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