ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

INVITATION TO THE DOCTORAL SEMINAR

CryptOpt: Verified Compilation with Randomized Program Search for Cryptographic Primitives

Chitchanok Chuengsatiansup | University of Klagenfurt

Chaired by Clemens Heuberger | Department of Mathematics

Wednesday, 12 March 2025 | 10:00–11:00

N.2.35

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 imple-

mentations of finite-field arithmetic for both Curve25519 and the Bitcoin elliptic curve secp256k1 for the relatively new Intel 12th and 13th generations.

We hope to see you there!

