PROPOSTE DI TESI IN CRITTOGRAFIA APPLICATA

La crittografia applicata trova ampia diffusione in numerosi ambiti applicativi: dai dispositivi mobili (smart-card, cellulare, palmare e simili) fino ai server di rete ad alta potenza. I sistemi di calcolo crittografici sono numerosi (a chiave segreta, pubblica, ecc) e alcuni di essi sono molto innovativi, complessi e flessibili. Dispositivi crittografici SW o HW sono ormai comunissimi e parte integrante di sistemi di calcolo o comunicazione di ogni tipo.

Si pongono pertanto diversi problemi originali in merito alla realizzazione efficiente (in SW o HW) di dispositivi crittografici innovativi (p. es. su curve ellittiche e simili) e in merito alla protezione di tali dispositivi contro metodi di attacco, in particolare di tipo “side-channel”, che sfruttano in modo combinato le caratteristiche fisiche del dispositivo e la struttura dell’algoritmo crittografico per aggirare la protezione crittografica.

In tale ambito sono proposti i due seguenti argomenti generali di tesi (per laurea magistrale) presso il Politecnico di Milano (Dip. di Elettronica a Informazione):

- *progetto e valutazione sperimentale (p. es. in VHDL) di co-processori crittografici efficienti HW per il calcolo di crittosistemi innovativi (p. es. curve ellittiche, e altri)*
- *studio di fattibilità e realizzazione sperimentale di metodi di attacco “side-channel”, di tipo in potenza e / o basati su guasti (power e fault injection-based attack), a dispositivi crittografici HW o SW, e valutazione di contromisure atte a prevenire, impedire o limitare l’attacco.*

Gli argomenti di tesi sono proposti in particolare per candidati iscritti al CdL di Ingegneria Informatica, ma se del caso anche alle altre ingegnerie ICT (Aut. Ele. e Tel.). Le tesi potranno, secondo il caso, essere svolte in parte come “stage” presso ST Microelectronics Italia (sede di Agrate Brianza, MI), presso il gruppo di ricerca AST (Advanced Systems and Technologies).

Milano, 2.5.2016

Per informazioni e / o colloquio, contattare (telefonare o scrivere a):

Relatore: prof. Luca Breveglieri

Tel: 02 2399 3653

Email: luca.breveglieri@polimi.it