Proceedings of FAVPQC 2022

Santiago Escobar[1], Ayoub Otmani[2], Sedat Akleylek[3,4] and Kazuhiro Ogata[5]

[1]*Polytechnic University of Valencia, Spain*
[2]*University of Rouen Normandie, France*
[3]*Ondokuz Mayis University, Turkey*
[4]*University of Tartu, Estonia*
[5]*Japan Advanced Institute of Science and Technology, Japan*

Preface

It is known that the most popular public-key cryptosystems used today will become insecure once sufficient strong quantum computers become available. To prepare for information security in the quantum computing era, post-quantum cryptosystems that are resistant to attacks from quantum computers have been built as replacements for the classical ones. Security verification of those post-quantum cryptographic protocols has got extensive attention from cryptography and security research groups in recent years. To address the challenge, the International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022) was held. We received six regular paper submissions and accepted five regular papers for presentation at the workshop through the standard reviewing process, where each of five papers were reviewed by three experts and one paper was reviewed by two experts. This volume contains one keynote (invited) talk abstract and four among the five ones.

The workshop was held in a hybrid style in Madrid, Spain on October 24, 2022 as a satellite event of the 23rd International Conference on Formal Engineering Methods (ICFEM 2022). Four papers were presented at the venue, while the keynote talk and one paper were presented online.

Program Committee

Sedat Akleylek, Ondokuz Mayis University, Turkey & University of Tartu, Estonia (co-chair)
Christophe Chareton, LORIA-CELLO, France
Santiago Escobar, Universitat Politecnica de Valencia, Spain (co-chair)
Daniel Gaina, Kyushu University, Japan
Cetin Kaya Koc, University of California Santa Barbara, USA
Benjamin Lipp, Max Planck Institute for Security and Privacy (MPI-SP), Germany

---

FAVPQC 2022: International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols, October 24, 2022, Madrid, Spain

sescobar@upv.es (S. Escobar); ayoub.otmani@univ-rouen.fr (A. Otmani); sedat.akleylek@bil.omu.edu.tr (S. Akleylek); ogata@jaist.ac.jp (K. Ogata)

CEUR Workshop Proceedings (CEUR-WS.org)

Catherine Meadows, Naval Research Laboratory, USA
Paolo Modesti, Teesside University, UK
Masaki Nakamura, Toyama Prefectural University, Japan
Kazuhiro Ogata, Japan Advanced Institute of Science and Technology, Japan (co-chair)
Ayoub Otmani, University of Rouen Normandie, France (co-chair)
Adrian Riesco, Universidad Complutense de Madrid, Spain
Min Zhang, East China Normal University, China

Organization Committee

Sedat Akleylek, Ondokuz Mayis University, Turkey & University of Tartu, Estonia
Santiago Escobar, Polytechnic University of Valencia, Spain
Kazuhiro Ogata, Japan Advanced Institute of Science and Technology, Japan
Ayoub Otmani, University of Rouen Normandie, France

Publicity Committee

Duong Dinh Tran, Japan Advanced Institute of Science and Technology, Japan (chair)

External Reviewers

Duong Dinh Tran, Japan Advanced Institute of Science and Technology, Japan