

**First SHA-3 Candidate Conference
Preliminary Participants List**

Martin Ågren
Lund University

Toru Akishita
Sony Corp.

Laurent Albanese
NAGRA FRANCE

Mohamed Ezzat Aly
Q2S/NTNU

Jorn Amundsen
NTNU/IDI

Elena Andreeva
ESAT/COSIC

Jean-Philippe Aumasson
FHNW

Onur Ozen
EPFL

Stanislav Bajer
NBU

Daniel Bernstein
University of Illinois at Chicago

Guido Bertoni
STMicroelectronics

Alex Biryukov
University of Luxembourg

Tor E. Bjorstad
University of Bergen, Norway

Charles Bouillaguet
ENS

Henno Brandsma
Ministry of Defense

Daniel Brown
Certicom Corp.

Mateusz Buczek
Military University of Technology

Bill Burr
NIST

Jon Callas
PGP Corp.

Anne Canteaut
INRIA

Shu-jen Chang
NIST

Lily Chen
NIST

Christophe Clavier
University of Limoges

Martin Cochran
Google, Inc.

Debra Cook
Inst. for Defense Analysis Center for
Computing Scie.

Joan Daemen
STMicroelectronics

Christophe De Canniere
K.U.Leuven

Benne de Weger
Eindhoven University of Technology

Markus Dichtl
Siemens AG

Andrey Dmukh
Federal Security Service

**First SHA-3 Candidate Conference
Participants List**

Donna Dodson
NIST

Riaal Domingues
Armcor Business Eclipse

Dennis Duckworth
Broadcom

Orr Dunkelman
ENS

Milos Dvorak
NBU

Baris Ege
METU - IAM

Niels Ferguson
Microsoft

Matthieu Finiasz
ENSTA

Ewan Fleischmann
University Weimar / Dresden

Christian Forler
Sirrix AG

Thomas Fuhr
DCSSI

Philippe Gaborit
University of Limoges

Roland Gillard
UJF

Michal Glet
Military University

Danilo Gligoroski
NTNU - Norway

Rafal Gliwa
Military Communication Institute

Richard Graveman
RFG Security

Carmi Gresssel
FortressGB Ltd. London

Michael Groves
CESG

Shay Gueron
University of Haifa and Intel Corp.

Jian Guo
Nanyang Technological University

Anwar Hasan
Univ. of Waterloo

Mehdi Hassanzadeh
University of Bergen

Philip Hawkes
Qualcomm International

Matt Henricksen
Institute for Infocomm Research

Shoichi Hirose
University of Fukui

Michal Hojsik
The Selmer Center, University of
Bergen

Seokhie Hong
CIST, Korea Univ.

Deukjo Hong
The Attached Institute of ETRI

Georg Illies
BSI

**First SHA-3 Candidate Conference
Participants List**

Sebastiaan Indesteege
Katholieke Universiteit Leuven

Tetsu Iwata
Nagoya University

Stéphane Jacob
INRIA

Cees J.A. Jansen
Compumatica Secure Networks
B.V.

Keting Jia
Shandong University

Charanjit Jutla
IBM

Ozgul Kucuk
K.U. Leuven

Marcelo Kaihara
EPFL

Orhun Kara
Tubitak

Grigory Karpunin
Moscow State University

Emilia Kasper
K.U. Leuven ESAT/COSIC

Shahram Khazaei
EPFL

Dmitry Khovratovich
University of Luxembourg

Jongsung Kim
CIST, Korea Univ.

Svein Johan Knapskog
NTNU/Q2S

Lars Knudsen
DTU

Cetin Koc
University of California

Onur Kocak
METU - IAM

Robert Koch
AMK-WFB

Peck Kong Beng
DSO National Laboratories

Mike Kounavis
INTEL Corp.

Takashi Kurokawa
NICT

Hidenori Kuwakado
Kobe University

Helge Laegreid
NC3A

Vincent Labie
Orange

Frederic Lafitte
RMA

Brian LaMacchia
Microsoft

Franck Landelle
DGA/CELAR

Gaetan Laurent
ENS

Yunqin Lin
Xiamen Langyue Software Co.,Ltd.

**First SHA-3 Candidate Conference
Participants List**

Stefan Lucks
Bauhaus-University Weimar

Vadim Lyubashevsky
Tel-Aviv University

Marco Macchetti
Nagracard SA

Megan Maguire
UCSB

John Manferdelli
Microsoft Corp.

Stephane Manuel
CRI Paris-Rocquencourt

Jason Martin
James Madison University

Mitsuru Matsui
Mitsubishi Electric

Shin'ichiro Matsuo
NTT Data Corp.

Krystian Matusiewicz
Technical University of Denmark

Dmitry Matyukhin
Federal Security Service

Aleksandra Mileva
Faculty of Informatics, University
Goce Delcev

Kelly Miller
U.S. Government

Kathryn Mills
Government of Canada

Carl Minden
University of California

Kazuhiko Minematsu
NEC Corp.

Shiho Moriai
Sony Corp.

Nicky Mouha
K.U.Leuven

Jorge Nakahara Jr.
EPFL

Mridul Nandi
NIST

Daniel Napiorkowski
MON

Maria Naya-Plasencia
INRIA Paris-Rocquencourt

Ivica Nikolic
University of Luxembourg

Ventzislav Nikov
NXP Semiconductors

Svetla Nikova
University Twente

Kenji Ohkuma
IPA

Sean O'Neil
VEST Corpo.

Hilarie Orman
PurpleStreak

Dag Arne Osvik
EPFL

Souradyuti Paul
NIST

**First SHA-3 Candidate Conference
Participants List**

Michael Peeters
NXP Semiconductors

Daniel Penazzi
Universidad Nacional de Cordoba

Rene Peralta
NIST

Thomas Peyrin
INGENICO

Gilles Piret
Oberthur Card Systems

Bart Preneel
Katholieke Universiteit Leuven

Marina Pudovkina
Moscow Engineering Physics
Institute

Xin Qiu
Motorola

Jean-Jacques Quisquater
Universiteit Catholique de Louvain

Christian Rechberger
IAIK, TU Graz

Francesco Regazzoni
UCL-ALaRI

Vincent Rijmen
Katholieke Universiteit Leuven

Ronald Rivest
MIT

Matt Robshaw
Orange Labs

Przemyslaw Rodwald
Military Communication Institute

Andrea Roeck
INRIA Paris-Rocquencourt

Bohuslav Rudolf
NBU

Juraj Sarinay
EPFL

Yu Sasaki
NTT Corp.

Werner Schindler
Bundesamt Sicherheit in der
Informationstechnik (BSI)

Martin Schläpfer
IAIK, TU Graz

Dorit Schlabs
AMK

Erik Schlegel
MPA

Bent Schmidt-Nielsen

Peter Schmidt-Nielsen

Bruce Schneier
BT

Rich Schroeppel
Sandia National Labs

Peter Schwabe
Eindhoven University of Technology

Nicolas Sendrier
INRIA

Adi Shamir
The Weizmann Institute

**First SHA-3 Candidate Conference
Participants List**

Kyoji Shibutani
Sony Corp.

Taizo Shirai
Sony Corp.

Vasily Shishkin
Federal Security Service

Douglas Shors
U.S. Government

Mohammad Reza Sohizadeh
abyane
University of Bergen

Vladimir Sperka
NBU

Martijn Stam
EPFL

Paul Stankovski
Lund University

Rune Steinsmo Odegard
Q2S

Richard Stong
IDA-CCR

Fatih Sulak
METU

Suneel Sundar
CCR

Cihangir Tezcan
Middle East Technical University

Saren Thomsen
Technical University of Denmark

Celine Thuillet
EADS Secure Networks

Elmar Tischhauser
K.U.Leuven, ESAT/COSIC

Elizabeth Topielec
U.S. Government

Jacob Topper
University of California

Deniz Toz
K.U.Leuven, ESAT/SCD-COSIC

Alex Troesch
UCSB

Michal Trojnara
Warsaw University of Technology

Gilles Van Assche
STMicroelectronics

Julien Van Hamme
Royal Military Academy

Dirk Van Heule
Royal Military School

Kerem Varici
K.U.Leuven Dept. ESAT/SCD-
COSIC

Natarajan Vijayarangan
Tata Consultancy Services

Nikolajs Volkovs
University of Toronto

Emmanuel Volte
University of Cergy-Pontoise and
Versailles-Saint Quentin

Cody Walker
UC Santa Barbara

Wei Wang
Shandong University

**First SHA-3 Candidate Conference
Participants List**

Dai Watanabe
HSDL, Hitachi, Ltd.

Christian Wenzel-Benner
ITK Engineering AG

David Wilson

Joel Wisdom
U.S. government

Hongjun Wu
Institute for Infocomm Research

Kan Yasuda
NTT Corp.

Hirotaaka Yoshida
Hitachi, Ltd.

Aileen Yinghui Zhang
DSO National Laboratories

Wentao Zhang
Institute of Software