

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Howard Heys Carlisle Adams (Eds.)

Selected Areas in Cryptography

6th Annual International Workshop, SAC'99
Kingston, Ontario, Canada, August 9-10, 1999
Proceedings



Springer

Series Editors

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

Volume Editors

Howard Heys
Faculty of Engineering and Applied Science
Memorial University of Newfoundland
St. John's, Newfoundland, Canada A1B 3X5
E-mail: howard@engr.mun.ca

Carlisle Adams
Entrust Technologies
750 Heron Road, Suite E08
Ottawa, Ontario, Canada K1V 1A7
E-mail: cadams@entrust.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Selected areas in cryptography : 6th annual international workshop ;
proceedings / SAC '99, Kingston, Ontario, Canada, August 9 - 11,
1999. Howard Heys ; Carlisle Adams (ed.). - Berlin ; Heidelberg ; New
York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ;
Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1758)
ISBN 3-540-67185-4

CR Subject Classification (1991): E.3, C.2, D.4.6, K.6.5, F.2.1-2, H.4.3

ISSN 0302-9743

ISBN 3-540-67185-4 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 is a company in the specialist publishing group BertelsmannSpringer
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author

Printed on acid-free paper

SPIN 10719627

57/3144

5 4 3 2 1 0

Preface

SAC'99 was the sixth in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Carleton University in Ottawa (1995 and 1997) and at Queen's University in Kingston (1994, 1996, and 1998). The intent of the annual workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC'99 workshop were:

- Design and Analysis of Symmetric Key Cryptosystems
- Efficient Implementations of Cryptographic Systems
- Cryptographic Solutions for Web/Internet Security

The timing of the workshop was particularly fortuitous as the announcement by NIST of the five finalists for AES coincided with the first morning of the workshop, precipitating lively discussion on the merits of the selection!

A total of 29 papers were submitted to SAC'99 and, after a review process that had all papers reviewed by at least 3 referees, 17 were accepted and presented. As well, two invited presentations were given: one by Miles Smid from NIST entitled "From DES to AES: Twenty Years of Government Initiatives in Cryptography" and the other by Mike Reiter from Bell Labs entitled "Password Hardening with Applications to VPN Security".

The program committee for SAC'99 consisted of the following members: Carlisle Adams, Tom Cusick, Howard Heys, Lars Knudsen, Henk Meijer, Luke O'Connor, Doug Stinson, Stafford Tavares, and Serge Vaudenay. As well, additional reviewers were: Christian Cachin, Louis Granboulan, Helena Handschuh, Julio Lopez Hernandez, Mike Just, Alfred Menezes, Serge Mister, Guillaume Poupard, Victor Shoup, Michael Wiener, and Robert Zuccherato.

The organizers are very grateful for the financial support for the workshop received from Entrust Technologies, the Department of Electrical and Computer Engineering at Queen's University, and Communications and Information Technology Ontario (CITO). Special thanks to Stafford and Henk must be given for, once again, hosting SAC and being responsible for all the local arrangement details. The organizers would also like to thank Sheila Hutchison of the Department of Electrical and Computer Engineering at Queen's University for administrative and secretarial help and Yaser El-Sayed from the Faculty of Engineering at Memorial University of Newfoundland for help in preparing the workshop proceedings.

On behalf of the SAC'99 organizing committee, we thank all the workshop participants for making SAC'99 a success!

Organization

Program Committee

Howard Heys (co-chair)	Memorial University of Newfoundland
Carlisle Adams (co-chair)	Entrust Technologies, Ottawa
Tom Cusick	SUNY, Buffalo
Lars Knudsen	University of Bergen
Henk Meijer	Queen's University at Kingston
Luke O'Connor	IBM, Zurich
Doug Stinson	University of Waterloo
Stafford Tavares	Queen's University at Kingston
Serge Vaudenay	Ecole Normale Supérieure, Paris

Local Organizing Committee

Stafford Tavares	Queen's University at Kingston
Henk Meijer	Queen's University at Kingston

Table of Contents

Cryptosystems and Pseudorandom Number Generators

A Universal Encryption Standard	1
<i>Helena Handschuh and Serge Vaudenay</i>	
Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator	13
<i>John Kelsey, Bruce Schneier, and Niels Ferguson</i>	
Elliptic Curve Pseudorandom Sequence Generators	34
<i>Guang Gong, Thomas A. Berson, and Douglas R. Stinson</i>	

Security Aspects of Block Ciphers

Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness ...	49
<i>Serge Vaudenay</i>	
Guesswork and Variation Distance as Measures of Cipher Security	62
<i>John O. Plam</i>	
Modeling Linear Characteristics of Substitution-Permutation Networks ...	78
<i>Liam Keliher, Henk Meijer, and Stafford Tavares</i>	
Strong Linear Dependence and Unbiased Distribution of Non-propagative Vectors	92
<i>Yuliang Zheng and Xian-Mo Zhang</i>	

Cryptanalysis of Block Ciphers

Security of E2 against Truncated Differential Cryptanalysis	106
<i>Shiho Moriai, Makoto Sugita, Kazumaro Aoki, and Masayuki Kanda</i>	
Key-Schedule Cryptanalysis of DEAL	118
<i>John Kelsey and Bruce Schneier</i>	
Efficient Evaluation of Security against Generalized Interpolation Attack ..	135
<i>Kazumaro Aoki</i>	

Efficient Implementations of Cryptosystems

Efficient Implementation of Cryptosystems Based on Non-maximal Imaginary Quadratic Orders	147
<i>Detlef Hühnlein</i>	

Improving and Extending the Lim/Lee Exponentiation Algorithm	163
<i>Biljana Cubaleska, Andreas Rieke, and Thomas Hermann</i>	

Software Optimization of Decorrelation Module	175
<i>Fabrice Noilhan</i>	

Cryptography for Network Applications

Pseudonym Systems	184
<i>Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf</i>	

Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures	200
<i>Douglas R. Stinson and R. Wei</i>	

Protecting a Mobile Agent's Route against Collusions	215
<i>Dirk Westhoff, Markus Schneider, Claus Unger, and Firoz Kaderali</i>	

Photuris: Design Criteria	226
<i>William Allen Simpson</i>	

Author Index	243
-------------------------------	------------