Call for Failures!

CFail, The Conference for Failed Approaches and Insightful Losses in Cryptology, will hold its third edition this year as an affiliated event to Crypto 2021. Our goal is to share insights and build a collective experience within the cryptographic community about how and why good ideas sometimes fail, and what we can learn from those failures.

Original contributions in all fields of cryptology are sought detailing currently unsuccessful but insightful attempts to:

- Prove or disprove a conjecture;
- Design or break a cryptographic algorithm;
- Simplify a cryptographic algorithm or concept;
- Implement a cryptosystem;
- Formulate a new security definition or reduction;
- Systematize a collection of ad-hoc attacks;
- Or any other task that is part of the practice of theoretical or applied cryptology, broadly construed.

Do you have insightful and exciting work sitting in a drawer somewhere because it never quite panned out or are you willing to share the series of failed attempts you went through before reaching a successful result?

Timeline

- Submission deadline: May 1, 2021; 23:59 AoE
- Notification deadline: June 15, 2021
- Conference: August, 14, 2021

Submission page: https://easychair.org/conferences/?conf=cfail2021

Instructions to Authors

For this year's edition we solicit anonymous submissions of extended abstracts consisting of up to 3 pages in any legible format. Submissions should be uploaded to EasyChair (https://easychair.org/conferences/?conf=cfail2021) in PDF form to be judged by the Program Committee. It is up to the authors to decide how they choose to engage the reviewing readers, who are not guaranteed to read or not read beyond any particular point. Clarity of exposition, educational value, and the ability to generalize conclusions into a wider setting will be strongly taken into account.

To allow for the submission of papers published elsewhere there will be no formal proceedings. Instead, accepted abstracts will be made available online before the conference. Authors of such submissions should make sure that they are re-framed in line with CFail's goals. In addition to this and to encourage the submission of works that would normally be harder to publish elsewhere (e.g., negative results) we partnered with the Computer Journal (https://academic.oup.com/comjnl). After the conference, authors of eligible accepted abstracts will be invited to submit a full version of their work to be reviewed for potential publication in the journal.

Authors of accepted abstracts will be given a 20-30 minute slot for presenting their submission at the conference followed by a 5-10 minute Q&A. Speakers and participants will not be required to travel physically and talks will be recorded and made available subject to speaker permission.

Please contact the general chair at allibishop@gmail.com or the program chair tomer.ashur@esat.kuleuven.be with any inquiries.

Program Committee

- Gunes Acar, KU Leuven
- Tomer Ashur, TU Eindhoven and KU Leuven (Program Chair)
- Shi Bai, Florida Atlantic University
- Zhenzhen Bao, Nanyang Technological University
- Lejla Batina, Radboud University
- Allison Bishop, Proof Trading (General Chair)
- Ilaria Chillotti, Zama, France
- Chitchanok Chuengsatiansup, The University of Adelaide
- Orr Dunkelman, University of Haifa
- Maria Eichlseder, Graz University of Technology
- Carla Ràfols, Universitat Pompeu Fabra
- Jian Guo, Nanyang Technological University
- Swee-Huay Heng, Multimedia University
- Yunwen Liu, National University of Defense Technology
- Atul Luykx, Google
- Giorgia Azzurra Marson, University of Bern and NEC Laboratories Europe
- Chloe Martindale, University of Bristol
- María Naya-Plasencia, INRIA
- Claudio Orlandi, Aarhus University
- Elisabeth Oswald, University of Klagenfurt
- Kenny Paterson, ETH Zurich
- Arpita Patra, Indian Institute of Science, Bangalore
- Eyal Ronen, Tel Aviv University
- Mike Rosulek, Oregon State University
- Reihaneh Safavi-Naini, University of Calgary
- Alessandra Scafuro, NCSU
- Nigel Smart, KU Leuven
- Alan Szepieniec, Nervos Foundation
- Avishay Yanai, VMWare