# 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** *Session Chair: Donghoon Chang* | |
| 9:00 – 9:10 | Welcome<br>*Tim Hall* |
| 9:10 – 9:40 | Testing Techniques in the CAVP<br>*Chris Celi* |
| 9:40 – 10:30 | Tutorial on Interactive and Automated Solvers<br>*Nicky Mouha* |
| 10:30 – 11:00 | Coffee Break |
| **Session 2 – Invited Talks (1)** *Session Chair: Tim Hall* | |
| 11:00 – 12:00 | CMVP as a Certification Program<br>*Gavin O'Brien* |
| 12:00 – 1:30 | Boxed Lunch |
| **Session 3 – Submitted Talks (1)** *Session Chair: Alex Calis* | |
| 1:30 – 2:00 | Formal Verification of Cryptographic Software at AWS - Current Practices and Future Trends<br>*Rod Chapman, Adam Petcher, Torben Hansen, Yan Peng, Tancrède Lepoint, Cameron Bytheway, Panos Kampanakis* |
| 2:00 – 2:30 | Cryptographic Validation Beyond Implementation Correctness<br>*Manuel Barbosa, François Dupressoir, Andreas Hülsing, Vincent Laporte, Pierre-Yves Strub* |
| 2:30 – 3:00 | Coffee Break |
| **Session 4 – Panel (1)** *Moderator: Adam Chlipala* | |
| 3:00 – 4:00 | Panel Discussion: The Role of Formally Verified Proofs for Cryptographic Standards and Implementations<br>*Panelists: Karthik Bhargavan, Rod Chapman, Pierre-Yves Strub* |
| 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)** *Session Chair: Adam Chlipala* | |
| 9:00 – 9:30 | Towards Formal Verification of the Confidential Computing Framework for RISC-V<br>*Wojciech Ozga, Lennard Gäher, Guerney D.H. Hunt, Avraham Shinnar, Elaine R. Palmer, Michael V. Le, Silvio Dragone* |
| 9:30 – 10:00 | A Comparison-Based Methodology for the Security Assurance of Novel Systems<br>*Jelizaveta Vakarjuk, Peeter Laud* |
| 10:00 – 10:30 | Formal Specifications for Certifiable Cryptography<br>*Manuel Barbosa, Karthikeyan Bhargavan, Franziskus Kiefer, Peter Schwabe, Pierre-Yves Strub, Bas Westerbaan* |
| 10:30 – 11:00 | Coffee Break |
| **Session 6 – Invited Talks (3)** *Session Chair: Nicky Mouha* | |
| 11:00 – 12:00 | A Baker's Dozen: 13 Challenges Seeking New Thought Leadership in Software Engineering<br>*Jeff Voas* |
| 12:00 – 1:30 | Boxed Lunch |
| **Session 7 – Invited Talks (4)** *Session Chair: Gavin O'Brien* | |
| 1:30 – 2:30 | A Verification-based Trustworthy Computing Platform<br>*Gregory Malecha* |
| 2:30 – 3:00 | Coffee Break |
| **Session 8 – Panel (2)** *Moderator: Chris Celi* | |
| 3:00 – 4:00 | Panel Discussion: Paths to Adoption of Formal Methods for Cryptographic Implementations<br>*Panelists: Alex Calis, Alicia Squires, TBD* |
| 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)** *Session Chair: Chris Celi* | |
| 9:00 – 9:30 | AI-assisted Formal Method Verifications on Cryptographic Designs and Implementations<br>*Long Ngo* |
| 9:30 – 10:00 | Which One to Apply: Formal Methods or Machine Learning?<br>*Yi Mao* |
| 10:00 – 10:30 | Modernizing FIPS for Safe Languages and Verified Libraries<br>*Jonathan Protzenko, Bas Spitters* |
| 10:30 – 11:00 | Coffee Break |
| **Session 10 – Invited Talks (5)** *Session Chair: Ben Livelsberger* | |
| 11:00 – 12:00 | The Fiat Cryptography Verified Code Generator and Experiences with Adoption<br>*Adam Chlipala* |
| 12:00 – 1:30 | Boxed Lunch |
| **Session 11 – Next Steps** *Moderator: Chris Celi* | |
| 1:30 – 2:30 | Structured Discussion – Next Steps |
| 2:30 – 3:00 | Coffee Break |
| **Session 12 – Closing** *Moderator: Nicky Mouha* | |
| 3:00 – 4:00 | Open Discussion |
| 4:30 | Shuttle Departs NCCoE to Return to Hotel |