October 7, 2025

HACS 2026 Overview

Sofía Celi, Deirdre Connolly, François Dupressoir,
Allen Gunn, Trevor Perrin, Cathie Yun

Introduction

Since 2016, the workshop on High Assurance Cryptographic Software has been bringing together cryptographic developers, cryptographers, and formal verification experts to improve the quality of cryptographic software. HACS has helped forge connections between these communities, leading to many new research projects, collaborations, and tool deployments (see https://hacs-workshop.org).

To foster small-group dynamics and community feeling, HACS is a small workshop: we aim for <100 attendees. The organizers select new focus topics each year and adjust the attendee mix to match, trying to strike a balance between evolution and continuity.

For HACS 2026 we will emphasize continuity: the 2025 event focused on ZK; proof assistants; and tool usability via an effort to define “ladders” of problems and solutions. We believe these activities were fruitful enough to continue for another year. We will additionally explore applications of machine learning and AI to formal verification and software assurance. In more detail, HACS 2026 will have the following focus topics:

- **Zero-Knowledge Proofs**. We’ll focus on correct and secure implementation of ZK circuits, compilers, and libraries; as well as security proofs for complex ZK systems, with an emphasis on reusable frameworks such as ZKVMs.

- **Proof Assistants** (EasyCrypt, Lean, F*, Isabelle, Rocq, etc.). We’ll focus on this class of tools for program verification, as well as creating and checking security proofs. We’ll continue and extend our outreach to the Lean community, which has been particularly active this year

- **Problem ladders for exploration of tool usability.** We will focus on identifying simple, self-contained **challenge problems** that can be arranged into illustrative pedagogical “ladders”. From there, we'll try to spur the development of **tutorials** showing how to tackle these problems with different tools. We’ll build on last year’s “proofs ladder” effort as well as try to spur similar efforts, e.g. for program verification.

- **Machine Learning and AI.** We will explore the use of ML/AI tools in combination with formal methods tools: where is this combination helpful, and what can we expect in the coming years? Where do these tools fall down, or mislead? We’ll also consider the broader assurance challenges created as AI is increasingly used to create software and proofs.

Of course, HACS will continue to focus on its core theme of correctness and security of crypto code, including formal generation and verification of code; as well as informal assurance practices. We'll cover other areas of cryptography (including PQC migration and signatures, anonymous credentials, MPC, FHE, PIR, threshold crypto, protocol design, web PKI, etc.) wherever we think our format and attendee mix can provide value.

The Plan for HACS 2026

HACS 2026 will be a three-day physical event in Taipei, Taiwan, with the main workshop days on March 6-7, and an optional hack day on March 8. This will be the Friday through Saturday prior to the Real World Crypto 2026 conference, which is scheduled for March 9–11, 2026 in Taipei. The event will be co-organized and facilitated by Allen Gunn of Aspiration.

As always, HACS will be a highly interactive event, where crypto implementers, researchers, and experts in high-assurance and formal methods have lots of time to meet, learn from each other, and launch collaborations.

To that end, we will avoid lectures delivered to the entire group. Instead, we hope to spend most time in small-group "working sessions", focused on interactive discussion and collaboration. Some of these working sessions will be planned in advance, but others will emerge based on attendee interest, during the event.

The organizers will spend significant time before the event discussing goals with attendees and arranging workshop sessions to advance concrete objectives.

HACS 2026 Organizers

Sofía Celi, Deirdre Connolly, François Dupressoir,
Allen Gunn, Trevor Perrin, Cathie Yun

HACS General Committee

Gilles Barthe, Karthik Bhargavan, Sofía Celi, Deirdre Connolly,
François Dupressoir, Allen Gunn, Diane Hosfelt, Ben Laurie,
Trevor Perrin, Peter Schwabe, Cathie Yun