Abstract

Researchers have found many flaws in hash function such as MD5 algorithm. It has been one of the most widely used hash algorithm and it has been indicated that there is a security threat in the algorithm. Furthermore, a MD5 hash output may not offer sufficient protection in the near future. So in this paper, to provide higher security protection for MD5 and MD5-512 bit algorithm unified architecture is developed to make stronger algorithm. These two algorithm structures are quite similar but different in speed and security level. It follows that they can be merged together to give new design that can perform two hash function. Thus a incorporated design allows applications to switch from one algorithm to another based on different necessities. MD5-512 design accepts the same input format as that of MD5.

References

Architecture based on MD5 and MD5-512 Bit Applications


Index Terms

Computer Science
Circuits And Systems

Keywords

MD5  Hash Function  MD5-512