

Preliminary Agenda

NIST Workshop on Formal Methods within Certification Programs (FMCP 2024)

Tuesday, July 23, 2024	
8:15	Shuttle Departs Hilton Garden Inn Rockville-Gaithersburg
8:30 – 9:00	Arrival/Badging/Continental breakfast
Session 1 – Opening <i>Session Chair: Donghoon Chang</i>	
9:00 – 9:10	Welcome <i>Tim Hall</i>
9:10 – 9:40	Testing Techniques in the CAVP <i>Chris Celi</i>
9:40 – 10:30	Tutorial on Interactive and Automated Solvers <i>Nicky Mouha</i>
10:30 – 11:00	Coffee Break
Session 2 – Invited Talks (1) <i>Session Chair: Tim Hall</i>	
11:00 – 12:00	CMVP as a Certification Program <i>Gavin O'Brien</i>
12:00 – 1:30	Boxed Lunch
Session 3 – Submitted Talks (1) <i>Session Chair: Alex Calis</i>	
1:30 – 2:00	Formal Verification of Cryptographic Software at AWS - Current Practices and Future Trends <i>Rod Chapman, Adam Petcher, Torben Hansen, Yan Peng, Tancrède Lepoint, Cameron Bytheway, Panos Kampanakis</i>
2:00 – 2:30	Cryptographic Validation Beyond Implementation Correctness <i>Manuel Barbosa, François Dupressoir, Andreas Hülsing, Vincent Laporte, Pierre-Yves Strub</i>
2:30 – 3:00	Coffee Break
Session 4 – Panel (1) <i>Moderator: Adam Chlipala</i>	
3:00 – 4:00	Panel Discussion: The Role of Formally Verified Proofs for Cryptographic Standards and Implementations <i>Panelists: Karthik Bhargavan, Rod Chapman, Pierre-Yves Strub</i>
4:30	Shuttle Departs NCCoE to Return to Hotel

Wednesday, July 24, 2024	
8:15	Shuttle Departs Hilton Garden Inn Rockville-Gaithersburg
8:30 – 9:00	Arrival/Badging/Continental breakfast
Session 5 – Submitted Talks (2) <i>Session Chair: Adam Chlipala</i>	
9:00 – 9:30	Towards Formal Verification of the Confidential Computing Framework for RISC-V <i>Wojciech Ozga, Lennard Gäher, <u>Guerney D.H. Hunt</u>, <u>Avraham Shinnar</u>, Elaine R. Palmer, Michael V. Le, Silvio Dragone</i>
9:30 – 10:00	A Comparison-Based Methodology for the Security Assurance of Novel Systems <i>Jelizaveta Vakarjuk, <u>Peeter Laud</u></i>
10:00 – 10:30	Formal Specifications for Certifiable Cryptography <i>Manuel Barbosa, <u>Karthikeyan Bhargavan</u>, Franziskus Kiefer, Peter Schwabe, Pierre-Yves Strub, Bas Westerbaan</i>
10:30 – 11:00	Coffee Break
Session 6 – Invited Talks (3) <i>Session Chair: Nicky Mouha</i>	
11:00 – 12:00	A Baker’s Dozen: 13 Challenges Seeking New Thought Leadership in Software Engineering <i>Jeff Voas</i>
12:00 – 1:30	Boxed Lunch
Session 7 – Invited Talks (4) <i>Session Chair: Gavin O’Brien</i>	
1:30 – 2:30	The Fiat Cryptography Verified Code Generator and Experiences with Adoption <i>Adam Chlipala</i>
2:30 – 3:00	Coffee Break
Session 8 – Panel (2) <i>Moderator: Chris Celi</i>	
3:00 – 4:00	Panel Discussion: Paths to Adoption of Formal Methods for Cryptographic Implementations <i>Panelists: Adesola Adegboye, Alex Calis, Jonathan Smith, Alicia Squires</i>
4:30	Shuttle Departs NCCoE to Return to Hotel

Thursday, July 25, 2024	
8:15	Shuttle Departs Hilton Garden Inn Rockville-Gaithersburg
8:30 – 9:00	Arrival/Badging/Continental breakfast
Session 9 – Submitted Talks (3) <i>Session Chair: Chris Celi</i>	
9:00 – 9:30	AI-assisted Formal Method Verifications on Cryptographic Designs and Implementations <i>Long Ngo</i>
9:30 – 10:00	Which One to Apply: Formal Methods or Machine Learning? <i>Yi Mao</i>
10:00 – 10:30	Modernizing FIPS for Safe Languages and Verified Libraries <i>Jonathan Protzenko, Bas Spitters</i>
10:30 – 11:00	Coffee Break
Session 10 – Invited Talks (5) <i>Session Chair: Ben Livelsberger</i>	
11:00 – 12:00	A Verification-based Trustworthy Computing Platform <i>Gregory Malecha</i>
12:00 – 1:30	Boxed Lunch
Session 11 – Next Steps <i>Moderator: Chris Celi</i>	
1:30 – 2:30	Structured Discussion – Next Steps
2:30 – 3:00	Coffee Break
Session 12 – Closing <i>Moderator: Nicky Mouha</i>	
3:00 – 4:00	Open Discussion
4:30	Shuttle Departs NCCoE to Return to Hotel