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 Subsequently, one paper was withdrawn, resulting in thirteen papers to be presented in the regular program.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