1st International Workshop on Advances in Asymmetric Cryptanalysis (AAC)

Abu Dhabi, UAE, March 5-8, 2024

The 1st International Workshop on Advances in Asymmetric Cryptanalysis (AAC'24) will be held physically in Abu Dhabi, UAE, as a single-day event during ACNS, March 5-8, 2024.

The field of asymmetric cryptography has been flourishing within the last years: researchers have been proposing various public key constructions ranging from well-established signature schemes to advanced protocols like homomorphic encryption, MPC or functional encryption. Almost all of them rely on certain hardness assumptions like factoring, discrete logarithm, lattice-based or code-based assumptions or those relying on solving multivariate systems. Understanding the concrete complexity of such problems is of paramount importance, not only in cryptography, but also in complexity theory and number theory. However, looking at the current trend in the cryptographic world, it appears that there are very few venues (if any) dedicated specifically to the cryptanalytic community: to people who design and implement new algorithms and provide new insights into the asymptotic and concrete hardness of cryptographic problems.

AAC 2024 fills the current gap in the cryptographic community by providing a dedicated platform for cryptanalysts. It aims to advance the field by bringing together experts in algorithm design and implementation, facilitating knowledge exchange, and encouraging collaboration. Additionally, AAC 2024 welcomes new joiners and less experienced attendees, aiming to expand the community and provide support for individuals at all levels of expertise.

Call for contributions

AAC 2024 invites paper submissions on any aspect of asymmetric cryptanlysis. This includes (but is not limited to): new algorithms for solving cryptographic relevant problems, efficient implementations of new or existing algorithms, algorithmic improvements to the state-of-the-art, detailed cost analyses or side-channel attacks. Additionally AAC 2024 also welcomes SoK (Systematization of Knowledge) papers, for which ”SoK” should be mentioned in the title.

Submissions should be processed in LaTeX following the Springer LNCS template. The pagelimit for submissions is 18 pages *excluding* references and any clearly marked appendices. Reviewers are not required to read appendices, submissions should therefore be self-contained without it. Papers must not be already published or submitted to another venue with proceedings. To submit a paper, please visit:

`https://easychair.org/my/conference?conf=aac24`

Authors of accepted papers must ensure that one of the authors will present their work in person at the workshop.

Important dates

- Submission deadline: **29th of November 2023**
- Notification: **22nd of December 2023**

Grants and Awards

To encourage greater student participation, ACNS'24 offers travel grants for students. More details about these grants can be found on ACNS'24 Student Travel Grants website `https://wp.nyu.edu/acns2024/student-travel-grants`

In addition, ACNS'24 gives a best workshop paper award, with 500 EUR prize sponsored by Springer.

Organizing Committee

Andre Esser, Elena Kirshanova and Javier Verbel (Technology Innovation Institute)

Program Committee

Leo Ducas (CWI, Netherlands)
Luca de Feo (IBM Research, Switzerland)
Philippe Gaborit (University of Limoges, France)
Ján Jančár (Masaryk University)
Alexander Karenin (Technology Innovation Inst., UAE)
Juliane Krämer (University of Regensburg Germany)
Péter Kutas (Eötvös Loránd University, Hungary)
Alexander May (Ruhr University Bochum, Germany)
Semyon Novoselov (I. Kant Baltic Federal Univercity)
Lorenz Panny (Technical University Munich, Germany)
Eamonn Postlethwaite (CWI, Netherlands)
Markku-Juhani O. Saarinen (PQShield, UK)
Paolo Santini (Università Politecnica delle Marche, Italy)
Damien Stehlé (CryptoLab, Korea)
Jean-Pierre Tillich (Inria de Paris, France)
Monika Trimoska (Radboud University, Netherlands)
Alexander Wallet (Inria Rennes, France)
Violetta Weger (Technical University Munich, Germany)