Correlations Aplenty - Linear Cryptanalysis of Block Ciphers

The advent of the Digital Age has brought upon us a world where information is a primary commodity. Thanks to the near omnipresence of computing devices, the collection and exchange of information is easier and more frequent than ever before. Soon, almost all electrically powered devices will contain a computer, and furthermore they will all be communicating with each other. The consequence is that a wealth of information about each of us is being recorded and transmitted around the world – information that most people will likely prefer to keep as private as possible. Thus, the trends of the modern age also bring with them an increasing focus on – and importance of – cryptography in order to provide secure communications. A core research area of cryptography is the construction of secure block ciphers – a so-called cryptographic primitive, their importance arise from the fact that a plethora of other cryptographic algorithms can be constructed from a block cipher. Clearly, it is crucial to have a high level of confidence in the security of such a building block. However, it is not known how to construct a block cipher which can be proven secure, and so instead, the security is evaluated by trying to mount every known attack against the cipher. A deep understanding of the different attack techniques is therefore essential in order to get an accurate assessment of a block cipher’s strength. This thesis explores one such attack technique: linear cryptanalysis. Being a central technique in the cryptanalyst’s tool kit, every new block cipher has to demonstrate resistance against this attack. Nevertheless, our understanding of this statistical attack is not complete, especially so for advanced variants where the stochastic variables we need to analyse are quite complex. Therefore, the following work is part of an effort to build advanced tools and models with the aim of providing more accurate analysis of advanced linear attacks. The first part of this thesis introduces block ciphers and notions of their security, followed by an introduction to linear cryptanalysis. The second part contains four publications that advance the field of linear cryptanalysis in several ways. They present new tools that help the cryptanalyst discover new linear attacks, and facilitated by these tools, new statistical models are presented. These models aim to remove many simplifying assumptions that have previously been made when evaluating linear attacks. We present new attacks on the block ciphers DES and present using these models, and the statistical behaviour of linear attacks is examined for a number of other block ciphers. It is shown that the type of probability distribution involved in a linear attack can vary wildly between ciphers, demonstrating that when we evaluate the effectiveness of such an attack, great care must be taken. Thus, while the work of this thesis does advance the frontier of linear cryptanalysis, it also shows that there is much unknown land yet to discover.

General information
State: Submitted
Organisations: Cyber Security, Department of Applied Mathematics and Computer Science
Contributors: Vejre, P. S.
Number of pages: 178
Publication date: 2018

Publication information
Publisher: DTU Compute
Original language: English
Research output: Research › Ph.D. thesis – Annual report year: 2018