Title: HACL*, a verified C library for modern cryptography

Authors: Jean-Karim ZINZINDOHOUE (INRIA Paris), Karthikeyan BHARGAVAN (INRIA Paris), Jonathan PROTZENKO (Microsoft Research), Benjamin BEURDOUCHE (INRIA Paris)

Abstract: We present HACL*, *a new verified cryptographic library, written and verified in F** and compiled to C. Our verification and compilation scheme guarantees that the compiled C code is memory-safe, functionally equivalent to runnable RFC-like specifications and resistant to some classes of side-channel attacks. The generated C code can be compiled with CompCert so that the F* security properties are propagated all the way down to assembly.

Our library can be used in two ways. One is as a standalone, fast and portable C library that can be included in existing applications. The other is to provide high-level cryptographic APIs for larger F* *projects such as miTLS, a reference TLS implementation. HACL** implements the NaCl API, which includes the Salsa stream-cipher family, the SHA2 hash family, the X25519 ECDH primitive, the Poly1305 hash function and the Ed25519 EDDSA signature scheme. These modern primitives are also sufficient to provide a full ciphersuite for TLS 1.3.

Our results show that it is now feasible to verify full-fledged cryptographic libraries in C without incurring any performance cost.