Report to AARMS

SAC Summer School (S3)
August 10 – 12, 2015
&
Conference on Selected Areas in Cryptography (SAC 2015)
August 12 – 14, 2015

Event Description Part 1 (SAC Summer School (S3))

The inaugural SAC Summer School (S3) was held on August 10–12, 2015, at Mount Allison University in Sackville, New Brunswick, Canada, immediately prior to the Conference on Selected Areas in Cryptography (SAC 2015). S3 was co-chaired by Orr Dunkelman (University of Haifa, Israel) and Liam Keliher (Mount Allison). The purpose of S3 was to provide participants with an opportunity to gain in-depth knowledge of specific areas of cryptography related to SAC 2015 topics by bringing together world-class researchers to give extended talks in their areas of specialty. Overall, S3 was designed to create a focused learning environment that was also relaxed and collaborative.

The SAC Summer School spanned 2.5 days, and had two main subject areas:

(1) *Design and analysis of symmetric key primitives and cryptosystems*
(2) *Privacy and anonymity enhancing technologies and their analysis*

Four outstanding researchers gave five half-day presentations within these areas:

- Jan Camenisch (IBM Research - Zurich, Switzerland)
- Kaisa Nyberg (Aalto University, Finland)
- Christian Rechberger (TU Denmark)
- Paul Syverson (Naval Research Laboratory, USA).

S3 Schedule

Monday, August 10 : MORNING
Differential Cryptanalysis [Christian Rechberger]

Monday, August 10 : AFTERNOON
Privacy and Anonymity (focus on Onion Routing) [Paul Syverson]

Tuesday, August 11 : MORNING
Linear Cryptanalysis (Kaisa Nyberg)

Tuesday, August 11 : AFTERNOON
Anonymous Credentials [Jan Camenisch]

Wednesday, August 12 : MORNING
Hash Functions [Christian Rechberger]

Event Description Part 2 (SAC 2015)

The Conference on Selected Areas in Cryptography (SAC) is a highly respected international cryptography conference held annually in Canada. Since its inception in 1994, SAC has earned a reputation for attracting a large number of high-quality, focused papers. SAC 2015 was hosted at Mount Allison University on August 12–14, 2015, and was co-chaired by Orr Dunkelman (University of Haifa, Israel) and Liam Keliher (Mount Allison). This is the second time that SAC has been held at Mount Allison (the first was in 2008).

One of the key strengths of the SAC conference is its highly international flavor. The SAC 2015 Program Committee consisted of 35 experts from 15 countries (of whom 7 were from Canada). The PC members reviewed 91 paper submissions, ultimately accepting 29 for presentation and publication (3 as short papers). The review process was very thorough; each submission received the attention of at least three reviewers, and at least five for submissions involving a Program Committee member. The 91 submission came from authors in 28 countries from every continent (except Antarctica), including a paper with a co-author from North Korea! Broken down by continent, 11 submissions were from North America (3 from Canada), 32 from Europe, 45 from Asia, 1 from Africa, 1 from South America, and 1 from Australia. Of the 29 accepted papers, 4 were from North America (1 from Canada), 14 from Europe, and 11 from Asia.

Each SAC conference has four main topic areas. The first three are permanent:

(1) Design and analysis of symmetric key primitives and cryptosystems including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes
(2) Efficient implementations of symmetric and public key algorithms
(3) Mathematical and algorithmic aspects of applied cryptology

The fourth topic area, chosen specifically for SAC 2015, was:

(4) Privacy and anonymity enhancing technologies and their analysis

SAC 2015 was slightly longer than most previous iterations (2.5 days instead of 2), and included 29 paper presentations, 3 of which were short papers. In addition, SAC 2015 featured invited talks by two renowned researchers:

- "Trust-Aware Traffic Security"
  Paul Syverson
  Center for High Assurance Computer Systems (CHACS), Naval Research Laboratory
  Washington, DC, USA
- "Generic Attacks against MAC Algorithms"
  Gaëtan Leurent
  INRIA (French Institute for Research in Computer Science and Automation)
  Paris, France

Summary Remark: Overall, SAC 2015 was very successful, and had a nice synergy with the SAC Summer School (S3) that preceded it (12 people attended both).

Participant Details

Over 30 students and early researchers participated in the SAC Summer School S3, surpassing the co-chairs' predicted attendance of 20–25. Of these 30+, 6 were from Atlantic Canada, and the remaining were national/international. Broken down another way, roughly 1/3 were from Canada/USA, 1/3 were from Europe, and 1/3 were from Asia.

SAC 2015 had 55 attendees, which is consistent with recent years. Of these, 5 were from Atlantic Canada and 50 were national/international. Broken down another way, there were 12 participants from Canada, 5 from the USA, 20 from Europe, and 18 from Asia.

Resulting Publications

The SAC proceedings are published each year in the Springer Lecture Notes in Computer Science series. (By design, the SAC Summer School has no directly associated publications.)

SAC 2015 proceedings: http://www.springer.com/cn/book/9783319313009

Scientific Highlights

All of the S3 presenters and SAC invited lecturers speakers are world-class researchers in their own right, but perhaps the highest profile speaker, at least in terms of his fame outside the research community, is Paul Syverson, co-creator of the Tor anonymity network. The National Security Agency (NSA) refers to Tor as "the king of high-secure, low-latency internet anonymity." Paul Syverson is a founder of both the Privacy Enhancing Technologies Symposium (PETS) and the ACM Workshop on Privacy in the Electronic Society (WPES). He has been recognized with an Electronic Frontier Foundation (EFF) Pioneer Award (given to the Tor Project in 2012), and was named one of the 100 Global Thinkers of 2012 by Foreign Policy Magazine. At both S3 and SAC, Paul spoke extensively about the technologies underlying Tor, describing how it facilitates anonymous communication in the presence of powerful adversaries such as repressive governments.

It is also significant that 6 papers presented at SAC concerned *authenticated encryption schemes*, a relatively new category of cryptographic algorithms that is receiving a significant amount of research attention. As an illustration of this, the CAESAR competition, which will run from 2014 to 2017, is focused on selecting a new suite of authenticated encryption algorithms; 4 of the 6 authenticated encryption papers presented at SAC directly analyzed CAESAR candidates.

Other Notable Information

The SAC Board has deemed the inaugural S3 to be a great success, and plans to continue holding S3 immediately before the SAC conference each August. (The 2016 version of S3 will also be an AARMS-sponsored event.)

Financial Details

NOTE: AARMS funds will be used for SAC Summer School (S3) expenses, as detailed below. S3 financial details are presented on this page. The financial details for the SAC conference are on the following page.

S3 Expenses Summary (all amounts in Canadian dollars)

Guest speaker travel:	9466.69
Guest speaker accommodation + food:	2497.15
Student sponsorship (accommodation):	414.00
Student sponsorship (food):	153.00
Van rental + gas (used as airport shuttle):	360.84
Miscellaneous/administration:	73.68
Registration packages:	74.68
Coffee breaks:	1318.00
TOTAL:	**14,358.04**

S3 Revenue Summary (all amounts in Canadian dollars)

Registration fees (industry attendees):	464.60
Mount Allison Dean of Science:	1000.00
IACR[(1)] funding:	6500.00
AARMS funding:	5000.00
TOTAL:	**12,964.60**

[(1)] IACR = International Association for Cryptologic Research

S3 Deficit

S3 ran a deficit of approximately CDN 1400. This will be covered using the surplus from SAC.

Use of AARMS Funds

AARMS funds will be used entirely for guest speaker travel, accommodation, and food. In support of the expense amounts listed above in these categories, the accompanying file **S3-receipts.pdf** contains travel claims and receipts for three of the four S3 speakers in the following amounts:

- Jan Camenisch:	3052.40
- Kaisa Nyberg:	1757.21
- Christian Rechberger:	2540.27
TOTAL:	**7349.88**

SAC 2015 Expenses Summary (all amounts in Canadian dollars)

Guest speaker travel:	3417.52
Guest speaker accommodation + food:	1113.19
Guest speaker registration reimbursement:	400.00
Student sponsorship (accommodation):	276.00
Van rental + gas (used as airport shuttle):	360.84
Miscellaneous/administration:	1144.13
Conference proceedings (Springer)	2000.00
Registration packages:	1514.21
Opening reception (August 12)	932.89
Banquet (August 13)	3542.81
Breakfasts & lunches (provided)	1300.00
Coffee breaks:	1607.40
TOTAL:	**17,608.99**

SAC 2015 Revenue Summary (all amounts in Canadian dollars)

Registration fees (student):	6456.08
Registration fees (non-student):	9650.83
Microsoft Research:	6075.00
IEEE New Brunswick chapter:	500.00
TOTAL:	**22,681.91**

SAC Surplus

SAC had a surplus of just over CDN 5000. As noted on the previous page, part of this will be used to cover the S3 deficit of approximately CDN 1400.

Respectfully submitted,

Orr Dunkelman & Liam Keliher