ID 1831

IL DIRETTORE GENERALE

Visto l'art. 7 comma 6 del Decreto Legislativo 30 marzo 2001 n. 165 e successive modificazioni e integrazioni;

Visto il Regolamento per l'affidamento a terzi estranei all'Università di incarichi di carattere intellettuale come modificato con decreto rettorale n. 0267760 del 23/04/2010;

Visto il Progetto "Towards fully automatic search of cryptographic trails" codice U-Gov CTE_INT21AVISC_01;

Visto l'avviso di conferimento rivolto al personale interno pubblicato sul sito web d'Ateneo Rep. n. 0035215/21 del 13/10/2021 che è andato deserto;

Visto l'avviso di procedura comparativa ID 1831 - Rep. n. 20245/2021 del 16/12/2021 per l'affidamento di un incarico di collaborazione di lavoro autonomo, della durata di 13 mesi e per un compenso di Euro 22.750,00 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore per attività di supporto alla ricerca;

Considerato che l'importo lordo pari a Euro 22.750,00 risulta congruo per l'attività in esso dedotta;

Verificata la disponibilità dei fondi posti a carico del progetto CTE_INT21AVISC_01 - n. di creazione U-Gov 35718;

Vista la determina di nomina della Commissione del 10/02/2022 - rep. 1623/2022 del 10/02/2022;

Visto il verbale di selezione titoli del 17/02/2022 da cui risultano attribuiti ai candidati i seguenti punteggi:

COGNOME E NOME	PUNTI
De Piccoli Alessandro	98/100
Pelizzola Simone	66/100

DETERMINA

L'approvazione degli atti della procedura comparativa ID 1831 - Rep. n. 20245/2021 del 16/12/2021.

L'autorizzazione alla stipula di un contratto individuale al Dott. Alessandro De Piccoli per attività di supporto alla ricerca finalizzata al raggiungimento dei seguenti obiettivi:

- Comprendere le principali proprietà e casi d'uso dei risolutori automatici utilizzati in ambito crittografico, studiando le principali librerie che li implementano;

- Comprensione e applicazione di tali risolutori per la ricerca di trail crittografici in un framework generico;
- Fase di sperimentazione, nella quale verranno ricercati trails crittografici mediante dispositivi High Performance Computing.

Svolgendo la seguente attività:

- Il collaboratore interverrà a supporto nelle varie attività del progetto, nello specifico:

– La prima fase del progetto sarà dedicata allo studio dello stato dell'arte e allo sviluppo di un framework generico (in un opportuno linguaggio di programmazione, es. python, e utilizzando determinate librerie, es. Sagemath) in cui l'input (es. funzioni hash, cifrari a blocchi, cifrari a flusso, permutazioni crittografiche, etc.), dato in pasto a diversi risolutori (SAT, SMT, MILP, CP, etc.), viene automaticamente elaborato. L'obiettivo di questa prima fase è quello di identificare un trail crittografico (lineare e differenziale) su un particolare "esempio giocattolo", e/o identificare limiti relativi alla lunghezza dei trails.

– La seconda fase del progetto sarà dedicata alla verifica del framework precedentemente sviluppato, testando input aventi diversa struttura e diverso design (es. DES, SHA-1, XTEA, etc.).

Tale attività sarà da svolgersi nell'ambito del Progetto "Towards fully automatic search of cryptographic trails" codice U-Gov CTE_INT21AVISC_01.

L'importo del contratto sarà di Euro 22.750,00 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore e avrà la durata di 13 mesi a favore del Dipartimento di Informatica "Giovanni degli Antoni".

Il corretto svolgimento dell'incarico sarà verificato dal Dott. Andrea Visconti.

Il costo di Euro 29.980,00 graverà sul progetto CTE_INT21AVISC_01 - n. di creazione U-Gov 35718 a carico del Dipartimento di Informatica "Giovanni degli Antoni".

IL DIRETTORE GENERALE

Roberto Conte

Conte Roberto Bruno
Università degli Studi
di Milano
14.04.2022 13:34:10
GMT+00:00