PROPOSTE DI TESI CON SECURITY PATTERN

https://www.securitypattern.com

LLL con hint di lunghezza variabile

Nell'ambito degli attacchi crittografici, un attacco molto interessante è basato sull'algoritmo di Lenstra–Lenstra–Lovász (LLL) per la riduzione delle basi di reticoli. Per esempio, questo algoritmo permette di estrarre la chiave di firma di un'implementazione di ECDSA, nel caso in cui un 'attaccante conosca alcuni bit dei nonce su più firme (vedi https://eprint.iacr.org/2020/728.pdf o https://blog.trailofbits.com/2020/06/11/ecdsa-handle-with-care/). I migliori attacchi di questo tipo sono in grado di ricavare la chiave segreta conoscendo anche solo 3 bit del nonce su qualche centinaio di firme (Sun, Chao, et al. "Guessing Bits: Improved Lattice Attacks on (EC) DSA with Nonce Leakage.").
In realtà però tutte le pubblicazioni dell'attacco basato su LLL prevedono che l'attaccante conosca un numero fisso di bit dei nonce per ogni firma. Nel caso di un attacco side-channel, invece, è possibile recuperare un numero variabile di bit del nonce per ogni firma, l'attaccante è quindi costretto ad utilizzare il numero minimo (fisso) di bit recuperati su ogni nonce per applicare l'attacco LLL, rallentando così l'attacco o riducendo la probabilità di successo. Questa tesi si propone quindi di studiare la possibilità di alimentare la matrice LLL con sistemi con un numero variabile di bit noti per ogni equazione, in modo da sfruttare tutti i bit di informazione che l'attaccante può recuperare.
Questa proposta di tesi permette allo studente di lavorare proficuamente anche da remoto.

Analisi di crittografia basata sulle permutazioni

Un'alternativa agli approcci classici di costruzione di crittosistemi simmetrici quali i block cipher, è la crittografia basata su permutazioni, diventata popolare grazie alla sua adozione nel nuovo standard di hash SHA3.
Negli ultimi anni inoltre le permutazioni sono state utilizzate per diverse proposte di crittografia "lightweight" e per diversi protocolli di rete, quali ad esempio Strobe e Blinker.
La proposta di testi mira a studiare la crittografia basata su permutazioni sotto questi diversi aspetti, dalla sicurezza ai protocolli derivati, passando per l'implementazione pratica su microcontrollore o FPGA.
Questa proposta di tesi permette allo studente di lavorare proficuamente anche da remoto.