

**WORKSHOP ON SELECTED AREAS IN
CRYPTOGRAPHY (SAC '97)**

August 11 – 12, 1997

WORKSHOP RECORD

School of Computer Science
Carleton University
Ottawa, Ontario
Canada
K1S 5B6

Preface

SAC '97 is the fourth in a series of annual workshops on Selected Areas in Cryptography. SAC '94 and SAC '96 were held at Queen's University and SAC '95 was held at Carleton University. The purpose of the workshop is to bring together researchers in cryptography and present new work on selected areas of interest. By concentrating on several selected areas we hope to facilitate a more comfortable atmosphere, allowing for increased interaction and in-depth discussion. The themes for this year's workshop are

- Efficiency in Cryptographic Systems,
- Symmetric Cipher Design & Implementation, and
- Protocols and Techniques for Web Security.

Of the 31 papers submitted to SAC '97, 20 were accepted for presentation at the workshop. We would like to thank the program committee members, Howard Heys, Henk Meijer, Stafford Tavares and Michael Wiener, who along with ourselves, participated in the selection process. As well, we would like to thank the following external reviewers for their help with the selections: Zhi-Guo Chen, Eric De Win, Václav Matyáš Jr., Serge Mister, Doug Stinson, Amr Youssef and Rob Zuccherato.

Complementing the Workshop Record that is made available to participants, this is the first year that the presented papers are available online. We thank the authors for the timely return of their papers in postscript form. The papers are available from the official SAC webpage located at <http://adonis.ee.queensu.ca:8000/sac/sac.html>.

SAC '97 is sponsored by the School of Computer Science at Carleton University, Entrust Technologies and the Interac Association. We would especially like to thank Rosemary Carter of the School of Computer Science for her assistance in every aspect of the organization of the workshop. As well, we would like to thank Richard Outerbridge for initiating the partnership between SAC '97 and the Interac Association. We also thank the International Association for Cryptologic Research (IACR) for their cooperation.

On behalf of the Organizing Committee, we welcome you to SAC '97, Carleton University and Ottawa.

Mike Just
Carlisle Adams
Ottawa, August 1997

Table of Contents

Invited Talk I

- Crowds, Anonymous Web Transactions 1
Avi Rubin

Symmetric Ciphers I

- Design of Substitution Blocks Satisfying Strict Avalanche Criterion 2
Martin Stanek and Daniel Olejár

- A New Substitution-Permutation Network Cipher Using Key-Dependent S-Boxes 13
Liam Keliher and Henk Meijer

- Nonexistence of Certain Quadratic S-boxes and Two Bounds on Nonlinear Characteristics of General S-boxes 27
Xian-Mo Zhang, Yuliang Zheng and Hideki Imai

- On the Design of Linear Transformations for Substitution-Permutation Encryption Networks 40
Amr Youssef, Serge Mister and Stafford Tavares

Invited Talk II

- DES, Triple-DES and AES 49
Lars Knudsen

Boolean Functions

- Smart Hill Climbing Finds Better Boolean Functions 50
William Millan, Andrew Clark and Ed Dawson

- Balanced Boolean Functions Satisfying PC(2) and Very Large Degree 64
Tomoyoshi Honda, Takashi Satoh, Tetsu Iwata and Kaoru Kurosawa

Stream Ciphers

On the Construction and Upper Bounds of Balanced and Correlation-immune Functions 73

Markus Schneider

Efficient Stream Cipher with Variable Internal State 88

André Zúquete and Paulo Geudes

A Systematic Procedure for Applying Fast Correlation Attacks to Combiners with Memory 102

M. Salmasizadeh, J. Golić, E. Dawson and L. Simpson

Working in $GF(2^n)$

Performance and Security of Block Ciphers Using Operations in $GF(2^n)$ 117

Shiho Moriai and Takeshi Shimoyama

Fast Arithmetic Operations over F_{2^n} for Software Implementation 131

Kazumaro Aoki and Kazuo Ohta

A Block-Ciphering Algorithm Based on Addition-Multiplication Structure in $GF(2^n)$ 145

Feng Zhu and Bao-An Guo

Symmetric Ciphers II

DES-80 160

Carlisle Adams

Differential Cryptanalysis of Feistel Ciphers and Differentially δ -uniform Mappings 172

Anne Canteaut

On Provable Security Against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Multiple Random Functions 185

Yasuyoshi Kaneko, Fumihiko Sano and Kouichi Sakurai

Invited Talk III

A bit of the story of PGP, future directions, and some public policy thoughts
on crypto 200

Phil Zimmermann

Cryptanalysis

Cryptanalysis of Akelarre 201

Niels Ferguson and Bruce Schneier

Two Rights Sometimes Make a Wrong 213

Lars Knudsen and Vincent Rijmen

Public-Key Cryptography

Proposal of a Fast Public Key Cryptosystem 224

Kouichi Itoh, Eiji Okamoto and Masahiro Mambo

Efficient Convertible Undeniable Signature Schemes 231

Markus Michels and Markus Stadler

One-Response Off-Line Digital Coins 244

Khanh Quoc Nguyen, Yi Mu and Vijay Varadharajan