ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

Invitation to the Doctoral Seminar

Prof. Chitchanok Chuengsatiansup
University of Klagenfurt

"CryptOpt: Verified Compilation with Randomized Program Search for Cryptographic Primitives"

N.2.35 | Wednesday, 12 March 2025 | 10:00 a.m.

Abstract

Cryptography has been extensively used to protect digital information on a wide range of devices. Therefore, the correctness, efficiency, and portability of cryptographic software are of utmost importance. While relying on a compiler-based code generation achieves portability, the efficiency of the produced code usually underperforms compared to the code written directly in assembly. On the other hand, writing code manually achieves high performance while costing experts' time, particularly when the target platform has changed. Regardless, either approach may still produce incorrect code. This talk presents CryptOpt, a verified compilation code generator that produces efficient code tailored to the architecture it runs on. On the optimization side, CryptOpt applies randomized search through the space of assembly program. On the formal-verification side, CryptOpt connects to the Fiat Cryptography framework and extends it with a new formally verified program-equivalence checker. The benchmark shows that CryptOpt produces fastest-known implementations of finite-field arithmetic for both

Curve25519 and the Bitcoin elliptic curve secp256k1 for the relatively new Intel 12th and 13th generations.

Clemens Heuberger and the Department of Mathematics look forward to seeing you at the talk!