Fungsi hash kriptografis dari graf ekspander Lubotzky Phillips Sarnak = Cryptographic hash function from Lubotzky Philips Sarnak expander graph

Susila Windarta, author

Abstrak

ABSTRAK
Salah satu aspek pengamanan informasi yang diberikan oleh kriptografi adalah layanan keutuhan data (data integrity). Layanan keutuhan data salah satunya dipenuhi oleh fungsi hash kriptografis. Saat ini banyak fungsi hash yang dikonstruksi berdasarkan konstruksi Merkle-Damgård, di antaranya keluarga Secure Hash Algorithm (SHA). Serangan yang berhasil dilakukan oleh Wang dkk. (2005) terhadap sifat collision resistant pada SHA1 menuntut adanya konstruksi fungsi hash yang baru. Pada tahun 2007, Charles dkk. mengusulkan konstruksi fungsi hash yang berdasarkan graf ekspander. Salah satu graf ekspander yang diusulkan adalah graf ekspander Lubotzky Phillips Sarnak (LPS).
Konstruksi, aspek keamanan, serangan serta modifikasi terhadap fungsi hash tersebut dibahas pada tesis ini. Serangan tersebut berdasar pada Tillich dan Zemor (2008) yang berhasil menemukan tumbukan (collision) secara efisien. Modifikasi dilakukan dengan mengganti setiap elemen pada himpunan generator graf dengan kuadratnya. Modifikasi tersebut mengakibatkan serangan untuk menentukan tumbukan yang berdasar Tillich dan Zemor (2008) lebih sulit untuk dilakukan.
<hr>
Abstract
One aspect of information security that given by cryptography is data integrity. Cryptographic hash function can be used to obtain data integrity. Today many hash functions are constructed based on the Merkle-Damgård construction, including family of Secure Hash Algorithm (SHA). The consequence of successful attack carried out by Wang et al. (2005) on collision-resistant properties of SHA1 is the need of new construction for hash function. In 2007, Charles et al. proposed construction of hash functions based on expander graphs. In the proposal, one of expander graph used is Lubotzky Phillips Sarnak (LPS) expander graph.
The construction of hash function based on LPS expander graph, its security aspects, an attack and modification on the hash function are discussed in this thesis. The attack is based on Tillich and Zemor (2008) who managed to find a collision efficiently. Modification is done by replacing each element in graph generator set with the square of the element, hence collision attack based on Tillich and Zemor (2008) is more difficult to do.