

SAC '96

**Third Annual Workshop on
*Selected Areas in Cryptography***

**15-16 August 1996
Workshop Record**

**Walter Light Hall
Queen's University
Kingston, Ontario
Canada K7L 3N6**

Preface

SAC '96 is the third of an annual series of workshops on Selected Areas in Cryptography. The first, SAC '94, was also held at Queen's University, and the second, SAC '95, was held at Carleton University. The purpose of the Workshop is to bring together researchers in cryptography to present new work on selected areas of current interest. It is hoped that focusing on a few topics will present a good opportunity for in-depth discussion in a relaxed atmosphere. The topics for SAC '96 include:

- New Block Ciphers
- Block Cipher Design Principles
- Efficiency in Public-Key Cryptography.

There are two invited presentations at SAC '96. One will be given by Paul Syverson entitled "Time in the Formal Analysis of Authentication Protocols". The other is by Serge Vaudenay entitled "Towards Provable Security for Feistel Ciphers". There is also a Panel Discussion on "Directions in Block Cipher Design".

Twenty four papers were submitted to SAC '96, from which fourteen were selected. Subsequently, one paper was withdrawn, resulting in thirteen papers to be presented in the regular program.

A subset of the papers accepted for SAC '96 will be invited for submission to a special issue of "Designs, Codes and Cryptography" to be refereed in accordance with the standard procedures for that journal.

The Program Committee members for SAC '96 are: Carlisle Adams, Howard Heys, Mike Just, Henk Meijer, Stafford Tavares and Mike Wiener.

We wish to thank the Department of Electrical and Computer Engineering, Queen's University, and Telecommunications Research Institute of Ontario (TRIO) for their support, and Kathy Williams and Patty Jordan for secretarial help.

On behalf of the Organizing Committee, we welcome you to SAC '96, Queen's University and Kingston.

Stafford Tavares and Henk Meijer
Local Arrangements Committee



SAC '96 Program

THURSDAY, AUGUST 15

10:00 **Opening Remarks**

Session 1: New Block Ciphers 1
Chair: Carlisle Adams

10:10 “Akelarre: A New Block Cipher Algorithm”, *G.Alvarez, D. de la Guía, F.Montoya, and A.Peinado, Instituto de Fisica Aplicada, Spain*

10:40 “CRISP: A Feistel Cipher With Hardened Key-Scheduling”, *M. Leech, Nortel, Canada*

11:10 Morning Break

Session 2: New Cipher Structures 30
Chair: Howard Heys

11:30 “Provably Secure and Efficient Block Ciphers”, *P. Morin, Carleton University, Canada*

12:00 “Message Encryption and Authentication Using One-Way Hash Functions”, *C.H. Lim, Baekdoo Info Crypt., Inc., Korea*

12:30 **Lunch: Queen’s University Club**

Session 3: Invited talk
Chair: Michael Weiner

14:15 *Invited Lecture by Paul Syverson, Naval Research Laboratory, Washington, DC*
Title: “Time in the Formal Analysis of Authentication Protocols”

Session 4: Boolean Functions and S-boxes 49
Chair: Serge Vaudenay

15:15 “New Bounds On The Number Of Functions Satisfying The Strict Avalanche Criterion”, *A.M. Youssef, T.W. Cusick, P. Stănică and S.E. Tavares, Queen’s University, Canada, and SUNY at Buffalo, USA*

15:45 “Difference Distribution Table of a Regular Substitution Box”, *X.-M. Zhang, University of Wollongong, Australia and Y.Zheng, Monash University, Australia*

16:15 Afternoon Break

	Session 5 Private-Key Cipher Design Principles I.....	61
Chair:	Michael Just	
16:30	“Practical S-box Design”, <i>S. Mister and C. Adams, Nortel, Canada</i>	
17:00	“Modelling Avalanche in DES-Like Ciphers”, <i>H. Heys, Memorial University, Canada</i>	
19:00	<i>Social Gathering and Dinner at Queen’s University Club</i>	
20:30	Panel Discussion: Directions in Block Cipher Design Location: Queen’s University Club	

FRIDAY, AUGUST 16

Session 6:	Invited talk	92
Chair:	Stafford Tavares	
9:00	<i>Invited lecture by Serge Vaudenay, Ecole Normale Superieure, Paris</i> <i>Title: “Towards Provable Security for Feistel Ciphers”</i>	
10:00	Morning Break	
Session 7:	Efficiency in Public-Key Cryptography.....	95
Chair:	Mike Wiener	
10:30	“Montgomery Multiplication in GF (2^k)”, <i>Ç.K. Koç and T. Acar, Oregon State University, USA</i>	
11:00	“A Parallel Implementation of RSA”, <i>D. Pearson, Cornell University, USA</i>	
11:30	“Sparse RSA Secret Keys and Their Generation”, <i>C.H. Lim and P.J. Lee, Pohang University of Science and Technology, Korea</i>	
12:00	Lunch	
Session 8:	Private-Key Cipher Design Principles II	132
Chair:	Henk Meijer	
14:00	“A New Class of Substitution-Permutation Networks”, <i>A.M. Youssef, S.E. Tavares, Queen’s University, Canada and H.M. Heys, Memorial University, Canada</i>	
14:30	“Nonlinear Generators with a Guaranteed Large Linear Complexity”, <i>P. Caballero-Gill and A. Fister-Sabater, Spain</i>	
15:00	Closing Remarks	

