Some observations on the cryptographic hash functions

Lavinia Ciungu of Mathematics, Polytechnical Univeristy, Bucharest, Romania

Abstract.In this paper we will make a discussion on the conditionswhen a strongly collision-free hash function is also one-wayhash function and also some considerations about the security ofChaum-van Pfitzmann hash function, namely it is analyzed thepossibility of birthday to this function.

1 Introduction

Hash functions are very important in cryptography where their main role is in the provision of message integrity checks anddigital signatures.Because the encryption and digital signature algorithms aregenerally slowly for the large messages, it is faster to apply a hash function to the message and then the cryptogtaphic algorithm to the message's hash value which is smaller comparedto the message itself.Many studies are dedicated to the security of hash functionstaking in consideration the properties of these functions,but there are still not definitively decided the conditionswhen the cryptographic hash function is considerated secure.In Introduction we remember some elements of Number Theory,the definition of cryptographic hash function and the principle of birthday attack.In Section 2 we discuss some properties of hash functionand in Section 3 we make some considerations regarding the security of Chaum-van Heijt-Pfitzmann hash function.