Crittoanalisi differenziale avanzata

Docenti: Massimiliano Sala (`sala@science.unitn.it`)
Anna Rimoldi (`rimoldi@science.unitn.it`)
Luogo: Facoltà di Scienze, Università degli Studi di Trento.
Ore di lezione: 20 ore frontali (20 ore a disposizione in laboratorio).
Periodo: 29 Novembre - 3 Dicembre 2010.

Abstract

Sebbene sia AES che Serpent nella loro interezza non risultano deboli, ci sono numerosi attacchi per versioni ridotte. Per AES-256 ci sono recentissimi attacchi fino al decimo round. In questo corso verrà effettuata un'analisi rigorosa degli attacchi moderni, compresi gli attacchi di crittanalisi differenziale avanzata, discutendone punti di forza e limitazioni.

A chi è rivolto

Il corso è rivolto a professionisti operanti nel campo della sicurezza informatica (PA o aziende private), sia con formazione matematica che con formazione tecnica (informatica, ingegneria, etc).

Programma

Il corso si articolerà nel seguente modo:

- descrizione approfondita dei crittosistemi AES, Serpent e KASUMI, comprese le varianti crittanalizzate recentemente. Collegamento con le caratteristiche di sicurezza per S-boxes e Mixing Layer dei due crittosistemi.
- Gli scenari di attacco ai block ciphers. Parole chiave: single-key, relate-key, random-key-sample, key recovery, distinguishers. Il ruolo del Key Schedule.
- Presentazione generale degli attacchi differenziali avanzati: Square attack, Partial sum, Boomerang, Amplified Boomerang, Rectangle, Impossible Differential, attacco misto Differential-Linear.
- Presentazione dei suddetti attacchi su: versioni ridotte di AES, versioni modificate di AES, versioni ridotte/modificate di Serpent, versioni ridotte di KASUMI. In particolare, spiegheremo l'attacco di Biryukov et al. (Eurocrypt 2010) che rompe AES-256 fino al decimo round.

- Attacco di distinguibilità misto algebrico-statistico ai translation-based, compreso AES (tutte le versioni), sviluppato dal nostro gruppo.
- Possibili collegamenti tra gli attacchi differenziali ed il nostro approccio.

Organizzazione e logistica

Data l'elevata specializzazione del corso, il numero massimo di partecipanti è di dieci persone. Si consiglia di inviare tempestivamente una mail al Prof. Sala o alla Dott. Rimoldi, segnalando l'intenzione di partecipare al corso.

Le lezioni si terranno la mattina dalle 9:00 alle 13:00 presso la Facoltà di Scienze dell'Università degli Studi di Trento, per una durata di una settimana (dal lunedì al venerdì). Il corso sarà effettuato dal 29 novembre al 3 dicembre.

Il pomeriggio degli stessi giorni, dalle 14:30 alle 18:30, verrà messo a disposizione dei partecipanti il laboratorio di Matematica Industriale e Crittografia, dove alcuni assistenti del Prof. Sala mostreranno come implementare su MAGMA le nozioni base apprese la mattina.

Costo del corso

Il costo didattico totale (lezioni frontali, laboratorio) è di 1000 euro (esente da IVA).

Modalità di pagamento

Il pagamento della relativa quota dovrà essere effettuato a ricezione della fattura (che sarà inviata entro il 15 novembre), mediante bonifico bancario:

Unicredit Banca Spa
Sede di Trento - Via Galileo Galilei, 1
IBAN IT37L0200801820000100807242
SWIFT UNCRIT2B0HV.

Causale: CRITTO10.