Marco Timpanella

Curriculum Vitæ

Interessi di ricerca

Strutture Geometriche sopra Campi Finiti, Teoria dei Codici, Crittografia.

Descrizione dell'attività di ricerca

I miei interessi scientifici si collocano principalmente nell'ambito delle Geometrie di Galois, ossia nell'ambito degli spazi affini e proiettivi definiti sopra un campo finito. La mia attività di ricerca è finalizzata allo studio di oggetti di tali spazi e delle loro proprietà combinatorie, algebriche e gruppali, anche in relazione a significative applicazioni alla Teoria dei Codici ed alla Crittografia. Lo studio sistematico di oggetti non-lineari in spazi proiettivi definiti sopra un campo di Galois è iniziato negli anni '50 con il lavoro di Beniamino Segre. L'idea fondamentale di Segre fu quella di associare opportune curve algebriche ad archi piani, introducendo così strumenti di geometria algebrica sopra campi finiti nell'ambito dello studio delle Geometrie di Galois. Questo approccio ha ricevuto un notevole impulso alla fine degli anni '80 con lo sviluppo della teoria di Stöhr-Voloch sul numero dei punti razionali di una curva algebrica definita sopra un campo finito. L'idea centrale di questa teoria è che curve con molti punti razionali devono avere proprietà di non classicità, quali ad esempio, nel caso piano, possedere un numero infinito di punti di flesso. Nel corso degli anni, nello spirito dell'approccio seguito da Segre, una combinazione di strumenti legati alla geometria algebrica sopra campi finiti, alla teoria di gruppi ed alla teoria dei numeri, uniti a sofisticati metodi di natura combinatoria, è stata utilizzata per studiare molteplici oggetti rilevanti collegati alle Geometrie di Galois, come (k, n)-archi, insiemi lineari, ovoidi, polinomi di permutazione e funzioni altamente non-lineari. In questo contesto, gli strumenti più utili risultano essere il teorema di Hasse-Weil e le sue generalizzazioni a dimensioni superiori, la teoria di Stöhr-Voloch e lo studio dei gruppi di automorfismi di curve algebriche in caratteristica positiva.

La mia produzione scientifica si colloca nelle seguenti problematiche centrali delle Geometrie di Galois:

(1) **Curve algebriche sopra campi finiti e loro applicazioni alle Geometrie di Galois.**

(1.1) *Curve con molti automorfismi*.

Nello sviluppo della teoria delle curve algebriche, una problematica rilevante è quante simmetrie (o automorfismi) una curva algebrica possa avere. Nel corso del XIX secolo, a seguito del lavoro fondamentale di Hurwitz, sono stati ottenuti numerosi profondi risultati su gruppi di automorfismi di curve algebriche definite sul campo dei numeri complessi. È

ben noto che se una curva $\mathcal{X}$ ha genere $g \geq 2$, allora il suo gruppo di automorfismi $Aut(\mathcal{X})$ è finito. Inoltre, quando la caratteristica del campo base è zero, la classica limitazione di Hurwitz per il numero di automorfismi di una curva algebrica è $|Aut(\mathcal{X})| \leq 84(g-1)$.

Una delle proprietà principali delle curve algebriche in caratteristica positiva è che esse possono avere gruppi di automorfismi molto più grandi (in rapporto al genere) rispetto al caso di caratteristica zero. La limitazione di Hurwitz potrebbe infatti fallire in caratteristica $p > 0$, se l'ordine di $Aut(\mathcal{X})$ è divisibile per p. Nonostante ciò, curve con molti automorfismi (ovvero che eccedono la limitazione di Hurwitz) sono oggetti piuttosto rari, come testimoniato da risultati di classificazione di Stichtenoth e Henn. La curva Hermitiana ad esempio è l'unica curva per cui $|Aut(\mathcal{X})| > 16g$ (Stichtenoth, 1973). Nel 1978, Henn ha invece classificato le curve di genere $g \geq 2$ con più di $8g^3$ automorfismi. Dalla classificazione di Henn, è possibile osservare che una caratteristica che accomuna le curve con più di $8g^3$ automorfismi è quella di avere p-rango uguale a 0. Il legame tra p-rango e gruppo di automorfismi di una curva algebrica è stato studiato da Nakajima nel 1987, il quale ha dimostrato che se l'ordine di un p-sottogruppo del gruppo di automorfismi della curva è maggiore di $2pg/(p-1)$, allora la curva ha p-rango uguale a 0. Di conseguenza, il p-rango influenza l'ordine di p-sottogruppi di $Aut(\mathcal{X})$. Nello stesso lavoro del 1987, Nakajima ha anche dimostrato la celebre limitazione $|Aut(\mathcal{X})| \leq 84g(g-1)$ per *curve ordinarie*, ovvero curve il cui p-rango coincide con il genere.

In caratteristica positiva, la limitazione di Hurwitz non è valida neanche per i sottogruppi di automorfismi che fissano un punto. Ad esempio, nel caso della curva Hermitiana, lo stabilizzatore di un punto $\mathbb{F}_{q^2}$-razionale ha ordine $q^3(q^2-1)$, che supera notevolmente la limitazione $84(g-1)$, dove $g = q(q-1)/2$ è il genere della curva Hermitiana. Questo solleva il problema di trovare condizioni sufficienti su una curva algebrica $\mathcal{X}$, affinchè la limitazione di Hurwitz valga per lo stabilizzatore di un punto $P \in \mathcal{X}$.
In [8] abbiamo dimostrato che se una curva è ordinaria (o, più in generale, se i secondi gruppi di ramificazione sono banali) e l'ordine dello stabilizzatore di un punto P è maggiore di $12(g-1)$, allora la curva è iperellittica e ordinaria, oppure ha p-rango uguale a 0. Utilizzando questo risultato, è stato anche possibile fornire una dimostrazione alternativa della celebre limitazione di Nakajima, abbassando la costante del bound da 84 a 48.

Uno dei più importanti problemi aperti nella teoria dei gruppi di automorfismi di curve algebriche in caratteristica positiva è capire se la limitazione di Nakajima sia ottimale, almeno asintoticamente (a meno della costante). In [2] abbiamo esibito l'esempio ad oggi più vicino in letteratura a tale bound, ovvero la curva di Dickson-Guralnick-Zieve (DGZ). Tale curva, che è definita a partire dai classici invarianti del gruppo proiettivo lineare $PGL(3,q)$ introdotti da Dickson nel 1911, ha un gruppo di automorfismi isomorfo a $PGL(3,q)$, il cui ordine verifica $|Aut(\mathcal{X})| \approx cg^{8/5}$. Per dimostrare che $PGL(3,q)$ è il gruppo di automorfismi della curva DGZ, è stato necessario combinare lo studio dell'azione e dei gruppi di ramificazione dei p-sottogruppi di $Aut(\mathcal{X})$ con la classificazione dei sottogruppi massimali di $PGL(3,q)$ di Mitchell (1911) e Hartley (1925). Quando $q = p$, abbiamo inoltre dimostrato che la curva DGZ è ordinaria. Secondo una celebre congettura di Guralnick e Zieve, la limitazione di Nakajima per curve ordinarie non è ottimale e può essere portata a $|Aut(\mathcal{X})| \leq Kg^{8/5}$, per una qualche costante K. Se tale congettura fosse vera, la curva DGZ avrebbe il massimo numero possibile di automorfismi (asintoticamente, a meno di una costante) per una curva ordinaria.

In [23] abbiamo ottenuto per la prima volta in letteratura una limitazione sull'ordine di gruppi di automorfismi in cui compaiono contemporaneamente il p-rango ed il genere della curva, facendo nuovi progressi verso la dimostrazione che il bound di Nakajima non è ottimale. L'approccio utilizzato è stato una combinazione di strumenti dalla teoria sui campi di funzioni razionali associati ad una curva algebrica, e profondi risultati di teoria dei gruppi come le classificazione di gruppi 2 transitivi di Hering, Holt e O'Nan.

Il ricorso ai risultati su gruppi 2 transitivi di Hering, Holt e O'Nan, ha anche permesso in [7] di classificare i gruppi di automorfismi di curve algebriche con due punti di Galois interni. Il concetto di *punto di Galois* per una curva piana C in $PG(2,\mathbb{K})$, ovvero un punto P tale che l'estensione di campi di funzioni razionali $\mathbb{K}(\mathcal{X})|\pi_P^*(\mathbb{K}(PG(1,\mathbb{K}))$ è di Galois, è stato introdotto da Yoshihara nel 1990. Da allora molti articoli sono stati dedicati al problema di determinare il numero di punti di Galois di una data curva algebrica. Mentre per curve non-singolari tale problema è stato risolto, se si ammettono singolarità la questione è molto più complicata. In questo caso, la nostra classificazione è stata possibile dimostrando che l'azione del gruppo generato dai due gruppi di Galois associati ai due punti di Galois è 2 transitiva, il che ci ha permesso di utilizzare i risultati di Hering, Holt e O'Nan precedentemente citati.

(1.2) *Archi da curve algebriche*.
La nozione di *k-arco* di uno spazio affine $AG(r,q)$ o proiettivo $PG(r,q)$ di dimensione $r \geq 2$ e definito sopra un campo $\mathbb{F}_q$ di Galois di ordine q è puramente combinatoria, essendo un k-arco un sottoinsieme di $k \geq r+1$ punti mai $r+1$ dei quali situati su di uno stesso iperpiano. Un k-arco è *completo* (o *massimale*) se non è contenuto in un $(k+1)$-arco dello stesso spazio. Dai k-archi si ottengono codici MDS (maximum distance separable codes) e viceversa; i codici MDS sono codici lineari che correggono il maggior numero di errori rispetto ai loro parametri (lunghezza e dimensione). Mediante una successione di $r-2$ proiezioni, ogni k-arco di uno spazio di dimensione r con $k > r$ si trasforma in $(k-r+2)$-arco piano. Anche per questo, i k-archi piani rivestono particolare importanza nelle Geometrie di Galois.
Uno dei più celebri risultati di Beniamino Segre è la caratterizzazione di archi grandi in piani di Galois di ordine dispari come insieme di punti di una conica irriducibile. Questo risultato ha aperto una strada al filone di ricerca che studia oggetti non lineari cercando di associare ad essi curve o varietà algebriche, in modo da poter utilizzare strumenti profondi di geometria algebrica.

Nel piano proiettivo, il concetto di arco si generalizza a quello di (k,n)-arco, ovvero un insieme di k punti di cui $n+1$ non sono mai allineati. Anche ad un (k,n)-arco piano è possibile associare un codice lineare di lunghezza k e dimensione 3. Le sue capacità di correzione di errori risultano tanto migliori quanto più è grande la differenza $k-n$. Il codice lineare associato ad un (k,n)-arco è pertanto particolarmente interessante quando k è grande rispetto a n. In particolare, il codice risulta ottimale rispetto al limite di Griesmer quando $k > (n-2)q+n$.

Un esempio naturale di (k,n)-arco di $PG(2,q)$ è rappresentato dall'insieme dei punti razionali di una curva algebrica di ordine n definita sopra $\mathbb{F}_q$. Tuttavia, tale (k,n)-arco è in generale incompleto. In [2,21], abbiamo fornito esempi di (k,n)-archi completi a partire da curve algebriche.

In particolare, in [21], abbiamo dimostrato che l'insieme dei punti $\mathbb{F}_{q^6}$-razionali di una curva

Hermitiana è un $(q^6+1+q(q-1)q^3, q+1)$-arco completo se q è sufficientemente grande. L'idea principale nel nostro approccio è quella di tradurre la condizione di collinearità tra punti dell'arco nell'esistenza di punti opportuni di varietà algebriche di dimensione 3 sopra $\mathbb{F}_q$.
In [2] invece, sfruttando le ricche proprietà combinatoriche della curva DGZ, abbiamo dimostrato che l'insieme dei suoi punti $\mathbb{F}_{q^3}$-razionali costituisce un $(q^6-q^5-q^4+q^3, q^3-q^2)$-arco completo.

(1.3) *Curve massimali*.
Lo studio sistematico di curve con molti punti razionali è iniziato con il lavoro pionieristico di J.P. Serre. Da allora, l'attenzione verso questo argomento è cresciuta notevolmente, sia per l'intrinseco interesse teorico che per i legami con la Teoria dei Codici e la Crittografia. Una curva algebrica proiettiva non singolare, assolutamente irriducibile di genere g sopra un campo finito $\mathbb{F}_q$ di ordine q ha al più $q+1+2g\sqrt{q}$ punti razionali, come affermato dal celebre teorema di Hasse-Weil. Utilizzando la funzione zeta, da tale limitazione segue l'ipotesi di Riemann per i campi di funzioni sopra campi di Galois (Bombieri, 1972/1973). Curve che raggiungono la limitazione di Hasse-Weil vengono dette *curve massimali*. Esempi di curve massimali sono le curve di Deligne-Lusztig associate al gruppo unitario (ovvero la curva Hermitiana), al gruppo di Suzuki e al gruppo di Ree.
Fra i metodi usati per la costruzione di curve massimali spicca quello di considerare curve quoziente di una curva data rispetto ad un suo sottogruppo di automorfismi. Si ha ad esempio che, per un risultato attribuito a Serre (1987), ogni curva ricoperta da una curva massimale, e quindi in particolare ogni sua curva quoziente, è ancora una curva massimale. Chiaramente, curve massimali di genere positivo possono esistere solo per campi di ordine quadrato. Un miglioramento della limitazione di Hasse-Weil nel caso in cui q non è un quadrato è stato fornito da Serre nel 1983. Tale limitazione è oggi nota come *Serre bound*. Mentre la letteratura sulle curve massimali è molto ricca, vi sono ad oggi relativamente pochi esempi di curve che verificano il Serre bound ma che non sono massimali.

Utilizzando i teoremi di Kani-Rosen e di Tate-Lachaud sulla decomposizione della varietà Jacobiana di una curva algebrica, in [24] abbiamo esibito nuovi esempi di curve algebriche di genere 10 che verificano le limitazioni di Serre e di Hasse-Weil. Tali esempi appartengono ad una famiglia che comprende le riduzioni modulo p delle classiche superfici di Riemann di Wiman (1896) e di Edge (1981).

In [19] introduciamo e studiamo una generalizzazione della curva di Bring (definita originariamente sul campo dei complessi) al caso di caratteristica positiva. La curva di Bring, definita in $PG(4,\mathbb{C})$ come l'intersezione delle ipersuperfici di equazioni $x_1^k+\ldots+x_5^k=0$, $k=1,2,3$, è ben nota in geometria algebrica classica avendo il massimo numero di automorfismi per una curva di genere 4 definita sul campo complesso. Una possibile (e naturale) generalizzazione di tale curva, valida per ogni campo $\mathbb{K}$ di caratteristica 0 o di caratteristica positiva $p \geq 7$, è la curva algebrica di $PG(m-1,\mathbb{K})$ definita come intersezione delle ipersuperfici di equazioni $x_1^k+\ldots+x_m^k=0$, con $k=1,\ldots,m-2$ e $m \geq 5$. Quando $m=5$, tale curva ha genere 4 ed è $\mathbb{F}_{p^2}$-massimale per infiniti primi p. Questo risultato da quindi nuovi contributi allo studio di curve $\mathbb{F}_{p^2}$-massimali di genere basso iniziato da Serre nel 1985. La massimalità di tali curve è stata dimostrata utilizzando i teoremi di Kani-Rosen e di Tate-Lachaud.

Infine, in [2] dimostriamo che la curva DGZ (precedentemente nominata in riferimento al

suo gruppo di automorfismi) ha il massimo numero di punti $\mathbb{F}_{q^3}$-razionali per una curva piana definita su $\mathbb{F}_{q^3}$ e avente stesso grado e genere della curva DGZ.

(2) **Teoria dei codici.**

(2.1) *Codici AG e codici quantici.*

Nel 1980, Goppa ha descritto un metodo per costruire dei codici lineari, oggi denominati *codici algebrico-geometrici* (brevemente AG) a partire da una curva algebrica. Come dimostrato da Goppa, il difetto di Singleton di tali codici è al più g/N, dove g è il genere della curva, mentre N può essere al massimo il numero di punti $\mathbb{F}_q$ razionali della curva. Ne segue che, a parità di genere, le curve massimali sono le curve migliori per costruire codici AG. In [1,4,11] abbiamo costruito codici AG estremamente performanti da tre diverse famiglie di curve massimali (Skabelund, Hermitiana, GK), sfruttando le ricche proprietà algebriche e combinatoriche di tali curve. Gli ingredienti fondamentali per determinare i parametri dei codici AG sono lo studio di spazi di Riemann-Roch e di semigruppi di Weierstrass (in un punto o in più punti della curva).

In seguito all'introduzione da parte di Shor di algoritmi in grado di risolvere in tempo polinomiale i problemi della fattorizzazione in numeri primi e del logaritmo discreto, il tema della quantum communication ha ricevuto notevole attenzione. In particolare, lo studio di metodi di correzione di errori in scenari quantistici ha ricevuto un grande impulso. La costruzione CSS (Calderbank-Shor-Steane, 1996) ha mostrato come i cosiddetti codici quantici possano in realtà essere ottenuti a partire da codici lineari classici che soddisfano determinate condizioni di auto-ortogonalità. Tra i codici lineari utilizzati per costruire codici quantici, i codici AG sono quelli presi maggiormente in considerazione. Per tali codici infatti, le condizioni di auto-ortogonalità sono ben note e facilmente controllabili.

In [1] abbiamo costruiamo codici AG con buoni parametri a partire dalle curve massimali di Skabelund, definite come estensioni cicliche delle curve di Suzuki e Ree. Tramite la CSS construction, abbiamo potuto anche ottenere famiglie di codici quantici.

In [4], ci concentriamo sulla costruzione di duali di codici AG a partire dalla curva Hermitiana. Tramite lo studio di semigruppi di Weierstrass in più punti, riusciamo ad esibire famiglie di codici la cui capacità di correttore è notevolmente superiore rispetto ai corrispettivi codici Hermitiani di tipo one-point aventi stessa lunghezza e dimensione. I codici ottenuti inoltre ereditano un gruppo di automorfismi dalla curva Hermitiana molto ampio, essendo isomorfo a $PGU(3, q)$. Questa proprietà è molto utile in quanto costituisce un valido aiuto nell'implementazione di efficienti algoritmi di decodifica dei codici.

Il semigruppo di Weierstrass in un punto P della curva GK (il primo esempio di curva massimale non ricoperta dalla curva Hermitiana) è stato calcolato esplicitamente da Giulietti e Korchmaros nel 2009 se P è $\mathbb{F}_q$-razionale e da Beelen e Montanucci se P è $\mathbb{F}_{q^6}$-razionale. In [11] abbiamo determinato il semigruppo di Weierstrass nel caso rimanente, ovvero se P è un punto della curva GK non $\mathbb{F}_{q^6}$-razionale, fornendo una esplicita descrizione per un insieme minimale di generatori per tale semigruppo. Questo risultato è stato poi utilizzato per costruire codici AG da punti $\mathbb{F}_{q^7}$-razionali della curva GK, e loro duali.

(2.2) *Codici MRD.*

Insiemi di matrici dotate della metrica del rango formano uno spazio metrico. Sottospazi lineari di questo spazio definiscono dei codici detti codici rank-metric, introdotti da Delsarte nel 1978. L'interesse verso questi oggetti è dovuto sia alle applicazioni pratiche nell'ambito del network coding, che al legame con altri oggetti matematici, come insiemi lineari,

polinomi linearizzati e semicampi. In particolare, un codice rank-metric si dice "maximum rank distance" (MRD) se sono ottimali rispetto alla capacità di correzione di errore a parità degli altri parametri.
In [17] abbiamo considerato una famiglia di codici rank-metric in $\mathbb{F}_q^{n\times n}$ collegati a polinomi della forma $x^{q^s} + \delta x^{q^{\frac{n}{2}+s}} \in \mathbb{F}_{q^n}[x]$. Questa famiglia, introdotta da Csajbók, Marino, Polverino e Zanella, è stata una fonte di esempi di codici MRD. Infatti, per q dispari, se $n = 8$ e $\delta^{1+q^4} = -1$, allora tali codici sono MRD. In [17] abbiamo dimostrato che questa condizione su δ è in realtà necessaria e sufficiente se si suppone che q sia sufficientemente grande. Le tecniche utilizzate sono di geometria algebrica sopra campi finiti e si basano sullo studio di una certa varietà algebrica $\mathbb{F}_q$-razionale di dimensione 3 nello spazio proiettivo 7-dimensionale.
In [22] abbiamo esibito un nuovo esempio di insieme lineare maximum scattered in caratteristica 2, e quindi nuovi esempi di codici MRD. Lo strumento fondamentale è stato lo studio delle componenti assolutamente irriducibili di varietà algebriche di dimensione 3 definite su campi finiti di ordine pari e l'applicazione di risultati di tipo Lang-Weil.

(2.3) *Codici lineari per la Crittografia.*
I codici minimali e i codici PIR sono due tipologie di codici lineari che trovano applicazioni in Crittografia. In particolare, i codici minimali hanno attratto un crescente interesse per via delle loro applicazioni ai secret sharing schemes. Infatti, nello schema di Massey, il supporto di una parola codice è visto come la struttura di accesso per recuperare un segreto comune, se si suppone che tale supporto non sia contenuto nel supporto di nessuna altra parola codice (ad eccezione delle parole codice proporzionali a quella data). Parole codice con questa proprietà sono dette minimali, e codici le cui parole sono tutte minimali si dicono codici minimali. Come recentemente dimostrato, i codici minimali corrispondono a particolari famiglie di blocking sets in spazi di Galois.
In [12] abbiamo mostrato come oggetti classici di geometria finita, quali quadriche e varietà Hermitiane, diano luogo a codici minimali. In [10], abbiamo determinato completamente la distribuzione dei pesi di particolari famiglie di codici minimali. In generale, la determinazione della distribuzione dei pesi di un codice lineare è un compito difficile, ma permette di ricavare diverse informazioni sul codice. Infine, in [20] indaghiamo le parole minimali di codici di valutazione da varietà di tipo norma-traccia.
I codici PIR trovano invece applicazioni nel cloud computing nell'ambito del problema del recupero privato delle informazioni. In [16] l'esistenza di codici PIR è ricondotta all'esistenza di particolari configurazioni combinatoriche. Attraverso strumenti di combinatoria e geometria finita, codici PIR con parametri migliori rispetto allo stato dell'arte sono presentati.

(3) **Funzioni sopra campi finiti e applicazioni.**
Un grande numero di funzioni su campi finiti hanno rilevanti applicazioni in diverse aree della matematica, quali ad esempio la Crittografia e la Teoria dei Codici. Esempi di tali funzioni sono polinomi di permutazione, funzioni planari (PN), funzioni APN, e loro generalizzazioni. Questi oggetti hanno ricevuto una notevole attenzione nelle ultime decadi. In alcune situazioni, al fine di ottenere risultati di non esistenza o costruzioni esplicite di tali oggetti, è utile associare a tali oggetti delle varieta su campi finiti e determinare delle limitazioni inferiori sul numero di punti razionali che esse possiedono. In tale ambito sono quindi fondamentali risultati quali il teorema di Hasse-Weil o sue generalizzazioni a dimensioni superiori. È

bene tuttavia specificare che tutti questi risultati necessitano che la varieta sotto esame sia assolutamente irriducibile o che possieda almeno una componente assolutamente irriducibile e definita sul campo base.

(3.1) *Polinomi di permutazione.*
Un polinomio $f(x) \in \mathbb{F}_q[x]$ è detto *polinomio di permutazione* di $\mathbb{F}_q$ se induce una permutazione degli elementi di $\mathbb{F}_q$. Un polinomio di permutazione di $\mathbb{F}_q$ che induce una permutazione su infinite estensioni di $\mathbb{F}_q$ si dice *eccezionale*. Lo studio di questi oggetti, iniziato con il lavoro fondamentale di Hermite e Dickson, è stato motivato dal loro intrinseco interesse teorico. Ad aumentare ulteriormente l'interesse verso i polinomi di permutazioni si sono aggiunti, negli ultimi decenni, i forti legami con aree più applicate della Matematica, quali Crittografia e Teoria dei Codici. In linea teorica, costruire un polinomio di permutazione di $\mathbb{F}_q$ non è complicato, essendo il loro numero $q!$. Tuttavia, per le applicazioni spesso sono richiesti polinomi di una forma specifica (con pochi termini o restrizioni sui coefficienti), o permutazioni con una struttura in cicli particolare. Esistono numerose famiglie di polinomi di permutazione che hanno strutture molto particolari. Tra di essere ricordiamo monomi, binomi, polinomi di Dickson, polinomi linearizzati. Per stabilire se una specifica famiglia di polinomi definisca una biezione di $\mathbb{F}_q$, metodi di geometria algebrica si sono rivelati spesso molto utili. Il collegamento tra curve e polinomi di permutazione è ben conosciuto: un polinomio $f(x) \in \mathbb{F}_q[x]$ è di permutazione di $\mathbb{F}_q$ se la curva algebrica C_f di equazione affine $(f(x) - f(y))/(x - y) = 0$ non ha punti $\mathbb{F}_q$-razionali in fuori dalla retta $x - y = 0$. In generale, questo metodo non è applicabile direttamente a causa della difficolta della ricerca diretta di punti razionali. Per questo motivo metodi basati sulla ricerca di componenti assolutamente irriducibili definite sullo stesso campo di definizione del polinomio vengono applicati. Teoremi di tipo Hasse-Weil sul numero di punti razionali sono dunque utilizzati per dedurre una limitazione inferiore a tale numero. L'esistenza di tali componenti nella curva C_f è provata attraverso metodi differenti, che vanno dall'analisi dei punti singolari, a stime su molteplicita di intersezione, alla ricerca di rami razionali.

Mentre la letteratura su monomi e binomi di permutazione è estremamente ricca, molto meno è noto per trinomi di permutazione. Una famiglia di polinomi particolarmente studiata nella teoria dei polinomi di permutazione è stata introdotta da Niho nel 1972. I polinomi di permutazione che appartengo a questa famiglia sono detti *polinomi di permutazione da esponenti Niho*, o semplicemente polinomi di tipo Niho. In [14], utilizzando gli strumenti di geometria algebrica sopra descritti, abbiamo studiato la generica famiglia di trinomi di tipo Niho nel caso q pari. Come prevedibile, la classificazione di trinomi di permutazione di questo tipo nel caso generale è estremamente complicata da ottenere, ma i risultati ottenuti possono essere applicati come punto di partenza nello studio di famiglie specifiche di trinomi di tipo Niho.
In [6], usando la connessione tra polinomi di permutazione e curve algebriche, abbiamo studiato una specifica famiglia di trinomi di tipo Niho, dimostrando che le condizioni sufficienti affinchè tali polinomi siano di permutazione sono anche necessarie.

(3.2) *Funzioni planari, APN, e loro generalizzazioni.*
La principale applicazione di funzioni definite sopra campi finiti in Crittografia riguarda la progettazione di particolari componenti (dette S-boxes) utilizzate nei moderni crittosistemi simmetrici. Affinché tali primitive siano resistenti ad attacchi di crittanalisi differenziale, è necessario utilizzare funzioni con particolari proprietà di non-linearità. In particolare,

dato $f \in \mathbb{F}_q[x]$, si richiede che l'equazione $f(x+a) - f(x) = b$ abbia poche soluzioni per ogni $a, b \in \mathbb{F}_q$, $a \neq 0$. Funzioni per cui tale equazione ammette sempre un'unica soluzione si dicono *planari*. Come dimostrato da Dembowski ed Ostrom (1968), le funzioni planari possono essere usate per costruire piani proiettivi finiti. In [18] la ricerca delle funzioni è stata estesa per la prima volta in letteratura a funzioni razionali (e non solo polinomiali). Infatti, nonostante sia noto che ogni funzioni di $\mathbb{F}_q$ può essere espressa in forma polinomiale, cercare funzioni planari razionali permette in taluni casi di usare risultati di tipo Hasse-Weil sui punti di varietà algebriche associate alla funzione razionale.

Se q è pari, una funzione non può mai essere planare. Quindi, in caratteristica 2, le funzioni migliori da un punto di vista crittografico sono le cosiddette *funzioni APN*, per le quali $f(x+a) - f(x) = b$ ammette al massimo due soluzioni. Nonostante l'utilità delle funzioni APN, non vi è apparentemente un legame tra queste e piani proiettivi (come succede per le funzioni planari). Per questo, Zhou ha recentemente introdotto una generalizzazione di funzione planare in caratteristica 2, le cosiddette funzioni *pseudo-planari* con proprietà simili della loro controparte in caratteristica dispari. In [5], attraverso lo studio delle componenti di una curva algebrica di grado 3, abbiamo fornito una classificazione completa per una famiglia di binomi pseudo-planari. In [3] invece abbiamo proposto una possibile generalizzazione del concetto di funzione planare valido in ogni caratteristica, e studiato funzioni ottimali rispetto a questa nuova definizione. Come osservato in lavori successivi, questa generalizzazione è di grande importanza in ambito crittografico, e si è aperto un filone di ricerca votato allo studio di queste famiglie di funzioni (solitamente denominate PcN e APcN).

In Crittografia, si richiede spesso che le funzioni APN da implementare siano anche delle permutazioni del campo base (di caratteristica 2). Tuttavia queste funzioni, dette *permutazioni APN*, sono estremamente rare, e pochissimo è noto in letteratura. Se $\mathbb{F}_q$ ha dimensione dispari come spazio vettoriale su $\mathbb{F}_2$, si conoscono due famiglie infinite di permutazioni APN, e due esempi sporadici. Se la dimensione invece è pari, solo un esempio sporadico, trovato da Browning, Dillon, McQuistan e Wolf nel 2009, è noto. A lungo si era addirittura ritenuto che non esistessero permutazioni APN nel caso di dimensione pari. In [14], tramite lo studio di un'opportuna varietà algebrica, abbiamo dimostrato che una famiglia di funzioni che contiene due esempi sporadici di permutazioni APN in dimensione 9, non ne contiene altri. Una tipologia ancor più particolare di funzioni permutazione APN, dette *funzioni crooked*, è stata introdotta nel 1998 da Bending e Fon-Der-Flaass. Oltre alla loro utilità pratica, questi oggetti sono di grande interesse combinatorico, essendo collegati a funzioni bent, Kerdock sets, grafi distance-regular, codici Preparata e codici BCH. In [15] abbiamo fornito risultati di non esistenza per funzioni crooked eccezionali,ovvero funzioni crooked per infinite estensioni di $\mathbb{F}_2$. L'approccio usato consiste nel collegare al problema una varietà algebrica e permette di fare passi avanti nella dimostrazione della congettura di Bierbrauer e Kyureghyan secondo cui tutte le funzioni crooked sono polinomi quadratici, ovvero del tipo $\sum_{i<j} a_{i,j} X^{2^i+2^j} + \sum_k b_k X^{2^k} + c$.

Formazione e posizioni

01.01.2022–presente **Ricercatore a tempo determinato (RtdA)**, *Università degli Studi di Perugia*, Perugia (Italia).
Progetto di ricerca: "Metodi matematici per la firma digitale ed il cloud computing".

01.09.2021–31.12.2021 **Postdoctoral Fellow**, *University College Dublin*, Dublino (Irlanda).
Progetto di ricerca: "Algebraic curves over finite fields and their applications to coding theory and cryptography".

01.12.2020–31.08.2021 **Assegnista di ricerca**, *Università degli Studi della Campania "Luigi Vanvitelli"*, Caserta (Italia).
Progetto di ricerca: "Coding Theory and Applications to Encryption" (S.S.D MAT/03).

01.11.2017–01.11.2020 **Dottorato in Matematica (XXXIII ciclo)**, *Università degli Studi della Basilicata*, Potenza (Italia), Eccellente cum laude.
Titolo della tesi: "Algebraic curves over finite fields and their applications"; supervisor: Prof. G. Korchmáros.
Borsa di studio a tematica vincolata sul progetto "Sviluppo e realizzazione di strumenti di sicurezza informatica per aziende del territorio mediante un approccio di Geometria Combinatoria", Industria 4.0.

19.10.2015–28.04.2017 **Laurea Magistrale in Matematica**, *Università degli Studi di Perugia*, 110/110 cum laude.
Titolo della tesi: "Codici da curve massimali"; relatore: Prof. M. Giulietti.

10.10.2011–25.02.2015 **Laurea Triennale in Matematica**, *Università degli Studi di Perugia*, 110/110 cum laude.
Titolo della tesi: "Preordini e rappresentazioni mediante famiglie di funzioni continue"; relatore: Prof. A. Caterino.

2006–2011 **Diploma di Maturità Scientifica**, *Liceo Scientifico Statale "Galileo Galilei"*, Perugia (Italia), 100/100 cum laude.

Premi, borse di studio, finanziamenti

2023 **Early Career Travel Award**
Assegnato da Society for Industrial and Applied Mathematics (SIAM) per la partecipazione alla conferenza "2023 SIAM Conference on Applied Algebraic Geometry".

2021 **Thomas Mitchell Medal of Excellence**
Assegnata da Irish Research Council in quanto ricercatore top-ranked nell'area STEM (*https://research.ie/what-we-do/loveirishresearch/blog/top-ranked-irc-postgraduate-and-postdoctoral-researchers-awarded-the-2021-medals-of-excellence/*).

2021 **Postdoc Grant of the Irish Research Council**
Progetto: "Algebraic curves over finite fields and their applications to coding theory and cryptography", EUR 96'417.
Unico vincitore per la sezione *"Pure Mathematics"*.
Progetto valutato top-ranked nella categoria STEM (Science, Technology, Engineering and Mathematics).

2020 **Postdoctoral fellowship**, Coding and Information Theory at Simula Group's.
EUR 160'000, *rifiutata.*

2019 **Finanziamento da parte del gruppo INdAM (GNSAGA)**, per la partecipazione a "SIAM 2019".

2019 **Finanziamento da parte del Bolyai Institute**, per un soggiorno di ricerca presso il Bolyai Institute.

2018 **Finanziamento da parte di University of Primorska**, per la partecipazione alla 8th PhD Summer School in Discrete Mathematics, Rogla (Slovenia).

2018 **Borsa di dottorato**, *Università degli Studi del Salento/Università della Basilicata.*

2018 **Borsa di dottorato**, *Università degli Studi di Trento.*
Rifiutata.

Coordinatore dei seguenti progetti scientifici

2023–2024 Progetto di ricerca GNSAGA-INDAM: "Curve algebriche e loro applicazioni" (codice CUPE55F22000270001) (Partecipanti: Arianna Dionigi, Barbara Gatti, Federico Alberto Rossi).

Comunicazioni scientifiche

13.07.2023 **SIAM Conference on Applied Algebraic Geometry (AG23) (su invito)**, *Eindhoven University of Technology, Eindhoven, The Netherlands*
Titolo della comunicazione: "*Algebraic Geometric Methods in Coding Theory and Cryptography: Some Recent Results*".

07.07.2023 **29th Nordic Congress of Mathematicians (with EMS) (su invito)**, *Aalborg, Denmark*
Titolo della comunicazione: "*From curves to codes: applying Algebraic Geometry in Coding Theory*".

22.06.2023 **International Conference on Finite Fields and Their Applications 2023 (Fq15)**, *Campus Condorcet, Aubervilliers, France*
Titolo della comunicazione: "*Algebraic curves in positive characteristic and their invariants*".

28.04.2023 **Ciclo di seminari del Corso di Laurea in Matematica**, *Università degli Studi di Perugia*
Titolo della comunicazione: "*Nuove sfide (e soluzioni) in Crittografia: computer quantistici e privacy*".

08.02.2023 **Young researchers@DMI: V Workshop of the Department of Mathematics and Computer Science University of Perugia**, *Perugia, Italia.*
Titolo della comunicazione: "*Algebraic curves and their applications*".

30.08.2022 **WAIFI 2022**, *Chengdu, China.*
Titolo della comunicazione: "*PIR codes from combinatorial structures*".

30.05.2022 **Combinatorics 2022**, *Università degli Studi di Modena e Reggio Emilia.*
Titolo della comunicazione: "*A generalization of Bring's curve in any characteristic*".

10.02.2022 **Algebra and Number Theory Seminars (su invito)**, *University College Dublin (UCD).*
Titolo della comunicazione: "*On a generalization of Bring's curve*".

22.09.2021 **Cryptography and Coding Theory First Annnual Conference**, *Unione Matematica Italiana e De Componendis Cifris.*
Titolo della comunicazione: "*PIR codes from combinatorial structures*".

02.03.2021 **eSeminar "Galois Geometries and Their Applications: young seminars" (su invito)**, *Università della Campania "Luigi Vanvitelli".*
Titolo della comunicazione: "*Algebraic curves and (one of) their applications*".

16.10.2019 **De Cifris incontra Perugia (su invito)**, *Università degli Studi di Perugia.*
Titolo della comunicazione: "*Una concreta applicazione della crittografia su curve ellittiche*".

12.07.2019 **SIAM Conference on Applied Algebraic Geometry 2019 (su invito)**, *University of Bern.*
Titolo della comunicazione: "*Codes and gap sequences of Hermitian curves*".

19.02.2019 **Presentazione progetti di Dottorato Industriale**, *Università degli Studi della Basilicata.*
Titolo della comunicazione: "*Curve Algebriche: dalla Teoria dei Codici alla Crittografia*".

04.06.2018 **Combinatorics 2018**, *Università degli Studi di Trento.*
Titolo della comunicazione: "*On the Dickson-Guralnick-Zieve curve*".

Organizzatore dei seguenti eventi scientifici

21.09.2023–22.09.2023 Membro del comitato organizzatore locale per il convegno annuale del gruppo UMI di Cittografia e Codici (`https://sites.google.com/view/crittografiaecodici/convegno-annuale-2023`)

13.06.2023–16.06.2023 Workshop "Algebraic curves over a finite field" (`https://sites.google.com/view/marcotimpanella/eventi/algebraic-curves-over-a-finite-field`)

2021–presente Galois geometry and their applications e-seminars.

2021–presente Galois geometry and their applications young e-seminars.

Referee per le seguenti riviste internazionali

Journal of Algebra (1)

IEEE Transactions on Information Theory (1)

IEEE Transactions on Communications (1)

Finite Fields and Their Applications (13)

Advances in Mathematics of Communications (4)
Designs, Codes and Cryptography (14)
Ars Combinatoria (1)
Cryptography and Communications (1)
Discrete Mathematics (1)
Journal of Applied Mathematics and Computing (1)
Mathematics (2)
Symmetry (1)
Electronic Research Archive (1)
MathSciNet (11)
zbMATH Open (6)

Referee per i seguenti convegni internazionali

"International Workshop on the Arithmetic of Finite Fields" WAIFI 2020.

Partecipazione a progetti di ricerca

Progetto P.R.I.N. 2020 "Geometrie di Galois e Strutture di Incidenza" (coordinatore del progetto M. Buratti).

Membership

- Socio fondatore dell'Associazione nazionale di Crittografia "De componendis Cifris" (`https://www.decifris.it/`).
- Membro del Gruppo Nazionale di ricerca INdAM per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA).
- Membro dell'Unione Matematica Italiana.

Pubblicazioni

[1] M. Montanucci, M. Timpanella and G. Zini, *AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves*, Journal of Geometry vol. 109, 23 (2018). (DOI:10.1007/s00022-018-0428-0)

[2] M. Giulietti, G. Korchmáros and M. Timpanella, *On the Dickson-Guralnick-Zieve curve*, Journal of Number Theory vol. 196, 114-138 (2019). (DOI:10.1016/j.jnt.2018.09.020)

[3] D. Bartoli and M. Timpanella, *On a generalization of planar functions*, M. J. Algebr. Comb., vol. 52, 187-213 (2020). (DOI:10.1007/s10801-019-00899-2)

[4] G. Korchmáros, G. P. Nagy and M. Timpanella, *Codes and gap sequences of Hermitian curves*, IEEE Transactions on Information Theory, vol. 66, 3547-3554 (2020). (DOI: 10.1109/TIT.2019.2950207)

[5] D. Bartoli and M. Timpanella, *A family of planar binomials in characteristic 2*, Finite Fields and Their Applications vol. 63, 101651 (2020). (DOI: 10.1016/j.ffa.2020.101651)

[6] D. Bartoli and M. Timpanella, *A family of permutation trinomials in* $\mathbb{F}_{q^2}$, Finite Fields and Their Applications vol. 70, 101781 (2021). (https://doi.org/10.1016/j.ffa.2020.101781)

[7] G. Korchmáros, S. Lia and M. Timpanella, *Curves with more than one inner Galois point*, Journal of Algebra vol. 566, 374-404 (2021), https://doi.org/10.1016/j.jalgebra.2020.08.024.

[8] S. Lia and M. Timpanella, *Bound on the order of the decomposition groups of an algebraic curve in positive characteristic*, Finite Fields and Their Applications vol. 69, 101771 (2021). (https://doi.org/10.1016/j.ffa.2020.101771)

[9] D. Bartoli and M. Timpanella, *On trinomials of type* $X^{n+m}(1 + AX^{m(q-1)} + BX^{n(q-1)})$, n, m *odd, over* $\mathbb{F}_{q^2}$, $q = 2^{2s+1}$, Finite Fields and Their Applications, vol. 72, 101816 (2021). (https://doi.org/10.1016/j.ffa.2021.101816)

[10] D. Bartoli, M. Bonini and M. Timpanella, *On the weight distribution of some minimal codes*, Designs, Codes and Cryptography, vol. 89, 471-487 (2021). (https://doi.org/10.1007/s10623-020-00826-8)

[11] S. Lia and M. Timpanella, *AG codes from* $\mathbb{F}_{q^7}$*-rational points of the GK curve*, Applicable Algebra in Engineering, Communication and Computing, (2021). (https://doi.org/10.1007/s00200-021-00519-2)

[12] M. Bonini, S. Lia and M. Timpanella, *Minimal linear codes from Hermitian varieties and quadrics*, Applicable Algebra in Engineering, Communication and Computing, (2021). (https://doi.org/10.1007/s00200-021-00500-z)

[13] D. Bartoli, M. Giulietti and M. Timpanella, *2-1 functions from Galois extensions*, Discrete Applied Mathematics, vol. 309, 194-201 (2022). (DOI:10.1016/j.dam.2021.12.008)

[14] D. Bartoli and M. Timpanella, *On a conjecture on APN permutations*, Cryptography and Communications, vol. 14, 925-931 (2022). (DOI:10.1007/s12095-022-00558-7)

[15] D. Bartoli, M. Calderini and M. Timpanella, *Exceptional crooked functions*, Finite Fields and Their Applications, vol. 84, 102109 (2022). (DOI:10.1016/j.ffa.2022.102109)

[16] M. Giulietti, A. Sabatini and M. Timpanella, *PIR codes from combinatorial structures*, Arithmetic of Finite Fields, WAIFI 2022, Lecture Notes in Computer Science, vol 13638. Springer, Cham (2023). (DOI:10.1007/978-3-031-22944-2_ 10)

[17] M. Timpanella and G. Zini, *On a family of linear MRD codes with parameters* $[8 \times 8, 16, 7]_q$, Designs, Codes and Cryptography, (2023). (DOI:10.1007/s10623-022-01179-0)

[18] D. Bartoli and M. Timpanella, *Investigating perfect nonlinear rational functions*, Annali di Matematica Pura e Applicata (2023). (DOI10.1007/s10231-023-01339-6)

[19] G. Korchmáros, S. Lia and M. Timpanella, *A generalization of Bring's curve in any characteristic*, sottomesso.

[20] D. Bartoli, M. Bonini and M. Timpanella, *Minimal codewords in Norm-Trace codes*, sottomesso.

[21] D. Bartoli and M. Timpanella, *Complete* $(q+1)$*-arcs in* $\mathrm{PG}(2,\mathbb{F}_{q^6})$ *from the Hermitian curve*, sottomesso.

[22] M. Timpanella, *On AG codes from a generalization of the Deligne-Lustzig curve of Suzuki type*, sottomesso.

[23] D. Bartoli, G. Longobardi, G. Marino and M. Timpanella, *On a family of MRD codes in even characteristic*, in preparazione.

[24] M. Giulietti, G. Korchmáros, S. Lia and M. Timpanella, *Automorphism groups of algebraic curves and p-ranks*, in preparazione.

[25] A. Iezzi, M. Q. Kawakita, M. Timpanella, *New sextics of genus 6 and 10 attaining the Serre bound*, sottomesso.

[26] D. Bartoli, N. Durante, G.G. Grimaldi, M. Timpanella, *Ovoids of* $Q^+(7,q)$ *of low-degree*, in preparazione.

[27] L. Landi, M. Timpanella, L. Vicino, *Two-point AG codes from one of the Skabelund maximal curves*, in preparazione.

[28] M. Timpanella, *Riemann surfaces with many automorphisms*, in preparazione.

Corsi di Dottorato tenuti

A.A. 2023–2024 **Algebraic curves and applications to cryptography and coding theory**, 20 ore, Università degli Studi "Federico II" di Napoli, previsto per Luglio 2024.

A.A. 2022–2023 **Galois theory and applications**, 30 ore, Università degli Studi di Firenze, dottorato in consorzio con l'Università degli Studi di Perugia e INdAM.

A.A. 2019–2020 **An introduction to elliptic curves over finite fields**, 8 ore, Eötvös Loránd University, Budapest, (Ungheria).

A.A. 2018–2019 **Elliptic curves over finite fields and Cryptography**, 20 ore, Bolyai Institute, Szeged, (Ungheria).

Attività didattica

A.A. 2022–2023 **Co-docenza "*Cryptography and applications*"**, per il Corso di Laurea Magistrale in Informatica e Matematica (14 ore), Università degli Studi di Perugia.

A.A. 2022–2023 **Co-docenza "*Geometria e Informatica*"**, per il Corso di Laurea Triennale in Ingegneria Industriale (22 ore), Università degli Studi di Perugia, polo scientifico didattico di Terni.

A.A. 2022–2023 **Didattica integrativa "*Algebra II*"**, per il Corso di Laurea Triennale in Informatica e Matematica (10 ore), Università degli Studi di Perugia.

A.A. 2022–2023 **Didattica integrativa "*Geometria II*"**, per il Corso di Laurea Triennale in Informatica e Matematica (20 ore), Università degli Studi di Perugia.

A.A. 2022–2023 **Professore a contratto per l'insegnamento di "*Matematica*"** , Corso di preparazione ai test TOLC-MED E TOLC-VET 2023/2024 (18 ore), Università degli Studi di Perugia.

A.A. 2022–2023 **Professore a contratto per l'insegnamento di "*Matematica*"** , corso di preparazione per i concorsi di ammissione ai Corsi di Laurea in Medicina e Chirurgia, Dipartimento di Medicina Sperimentale (22 ore), Università degli Studi di Perugia.

A.A. 2021–2022 **Co-docenza "*Cryptography and applications*"**, per il Corso di Laurea Magistrale in Informatica e Matematica (21 ore), Università degli Studi di Perugia.

A.A. 2021–2022 **Professore a contratto per l'insegnamento di "*Matematica*"** , corso di preparazione per i concorsi di ammissione ai Corsi di Laurea in Medicina e Chirurgia, Dipartimento di Medicina Sperimentale (22 ore), Università degli Studi di Perugia.

A.A. 2020–2021 **Membro della commissione giudicatrice degli esami di profitto dei corsi di "*Algebra I*", "*Geometria II*"**, per il Cdl triennale in Matematica e **del corso di "*Crittografia e Applicazioni*"**, per il Cdl magistrale in Matematica ed Informatica (18 ore), Università degli Studi di Perugia.

A.A. 2019–2020 **Membro della commissione giudicatrice degli esami di profitto dei corsi di "*Algebra I*", "*Geometria II*"**, per il Cdl triennale in Matematica e **del corso di "*Crittografia e Applicazioni*"**, per il Cdl magistrale in Matematica ed Informatica (30 ore), Università degli Studi di Perugia.

A.A. 2019–2020 **Ciclo di seminari: "*Suzuki groups and their geometries*"**, (6 ore), Università degli Studi della Basilicata, Potenza, (Italia).

A.A. 2019–2020 **Professore a contratto per l'insegnamento di "*Matematica*"** , corso di preparazione per i concorsi di ammissione ai Corsi di Laurea in Medicina e Chirurgia, Dipartimento di Medicina Sperimentale (22 ore), Università degli Studi di Perugia.

A.A. 2018–2019 **Membro della commissione giudicatrice degli esami di profitto dei corsi di "*Algebra I*", "*Geometria II*"**, per il Cdl triennale in Matematica e **del corso di "*Crittografia e Applicazioni*"**, per il Cdl magistrale in Matematica ed Informatica (13 ore), Università degli Studi di Perugia.

Tesi di Laurea di cui sono relatore

A.A. 2022–2023 L. Lucarini, *Protocolli per secure multiparty computation*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

A.A. 2022–2023 A. Giannoni, *Exceptional scattered sequences*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

A.A. 2022–2023 A. Ficola, *Crittografia basata su isogenie*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

A.A. 2021–2022 B. Benfaremo, *Codici per il cloud computing*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

A.A. 2021–2022 A. Sonaglioni, *Crittografia post-quantum per firme digitali*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

A.A. 2021–2022 G. Taddei, *Firme digitali per criptovalute*, Laurea Magistrale in Matematica, Università degli Studi di Perugia.

Attività organizzativa e di coordinamento

1.11.2022 – 31.10.2025 Membro della Giunta del Dipartimento di Matematica e Informatica per il triennio accademico 2022/2025.

Scuole estive seguite

07.06.2021–11.06.2021 **Online Summer School in Algebraic Coding Theory**, *University of Zurich*, (Svizzera).

10.06.2019–14.06.2019 **2nd Scientific School on Blockchain and distributed ledger technologies**, *Technology Park of Sardinia*, Pula, (Italia).

23.07.2018–17.08.2018 **Summer School in Mathematics (SMI)**, *Università di Perugia.*
Corsi seguiti:
- Commutative Algebra and Geometry;
- Complex Analysis.

01.07.2018 – 07.07.2018 **8th PhD Summer School in Discrete Mathematics**, Rogla, (Slovenia).

Altro - public engagement

21.04.2023 ***Privacy e sicurezza: un ponte tra Crittografia e Teoria dei Codici***, XII Festa di Scienza e Filosofia, Foligno.

8.03.2023 ***Mani in pasta in Crittografia***, attività di orientamento per studenti della scuola secondaria superiore "Galeazzo Alessi".

24.02.2023 ***Polinomi simmetrici, identità di Viète e di Newton-Girard***, webinar di preparazione per la gara di Matematica "Premio Danti 2023", Università degli Studi di Perugia.

21.02.2023 ***La Matematica della Crittografia: da Cesare alla Playstation***, webinar di orientamento per #UnipgOrientaExpress.

13.12.2022 ***Mani in pasta in Crittografia***, attività di orientamento per studenti della scuola secondaria superiore "Jacopone da Todi".

13.05.2022 ***Problems on codes***, lezione per il corso "De Cifris Trends in Modern Cryptography", Università degli Studi di Trento.

07.04.2022 ***RSA e test di primalità***, lezione per la competizione nazionale "Cyberchallenge.it", Università degli Studi di Perugia.

09.03.2022 ***Introduzione alla teoria dei grafi***, webinar di preparazione per la gara di Matematica "Premio Danti 2022", Università degli Studi di Perugia.

23.05.2018 ***Crittografia a chiave pubblica***, Seminario presso Smart P@per S.p.a, Università degli Studi della Basilicata.

21.05.2018 ***Crittografia simmetrica***, Seminario presso Smart P@per S.p.a, Università degli Studi della Basilicata.

Esperienze lavorative

21.05.2018–31.10.2020 Collaborazione con l'azienda Smart P@per S.p.a per l'implementazione di un crittosistema basato su curve ellittiche.

Ulteriori titoli

2023 – presente **Membro dell'Albo dei formatori della fondazione I.T.S Umbria Academy**, per le unità formative: Cyber Security e Data Security.

2017/2018 – presente **Attribuzione del titolo di "*Cultore della materia*"**, per gli insegnamenti di "Geometria II" ed "Algebra I" per il Cdl triennale in Matematica, *Università degli Studi di Perugia.*

2017/2018 – presente **Attribuzione del titolo di "*Cultore della materia*"**, per l'insegnamento di "Crittografia e Applicazioni" per il Cdl magistrale in Matematica ed Informatica, *Università degli Studi di Perugia.*

Competenze

Conoscenza della lingua inglese

C1 *Oxford School of Languages certificate*

Computer skills

Application: MAGMA, C++, R, MATLAB

Documentation: MS Office, LaTeX

CONSAPEVOLE CHE CHIUNQUE RILASCIA DICHIARAZIONI MENDACI È PUNITO AI SENSI DEL CODICE PENALE E DELLE LEGGI SPECIALI IN MATERIA, AI SENSI E PER GLI EFFETTI DEGLI ART. 75 e 76 DPR 445/2000.

Perugia, 23 Maggio 2023