Journal of Cryptographic Engineering (2024) 14:129
https://doi.org/10.1007/s13389-023-00345-x

CORRESPONDENCE

Editorial about PROOFS 2021

Fan Zhang[1]

Received: 27 November 2023 / Accepted: 29 November 2023 / Published online: 29 January 2024

The tenth International Workshop on Security Proofs for Embedded Systems (PROOFS) continues its important mission of promoting methodologies to improve confidence in the security of embedded systems containing cryptographic algorithms. As embedded devices proliferate rapidly, provable security is essential to guard against rising threats like side-channel attacks, hardware trojans, and more. PROOFS 2021 brought together leading researchers across theory and practice to push forward the state-of-the-art.

This year's workshop was originally scheduled to take place in Beijing China, on August 24, co-located with CHES 2021. However, due to the bad situation of COVID-19, this final event took place online. The technical program featured an excellent invited talk along with paper presentations and discussions.

Facing the backdrop of the growing dangers to embedded systems security, PROOFS 2021 tackles these issues by furthering provable safeguards rooted in formal techniques, evaluations, benchmarks, and more. As embedded devices quickly spread, the necessity for rigorous security guarantees has become clear.

The presentations of PROOFS addressed emerging threats to embedded systems. Prof. Sun Jun of Singapore Management University gave an invited talk on AI security. As neural networks proliferate, risks like adversarial and backdoor attacks materialize. Prof. Jun discussed challenges verifying these non-traditional systems and presented promising research into formally proving properties like backdoor absence.

The remaining portion of the program encompassed the delivery of six contributed papers, for which the authors were extended an invitation to submit revised papers for inclusion in this special issue of the *Journal of Cryptographic Engineering* focusing on PROOFS.

The organizers of the PROOFS workshop express their gratitude to the program committee for their diligent efforts in reviewing, evaluating, and providing feedback on the submissions. We would like to extend our sincere appreciation to the program committee of PROOFS 2021, comprising the following individuals:

- Ludovic Apvrille, Telecom ParisTech
- Shivam Bhasin, Temasek Labs@NTU
- Olivier Bronchain, UCL
- Lei Bu, Nanjing University
- Guo Chun, IIE, CAS
- Naofumi Homma, Tohoku University
- Cetin Koc, University of California Santa Barbara
- Quentin Meunier, Université Pierre et Marie Curie
- Debdeep Mukhopadhyay, IIT Kharagpur, India
- Changhai Ou, Nanyang Technological University
- Guilherme Perin, LIRMM
- Francesco Regazzoni, ALaRI - USI (Switzerland)
- Fu Song, ShanghaiTech University
- Gilles Van Assche, STMicroelectronics
- An Wang, Beijing Institute of Technology
- Xiaofei Xie, Kyushu University
- Yongwang Zhao, Zhejiang University

We anticipate the continued success of PROOFS workshops in enabling progress on embedded security through formal methods, evaluation, testing, and provable techniques.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

✉ Fan Zhang
fanzhang@zju.edu.cn

[1] Zhejiang University, Hangzhou, China