



Allegato 1 al Bando di cui al DR

DIPARTIMENTO DI MATEMATICA E INFORMATICA

Procedura pubblica di selezione per la sottoscrizione di un contratto di diritto privato per l'instaurazione di un rapporto di lavoro subordinato quale ricercatore universitario a tempo determinato, ai sensi dell'art. 24 - comma 3 - lettera a) della legge 30.12.2010 n. 240 – COD. RTDA-2024-05:

Gruppo Scientifico	
Disciplinare	01/MATH-02 – Algebra e Geometria
Profilo: Settore Scientifico	MATH-02/B – Geometria
Disciplinare	
Durata contrattuale	3 anni, eventualmente prorogabili per ulteriori due, in regime di tempo pieno
Sede di servizio	Università degli Studi di Perugia – Dipartimento di Matematica e Informatica
Docente Referente	Prof. Massimo Giulietti
Lingua straniera richiesta	Inglese
Numero massimo pubblicazioni	12
Progetto	PNRR "SERICS - AQuSDIT" - CUP H73C22000880001

Il contratto è finalizzato allo svolgimento delle seguenti attività di ricerca, di didattica, di didattica integrativa e di servizio agli studenti:

- **Attività di ricerca:** avrà come oggetto *“Metodi matematici per lo sviluppo di crittografia sicura in sistemi distribuiti” (“Mathematical methods for the development of secure cryptography in distributed systems”)*.

Descrizione sintetica: Ricerca nel campo della crittografia, con particolare riferimento a primitive e protocolli applicabili a sistemi distribuiti. L'attività di ricerca riguarderà metodi geometrici applicabili a protocolli e schemi post-quantum per cifratura asimmetrica, scambio di chiavi e firma digitale, focalizzandosi alle applicazioni alla *“Somewhat omomorphic Encryption” (SWE)* e/o Private Information Retrieval (PIR) basati su codici lineari. Le attività saranno inserite nell'ambito del progetto *“Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing”* – Acronimo: AQuSDIT, ammesso a finanziamento a seguito di avviso pubblico per la presentazione di proposte di intervento per la realizzazione di attività di ricerca fondamentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 5 - Cryptography and Distributed Systems Security (Università della Calabria).



- **Attività didattica, didattica integrativa e servizio agli studenti:** 350 ore annue (regime a tempo pieno) prevalentemente nell'ambito del settore scientifico disciplinare MATH-02/B, di cui non più di 180 ore per attività di didattica ufficiale.

Requisiti di ammissione richiesti per la partecipazione alla procedura selettiva:

1. Titolo di Dottore di ricerca in "Matematica" o "Matematica e Applicazioni" o titolo equivalente.
2. Esperienza maturata nel campo della ricerca e/o della didattica, comprovante il possesso di solide competenze di base nel settore scientifico disciplinare MATH-02/B.

Calendario discussione e relativi avvisi.

Il giorno **14.11.2024** verrà pubblicato, nel sito web dell'Ateneo (www.unipg.it) selezionando in sequenza le voci "Ateneo" - "Concorsi" - "Personale docente" - "Procedure di valutazione comparativa Ricercatori a tempo determinato", **un Avviso dirigenziale con il quale si renderà noto:**

- la data in cui verrà pubblicato l'Avviso dirigenziale con il quale saranno comunicati l'elenco dei candidati ammessi alla discussione ed il diario e la modalità di espletamento della discussione stessa;
- l'eventuale rinvio di pubblicazione del suddetto Avviso, ovvero ogni altra eventuale comunicazione concernente la presente procedura selettiva.