

: Pen note

گروه مجموعه است دو عامل را که دارند تعریف خود را باشد سه خاصیت طلاقته باشد

$(G, *)$

گروه که عضو معلوم دارد گروه آن است

$\{1, 2, \dots, n-1\}$ این گروه خواست جول دو عامل را که دارند توان تعریف شوند

$(Z_n, +) \rightarrow a+b \bmod n \in Z_n$

$a, b \in Z_n$

ععنو شدن
ععنو معلوم

$(Z_n, *) \rightarrow a \cdot b \bmod n \in Z_n$

$a, b \in Z_n$

ععنو شدن
ععنو معلوم

ناره مکرر به سط اولیه $\text{GCD}(a, n) = 1$ باشد

این گروه ایجاد نیست جول میباشد

هر اعشار کن معلوم ندارد

برای اولیه Z_n سبب برگردانه باشند n که عدد اول باشد $\text{GCD}(p, n) = 1$ باشد

$(Z_p, *) \rightarrow$ آنکه است

سیار: باید نکه گروه سبب به دو عامل گروه آن باشد و وزیر نیز رشت به این دو عامل داشته باشد.

$(F, +, \cdot)$

$a, b, c \in F$

$\rightarrow (F, +) \rightarrow (AG)$ گروه آنچه
لها صفت هر کمتر
 $\rightarrow (F, \cdot) \rightarrow (AG)$ لها صفت زیر کمتر
 $\rightarrow a \cdot (b+c) = a \cdot b + a \cdot c \rightarrow$ دیجیست

جیا نیک میباشد و خاصیت دارد.

$\text{order}(F) = n$ \rightarrow سیار

$(Z_{p^1}, +, \cdot) \rightarrow$ سیار ستم
 $\rightarrow GF(p) \rightarrow$ سیار اول \rightarrow Prime Field

$GF(2) \rightarrow$ دی اعشار آن که همروند است \rightarrow میان سیار دو دو

دسته: داشتن یک عدد اول P و یک عدد ممتد n که میان متأثر باشد از متبادر P^n وجود دارد. این میان متأثر را با $GF(P^n)$ نامی داده. این فرایم را در فضای n -بعدی Field می‌نامیم.

متأثر میان اول طبق و مبنای اعداد n را نویسند. بنابراین متأثر میان $GF(P^n)$ را در فضای n -بعدی Field می‌نامیم.

میان را با $(GF(P))^{(n)}$ نویسند. این میان را با $(GF(P))^n$ نویسند. این میان را با $GF(P^n)$ نویسند.

If $\sum_{i=1}^C i = \varnothing \rightarrow \text{Then Field Characteristic } C = \varnothing \rightarrow C = 2$

$$GF(2) = \{0, 1\} \Rightarrow 1+1 \stackrel{2}{=} \varnothing \rightarrow C = 2$$

$$GF(P) \rightarrow P = \text{جذری}$$

$$GF(P^n) \rightarrow P^n = \text{جذوری}$$

$$GF(2^10) \leftarrow GF(4^5) = 2 \text{ جذری} \quad GF(2^4) = 2 \text{ جذری} : \int_0^1$$

$$(a+b)^2 = a^2 + 2ab + b^2 \text{ mod } 2 \quad \text{لیکن } a, b \in GF(2^n) \text{ هستند: جزءی از } GF(2^n) \text{ binary extension field}$$

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2 \quad \checkmark$$

$$(a+b+c)^2 = a^2 + b^2 + c^2 \quad \left(\sum_{i=1}^k a_i \right)^2 = \sum_{i=1}^k a_i^2 \quad \text{لیکن } a_1, a_2, \dots, a_k \in GF(P^n) \quad a \text{ است: جذری}$$

: $\text{order}(\alpha)$

جزءی از $\alpha^2, \alpha^3, \dots \in GF(P^n)$ است. لیکن $\alpha \in GF(P^n)$

آنرا $\alpha^m = 1$ باشد. سپس α کوچکترین عدد ممتد m است که $\alpha^m = 1$ باشد. این m را $\text{order}(\alpha)$ می‌نامیم.

$$\alpha^m = 1 \rightarrow m = \text{order}(\alpha)$$

³ $\alpha^k = 1$, $\text{order}(\alpha) = m \Rightarrow m | k \Rightarrow \begin{cases} k = im \\ G/N \end{cases}$: 从 G 到 G/N 的映射是满的

عندراویه در مک میان شاهزاده عذر گفته اس نمک است از مرتبه میان باشد عذر اولیه کوئن.

$d \in GF(p) \rightarrow$ If $\text{order}(d) = p-1$ Then d is primitive element

$\alpha \in GF(p^n) \rightarrow$ If $\text{order}(\alpha) = p^n - 1$ then α is primitive element

بعز عنصر اولیه، عنصر است که در توان مانند نوکری هم اعشار میان انسازد.

عنصر های متمایز عضو اول و سازه هستند (اهمیت و کمی)

— هر سیان سماو تیکا دک عنصر اولیه دارد. نه سماو اعضاو غیر لیز دک سیان لاباتو اعضاو محساز.
— تصنیف حدائق بگو

نحو اعشار میان بایوسیو و در رابطه با زیستی و این

$$x^q \in GF(q) \rightarrow x^q - x = 0 \Rightarrow x^q = x \Rightarrow x^{q-1} = 1$$

مختصر مجموعه

۱- می‌سایم همچو خوش خوش

polynomial over infinite field \Rightarrow ساده لهم لهم

مش جنگ علیاً نا استفاده نه اعطا و نه کسی ای بی هدایت ذمی میشوند و سعادت

$a_i \in GF(P) \rightarrow A(x) = a_0 + a_1 x + a_2 x^2 + \dots \rightarrow$ $\bigcup_{i=0}^{\infty} a_i x^i$ شکلی

سماهی از جمله ای با معنی است که تهدید خواهی بعین همین صفات باشد. بنابراین

بـ الـ عـلـمـ وـ سـبـبـ اـسـتـ

$$A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \quad \& \quad a_n \neq 0 \Rightarrow \deg(A(x)) = n$$

If $a_n = 1$ Then monic polynomial \rightarrow monic polynomial

reCiprocal polynomials sum of terms

$$A^*(x) = x^n A(x^{-1}) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$$

irreducible polynomial is $\zeta^6 + \zeta^3 + 1$

$$\text{J: } \text{GF}(2) \rightarrow \frac{(x^3+1)}{x+1} = x^2 + x + 1 \quad \text{جنس ناپیر}$$

قیمتی معمولی و مرد عدست m داشتند که جینهای جنس ناپیر برخوبی می‌باشد و از m موجود است.

قیمتی از $\text{GF}(q)$ داشتند که جینهای جنس ناپیر برخوبی $\text{GF}(q^m)$ از درجه m باشد، آنها $f(x)$ دارند که متعلق به میان است. این میان سر نویس است و در $\text{GF}(q^m)$ دارد.

لطفاً متن کشی $\text{GF}(2^6) = \text{GF}((2^2)^3)$ معرفی شده باشد. آنها روز x^3+x+1 دارند.

$\alpha, \alpha^2, \alpha^4, \dots, \alpha^{m-1} \in \text{GF}(q^m)$ با رسانیدند که α^n متعلق به میان است.

سرد جینهای $f(x) = x^m + \sum_{i=0}^{m-1} f_i x^i$

$f_i \in \text{GF}(2)$

$f_m = 1$

$f_0 = 1$

$f_1 = 1$

$f_2 = 1$

$f_3 = 1$

$f_4 = 1$

$f_5 = 1$

$f_6 = 1$

$f_7 = 1$

$f_8 = 1$

$f_9 = 1$

$f_{10} = 1$

$f_{11} = 1$

$f_{12} = 1$

$f_{13} = 1$

$f_{14} = 1$

$f_{15} = 1$

$f_{16} = 1$

$f_{17} = 1$

$f_{18} = 1$

$f_{19} = 1$

$f_{20} = 1$

$f_{21} = 1$

$f_{22} = 1$

$f_{23} = 1$

$f_{24} = 1$

$f_{25} = 1$

$f_{26} = 1$

$f_{27} = 1$

$f_{28} = 1$

$f_{29} = 1$

$f_{30} = 1$

$f_{31} = 1$

$f_{32} = 1$

$f_{33} = 1$

$f_{34} = 1$

$f_{35} = 1$

$f_{36} = 1$

$f_{37} = 1$

$f_{38} = 1$

$f_{39} = 1$

$f_{40} = 1$

$f_{41} = 1$

$f_{42} = 1$

$f_{43} = 1$

$f_{44} = 1$

$f_{45} = 1$

$f_{46} = 1$

$f_{47} = 1$

$f_{48} = 1$

$f_{49} = 1$

$f_{50} = 1$

$f_{51} = 1$

$f_{52} = 1$

$f_{53} = 1$

$f_{54} = 1$

$f_{55} = 1$

$f_{56} = 1$

$f_{57} = 1$

$f_{58} = 1$

$f_{59} = 1$

$f_{60} = 1$

$f_{61} = 1$

$f_{62} = 1$

$f_{63} = 1$

$f_{64} = 1$

$f_{65} = 1$

$f_{66} = 1$

$f_{67} = 1$

$f_{68} = 1$

$f_{69} = 1$

$f_{70} = 1$

$f_{71} = 1$

$f_{72} = 1$

$f_{73} = 1$

$f_{74} = 1$

$f_{75} = 1$

$f_{76} = 1$

$f_{77} = 1$

$f_{78} = 1$

$f_{79} = 1$

$f_{80} = 1$

$f_{81} = 1$

$f_{82} = 1$

$f_{83} = 1$

$f_{84} = 1$

$f_{85} = 1$

$f_{86} = 1$

$f_{87} = 1$

$f_{88} = 1$

$f_{89} = 1$

$f_{90} = 1$

$f_{91} = 1$

$f_{92} = 1$

$f_{93} = 1$

$f_{94} = 1$

$f_{95} = 1$

$f_{96} = 1$

$f_{97} = 1$

$f_{98} = 1$

$f_{99} = 1$

$f_{100} = 1$

$f_{101} = 1$

$f_{102} = 1$

$f_{103} = 1$

$f_{104} = 1$

$f_{105} = 1$

$f_{106} = 1$

$f_{107} = 1$

$f_{108} = 1$

$f_{109} = 1$

$f_{110} = 1$

$f_{111} = 1$

$f_{112} = 1$

$f_{113} = 1$

$f_{114} = 1$

$f_{115} = 1$

$f_{116} = 1$

$f_{117} = 1$

$f_{118} = 1$

$f_{119} = 1$

$f_{120} = 1$

$f_{121} = 1$

$f_{122} = 1$

$f_{123} = 1$

$f_{124} = 1$

$f_{125} = 1$

$f_{126} = 1$

$f_{127} = 1$

$f_{128} = 1$

$f_{129} = 1$

$f_{130} = 1$

$f_{131} = 1$

$f_{132} = 1$

$f_{133} = 1$

$f_{134} = 1$

$f_{135} = 1$

$f_{136} = 1$

$f_{137} = 1$

$f_{138} = 1$

$f_{139} = 1$

$f_{140} = 1$

$f_{141} = 1$

$f_{142} = 1$

$f_{143} = 1$

$f_{144} = 1$

$f_{145} = 1$

$f_{146} = 1$

$f_{147} = 1$

$f_{148} = 1$

$f_{149} = 1$

$f_{150} = 1$

$f_{151} = 1$

$f_{152} = 1$

$f_{153} = 1$

$f_{154} = 1$

$f_{155} = 1$

$f_{156} = 1$

$f_{157} = 1$

$f_{158} = 1$

$f_{159} = 1$

$f_{160} = 1$

$f_{161} = 1$

$f_{162} = 1$

$f_{163} = 1$

$f_{164} = 1$

$f_{165} = 1$

$f_{166} = 1$

$f_{167} = 1$

$f_{168} = 1$

$f_{169} = 1$

$f_{170} = 1$

$f_{171} = 1$

$f_{172} = 1$

$f_{173} = 1$

$f_{174} = 1$

$f_{175} = 1$

$f_{176} = 1$

$f_{177} = 1$

$f_{178} = 1$

$f_{179} = 1$

$f_{180} = 1$

$f_{181} = 1$

$f_{182} = 1$

$f_{183} = 1$

$f_{184} = 1$

$f_{185} = 1$

$f_{186} = 1$

$f_{187} = 1$

$f_{188} = 1$

$f_{189} = 1$

$f_{190} = 1$

$f_{191} = 1$

$f_{192} = 1$

$f_{193} = 1$

$f_{194} = 1$

$f_{195} = 1$

$f_{196} = 1$

$f_{197} = 1$

$f_{198} = 1$

$f_{199} = 1$

$f_{200} = 1$

$f_{201} = 1$

$f_{202} = 1$

$f_{203} = 1$

$f_{204} = 1$

$f_{205} = 1$

$f_{206} = 1$

$f_{207} = 1$

$f_{208} = 1$

$f_{209} = 1$

$f_{210} = 1$

$f_{211} = 1$

$f_{212} = 1$

$f_{213} = 1$

$f_{214} = 1$

$f_{215} = 1$

$f_{216} = 1$

$f_{217} = 1$

$f_{218} = 1$

$f_{219} = 1$

$f_{220} = 1$

$f_{221} = 1$

$$\varphi(24) = \varphi(2^3 \cdot 3) = 24 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 8$$

سال

متاد حینهای از دارایی بیشتر از درجه m عارست ازه

$$\varphi(2^{m-1})$$

هر رسمی هار یک چند جمله ای بخشنود می هم درجه هست. هر رسمی هار یک چند جمله ای اولیه دلایل مرتبه هر کسی از صیغه است که سلسله وده. در مرتبه هر رسمی هاست

عاسی اعضا در میان نعم یافته: $GF(P^m)$

عاسی که از نعم یافته: برای این عاسی باشد یک عنصر اولیه داشته باشیم. (ا) این (توان ساز) که علاوه بر آن عسا

نار تولید کنند خواهد بود (x) یک چند جمله ای از درجه m بروی $GF(P)$ باشد رسمی این چند جمله ای عضو میان نعم یافته خواهد بود.

و مرتبه در $1 - P^m$ است. پس عاصی اعضا در میان نعم یافته ندارید کنند. به سکر زیر:

$$d \in GF(P^m) \rightarrow \left\{ 0, \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{P^m-2} \right\} \rightarrow \begin{matrix} \text{اعضا در میان} \\ \text{نعم یافته} \end{matrix}$$

با این روش چند ساده ساخته دفعه میل در میان

$$\alpha^a + \alpha^b = ? \quad \text{اما} \quad \alpha^a \cdot \alpha^b = \alpha^{a+b}$$

برای حل مشکل جمع ارجمند استفاده در میان بنیجود

عصر اولیه باشد حدود زیرا در میان

α^0	*
1	α^1
2	
3	
4	
5	
6	
7	

در میان $GF(2^3)$ (چند جمله ای در میان)

داست.

$$2 \in GF(5) \rightarrow \begin{cases} 2 \\ 2 \times 2 = 4 \\ 2 \times 2 \times 2 = 8 \stackrel{5}{=} 3 \\ 2^4 = 16 \stackrel{5}{=} 1 \end{cases} \xrightarrow{\text{اول است}} \begin{array}{l} \text{اول است } m+1=5 \leftarrow m=4 \quad \int_0^5 \\ \text{اول است } m+1=7 \leftarrow m=6 \end{array} \xrightarrow{\text{اول است } m+1=11 \leftarrow m=10} \begin{array}{l} P(x) = x^5 + x^3 + x^2 + x + 1 \\ \downarrow \\ \text{محض باید مخواست} \end{array}$$

$\Rightarrow A = P$

\int_0^6

$$\xrightarrow{\text{اول است } m+1=7 \leftarrow m=6} \xrightarrow{\text{اول است } m+1=11 \leftarrow m=10} \xrightarrow{\text{اول است } m+1=15 \leftarrow m=14} \begin{array}{l} P(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \end{array}$$

$\Rightarrow A = P$

\int_0^6

: primitive polynomial

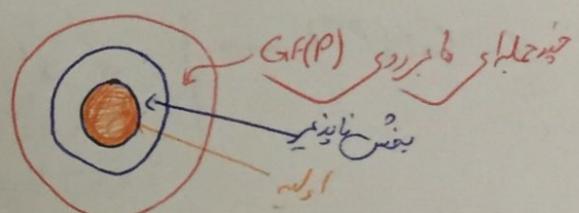
تقریباً با صحت عصر اولیه محیصت شده

$f(x) | x^n - 1$ که جمله اول بعنوان ناپذیر نظر $GF(P)$ از دجه m اول است، اگر دو جمله اول عدد مستب غایب باشند

$$n = P^r - 1$$

موزونگانه باشد

$$x^{P^r} - x^r = 0$$



$$x^n - 1 \leftarrow x^4 + x + 1 | x^{15} - 1 \leftarrow GF(2) \text{ بجز } x^4 + x + 1$$

$$x^n - 1 \leftarrow x^4 + x^3 + x^2 + x + 1 | x^{15} - 1$$

$GF(2)$ اولیه $x^2 + x + 1 | x^3 + 1$ است

$GF(2^2)$ ریشه اک تو

نکته جمله اول اولیه بجز اینجا اینجا اینجا

$$f_{(+)} = \begin{cases} 1 & t=1 \\ t \cdot \pi \left(1 - \frac{1}{P_i} \right) & t \neq 1 \end{cases}$$

نکته این دو مجموعه متساوی هستند

عمر لک (سال)	نامیں جنگلیاں	عمر مبارکہ
0	ي	000
1	1	001
α	α	010
α^2	α^2	100
α^3	$\alpha+1$	011
α^4	$\alpha^2+\alpha$	110
α^5	$\alpha^2+\alpha+1$	111
α^6	α^2+1	101

$$\alpha^2 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + 1 + \alpha^2$$

$$\alpha^6 = (\alpha^3)^2 = (\alpha + 1)^2 = \alpha^2 + 1$$

نکتہ: دراں روشن جم سادھے کرنے کے لئے اسکا مرتباً وظیفہ تسلیم بینک علاحت
برداشت سمات۔ (صحن۔ مسکل و جم سادھے)۔

$$S = \alpha^3 + \alpha^4 + \alpha^2 + 1$$

$$5 = \alpha^3 + \alpha^4 + \alpha^2 + 1 = \alpha + 1 + \alpha^2 + \alpha + \alpha^2 + 1 = \phi$$

Conrad Gileiz

چند جمله ای دو کاتن در طول میان (لا تسلیم کرد چند جمله ای مساعده نایمه و سعاد) (چند جمله ای اکبر بک از متون هار چند جمله ای مساعده است)

لایه ریاضی پنجم متوسطه
برای کسانی که نیاز ندارند

$$d^a \cdot d^b = d^{a+b \text{ mod } (q-1)}$$

$$d^{q-1} = d \rightarrow d^{q-1} \equiv 1$$

$$S = 2x^3 + x + 1 \quad : \text{Jus}$$

$$\text{حامل صفر} - \text{در عنصر معمولی در } \mathbb{F}_{2^3} \text{ همان سه ای} \\ (1) + (x^3 + 1) = x^3 + 1^2 + 1^2 + 1 + 1 \mod x^3 + x + 1 =$$

$$= \alpha^3 + 1 \text{ mod } \alpha^3 + \alpha + 1 = \alpha + 1 + 1 = \alpha$$

$$P = (\alpha^2 + \alpha + 1)(\alpha + 1) \bmod (\alpha^3 + \alpha + 1) = \frac{\alpha^5 \cdot \alpha^3}{\bmod (2 \cdot 1) = 7} = \alpha^8 = \alpha$$

$$g = 2^3 = 8$$

Bases for extension fields

الله يحيى بن عبد الله

دھنیف: یک صہبہ از ۷ عصر از میاں $GF(P^m)$ کے مستعمل خلیج پاسن سکل کے پایہ بدلار $GF(P)$ بروئی و دھن. (سیز این عصر لانوچان) با ترکیب خلیج تبیه نوست) دراں عالمت ہر عصر از $GF(P^m)$ با استفادہ از ترکیب خلیج این پایہ بدل نہیں اس.

y	$\log_{\alpha} y$	$\log_{\alpha} (y+1)$
0	*	0
1	0	*
α	1	3
α^2	2	6
α^3	3	1
α^4	4	5
α^5	5	4
α^6	6	2
7	7	

$$S = \alpha^3 + \alpha^4 + \alpha^2 + 1$$

6 per cent

حال حرقان عملیات بعثت اسلامیه فردا

$$\begin{aligned} S &= \underbrace{\alpha^3 + 1}_{=} + \alpha^4 + \alpha^2 = \alpha^2 + \alpha^2(\alpha^2 + 1) = \alpha^4 + \alpha(\alpha^4 + 1) = \\ &= \alpha^4 + \alpha \cdot \alpha^3 = \alpha^4 + \alpha^4 = \phi \end{aligned}$$

این مجموعه مذکور است جو \mathbb{F}_{2^m} به حاصل قطعی بخانم از $2^m \times m$ دارد (یعنی $(GF(2^m))^m$)
در این مجموعه ~~هم~~ اعداد مستقل هستند اما مجموع عکس علایات بوده است.

نامه (جذع‌الادار

خصل لئے اور سی دی جنہیں
(یعنی خود را لیے اسٹ) (دارم)

$$f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_1x + f_0 \in \mathbb{Q}_F(p)$$

$$\hookrightarrow F(\alpha) = 0 \implies \alpha^m = -\left(f_{m-1} \cdot \alpha^{m-1} + \dots + f_1 \cdot \alpha + f_0\right)$$

طریق دو دسته مذکور می شوند.

$$\alpha^{m+1} = - (f_{m-1}\alpha^m + \dots + f_1\alpha^2 + f_0\alpha) = - (f_{m-1}(f_{m-1}\alpha^{m-1} + \dots + f_1\alpha + f_0) + \dots + f_1\alpha + f_0) =$$

$$= f_{m-1}(f_{m-1}\alpha^{m-1} + \dots + f_1\alpha + f_0) - (f_{m-2}\alpha^{m-1} + \dots + f_0\alpha + 0)$$

در راسته بین ترتیب و توان ناگفته مانند α^{m-1} ، α^{m-2} ، \dots ، α^1 ، α^0 است.

میان مکان هایی که علاوه بر شهر میان آنها نیز دارند، در اینجا شکل ترک خطر زبردست است.

$$a_{m-1} \alpha^{m-1} + \dots + a_1 \alpha = \alpha^0$$

است. (موجعه صفر) $a_i \in Gf(P)$ وابوچ

نکتہ: ایک عوامی نہاد ہے جس کا عمل اسکا (یعنی جو خصائص نظریہم کا درجہ سلسلہ کا دھنیز ہے) بسیاریہ میں

$$\sqrt{x^3 + x + 1}$$

$$\alpha \in GF(2^3) \rightarrow \text{يساوى} \rightarrow \alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1 \quad \begin{matrix} \text{سبت} \\ \text{مقدار} \end{matrix}$$

گاهی مجموعه $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ میزد و در اینجا α یک جذب‌حلقه‌ای است (نامیده می‌شود).

$\forall A \in GF(P^m)$, $a_i \in GF(P)$

$$A = a_{m-1} \cdot \alpha^{m-1} + a_{m-2} \cdot \alpha^{m-2} + \dots + a_1 \cdot \alpha + a_0.$$

برای هر دو

$\{1, \alpha, \dots, \alpha^{m-1}\}$ رسمیت جذب‌حلقه‌ای بغض نایمود و عنوان می‌باشد (از درجه m برخوبی) آنچه اعشار مجهود می‌شود مسئله حلخال‌هندی و درستی که ای جذب‌حلقه‌ای سلسله و دهندر طبقاً مذکور که تراز $1 - P^m$ خواهد بود و عنصر اولیه ذکر اندیشه برای اعشار میانی این تردد است.

آنچه در رسمیت جذب‌حلقه باشد $F(x) = P(x)Q(x)$ و که بر جنر نایمود نسبت در $F(x)$ است $\Rightarrow \{1, \alpha, \dots, \alpha^{m-1}\}$ مسئله حلخال شود. در آنچه در درجه $(P(x))K^m$, $\deg(P(x)) < m$ طبقاً $F(x) = P(x)Q(x)$ در آنچه در درجه $(Q(x))K^m$, $\deg(Q(x)) < m$ باشد و این بمعنای است که ترکیب خط حد الگه بارچه $1 - m$ وجود دارد و این هم بمعنای مسئله حلخال شود. مجهوده مذکور است.

(NB) normal bases: پایه متریک

در این صورت، به صورت مسأله ای ای جذب‌حلقه و زیر مسئله زیر مسئله $\beta \in GF(P^m)$ می‌شود که این مسئله حلخال باشد.

$$\{\beta, \beta^\rho, \beta^{\rho^2}, \dots, \beta^{\rho^{m-1}}\}$$

$$A \in GF(P^m) \Rightarrow A = a_{m-1} \beta^{m-1} + a_{m-2} \beta^{\rho^{m-2}} + \dots + a_1 \cdot \beta^\rho + a_0 \cdot \beta$$

با استفاده از جذب‌حلقه معرفی شده (یادداشت میان) این مسئله حلخال می‌شود.

$$f(x) = x^3 + x^2 + 1 \quad \text{جذب‌حلقه} \quad f(\alpha) = 0 \Rightarrow \alpha^3 + \alpha^2 + 1 = 0 \Rightarrow \alpha^3 = \alpha^2 + 1$$

لذا ای جذب‌حلقه معرفی شده اولیه نیست. سه اعشار میان می‌شود.

	α^0	α^{2d+1}	α^{2d+2d}	α^{4d+2d}	$\alpha^{4d+2d+1}$
0	*	0	000	000	0
1	000	1	001	111	$\alpha^4 + \alpha^2 + \alpha$
α	001	α	010	α^2	α
α^2	α^0	α^2	100	α^0	α^2
α^3	α^1	$\alpha^2 + 1$	101	101	$\alpha^4 + \alpha$
α^4	100	$\alpha^2 + \alpha$	111	100	α^4
α^5	101	$\alpha + 1$	011	110	$\alpha^4 + \alpha^2$
α^6	110	$\alpha^2 + \alpha$	110	011	$\alpha^2 + \alpha$

* α^0 α^{2d+1}
 $\alpha^{4d+2d+1}$

$$\alpha^4 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha^2 + \alpha$$

$$\alpha^5 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1$$

→ α^{2d+1}

نکه: دنایس زمکل معمولاً معنی آن سیارات کل برابر باشد.

$$\alpha^4 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1 + \alpha^2 + \alpha = 1$$

$$\alpha^3 + \alpha^2 + 1 = \alpha^2 + \alpha^4 + \alpha^2 + \alpha = \alpha^4 + \alpha$$

$$\alpha^4 = \alpha + 1 = \alpha + \alpha^4 + \alpha^2 + \alpha = \alpha^4 + \alpha^2$$

تعمیر طبقه

دعاوی: $\{B_i\} \subset \text{دانایس}$ در نظر نمایم. زمکل $\{B_i\}$ عضور امتعال بـ مسار $Gf(P)$ باشد و داده شده باشد.

$$A = \sum_{i=0}^{m-1} a_i d_i = \sum_{i=0}^{m-1} b_i \beta_i \quad a_i, b_i \in Gf(P)$$

آخر مجموعه مار $\{\beta_i\}, \{d_i\}, \{b_i\}, \{a_i\}$ در نظر نمایم.

$$A = a \cdot \alpha^T = b \cdot \beta^T$$

$$\beta^T = C \cdot \alpha^T$$

زمکل اصلی ماتریس C در رابطه زیر صدق خواهد.

$$a \cdot \alpha^T = b \cdot \beta^T = b \cdot (C \cdot \alpha^T) \Rightarrow a = bC$$

درست: دو دیگر حین تحلیل از زمکل A در نظر نمایم.

$$\alpha = \{1, \alpha, \alpha^2\}, \quad \beta = \{1, \alpha^2, \alpha^4\}$$

الآن: محاسبه ماتریس C باوجه به جدول دنایس اعشار مسار $(*)$.

$$\begin{pmatrix} \alpha^4 \\ \alpha^2 \\ \alpha \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha^2 \\ \alpha \\ 1 \end{pmatrix}$$

NB

برای تبدیل ماتریس مرتعنص از پایه متریک به پایه خوبی‌گاری توان از استفاده کرد. همان‌طوری که $b = (011)_N$ است.

$$(011)_N \xrightarrow{\text{متریک خوبی}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \xrightarrow{\text{متریک خوبی}} (110)_{PB}$$

از این سه ماتریس متریک خوبی استفاده شود.

حالتی

$$f(x) = a_{m-1} \cdot x^{m-1} + a_{m-2} \cdot x^{m-2} + \dots + a_0, \quad \alpha \in GF(P^m)$$

$$a_i \in GF(2), \quad \alpha \in GF(2^m)$$

$$F(\alpha) = 0 \rightarrow (a_{m-1} \cdot \alpha^{m-1} + \dots + a_1 \cdot \alpha + a_0) = 0$$

$$a_{m-1} (\alpha^{m-1})^2 + \dots + a_1 \cdot \alpha^2 + a_0 = 0$$

$$F(\alpha^2) = 0 \rightarrow a_{m-1} (\alpha^2)^{m-1} + \dots + a_1 \cdot \alpha^2 + a_0 = 0$$

نکره اینکه سیم در خوبی‌گاری در $x^n - 1$ باشد و که $F(\alpha) | x^n - 1$ باشد که مطلب شرایطی است.

$$\text{ابتدا } ord(\alpha) = 3 \leftarrow x^3 - 1 \Rightarrow \text{خوبی‌گاری} \\ ord(\alpha) = 5 \leftarrow x^5 - 1 \Rightarrow \text{خوبی‌گاری}$$

برای محدودیت خوبی‌گاری در n کافیست آنرا معملاً برای n بگیری.

برو خوبی‌گاری در نظر گیرنده باش.

در نظر گیرنده باش سب سیمیه سدن محاسبات و ساده‌گاری کار شو و ... در نظر گیرنده سیمیه سدن.

عمل میکند - باید که

جزئی نیست در عین حال روابط از میان $A, B \in GF(P^m)$ داریم $\{a_i\}, \{d_j\}$ داریم.

$$A \cdot B = \sum_{i=0}^{m-1} a_i \cdot d_i \cdot \sum_{j=0}^{m-1} b_j \cdot d_j \quad a_i, b_j \in GF(P)$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i \cdot b_j \cdot d_i \cdot d_j \quad \text{از } a_i, d_j \in GF(P) \text{ است} \rightarrow a_i \cdot d_j = \sum_{l=0}^{m-1} C_{i,j} \cdot d_l \quad ①$$

$$\stackrel{①}{=} \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{l=0}^{m-1} a_i \cdot b_j \cdot C_{i,j} \cdot d_l \quad \text{نمایه از بحث هر دو در میان } GF(P) \text{ است پس بحث این مورد } O(m^3) \text{ است.}$$

بعارت دیگر دالت خوب بود در نظر داشت باشد خاصه میکند - بنابراین عامل های میان $O(m^3)$ میکند.

صریح - درایه جزء هایی

? استفاده از طبله خوبی از سید چند که میکند و داشت.

میکند درایه جزء هایی بطورت پیش

$$C = A \cdot B \mod F(x)$$

$$= A \cdot (b_0 + b_1 \cdot x + b_2 x^2 + \dots + b_{m-1} x^{m-1}) \mod F(x)$$

$$= b_0 \cdot A + b_1 \cdot x \cdot A + b_2 \cdot x^2 \cdot A + \dots + b_{m-1} \cdot x^{m-1} \cdot A \mod F(x)$$

$(2H, GF(2^m))$ PB mult

الgoritم در چه چیزی از اینست که از: صفت برآورده

Input: $A, B \in GF(2^m) \Rightarrow F(x)$ میتوانیم output: $C = A \cdot B \mod F(x)$

step1: $P = A \cdot b$

If $b_i = 1$
 $C = A \cdot b$
else
 $C = \emptyset$; } $\Rightarrow C = b \cdot A \Rightarrow C = A$ که میکند درایه جزء هایی را دارد $\Rightarrow C, P$ میکند
شاید (A, b) است آنرا C میکند C است آنرا b میکند A است آنرا C میکند b است آنرا A میکند

step2: For $i = 1$ to $m-1$ {
 $P = x \cdot P \mod F(x);$
If $b_i = 1$
 $C = C + P;$ } $C = C + b_i \cdot P$ سنترو ده سنترو ده

• $\mu_{i+1} \equiv \mu_i \pmod{m-1}$, $A_0 = A$, $A_i = \alpha A_{i-1} \pmod{F(n)}$

$$C = AB = b_0 \cdot A_0 + b_1 \cdot A_1 + \dots + b_{m-1} \cdot A_{m-1}$$

H2L mult

حال امکان سنت هار درازش بعثت سنت هار که درازش بود.

$$C = (A \cdot b_{m-1} \cdot x^{m-1} + A \cdot b_{m-2} \cdot x^{m-2} + \dots + A \cdot b_1 \cdot x + A \cdot b_0) \bmod F(x)$$

$$= ((Ab_{m-1} \cdot x + Ab_{m-2}) \cdot x + \dots) x + Ab_0 \bmod F(n)$$

$$= \left(\dots \left(A b_{m-1} n \cdot \text{mod } F(n) \right) + A \cdot b_{m-2} \right) x \cdot \text{mod } F(n) \dots) n \cdot \text{mod } F(n) + A b_m$$

Input: $A, B \in GF(P^m)$, $F(x) \in \mathbb{C}[x]^{\text{irr}}$, output: $C = A \cdot B \bmod F(x)$

Step I: $C = \emptyset$ \rightarrow ~~subset~~ \rightarrow ~~subset~~

Step2: For $i = m-1$ to ϕ /

$$C = \alpha \cdot C_{\text{model}} f(\alpha); \quad \longrightarrow$$

$$C = C_0 + A b_i ;$$

(Linear Feedback Shift Register)

لطفاً مجازی صدر $Gf(2^m)$ در طبقهٔ جنگجویان را استفادهٔ از $LFSR$ کنید.

$$\text{دراست} \quad F(y) = \sum_{i=1}^{m+1} f_i y^i$$

دراست

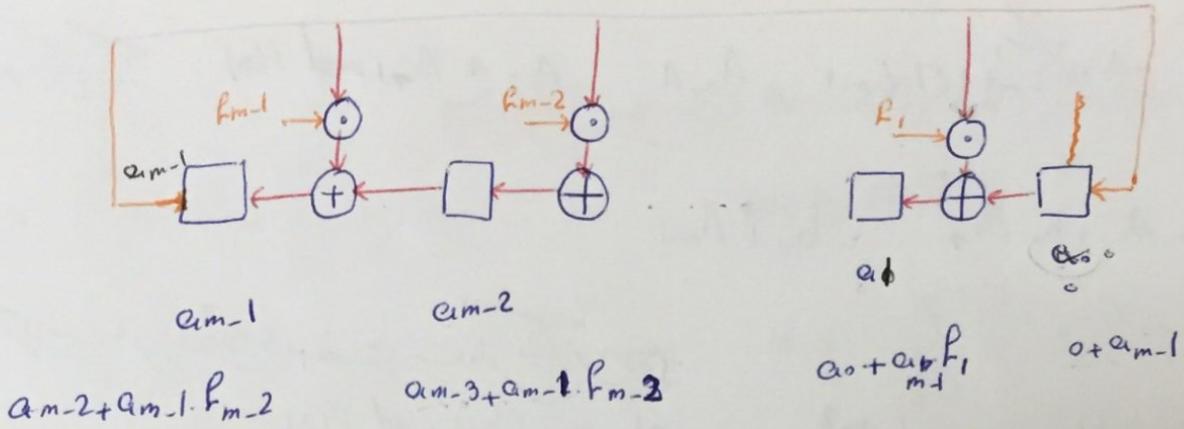
$$AE GF(2^m) \rightarrow x \cdot A = x \sum_{i=0}^{m-1} a_i x^i = \sum_{i=0}^{m-1} a_i \cdot x^{i+1} = \sum_{i=0}^{m-2} a_i \cdot x^{i+1} + a_{m-1} \cdot x^m$$

. if m >= 1 f(x) \neq 0

$$F(g) = \sum_{i=0}^m p_i g_i - \phi \quad \text{if } F(x) \neq 0$$

$$x^m = \sum_{i=0}^{m-1} p_i x^i \quad \Rightarrow \quad \sum_{i=0}^{m-2} a_{ii} \cdot x^{i+1} + a_{m-1} \sum_{i=0}^{m-1} p_i \cdot x^i = (a_{m-2}, a_{m-3}, \dots, a_0)^T$$

$$+ a_{m-1} (P_{m-1}, P_{m-2}, \dots, P_1, P_0)$$



حالت اولیه
متقارن بود

۱۰- کار خنده رسمی و اینکه عنصر را انجام می‌دهد. در واقع shift و چیزی (درست نیست) انجام می‌دهد.

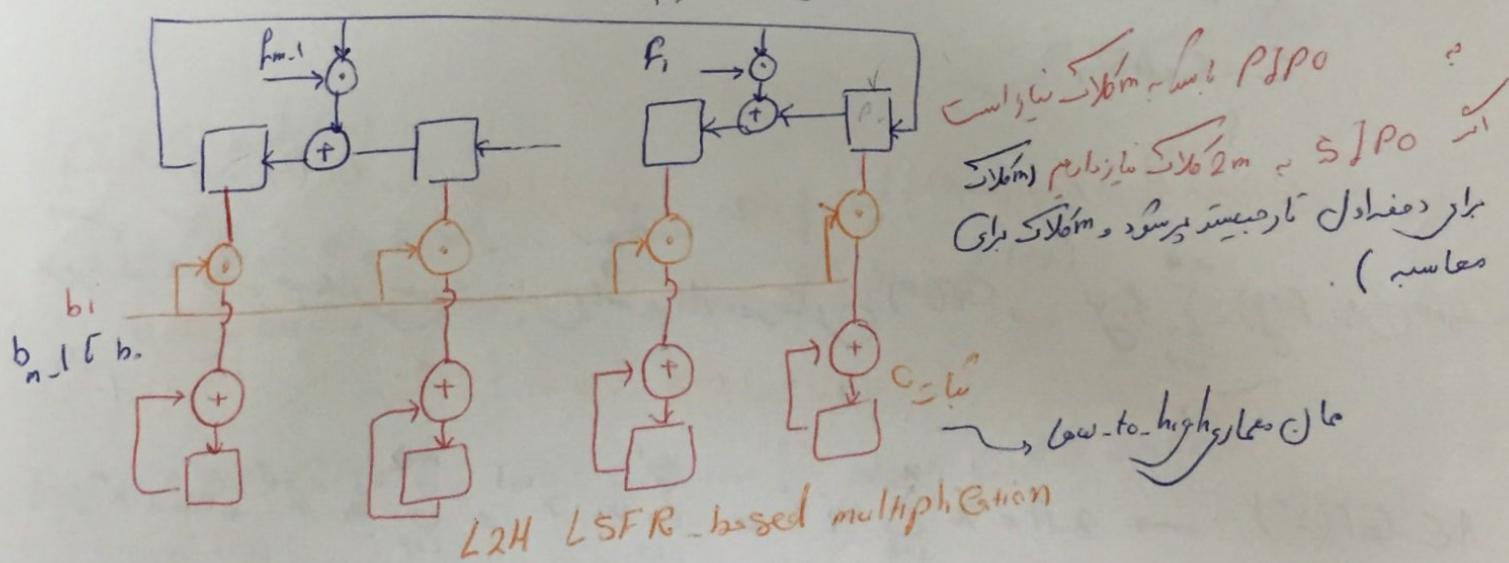
$$F[m-1:0] \leftarrow \{A[m-2:0], \phi\} + F[m-1:0] \Rightarrow \underbrace{\dots}_{\text{add } A[m-1:0]} \text{ and } xA \text{ has } C_1$$

$$\leftarrow C = b_{m-1} \cdot A_{m-1} + b_{m-2} \cdot A_{m-2} + \dots + b_0 \cdot A_0 \quad \leftarrow C = A \cdot B \bmod F(x)$$

$$A_0 = A \quad A_i = x \cdot A_{i-1} \bmod F(x)$$

مادر نظر مترجم

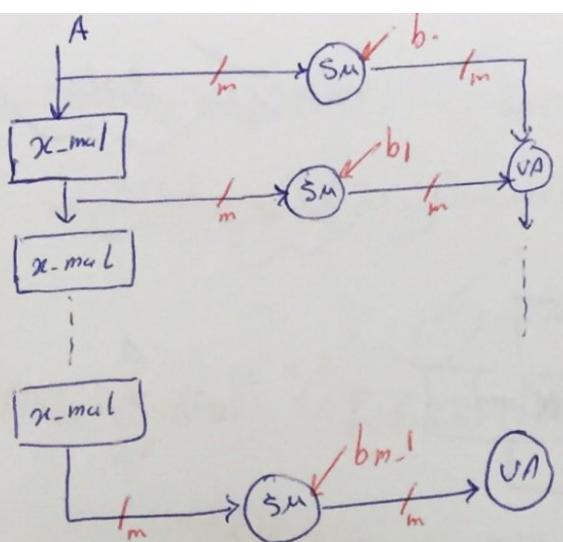
میں اسی میں مانسیت درست رائے کا دلیل ہے۔



$$\left. \begin{array}{l} \text{نقداد FF ها} = 2^m \\ \text{نقداد XOR ها} = 2^{m-1} \\ \text{نقداد AND} = 2^{m-1} \end{array} \right\} \Rightarrow \begin{array}{l} O(m) \\ (\text{از ورودی}) \end{array}$$

نماینده سمعکار می باشد

$$O(m^2) = (\text{Ans}) \quad \text{J}^2; \times \text{also } \checkmark \text{ more}$$



میل مدار به صورت ترکیبی دو سوی پیچیده سطحی
برای بروزگاردن و درینک مکان اینها را می‌دانند.

$$\begin{aligned} O(m^2) &\rightarrow \text{پیچیدگی ساخت} \\ O(1) &\rightarrow \text{پیچیدگی زمان} \\ O(m^2) &\leftarrow AT \end{aligned}$$

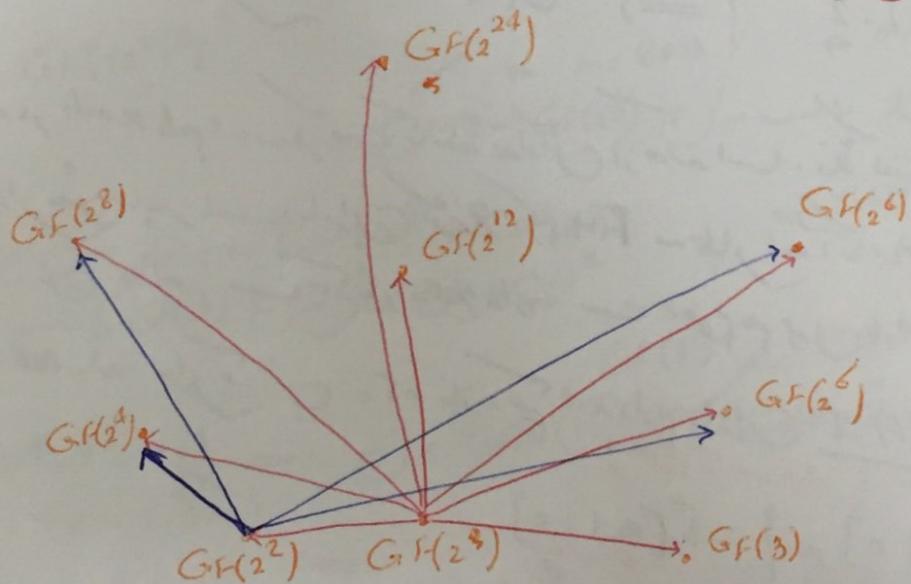
صریب با استفاده از زیرمیارها

۱) بحال صریب های انتخاب شده برای زیرمیار $GF(2)$ مجموع میان $GF(2^m)$ است همین امر از مرتبه m بهم
داد و در واقع صریب طبق زیرمیار های دلخواه نیز انجام دارد.

$$GF(2^{24}) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

متعدد اولیه های
نیازمند زیرمیار های

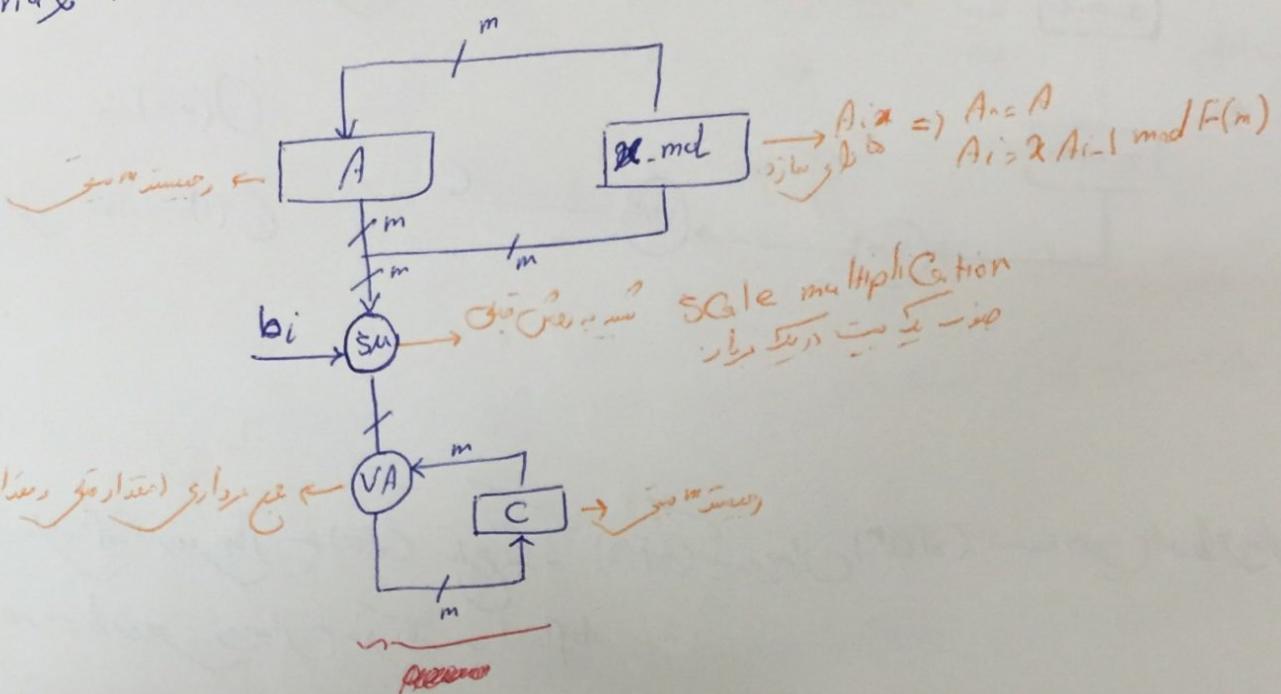
۲) زیرمیاری های دست پس زیرمیار آنهاست.



عمران مکار H2L ایز دندرمت

bit-serial PB mult (L2H)

خاص هنر سینما در می خواهد



نیاز داشتند تا از x -mol/L میزان m باشد. میزان m که در x -mol/L میزان m است، برابر با $m = M \cdot x$ است. بنابراین $m = M \cdot x$ است.

$$\#x_{\mathcal{R}} = m + H(F) - 2$$

نیاز به دو قدرم بایاریست
ست m است در این نسبت

$$x_A = \left\{ A[m-2:0] \right\}_{10} + \left\{ \begin{matrix} m-1 & :0 \\ 1 & :0 \end{matrix} \right\}$$

نیاز به دو قدرم بایاریست
 $0 \oplus 1 = 1 \Rightarrow$ دو قدرم بایاریست

نمایه دار است نیاز به دو قدرم بایاریست

bit-parallel PB mul in GF(2^m)

نماشی صریح معاذن در طایفه حبشه علماء و

ب) طبقه کار باشد از $GF(2^m)$ است پس حقول

$GF(2^m) \subseteq GF(2^n)^k$

اعمار $GF(2^n)$ باستفاده از ترتیب خط غایر (عنصر مستقل خط) پس زیر عبارت داد.

(1) مکعب جمله ای بعنوان ناپیر مانند $(x)_n$ از درجه k بر روی $GF(2^n)$ انتخاب کنیم.

$$f(x) = \sum_{i=0}^{k-1} b_i x^i \quad b_i \in GF(2^n)$$

$$\{1, x, x^2, \dots, x^{k-1}\}$$

(2) پایه از رسیدن مکعب جمله ای سهل گردد.

$GF(2^n) = GF(2^m)$ $a_i \in GF(2^n)$

پس اعماق حقول: صورت زیر بازی مکعب جمله ای ناپیر دارد.

$$A = \sum_{i=0}^{k-1} a_i x^i \quad A \in GF((2^n)^k)$$

کلمه \oplus مینیمیلیار از درجه k بر روی $GF(2)$ بعنوان ناپیر باشد و k, n بسته بهم اول باشند این مکعب جمله ای بر روی $GF(2^n)$ نیز بعنوان ناپیر است.

س) مرضن کنیم $m = 104$

بر ساخت $GF(2^{104})$ از ساخت سیال $GF(2^8) GF(2^8)$ استفاده کنیم.

(1) ساخت سیال $GF(2^8)$

$$GF(2^{104}) = GF((2^8)^{13})$$

$$m = 8 * 13$$

(2) ساخت سیال $GF(2^{104})$ بر روی $F(x)$

$$G(x) = x^8 + x^7 + x^3 + x^2 + 1$$

حال میتوان با استفاده از مکعب جمله ای $F(x)$ سیال $GF(2^8)$ بر روی سیال $GF(2^8)$ ساخت.

باید دقت داشت که اعمال معاملات اعماق سده را بر میتوان $GF(2^8)$ است پس اعماق بردارهای 8 بیو هستند.

مقدمة

مقدمة دریج $\text{GF}(2^m)$ در PB ایستاده است

یک دویست کاراکتر از هر دو عدد در خود است.

$A \in \text{GF}(2^m)$, $F(x) = \sum_{i=0}^{m-1} a_i x^i$ \rightarrow مقدمة از هر دویست کاراکتر در خود است و a_i مقدمة از $\{1, x, x^2, \dots\}$ است.

$$A^2 = \sum_{i=0}^{m-1} a_i x^i \Rightarrow A^2 = \left(\sum_{i=0}^{m-1} a_i x^i \right)^2 = \sum_{i=0}^{m-1} a_i \cdot x^{2i} \pmod{F(x)}$$

برای این طبقه ایجاد کنید

$$A^2 = a_{m-1} \cdot x^{2m-2} + a_{m-2} \cdot x^{2m-4} + \dots + a_0 =$$

AH

$$= (a_{m-1} \cdot x^{m-3} + \dots + \underbrace{a_{m+3} x^2}_{\text{برای}} + \underbrace{a_{m+1} x^{m+1}}_{\text{برای}} + \underbrace{(a_{m-2} x^{m-1} + \dots + a_1 x^2 + a_0)}_{AL})$$

AH

$$AH = x^{m+1} \pmod{F(x)}$$

$$x^m = \sum_{i=0}^{m-1} b_i x^i \Rightarrow x^{m+1} = b_{m-1} \cdot x^m + \sum_{i=0}^{m-2} b_i x^{i+1} = b_{m-1} \cdot \sum_{i=0}^{m-1} b_i x^i + \sum_{i=0}^{m-2} b_i x^{i+1}$$

$$\sum_{i=1}^{m-1} b_i x^i$$

مقدمة

(1) مقدمة AL (تحلیل زیر)
که $x^{m+1} = b_{m-1} x^m + \sum_{i=0}^{m-2} b_i x^{i+1}$

(2) مقدمة AH (تحلیل زیر)
 $AH = \sum_{i=0}^{m-1} b_i x^i$

آنچه در این دو تحلیل را مشاهده کردیم این است که $x^{m+1} = b_{m-1} x^m + \sum_{i=0}^{m-2} b_i x^{i+1}$ است اما این نتیجه نباید صادق باشد که $x^{m+1} = b_{m-1} x^m + \sum_{i=0}^{m-2} b_i x^{i+1}$ است. این نتیجه در اینجا صادق نمی‌باشد زیرا $b_{m-1} = 1$ است.

لذا این روش بعیدی کند است. این روش $A^2 = AXA$ دارد. در این روش تحلیل AH دارد و از طرف AL نیز دارد.

پس از آنکه AH که مقدمة است. از طرف دیگر این $F(x)$ مقدمة از $\{1, x, x^2, \dots\}$ است. در نظر نگیرید که AH مقدمة از $\{1, x, x^2, \dots\}$ است.

جذر \sqrt{AB} با استفاده از $GF(2^m)$

$$AG GF(2^m), (A)^{\frac{1}{2}} = (\underline{A^{2^m}})^{\frac{1}{2}} = A^{2^{m-1}} \bmod F(x) \quad A = \sum_{i=0}^{m-1} a_i x^i$$

آنچه بتوان خود را درست کرد ممکن

این سوز برای جذر رایه A را درجه 2^{m-1} رسماً نمایند و بحسب زاید در دنباله از پیش دلخواه استفاده کنیم

$$\alpha, \beta \in GF(2^m)$$

$$(\alpha + \beta)^2 = \alpha^2 + \beta^2 \Rightarrow \alpha + \beta = (\alpha^2 + \beta^2)^{\frac{1}{2}} \xrightarrow{\alpha^2 = C, \beta^2 = D} C^{\frac{1}{2}} + D^{\frac{1}{2}} = (C+D)^{\frac{1}{2}}$$

مزون m همراه باس

$$\beta = A^{\frac{1}{2}} = (a_{m-1}x^{m-1} + \dots + a_1x + a_0)^{\frac{1}{2}} \xrightarrow{\text{دان مذکور مزدیدارم}} \text{جزء کشم}$$

$$= [(a_{m-1}x^{m-1} + a_{m-3}x^{m-3} + \dots + a_2x^2 + a_0) +$$

* توان بزرگتر از $\frac{m}{2}$ است اینجا ممکن نموده اند

$$(a_{m-2}x^{m-2} + a_{m-4}x^{m-4} + \dots + a_1x)]^{\frac{1}{2}} =$$

$$= (a_{m-1}x^{\frac{m-1}{2}} + a_{m-3}x^{\frac{m-3}{2}} + \dots + a_2x + a_0) +$$

* $\xrightarrow{\text{Rewiring}} \text{به می باشد.}$

$$x^{\frac{1}{2}} (a_{m-2}x^{\frac{m-3}{2}} + a_{m-4}x^{\frac{m-5}{2}} + \dots + a_1) \xrightarrow{\text{درجه آن } \frac{m}{2} \text{ است}} \text{به می باشد.}$$

نیاز به یک همه عامل است درجه m داریم.

$$x^{\frac{1}{2}} \bmod F(x) = (x^{\frac{m}{2}})^{\frac{1}{2}} = x^{\frac{m-1}{2}} \bmod F(x)$$

برای $\frac{m}{2}$ دلخواه

* $x^2 = x^4 \equiv x(x^3) = x(x+1) = x^2 + x \rightarrow$ از مجموع ممکن است

$$F(x) = x^3 + x + 1 \quad \text{درجه این فرمول ممکن است.}$$

صلح خواهد

Be قیس (1)

$$x^{\frac{1}{2}} \xrightarrow{\text{محاسبه}} B_0 \xrightarrow{\text{محاسبه}} B_0 \xrightarrow{\text{محاسبه}} B_0$$

درجه $\frac{m}{2}$ که ممکن است

Scanned by CamScanner

B_0, B_0

(3)

توان رسانید

RSA

$\rightarrow b$

integrale $\frac{\partial \phi_1}{\partial x_1} dx_1 + \frac{\partial \phi_2}{\partial x_2} dx_2$ \leftarrow DH (regenchange)

$$R_{SA} = \frac{\mu^e m_0 N}{\pi r^2 h}$$

درینه های راهنمایی کارکارا و مساله های مرتبط با آنها در اینجا مورد بررسی قرار نموده است.

$$\text{DH (key exchange)} \Rightarrow a^{e_1} \xrightarrow{\quad} a^{e_2} \Rightarrow \overset{a^{e_1}}{\cancel{a^{e_2}}} \cdot \overset{a^{e_2}}{\cancel{a^{e_1}}} \cdot a^{e_1 e_2}$$

$$E = e_{m-1} \cdot 2^{m-1} + e_{m-2} \cdot 2^{m-2} + \dots + e_1 \cdot 2 + e_0$$

$$\beta^E = \beta^{e_{m-1}} \cdot \beta^{m-1} \beta^{e_{m-2}} \cdot \beta^{2^{m-2}} \cdots \beta^{e_1} \beta^{e_0}$$

$$\beta^E = \left(\dots \left((\beta^{E_{m-1}})^2 \beta^{E_{m-2}} \right)^2 \dots \right)^2 \beta^{E_1}$$

In: BG G and E

$\text{nat}^{\circ}\text{B}^E$

Step 1: $A = B$

Step 2: { ~~dict~~
 ~~list~~

~~2000~~ ~~2000~~

for $i=m-2$ to ϕ

$$A = A^2 \rightarrow H2X$$

$A = A^2$; $\rightarrow H2X \rightarrow$
 $A = A \cdot B$ $e_i \rightarrow$ squaring \rightarrow side channel \rightarrow $e_i = e_i^2$
 $e_i = e_i^2$ \rightarrow $e_i = 1$ \rightarrow $e_i = 1$ \rightarrow $e_i = 1$

side cable
channel

1960 m. - !

$\rho_1 \in H(E)$. 1

Scanned by CamScanner

حال تول (E) با توجه کار K می‌باشد

$$E = E_{t-1} \cdot r^{t-1} + E_{t-2} \cdot r^{t-2} + \dots + E_1 \cdot r + E_0$$

(Laguerre's Zero Radius)

$$r = 2^k, E_i \in \{0, 1, \dots, 2^k - 1\}$$

$$B^E = B^{E_{t-1} \cdot r^{t-1}} \cdot B^{E_{t-2} \cdot r^{t-2}} \cdots B^{E_1 \cdot r} + B^{E_0}$$

$$= \left(- \left((\beta^{E_{t-1}})^r \beta^{E_{t-2}} \right)^r \dots \right)^r \beta^{E_0}$$

Algorithm

Inpat: $B \in G$, int K, E outpat: B^E

Step 1: Pre Computation of B^{E_i} where $E_i < 2^{k-1}$

for $i=1$ to 2^k-1 { $B = \underline{B^{i-1}} B^i$ } $\boxed{B^0 = I}$

Step 2: $A = B^{E+1}$ متوجه شدن از مقدار سایر اندیس‌ها

Step 3: For $i = t-2$ to \emptyset

$$A = A^R \rightarrow \text{جهان از زمین ناردن}$$

$$A = A \cdot B^{E_i} \rightarrow \text{کسر حاصل کرد و اینم را بخواهیم داشت}$$

حالات تقدیر کننده که مطابق باست $A =$ بار است دنباله

متوجه $P-1$ ($t-1$)

$$r=2^k, \quad t = \lceil \frac{m}{k} \rceil$$

ساده دهناری نیست. (ارس ۲۰ حالت)

این روش میتواند با استفاده از PNC Computing Base و DH نسبت به این روش ساده باشد.

بررسی ازاین معملاست

علمیه دهم
(هدف از این محاسبه کاوسن ساخته باش است)

یکی از معاملات اولیه را طور خود نمایی بینت تحلیل که نتایج غیر منطقی باشند و در پرونده است:

$$E_i = 2^{h_i} u_i$$

$$E_i = 2^{h_i} u_i$$

از مجموع الگوریتم

Input: $B \in G$, integer K, E output: B^E

Step 1: $B_0 = 1, B_1 = B, B_2 = B^2$

for $i = 1$ to $2^{K-1}-1$ $\{B_{2i+1} = B_{2i-1} B_2\} \Rightarrow$ تعداد محاسبات نصف شد.

Step 2: Find h_{t-1}, u_{t-1} from $E_{t-1} \rightarrow A = (B_{u_{t-1}})^{2^{h_{t-1}}}$

$$B_{t-1} = B^{h_{t-1} u_{t-1}} = (B^{u_{t-1}})^{2^{h_{t-1}}}$$

Step 3: for $i = t-2$ to 0 جوں کا افزایش آغاز کیا جائے گا.

Find h_i, u_i from E_i

$$A = (A^{2^{k-h_i}} B_{u_i})^{2^{h_i}} = A^{2^k} (B_{u_i})^{2^{h_i}}$$

در اینجا تعداد محاسبه از روشن بگواست.

For $t=5$ سیم سری

کامپیوٹر

$$k=3, E = 1011011100101$$

حال آنکہ اینکا نتیجه نیز اعمال مسروق

کوئی اثر نداشته سب سیم سری در نظر نگیریم که ابتدا داشتار کیز است.

با این نتیجہ

بررسی کل جوں 5 رقم است 5 حذف - انجام موسود. اما در وسیع جدید جوں 4 رقم دارد 4 حذف - 3 انجام داد

وسیع نویں رسانی رسانی (Sliding window) پنجه لفڑی

output: B^E

Input: $B \in G$, integer K, E

Step 1: $B_0 = 1$, $B_1 = B$, $B_2 = B^2$

for $i=1$ to $2^{k-1}-1$ { $B_{2i+1} = B_{2i-1} \cdot B_i$ }

Step 2: $A = 1, i = m - 1$

step 3: while $i \geq 0$ {

$$\int f \quad e_i = \phi \quad \longleftrightarrow \quad \begin{cases} A = A^2 \\ i = i - 1 \end{cases}$$

Lemma: If $\ell \in \mathcal{L}$ and $\ell \neq \ell'$, then ℓ has length $\leq k$.
 Let e_1, e_2, \dots, e_l be the edges of ℓ . Then there exists $i \in \{1, 2, \dots, l-1\}$ such that $e_i = e_{i+1}$.

else ($e_i \neq b$) \rightarrow { ① find the length
and $eL = 1$
وهي تعرف بالـ
② $i = L - 1$
③ $A = A^{2^{i-L+1}}$ $B(s)_2$

منه این روش، بر این مکان مبنی داشت که عموماً بطریق مایلینس بقداد هنر تئاتر نیاز دارد.

جیسے یار دھم:

نمایش اعداد علامت دار

حال اعداد معربیجت باشید و در حال حواهم اعداد علامت دار را هم ساند دھشم.

طبعنا درجین حالن داریم : طبعنا درجین حالن داریم : $(E) \times 10^{\pm n}$ آنچه می‌دانیم را در اینجا 2 رقم علامت دار (Radix-2 signed Digit) نویسیم.

$$E = \sum_{i=0}^{m-1} e_i 2^i, \quad e_i \in \{ -1, 0, 1 \}$$

$$E = (e_{m+1}, e_{m+2}, \dots, e_1, e_0)_{50} \quad \text{دیگر علاست ادار}$$

$$6 = (101_0)_{50} = (1\bar{1}1_0)_{50} \Leftrightarrow 6 = (0110)_2 \quad \text{در مبنای 2}$$

در مبنای 50 سیگنال امداد و نجات داریم. جول در غایبی

حالو تساخا $\left[\begin{smallmatrix} -1 & 2 \\ 2 & -1 \end{smallmatrix} \right]$ عدد داریم سه کوچک

۱۱) $e_{\alpha\beta} = \delta_{\alpha\beta}$ باستعداد زووم دارد آنرا $e_{\alpha\beta}$ باید مزد است.

(NAF) نم عدد همچویز؟

$E = (e_{m-1}, e_{m-2}, \dots, e_1, e_0)$ و در همین همچویز هم عنصر ناپسند کارمزم عنصر همچویز NAF است.

اگر صد - هم در دویست کارمزم همچویز باشد NAF است سوچیج دویست $\Rightarrow \{ \forall i, 0 \leq i \leq m-2, e_i \cdot e_{i+1} = 0 \}$ همچویز عنصر نیست.

نامه حم:

* نمایش NAF بکاربرد صحیح می‌باشد.

* هنر نمایش NAF تغیر من در (نمایه از عنصرها حاصل است)

* مانند هنر نمایش در نمایش NAF در حال حاضر در نمایش با نیاز $m/2$ است (در حال حاضر در نمایش با نیاز $m/3$ است)

* اگر نقدست ما در نمایش در نمایش با نیاز $m/2$ در نمایش NAF حداقل $m+1$ است.

الگوریتم فرآیند در هم NAF

In: $E = (e_{m-1}, e_{m-2}, \dots, e_1, e_0)$

out: $E = (z_m z_{m-1} \dots z_1 z_0)_{BNAF} \rightarrow \text{binary NAF} \rightarrow \text{نحو اعداد را است.}$

step1: $E = (0 e_{m-1} e_{m-2} \dots e_1 e_0)_2 \rightarrow$

step2: $\underbrace{\begin{matrix} e^m \\ 011 \dots 10 \end{matrix}}_k \rightarrow \underbrace{\begin{matrix} e^m \\ 100 \dots 010 \end{matrix}}_{k+1} \rightarrow$ نمایش با نیاز داشتند و همچویز

step3: $i = 0$;

step4: while $i < m$ do {

If $(e_{i+1} e_i = 0) \rightarrow$ نمایش NAF \Rightarrow باید تجربه شود آنرا زدن علاوه بر e_{i+1}, e_i است.

$z_{i+1} = 2e_{i+1} + e_i \rightarrow$ نمایش $11 \rightarrow 0$ و $11 \rightarrow 1$

$z_{i+1} = 0$;
 $i = i + 2$ } در ناتکه رونمایش

else

{
 $z_i = e_i$;
 $i = i + 1$;
}

$$E = \left(d_0 \underbrace{111}_\text{Step 3} \underbrace{011}_\text{Step 2} \circ \underbrace{1}_\text{Step 1} \right)_2 \rightarrow \begin{matrix} \text{Step 2} \\ \text{Step 1} \end{matrix}$$

حدر هم طاھر کشم اور آئو رہا آئے دار ۱۱ → حل بسا سو
۱۰۱ ۰۱ ۰۱ ۰۱ (۱۰۱۰۰۰۱۰۱۰۱) MAF

Step 7: $i = 9$

Step 2: while $E > 0$ do {

If E is odd \rightarrow

$$z_i = 2 - (E \bmod 4)_i \rightarrow$$

else

$$z_i = \phi \circ$$

آرمانیت مزد

$$E = q_2 \cdot 2 + r \rightarrow q_2 = \frac{E - r}{2}$$

اکٹھے مزدیسنا کے خواہ

ڈس سر ۲۴ بیز فج اسٹ

Lat -10° E-8 °

محلی جز $n = E_{\text{mod}} 4$ ۰

مس کو ترازو 311 مس 3 بدرہ آئیں

$$r = 2 - (E \bmod 4)$$

مکالمہ حسابتیں تسلیم کرنے والے بھروسے نہیں۔

$\frac{6}{2}$	خانم	نام
$\frac{3}{2}$	3*	0
$\frac{1}{2}$	1*	1
0	0	1
0	0	0

$$\Rightarrow G = (0110)_2 \Rightarrow \underbrace{0}_{\text{بیت مکانی}} \underbrace{1}_{\text{بیت ایندکس}} \underbrace{1}_{\text{بیت ایندکس}} \underbrace{0}_{\text{بیت مکانی}}$$

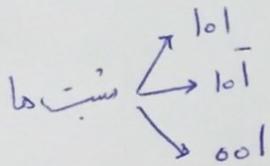
نیست جمل فردس دیگر با استفاده از سیرمه ناید (با اینجا می خواهد اینجا داشته باشد) (در خارج صفت مردم از موافق ناید اینجا داشته باشد)

$$\begin{array}{c}
 \text{خارج الماء} & \text{inside water} \\
 \frac{6}{2} & 3 & 0 \\
 \frac{3}{2} & 2 & \bar{1} \Rightarrow 3 = 2 \times 2 - 1 \cancel{\rightarrow} \\
 \frac{2}{2} & 1 & 0 \\
 \frac{1}{2} & 0 & 1 \Rightarrow 6 = (1, 0, \bar{1}, 0)_{NAF}
 \end{array}$$

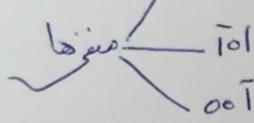
ادغام کردن NAF با تغییر رسانه افر و استفاده از پنجه مترک :

$$K = 3$$

$$E = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix} \right) NAF$$



- تخلص دنگات قبل در محاسبات اولیه جو اهم اهمانه سده میگردد محاسبات
جنبه دارم.



تحا این اعداد نسبت و منخر خواهد داشت

س در محاسبات اولیه باید $B_2, B_3, B_5, B_{-1}, B_{-3}$ حساب کرد و سدر B_2 هم بخواهد

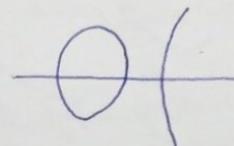
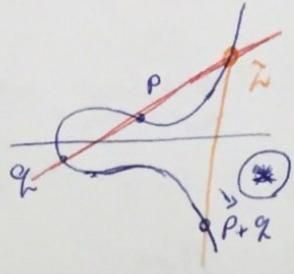
اما اینجا باید B_2 رسم حساب کرد. بعد محاسبه B_2 باید B_2 معلوم شود.

منظر E صور نسبت های که است در NAF در پنجه داریم اما در حالت مدار پنجه داریم که نسبت های NAF هم است نداد پنجه های آن کار نمیکند.

درین مرور NAF نداد پنجه های رنگی نمیکند.

Elliptic Curve Cryptography

حاسه سیم خود را در این کارتر بخواهد



این دو مصطلح در نظر می‌گیریم و داشته باشیم و بخواهیم با هم جمع کنیم

ابتدا نقاط P و Q را وصل کرده و ادامه جمع کا منجز را مجدداً نظر نماییم که در حالت صفرها ادامه دادیم

نمایه داده و می‌شود Point Addition.

این سه نوع از قطعه‌های، مانند نقاطه جم در بخشی متفاوت و کثیر Point Infinity.

این نقطه مانند جم می‌باشد.

این می‌باشد جم بین آن میان میان دو نقطه تابع باشند و در نظر می‌گیریم مجموع داده است.

point doubling

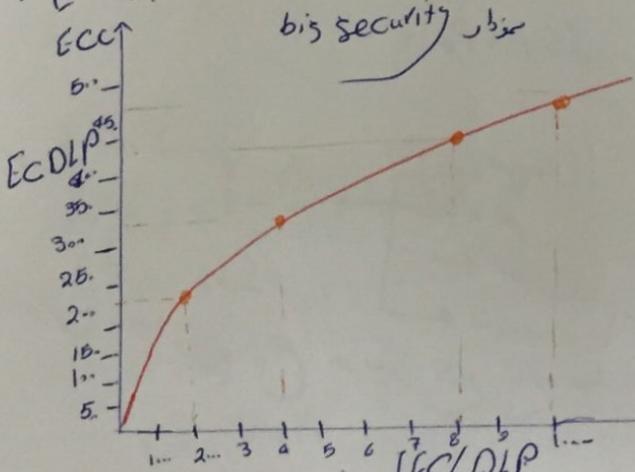
منجز کوئی ندارد بلکه در نظر منجز اول قطعه (نقطه اندیز)

$$\log_Q \alpha = k \rightarrow \text{مشابه کاربری لمسه} \rightarrow \text{Discrete log problem}$$

یافتن k بسخت است

$$\Rightarrow Q = kP \rightarrow \log_P Q = k \rightarrow \text{EC DLP} \rightarrow \text{Elliptic Curve Discrete log problem}$$

bis security



یعنی $\text{EC}(2^{128})$ مقایه $\text{RSA}(4096)$ است

الجیه بحیثی محاسبات در RSA ساده تر است.

اما در حالت پایه سازنر با وضعیت security معادل ECC است

RSA، ساخت چیزی بکرستن کرد (که در ECC بحیثی)

محاسبات داده اما جزو در حالت security میزان شادست هارن از RSA است در حالت میزان شادست ().

ECM: اسکالر دستور پیغام

ایک منحون پیغام مجموعه از ا نقاط است که در معادله $y = mx + b$ می باشد. (نقاط در معادله میتوانند صدق و نداشت) و این معادله در $GF(2^m)$ در نظر گرفته می شود.

$$y^2 + xy = x^3 + \alpha x^2 + \beta \quad \alpha, \beta \in GF(2^m), \beta \neq 0$$

نقطه پیغام $P = (x, y)$ در $GF(2^m)$ می باشد.

اگر E سالم مجموعه نقاط (x, y) باشد که در معادله مذکور صدق نمایند، این مجموعه ممکن است نقطه خارج از نقطه در بخش اول باشد.

$$P_0 + V = I + P = P$$

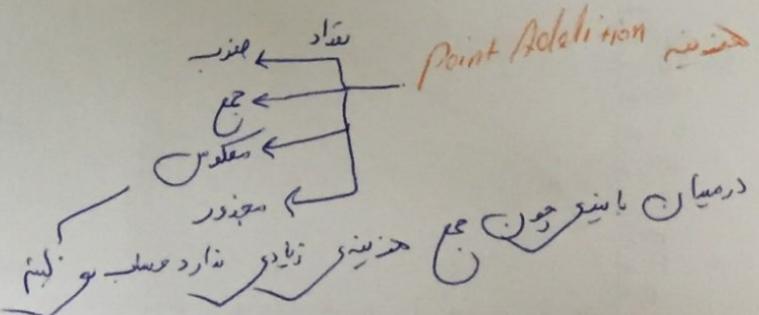
و نقطه خارج قرینه در E باشند داریم:

$$P_0 + P_1 = P_2 = (x_2, y_2)$$

$$x_2 = \begin{cases} \left(\frac{y_0 + y_1}{x_0 + x_1}\right)^2 + \left(\frac{y_0 + y_1}{x_0 + x_1}\right) + x_0 + x_1 + d, & \text{IF } P_0 \neq P_1 \\ x_0^2 + \frac{\beta}{x_0^2} & \text{IF } P_0 = P_1 \end{cases}$$

$$y_2 = \begin{cases} \left(\frac{y_0 + y_1}{x_0 + x_1}\right) (x_0 + x_2) + x_0 + y_0 & \text{IF } P_1 \neq P_0 \\ x_0^2 + (x_0 + \frac{y_0}{x_0}) x_2 + x_2 & \text{IF } P_1 = P_0 \end{cases}$$

$P_0 \neq P_1 \rightarrow \text{Point Addition}$



$$\left(\frac{y_0 + y_1}{x_0 + x_1}\right)^2 + \left(\frac{y_0 + y_1}{x_0 + x_1} * \frac{1}{x_0 + x_1}\right) + \left(\frac{y_0 + y_1}{x_0 + x_1}\right) (x_0 + x_2) + x_0 + y_0 \quad (3)$$

31

Point Addition

$$P_0 = P_1 \quad (P_0 \oplus P)$$

$$\frac{x_0^2 + \beta}{x_0^2} \quad (2)$$

مقدار
مقدار
مقدار

$$x_0^2 + \left(x_0 + \frac{\beta}{x_0} \right) x_2 + x_2$$

$$\frac{x_0^2}{x_0^2}$$

مقدار
مقدار

مقدار 2 مقدار 1 ، مقدار 2

پس از اعداد متساوی باشند حوزه پیچیدگی بسته است.

(یک نقطه هست)

$$Q = kP = \underbrace{(P \cup P \cup \dots \cup P)}_{(n)}$$

عدد متساوی

$$k = (k_{n-1} \ k_{n-2} \ \dots \ k_1 \ k_0) \quad k_i \in \{0, 1\} \quad 0 \leq i \leq n-1$$

$$kP = \left(\sum_{i=0}^{h-1} k_i \cdot 2^i \right) P = (k_{n-1} \cdot 2^{h-1} P) \cup (k_{n-2} \cdot 2^{h-2} P) \cup \dots \cup (k_1 \cdot 2^1 P) \cup (k_0 P)$$

$\underbrace{k_0}_{K_0 \neq 0} \cup \underbrace{O_{2^h}}$

$$= 2 \left(2 \left(2 \dots \left(2(k_{h-1}P) \cup k_{h-2}P \right) \cup \dots \right) \cup k_1P \right) \cup k_0P$$

اینها همانند کوچکترین قسمت های کوچکتر از kP هستند که در آنها $k_i \neq 0$ است

$\rightarrow k_0 = 0 \Rightarrow k_0P = \emptyset$

$\boxed{k = k_0P}$

$\rightarrow k_0 = 1 \Rightarrow kP = P$

Input : P, K Output : $Q = KP$

$$Q = \emptyset;$$

for ($j = h-1$; $j \geq 0$; $j = j+1$) {

$Q = 2Q$; Point Addition و Point doubling

If ($k_j \neq 0$) انجام می شود

$Q = Q + P$; Point Addition و Point doubling

{ اگر بصریت اعداد مستقر باشد در این

جای آن را با k_j بفرمایی تحت از آن ترتیب را داشته باشند.

Input: P , k
 if $i \leq 50$

Output: $Q = kP$

$Q = V$

for ($j = h - 1$; $j \geq 0$; $j = j + 1$) {

$Q = 2Q;$

$IF (k_{j+1} = 1)$

$Q = Q \cup P_j$

else $IF (k_{j+1} = 0)$

$Q = Q \cup (-P_j)$

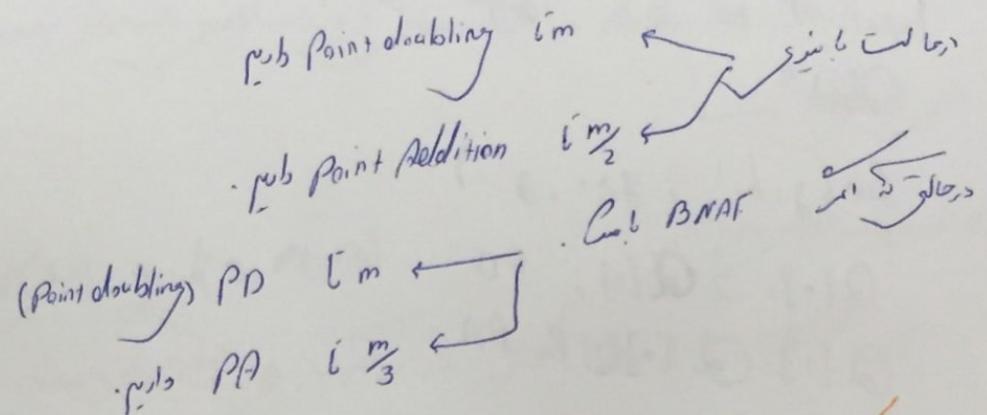
}

$$\boxed{P(x, y) \rightarrow -P = (x, x+y)}$$

حلبیه حیدر دهم

حسابیه سینیه الکترونیک

Q



استادها زعماً وحومات عمليات رعنادی (عزم الورسنه) میز رانه اطلاعات مخفی نظر طرد
حالات کاتل مابغز 2 بزر است.

(SPA) Simple Power Analysis

(DPA) Differential Power Analysis

(SPA) ۱۵ تعلم ساده

$$Q = \emptyset$$

در الورسنه ریبورنس * حسابیه داردیه بستار طرد واسیه است.

for($j=h-1, j\geq 0, j-$) $(-j, 1)$ دلیل وجود حسابیه در هر زیر سطیه بستار طرد (اطلاعات مخفی)

$$Q = 2Q$$

و شکل ۱۴ SPA

If ($k_j \neq \phi$)

$$Q = Q \cup P; *$$

$\xrightarrow{k_j \neq \phi} PD$ $\xrightarrow{k_j = \phi} PD + PA$

کسر میت عاری از PD, PA
دارد نیایر و میان حسابیه میان

مخفی دو حالت دلیلیت کرد

(SPA) Counter measure

اضست پر هزنه لایه دار دستگار طرد اطلاعات مخفی همواره انجام دهیم و بعد سبیه بستار طرد تعیین دهیم.

(SPA RA) (SPA Resistance Algorithm)

Input: P, k ; Output: $Q = kp$

$Q_{[0]}$

for ($j = h-1$; $j > 0$, $j -$)

$Q_{[0]} = 2Q_{[0]}$; PD

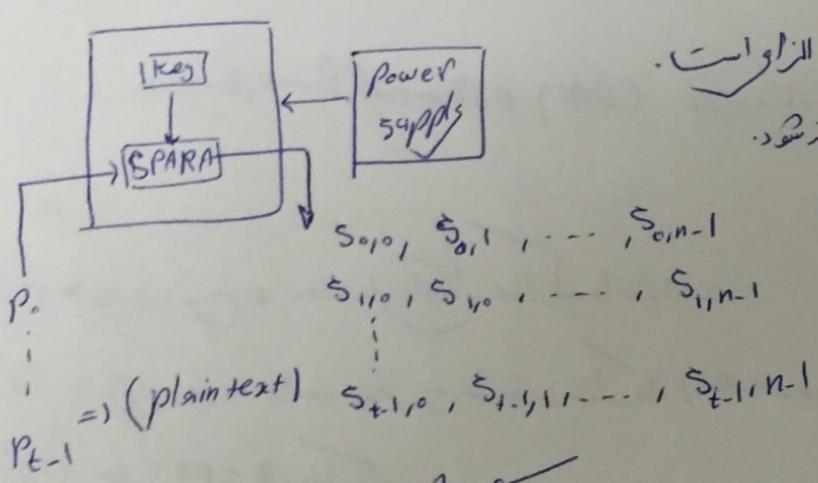
$Q_{[1]} = Q_{[0]} \oplus P$; PA

$Q_{[0]} = Q_{[k_j]}$

$Q = Q_{[0]}$

جزءی از Q علاوه بر $Q_{[0]}$ سایر زیر مجموعات
ما را حساب مقدار k_j داشت $Q_{[0]} \oplus \dots \oplus Q_{[k_j-1]}$ باشد
استال در حساب $Q_{[0]}$

(2) خطای تحلیل مقادیر غایب



خطای تحلیل جایگزین همین متن از الگوریتم الزاوی است.
این خطای تحلیل DPA یک کامپیوچر جیساز در نظر نشده بود.
(Partitioning Function)

$\{Q_{[j]}$
 \Rightarrow plain
text

خطای تحلیل RSARA از توافق بعنوان تابع جیساز در نظر نشده.

* تبار (معنی اینکه تفظیع مختلف محاسبات انجام نموده و با اینکه هر بار متفاوت خواهد شد) n مقدار در هر بار هسته (جایگزین) خواهد بود.

* به صورت سورجینی، فقط این الگوریتم خود را محاسبه عمیم مقدار PF (تابع جیساز) را بدست آورید.
(لازم هست ملیه خود را نهاد)

با توجه به مقدار تابع جیساز که توافد نیاید ناسی سوی مذکور را تغییر داده که در دو مجموعه همراه با یک مثابه

$$S_0 = \{ \{ S_{i,j} \} \mid PF_{P_i} = 0 \}$$

$$S_1 = \{ \{ S_{i,j} \} \mid PF_{P_i} = 1 \}$$

برهان مجموعه از اعضا در مسنه آنقدر مطروح است.

$\beta = \{b_1, b_2, \dots, b_n\}$ مجموعه متمام از عناصر مجموعه α باشد که صورت $s \cdot \beta$ مجموعه متمام باشد.

حکم اعشار β نوشت

در مردم آلمانی داریم:

If $s, t \in D$ Then $\text{gcd}(s, t) = \text{gcd}(s, rt - rs)$ بجز $\text{gcd}(s, r, t)$ در ترکیب تنظیم است. این عبارت همان روش فرمایش در محاسبه gcd است.

با این روش بسیار سریع است. gcd طبق صورت متداول تغییر نمود. (هنر روش به عنوان روش محاسبه آلمانی مطرح شده است).

الgoritم - الگوریتم محاسبه -

Input: $a, b \in D$ & $g(a) \gg g(b)$

output: $d = \text{gcd}(a, b)$

step 1: $r_1 = a$; $r_0 = b$, $i = 1$

step 2: do 1

$i = i + 1$

If $g(r_i)(g(r_{i-1}))$ Then $r_i = r_{i-2} - \frac{r_i}{r_{i-1}} \cdot r_{i-1} \Rightarrow$ اگر r_i در مجموعه D باشد سپس $g(r_i)(g(r_{i-1}))$ بشه

{ while ($r_i \neq 0$);

step 3: $d = r_1$

$\text{gcd}(84, 54)$:

51: r_1 , $r_0 = 54$ $i = 1$

52: $d = r_3 = 6$

i	$r_i = r_{i-2} - \frac{r_i}{r_{i-1}} \cdot r_{i-1}$
1	$30 = 84 - 1 \times 54$
2	$24 = 54 - 1 \times 30$
3	$6 = 30 - 1 \times 24$
4	$0 = 24 - 4 \times 6$

میانلاین مجموع در هر مجموعه S_1, S_2 اگر $\text{Av}_m(S_1) > \text{Av}_m(S_2)$ باشد میتوانیم $\text{Av}_m(S_1) - \text{Av}_m(S_2)$ را مقدار فاصله بین S_1 و S_2 نامید. تابع f اگر دو مجموعه S_1, S_2 را میخواهد مقدار $\text{Av}_m(f(S_1)) - \text{Av}_m(f(S_2))$ را مقدار فاصله بین $f(S_1)$ و $f(S_2)$ خواهد داشت. دست مدل توانی که رفتته بوده تعداد P_i را کجا میتوانند.

جدول ماتریس DPA را ECC است که اینها به همراه تکمیلی خود دارند. پس بجز مقدار 28 256 بایز است تا ECC را بسیاری از مسائل رالستی میباشد است ذهن تعلیل و ذهن در تعلیل و spike شوند اینها در دست DPA ماده بنوده است.

که صفت ماتریس DPA : $DPA = DPA^T$ صفت و که این معنی دارد DPA سفت ماتریس DPA است. (چون بقدر trace بزرگتر نیاز دارد) این مفهوم را میتوان اینها است به این طبیعه (۱) بعد از مرکز محاسبه صدراست اسکالر بطریق تهاب از عرض سود (در جایز) حوز محاسبات درست مانند Euclidean Domain که (آنها را) به که مقدار مستقر در حالت تنافی محکم میشوند. همچنان از نماینده از متفاوت در جایز که عدد در SD نماینده داده شده باشد. نماینده در SD میتواند در مجموع 50 میله موقن به 3 میله بزرگ باشد.

حلسه پنجم

Euclidean Domain

دانش آموز

مجموعه D مجموعه $(+, \cdot)$ داشته اند و است بطریق $a, b, c \in D$, $a \neq 0$, $ab = ac \Rightarrow b = c$

خاصیت توسعی پذیر است به $+$

از اینها (Z) و محدود است باشد این نماینده داده شوند

لطفاً برای اینها $a, b, c, d \in D$ میتوانند بمعنی $b = d$ باشند

لطفاً اگر n درجه f باشد و در آنها $g(n) = \deg f$

نحوه درس کنتم سه بحث در درس محاسبه برمیگشت. درس بحث است

i	$r_i = r_{i-2} - q_i \cdot r_{i-1}$
1	$\frac{-24}{r_1} = 84 - 2 \times \frac{54}{r_0}$
2	$6 = 54 - (-2) \times (-24)$
3	$0 = -24 - (4) \times 6$

جواب $g(n)$ میباشد جو $g(r_i) / g(r_{i-1})$ قدر مطلق دینامیک است این $g(r_3) = 24$ $(g(r_2) = 54)$

درین درس باید صلحه بجهاب رسید

الgoritam یعنی چیزی باشه

درین درس علاوه بر gcd که در الگوریتم مطابق خواهد بود، ترکیب منظره a, b, q ایجاد شده، نیز معتبر خواهد بود.

Input: $a, b \in D$, $g(a) \gg g(b)$ output: $d = gcd(a, b)$, a', b' such that
 $a \cdot a' + b \cdot b' = d$
 ترکیب منظره a, b, q ایجاد شده.

step1: $r_{-1} = a$, $r_0 = b$, $s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$, $t_0 = 1$, $i = 1$

step2: do {

$i = i + 1;$

If $g(r_i) < g(r_{i-1})$ Then $r_i = r_{i-2} - q_i \cdot r_{i-1}$

$s_i = s_{i-2} - q_i \cdot s_{i-1}$

$t_i = t_{i-2} - q_i \cdot t_{i-1}$

{while ($r_i \neq 0$)

step3: $d = r_{i-1}$

$a' = s_{i-1}$

$b' = t_{i-1}$

$gcd(84, 54), a', b'$

لطفاً

step1: $r_{-1} = 84$, $r_0 = 54$, $s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$, $t_0 = 1$, $i = 1$

i	q_i	r_i	s_i	t_i
-1	-	84	1	0
0	-	54	0	1
1	1	30	1	-1
2	1	24	-1	2

i	q_i	r_i	s_i	t_i
3	1	6	2	-3
4	4	0	-9	14

$$\text{Step 3: } d=6, a'=2, b'=-3 \quad \frac{2 \times 84 - 3 \times 54}{a' \quad a' \quad b' \quad b'} = \frac{6}{d}$$

الورقة هار معاشر ملخص

1) $A \in GF(2^m)$
معرفه بردار مرسان
جودت ساز
 $\Rightarrow A = A^{2^m} \times A^{-2} \rightarrow A^{-1} = A^{2^m-2}$
که درست است که عدد طبقات 2^m-2 مساوی است
(معروض توان رسانه های متعارف ناچیز است زیرا علاوه بر توان (سلوژاره).

2) If $A \cdot B = 1 \pmod{F(x)}$ Then $A^{-1} = B \pmod{F(x)}$

برای B, A
جودت ساز

$$\begin{bmatrix} 1 & B \\ A & 1 \end{bmatrix} \begin{bmatrix} F(x) \\ B \end{bmatrix} = 1$$

برای $A \cdot B = 1 \pmod{F(x)}$ به صورت ماتریس نوشته

ازین طریق میتوانیم از دو خط A^{-1} حساب کنیم

3) EEA (Extended Euclidean Algorithm)

$A(x), B(x) = 1 \pmod{F(x)}$
 $\downarrow A(x)B(x) + F(x)C(x) = 1 \Rightarrow$ اثبات برای $F(x), C(x) = 1 \pmod{F(x)}$
 حل مبارت بالا خواهد بود.

If $\gcd(F(x), A(x)) = 1$ Then \Rightarrow can calculate the $B(x), C(x)$

این EEA نتیجه باشید $\gcd(F(x), A(x)) = 1$ است. سه استعداد از $F(x)$ و $A(x)$ و $B(x)$ میباشد.

Input: $F(x)$, $A(x) \neq 0$ output: $B(x) = A^{-1}(x) \pmod{F(x)}$

Step 1: $R^{(-1)}(x) = F(x)$, $R^{(0)}(x) = A(x)$
 برای درجه اول را برای $F(x)$ مبارزه کنیم.
 $A(x) = R^{(0)}(x) \cdot F(x)$, $F(x)$ نویسید از دو دو
 جزو دارد.

32

$$\deg U^{(i)}(x) + \deg R^{(i-1)}(x) = m \implies \text{لطفاً درجه رجبيست} \quad R^{(i-1)}, U^{(i)} \in \mathbb{C}^m$$

باينه داشت. اين مرضن به حالت 4 بات مبارزه باشند.

$$\begin{matrix} U^{(i-1)} & U^{(i)} \\ R^{(i-1)} & R^{(i)} \end{matrix}$$

$$\deg U^{(i)}(x) + \deg R^{(i)} < m$$

از اينجا همچو باشد

باشد $\deg U^{(i-1)} + \deg R^{(i-1)} < m$

رسونانه درجه رجبيست m باشند

$$\begin{array}{c} Lsb(U) \downarrow \quad Lsb(R) \downarrow \\ \boxed{\begin{array}{|c|c|} \hline U^{(i-2)}(x) & R^{(i-2)}(x) \\ \hline \end{array}} \\ Lsb(U) \quad MSB(U) \quad MSB(R) \end{array}$$

حول حسب shift در دو نوبت

دو باره حسب نوبت باعث شد

باينه $Lsb(R)$ با $Lsb(U)$ فرسيم

با $MSB(R)$ با $MSB(U)$ فرسيم

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

حال آندر shift با $R^{(i-1)}(x)$ و $U^{(i-1)}(x)$ باعث شد

$$\deg R^{(i-1)}(x) = R^{(i-2)}(x) + Q^{(i)}(x)R^{(i-1)}(x)$$

در خط

لطفاً $Q^{(i)}$ را اسماً دهیم.

باينه اين منظر را پنهان به طل علاوه بر $U^{(i-1)}(x)$ و $R^{(i-1)}(x)$ داشتند.

$$\begin{array}{r} 1010111 \\ \times 101 \\ \hline 100 \\ \hline \end{array}$$

$$m=4 \quad \text{پنهان 4 اعداد} \quad (d)$$

$$LUT[k] = g - 1 - \lceil \log_2 k \rceil$$

$$1 \leq k \leq 2^g - 1$$

طول زنجير است

باينه از طول 9 باشند.

تا پنهان آخوند بطول 9 باشند.

باينه از طول 9 باشند.

$$U^{(1)}(x) = 0, \quad U^{(0)}(x) = 1, \quad i=0$$

تحاصل على مراتب $B(x)$
معاسبة فرط

step 2: do {

$$i = i + 1;$$

$$Q^{(i)}(x) = \left\lfloor R^{(i-2)}(x) / R^{(i-1)}(x) \right\rfloor *$$

$$R^{(i)}(x) = R^{(i-2)}(x) - Q^{(i)}(x) \cdot R^{(i-1)}(x)$$

جمع دو قسم در حین عملیات

$$U(x) = U^{(i-2)}(x) + Q^{(i)}(x) \cdot U^{(i-1)}(x)$$

{ while ($R^{(i)} \neq 0$)

step 3: $B(x) = U^{(i-1)}(x)$.

چون $i=4$ است
چون $R^{(i)} = 0$ است
چون $U^{(i-1)}$ باقیمانده است

عملیات این روش ها 4 جبریست مقدار دنیاز و تقسیم هم موجود در خط * است که سبب تسریع در این جمع دو قسم در حین عملیات

امنت

حلبیه بازدید همچو

$$Q^{(i)}(x) = \left\lfloor R^{(i-2)}(x) / R^{(i-1)}(x) \right\rfloor$$

$$\text{degree } R^{(i-1)}(x) = \text{degree } R^{(i-2)}(x) - \text{degree } Q^{(i)}(x) \Rightarrow$$

حال صورت

$$= \text{degree } R^{(i-3)}(x) - \text{degree } Q^{(i-1)}(x) - \text{deg } Q^{(i)}(x)$$

+ جمله بیشتر

$$= \text{degree } R^{(-1)}(x) - \sum_{j=1}^i \text{deg } Q^{(j)}(x)$$

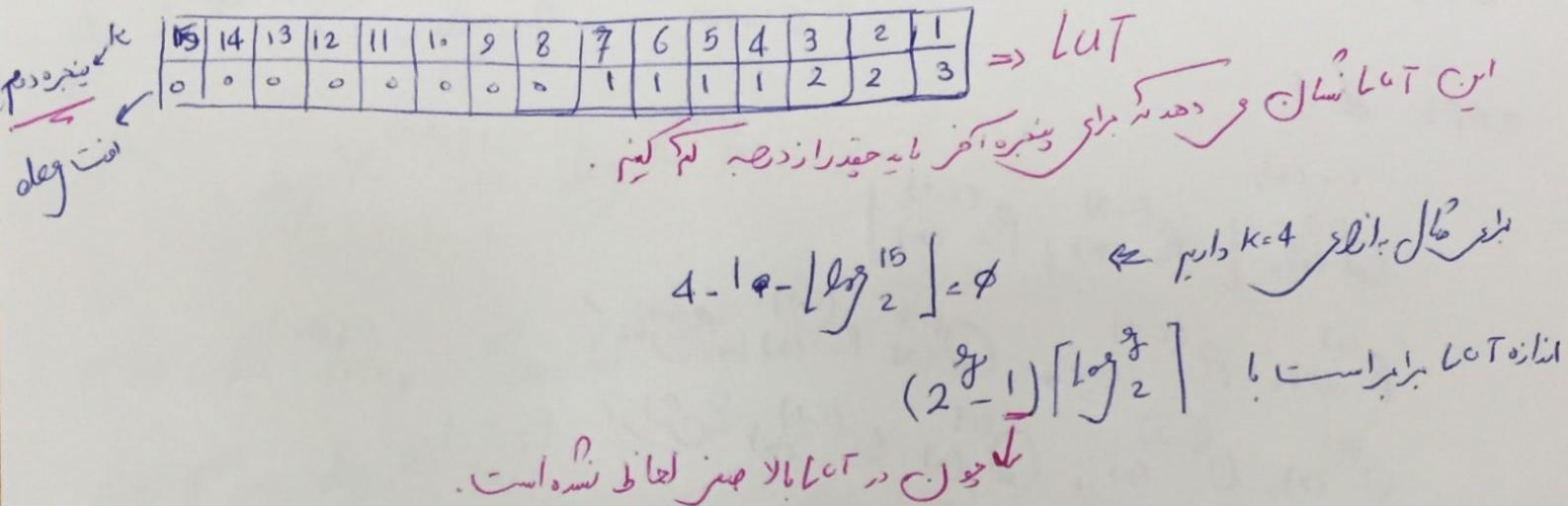
این مجموع

$$\text{deg } U(x) = \text{deg } U^{(i)}(x) + \text{deg } Q^{(i)}(x) = \text{deg } U^{(i-2)}(x) + \text{deg } Q^{(i-1)}(x) + \text{deg } Q^{(i)}(x) =$$

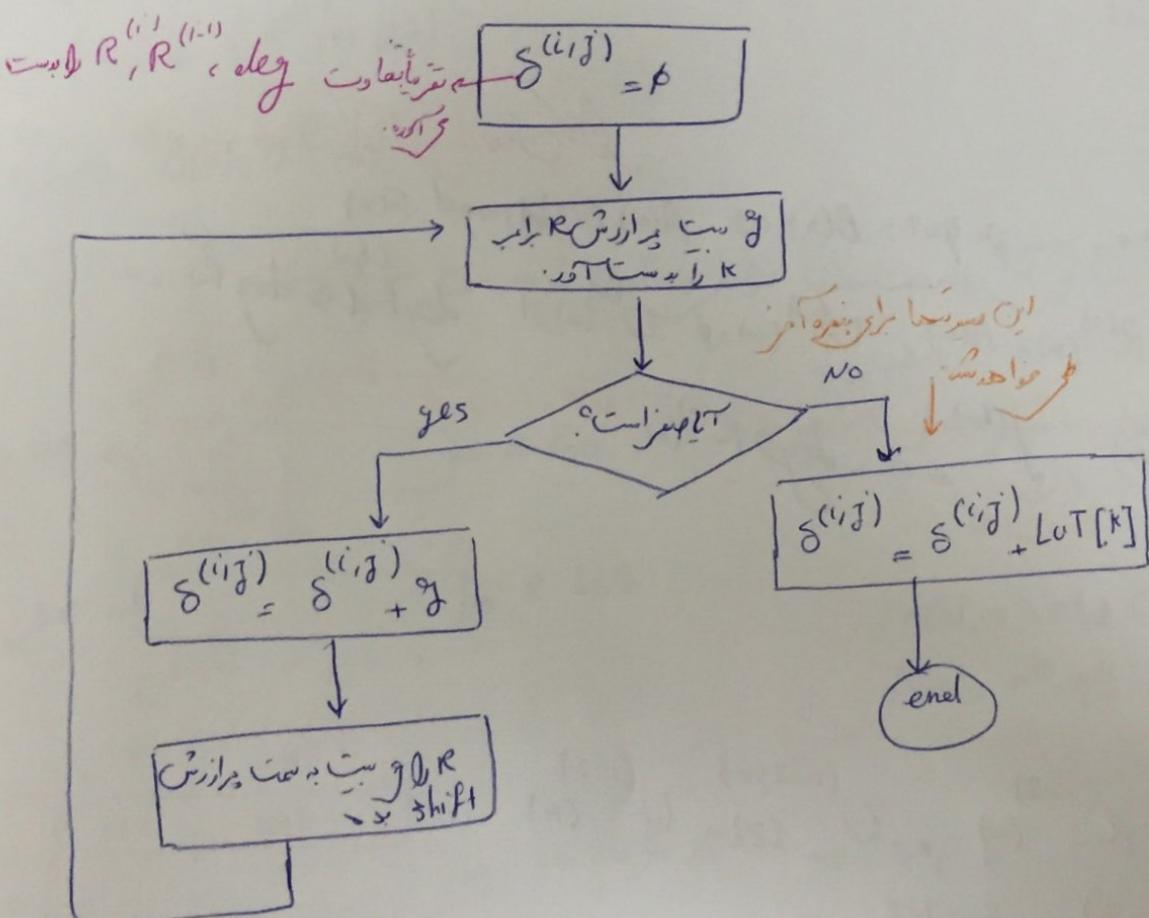
$$= \left[\text{deg } U(x) + \sum_{j=1}^i \text{deg } Q^{(j)}(x) \right]$$

۴۱

اگر دستور $R \leftarrow R \cdot K$ که طول آن را و است هم و سیت حاصل نیست باید بمانده g از $\deg LUT$ کم باشد.



الgoritم در مساله دیگر با این روش



مهمة سائر دھم بـ الـ

Step 1: $R^{-1}(x) = F(x)$, $R^0(x) = A(x)$, $U^{(-1)}(x) = \emptyset$, $U^0(x) = 1$

Step 2: do {

$$i = i + 1;$$

$$Q^{(i)}(x) = \left\lfloor R^{(i-2)}(x) / R^{(i-1)}(x) \right\rfloor$$

$$R^{(i)}(x) = R^{(i-2)}(x) + Q^{(i)}(x) R^{(i-1)}(x) \rightarrow R^{(i)}$$

$$U^{(i)}(x) = U^{(i-2)}(x) + Q^{(i)}(x) \cdot U^{(i-1)}(x) \rightarrow U^{(i)}$$

{ while ($R^{(i)}(x) \neq 0$)

Step 3: $B(x) = U^{(i)}$

القسم المتبقي من الباقي

Input: $F(x), A(x) \neq 0$. Output: $B(x)$ s.t. $A(x) \cdot B(x) \equiv 1 \pmod{F(x)}$

Step 1: $R^{(-1)} = F(x)$, $R^0(x) = A(x)$, $U^{(-1)}(x) = \emptyset$, $U^0(x) = 1$, $\deg R^{(-1)}(x) = \deg R^0(x) = m$

Find $\deg R^{(i)}(x)$, $\text{if } \underline{\text{deg}} = m - \deg R^0(x) \text{ find } \underline{\text{deg}} R^{-1}(x)$
else $\underline{\text{deg}}$

Step 2: do {

$$i = i + 1;$$

$$j = 0;$$

$$R^{(i-2, j)}(x) = R^{(i-2)}(x), U^{(i-2, j)}(x) = U^{(i-2)}(x)$$

* while ($\alpha^{(i, j)} > 0$) do {

$$R^{(i-2, j+1)}(x) = R^{(i-2, j)}(x) - \alpha^{(i, j)} R^{(i-1)}(x) \rightarrow R^{(i-2, j+1)}$$

$$U^{(i-2, j+1)}(x) = U^{(i-2, j)}(x) + \alpha^{(i, j)} U^{(i-1)}(x) \rightarrow U^{(i-2, j+1)}$$

Q $j = j + 1$

43 Find $\delta^{(i,j)}$ from LUT: \rightarrow الگوریتم مهاسنیتی بارز

$$\deg R_{(n)}^{(i-2,j)} = \deg R_{(n)}^{(i-2,j-1)} - \delta^{(i,j)}$$

$$d^{(i,j)} = \deg R_{(n)}^{(i-2,j)} - \deg R_{(n)}^{(i-1)}$$

$$R_{(n)}^{(i)} = R_{(n)}^{(i-2,j)} \text{ if } U_{(n)}^{(i)} = U_{(n)}^{(i-2,j)};$$

$$\deg R_{(n)}^{(i)} = \deg R_{(n)}^{(i-2,j)}; \quad \text{عوینت کل حفظ شاهزاده}$$

$$\deg d^{(i+1,0)} = -d^{(i,j)} \Rightarrow \text{معادله معکوس}$$

while ($R_{(n)}^{(i)} \neq 0$)

$$\text{step 3: } B(n) = U_{(n)}^{(i-1)}.$$

واعد کردن در عبارت خصوصاً هنالک \sum بحث است امداد سودا زدن تقریر سدید برآست.

$$U_{LSB} \leftarrow \boxed{\begin{array}{|c|c|} \hline & 1 \\ \hline \end{array}} \leftarrow R_{LSB}$$

: دقت رفتار shift داد طبق میسر و طول R است خواهد بود

$$U_{LSB} \leftarrow \boxed{\begin{array}{|c|c|} \hline & 1 \\ \hline U_{(i-2)} & R_{(i-1)} \\ \hline \end{array}} \rightarrow R_{LSB}$$

$$A(n) = x^3 + x^2 + 1 \in GF(2^5)$$

$$f_r(n) = x^5 + x^2 \quad g = x^2$$

$$\begin{matrix} i=1 \\ j=1 \end{matrix} \left\{ \begin{array}{|c|c|} \hline 100 & 100101 \\ \hline U_{(i-1)} & R_{(i-1)} \\ \hline 0 & 1110 \\ \hline \end{array} \right. \Rightarrow \text{initialization} \Rightarrow \text{step 1}$$

دو نامنابه دیگر داشته باشند $R_{(i-1)}, R_{(i-1)}$ (deg $d^{(i,j)}$)
معکوس شود.

$$\begin{matrix} i=1 \\ j=1 \end{matrix} \left\{ \begin{array}{|c|c|} \hline 100 & 11101 \\ \hline 001 & 1110 \\ \hline \end{array} \right. \rightarrow \text{دو نامنابه داشته باشند shift } U_{(i-1)}$$

کنایه deg آنها
است هموزن سبب است
و زاده (100)



$i=2$	$j=1$	<table border="1"> <tr><td>100</td><td>1</td></tr> <tr><td>011</td><td>1110</td></tr> </table>	100	1	011	1110	شادت داریم نمایستادن مرتباً رکم	بر این اتفاق نه کس نمی‌داند دست سوکا.
100	1							
011	1110							
$i=2$	$j=0$	<table border="1"> <tr><td>011</td><td>1110</td></tr> <tr><td>100</td><td>1</td></tr> </table>	011	1110	100	1	شادت داریم (و سفید و صفر)	
011	1110							
100	1							

$i=2, j=1$	<table border="1"> <tr><td>011</td><td>0110</td></tr> <tr><td>100011</td><td>1</td></tr> </table>	011	0110	100011	1
011	0110				
100011	1				

$i=2, j=2$	<table border="1"> <tr><td>011</td><td>10</td></tr> <tr><td>100101</td><td>1</td></tr> </table>	011	10	100101	1
011	10				
100101	1				
$i=2$	<table border="1"> <tr><td>011</td><td>10</td></tr> <tr><td>101001</td><td>1</td></tr> </table>	011	10	101001	1
011	10				
101001	1				

$$\beta(x) = \bigcup_{(011)}^{(1)} = x^2 + x$$

$$A(x) \cdot B(x) \equiv 1 \pmod{F(x)} \implies (x^2 + x)(x^3 + x^2 + x) \equiv x^5 + x^4 + x^3 + x^2 \equiv 1 \pmod{F(x)}$$

امام الدرس

کلاس امیر حبیب‌زاده در این مقاله
بررسی کرد، $\mathbb{Z}_7[x]$ و $\mathbb{Z}_{11}[x]$ را بررسی کرد.

سایر بلاگ‌واری

حاسوب حملة حمل

(AJA) Almost Inv. Algorithm

Input: $A \in GF(2^m)$, $F(x)$

Output: β & k s.t. $x^k = A \cdot B \bmod F(x)$

الgoritم ملخص تعریف

دراخوا است بعین دل ملکس طبقه تعریف تسلیمه.

step 1: $U=A$, $V=F$, $B=I$, $C=\emptyset$, $k=0 \rightarrow$ initialization $x=0, y=1$

step 2: while U is a factor of x do {

$$U=U/x, C=C/x, k=k+1, x=x+y$$

step 3: If $U=I$ then return(β, k) \rightarrow

اعمال الورث

step 4: If $\deg(U) < \deg(V) \Rightarrow U \leftrightarrow V, B \leftrightarrow C, x \leftrightarrow y$

step 5: $U=U+V, B=B+C$ \rightarrow اعمال الورث، x, y نسباً مثلثيّة

step 6: Go to step 2

طريق صریح الورث

$$x^k U = BA + XF \rightarrow A = I * A + 0 \Rightarrow$$

$$x^k V = CA + YF \rightarrow F = 0 + F \Rightarrow$$

برهان راست

العلام بالس در step 3 در $y=1, z=0$

ابتدا در الورث

$$A = I * A + 0 \rightarrow x^k = BA + QF \Rightarrow$$

دالع اساساً ملحوظ راست

$x \leftrightarrow y$ in step 4 در $y=y \cdot n$ باشد initial, step 1, $x=x+y$ در step 5

دوسن کا استو - اسٹر (بدون درستگاری متن بیان (کاہر پیا زندگی سو ماجولار نیست))
 همین مرض کی $m=2^t$ و t عدد طبعی است. (کام 2^t بود)
 باعذارہ لازم انجام در ہم ناسط برقرار رہے (Zero padding)

$A = \text{telegr}_{\frac{m}{2}} \text{ از } \text{telegr}_{\frac{m}{2}} \text{ میسر است و صفت } A \text{ کا } \text{telegr}_{\frac{m}{2}} \text{ میسر است تھیں کہ } A \text{ کا } \text{telegr}_{\frac{m}{2}}$

$$A = x^{\frac{m}{2}} (a_{m-1} \cdot x^{\frac{m}{2}-1} + \dots + a_{\frac{m}{2}}) + (a_{\frac{m}{2}-1} \cdot x^{\frac{m}{2}-1} + \dots + a_0) \Rightarrow$$

$$\underbrace{x^{\frac{m}{2}}}_{\text{کام } m=2^t} \underbrace{a_{m-1}, \dots, a_{\frac{m}{2}}}_{A_H} \quad \underbrace{a_{\frac{m}{2}-1}, \dots, a_0}_{A_L}$$

$$A = x^{\frac{m}{2}} A_H(x) + A_L(x)$$

$$B = x^{\frac{m}{2}} B_H(x) + B_L(x)$$

$\boxed{\text{eleg}(A_H, A_L, B_L, B_H) \leq \frac{m}{2}-1}$ کام بذکر است کہ

level one
 $D_0(x) = A_L \cdot B_L$

$$D_1(x) = [A_L + A_H] [B_L + B_H] = A_L \cdot B_L + A_H \cdot B_L + A_L \cdot B_H + A_H \cdot B_H \Rightarrow A_H \cdot B_L + B_H \cdot A_L = D_1 - D_0 - D_2$$

$$D_2(x) = A_H \cdot B_H$$

لیکن D_1, D_2, D_0 کو جمع کر کر $D_1 + D_2 + D_0 = A \cdot B$ کا حاصل کریں گے

$$D(x) = \frac{D_0(x)}{A_L \cdot B_L} + x^{\frac{m}{2}} \left[\frac{D_1(x)}{A_L \cdot B_H + B_L \cdot A_H} - \frac{D_2(x)}{A_H \cdot B_H} \right] + x^m D_2(x)$$

لیکن D_2, D_1, D_0 کو جمع کر کر $D_1 + D_2 + D_0 = A \cdot B$ کا حاصل کریں گے

بایکاری $\frac{m^2}{4}$ از بحیرہ میں کا نہ سہاست.

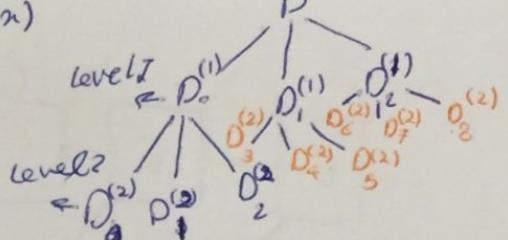
اما هنوز $O(A \cdot B)$ مان m^2 است. حال آنکه قبل از این به همین دقت باشد D_0, D_1, D_2 نام بروش قبل از این به همین دقت باشد (And) است.

با این ترتیب داریم

$$D_0^{(1)}(x) = D_0^{(2)}(x) + x^{\frac{m}{4}} \left[D_1^{(2)}(x) - D_0^{(2)}(x) - D_2^{(2)}(x) \right] + x^m D_2^{(2)}(x)$$

$$D_1^{(1)}(x) = D_3^{(2)}(x) + x^{\frac{m}{4}} \left[D_4^{(2)}(x) - D_3^{(2)}(x) - D_5^{(2)}(x) \right] + x^m D_5^{(2)}(x)$$

$$D_2^{(1)}(x) = D_6^{(2)}(x) + x^{\frac{m}{4}} \left[D_7^{(2)}(x) - D_6^{(2)}(x) - D_8^{(2)}(x) \right] + x^m D_8^{(2)}(x)$$



$$\deg D_i^{(2)} < \frac{m}{4} \quad (\text{در مرحله بايد بجزء را برسد.})$$

آخر به همین ترتیب ادامه دهنده جزو مرحله خواهد بود. $t = \log_2^m$ است جزو مرحله

$$\boxed{\# \text{mult} = 3 \log_2^m} \quad \leftarrow \begin{array}{l} \text{3 صندوق در مرحله قبل است. در مقاسی داریم} \\ \text{هر 3 جزو میتوان به } \frac{m}{2} \text{ جزو برسد.} \end{array}$$

در مرحله در صندوق در مرحله قبل به 3 صندوق تقسیم شود و جزو درخت ساخته داده شد. $t = \log_2^m$ است

$$\# \text{mult} = 3 \log_2^m$$

\Leftrightarrow با این روش ما صندوق در $GF(P)$ داریم (آخر $GF(2)$ باشد) $t = \log_2^m$ است

$$\# \text{mult} = 3 \log_2^m = m \log_2^3 \quad (\text{با این روش زیر مجموعه شده (از Sub-quadratic)}} \quad \text{با این روش میتوان به } \frac{m}{2} \text{ صندوق برسد.})$$

$$A = A_H A_M A_L \quad (\text{با این روش میتوان به } \frac{m}{2} \text{ صندوق برسد.})$$

$$A = x^{\frac{2m}{3}} \cdot A_H + x^{\frac{m}{3}} A_M + A_L \quad (\text{با این روش میتوان به } \frac{m}{2} \text{ صندوق برسد.})$$

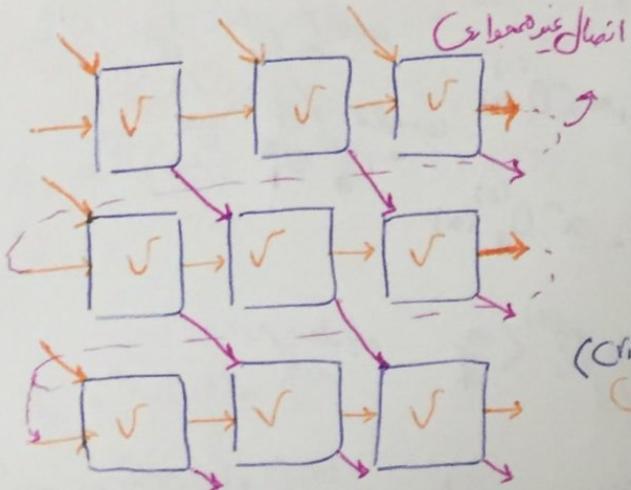
حاسوب های جیبی

Systolic

محاسبه سیستولیک

محاسبه کردن راهنمایی دارند.

سیستولیک pipeline دو بیان



محاسبه محاسبه سیستولیک مسیر از تراول سلول است. در محاسبه سیستولیک ایدئال، هم‌آمیز سلول مابین این سلول‌ها با سلول های هم‌جوار ارتباط دارند. (دجالت ایدئال). سلول مابین های این سلول‌ها تراول

(Critical Path Length) CPL

نامیده می‌شوند.

به نسبت تعداد سلول مکاهش یا به سفر در آن می‌توان سرمه

اندروابط سلول های هم‌جوار کمینه سیستولیک (semi-systolic) نامیده می‌شود.

اگر سمت هم‌جوار برقرار باشد اما سلول مابین نباشد، آن محاسبه سیستولیک نباشد. مسیر سلول نزدیکی (proximity) طبقه بندی (classification) افزایش خواهد داشت.

مثال:

اگر صد ب لایه صورت ماتریس بیوسیم و تراست ب صورت

$$A(x), B(x) \in GF(2^3)$$

$$A(x) = a_0 + a_1 x + a_2 x^2$$

$$B(x) = b_0 + b_1 x + b_2 x^2$$

$$f(x) = x^3 + x + 1$$

$$C = A(x) \cdot B(x) \bmod f(x)$$

$$= b_0(a_0 + a_1 x + a_2 x^2) + [b_1 x(a_0 + a_1 x + a_2 x^2) + b_2 x^2(a_0 + a_1 x + a_2 x^2)] \bmod f(x)$$

جول تغییر دهنده انتقال خواهد
بود $\bmod f(x)$ نباشد.

49

$$= b_0(a_0 + a_1x + a_2x^2) + \left[\underbrace{\left(b_1(a_0x + b_1a_1x^2 + b_1a_2x^3) \right) \bmod \Sigma(x)}_{\overbrace{b_1a_0x + b_1a_1x^2 + b_1a_2(x+1)}} \right] +$$

$$b_1(a_2 + (a_0 + a_1)x + a_1x^2)$$

$$+ b_2(a_1 + (a_2 + a_1)x + (a_0 + a_2)x^2)$$

طريق سهل

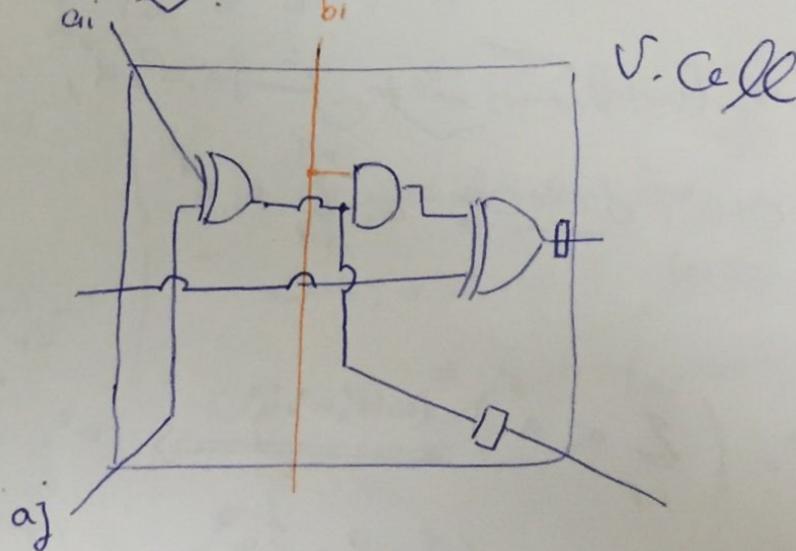
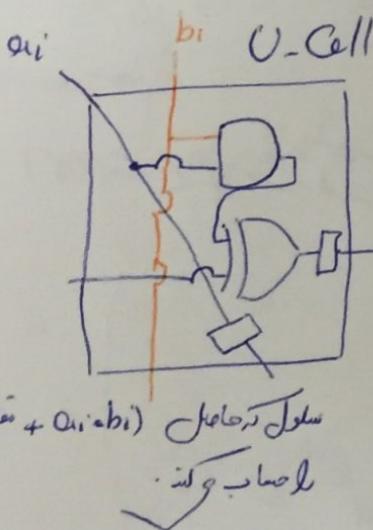
$$= (b_0a_0 + b_1a_2 + b_2a_1) + x(b_0a_1 + (a_0 + a_2)b_1 + b_2(a_2 + a_1)) + x^2(b_0a_2 + b_1a_1 + b_2(a_0 + a_2))$$

مقدار جزء مترافق

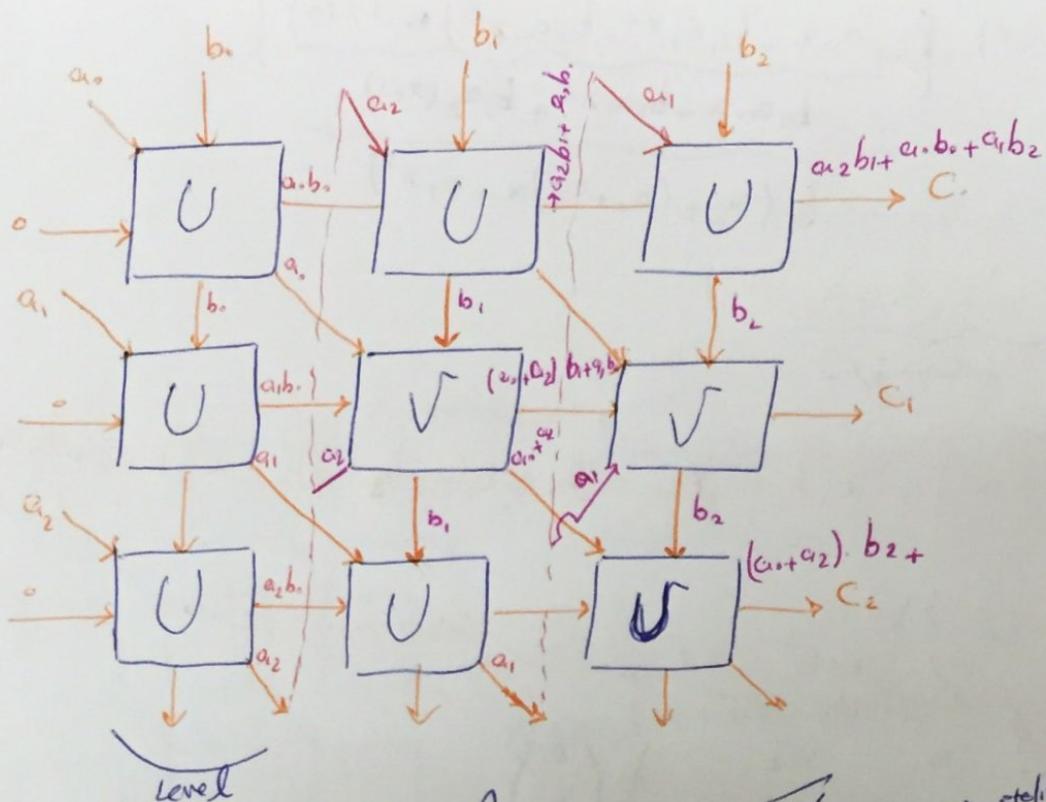
$$C = \begin{pmatrix} C_0 \\ C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_0 + a_1 & a_1 + a_2 \\ a_2 & a_1 & a_0 + a_2 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix}$$

این مجموعه از تابعیت دارد که xR تابعیت باشد

این مجموعه از تابعیت دارد که $(a_i, b_j) + (a_k, b_l)$ باشد



ناتایلر خواهیم داشت.



نموداری از متریک روتینی (semi-systemic) FFZ که ممکن است معاوی خواهد بود. نایابان مفهومی ما تازه زار. جول از طبقه کلی آنهاست که ممکن است مذکور شده در این درست تبلیغاتی level متریک که معاوی باشد.

جلوی ریتم.

حل سیفر دهم

مسئلہ مختصر باشند پایه مندرجہ طبقہ مذکور میں مذکور نامہ.

$$\alpha \in GF(2^m) \quad \text{نایاب} \quad \alpha = \sum_{i=0}^{m-1} a_i \alpha^{2^i}$$

$a_i \in GF(2)$

$$\alpha^2 = \left(\sum_{i=0}^{m-1} a_i \alpha^{2^i} \right)^2 = \frac{(a+b)^2 = a^2 + b^2}{\text{پسندیده}} \Rightarrow \alpha^2 = \sum_{i=0}^{m-1} a_i \cdot \alpha^{2^{i+1}}$$

$(\sum a_i)^2 = \sum a_i^2$

$$\alpha^2 = \sum_{i=0}^{m-1} a_i \cdot \alpha^{2^{i+1}} = \sum_{i=1}^m a_{i-1} \alpha^{2^i} = \sum_{i=1}^{m-1} a_{i-1} \alpha^{2^i} + a_{m-1} \alpha^2$$

در اینجا مذکور شده می‌باشد که α متریک مذکور شده را دارد.

$$= (a_{m-1}, a_0, a_1, a_2, \dots, a_{m-2}) (\alpha \alpha^2 \alpha^{2^2} \dots \alpha^{2^{m-1}})^T$$

درایه دستی از محاسبه مجموعه کمینه شدن در روش Rotation دستی است. بسته به محدودیت های محاسباتی این روش از روش Re-wrapping shift فوجی بهتر است. این روش خواهد بود.

شماره

$$\alpha^{2^j} = (\alpha_{m-j}, \alpha_{m-j+1}, \dots, \alpha_{0}, \alpha_1, \dots, \alpha_{m-j-1}) \cdot \underline{\alpha}^T$$

برای این مرور از این صنایع

$$\alpha_j = (\alpha^2) \langle i+1 \rangle_m$$

است. این مساحت

$$(\alpha^{2^j})_i = (\alpha) \langle i-j \rangle_m$$

$$\alpha = \sum_{i=0}^{m-1} \alpha_i \alpha^{2^i} = \underline{\alpha} \underline{\alpha}^T = \underline{\alpha} \cdot \underline{\alpha}^T$$

کسر در پیش

$$C = \underline{a} \cdot \underline{b}$$

$$= \sum_{i=0}^{m-1} C_i \alpha^{2^i} = \underline{\alpha} \underline{\alpha}^T \underline{\alpha} \underline{b}^T = \underline{\alpha} M \underline{b}^T$$

$$M = \underline{\alpha}^T \underline{\alpha} = (\alpha^2 \alpha^2 \alpha^2 \dots \alpha^{2^{m-1}})^T \cdot (\alpha^2 \alpha^2 \alpha^2 \dots \alpha^{2^{m-1}}) =$$

$$M = \begin{pmatrix} \alpha^{2+2} & \alpha^{2+2} & \dots & \alpha^{2+2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2+2} & \alpha^{2+2} & \dots & \alpha^{2+2} \\ \alpha^{2^{m-1}+2} & \alpha^{2^{m-1}+2} & \dots & \alpha^{2^{m-1}+2} \end{pmatrix} \Rightarrow$$

شماره ملی باید باشد پس سوت
ترسیخ
لیست از $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{2^{m-1}}$

$$= M_0 \alpha + M_1 \alpha^2 + M_2 \alpha^4 + \dots + M_{m-1} \alpha^{2^{m-1}}$$

شماره ملی
باشد α^{2^m}

در واقع ماتریس ممکن است آنها $(m \times n)$ از $GF(2)$ باشند و معمولی خواهند بود.

$$C_{m-1} = \underline{a}_m \underline{\mu}_{m-1} \underline{b}^T$$

دیار دش ترین سنت

$$C = a M b^T$$

$$C_{m-2} = \underline{\alpha} \mu_{m-2} \underline{b}^T$$

$$C_{m-1-k} = \underline{\alpha} \mu_{m-1-k} b^+ \xrightarrow{* \text{ (w)}} (\alpha^{2j})_i = (\alpha)_{\langle i-j \rangle_m}$$

$$C_{m-1-K} = \left(C^2 \right)_{m-1} \Rightarrow C^{2K} \text{ معملات} \\ \alpha M b^T \text{ معملات} \quad \text{نوسن} \quad \text{نوسن} \quad \text{نوسن}$$

$$C_{m-1-k} = \left(C^2 \right)_{m-1} = \underbrace{\left(\alpha^2 \right)^k}_{m \in \mathbb{N}} M_{m-1} \left(b^2 \right)^T$$

so shift. m-1

$$C = \alpha M b^T \Rightarrow C^2 = (\alpha^2) M (b^2)^T$$

$$\boxed{C_{m-1} = \alpha M_{m-1} b^T}$$

$$C_{m-1} = \left(\underline{\alpha_m} \right) \mu_{m-1} \left(\underline{b}^T \right)^T$$

$$C_{m-2} = \left(\underline{\alpha_m^2} \right) \mu_{m-1} \left(\underline{b^2}^T \right)^T \Rightarrow \cancel{\text{معادل}} \rightarrow \text{معادل} \quad \text{لـ} \underline{\alpha_m^2}$$

$$C_{m-2} = \left(\frac{a^2}{\alpha} \right) M_{m-1} \left(\frac{b^2}{\beta} \right)^T \Rightarrow$$

اگر $M_{m-1} - k = 1$ است و در صاحله سنتی ب قبل یک مغایر دارد که درایه زیر همین ندارد.

53

• $\text{C}_m = F(x) = x^4 + x^3 + x^2 + x + 1$ \downarrow $F(d) = \Phi$ \downarrow reduces to 1 $\rightarrow \text{C}_m = \underline{\underline{x^4}}$ $\therefore \text{find } G(F(2^4))$ $\rightarrow \text{J}_4$

این حیثیت از بین نایاب راست چو
 $4+1=5$ عدد اول است ۵

• $f(x) \mid x^5 + 1$ است وقارن AoP $f(x)$. \square

$$1 + \zeta^{\frac{1}{d-1}} \in \mathbb{F}_q(\zeta) \rightarrow \overline{(\zeta^{\frac{1}{d-1}})} \in \mathbb{F}_{q^{d-1}}$$

$$\left\{ \alpha, \alpha^2, \alpha^4, \underline{\alpha^8} \right\}_{\alpha^{2m-1}} \text{Log}_2 b$$

$$d^3 \rightarrow 3$$

$$\mu = \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^5 & \alpha^9 \\ \alpha^3 & \alpha^4 & \alpha^6 & \alpha^{10} \\ \alpha^5 & \alpha^6 & \alpha^8 & \alpha^{12} \\ \alpha^9 & \alpha^{10} & \alpha^{12} & \alpha^{16} \end{pmatrix}$$

$$\left(\begin{array}{ccccc} d^2 & d^8 & 1 & d^4 \\ d^8 & d^4 & d & 1 \\ 1 & d & d^8 & d^2 \\ d^4 & 1 & d^2 & d \end{array} \right)$$

$$\Rightarrow M_0 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \boxed{\text{I}}$$

$$\mu_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

با توجه به اینجا حاصل درک است که در طبقه Mi میتواند بدیگرها بی برآمدت در سیمهای باشند از این طبقه دارای بخوبی

$$M_{i+1} = M_i \uparrow$$

ادیانت shift + 0 میباشد
دیگر سطر را کام نهایت shift + 1 میباشد

لمس فرد هم

کا

$H(M_i)$ تعداد رای های عینکی
Hamming weight

تعداد ممکن نشانه های هم برتر بودن این ماتریس ها سمعت یافته هم هست.

در واقع پس از برتر قاده های داشت.
2) $C_d = H(M_i) \Rightarrow C_d = H(M_j)$

3) If $C_d = 2^{m-1}$ Then is optimal normal basis (ONB)
دیگر بحث نداریم

و در ONB موجود دارد.
برانگیزید [ONB باشد باید دستیاً های سطیح بخواهند آنها AOP داشته باشند. هر واقع حینه ای از مخفف
[ONB] \rightarrow اول باشد. $m+1$ شرط
 $Gf(m+1)$ 2 عنصر اولیه

: ONB I

$Gf(m+1)$ عنصر اولیه در $(2m+1) \equiv 3$, $2^m \equiv 1$

: ONB II

که تواند $Gf(2^m)$ ایجاد کند، $Gf(2^m) = Gf(2^m)^T Gf(2^m) = Gf(2^m) Gf(2^m)^T$

برای محاسبه ممکن است حینه های ممکن دارند
حل معادله ممکن ممکن
EEA روش اولیه هم یافته
 $Gf(2^m) A^{2^m} = A \rightarrow A^{2^{m-2}} = A^1$
حال درست هم با هر ممکن $Gf(2^m)$ ایجاد نمی کند.

$$A \in Gr(2^m)$$

که درجه حرارت زیراست 2^m
 بسیار باشد و تراز مکانیکی $m-1$ است.
 $A^{-1} = A^{2^m-2}$ می‌باشد.

$$\mu(m-1) = 1 + \underbrace{1 + \mu\left(\frac{m-2}{2}\right)}_{نبارهت} \quad \text{زء}$$

برای معرفی اینجا *

$$m-1 = 162 = (10100010)^2$$

$$\mu_1(162) = \left\lfloor \log_2 162 \right\rfloor + H(162) - 1 = 7 + 3 - 1 = 9$$

Scanned by CamScanner

صریح - با استفاده از یک دوگان half basis $\leftarrow (DB)$

این دوگان مجموعه ای از دو یکار مستقل هستند و ممکن است به ترتیب معرفت داشته باشند اما باز هم این دوگان نسبت

به صورت واسیه تقدیف می شوند. دوگانی که دوگان جزئی از

کام \leftarrow که معرفت عکس در صارع نهیم باشد به صیار باید این را درست

$$Tr(x) = \sum_{i=0}^{m-1} x^i, x \in GF(2^m)$$

بعد از تقدیف دوگان $\leftarrow (DB)$

اگر دوگانی داشته باشیم به شکل زیر \leftarrow مستلزم است $B_2 = \{\beta_0, \beta_1, \dots, \beta_{n-1}\}$, $B_1 = \{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$ هستند و توانسته باشند \leftarrow دوگان \leftarrow دوگانی که از اعشار \leftarrow داشته باشند \leftarrow $B_2, B_1 \subseteq GF(2^m)$

$$Tr(\beta_i \gamma_j) = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{if } i \neq j \end{cases}$$

Traces \leftarrow اعشار در صیار \leftarrow اندیس صیار دارند باشد سود \leftarrow حاصل از اعشار صیار \leftarrow اندیس صیار ندارند باشد صفر شوند.

حال فرض کنید دوگان (B_1) که مجموعه ای از $\left\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\right\}$ و دوگان رسمی جزئی از دوگان صیار است.

$$\alpha \in GF(2^m) \Rightarrow \alpha = \sum_{i=0}^{m-1} a_i \cdot \alpha^i \rightarrow DB \leftarrow$$

است. دوگان صورت خواهیم داشت:

با توجه به اعلیه B_2 که مجموعه ای از B_1 (این جزئی از) است، عوامی α را به صورت زیر نمایی دهیم:

$$\alpha = \sum_{i=0}^{m-1} a'_i \cdot \beta_i \Rightarrow DB$$

نهاده است در این است که
نمایشی را از متادارست داشت

حال آنچه را بروز محسوس نماییم.

$$Tr(\alpha^j \cdot \alpha) = Tr\left(\alpha^j \sum_{i=0}^{m-1} a'_i \cdot \beta_i\right) = \sum_{k=0}^{m-1} \left(\alpha^j \sum_{i=0}^{m-1} a'_i \cdot \beta_i\right)^k = \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} a'_i \cdot \beta_i \cdot \alpha^j\right)^k$$

DB \leftarrow $\sum_{i=0}^{m-1} a'_i \cdot \beta_i$

$$= \sum_{k=0}^{m-1} \sum_{i=0}^{m-1} a'_i (B_i \alpha^j)^{2^k} = \sum_{i=0}^{m-1} e'_i \sum_{k=0}^{m-1} (B_j \alpha^j)^{2^k}$$

Trace و تابع خط است).

$$= \sum_{i=0}^{m-1} a'_j \text{Tr}(B_i \alpha^j) \Rightarrow \text{تحاصله} \text{ تابع} \text{ Trace} \text{ است}.$$

با وجود به تعریف داریم (جزو $\sum a'_i \alpha^i$ دوستان هست) $\sum a'_i \alpha^i$ میزد.

$$\text{Tr}(B_i \alpha^j) = 1 \quad \xrightarrow{i=j}$$

$\xrightarrow{\text{نایابی}} \boxed{\text{Tr}(\alpha^j a_i) = a'_j}$

$$\text{Tr}(\alpha^j a_i) = a'_j \leftarrow \text{DB منطبق در} \quad \text{جزو} \quad \text{است}$$

a'_j $\xrightarrow{\text{نایابی}} \text{DB منطبق در} \quad \text{جزو} \quad \text{است}$

حمسه سمعت
منطبق است.
 $a \xrightarrow{\text{}} DB \Rightarrow a'_i \text{ منطبق در} \quad \text{جزو} \quad \text{است}$
 $a \xrightarrow{\text{}} PB \Rightarrow a'_i \text{ منطبق در} \quad \text{جزو} \quad \text{است}$

حمسه سمعت
منطبق است $a, b \in GF(2^m)$
برای هر DB لازم نیست مرد a, b, a'_i, b'_i در DB باشند DB a, b در DB است اما a'_i, b'_i ممکن است در DB باشند (جزو DB داشته است).

$$C_{DB} = \bigoplus a'_i p_B \cdot b'_i$$

$$= (a_0 + a_1 \alpha + a_2 \alpha^2 + \dots + a_{m-1} \alpha^{m-1}) \cdot b_{DB} =$$

$$= a_0 b_{DB} + a_1 \cdot \alpha b_{DB} + a_2 \alpha^2 b_{DB} + \dots + a_{m-1} \cdot \alpha^{m-1} b_{DB} =$$

polynomial $\xrightarrow{\text{نایابی}} \alpha b_{DB} \rightarrow$ حمسه سمعت $\sum a_i b_i$ ممکن است α باشد.

$$\underbrace{PB}_{\text{حاتم هزب می درد DB است}} \underbrace{\alpha \cdot b_{DB}^j}_{DB \in \mathbb{F}_q^m} \xrightarrow{\text{حول DB به } \alpha \cdot b_{DB}^j} (\alpha \cdot b_{DB})_j = Tr(\alpha b \alpha^j) =$$

خواص حذف

$$DB \in \mathbb{F}_q^m \quad \alpha \in \mathbb{F}_q$$

نایابی \mathcal{J} ایم عصر بیان هزب در راهنمای $b_j' \Rightarrow$ b_{j+1}' نایابی \mathcal{J} ایم عصر قبل از هزب است و \sum shift موتور است.

$$(\alpha \cdot b)'_{m-1} = Tr(\alpha b \alpha^{m-1}) = Tr(\alpha^m b) \quad \text{(*)}$$

برهان باشد این دارد

$$= Tr\left(\sum_{i \neq m} f_i \alpha^i b\right) = \sum_{i \neq m} f_i Tr(\alpha^i b) =$$

$$= \sum_{i \neq m} f_i b_i' \quad \Rightarrow \quad \alpha \cdot b_{DB} = (b' b_2' \dots b_{m-1}') \sum_{i \neq m} f_i b_i' \cdot B^T$$

فرض کنیم α رسمی باشد از \mathbb{F}_q

$$f(x) = x^m + \sum_{i \neq m} f_i x^i \quad \text{(*)}$$

$$f(\alpha) = 0 \rightarrow \alpha^m = \sum_{i \neq m} f_i \alpha^i$$

$$(B_1 \ B_2 \ \dots \ B_{m-1})^T$$

با خوبی به محاسبات $\mathcal{L}SFR$ برداشتن هزب کاری داشت $\mathcal{L}SFR$ با محاسبه استخراج شده.

دیگری مثل Triangular basis

$$V = \{v_0, v_1, \dots, v_{m-1}\} \quad \mathcal{B} = \{w_0, w_1, \dots, w_{m-1}\} \quad \text{برهان از}$$

$$\begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{m-1} \end{pmatrix} = \begin{pmatrix} \text{نوار} \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{m-1} \end{pmatrix}$$

حاتم هزب عناصر زیر قطعه هزب است

دیگری مثل $\mathcal{L}SFR$

$$P = \sum_{i=0}^{m-1} k_i w_i \quad k_i = T \cdot w_i$$

مزمن است که پذیری خوبی را باشیم و نیافریده از خوبی از داریم که رسیده باشیم و داشته باشیم.

$$\Omega = \{1, \omega, \omega^2, \dots, \omega^{m-1}\}$$

$$\underbrace{F(\omega) = 0}_{\text{从 } f(x) = x^m + \sum_{i=0}^{m-1} b_i x^i \text{ 得}} \Rightarrow F(\omega) = \omega^m + \sum_{i=0}^{m-1} b_i \cdot \omega^i = \rho \rightarrow \textcircled{1}$$

$$\sum_{i=1}^{m-1} p_i \omega^i = 1$$

$$\omega^{-1} = \sum_{i=1}^m h_i \omega^{i-1} = \sum_{i=4}^{m-1} h_{i+1} \cdot \omega^i$$

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{m-1} \end{pmatrix} = \begin{pmatrix} f_1 & f_2 & \cdots & f_m & f_m \\ f_2 & f_3 & \cdots & f_m & 0 \\ \vdots & & \ddots & f_m & 0 \\ f_m & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{m-1} \end{pmatrix}$$

برلمان استاد

$$V_0 = \sum_{i=1}^m h_i w^{i-1} = \sum_{i=0}^{m-1} h_{i+1} w^{i+1}, \quad \gamma_{m-1} = h_m = 1 \quad (1)$$

برهان

جول دنیا فرید

$$g_i = \sum_{j=\psi}^{m-i-1} f_{i+j+1} \cdot w^j$$

$$C_n = A_n B_n = \sum_{i=0}^{m-1} a_i \cdot \omega^i B_n \xrightarrow{\begin{array}{l} B_n = B_0 \\ \omega B_n = B_1 \\ \vdots \\ \omega^{i-1} B_n = B_{i-1} \end{array}} \sum_{i=0}^{m-1} a_i B_i$$

$$\omega \beta_i = \omega \sum_{i=0}^{m-1} \hat{b}_i \cdot \hat{\delta}_i = \omega \sum_{i=0}^{m-1} \hat{b}_i \sum_{j=0}^{m-i-1} f_{i+j+1} \cdot \omega^j = \sum_{i=0}^{m-1} \hat{b}_i \sum_{j=0}^{m-i-1} f_{i+j+1} \omega^{j+1}$$

$$= \sum_{i=0}^{m-1} \hat{b}_i \sum_{j=1}^{m-i} f_{i+j} \cdot \omega^j = \sum_{i=0}^{m-1} \hat{b}_i \sum_{j \neq i}^{m-i} b_{ij} \omega^j \cdot f_i$$

$$= \sum_{i=0}^{m-1} \hat{b}_i \left[\sum_{j=0}^{m-(i+1)-1} f_{(i+1)+j+1} \cdot \omega^j - f_i \right] \xrightarrow{\text{cancel } f_i} \sum_{i=0}^{m-1} \hat{b}_i [y_{i+1} - f_i] =$$

$$= \sum_{i=0}^{m-1} \hat{b}_i y_{i+1} - \sum_{i>0}^{m-1} \hat{b}_i h_i = \cancel{\hat{b}_0 y_1} + \sum_{i=1}^{m-1} \hat{b}_i y_{i+1} + \sum_{i>0}^{m-1} \hat{b}_i h_i \Rightarrow$$

$\checkmark L = \sum_{i=0}^m b_i w_i \stackrel{Q_L}{=} \phi \quad \stackrel{Q^*}{=} \psi$

این ممکن است خواه است من خواه است.

$$w\beta_\lambda = \left(\hat{b}_1 \hat{b}_2 \dots \hat{b}_{m-1} \left(\sum_{i=1}^{m-1} \hat{b}_i f_i \right) \right) \cdot \hat{\Lambda}^*$$

مُنْهَى مُنْهَى مُنْهَى

مُكْتَسِب مُكْتَسِب مُكْتَسِب

لـ ω نسبـة الـ shift \rightarrow نـسبة الـ shift
 (LSB) \rightarrow نـسبة الـ shift

$$(\omega^i A)_{hj} = \xrightarrow{\text{shift}} (\omega^i A)_{nj} = (\omega^{i-1} A)_{n(j+1)} \Rightarrow$$

جزوی کمتر از ω دارد
دیگر جز داریم.

$$(\omega^i A)_{\wedge j} = (\omega^{i-(i-j)} A)_{\wedge j+(i-j)} = (\omega^j A)_{\wedge j}$$

$$C_n = A_n B_n \Rightarrow \sum_{j=1}^{m-1} C_{nj} y_j = \sum_{i=1}^{m-1} A_{ni} \omega^i b_i = \sum_{i=1}^{m-1} \sum_{j=1}^{m-1} (A\omega^i)_{nj} y_j b_i$$

گرانیت ذات محدود است.

$$= \sum_{j \neq i}^{m-1} \left[\sum_{i=1}^{m-1} (A\omega^j)_{ii} b_i \right] y_j \rightarrow C_{rj} = \sum_{j \neq i}^{m-1} (A\omega^j)_{ii} b_i = 1$$

مقدار C_j دلخواه

$$c_{nj} = \sum_{j=1}^{m^d} (A\omega^d)_{n,j} b_i = \{(A\omega^d)_{n,1}, (A\omega^d)_{n,2}, \dots, (A\omega^d)_{n,m^d}\} \{b_1, b_2, \dots, b_{n-1}\}$$

