

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1556

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Stafford Tavares Henk Meijer (Eds.)

Selected Areas in Cryptography

5th Annual International Workshop, SAC'98
Kingston, Ontario, Canada, August 17-18, 1998
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Stafford Tavares
Henk Meijer
Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario K7L 3N6, Canada
E-mail: tavares@ee.queensu.ca
henk@qucis.queensu.ca

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Selected areas in cryptography : 5th annual international workshop ; proceedings / SAC '98, Kingston, Ontario, Canada, August 17 - 18, 1998. Stafford Tavares ; Henk Meijer (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1556)
ISBN 3-540-65894-7

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743

ISBN 3-540-65894-7 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10693237 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

SAC D8 is the fifth in a series of annual workshops on Selected Areas in Cryptography. SAC D4 and SAC D6 were held at Queen's University in Kingston and SAC D5 and SAC D7 were held at Carleton University in Ottawa. The purpose of the workshop is to bring together researchers in cryptography to present new work on areas of current interest. It is our hope that focusing on selected topics will present a good opportunity for in-depth discussion in a relaxed atmosphere. The themes for the SAC D8 workshop were:

- Design and Analysis of Symmetric Key Cryptosystems
- Efficient Implementations of Cryptographic Systems
- Cryptographic Solutions for Internet Security
- Secure Wireless/Mobile Networks

Of the 39 papers submitted to SAC D8, 26 were accepted and two related papers were merged into one. There were also two invited presentations, one by Alfred Menezes entitled "Key Agreement Protocols" and the other by Eli Biham entitled "Initial Observations on SkipJack: Cryptanalysis of SkipJack-3XOR". There were 65 participants at the workshop.

The Program Committee members for SAC D8 were Carlisle Adams, Tom Cusick, Howard Heys, Henk Meijer, Doug Stinson, Stafford Tavares, Serge Vaudenay, and Michael Wiener. We also thank the following persons who acted as reviewers for SAC D8: Zhi-Guo Chen, Mike Just, Liam Keliher, Alfred Menezes, Serge Mister, Phong Nguyen, David Pointcheval, Thomas Pornin, Guillaume Poupard, Yiannis Tsiumi, Amr Youssef, and Robert Zuccherato.

This year, in addition to the Workshop Record distributed at the workshop, the papers presented at SAC D8 are published by Springer-Verlag in the Lecture Notes in Computer Science Series. Copies of the Springer Proceedings are being sent to all registrants.

The organizers of SAC D8 are pleased to thank Entrust Technologies for their financial support and Sheila Hutchison of the Department of Electrical and Computer Engineering at Queen's University for administrative and secretarial help. Yifeng Shao put together the Workshop Record and provided invaluable assistance in the preparation of these Proceedings. We also thank Laurie Ricker who looked after registration.

November 1998

Stafford Tavares and Henk Meijer
SAC D8 Co-Chairs

Organization

Program Committee

Carlisle Adams	Entrust Technologies
Tom Cusick	SUNY Buffalo
Howard Heys	Memorial University of Newfoundland
Henk Meijer	Queen's University
Doug Stinson	University of Waterloo
Stallord Tavares	Queen's University
Serge Vaudenay	Ecole Normale Supérieure/CNRS
Mike Wiener	Entrust Technologies

Local Organizing Committee

Stallord Tavares (Co-Chair)	Queen's University
Henk Meijer (Co-Chair)	Queen's University

Table of Contents

Design of Secret Key Cryptosystems

Feistel Ciphers with L_2 -Decorrelation	1
<i>Serge Vaudenay (Ecole Normale Supérieure/CNRS)</i>	
Key-Dependent S-Box Manipulations	15
<i>Sandy Harris (Kaya Consulting), Carlisle Adams (Entrust Technologies)</i>	
On the Two \square sh Key Schedule	27
<i>Bruce Schneier, John Kelsey, Doug Whiting (Counterpane Systems), David Wagner (University of California, Berkeley), Chris Hall (Counterpane Systems)</i>	
Toward Provable Security of Substitution-Permutation Encryption Networks	43
<i>Zhi-Guo Chen, Stafford E. Tavares (Queen's University)</i>	

Randomness and Computational Issues

An Accurate Evaluation of Maurer's Universal Test	57
<i>Jean-Sébastien Coron (Ecole Normale Supérieure), David Naccache (Gemplus Card International)</i>	
Computational Alternatives to Random Number Generators	72
<i>David M'Raihi (Gemplus Corporation), David Naccache (Gemplus Card International), David Pointcheval, Serge Vaudenay (Ecole Normale Supérieure)</i>	
Storage-Efficient Finite Field Basis Conversion	81
<i>Burton S. Kaliski Jr., Yiqun Lisa Yin (RSA Labs)</i>	
Verifiable Partial Sharing of Integer Factors	94
<i>Wenbo Mao (HP Labs U.K.)</i>	

Analysis of Secret Key Cryptosystems

Higher Order Differential Attack Using Chosen Higher Order Differences .	106
<i>Shiho Moriai (NTT Labs), Takeshi Shimoyama (TAO), Toshinobu Kaneko (TAO & Science University of Tokyo)</i>	
On Maximum Non-averaged Differential Probability	118
<i>Kazumaro Aoki (NTT Labs)</i>	

Cryptanalysis of RC4-like Ciphers	131
<i>Serge Mister (Entrust Technologies),</i> <i>Stafford E. Tavares (Queen's University)</i>	

Cryptographic Systems

Key Preassigned Traceability Schemes for Broadcast Encryption	144
<i>Doug R. Stinson, R. Wei (University of Waterloo)</i>	
Mix-Based Electronic Payments	157
<i>Markus Jakobsson (Bell Labs), David M'Raihi (Gemplus Corporation)</i>	
Over the Air Service Provisioning	174
<i>Sarvar Patel (Lucent Technologies)</i>	

Public Key Cryptosystems

Faster Attacks on Elliptic Curve Cryptosystems	190
<i>Michael J. Wiener, Robert J. Zuccherato (Entrust Technologies)</i>	
Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$	201
<i>Julio López (University of Valle),</i> <i>Ricardo Dahab (State University of Campinas)</i>	
Cryptanalysis of a Fast Public Key Cryptosystem Presented at SAC 97	213
<i>Phong Nguyen, Jacques Stern (Ecole Normale Supérieure)</i>	
A Lattice-Based Public-Key Cryptosystem	219
<i>Jin-Yi Cai, Tom Cusick (SUNY Buffalo)</i>	

Design and Implementation of Secret Key Cryptosystems

Fast DES Implementation for FPGAs and Its Application to a Universal Key-Search Machine	234
<i>Jens-Peter Kaps, Christof Paar (Worcester Polytechnic Institute)</i>	
IDEA: A Cipher for Multimedia Architectures?	248
<i>Helger Lipmaa (AS Küberneetika)</i>	
A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis	264
<i>Masayuki Kanda, Youichi Takashima (NTT Labs),</i> <i>Tsutomu Matsumoto (Yokohama National University),</i> <i>Kazumaro Aoki, Kazuo Ohta (NTT Labs)</i>	
The Nonhomomorphicity of Boolean Functions	280
<i>Xian-Mo Zhang (University of Wollongong),</i> <i>Yuliang Zheng (Monash University)</i>	

Attacks on Secret Key Cryptosystems

Cryptanalysis of ORYX	296
<i>David Wagner (University of California, Berkeley),</i>	
<i>Leone Simpson, Ed Dawson (Queensland University of Technology),</i>	
<i>John Kelsey (Counterpane Systems),</i>	
<i>Bill Millan (Queensland University of Technology),</i>	
<i>Bruce Schneier (Counterpane Systems)</i>	
A Timing Attack on RC5	306
<i>Helena Handschuh (ENST & Gemplus),</i>	
<i>Howard M. Heys (Memorial University of Newfoundland)</i>	
Cryptanalysis of SPEED	319
<i>Chris Hall, John Kelsey (Counterpane Systems),</i>	
<i>Vincent Rijmen (K. U. Leuven),</i>	
<i>Bruce Schneier (Counterpane Systems),</i>	
<i>David Wagner (University of California, Berkeley)</i>	

Invited Talks

Authenticated Diffie-Hellman Key Agreement Protocols	339
<i>Simon Blake-Wilson (Certicom Research),</i>	
<i>Alfred Menezes (University of Waterloo)</i>	
Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR	362
<i>Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson</i>	
<i>(Technion - Israel Institute of Technology),</i>	
<i>Adi Shamir (Weizmann Institute of Science)</i>	

Author Index	377
--------------------	-----