The explicit construction of a new family of expander graphs of large girth and their cryptographic applications.

Urszula Romańczuk, Vasyl Ustymenko
Maria Curie-Skłodowska University in Lublin (Poland)

urszula_romanczuk@yahoo.pl, vasyl@hektor.umcs.lublin.pl

It is known that random graphs of large girth with good expansion property can be constructed. The explicite constructions of families of graphs of large girth or families of expander graphs of bounded degree can be counted as pseudorandom graphs. Known families of such graphs are edge transitive (special Cayley graphs $X(p,q)$ for $PSL_2(q)$ [2], [4]) or graphs $CD(n,q)$ [3]. The family $X(p,q)$ is a family of Ramanujan graphs. The family $CD(n,q)$ is a family of almost Ramanujan graphs. It is known that if $n \geq 5$ these graphs are not Ramanujan despite the projective limit $CD(q)$ of $CD(n,q)$ is a q-regular tree. The reason is that the eigenspace of $CD(q)$ is not a Hilbert space (topology is p-adic).

We present a families of graphs of large girth with good expansion properties which similarly with random graphs have no edge transitive automorphism groups. So such a graph is a better approximation of random graph, which has no symmetries at all. We are interested in sequences of q-regular algebraic graphs Γ_i, defined by nonlinear equations, such that their projective limit T is well defined and does not contain cycles. So, the girth of Γ_i is growing with the growth of parameter i. We assume additionally that Γ_i, $i \to \infty$ is a family of expanders. So the upper limit of second largest eigenvalues of Γ_i is bounded away from q. The talk is dedicated to new applications of such simple graphs of increasing girth with good expansion properties to the and designing of multivariate cryptographical algorithms (stream ciphers, key exchange protocols, public key algorithms digital signatures,constructions of hash functions). We speak about the usage of classical explicit constructions (see [3], [5]) as well as applications of the new families of algebraic graphs.

Multivariate Cryptography in the narrow sense (see [1]) is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over finite fields. In certain cases these polynomials could be defined over both a ground and an extension field. If the polynomials have the degree two, we talk about multivariate quadratics. Solving systems of multivariate polynomial equations is proven to be NP-Hard or NP-Complete. That is why these schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes based on difficult problems of Number Theory.

Keywords

family of graphs of large girth, expanding graphs, families of algebraic graphs, Ramanujan graphs, multivariate cryptography

Bibliography

[1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, Springer, Advances in Information Security, 25 (XVIII) (2006): 260.

[2] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[3] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[4] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.

[5] V. A. Ustimenko, U. Romańczuk, *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.