De Cifris a Perugia

M. Giulietti

Dipartimento di Matematica e Informatica
Università degli Studi di Perugia

Chi siamo

- Giorgio Faina - PO MAT/03
- Massimo Giulietti - PA MAT/03
- Fernanda Pambianco - PA MAT/03
- Stefano Marcugini - PA INF/01
- Marco Baioletti - RU INF/01
- Daniele Bartoli - RTD MAT/03
- Francesco Peverini - stagista presso GSEC

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

- Secret Sharing Schemes
- Codici MDS da curve ellittiche
- Codici di ricoprimento da curve ellittiche
- Codici algebrico geometrici da curve di genere superiore (in particolare massimali)
- Codici lineari come n-insiemi di $PG(r, q)$

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): condizione sufficiente di esistenza per un sss ideale per struttura d'accesso a t livelli con livello di sicurezza $1/q$:

$$q > t \cdot \binom{\#X}{t}$$

- problema: stessa sicurezza, più partecipanti

Alcuni risultati

- $t = 2$: 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.)

Curve Ellittiche e Codici MDS

$[n, k, d]_q$- codici MDS non estendibili sono equivalenti ad *archi completi* di $PG(n-k-1, q)$ di cardinalità n

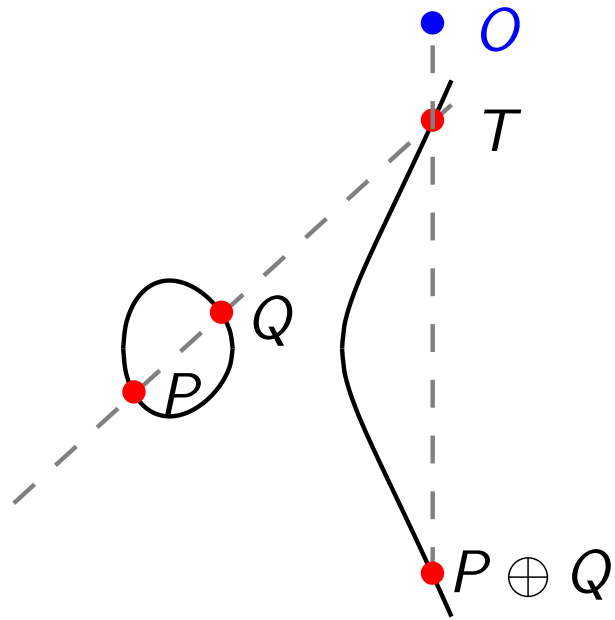
arco di $PG(r, q)$: punti ad $r+1$ ad $r+1$ indipendenti

arco completo: massimale rispetto all'inclusione

$\mathcal{X}$ curva ellittica

$\mathcal{X}$ curva ellittica

$\mathcal{X} : Y^2 = X^3 + AX + B$



$G = \mathcal{X}(\mathbb{F}_q)$

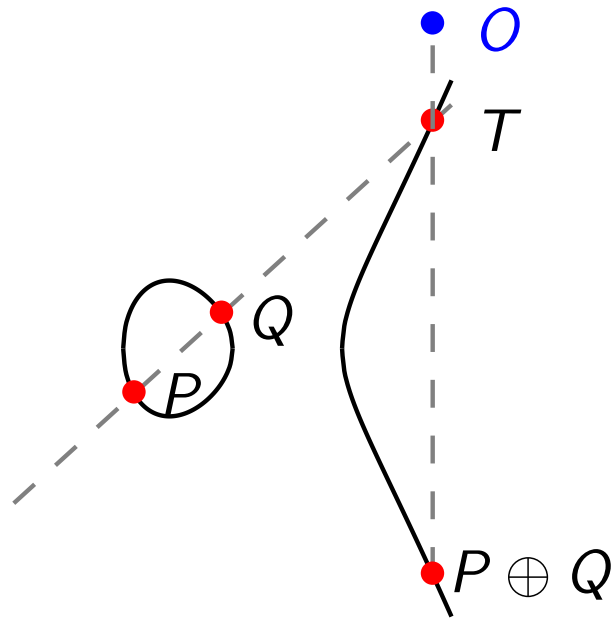
- per un sottogruppo K di indice m con $(3, m) = 1$

$$S = K \oplus Q, \qquad Q \notin K$$

è un arco

$\mathcal{X}$ curva ellittica

$\mathcal{X} : Y^2 = X^3 + AX + B$



$G = \mathcal{X}(\mathbb{F}_q)$

- per un sottogruppo K di indice m con $(3, m) = 1$

$$S = K \oplus Q, \qquad Q \notin K$$

è un arco

- Quando è completo?

Tate-Lichtenbaum pairing

G ciclico $\quad m \mid q-1 \quad m$ primo

Tate-Lichtenbaum pairing

G ciclico $\qquad$ $m \mid q-1$ $\qquad$ m primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

Tate-Lichtenbaum pairing

G ciclico $\qquad m \mid q-1 \qquad m$ primo

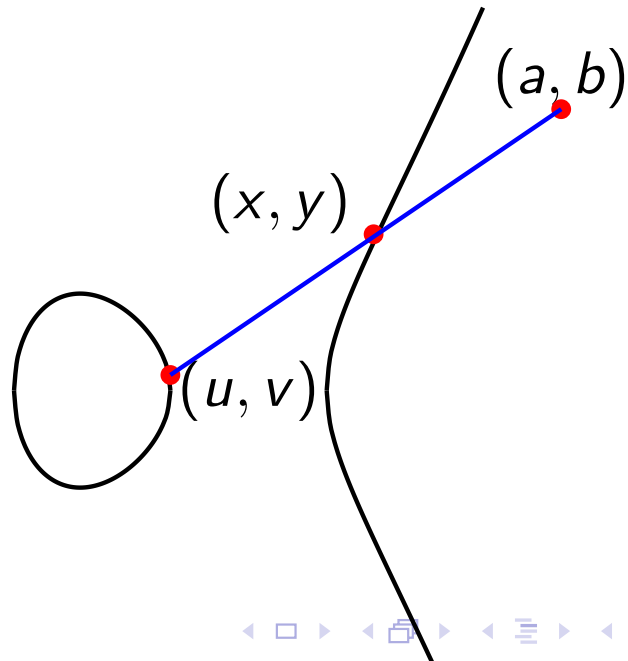
$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

Tate-Lichtenbaum pairing

G ciclico $\qquad$ $m \mid q-1$ $\qquad$ m primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

$P = (a, b)$ allineato con $(x, y), (u, v) \in S$ se esistono $x, y, u, v, t, z \in \mathbb{F}_q$ con



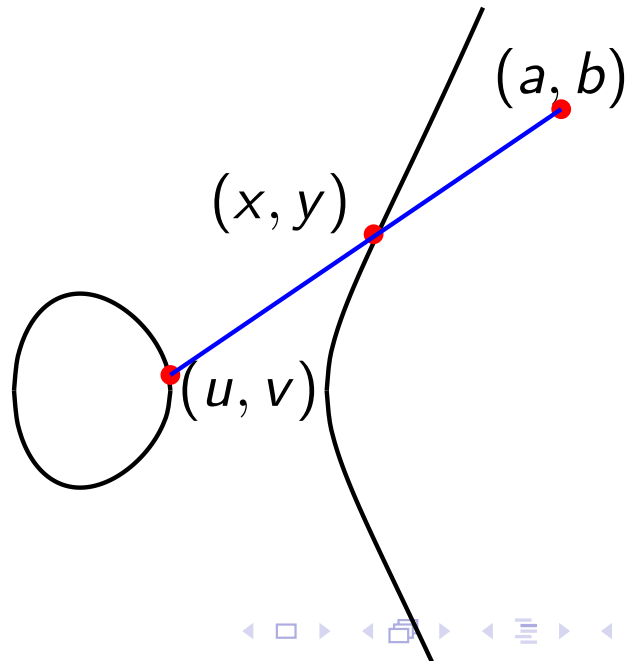
Tate-Lichtenbaum pairing

G ciclico $\qquad m \mid q-1 \qquad m$ primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

$P = (a, b)$ allineato con $(x, y), (u, v) \in S$ se esistono $x, y, u, v, t, z \in \mathbb{F}_q$ con

$$\begin{cases} y^2 = x^3 + Ax + B \\ v^2 = u^3 + Au + B \end{cases}$$



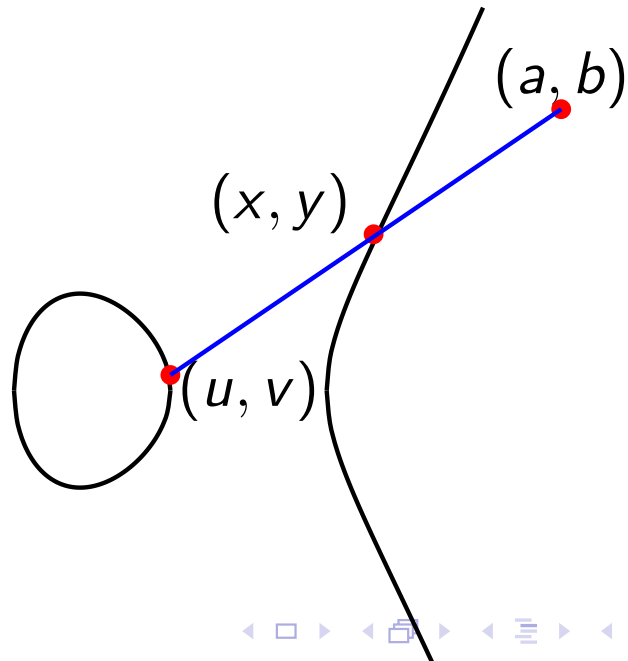
Tate-Lichtenbaum pairing

G ciclico $\qquad m \mid q-1 \qquad m$ primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

$P = (a, b)$ allineato con $(x, y), (u, v) \in S$ se esistono $x, y, u, v, t, z \in \mathbb{F}_q$ con

$$\begin{cases} y^2 = x^3 + Ax + B \\ v^2 = u^3 + Au + B \\ \alpha(x, y) = dt^m \\ \alpha(u, v) = dz^m \end{cases}$$



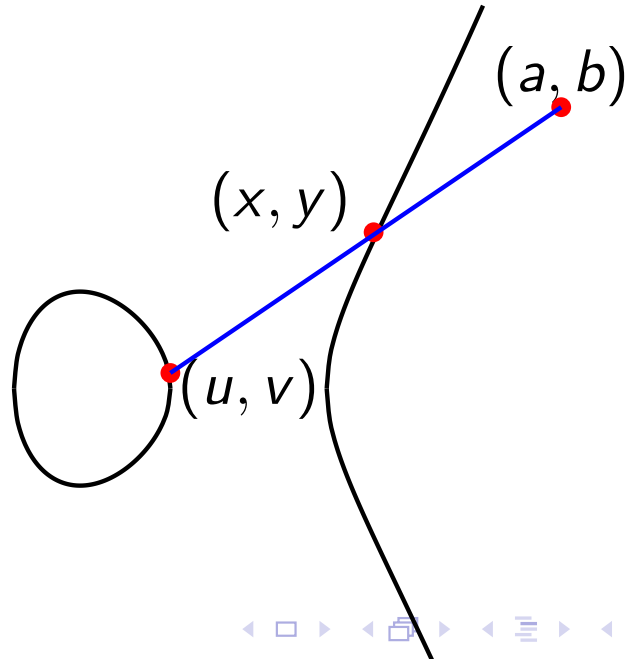
Tate-Lichtenbaum pairing

G ciclico $\qquad m \mid q-1 \qquad m$ primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

$P = (a, b)$ allineato con $(x, y), (u, v) \in S$ se esistono $x, y, u, v, t, z \in \mathbb{F}_q$ con

$$\begin{cases} y^2 = x^3 + Ax + B \\ v^2 = u^3 + Au + B \\ \alpha(x, y) = dt^m \\ \alpha(u, v) = dz^m \\ \det \begin{pmatrix} a & b & 1 \\ x & y & 1 \\ u & v & 1 \end{pmatrix} = 0 \end{cases}$$



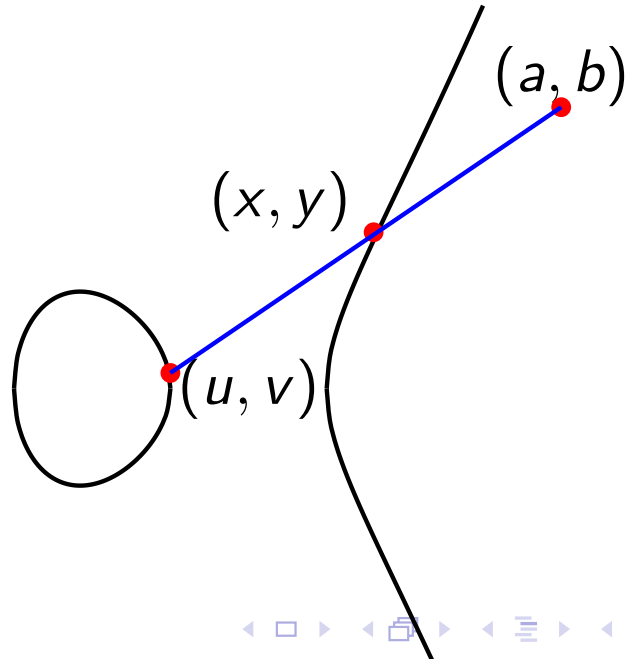
Tate-Lichtenbaum pairing

G ciclico $\qquad m \mid q-1 \qquad m$ primo

$$S = \{R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ per qualche } t \in \mathbb{F}_q^*\}$$

$P = (a, b)$ allineato con $(x, y), (u, v) \in S$ se esistono $x, y, u, v, t, z \in \mathbb{F}_q$ con

$$\mathcal{C}_P : \begin{cases} y^2 = x^3 + Ax + B \\ v^2 = u^3 + Au + B \\ \alpha(x, y) = dt^m \\ \alpha(u, v) = dz^m \\ \det \begin{pmatrix} a & b & 1 \\ x & y & 1 \\ u & v & 1 \end{pmatrix} = 0 \end{cases}$$



Anbar-G.

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un arco completo di $PG(2,q)$ di cardinalità al più

$$m + \lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 31$$

Anbar-G.

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un arco completo di $PG(2,q)$ di cardinalità al più

$$m + \lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 31 \qquad \sim q^{3/4}$$

codimensione generale

Bartoli-G.-Platoni

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un arco completo di $PG(N,q)$ di cardinalità

$$k \leq (\lceil (N+1)/2 \rceil - 1)(\#S-1) + 2\frac{m+1}{N-1} + 2(N+1)$$

codimensione generale

Bartoli-G.-Platoni

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un arco completo di $PG(N,q)$ di cardinalità

$$k \leq (\lceil (N+1)/2 \rceil - 1)(\#S - 1) + 2\frac{m+1}{N-1} + 2(N+1) \sim (\lceil (N+1)/2 \rceil - 1) q^{3/4}$$

codimensione generale

Bartoli-G.-Platoni

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un arco completo di $PG(N,q)$ di cardinalità

$$k \leq (\lceil (N+1)/2 \rceil - 1)(\#S-1) + 2\frac{m+1}{N-1} + 2(N+1) \sim (\lceil (N+1)/2 \rceil - 1) q^{3/4}$$

se m è un divisore primo di $q-1$ con $m < \sqrt[4]{q/64}$, allora esiste un codice MDS di codimensione r e raggio di ricoprimento $r-1$ con lunghezza al massimo

$$\sim (\lceil r/2 \rceil - 1) q^{3/4}.$$

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* (Peverini presso GSEC)
- Watermarking in relazione al potenziamento di immagini di tipo medico (TAC senza mezzo di contrasto).

Didattica

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 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