Welcome to FAVPQC 2022!

International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022

An **ICFEM 2022** satellite workshop, Madrid, Spain, October 24, 2022

FAVPQC 2022 for the international research project

Formal Analysis and Verification of Post-quantum Cryptographic Protocols (PAVPQC)

by

Santiago Escobar, Polytechnic University of Valencia

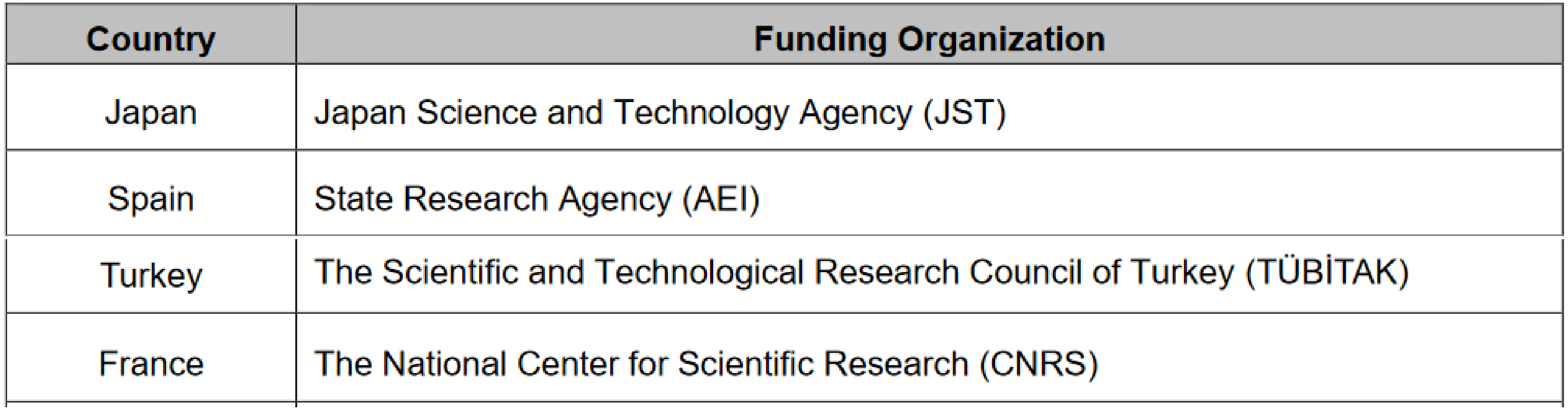
Ayoub Otmani, University of Rouen Normandie

Sedat Akleylek, Ondokuz Mayis University & University of Tartu

Kazuhiro Ogata, JAIST

FAVPQC 2022 for the international research project

Funded by the following organizations:



Country	Funding Organization
Japan	Japan Science and Technology Agency (JST)
Spain	State Research Agency (AEI)
Turkey	The Scientific and Technological Research Council of Turkey (TÜBİTAK)
France	The National Center for Scientific Research (CNRS)

in EIG CONCERT-Japan within the Framework of the Strategic International Collaborative Research Program (SICORP)

Session 1 (9:00-10:30): Formal methods for quantum computing

- 9:00-10:00: Invited talk by Yuxin Deng (ECNU). Formal Verification of Quantum Protocols
- 10:00-10:30: Tsubasa Takagi. An Algebra of Quantum Programs with the Kleene Star Operator

Coffee break (10:30-11:00)

Session 2 (11:00-13:00): Formal specification and verification of post-quantum cryptographic protocols

- 11:00-11:30: Katharina Kreuzer. Verification of the (1-δ)-Correctness Proof of CRYSTALS-KYBER with Number Theoretic Transform
- 11:30-12:00: Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek and Ayoub Otmani. Formal specification and model checking of lattice-based key encapsulation mechanisms in Maude
- 12:00-12:30: Víctor García and Santiago Escobar. Modeling and verification of the post-quantum key encapsulation mechanism KYBER using Maude
- 12:30-13:00: Duong Dinh Tran, Canh Minh Do, Santiago Escobar and Kazuhiro Ogata. Hybrid Post-Quantum TLS formal specification in Maude-NPA - toward its security analysis

We appreciate very much the big efforts made by

- All authors of the papers submitted to FAVPQC 2022
- All PC members
- All external reviewers
- Publicity chair Duong Dinh Tran
- All organizers of ICFEM 2022, especially, Adrian Riesco

A brief introduction to the keynote speaker

Yuxin Deng received the B.Eng. and M.Sc. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1999 and 2002, respectively, and the Ph.D. degree in computer science from Ecole des Mines de Paris, Paris, France, in 2005.

He is currently a Professor in the East China Normal University, Shanghai, China. His research interests include concurrency theory, especially about process calculi, and formal semantics of programming languages, as well as formal verification.

Formal Verification of Quantum Protocols