Cryptology ePrint Archive: Report 2011/679

CTL: A Platform-Independent Crypto Tools Library Based on Dataflow Programming Paradigm

Junaid Jameel Ahmad and Shujun Li and Ahmad-Reza Sadeghi and Thomas Schneider

Abstract: The diversity of computing platforms is increasing rapidly. In order to allow security applications to run on such diverse platforms, implementing and optimizing the same cryptographic primitives for multiple target platforms and heterogeneous systems can result in high costs. In this paper, we report our efforts in developing and benchmarking a platform-independent Crypto Tools Library (CTL). CTL is based on a dataflow programming framework called Reconfigurable Video Coding (RVC), which was recently standardized by ISO/IEC for building complicated reconfigurable video codecs. CTL benefits from various properties of the RVC framework including tools to 1) simulate the platform-independent designs, 2) automatically generate implementations in different target programming languages (e.g., C/C++, Java, LLVM, and Verilog/VHDL) for deployment on different platforms as software and/or hardware modules, and 3) design space exploitation such as automatic parallelization for multi- and many-core systems. We benchmarked the performance of the SHA-256 and AES implementations in CTL on single-core target platforms and demonstrated that implementations automatically generated from platform-independent RVC applications can achieve a run-time performance comparable to reference implementations manually written in C and Java. For a quad-core target platform, we benchmarked a 4-adic hash tree application based on SHA-256 that achieves a performance gain of up to 300% for hashing messages of size 8 MB.

Category / Keywords: Crypto Tools Library (CTL), Reconfigurable Video Coding (RVC), dataflow programming, reconfigurability, platform independence, multi-core.

Publication Info: This is the extended edition of a full-length paper accepted to 16th International Conference on Financial Crypto\-graphy and Data Security (FC 2012), whose proceedings is to be published as a volume of Lecture Notes in Computer Science (LNCS) by Springer in 2012. The copyright of the published edition is held by the International Financial Cryptography Association (IFCA).

Date: received 15 Dec 2011, last revised 21 May 2012

Contact author: Junaid Ahmad at uni-konstanz de