IndoMS Journal on Industrial and Applied Mathematics
Volume. **1**, Issue. 1 (2014), pp. 9-16

MODIFICATION OF LUBOTZKY–PHILLIPS–SARNAK HASH FUNCTION

SUSILA WINDARTA, PETER JOHN, KIKI ARIYANTI SUGENG*

Abstract. Data security is important aspect in information security. Cryptographic hash function can be used to obtain data integrity. Collision resistant is one of important properties of a hash function. Hash function f is called to satisfied the collision resistant if given a hash value $f(m)$ then it will difficult to find other value m' from domain of f which has a hash value $f(m')$, where $f(m') = f(m)$ and $m \neq m'$. In 2008, Tillich-Zemor proved that the hash function of LPS expander graph constructed by Charles–Goren–Lauter does not satisfies collision resistant. To avoid that, as Tilich and Zemor suggestion, the improvement done by transforming the generator set S_p of hash function to be generator setS_p^2. This paper gives mathematically verification that the Tillich–Zemor Theorem cannot be applied in the transformation of the hash function constructed by generator set S_p^2. Moreover, the implementation of the modification of hash function and also its properties are also given.

Key words. *hash function, expander graph, LPS hash, collision resistant*

Abstrak. Kerahasiaan data merupakan aspek penting dalam kerahasiaan informasi. Fungsi hash kriptografi dapat digunakan untuk integritas data. Ketahanan tumbukan merupakan salah satu sifat penting dari suatu fungsi hash. Suatu fungsi hash f disebut memenuhi sifat ketahan tumbukan jika diberikan suatu nilai hash $f(m)$ maka akan sulit untuk mencari nilai m' dari domain f yang mempunyai nilai hash $f(m')$, dimana $f(m') = f(m)$ dan $m \neq m'$. Di tahun 2008, Tillich–Zemor membuktikan bahwa fungsi hash dari graf ekspander LPS yang dikonstruksi oleh Charles–Goren–Lauter tidak memenuhi sifat ketahanan tumbukan. Untuk mengatasi kekurangan sifat ini maka dilakukan perbaikan, seperti yang disarankan Tillich dan Zemor, dengan melakukan transformasi himpunan generator S_p dari fungsi hash menjadi himpunan generator S_p^2. Pada makalah ini diberikan verifikasi matematis bahwa teorema Tillich–Zemor tidak dapat digunakan untuk himpunan generator S_p^2. Lebih lanjut, implementasi dari modifikasi serta sifat-sifat setelah modifikasi juga diberikan.

Kata kunci. *fungsi hash, graf ekspander, hash LPS, ketahanan tumbukan*