Report on
Conference on Selected Areas in Cryptography (SAC 2016)
and SAC Summer School (S3)
Nov. 30, 2016

submitted by Dr. Howard Heys
Memorial University of Newfoundland
(hheys@mun.ca)

Date:	August 8-9, 2016 (Summer School) August 10-12, 2016 (Main Conference)
Location:	Memorial University, St. John's campus
Conference Home Web Site:	www.sacconference.org
AARMS Funding:	$5000

Description of the Conference

The Conference on Selected Areas in Cryptography (SAC) series started as a Workshop in 1994, when it first was held at Queen's University in Kingston. SAC has been held annually since 1994 in several Canadian locations and it is the only international conference series on cryptography that is held annually in Canada. Since 2006, the conference has been organized in co-operation with the International Association for Cryptologic Research (IACR), the premier international organization for the promotion of cryptographic research.

During the last 23 years, SAC has established itself as an internationally reputed venue for researchers in cryptography to present and discuss new work on selected areas of current interest in a relaxed and friendly atmosphere. Besides advancing cryptologic research, one of the goals of SAC is to promote young researchers. This is achieved by various means, such as organizing a summer school and involving junior scientists in the program committee with a lighter reviewing load and mentoring them.

This year, SAC took place on August 10th to 12th at Memorial University of Newfoundland (MUN), St. John's. This is the second time that SAC has been hosted in St. John's, and the fourth time in an Atlantic Canadian province.

To keep the conference series focused, each year only results in four themes are presented. Three themes are fixed, and the fourth theme is specially chosen every year. The four themes for SAC 2016 were:

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, and
4. Side channel, fault and related attacks on symmetric and asymmetric cryptographic primitives and their countermeasures.

A total of 100 submissions were received and reviewed, with only 28 papers accepted for presentation. The large number of submissions, resulting in an acceptance rate of only 28% is a testament to the strong reputation of the SAC conference, which has established itself as one of the best cryptography conferences held each year.

In addition to these 28 papers, two renowned international researchers were invited to give presentations at the conference. Douglas Stebila gave the Stafford Tavares Lecture on "Post-Quantum Key Exchange for the Internet" and Francesco Regazzoni talked on "Physical Attacks and Beyond".

Participation

SAC had participation from researchers around the world, as well as local attendees. Attendees can be broken into 4 groups:

(1) Attendees of S3 only
(2) Attendees of SAC Conference only
(3) Attendees of both SAC and S3
4) Invited Speakers

A summary of the origins of participants is given in the following table.

	Regional - Atlantic Canadian	Canadian - outside Atl. Can.	International (US, Eur, Asia)	# Students	# Non-students	Total
S3 only	8	0	0	8	0	8
SAC only	1	11	25 (7, 12, 6)	7	30	37
S3+SAC	3	3	15 (3, 9, 3)	15	6	21
Invited Speakers	0	1	3 (1, 2, 0)	0	4	4
Total S3	**11**	**4**	**18**	**23**	**10**	**33**
Total SAC	**4**	**15**	**43**	**22**	**40**	**62**
Total of S3 and/or SAC	**12**	**15**	**43**	**30**	**40**	**70**

The table is somewhat complex. However, the bottom row is probably the most important as it reflects the number of participants in either S3, SAC, or both. In summary, 70 researchers (including the invited speakers) participated in SAC/S3, with 30 of these being students. Twelve of these participants were from Atlantic Canada, with a very noticeable attendance of Atlantic Canadians at S3, while 43 attendees came from international institutions. We are pleased with this level of attendance, as this is in keeping with the attendance at previous conferences. As expected, the local academic community, particularly students were able to benefit through the summer school by bringing world-leading researchers to St. John's.

Financial Summary

The financial summary is given in the following tables. Note that any surplus funding (up to $4300) from the conference must be returned to the Memorial University Conference Fund. Also, the $10000 seed funding from the SAC Conference Fund is expected to be forwarded to the next conference, SAC 2017, as seed funding.

SUMMARY	
Revenues	$48550.00
Expenses	$46734.22
Surplus (to be returned to Memorial Univ. Conference Fund)	$1815.78

REVENUES	Description	Total
SAC Registration Fees	32 non-student, early @$500	$16000
	4 non-student, regular @$550	$2200
	20 student, early @$300	$6000
	2 student, regular @$350	$700
S3 Registration Fees	29 attendees @$100	$2900
Extra	Banquet ticket	$80
Total Fees		**$27880**
Sponsorship	Memorial Univ. Faculty of Engineering	$3000
	Memorial Univ. Dept. of Elec. and Comp. Eng.	$2000
	Memorial Univ. Conference Fund (refundable if surplus)	$4300
	Microsoft ($5000 USD)	$6370
	AARMS	$5000
Total Sponsorship		**$20670**
Seed Funding	Loan from SAC Conference Fund	$10000
Total Revenues		**$58550**
	Seed funding to be forwarded to SAC 2017	–$10000
Total Available		**$48550**

EXPENSES	Description	Total
Conference Management	Memorial Univ. Conference Service fees	$8084.35
Paper Management	License for "EasyChair" support	$429.22
Banquet	Rental of "The Rooms"	$1723.64
	Catering for dinner	$6130.65
Lunches/Nutrition Breaks	Reception for S3 Lunches, nutrition breaks for S3 and SAC	$7241.15
Speaker Airfares	Speaker 1	$2129.58
	Speaker 2	$3525.49
	Speaker 3	$748.34
	Speaker 4	$1580.61
Speaker Expenses	Total for all speakers	$1600.44
Speaker Hotel	Rooms for speakers and SAC welcoming reception	$5845.35
Conference Swag	Bags (see Appendix C) and USB memory keys	$1728.13
Taxes	HST on conference registration fees	$3567.27
Total Costs to Date	Exact costs to date	**$44334.22**
Future Costs (estimate)	Fees to Springer for extra proceedings copies and mailing of proceedings to attendees (to be due in spring 2017)	$2400
Final Total Costs	Based on total costs to date and estimate of future costs	**$46734.22**

Scientific Program Summary

The full conference program is included in Appendix A.

Conference Proceedings

Although the conference is held in Canada and is a focal point for the Canadian cryptographic community, the conference is truly international, with a program committee consisting of top international researchers in cryptography. Accepted papers come from all over the world, with the vast majority selected from outside Canada. The conference proceedings will be published in the well-regarded Lecture Notes in Computer Science series by Springer. They will be available in the spring of 2017 and mailed directly to conference attendees, as well as being available for purchase directly from Springer.

Review Process

The Program Committee for SAC 2016 comprised a total of 46 members. The review process was thorough – each submission received the attention of at least three reviewers, with almost all accepted papers being reviewed by four. Submissions involving a Program Committee member required at least five reviews. A total of 441 reviews were uploaded, of which 154 were written by 115 external subreviewers. The reviews were then followed by deep discussions, which contributed in a decisive way to the quality of the final selection.

Summer School

For the second time, the SAC Summer School (S3) took place just before the conference, August 8 and 9. In line with the selected topics of the latter, the overall theme of the Summer School was Secure and Efficient Implementation of Cryptographic Algorithms and was comprised of the following talks and speakers:

- Hardware Implementation of Public Key Cryptography
  Tim Guneysu, University of Bremen and DFKI, Germany
- Software Implementation of Public Key Cryptography
  Patrick Longa, Microsoft Research, USA
- Secure Hardware Implementation of Symmetric Key Ciphers (Including Side Channel Resistance)
  Francesco Regazzoni, ALaRI–USI, Lugano, Switzerland
- Implementation and Analysis of Cryptographic Protocols
  Douglas Stebila, McMaster University, Canada

Detailed speaker bios are presented in Appendix B.

Select Paper Highlights

(1) "Post-Quantum Key Exchange for the Internet"
Douglas Stebila

> The prospect of quantum computing poses a threat to the main forms of public key cryptography used in widely deployed security applications, including the Transport Layer Security (TLS) protocol. In this talk, two key exchange protocols built from lattice-based problems are presented: A ring-LWE key exchange protocol offers conjectured 80-bit quantum security requiring about 8 KiB of communication to establish a key, and a LWE key exchange

protocol offers conjectured 128-bit quantum security using about 22 KiB of communication to establish a key. These key exchange protocols are evaluated in the context of the TLS protocol: when all aspects of the TLS handshake are included, especially the RSA or ECDSA signatures, the communication and computation overhead of moving to quantum-resistant cryptography are muted: for example, our LWE key exchange increases TLS total handshake latency by a factor of 1.6x, and throughput by a factor of 1.2x when serving 100 KiB web pages.

(2) "Keymill: Side-Channel Resilient Key Generator - A New Concept for SCA-Security Design"
Mostafa Taha, Arash Reyhani-Masoleh, and Patrick Schaumont

In this paper, the authors consider a new paradigm to providing security against side channel attacks against cryptographic implementations. They propose the design of a new keystream generator immune to side channel analysis attacks. The fundamental idea is to mix key bits in a special way that expands the size of any useful key hypothesis to the full entropy, which enables SCA-security that is equivalent to the brute force. The approach works on top of any unprotected block cipher for mathematical security. The proposed primitive is generic and can turn any block cipher into a protected mode using only 775 equivalent NAND gates.

(2) "PhiRSA: Exploiting the Computing Power of Vector Instructions on Intel Xeon Phi for RSA"
Yuan Zhao, Wuqiong Pan, Jingqiang Lin, Peng Liu, Cong Xue and Fangyu Zheng

The authors of this paper propose a vector-oriented Montgomery multiplication design based on vector carry propagation chain method to fully exploit the computing power of vector instructions on Intel Xeon Phi. The Intel Xeon Phi is a highly parallel coprocessor of Many Integrated Core (MIC) architecture, with up to 61 cores and one 512-bit Vector Processing Unit (VPU) in each core, which offers the potential to achieve both high throughput and small latency. The resulting design sharply reduces the number of instructions and the VPUs are fully pipelined and maintain carry bits in vector mask registers. The results achieve 4.1 to 8.5 times performance of the existing RSA implementations on Intel Xeon Phi, exhibit high throughput comparable to those on GPUs but with much less parallel tasks, and small latency comparable to those on CPUs.

(4) "Fixed-Point Arithmetic in SHE Schemes"
Anamaria Costache, Nigel P. Smart, Srinivas Vivek and Adrian Waller

This paper investigates fixed-point arithmetic in ring-based Somewhat Homomorphic Encryption (SHE) schemes. The authors consider two fixed-point representations and show that they are isomorphic. In addition, they produce lower bounds on the plaintext modulus and degree of the ring needed to support complex homomorphic operations. Finally, they present an application of these bounds to homomorphic image processing.

(5) "Improved Algebraic MACs and Practical Keyed Verification Anonymous Credentials"
Amira Barki, Solenn Brunet, Nicolas, Desmoulins and Jacques Traore

This paper proposes a new method for anonymous credential systems. The method is based on the Keyed Verification Anonymous Credentials (KVAC) system proposed by Chase, et al. in 2014, which relies on algebraic Message Authentication Codes (MACs) in prime-order groups. The proposed system provides multi-show unlinkability of credentials and is of complexity O(1) in the number of group elements. The resulting system is shown to be provably secure in the random oracle model and highly efficient for constrained devices (as demonstrated by implementation on a standard NFC SIM card).

Appendix A – SAC Program

SAC 2016 Program

All talks will take place in room SN2109 in the Science Building.

Tuesday, August 9

5:30-7:00	**Welcome Reception** ("The Narrows" in Sheraton Hotel)

Wednesday, August 10

8:30-9:00	**Registration** (Room SN2109 in Science Building)

9:00-9:10	**Opening Remarks**

9:10-10:25	**Session 1: Side Channels and Fault Attacks I** (Chair: Orr Dunkelman)

Detecting Side Channel Vulnerabilities in Improved Rotating S-box Masking Scheme — Presenting Four Non-profiled Attacks
Zeyi Liu, Neng Gao, Chenyang Tu, Yuan Ma and Zongbin Liu

Bridging the Gap: Advanced Tools for Side-Channel Leakage Estimation beyond Gaussian Templates and Histograms
Tobias Schneider, Amir Moradi, Francois-Xavier Standaert and Tim Güneysu

Uniform First-Order Threshold Implementations
Tim Beyne, Begül Bilgin and Vincent Rijmen

10:25-10:45	**Coffee/Nutrition Break**

10:45-11:35	**Session 2: Design and Implementation of Symmetric Cryptography** (Chair: Tim Güneysu)

On the Construction of Hardware-friendly 4x4 and 5x5 S-boxes
Stjepan Picek, Bohan Yang, Vladimir Rozic and Nele Mentens

All the AES You Need on Cortex-M3 and -M4
Peter Schwabe and Ko Stoffelen

11:35-11:45	**Break**

11:45-12:35	**Invited Talk:** (Chair: Howard Heys) Francesco Regazzoni – "Physical Attacks and Beyond"

12:35-2:10	**Lunch** (Hatcher House, East Room)

2:10-3:25	**Session 3: Efficient Classical Public Key Cryptography** (Chair: Nigel Smart)

Fast, Uniform Scalar Multiplication for Genus 2 Jacobians with Fast Kummers
Ping Ngai Chung, Craig Costello and Benjamin Smith

PhiRSA: Exploiting the Computing Power of Vector Instructions on Intel Xeon Phi for RSA
Yuan Zhao, Wuqiong Pan, Jingqiang Lin, Peng Liu, Cong Xue and Fangyu Zheng

FourQNEON: Faster Elliptic Curve Scalar Multiplications on ARM Processors
Patrick Longa

3:25-3:45	**Coffee/Nutrition Break**

3:45-5:00	**Session 4: Cryptanalysis of Symmetric Primitives I** (Chair: Dustin Moody)

New Second Preimage Attacks on Dithered Hash Functions with Low Memory Complexity
Muhammad Barham, Orr Dunkelman, Stefan Lucks and Marc Stevens

New Differential Bounds and Division Property of LILLIPUT: Block Cipher with Extended Generalized Feistel Network
Yu Sasaki and Yosuke Todo

Cryptanalysis of Simpira
Christoph Dobraunig, Maria Eichlseder and Florian Mendel

Thursday, August 11

9:00-10:15	**Session 5: Lattice-Based Cryptography** (Chair: Patrick Longa)

Fixed-Point Arithmetic in SHE Schemes
Anamaria Costache, Nigel P. Smart, Srinivas Vivek and Adrian Waller

A Full RNS Variant of FV like Somewhat Homomorphic Encryption Schemes
Jean-Claude Bajard, Julien Eynard, Anwar Hasan and Vincent Zucca

Security Considerations for Galois RLWE Families
Hao Chen, Kristin Lauter and Katherine Stange

10:15-10:35	**Coffee/Nutrition Break**

10:35-11:50	**Session 6: MACs and PRNGs** (Chair: Douglas Stebila)

Output Masking of Tweakable Even-Mansour can be Eliminated for Message Authentication Code
Shoichi Hirose, Yusuke Naito and Takeshi Sugawara

Improved Algebraic MACs and Practical Keyed-Verification Anonymous Credentials
Amira Barki, Solenn Brunet, Nicolas Desmoulins and Jacques Traore

A Robust and Sponge-Like PRNG with Improved Efficiency
Daniel Hutchinson

Lunch (box lunch available)

Afternoon - **Puffin/Whale Watching Tour** (optional, must be pre-purchased)

Conference Banquet ("The Rooms" Museum)
6:30-7:30 Pre-dinner drinks
7:30-10:00 SAC Conference Banquet

Sponsored by: Microsoft Research

Friday, August 12

9:10-10:25	**Session 7: Side Channels and Fault Attacks II** (Chair: Anwar Hasan)

Attacking Embedded ECC Implementations Through cmov Side Channels
Erick Nascimento, Lukasz Chmielewski, David Oswald and Peter Schwabe

Lattice Attacks against Elliptic-Curve Signatures with Blinded Scalar Multiplication
Dahmun Goudarzi, Matthieu Rivain and Damien Vergnaud

Loop-Abort Faults on Lattice-Based Fiat-Shamir and Hash-and-Sign Signatures
Thomas Espitau, Benoît Gérard, Pierre-Alain Fouque, and Mehdi Tibouchi

10:25-10:45	**Coffee/Nutrition Break**

10:45-11:35	**Session 8: Cryptanalysis of Symmetric Primitives II** (Chair: Hamid Usefi)

An Efficient Affine Equivalence Algorithm for Multiple S-Boxes and a Structured Affine Layer
Jung Hee Cheon, Hyunsook Hong, Joohee Lee and Jooyoung Lee

Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3
Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent and John Schanck

11:35-11:45	**Break**

11:45-12:35	**Stafford Tavares Invited Lecture:** (Chair: Mike Jacobson) Douglas Stebila – "Post-Quantum Key Exchange for the Internet"

12:35-2:10	**Lunch** (Hatcher House, East Room)

2:10-3:25	**Session 9: Efficient Symmetric Primitives** (Chair: Francesco Regazzoni)

Hold Your Breath, PRIMATEs Are Lightweight
Danilo Šijačić, Andreas Brasen Kidmose, Bohan Yang, Subhadeep Banik, Begül Bilgin, Andrey Bogdanov and Ingrid Verbauwhede

Keymill: Side-Channel Resilient Key Generator
Mostafa Taha, Arash Reyhani-Masoleh and Patrick Schaumont

Lightweight Fault Attack Resistance in Software Using Intra-Instruction Redundancy
Conor Patrick, Bilgiday Yuce, Nahid Ghalaty and Patrick Schaumont

3:25-3:45	**Coffee/Nutrition Break**

3:45-5:00	**Session 10: Cryptanalysis of Asymmetric Primitives** (Chair: Petr Lisonek)

Sieving for Closest Lattice Vectors (with Preprocessing)
Thijs Laarhoven

Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
Dustin Moody, Ray Perlner and Daniel Smith-Tone

Solving Discrete Logarithms on a 170-bit MNT Curve by Pairing Reduction
Aurore Guillevic, François Morain and Emmanuel Thomé

Appendix B – Summer School Speaker Bios

Tim Güneysu, *University of Bremen & DFKI, Germany*
Tim Güneysu is an associate professor and head of the research group for Computer Engineering and IT-Security (CEITS) at University of Bremen. His group was established in corporation with the German Research Center for Artificial Intelligence (DFKI) as part of Germany's Excellence Initiative. Tim's primary research topics are in the secure design and implementation of embedded and hardware-based systems, including aspects such as long-term secure cryptography, lightweight and hardware-entangled cryptography. He was a leading developer of the FPGA-based COPACOBANA cluster system that was specifically designed for the task of cryptanalysis. Prior to his current position, Tim was assistant professor and head of the Hardware Security Group at the HGI at Ruhr-University Bochum.

Patrick Longa, *Microsoft Research, USA*
Patrick Longa is a cryptography researcher and developer with the MSR-T Security and Cryptography Group at Microsoft Research, in Redmond. His research interests involve elliptic curve and pairing-based cryptography, post-quantum cryptography, efficient algorithmic design, computer arithmetic, high-performance implementation of cryptographic systems, and side-channel analysis. He is a co-designer of the elliptic curve FourQ, and has written numerous high-performance cryptographic libraries including SIDH, FourQlib, LatticeCrypto, and MSR ECCLib. Patrick got his PhD in Electrical and Computer Engineering from the University of Waterloo, Canada, in 2011. During his time at Waterloo, he was also a member of the Centre for Applied Cryptographic Research (CACR) and the Laboratory for Side-Channel Security of Embedded Systems. He was awarded with the NSERC Alexander Graham Bell Canada Graduate Scholarship. You can learn more about Patrick at http://research.microsoft.com/en-us/people/plonga.

Francesco Regazzoni, *ALaRI - USI, Lugano, Switzerland*
Dr. Francesco Regazzoni is a postdoctoral researcher at the the ALaRI Institute of University of Lugano (Lugano, Switzerland). He received his Master of Science degree from Politecnico di Milano and completed his PhD at the ALaRI Institute of University of Lugano. He has been assistant researcher at the Université Catholique de Louvain and at Technical University of Delft, and visiting researcher at several institutions, including NEC Labs America, Ruhr University of Bochum, EPFL, and NTU. His research interests are mainly focused on embedded systems security, covering in particular side channel attacks, electronic design automation for security, and low energy. For more information, visit Francesco Regazzoni's web page.

Douglas Stebila, *McMaster University, Canada*
Dr. Douglas Stebila is an Assistant Professor in cryptography at McMaster University in Hamilton, Ontario, Canada. His research focuses on improving the security of Internet cryptography protocols such as SSL/TLS and SSH and developing practical quantum-safe cryptosystems. His previous work on the integration and standardization of elliptic curve cryptography in SSL/TLS has been deployed on hundreds of millions of web browsers and servers worldwide. He holds an MSc from the University of Oxford and a PhD from the University of Waterloo.

Appendix C – SAC Bag

Below are photos of SAC conference bag handed out to attendees of the conference. Note the AARMS logo on the bag to credit AARMS sponsorship of the conference.