Funzioni non lineari in Crittografia Simmetrica

Daniele Bartoli

University of Perugia, Italy

Perugia - 16/10/2019

- S. Murphy (1990) studia il FEAL-4 (Fast data Encipherment ALgorithm), un cifrario a blocchi proposto come sostituto del DES. Deve considerare soluzioni di equazioni della forma

$$G(x+a)+G(x+b)=d$$

- Eli Biham and Adi Shamir (1990) studiando il DES scoprono che per alcune fissate differenze di plaintext, le differenze dei valori criptati appaiono molto più frequentemente di altre (non hanno distribuzione casuale). Questo può essere usato per avere informazioni sulla chiave.
- Grande interesse per le cosiddette derivate discrete. In genere si cercano funzioni che abbiano derivata discreta la più uniforme possibile (perfect nonlinear functions, almost perfect nonlinear functions)

$q = p^h$, p primo
$\mathbb{F}_q$ campo con q elementi

Definizione (K. Nyberg (1993))

$f : \mathbb{F}_q \to \mathbb{F}_q$

$$\delta(a,b) = \#\{x \ : \ F(x+a) - F(x) = b\}, \quad \Delta_F = \max_{a \in \mathbb{F}_q^*, b \in \mathbb{F}_q} \delta(a,b)$$

F *è detta* *differentially Δ_F-uniform*

$F : \mathbb{F}_{2^n} \to \mathbb{F}_2$ e Δ_F è il più piccolo possibile (2^{n-1}) F è detta perfect nonlinear Meier-Staffelbach (1989). Sono equivalenti alle Bent functions (Rothaus, 1976)

Definizione

q dispari

$f : \mathbb{F}_q \to \mathbb{F}_q$ *è detta planare (o Perfect nonlinear) se*

$$\forall \epsilon \in \mathbb{F}_q \Longrightarrow x \to f(x+\epsilon) - f(x)$$

è una permutazione di $\mathbb{F}_q$.

- Costruzione di piani proiettivi finiti

  P. Dembowski and T. G. Ostrom (1968)

- Relative difference sets

  M. J. Ganley and E. Spence (1975)

- Codici correttori di errore

  C. Carlet, C. Ding, and J. Yuan (2005)

- S-boxes in block ciphers

  K. Nyberg and L. R. Knudsen (1993)

Remark

Se $q = 2^n$ allora questo non può mai accadere: al massimo è $2 - 1$.

Definizione

q pari

$f : \mathbb{F}_q \to \mathbb{F}_q$ *è detta Almost Perfect Nonlinear (APN) se*

$$\forall \epsilon \in \mathbb{F}_q \implies x \to f(x + \epsilon) + f(x)$$

è $2 - 1$.

Definizione (Zhou, 2013)

q pari

$f : \mathbb{F}_q \to \mathbb{F}_q$ *è detta* *planare* *se*

$$\forall \epsilon \in \mathbb{F}_q \Longrightarrow x \to f(x+\epsilon) + f(x) + \epsilon x$$

è una permutazione di $\mathbb{F}_q$.

- Codici correttori di errore
- Relative difference sets
- S-boxes in block ciphers

Remark

Un polinomio linearizzato ($\sum_i a_i X^{2^i}$) *è sempre planare:*

$$f(x+\epsilon)+f(x)+\epsilon x=\sum_i a_i(x+\epsilon)^{2^i}+\sum_i a_i x^{2^i}+\epsilon x=\epsilon x+\sum_i a_i \epsilon^{2^i}$$

Theorem (B.-SCHMIDT, 2019)

Sia $f \in \mathbb{F}_q[X]$ *di grado al più* $q^{1/4}$. *Allora* f *è planar* $\iff$ f *è polinomio linearizzato*

- Varietà e curve algebriche in caratteristica positiva
- Rami centrati in punti singolari
- Trasformazioni locali quadratiche

Laurea Magistrale in Matematica

Curriculum “MATEMATICA PER LA CRITTOGRAFIA”

Piano di Studi

I Anno - I Semestre		I Anno - II Semestre	
Algebra Commutativa e Computazionale	Mat/02	Analisi Funzionale	Mat/05
Geometria Differenziale	Mat/03	Crittografia e Applicazioni	Mat/03
Programmazione II	Inf/01	Probabilità e Statistica II	Mat/06
Teoria dei Codici	Mat/03	Sicurezza Informatica	Inf/01
II Anno - I Semestre		**II Anno - II Semestre**	
Geometria Algebrica	Mat/03	Combinatorics	Mat/03
Modelli Matematici per le Applicazioni	Mat/07	Modellistica Numerica	Mat/08
Calcolabilità e Complessità Computazionale	Inf/01	Ulteriori Attività formative	
Approssimazione Numerica e Applicazioni	Mat/08	TESI	

- Geometria Differenziale, Analisi Funzionale, Probabilità e Statistica, Modelli Matematici per le Applicazioni
- Informatica: Programmazione II
  Sicurezza Informatica
  Calcolabilità e Complessità Computazionale
- Matematica: Algebra Commutativa e Computazionale
  Crittografia e Applicazioni
  Teoria dei Codici
  Combinatorics
  Geometria Algebrica

Teoria dei Codici

Codici lineari e multinsiemi di spazi proiettivi. Curve algebriche su campi finiti, campi di funzioni. Codici Reed-Solomon. Codici algebrico-geometrici. Codici di Goppa one-point. Codici hermitiani. Cenni alle curve ellittiche in crittografia.

Crittografia e Applicazioni

Crittografia classica. Segretezza perfetta. Prodotto di crittosistemi. Cifrari a blocchi: DES, AES. Funzioni hash in crittografia. Funzioni hash iterate. La costruzione di Merkle-Damgard e algoritmi SHA. Crittografia a chiave pubblica. Crittosistema di ElGamal. Curve ellittiche. Firma digitale. Schema di firma di ElGamal. DSA e Elliptic Curves DSA. Secret sharing schemes.

Sicurezza Informatica

Storia della Sicurezza Informatica. Policies, Metodi di autenticazione, Concept of trust and trustworthiness, Principles of Secure Design, Defensive Programming, Threats and Attacks, Network Security, Cryptography.

Esami caratterizzanti di Matematica

Principali argomenti caratterizzanti

- Crittografia e Applicazioni:
  Curve ellittiche Realizzazioni Geometriche di SSS
- Teoria dei Codici: Codici Algebrico-Geometrici
- Combinatorics: Codici lineari $\leftrightarrow$ Sistemi di punti proiettivi
  Realizzazioni Geometriche di SSS
- Geometria Algebrica: Anche su campi finiti
  Curve ellittiche

Stages e tirocini formativi

Grazie alla collaborazione con l'analogo percorso di Trento

- Stages/Tirocini curriculari presso aziende ed istituzioni di prestigio: fondazione GSEC e Aruba
- Stage post laurea presso Poste Italiane