htw saar

Studiengang Kommunikationsinformatik (Master)
Studiengang Praktische Informatik (Master)
Prof. Dr.–Ing. Damian Weber

Projekt Kryptographie

Sommersemester 2016

Ziel ist das Verstehen und Ausführen von Attacken auf symmetrische Kryptoverfahren. Wir befassen uns mit den Basisattacken differentielle und lineare Kryptoanalyse. Moderne Chiffren wie etwa die Finalisten aus dem AES–Wettbewerb sind zwar vom Design her immunisiert gegen diese Art von Attacken. Dennoch gibt es immer wieder Firmen, die ihre ,,eigene" supersichere, unknackbare Verschlüsselung anbieten. Da die Autoren solcher Verfahren den Hintergrund der Designentscheidungen moderner Kryptoverfahren nicht kennen, sind dort Techniken wie differentielle und lineare Kryptoanalyse besonders wirkungsvoll. Desweiteren ermöglicht die Kenntnis dieser Techniken die Entwicklung eigener Verfahren, die immun gegen diese Attacken sind.

FEAL war eines der ersten ernstzunehmenden symmetrischen Verfahren nach dem DES. Da die genannten Techniken zu diesem Zeitpunkt noch kaum im Einsatz waren, gibt es auf dieser Basis gut verständliche Angriffe gegen FEAL. Projekte 1 und 2 befassen sich hiermit.

SIMON ist ein leight–weight Chiffre, der von der NSA vorgeschlagen wurde. Wegen seiner einfachen Struktur kann der in RFID-Tags zum Einsatz kommen. Ob die Security ebenfalls leight–weight ist, muss sich erst noch zeigen. Inzwischen gibt es differentielle Angriffe für eine reduzierte Anzahl von Runden. Projekt 3 befasst sich mit dem Verständnis einer solchen Attacke.

Die Attacken betreffen meist eine reduzierte Rundenzahl. Je nachdem, wieviele restliche Möglichkeiten für die Keybits übrig bleiben (z.B. 2^{50} bei SIMON32/64), ergibt sich eine relativ lange Laufzeit zum Finden des richtigen Keys. Um beeindruckende Resultate zu erzielen, ist es ratsam, eine Programmiersprache mit compiliertem Code zu benutzen (C/C++).

Die Projektteams sollen in der Regel aus 2 Personen bestehen.

Eine weiteres mögliches Projekt ist das Verstehen und die Implementierung der Drown-Attacke. Hierfür muss SSL/TLS erarbeitet werden. Ein Webserver der sowohl das SSLv2– als auch das TLS–Protokoll unterstützt ist anfällig.

1 FEAL-Differential-Cryptanalysis Attacke

a) Implementieren Sie FEAL.

b) Lesen Sie *The Cryptanalysis of FEAL with twenty chosen Plaintexts* von Sean Murphy.

c) Implementieren Sie die Attacke.

d) Belegen Sie erfolgreiche Ausführungen der Attacke.

2 FEAL-Linear-Cryptanalysis Attacke

a) Implementieren Sie FEAL.

b) Lesen Sie *Linear Cryptanalysis of the Fast Data Encipherment Algorithm* von Kazuo Ohta and Kazumaro Aoki.

c) Implementieren Sie die Attacke.

d) Belegen Sie erfolgreiche Ausführungen der Attacke.

3 SIMON-Impossible-Differential-Attacke

a) Implementieren Sie SIMON.

b) Lesen Sie *Impossible Differential Cryptanalysis of Reduced Round SIMON* von Chen, Wang, Wang

c) Implementieren Sie die Attacke.

d) Belegen Sie erfolgreiche Ausführungen der Attacke.

4 Implementierung der DROWN–Attacke

a) Lesen Sie *DROWN: Breaking TLS using SSLv2* von Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar and Yuval Shavitt.

b) Konfigurieren Sie einen Webserver mit SSLv2 und TLS.

c) Schreiben Sie ein Scanning–Tool, das erkennt, ob ein Webserver anfällig für DROWN ist.

d) Implementieren Sie die DROWN–Attacke und belegen Sie erfolgreiche Ausführungen.