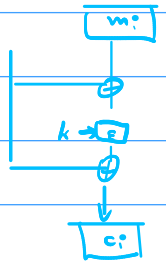
Cifrario a blocchi → come lo si usa. ECB

CBC → chosen plaintext.
XTS

N.B in CBC si conosce che cosa viene codificato mediante il cryptosistema a blocchi (nell'ipotesi di attacchi chosen plaintext) e si può anche scegliere il tipo di testo

$$c_{i+1} = \mathcal{E}(c_i \oplus m_{i+1}, k)$$



XTS $\quad c_i = \mathcal{E}(a^i \oplus m_i, k) \oplus a^i$

IMPORTANTE NON AVERE UN SISTEMA CHE SI TRASFORMI IN UN ORACOLO

→ NON SI DEVE PERMETTERE IN GENERALE ALL'AVVERSARIO DI CODIFICARE UN NUMERO NON LIMITATO DI MESSAGGI A SUA SCELTA.

chosen plaintext.

Usi dei campi finiti → $(\mathbb{Z}_p, +, \cdot)$

$(\mathbb{F}_{p^n}, +, \cdot)$

N.B $\mathbb{Z}_{p^n} \neq \mathbb{F}_{p^n}$

$\mathbb{Z}_{p^n}$: non è un campo se $n > 1$ — $\mathbb{F}_{p^n}$: campo

OSS: Il gruppo $(\mathbb{Z}_{p^n}, +)$ è ciclico, generato da $[1]_{p^n}$

$[0]_n\ [1]_n \ \_\_\_ \ [p^n - 1]_n$

Il gruppo $(\mathbb{F}_{p^n}, +)$ è abeliano elementare →

corrisponde al gruppo additivo dei vettori di $\mathbb{Z}_p^n$ (n. vett. di dim $= n$ su $\mathbb{Z}_p$)

ed ogni suo elemento $\neq 0$ ha ordine p

↓

NON È CICLICO!!

OSS NOI ABBIAMO IDENTIFICATO GLI ELEMENTI DI $\mathbb{Z}_{2^8}$ CON BYTES, per cui, in ultima istanza, li rappresentiamo CON DEI NUMERI → ATTENZIONE: la somma è lo XOR e non la somma di interi modulo qualcosa.

-

- $(\mathbb{Z}_p^*, \cdot)$ è un gruppo ciclico di ordine $p-1$
- $(\mathbb{F}_{p^n}^*, \cdot)$ è un gruppo ciclico di ordine p^n-1

[N.B. $(\mathbb{Z}_{p^n}^*, \cdot)$ è un gruppo di ordine $\varphi(p^n) = p^n(1-\frac{1}{p})$ ma non è ciclico in generale].

I gruppi moltiplicativi di $\mathbb{F}_{p^n}$ $(n \geq 1)$ sono gruppi "buoni" per i crittosistemi basati su DLOG.

→ è facile implementarli.

→ DLOG NON È BANALE → DATO g generatore di $\mathbb{F}_{p^n}^*$ E h elemento di $\mathbb{F}_{p^n}^*$ è difficile trovare a: $g^a = h$

↓

sono i gruppi "campione" per DLOG.

$(\mathbb{Z}_p^*, \cdot)$ con p grande; $p \approx 2^{1024}$

$(\mathbb{F}_{2^n}^*, \cdot)$ con 2^n del medesimo ordine di grandezza.

N.B $2^n - 1$ può anche essere primo.

$p-1$ con p primo è sempre pari

↓

per $\mathbb{Z}_p^*$ si dice che a parte 2 ci sia un divisore primo grande di $(p-1)$

Si può fare di meglio?

→ [∃ gruppi ciclici usabili (= facili da implementare) in cui DLOG è difficile e i cui elementi sono "più piccoli" di 1024 bits?]

N.B per El Gamal ogni codifica richiede di trasmettere 2 elementi di gruppo → el. di 1024 bits

↓ ogni codifica richiede di trasmettere 2048 bits]

In generale i cryptosistemi a chiave pubblica si usano per negoziare chiavi (ad es. per AES) di 256 bits

↓

overhead di un fattore almeno x10.

SOLUZIONE: costruire dei gruppi a partire da enti geometrici → CRITTOGRAFIA SU CURVE ELLITTICHE.

IDEA: considerare degli insiemi di punti in un piano/spazio affine (ampliato) e definire una regola di somma su di essi.

→ facile da calcolare
→ definire una struttura di gruppo abeliano (Vel. abbia inverso; ci sia l'el. neutro, valga la prop. associativa e commutativa).
→ rispetto cui DLOG sia difficile

Le cosiddette curve ellittiche sono dotate di una struttura che va bene.

Lavoriamo in $AG(2,\mathbb{k})$ o in $PG(2,\mathbb{k})$.

$AG(2,\mathbb{k})$ = spazio affine i cui punti sono gli elementi di $\mathbb{k}^n$ e tale che $\forall\, P,Q \in AG(2,\mathbb{k})$ il vettore $\overrightarrow{PQ}$ è esattamente $Q-P$

piano affine (cartesiano) sul campo $\mathbb{k}$.

Una <u>curva algebrica</u> in $AG(2,\mathbb{k})$ definita da un polinomio $f(x,y) \in \mathbb{k}[x,y]$ con $f(x,y)$ non costante è l'insieme dei punti $V(f) := \{(x,y) \in AG(2,\mathbb{k}) \mid f(x,y)=0\}$.

<u>N.B</u> In generale se $\mathbb{k}$ non è algebricamente chiuso una curva

algebrica non è caratterizzata dall'insieme dei suoi punti.

Es. $\mathbb{K}=\mathbb{R}$ $\quad f(x,y)=x^2+y^2+1 \quad V(f)=\emptyset$

$g(x,y)=x^4+1 \quad V(g)=\emptyset$

Se $\overline{\mathbb{K}}$ è alg. chiuso (ad es. $\overline{\mathbb{K}}=\mathbb{C}$) $\Rightarrow$ esiste un teorema che garantisce che ad ogni polinomio $f(x,y)$ non costante è associato un insieme di punti di $AG(2,\mathbb{K})$ e viceversa che ad ogni insieme siffatto è associato un opportuno ideale di $\mathbb{K}[x,y]$ in modo unico generato da un polinomio e che contiene $f(x,y)$.

[Nullstellensatz]

$$f(x,y)=(x^2+1)^2 \qquad V(f)=V(x^2+1)$$

$$f \longrightarrow V(f)$$

$$V(f) \longrightarrow I(V(f))=\{g(x,y)\in\overline{\mathbb{K}}[x,y] \mid \forall (\bar{x},\bar{y})\in V(f),\ g(\bar{x},\bar{y})=0\}$$

[Noi però vogliamo lavorare su campi finiti che non sono algebricamente chiusi.]

Ci servirà anche poter considerare i punti impropri di una curva.

$$PG(n,\mathbb{K}) := \frac{\mathbb{K}^{n+1}\setminus\{\underline{0}\}}{\mathbb{K}^*}$$

geometria proiettiva.

Gli elementi di $PG(n,\mathbb{K})$ (punti) sono le classi di proporzionalità dei vettori di $\mathbb{K}^{n+1}$ diversi dal vettor nullo $\rightarrow$ alternativamente i

- PUNTI DI $PG(n,\mathbb{K})$ $\leftrightarrow$ sottospazi 1-dim. di $\mathbb{K}^{n+1}$
- SOTTOSPAZI t-dimensionali di $PG(n,\mathbb{K})$ $\leftrightarrow$ sottospazi vettoriali di dim $t+1$ di $\mathbb{K}^{n+1}$
- (rette) $\leftrightarrow$ sottospazi di dim = 2.
- INCIDENZA = $\subseteq$

dato $AG(n,\mathbb{K})$ noi possiamo immergere $AG(n,\mathbb{K})$ in $PG(n,\mathbb{K})$ nel seguente modo

$AG(n,\mathbb{K})$

φ

punto $(x_1 \dots x_n) \longmapsto \langle (x_1 \dots x_{n+1}) \rangle \leq \mathbb{K}^{n+1}$

direzione $(l_1 \dots l_n) \longmapsto \langle (l_1 \dots l_{n0}) \rangle \leq \mathbb{K}^{n+1}$

punto improprio.

Si verifica che φ è una bigezione fra

$\{$punti di $AG(n,\mathbb{K})\} \cup \{$direzioni di $AG(n,\mathbb{K})\}$

$\rightarrow \{$punti di $PG(n,\mathbb{K})\}$

ed in particolare dato un sottospazio di $AG(n,\mathbb{K})$ di dim t, l'immagine di questo sottospazio + le sue direzioni

è un sottospazio di $PG(n, \mathbb{K})$.

In particolare, sia ora

$a_1X_1 + a_2X_2 + \dots + a_nX_n + \beta = 0$ l'equazione di un iperpiano in $AG(n, \mathbb{K})$

$\Rightarrow$ l'immagine di tale iperpiano in $PG(n, \mathbb{K})$ ha equazione $a_0x_0 + a_1x_1 + \dots + a_nx_n + \beta x_{n+1} = 0$

Infatti ogni punto $(X_1 \dots X_n)$ viene mandato in un p.to $\phi((X_1 \dots X_n, 1))$ e ogni direzione $(l_1 \dots l_n)$ soluzione dell'eq. omogenea associata

$$a_1X_1 + \dots + a_nX_n = 0$$

viene mandata in $\phi((l_1 \dots l_n 0))$

e vediamo che esattamente questi soddisfano $a_0x_0 + \dots + a_nx_n + \beta x_{n+1} = 0$ (*)

viceversa, supponiamo $\phi((a_1 \dots a_{n+1}))$ soddisfi (*) $\Rightarrow$ se $a_{n+1} \neq 0$ abbiamo

$\left(\frac{a_1}{a_{n+1}}, \dots \frac{a_n}{a_{n+1}}\right)$ soddisfa

$a_1X_1 + \dots a_nX_n + \beta = 0 \rightarrow$ punto dell'iperpiano.

$\Rightarrow$ se $a_{n+1} = 0 \Rightarrow (a_1 \_\_\_ a_n)$ soddisfa

$a_1 x_1 + \_\_\_ a_n x_n = 0$

$\Rightarrow$ direzione contenuta nell'iperpiano.

Quello che vale per gli iperpiani si applica anche alle loro intersezioni $\rightarrow$ a tutti i sottospazi.

$n = 2$ $\quad AG(2, \mathbb{K})$ $\quad PG(2, \mathbb{K})$

$ax + by + c = 0$ $\quad ax_1 + bx_2 + cx_3 = 0$

$x = \frac{x_1}{x_3} \quad y = \frac{x_2}{x_3} \longrightarrow a\frac{x_1}{x_3} + b\frac{x_2}{x_3} + c = 0$

moltiplicando per x_3 $\rightarrow$ $ax_1 + bx_2 + cx_3 = 0$

punti: propri $\quad$ punti propri ed impropri (per $x_3 = 0$)

più in generale, se abbiamo una eq. affine $f(x, y) = 0$ che definisce la nostra curva, possiamo scrivere una eq. omogenea che la definisce in $PG(2, \mathbb{K})$ prendendo

$$F(x_1, x_2, x_3) := x_3^{\deg f} \cdot f\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)$$

dove per $\deg f$ intendo il max grado totale di f.

Più in dettaglio.

Dato $PG(n,\mathbb{K})$ sia Σ_∞ il suo iperpiano di eq. $x_{n+1}=0$

Sia ora $W \leq \mathbb{K}^{n+1}$ con $W \not\subseteq \Sigma_\infty$.

Poniamo inoltre $\forall X \in \mathbb{K}^{n+1}$, $X=(x_1 \dots x_n x_{n+1}), x_{n+1}\neq 0$

$$\bar{\vartheta}(X) = \left(\frac{x_1}{x_{n+1}} \dots \frac{x_n}{x_{n+1}}\right)$$

e $\forall M \leq \mathbb{K}^n$, $M \not\subseteq \Sigma_\infty$

$$\vartheta(M) = \{\bar{\vartheta}(X) \mid X \leq M ; \dim X = 1\}.$$

Allora $\vartheta(M)$ è un sottospazio affine di $AG(n,\mathbb{K})$

ed il corrispondente sottospazio di traslazione è dato da

$$S = \{(x_1 \dots x_n) \in \mathbb{K}^n \mid (x_1 \dots x_n\ 0) \in M \cap \Sigma_\infty\}.$$

Viceversa, dato $\mathcal{C} = [P; \omega] \leq AG(n,\mathbb{K})$ il corrispondente sottospazio di $PG(n,\mathbb{K})$ è dato da $\tilde{\mathcal{C}} := \mathcal{L}(\tilde{\vartheta}(R) \mid R \in \mathcal{C})$

ove $\vartheta((p_2 \dots p_n)) = \mathcal{L}((p_2 \dots p_n 1))$ □

Esempio $f(x,y) = x^3 + xy + 3$

$$F(x_1,x_2,x_3) = x_3^3 \cdot f\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right) =$$

$$= x_3^3 \left(\frac{x_1^3}{x_3^3} + \frac{x_1 x_2}{x_3^2} + 3\right) =$$

$$= x_1^3 + x_1 x_2 x_3 + 3x_3^3$$

punti propri $\rightarrow x_3 \neq 0$

punti impropri $x_3 = 0$

$$f(x,y) = x^2y^2 + x^3 + y$$

$$F(x_1,x_2,x_3) = x_1^2x_2^2 + x_1^3x_3 + x_2x_3^3$$

Se $f(x,y)$ è un polinomio che descrive la curva $\mathcal{V}(f)$ in $AG(2,\mathbb{K})$, chiameremo punti impropri di $\mathcal{V}(f)$ i punti di $\bar{\mathcal{V}}(F(x_1,x_2,x_3)) \cap [x_3 = 0]$ in $PG(2,\mathbb{K})$

ove per $\bar{\mathcal{V}}(F(x_1,x_2,x_3))$ intendo

$$\bar{\mathcal{V}}(F) = \{ \mathcal{L}((x_1,x_2,x_3)) \in PG(2,\mathbb{K}) \mid F(x_1,x_2,x_3) = 0 \}$$

$$F = x_3^{\deg f} f\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right).$$ equazione omogenea di f

Def: Si dice curva iperellittica in $AG(2,\mathbb{K})$ una curva di equazione

$$y^2 + y\,p(x) = f(x)$$

$\deg f(x) = 2g+1 \geq 3$

$\deg p(x) \leq g+2$

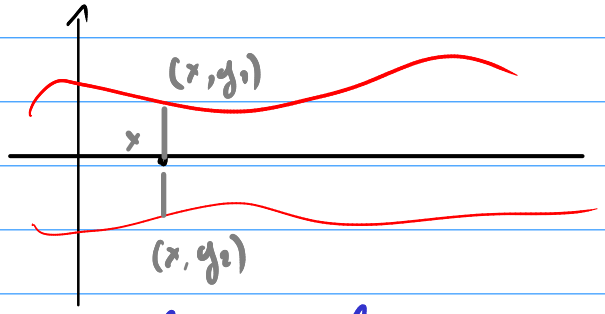
con $f(x)$ polinomio irriducibile in X

$\deg f(x) \geq 3$

Sostanzialmente $\forall x \in \mathbb{K}$

$$y^2 + y\,p(x) - f(x) = 0 \quad (*)$$

ci troviamo 2 valori di y corrispondenti (se $\mathbb{K}$ alg. chiuso).



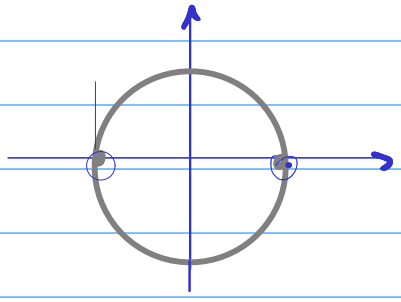
In generale, in funzione del Δ di $(*)$ avremo

0, 1 oppure 2 valori possibili per y

Esempio di funzioni di quel tipo

$$y^2 = 1 - x^2$$

$\mathbb{K} = \mathbb{R}$



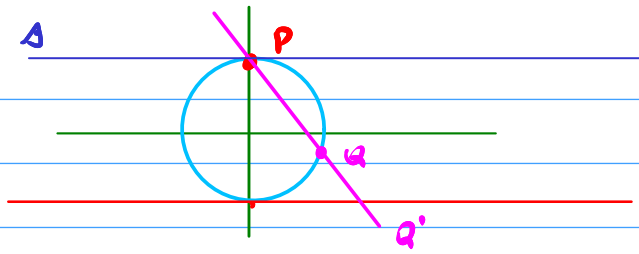
se $x^2 > 1$ ⇓ 0 sol.

se $x^2 = 1$ ⇓ 1 sol.

$0 \leq x^2 \leq 1$ ⇒ 2 sol.

Il caso della circonferenza non è interessante

oss: Sia $\mathcal{C}$ una conica irriducibile su $\mathbb{F}_q$ con $\mathbb{F}_q$ campo finito ⇒ $\mathcal{C}$ ha tanti punti quanti: una retta e questi sono $q+1$



$s_\infty = r_\infty$ ha una biiezione fra i punti di s e quelli di r

Più rigorosamente, si prende una conica generale in $AG(2, \mathbb{F}_q)$, si fissa un suo punto P e si considera una retta r esterna alla conica e il fascio di rette per P.

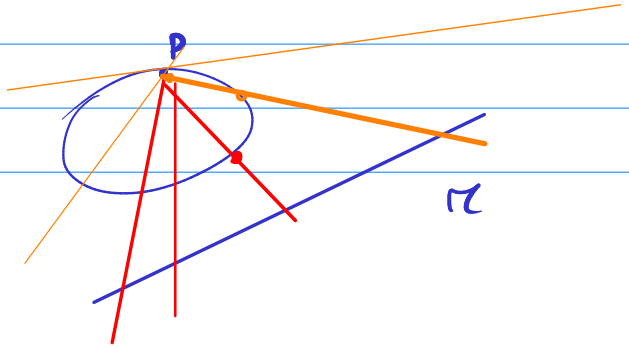
Ogni retta del fascio interseca r in punti distinti. (inclusi quelli impropri)

D'altro canto per ogni punto Q della conica con $Q \neq P$ passa una e una sola retta del fascio (2-secanti) e se $Q = P$ vi è una unica retta che incontra la conica in P 2 volte

$\Rightarrow$ c'è una biiezione fra:

1) punti della conica
2) rette del fascio per P
3) punti sulla retta r.

} sono tutti $q+1$



Def: Si dice cubica ellittica una curva ipoellittica (equivalente ad una curva) di equazione

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Se $\mathbb{K} \neq \mathbb{F}_{2^n}, \mathbb{F}_{3^n}$

$$y^2 = x^3 + ax + b$$

$$4a^3 + 27b^2 \neq 0$$

↑ il polinomio $f(x)$ ha grado 3 $m(x)$ ha grado 1