

Pengaruh transformasi himpunan pembangkit pada fungsi hash dari graf ekspander Lubotzky-Phillips-Sarnak = The influence of transformation of generator set in Hash function from Lubotzky-Phillips-Sarnak expander graph

Peter John, examiner

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20312923&lokasi=lokal>

Abstrak

ABSTRAK

Ketahanan tumbukan adalah salah satu sifat penting dari suatu fungsi hash. Suatu fungsi hash f dikatakan mempunyai sifat ketahanan tumbukan jika diberikan suatu nilai hash $f(m)$ maka sulit menemukan suatu anggota domain m' yang mempunyai nilai hash $f(m')$, dengan $f(m') = f(m)$ tetapi $m' \neq m$. Pada tahun 2008, Tillich-Zemor membuktikan bahwa fungsi hash yang dibangun dari graf ekspander LPS yang dikonstruksi oleh Charles-Goren-Lauter (2007) tidak memenuhi sifat ketahanan tumbukan. Untuk menghindari hal tersebut dilakukan perbaikan dengan melakukan transformasi himpunan pembangkit sp dari fungsi hash menjadi himpunan pembangkit $SP 2$. Pada tesis ini dilakukan pembuktian secara matematis bahwa Teorema Tillich-Zemor tidak dapat digunakan pada hasil transformasi fungsi hash yang dibangun dengan himpunan pembangkit $sp 2$.

ABSTRACT

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 another m' from domain off 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 (2007) does not satisfies collision resistant. To avoid that, the improvement done by transforming the generator set SP of hash function to be generator set $SP 2$. This thesis is done a mathematically prove that the Tillich-Zemor Theorem cannot be applied in the transformation of the hash function constructed by generator set $5/$.