International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 7 No. II (March, 2013), pp. 79-98

ALTERNATE FORM OF TILLICH - ZEMOR HASH FUNCTION WHICH RESISTS SECOND PREIMAGE

K. T. JOJU[1] AND P. L. LILLY[2]

[1] Department of Mathematics,
Prajyoti Niketan College,
Pudukad, Kerala, India,
[2] Department of Mathematics,
St. Joseph's College,
Irinjalakuda, Kerala, India

Abstract

At CRYPTO, 94 Tillich and Zemor proposed a family of hash functions based on computing a suitable matrix product in groups of the form $SL_2(F_2n)$. But Markus Grassl, Ivana Illich, Spyros Magliveras and Rainer Steinwadt found collision for the same between palindrome bit strings of length $2n+2$. Christophe Petit, Jean-Jaques Quisquater found the second preimage and preimage for the same. We construct an alternate form of Tillich-Zemor hash function namely keyed hash function by using the same generators of Tillich-Zemor hash function, which resists the second preimage.

Key Words : *Collision, Group, Hash function, Irreducible polynomial, Preimage, Second preimage.*