Secure Computation Under Network and Physical Attacks

Alessandra Scafuro

Abstract

Questa tesi propone protocolli crittografici la cui sicurezza è preservata anche quando l'esecuzione degli stessi è interfogliata con l'esecuzione di altri protocolli. Questo grado di sicurezza è necessario per applicazioni eseguite su dispositivi connessi alla rete che gestiscono diverse applicazioni in concorrenza. Inoltre, questa tesi considera anche attacchi fisici, come attacchi di reset, nei quali un avversario riesce a forzare una macchina ad usare la stessa randomness in diverse esecuzioni.

La tesi è organizzata in tre parti.

La prima parte propone protocolli la cui sicurezza è formalmente dimostrata in accordo alla definizione di Universal Composability. Questa definizione garantisce il massimo livello di sicurezza, ma la sua realizzazione richiede l'uso di assunzioni di setup. I protocolli proposti in questa tesi usano hardware esterno (PUFs, Physically Uncloneable Functions) come assunzione di setup.

La seconda parte della tesi considera invece protocolli proposti nella letteratura, che sono sicuri secondo una definizione meno generale di sicurezza, ma che non richiedono assunzioni di setup e che presentano un numero di round ottimale. In questa tesi si dimostra che la prova di sicurezza di alcuni di questi protocolli presenta delle imperfezioni e come risultato i protocolli non sono sicuri. Questo lavoro prima identifica i problemi nei protocolli precedenti e poi propone nuovi protocolli che ottengono la definizione di sicurezza promessa.

La terza parte della tesi considera attacchi di reset e propone un protocollo per schemi di identificazione la cui sicurezza è garantita anche quando una delle parti che eseguono il protocollo è forzata ad eseguire il protocollo usando la stessa randomness usata nelle esecuzioni precedenti.