UNIVERSITÀ DEGLI STUDI DI MILANO

ID 1711

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 "Algebraic analysis of HMAC-SHA-1";
Visto: l'avviso di conferimento rivolto al personale interno prot. 0039148/20 del 23/12/2020 e pubblicato all'albo della struttura e sul sito web d'Ateneo;
Considerato: che tale avviso di conferimento rivolto al personale interno è andato deserto;
Visto: l'avviso di procedura comparativa ID 1711 – prot. n. 1221/2021 del 30/01/2021 per l'affidamento di un incarico di collaborazione di lavoro autonomo, della durata di 12 mesi e per un compenso di 17.000,00 Euro lordo al collaboratore per attività di supporto alla ricerca, per il 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;
- Comprendere e applicare tali risolutori per la ricerca di trail crittografici in un framework generico;
- Ricercare trails crittografici nella fase di sperimentazione mediante dispositivi High Performance Computing.

Svolgendo la seguente attività:

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

- nella prima fase, studio approfondito della letteratura (risolutori SAT, SMT, MILP, CP, etc.), comprensione delle più importanti librerie utilizzate per implementare i risolutori automatici in ambito crittografico e riproduzione dei risultati descritti nella letteratura;
- nella seconda fase, sviluppo di un framework (in un opportuno linguaggio di programmazione, es. python, e utilizzando determinate librerie, es. Sagemath) che

prenda come input algoritmi/primitive crittografiche (es. funzioni hash, cifrari a blocchi, cifrari a flusso, permutazioni crittografiche, etc.) ed elabori gli input per mezzo di diversi risolutori automatici identificando un trail crittografico lineare e differenziale su particolari "esempio giocattolo" e/o identifichi i limiti relativi alla lunghezza di tali trails;

- infine nella terza fase verifica del framework sviluppato nella seconda fase del progetto testando input di diversa struttura e con specifici design (es. SHA-1, DES, AES, Gimli, etc.);
- il collaboratore dovrà supportare il Responsabile Scientifico nella produzione corposa e ben documentata di quattro dettagliati documenti scritti in inglese che descrivono da una parte il lavoro di ricerca svolto fino al 3°, 7° e 12°mese del contratto annuale e dall'altra il software realizzato prendendo nuovi strumenti e testando nuovi algoritmi crittografici rispetto a quelli utilizzati nella prima annualità del progetto; il collaboratore dovrà infine partecipare alla presentazione orale dell'attività svolta e dei risultati ottenuti presso l'azienda finanziatrice.

Visto: il verbale di selezione del 23/03/2021 da cui risulta non essere pervenuta alcuna domanda di partecipazione in risposta all'avviso pubblico ID 1711 (prot. n. 1221/2021 del 30/01/2021);

DETERMINA

per quanto indicato in premessa, che la procedura ID 1711 – prot. n. 1221/2021 del 30/01/2021 è andata deserta per assenza di candidature.

IL DIRETTORE GENERALE

Roberto Conte

CONTE ROBERTO BRUNO
UNIVERSITÀ DEGLI STUDI
DI MILANO
24.03.2021 07:46:29 UTC