Chapter 1

Introduzione

Per meglio comprendere le tematiche di questa tesi è di fondamentale importanza introdurre al contesto storico e informatico in cui si inserisce. Nel contesto in questione l'utente passa da essere un semplice fruitore passivo dei servizi, a diventare sempre più un elemento cardine della piattaforma in quanto monetizzabile tramite le informazioni che lo riguardano. Questo cambiamento di prospettiva porta la persona al centro dell'interesse delle aziende, che potranno trarre guadagno movimentando e memorizzando quantità sempre maggiori di dati. Queste nuove dinamiche hanno fatto si che, per mantenere protetta ed intatta la privacy dei possessori dei dati, venissero sviluppate delle nuove tecniche di sicurezza informatica. Partendo da questi presupposti, la tesi si sviluppa analizzando la letteratura preesistente in materia e sperimentando un nuovo approccio alla problematica.

L'approccio maggiormente impiegato nella letteratura studiata è quello definito SMPC, ovvero la "secure multi party computation". Essa si presenta come sotto categoria della crittografia e si pone come obiettivo quello di elaborare metodi di calcolo congiunto di una funzione sugli input privati di due o più parti coinvolte. Una volta sviscerate tutte le caratteristiche di questo tema, la tesi sposta la sua attenzione su quello che sarà il vero argomento centrale di essa: la "Two party computation" e come renderla più efficiente.

Si tratta di una particolare sotto-categoria delle SMPC che descrive uno scenario in cui due parti comunicano tra di loro per la risoluzione di un problema, senza però scambiarsi informazioni sensibili e senza ricorrere all'utilizzo di una terza parte fidata.

Il padre di questo approccio è Yao, il quale ha sviluppato lo "Yao garbeled circuit". Questo tipo di circuito, nelle sue varie fasi, permette di raggiungere l'obbiettivo di privacy mediante l'utilizzo di un circuito virtuale in cui gli utenti inseriscono i propri input crittografati e non verranno a conoscenza, al termine delle operazioni, di altri dati se non i propri input e l'output finale del circuito.

Nella letteratura citata, questo tipo di approccio viene applicato solo e soltanto a circuiti di tipo booleano. La finalità di questa tesi è dunque quella di studiare se, applicando un circuito con logica multi valore a questi sistemi, sia possibile ottenere una riduzione dei costi operazionali per conseguire una miglior performance del protocollo.

Prima di intraprendere questa analisi è stato necessario soffermarsi su quali fossero i metodi più efficaci per ottenere una corretta conversione dei circuiti da binari a multi valore. Per conversione efficace si intende quella conversione che non va a snaturare la struttura del circuito e che rende quindi possibile una comparazione finale con i dati forniti dalla letteratura. Un ulteriore strumento analizzato ed utilizzato è la sintesi dei circuiti, che viene applicata sia ai circuiti booleani che a quelli multi valore, in modo tale da andare a ripulire la struttura da ridondanze e strutture ininfluenti ai fini dei calcoli. Gli strumenti di sintesi in nostro possesso hanno giocato un ruolo fondamentale ai fini dell'analisi, in quanto i tool disponibili per gestire la logica multi valore sono datati e non implementati o aggiornati nel tempo.

Per far fronte a questa carenza, la direzione della tesi si è spostata verso un approccio "ibrido" alla questione. L'obbiettivo di questo metodo è quello di poter andare a sfruttare e valorizzare i punti di forza di entrambe le logiche. Nel caso della logica multi valore, riducendo il numero degli input che le parti devono devono inserire e limitando drasticamente la dimensione del dominio, è stato possibile ridurre i costi computazionali del processo. Dall'altra parte invece, nel caso della logica booleana, sfruttando gli strumenti di sintesi più evoluti ed implementati nel tempo è stato possibile ridurre notevolmente le dimensioni della struttura del circuito, riducendo ulteriormente i costi computazionali del processo.

I risultati finali della tesi hanno dimostrato che l'approccio ibrido può essere considerato interessante in quanto, nella maggior parte dei casi, è stato possibile notare una riduzione sostanziale dei costi del circuito in esame rispetto ad un normale circuito booleano sintetizzato.