Round-Function-Recovery Attacks Against Feistel Networks

Fatma Betul Durak
Dept. of Computer Science

9/6/2017 at 01:00 pm
CoRE B (305)

Abstract

Feistel Networks (FN) are now massively being used to encrypt credit card numbers through format-preserving encryption (FPE). In our work, we focus on FN with two branches, entirely unknown round functions, modular additions, and when the domain size of a round function (called N) is small. We investigate round-function-recovery attacks.

The best-known attack so far is an improvement of Meet-In-The-Middle (MITM) attack by Isobe and Shibutani from ASIACRYPT 2013 with optimal query complexity q=r \frac{N}{2} and time complexity N^{ \frac{r-4}{2}N + o(N)}, where r is the number of rounds. We construct an algorithm with a surprisingly better complexity when r is too low, based on partial exhaustive search. When the query complexity varies from the optimal to the one of a codebook attack q=N^2, our time complexity can reach N^{O \left(N^{1-\frac{1}{r-2}} \right) }. It crosses the complexity of the improved MITM for q \sim N\frac{\mathrm{e}^3}{r}2^{r-3}.

We also estimate the lowest secure number of rounds depending on N and the security goal. We show that the FPE constructions FF1 and FF3 form NIST and ANSI standards cannot offer a 128-bit security (as they are supposed to) for N \leq 11 and N \leq 17, respectively, and improve the results by Durak and Vaudenay from CRYPTO 2017.

Defense Committee: Prof. David Cash (Chair), Prof. Rebecca Wright, Prof. Shubhangi Saraf, Prof. Thomas Ristenpart (Cornell Tech)