AVVISO N. 238/2018
selezione pubblica, per titoli ed esami, per l'attribuzione di
n. 1 assegno di ricerca "post dottorale" (categoria B)
presso il Dipartimento di Scienze Matematiche "G. L. Lagrange".

Il Politecnico di Torino intende attribuire n. 1 assegno per lo svolgimento di attività di ricerca nell'ambito del programma di ricerca: **"Crittografia post-quantum",** di cui alla scheda allegata.

Campo di ricerca:	**Mathematics**
Settore Scientifico Disciplinare:	**MAT/03 – Geometria**
Durata assegno:	**1 anno**
Importo lordo assegno:	**Euro 22.000,00 annui lordi**.

La domanda di partecipazione alla selezione, *redatta sull'apposito modulo e corredata della documentazione indicata nel bando generale per l'attribuzione di assegni di ricerca*, dovrà essere presentata presso l'Area Risorse Umane e Organizzazione - Ufficio Valutazioni Comparative e Assegni di ricerca – stanza n. 6 – **dal lunedì al giovedì dalle ore 9.00 alle ore 12.00 e dalle ore 14.00 alle ore 16.00, il venerdì dalle ore 9.00 alle ore 12.00**, ovvero inviata via posta, corriere o tramite fax, allegando copia di un documento di riconoscimento in corso di validità, al n. 0110905919, **entro le ore 16.00 del giorno 22.10.2018**. La data di arrivo sarà comprovata dal timbro a calendario apposto dall'ufficio. Non saranno ritenute valide le domande pervenute oltre il suddetto termine.

La selezione verrà effettuata, per titoli e colloquio, secondo il programma d'esame sotto indicato:

Titolo di studio richiesto per la partecipazione:	Dottorato di ricerca in Matematica, o titolo universitario straniero equivalente.
Campi su cui dovranno vertere i titoli:	Matematica applicata alla crittografia.
Temi del colloquio:	Il colloquio verterà sui seguenti argomenti: • Algebra collegata alle applicazioni crittografiche; • Curve ellittiche; • Sistemi a chiave pubblica e crittografia post-quantum. Saranno, inoltre, discussi i titoli ammessi a valutazione e accertata la conoscenza della lingua inglese e per i cittadini stranieri anche di quella italiana.

CALENDARIO DELLE PROVE:

Affissione elenco valutazione titoli:	il 30.10.2018 – ore 08,00 alla bacheca del Dipartimento di Scienze Matematiche "G. L. Lagrange" del Politecnico di Torino – Torino - C.so Duca degli Abruzzi, 24.
Colloquio:	il 31.10.2018 – ore 09,00 presso il Dipartimento di Scienze Matematiche "G. L. Lagrange" - Politecnico di Torino – Torino – C.so Duca degli Abruzzi, 24.

Area Risorse Umane e Organizzazione
Servizio Selezione e Gestione del Personale
Ufficio Valutazioni Comparative e Assegni di Ricerca
Politecnico di Torino Corso Duca degli Abruzzi, 24 – 10129 Torino – Italia
tel: +39 011 090 6136 - 6229 – 6119 - 5923 - 6052 fax: +39 011.090.5919
ruo.assegnidiricerca@polito.it www.swas.polito.it/services/ampe/

Titoli:
Sono valutati, purché in settori attinenti a quello per il quale è bandito l'assegno, i seguenti titoli:
- il dottorato di ricerca fino a 10 punti;
- il voto di laurea fino a 5 punti;
- pubblicazioni fino a 15 punti;
- i diplomi di specializzazione e gli attestati di frequenza di corsi di perfezionamento post laurea conseguiti in Italia o all'estero fino a 10 punti;
- lo svolgimento di documentata attività di ricerca (compresa quella effettuata nell'ambito dello svolgimento della tesi di laurea o di dottorato) presso soggetti pubblici e privati con contratti, borse di studio o incarichi, sia in Italia che all'estero, fino a 20 punti con un massimo di 4 punti all'anno.

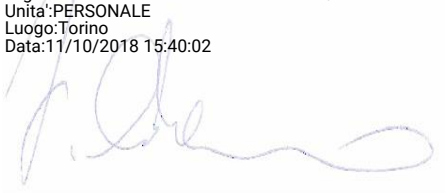
Coloro che hanno prodotto domanda dovranno presentarsi nel luogo, giorno ed ora su indicati, muniti di valido documento di riconoscimento.

Il bando generale per l'attribuzione degli assegni di ricerca, cui si rinvia per gli aspetti procedurali, e il "Regolamento per l'attribuzione di assegni per la collaborazione ad attività di ricerca" sono disponibili su internet al seguente indirizzo: http://www.swas.polito.it/services/concorsi/.

Torino, 11.10.2018

LA DIRETTRICE GENERALE
(Dott.ssa Ilaria ADAMO)

Firmato digitalmente da:Ilaria Maria Quanita Adamo
Organizzazione:POLITECNICO DI TORINO/00518460019
Unita':PERSONALE
Luogo:Torino
Data:11/10/2018 15:40:02



Allegato A)

DENOMINAZIONE PROGRAMMA DI RICERCA:

Crittografia post-quantum

Post-quantum cryptography

ACRONIMO PROGRAMMA DI RICERCA

CPQ

DURATA E DATA DI INIZIO DEL PROGRAMMA DI RICERCA

1 anno dal 01/12/2018 al 30/11/2019

CONTENUTO E FINALITÀ PROGRAMMA DI RICERCA:

Nell'ambito della crittografia post-quantum, recentemente, a fianco alle soluzioni che coinvolgono l'uso di codici e reticoli, sono state avanzate proposte per la realizzazione di una versione post-quantum del criptosistema RSA. Tuttavia, tale versione richiede un uso di chiavi di grandi dimensioni, rendendo non efficiente la soluzione proposta.
Dal momento che gli schemi stile RSA basati su curve, ed in particolari coniche, forniscono un'efficienza migliore del classico RSA in fase di decriptazione, si propone di studiare tali varianti dell'RSA per migliorare l'efficienza della sua versione post-quantum.
Per migliorarne ulteriormente l'efficienza si propone quindi di studiare gli schemi stile RSA su curve usando un modulo di base che sia prodotto di più primi o prodotto di potenze di primi (anziché utilizzare il prodotto di due numeri primi come nel classico RSA).

In the field of post-quantum cryptography, recently, alongside solutions that involve the use of codes and lattices, proposals have been made for the implementation of a post-quantum version of the RSA cryptosystem. However, this version requires the use of large keys, making the proposed solution inefficient.
Since the RSA schemes based on curves, and in particular conics, provide better efficiency than the classic RSA during decryption, it is proposed to study such variants of the RSA to improve the efficiency of its post-quantum version.
To further improve its efficiency, it is therefore proposed to study the RSA-style schemes on curves using a module that is product of more than two primes or product of prime powers (instead of using the product of two prime numbers as in the classic RSA).

PRESTAZIONI RICHIESTE ALL'ASSEGNISTA DI RICERCA

L'assegnista si prevede che approfondisca le possibili generalizzazioni dei vari sistemi RSA nello scenario post-quantum, presentando i risultati in pubblicazioni, convegni e seminari.