On expanding graphs of large girth and new families of message authentication codes

O. S. Pustovit[1],

[1] Institut of telecommunications and global information space, Kyiv, Ukraine

pustovitoleksandr0709@gmail.com, vasylustimenko@yahoo.pl

The construction of families of regular expanding graphs is a well-known problem in Spectral Graph Theory. Researchers are looking for families of connected q-regular graphs G_i with the sequence of second largest eigenvalues λ_i bounded away from q.

The design of families of q-regular graphs with large girth of order v_i, where the length of the minimal cycle g is grows proportionally to $log_{q-1}(v_i)$, is an important problem in extremal graph theory.

Only a few families of graphs with large girth that are also expanding graphs are well-known. For applications, families with arbitrarily large degree turn out to be very useful. Specialists in informatics have selected the following 3 families for use in Computer Science: Cayley Ramanujan graphs constructed by G. Margulis [1] and investigated Lubotzky, Philips and Sarnak (see [2]) , Pizer's Ramanujan graphs of Cayley type [3] and graphs $CD(n, q)$ defined by F.Lazebnik, V. Ustimenko and A. Woldar [4]. The first historical application of these families was in the constructions of Low-Density Parity-Check codes for satellite communications. Studies of the properties of these codes demonstrate that graphs $CD(n, q)$ offer advantages compared to the aforementioned Ramanujan graphs [5].

Other applications is about the usage of these graphs in the construction of stream ciphers. Ciphers based on graphs $CD(n, q)$ has advantage because they have essential resistance to adversarial attacks with the knowledge of some plaintexts together with the corresponding ciphertext (see [10] and further references).

In our talk we discuss the applications of expanding graphs in the construction of Message Authentication Codes (MACs), comparing the usage of Cayley Ramanujan graphs and Pizer's graphs [6], [7] with applications of $CD(n, q)$ graphs [8], [9]. Finally we present a new family of MACs based on $CD(n, q)$ graphs and their generalizations proposed in [10]. We discuss the advantages of the new algorithm compared to the previously previously known ones.

The need for further research into cryptographically stable MACs, i.e. key dependent hash functions - is caused by cybersecurity challenges, the expansion of the global information space, expectations of quantum computers appearance and the development of blockchain technologies, which require the hashing of data of arbitrary size with its transformation into sequences of bits which form digests of the so-called blockchains. The proposed algorithms, which are sensitive to document modifications, will be used for cyberattack detection and auditing of all files after an intrusion has been detected. The proposed algorithms can process data in the form of text, audio and video files, files with various extensions such as $.avi$, $.tif$, $.pdf$, etc. The algorithms can generate digests of already encrypted files, enabling integrity checks without description. The proposed digest generation methods have a stream-based nature, the speed for constant m is linearly dependent on variable n. The growth of n increases the cryptographic stability.

1. Margulis G., Explicit constructions of graphs without short cycles and low density codes. Combinatorica, 1982, V. 2, 71 – 78.
2. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. Combinatorica, 1988, V. 8,261 – 277.
3. Pizer A. K., Ramanujan Graphs and Hecke Operators. Bulletin of the AMS, 1990, V. 23, No.1.

4. Lazebnik F., Ustimenko V., Woldar A., A New Series of Dense Graphs of High Girth. Bulletin of the AMS, 1995, V. 32, No.1. 73 – 79.
5. MacKay D., Postol M. , Weakness of Margulis and Ramanujan Margulis Low Dencity Parity Check Codes. Electronic Notes in Theoretical Computer Science, 2003, V. 74.
6. Denis X. Charles, Eyal Z. Goren, Kristin E. Lauter., Cryptographic hash functions from expander graphs. Journal of Cryptology, 2009, V. 22, 93 – 113.
7. Tomkins H, M. Nevins M, Salmasian H. New Zemor-Tillich type hash functions over GL2(F). J. Math. Cryptol.,2020, V. 32, No.1. 236 – 253.
8. Ustimenko V, Pustovit O., On New Stream Algorithms for Generation of Documents Dijests with High Avalanche Effect, 2019, Mathematical and computer modelling, Series Physics and Mathematics, 2019, V. 19, 131 – 135.
9. Polak M, Zhupa E., Keyed hash function from large girth expander graphs, Albanian J. Math., 2022, V. 16, No 1 25 – 39.
10. Chojecki T, Erskine G, J. Tuite J, Ustimenko V,On affine forestry over integral domains and families of deep Jordan Gauss graphs. European Journal of Mathematics, 2025, V. 11, No 10.