UNIVERSITÀ
DI SIENA
1240

DIPARTIMENTO
INGEGNERIA DELL'INFORMAZIONE E
SCIENZE MATEMATICHE

SCHEDA PROGETTO

TITOLO DELL'*ATTIVITÀ DI PROGETTO*

Studio di tecniche di calcolo universali nel dominio cifrato, con particolare riferimento all'approssimazione lineare a tratti di funzioni mono o multidimensionali

SOGGETTO PROPONENTE

Prof. Mauro Barni

OBIETTIVI/FINALITA`: descrizione *dell'attività di progetto*

L'obiettivo del progetto è lo sviluppo di protocolli crittografici che, pur operando nel dominio cifrato, permettano l'applicazione di una qualsiasi funzione ai dati ingresso al problema. I protocolli dovranno basarsi su tecniche di multiparty computation e sull'utilizzo della tecnologia dei "Garbled Circuits". Il progetto prevede lo sviluppo di un prototipo che implementi alcune delle soluzioni individuate e l'utilizzo del prototipo per la valutazione delle prestazioni dei protocolli in termini di tempi di calcolo.

RESPONSABILE *dell'attività di progetto*

Prof. Mauro Barni

Il Responsabile dell'attività oggetto della collaborazione garantisce il rispetto delle modalità di espletamento della collaborazione stessa, al solo fine di valutare la rispondenza del risultato con quanto richiesto e la sua funzionalità rispetto agli obiettivi prefissati. Dovranno essere indicate le fasi/sottofasi e i tempi di realizzazione dell'attività (arco di tempo complessivo). Si richiede di prevedere i tempi di realizzazione anche per le fasi dell'attività che si estendono oltre l'anno, anche se in modo meno puntuale. Nell'ultima colonna devono essere indicati i risultati che si intende raggiungere per ciascuna fase. Il numero delle fasi deve essere proporzionato alla durata dell'incarico.

DESCRIZIONE FASI E SOTTOFASI *dell'attività di progetto*	**Tempi di realizzazione (n. giorni)**	**Obiettivi delle singole fasi**
Individuazione di uno o più protocolli basati su Garbled Circuit per l'approssimazione universale delle funzioni	**15**	**Definizione del protocollo**
Implementazione di uno o più protocolli e valutazione delle prestazioni	**15**	**Analisi delle prestazioni dei protocolli proposti**

DURATA complessiva dell'attività (giorni): 30 giorni

Il Proponente
Prof. Mauro Barni

Il Responsabile del progetto
Prof. Mauro Barni

Via Roma,56, 53100 Siena

Segreteria Amministrativa tel +39 0577 234850 – 1092; fax +39 0577 233609; amministrazione@diism.unisi.it

Ufficio Didattica e Studenti tel +39 0577 233618; fax +39 0577 233602; didattica.diism@unisi.it

www.diism.unisi.it