Abstract Submitted
for the MAR12 Meeting of
The American Physical Society

Implementation of cryptographic hash function SHA256 in C++

AKASH SHRIVASTAVA, Manipal Institute of Technology, Udipi, Karnataka, India

— This abstract explains the implementation of SHA Secure hash algorithm 256 using C++. The SHA-2 is a strong hashing algorithm used in almost all kinds of security applications. The algorithm consists of 2 phases: Preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into m-bits blocks, and setting initialization values to be used in the hash computation. It generates a message schedule from padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the computation is used to determine the message digest. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits. The algorithm outputs a 256 bits message block with an internal state block of 256 bits and initial block size of 512 bits. Maximum message length in bit is generated is 2^{64}-1, over all computed over a series of 64 rounds consisting or several operations such as and, or, Xor, Shr, Rot. The code will provide clear understanding of the hash algorithm and generates hash values to retrieve message digest.

Keshav Shrivastava
University of Hyderabad

Date submitted: 10 Nov 2011

Electronic form version 1.4