SAC Summer School (S3) 2018 – Program

all sessions will take place in the University of Calgary, ICT Building, room 116

Design, Applications and Implementation of Lightweight Cryptographic Algorithms

Monday, 13 Aug 2018

08:30 – 09:10: Registration (ICT Building, room 114)

09:10 – 09:15: Opening Remarks

S3 Session 1: **Design of lightweight symmetric-key algorithms**
Andrey Bogdanov (Technical University of Denmark)

09:15 – 10:30: Design of lightweight symmetric-key algorithms I

10:30 – 11:00: coffee break

11:00 – 12:15: Design of lightweight symmetric-key algorithms II

12:15 – 13:45: LUNCH

S3 Session 2: **Applications and Standardization of lightweight cryptography**
Meltem Sonmez Turan (NIST)

13:45 – 15:00: Applications and Standardization of lightweight cryptography I

15:00 – 15:30: coffee break

15:30 – 16:45: Applications and Standardization of lightweight cryptography II

Tuesday, 14 Aug 2018

S3 Session 3: **Cryptographic hardware engineering**
Francesco Regazzoni (Università della Svizzera italiana - USI)

09:15 – 10:30: Cryptographic hardware engineering I

10:30 – 11:00: coffee break

11:00 – 12:15: Cryptographic hardware engineering II

12:15 – 13:45: LUNCH

S3 Session 4: **Cryptographic software engineering**
Daniel J. Bernstein (University of Illinois at Chicago)

13:45 – 15:00: Cryptographic software engineering I

15:00 – 15:30: coffee break

15:30 – 16:45: Cryptographic software engineering II