Cryptology ePrint Archive: Report 2011/116

Short-output universal hash functions and their use in fast and secure message authentication

Long Hoang Nguyen and Andrew William Roscoe

Abstract: Message authentication codes usually require the underlining universal hash functions to have a long output so that the probability of successfully forging messages is low enough for cryptographic purposes. To take advantage of fast operation on word-size parameters in modern processors, long-output universal hashing schemes can be securely constructed by concatenating several instances of short-output primitives. In this paper, we describe a new method for short-output universal hash function termed digest() suitable for very fast software implementation and applicable to secure message authentication. The method possesses a higher level of security relative to other well-studied short-output universal hashing schemes. Suppose that the universal hash output is fixed at one word of b bits, then the collision probability of ours is 2^{1-b} compared to 6 * 2^{-b} of MMH, whereas 2^{-b/2} of NH within UMAC is far away from optimality. In addition to message authentication codes, we show how short-output universal hashing is applicable to manual authentication protocols where universal hash keys are used in a very different and interesting way.

Category / Keywords: universal hash function

Publication Info: To appear in the 19th Proceedings of the International Workshop on Fast Software Encryption FSE 2012, Washington DC

Date: received 8 Mar 2011, last revised 28 Feb 2012

Contact author: Long Nguyen at cs ox ac uk