CALL FOR PAPERS
SAC 2002

Ninth Annual Workshop on Selected Areas in Cryptography
to be held at:
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
August 15-16, 2002

Workshop Themes

Original papers on the following workshop themes are solicited:

1. Design and analysis of symmetric key cryptosystems
2. Primitives for private key cryptography, including block and stream ciphers, hash functions and MACs
3. Efficient implementation of cryptographic systems in public and private key cryptography
4. Cryptographic solutions for mobile and wireless network security

Instructions for Authors

A submission must consist of an extended abstract of at most 15 pages, clearly indicating the results achieved, their significance, and their relation to other work in the area. Authors can either send one copy of a Postscript file by email to `sac2002@engr.mun.ca` or send ten copies of the submission to

Kaisa Nyberg
Nokia Research Center
Itamerenkatu 11-13
FIN-00180 Helsinki, Finland
Phone: +358 7180 37384

The deadline for submission by email is May 3, 2002. The submissions by mail must also arrive by May 3, or must be postmarked on April 26, 2002, and sent by airmail. Submissions not meeting these guidelines risk rejection without consideration of their merits. The notification of the committee's decision will be sent to authors by June 19, 2002. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Conference Proceedings

As in previous years, the workshop record of presented papers will be available to participants. Following the workshop, the formal proceedings will be published by Springer-Verlag in the *Lecture Notes in Computer Science* series. Instructions about the final copy for the proceedings will be sent to the authors of the papers presented at the workshop. The final copies of the presented papers will be due on September 15, 2002. Final papers arriving too late will be removed from the proceedings.

Important Dates:

Submission	May 3, 2002
Acceptance	June 19, 2002
Workshop	August 15-16, 2002
Proceedings version	September 15, 2002

Program Committee:

Stefan Brands	Credentica Inc., Canada	Kaisa Nyberg (co-chair)	Nokia Research Center, Finland
Henri Gilbert	France Telecom, France	Reihaneh Safavi-Naini	Univ. of Wollongong, Australia
Guang Gong	University of Waterloo, Canada	Douglas Stinson	University of Waterloo, Canada
Helena Handschuh	Gemplus, France	Stafford Tavares	Queen's University, Canada
Howard Heys (co-chair)	Memorial Univ. of Nfld., Canada	Serge Vaudenay	EPFL, Switzerland
Helger Lipmaa	Helsinki Univ. of Tech., Finland	Michael Wiener	Canada
Tal Malkin	AT&T Research, USA	Robert Zuccherato	Entrust, Inc., Canada
Mitsuru Matsui	Mitsubishi Electric, Japan		

Further Conference Information:

Web Page: `http://www.engr.mun.ca/~sac2002`
E-mail: `sac2002@engr.mun.ca`