Cryptanalysis on Hash Functions Based on Ramanujan Graphs

趙, 亨騄

https://doi.org/10.15017/1806832

出版情報：九州大学, 2016, 博士（数理学）, 課程博士
バージョン：
権利関係：全文ファイル公表済

（様式３）

氏　　名　：趙 亭ロク

論 文 名　：Cryptanalysis on Hash Functions Based on Ramanujan Graphs
（ラマヌジャングラフを用いたハッシュ関数の暗号解析）

区　　分　：甲

論文内容の要旨

Hash function is a fundamental tool in cryptography. In December 15th, 2016, The National Institute of Standards and Technology (NIST) announced that they accept submissions for post-quantum candidate algorithms. NIST asked cryptographists to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. According to their report on post-quantum cryptography, for hash functions against impact from large-scale quantum computer, it needs larger output.

LPS hash functions, which are constructed as a random walk based on the optimal expander graphs of Lubotzky, Phillips and Sarnak, were proposed by Charles, Goren and Lauter at *Journal of Cryptology* in 2009. Finding collisions of Cayley hash functions is finding cycles in their based graphs. It implies that finding a non-trivial factorization of the identity in relation to some particular elements of a projective group of matrices. Tillich and Zèmor exhibited an algorithm for finding collisions of LPS hash functions that runs in time quasi-linear n, where n is the hashcode size.

Cayley hash functions are a family of cryptographic hash functions constructed from Cayley graphs, with appealing properties such as a natural parallelism and a security reduction to a clean, well-defined mathematical problem. As this problem involves non-Abelian groups, it is a priori resistant to quantum period finding algorithms and Cayley hash functions may therefore be a good foundation for post-quantum cryptography. Four particular parameter sets for Cayley hash functions have been proposed in the past, and so far dedicated preimage algorithms have been found for all of them. These algorithms do however not seem to extend to generic parameters, and as a result it is still an open problem to determine the security of Cayley hash functions in general.

This thesis studies the different algebraic way to construct the Cayley graphs of Lubotzky et al., corresponding to Chiu's cubic Ramanujan graphs. We design a polynomial time preimage attack against the resulting Cayley hash function based on Chiu's cubic Ramanujan graphs, showing that these particular parameters like the previous ones are not suitable for the construction. We extend our attacks on hash functions based on similar Cayley graphs as Chiu's cubic Ramanujan graphs. On the positive side, we then suggest some possible ways to construct the Cayley hashes that may not be affected by this type of attacks. Our results contribute to a better understanding of the hard problems underlying the security of Cayley hash functions.