Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Cryptographic hash functions based on Triplet and Sextet graphs

Hyungrok Jo * Shohei Satake †

Keywords: hash function, graph theory, group word problem

Abstract

A hash function is one of most important concepts as a primitive in cryptography. Especially, many attempts to close to idealistic hash functions based on sophisticated mathematical backgrounds are encouraging in these days. One of the most successful suggestions for cryptographic hash functions is a hash function based on expander graphs which are proposed by Charles et al. [3] in 2006 (see also [7]). It became the key ingredient of constructing one of main Isogeny-based cryptography such as SIDH (Supersingular Isogeny Diffie-Hellman) key exchange.

In this talk we provide cryptographic hash functions based on triplet and sextet graphs which are cubic high-girth graphs. Triple and sextet graphs are introduced by Biggs [1] and Biggs & Hoare [2] in 1983, respectively. Since both of graphs can be generated from 2 by 2 matrix over a finite field, we follow up the way to construct hash functions by Zémor [8] and Charles et al. [3].

Triplet and sextet graphs are good candidates of underlying graphs of hash functions because of the following reasons. First these graphs have *large girth*, where the girth of a graph G is the length of the shortest cycles in G. High girth implies the *collision resistance* of the corresponding hash function. It was proved in [1, 5] that a triplet graph with n vertices has girth $\Omega(\log_2 n)$ $(n \to \infty)$. For sextet graphs, it was conjectured in [2] that the girth of a sextet graph with n vertices would be $\Omega(\log_2 n)$ $(n \to \infty)$, and numerical results on small sextet graphs support this conjecture ([2]).

Next triplet and sextet graphs have an *expansion property*, which intuitively means that every vertex-subset (of appropriate size) has large neighbour. This fact affects to the property of the corresponding hash function as *preimage resistance* ([4]). Here for a graph G with vertex set V and a subset $X \subset V$, the neighbour $N_G(X)$ of X is the set of vertices in $V \setminus X$ adjacent to some vertex $x \in X$. It was proved in [6] that if a cubic graph G with n vertices has girth at least $c \log_2 n$, then there exists a constant $\varepsilon > 0$ such that for any subset $X \subset V$ with $|X| = O(n^\alpha)$ $(n \to \infty)$ and a constant $\alpha < (c \log_2 3)/4$ we have $|N_G(X)| > \varepsilon |X|$. This fact implies an expansion property of triplet and sextet graphs.

References

[1] N. L. Biggs, "Graphs with large girth," *Ars Combin.*, vol. 25-C, pp. 73–80, 1988.

[2] N. L. Biggs and M. L. Hoare, "The sextet construction for cubic graphs," *Combinatorica*, vol. 3, no. 2, pp. 153–165, 1983.

[3] D. X. Charles, K. E. Lauter and E. Z. Goren, "Cryptographic hash functions from expander graphs," *J. Cryptol.*, vol. 22, no. 1, pp. 93-113, 2009.

[4] O. Goldreich, "Candidate one-way functions based on expander graphs," *Lecture Notes in Comput. Sci.*, vol. 6650, pp. 76–87, 2011.

[5] M. Hoare, "Triplets and hexagons," *Graphs and Combin.*, vol. 9, no. 2–4, pp. 225-233, 1993.

[6] N. Kahale, *Expander Graphs*, Ph.D thesis, Massachusetts Institute of Technology, 1993.

[7] C. Petit, *Cryptographic Hash Functions from Expander Graphs*, Ph.D thesis, Université catholique de Louvain, 2009.

[8] G. Zémor, "Hash functions and graphs with large girths," *In Workshop on the Theory and Application of of Cryptographic Techniques.* Springer, Berlin, Heidelberg., pp. 508-511, 1991.

* Yokohama National University, Institute of Advanced Sciences,79-5 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa (jo-hyungrok-xz@ynu.ac.jp)

† Faculty of Advanced Science and Technology, Kumamoto University, 2-39-1, Kurokami, Chuo, Kumamoto, 860-8555, Japan (shohei-satake@kumamoto-u.ac.jp)