High-Speed and Correct Implementations in Cryptography
-- on generating formally-verifiable speed-critical code

Bo-Yin Yang

Institute of Information Science,
Academia Sinica
Taipei, Taiwan

Abstract:

We discuss high-speed cryptographic software and their formal verification. We consider speed-record setting, hand-optimized assembly software on the Curve25519 Elliptic curve, specifically the key exchange protocol presented by Bernstein et al. at CHES 2011. Two versions for different microarchitectures are available. We successfully verify the core part of the computation, and reproduce detection of a bug in a previously published edition. An SMT solver supporting array and bit-vector theories is used to establish almost all properties. Remaining properties are verified in a proof assistant with simple rewrite tactics. We also exploit the compositionality of Hoare logic to address the scalability issue. Essential differences between both versions of the software are discussed from a formal-verification perspective.