Automatic Cryptanalysis of Stream Ciphers

We are today surrounded by many communicating electronic devices. The security of such devices is often critical to their functionality. Stream ciphers are widely exploited to provide confidentiality of the electronically transmitted data. Compared to other primitives, stream ciphers are competitive in software applications with exceptionally high speed, and in hardware applications with exceptionally small footprint. Notable examples of stream ciphers include the A5/1 in GSM standard and RC4 in WPA and TLS protocols.

Cryptanalysis is the study of how to crack encryption algorithms or their implementations. Typically, a cryptanalyst proposes attacks on a particular cipher by hand or ad hoc computer search algorithm. It appears that a lot of time and effort in programming is required to attack any particular cipher. In order to avoid extensive manual work, cryptographic researchers tend to develop automatic tools, with which many cryptographic primitives can be analyzed in a general framework. Automatic “black box” techniques, such as SAT or MILP solvers, have become increasingly sophisticated and powerful. Indeed, they have been employed to attack many block ciphers. It turns out automatic tools can outperform human cryptanalysts in some occasions. On the other hand, the tools can be used to prove security bounds against various cryptanalysis. Hence, the cipher designers also benefit from the tools.

This thesis project aims to develop automatic tool for the analysis of stream ciphers. We are expected to model the cryptanalysis problem by programming language and then solve the problem by existing software. To our end, knowledge of programming languages (e.g. C) is required. Any background on mathematical optimization and/or dynamic programming would be advantageous. By doing this project, the student will have a better understanding of symmetric cryptanalysis and algorithm design techniques, which is beneficial for career development.

More information on cryptographic tools can be found at [http://www.ecrypt.eu.org/tools/](http://www.ecrypt.eu.org/tools/).

Practicalities

Promoter: Bart Preneel
Daily supervisor: Chaoyun Li chaoyun.li@esat.kuleuven.be office B01.18
Nature of the work: 30% literature, 20% theoretical work, 50% software
Number of students: 1