Abstract

Message Integrity and authenticity are the primary aim with the ever increasing network protocols' speed. Cryptographic Hash Functions are main building block of message integrity. Many types of hash functions are being used and developed. In this paper, we propose and describe a new keyed hash function. This newly designed function produces a hash code of 128 bits for an arbitrary length input. The function also uses a key during hashing, so any intruder that does not know key, cannot forge the hash code, and, thus it fulfills the purpose of security, authentication and integrity for a message in network. The paper discusses the algorithm for the function design, its security aspects and implementation details.

References

Design and Analysis of a New Hash Algorithm with Key Integration

- Endreeva E, Preneel B. A Three-Property-Secure Hash Function. SAC'09, LNCS Springer-Verlag 2009; 5381: 228-244.
- Public-Key Cryptography Standards (PKCS): PKCS #7: Cryptographic Message Syntax Standard: 3. 6 Other Cryptographic Techniques: 3. 6. 6 What are MD2, MD4, and MD5?. RSA Laboratories. Retrieved 2012-10-03.
- Hirose S, Park JH, Yun A. A Simple Variant of the Merkle-Damgard Scheme with a Permutation. Asiacrypt'08, LNCS Springer-Verlag 2008; 4833: 113-129.
- Tirtea R. Cryptographic hash functions, trends and challenges. Journal of Computer

**Index Terms**

Computer Science  
Algorithms

**Keywords**

Authentication  Integrity  Key  MAC  MD5  Security.