Curve Algebriche in Crittografia

M. Giulietti

Dipartimento di Matematica e Informatica
Università degli Studi di Perugia

La De Cifris incontra Roma
Roma, 4 ottobre 2018

De Cifris a Perugia

- Giorgio Faina - MAT/03
- Massimo Giulietti - MAT/03
- Fernanda Pambianco - MAT/03
- Stefano Marcugini - INF/01
- Marco Baioletti - INF/01
- Daniele Bartoli - MAT/03
- Ex studenti

Attività

- Ricerca: pura ed applicata
- Didattica: curriculum specifico della laurea magistrale in Matematica
- Public engagement: parte attiva di progetti di awareness nelle scuole (es. PLS), progetti museali (Vision); interventi presso mostre ed esposizioni (es. *Enigma: Cifrare e decifrare: linguaggi nascosti*, tenutasi presso la provincia di Perugia)

Ricerca pura

Teoria dei Codici e Crittografia legate alle **Geometrie di Galois** e alla **Geometria algebrica in caratteristica positiva**

- Crittografia su Curve Ellittiche
- Secret Sharing Schemes
- Funzioni APN e funzioni planari
- Codici algebrico geometrici da curve di genere superiore (in particolare massimali)
- Codici lineari come n-insiemi di $PG(r, q)$

Curve ellittiche in crittografia

- ECDH, ECDHE
- ECDSA

Curve ellittiche in crittografia

- ECDH, ECDHE
- ECDSA
- post quantum? SIDH: Supersingular Isogeny Diffie-Hellman
  - una delle lunghezze di chiave più piccole nell'ambito delle proposte post-quantum
  - supporta perfect forward secrecy (PFS) (a differenza di NTRU e Ring-LWS).
  - la chiave può essere generata in 200 millisecondi.

Curve ellittiche supersingolari

Theorem (Hasse-Weil)

Data una curva algebrica definita su un campo con q elementi e di genere g il suo numero N di punti soddisfa

$$q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}$$

- Una curva ellittica definita sul campo con p^2 elementi è **supersingolare** se vale una delle due uguaglianze
- In generale una curva per cui vale $N = q + 1 + 2g\sqrt{q}$ si dice **massimale**

Curve algebriche in crittografia simmetrica

Definition

Una funzione $f : \mathbb{F}_q \to \mathbb{F}_q$ si dice **planare** o **Perfect Non-linear** se

$D_a(f) : x \mapsto f(x+a) - f(x)$ è biiettiva per ogni $a \in \mathbb{F}_q$, $a \neq 0$

Definition

Sia q pari. Una funzione $f : \mathbb{F}_q \to \mathbb{F}_q$ si dice **APN** se

$f(x+a)-f(x) = b$ ha al massimo 2 soluzioni per ogni $a, b \in \mathbb{F}_q$, $a \neq 0$

Definition

Sia q pari. Una funzione $f : \mathbb{F}_q \to \mathbb{F}_q$ si dice **planare** se

$E_a(f) : x \mapsto f(x+a) - f(x) + ax$ è biiettiva per ogni $a \in \mathbb{F}_q$, $a \neq 0$

Theorem

Sia q pari. Sia $f : \mathbb{F}_q \to \mathbb{F}_q$ polinomiale di grado d, con $d \geq 9$ e $d < 0.45q^{1/4} + 0.5$.

Allora f è **APN** *solo se la superficie di equazione*

$$\mathcal{S} : \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)} = 0$$

non ha componenti assolutamente irriducibili definite su $\mathbb{F}_q$

Theorem

Sia q pari. Sia $f : \mathbb{F}_q \to \mathbb{F}_q$ polinomiale di grado d, con $d \geq 9$ e $d < 0.45q^{1/4} + 0.5$.

Allora f è **APN** *solo se la superficie di equazione*

$$\mathcal{S} : \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)} = 0$$

non ha componenti assolutamente irriducibili definite su $\mathbb{F}_q$

Theorem (Bartoli-Schmidt, 2018)

Sia q pari. Sia $f : \mathbb{F}_q \to \mathbb{F}_q$ polinomiale di grado d, con $d \geq 9$ e $d < 0.45q^{1/4} + 0.5$.

- *Se f è APN allora d è multiplo di 4.*
- *Se f è planare allora il grado di ogni monomio di f è una potenza di 2.*

Secret Sharing

$$\Gamma \subset \mathcal{P}(X)$$

struttura d'accesso

Se

$$\eta : X \cup \{s\} \to PG(r, q)$$

è tale che $\{x_1, x_2, \ldots, x_n\} \in \Gamma$ se e solo se
$\eta(s) \in \langle \eta(x_1), \eta(x_2), \ldots, \eta(x_n) \rangle$ allora esiste un secret sharing schemes perfetto ideale dove l'insieme dei possibili segreti è q

Strutture multilivello

- Brickell (1989): esistenza di un sss ideale per struttura d'accesso a t livelli con livello di sicurezza

$$\epsilon < \frac{1}{t \cdot \binom{\#X}{t}}$$

- problema: stessa sicurezza, più partecipanti

Alcuni risultati ($q = 1/\epsilon$)

- $t = 2$: caratterizzazione $\#X = q + 1 + t$ per q dispari (Beato-G.-Faina)
- $t = 3$: $\#X = \frac{1}{8}(q-1)(\sqrt{q}+1)$ per q quadrato dispari (G. - Vincenti)
- $t = 4$: q potenza quarta, $\sqrt[4]{q} \equiv 2 \pmod 3$

$$\#X = \frac{1}{96}(\sqrt[2]{q})(\sqrt[4]{q} - 3)$$

per $\sqrt[4]{q} \equiv 1 \pmod 4$,

$$\#X = \frac{1}{24}(\sqrt[2]{q})(\sqrt[4]{q} - 3)$$

per $\sqrt[4]{q} \equiv 1 \pmod 4$ (Bartoli-G.)

Ricerca applicata

- algoritmi su curve ellittiche: miglioramenti algoritmo di Miller per il calcolo del Weil pairing (Baioletti)
- Blockchain e PSD2: *Revised Payments Service Directive: A Blockchain-based Implementation Model* (Leccese-Peverini presso GCSEC)
- Watermarking in relazione al potenziamento di immagini di tipo medico (TAC senza mezzo di contrasto). Progetto cofinanziato dalla *Fondazione Cassa di Risparmio di Perugia*

Laurea Magistrale in Matematica
Curriculum
“MATEMATICA PER LA SICUREZZA INFORMATICA"

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 BCH e codici ciclici. Codici algebrico-geometrici. Codici di Goppa one-point. Primi cenni alle curve ellittiche in crittografia.

Crittografia e Applicazioni

Crittografia classica. Segretezza perfetta. Cifrari a blocchi: DES, AES. Funzioni hash in crittografia. La costruzione di Merkle-Damgard e algoritmi SHA. Crittografia a chiave pubblica. DH e RSA. Curve ellittiche. Firma digitale. DSA e ECDSA. Blockchain. 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.

Stages e tirocini formativi

- Stages/Tirocini curriculari presso aziende ed istituzioni di prestigio: fondazione GCSEC e Aruba
- Stage post laurea presso GCSEC e NTT DATA
- Dottorati di ricerca