Security Arguments and Tool-based Design of Block Ciphers

Security Arguments and Tool-based Design of Block Ciphers

Dissertation Thesis

Friedrich Wiemer

16th August 2019

Submitted in partial fulfillment of the requirements
for the degree of Doktor der Naturwissenschaften

to the

Faculty of Mathematics
at Ruhr-Universität Bochum

1st Reviewer Prof. Dr. Gregor Leander
2nd Reviewer Prof. Dr. Alexander May

IMPRINT

Security Arguments and Tool-based Design of Block Ciphers

Published by the Ruhr-Universität Bochum, Bochum, Germany.

COLOPHON

This thesis was typeset using LaTeX and the `memoir` documentclass. It is based on Aaron Turon's thesis *Understanding and expressing scalable concurrency*[1], itself a mixture of `classicthesis`[2] by André Miede and `tufte-latex`[3], based on Edward Tufte's *Beautiful Evidence*.

The bibliography was processed by Biblatex. All graphics and plots are made with PGF/Ti*k*Z.

The body text is set 10/14pt (long primer) on a 26pc measure. The margin text is set 8/9pt (brevier) on a 12pc measure. Matthew Carter's Charter acts as both the text and display typeface. Monospaced text uses Jim Lyles's `Bitstream Vera Mono` ("Bera Mono").

[1] https://people.mpi-sws.org/~turon/turon-thesis.pdf

[2] https://bitbucket.org/amiede/classicthesis/

[3] https://github.com/Tufte-LaTeX/tufte-latex

If we knew what it was we were doing,
it would not be called research, would it?
—Albert Einstein

Abstract

Block ciphers form, without doubt, the backbone of today's encrypted communication and are thus justifiably the workhorses of cryptography. While efficiency of modern designs improved ever since the development of the DES and AES, the case with the corresponding security arguments differs. The thesis at hand aims at two main points, both in the direction of improving security analysis of block ciphers.

Part I studies a new notion for the better understanding of a special type of cryptanalysis and proposes a new block cipher instance. This instance comes with a tight bound on any differential, to the best of our knowledge the first such block cipher.

Part II turns to automated methods in design and analysis of block ciphers. Our main contribution here is an algorithm to propagate subspaces through encryption rounds, together with two applications: an algorithmic security argument against a new type of cryptanalysis and an idea towards the automation of key recovery attacks.

Abstract

Block ciphers form, without doubt, the backbone of today's encrypted communication and are thus justifiably the workhorses of cryptography. While efficiency of modern designs improved ever since the development of the DES and AES, the case with the corresponding security arguments differs. The thesis at hand aims at two main points, both in the direction of improving security analysis of block ciphers.

Part I studies a new notion for the better understanding of a special type of cryptanalysis and proposes a new block cipher instance. This instance comes with a tight bound on any differential, to the best of our knowledge the first such block cipher.

Part II turns to automated methods in design and analysis of block ciphers. Our main contribution here is an algorithm to propagate subspaces through encryption rounds, together with two applications: an algorithmic security argument against a new type of cryptanalysis and an idea towards the automation of key recovery attacks.

Abstract

Block ciphers form, without doubt, the backbone of today's encrypted communication and are thus justifiably the workhorses of cryptography. While efficiency of modern designs improved ever since the development of the DES and AES, the case with the corresponding security arguments differs. The thesis at hand aims at two main points, both in the direction of improving security analysis of block ciphers.

Part I studies a new notion for the better understanding of a special type of cryptanalysis and proposes a new block cipher instance. This instance comes with a tight bound on any differential, to the best of our knowledge the first such block cipher.

Part II turns to automated methods in design and analysis of block ciphers. Our main contribution here is an algorithm to propagate subspaces through encryption rounds, together with two applications: an algorithmic security argument against a new type of cryptanalysis and an idea towards the automation of key recovery attacks.

Contents

List of Figures

List of Tables

Part I

PROLOGUE

Part II

EPILOGUE

Versicherung an Eides Statt

Ich versichere an Eides statt, dass ich die eingereichte Dissertation selbstständig und ohne unzulässige fremde Hilfe verfasst, andere als die in ihr angegebene Literatur nicht benutzt und dass ich alle ganz oder annähernd übernommenen Textstellen sowie verwendete Grafiken, Tabellen und Auswertungsprogramme kenntlich gemacht habe.

Außerdem versichere ich, dass die vorgelegte elektronische mit der schriftlichen Version der Dissertation übereinstimmt und die Abhandlung in dieser oder ähnlicher Form noch nicht anderweitig als Promotionsleistung vorgelegt und bewertet wurde.

Datum

Unterschrift