este intrarea de la A_i
  a) x_i - valoare trebuie să rămână secretă pt ceilalți participanți A_j, $i \neq j$.
  b) fiecare utilizator trebuie să aibă încredere în procesul de calcul

Ex Avem $n = 6$ utilizatori care au 6 valori secrete $x_1, x_2, \dots, x_6$.
Funcția $f(x_1, \dots, x_6) = x_1x_2 + x_3x_4 + x_5x_6$ se poate calcula prin
- 3 porți multiplicative / 3 multiplicative gates
- 2 porți aditive / 2 additive gates.

Partajarea valorilor

Fiecare participant A_i alege aleator $f_1, \dots, f_t \in \mathbb{F}_p$ și construiește polinomul de partajare

$$h_i(x) = x_i + f_1 x + \dots + f_t x^t$$

Utilizatorul A_j primește de la utilizatorul A_i un reprezentant al valorii secrete x_i

$$x_i^{(j)} = h_i(j)$$

Același lucru se întâmplă și pentru $i = j$.
Fiecare utilizator evaluează circuitul folosind doar valorile primite. Utilizatorul j va folosi valorile

$$x_1^{(j)}, x_2^{(j)}, \dots, x_n^{(j)}$$

Cum construim cele două tipuri de porți?
a) Poarta aditivă
b) Poarta multiplicativă.

a) Poarta aditivă

- Doar se efectuează calculele modulo p
- Avem două valori partajate $a^{(i)}$ și $b^{(i)}$ care ajung la poarta aditivă
  ↳ polinoamele de partajare

$$f(x) = a + f_1 x + f_2 x^2 + \_ + f_t x^t$$
$$g(x) = b + g_1 x + g_2 x^2 + \_ + g_t x^t$$

- $a + b = c \mod p$

$f + g = h$ în $\mathbb{Z}_p[x]$ $\not\Rightarrow$ $c^{(i)} = h(i) = (f(i) + g(i)) = a^{(i)} + b^{(i)}$

$\Rightarrow$ fiecare utilizator trebuie doar să adune valorile partajate.

OBS Același lucru se întâmplă pentru ~~se~~ scăderea

b) Poarta multiplicativă

R: interpolare Lagrange
$f(x)$ polinom
se cunosc valorile $f(j)$ $\not\Rightarrow$ există un vector $(r_1, \_, r_u)$ așa.

$$f(0) = \sum_{i=1,u} r_i f(i)$$

OBS
- vectorul funcționează pentru toate polinoamele de grad $\leq u-1$
- vectorul se vector de recombinare

- fiecare utilizator are o valoare partajată pentru a și b

$a^{(i)} = f(i)$ unde $f(0) = a$
$b^{(i)} = g(i)$ $g(0) = b$

vrem $c^{(i)} = h(i)$ așa pt un anume $h(x)$, $h(0) = c = ab$

Pasii principali

P1) Local, fiecare utilizator calculează $d^{(i)} = a^{(i)} b^{(i)}$

P2) Fiecare utilizator creează un polinom $\delta_i(x)$ de grad cel mult t a.î. $\delta_i(0) = d^{(i)}$

P3) Fiecare utilizator i transmite fiecărui utilizator j (inclusiv lui) valoarea $d_{i,j} = \delta_i(j)$.

P4) Fiecare utilizator i calculează

$$c^{(i)} = \sum_{j=1,u} x_j d_{i,j}$$