The northernmost crypto workshop ever organised, **Arctic Crypt 2016,** will take place in the period of **July 17-22** in spectacular arctic surroundings under the midnight sun in ***Longyearbyen, Svalbard*** at 78° north.

CALL FOR PAPERS

Workshop format
The program will be constructed around a series of 10-12 invited tutorial talks. Among the confirmed invited speakers (as of January 2016) are Dan Bernstein, Joan Daemen, Thomas Johansson, Tanja Lange, Gregor Leander, Willi Meier, Christian Rechberger, Ron Rivest, and Adi Shamir. In addition, we solicit submissions of papers within the scope of the workshop as indicated below. We anticipate that there will be space for 20+ submitted papers.

Workshop scope
Original contributions on all technical aspects of cryptology are solicited for submission to Artic Crypt. Submissions are welcome on any cryptographic topic including, but not limited to:

- Foundational theory
- The design, proposal, and analysis of cryptographic primitives
- Crypto protocols, side-channel attacks, and other aspects of implementation
- Information theoretic approaches to digital security
- Recent trends in cryptography

Important dates

- Submission deadline: February 15, 2016
- Notification: April 1, 2016
- Workshop dates: July 17 – 22, 2016

Instructions for Authors
Submissions to Arctic Crypt should be at most 15 pages including the title page, references, and figures. Font size should be at least 11pt with reasonable margins. Submissions should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the contribution of the paper so that it is understandable to a non-expert in the field. Submissions must be presented in a way that allows the understanding and verification of the claimed results with reasonable time and effort. Submissions must be anonymous, with no author names, affiliations, or obvious references. Papers must be submitted electronically at *https://easychair.org/conferences/?conf=arcticcrypt2016* .

Pre-proceedings and special issue in CCDS
All the participants will receive an electronic copy of the pre-proceedings of the workshop containing all the accepted papers for the workshop. The authors of accepted papers will be invited to submit a full paper to appear (after a new round of reviewing) in a special issue in the journal:
Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences.

Organization
Program co-chairs: Tor Helleseth (U. Bergen), Bart Preneel (U. Leuven),
General chair: Øyvind Ytrehus (Simula@UiB and U. Bergen)

Stipends
A limited number of stipends will also be available for students presenting an accepted paper and are unable to obtain funding to attend the workshop. Application for stipends should be sent to **Tor Helleseth** (Tor.Helleseth@ii.uib.no) or **Øyvind Ytrehus** (Oyvind.Ytrehus@ii.uib.no).

See also http://arcticcrypt.b.uib.no/