Implementierung der FEAL-Differentrial-Cryptanalysis Attacke nach Murphy

Lukas Becker Juri Golanov

August 23, 2016

Inhaltsverzeichnis

1 Einleitung

Seit jehher herrscht in der Kryptographie ein Rennen zwischen Forschern, die neue Verfahren entwickeln und Leuten, welche die Schwachstellen in den Verfahren suchen, um diese für ihre Zwecke auszunutzen. Bei der Suche nach *dem* sicheren Krypto-Verfahren helfen Paper, wie das von Sean Murphy[2]. Sie zeigen den Forschern die Schwachstellen ihrer Algorithmen auf und wie diese in einer Attacke ausgenutzt werden. Durch diese Erkenntnisse können dann alte Verfahren verbessert oder neue entwickelt werden, um die jetzt bekannten Schwächen zu beseitigen.

In der folgenden Ausarbeitung werden wir uns der Implementierung der *Krypto-Attacke auf den FEAL Algorithmus mit 20 Plaintextblöcken oder weniger*[2] von Sean Murphy befassen.

1.1 Aufbau

Zunächst werden wir das FEAL Krypto-Verfahren an sich beleuchten. Dazu gehören einmal der Aufbau der Logik, sowie die verwendeten Algorithmen und Funktionen.
Im nächsten Schritt wird auf die von Sean Murphy entwickelte Attacke eingegangen. Hier wird vorallem aufgezeigt welche Schwächen Murphy in dem Verfahren entdeckt hat und wie er diese ausnutzt.
Nach der Theorie folgt dann die Implementierung der Attacke. Dieses Kapitel beschreibt überwiegend den Projektverlauf vom ersten Auseinandersetzen mit dem Paper bis hin zum fertigen Programm.
Im Anschluss wird ein Fallbeispiel einer Attacke durchgespielt, um zu veranschaulichen wie das Programm, also die Attacke, vorgeht, um verschlüsselte Texte ohne Wissen des Schlüssels zu entschlüsseln.
Danach wird auf Probleme eingangen, denen wir beim Bewältigen des Problems begegnet sind, sowie der resultierende Lösungsweg.
Abschließend folgt eine kurze Konklusion zu dem fertigen Projekt.

2 FEAL

3 Attacke nach Murphy

4 Implementierung

5 Fallbeispiel

6 Probleme

7 Konklusion

References

[1] A. Shimizu and S. Miyaguchi, “Fast Data Encipherment Algorithm FEAL”, Advances in Crptology - Eurocrypt 87, Lecture Notes in Computer Science 304.

[2] Sean Murphy, “The Cryptanalysis of FEAL-4 with twenty chosen plaintexts”, Journal of Cryptology. 2, Nr. 3, Januar 1990.