On extremal graphs, affine Cremona semigroups and new solutions of Post Quantum Cryptography

Vasyl Ustimenko, Olexandr Pustovit

Explicit constructions in Extremal graph theory give appropriate lower bound for Turan type problems. In the case of prohibited cycles explicit constructions can be used for various problems of Information Security. We observe some recent theoretical applications of algebraic constructions of regular graphs of large girth [1] and graphs with large cycle indicator [2] to Coding Theory and Cryptography and their implementations.

This research is comlited within intermatiomal project on Multivariate Cryptography with participants from Ukraine, Poland and USA (see [2]-[10]). In particular we present new postquantum algorithms of Non-commutative cryptography defined in graph theoretical terms and new key dependent Message Authentication Codes.

References

1. F. Lazebnik, V. Ustimenko, A. J.Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 1, 73–79.
2. M. Polak, U. Romanczuk, V. Ustimenko A. Wroblewska, *On the applications of Extremal Graph Theory to Coding Theory and Cryptography*, Electronic Notes in Discrete Mathema Discrete Mathematics, (2017), no. 43, 329–342.
3. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, *On the constructions of new symmetric ciphers based on non-bijective multivariate maps of pre-scribed degree*, Security and Communication Networks , Volume (2019), Article ID 2137561, 15 pp., https://doi.org/10.1155/2019/2137561.
4. V. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations*, Dopov. Nath Acad of Sci, Ukraine (2017), no. 5, 17–24.
5. V. Ustimenko, *On the families of stable transformations of large order and their cryptographical applications*, Tatra Mt. Math. Publ. **70** (2017), 107–117.
6. V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism*, Dopov. Nath Acad of Sci, Ukraine (2018), no. 10, 26–36.
7. V. Ustimenko, M. Klisowski , *On Noncommutative Cryptography with cubical multivariate maps of predictable density*, Proceedings of "Computing 2019" conference, London, 16-17, July,to appear in in Springer series "Advances in Intelligent Systems and Computing".
8. V. Ustimenko , *On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography*, Cryptology ePrint Archive, 133, (2019).
9. Ustimenko V. O., Pustovit O.S., *On new algorithms for the audit of digital documents, their implementation and cybersecurity applications*, Collective monographs of proceedings of XVI, International conference, Kyiv (Puscha-Vodytsa) (2018), 170–174.
10. Ustimenko V. O., Pustovit O.S., *On new stream algorithms of generating of digests of digital documents with high avalanch effect*, Collective monograph "Mathematics and Computer modelling", ser. of physic.-math., Proceedings of International symposium "Problems of computational optimisations, Kyiv, Institute of Cybernetics of acad. V. M. Glushkov, September 24-27, 2019 (to appear).

Contact information

Vasyl Ustimenko
Department of Mathematics, Physics and Informatics, University of Marie Curie-Sklodowska, Lublin, Poland
Email address: vasylustimenko@yahoo.pl

Olexandr Pustovit
Department of ontological systems and applied algebraic combinatorics, Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine (ITGIP NAS of Ukraine), Kyiv, Ukraine
Email address: sanyk_set@ukr.net

Key words and phrases. Extremal graphs, Information Security, Post Quantum Cryptography, Message Authentication Codes

Exponential sums on the sequences of inversive congruential pseudorandom numbers with the variable shifts

Pavel Varbanets, Sergey Varbanets

The investigation of the sequences $\{x_n\}$ of pseudorandom numbers under the interval [0,1) can be executed by the estimates of special exponential sums over the sequences of these numbers. A nontrivial estimate of such sum was being obtained by H. Niederreiter in the work [**1**]:

Let $\{x_k\}$ is the linear congruential pseudorandom numbers with the period τ produced by the congruential recursion $x_{n+1} \equiv ax_n + b \pmod m$. Then

$$\left|\sum_{n=0}^{N-1} e^{2\pi i \frac{hx_n}{m}}\right| \le \left(\frac{m\tau}{\ell}\right)^{\frac{1}{2}} \left(\frac{2}{\pi}\log\tau + \frac{3}{4}\right),$$

where $1 \le N \le \tau$; ℓ is the exponent of $a \pmod m$.

In our talk we consider the analogous exponential sum for the sequence $\{x_n\}$ generated by the inversive congruential generators of type

(1) $x_{n+1} \equiv \frac{a}{x_n} + b(n) \pmod{p^m}$,
(2) $x_{n+1} \equiv \frac{a}{x_{n-1}x_n} + b(n) \pmod{p^m}$

with conditions $(a,p) = 1$, $b(n) \equiv 0 \pmod{p^\beta}$ for all $n \in \mathbb{N}$.

Moreover, we use the representations $\{x_n\}$ as a polynomials on n over $\mathbb{Z}_{p^m}$ and derive the nontrivial estimates for "Kloosterman sums" on the sequences of pseudorandom numbers produced by the recursion (1) or (2).

References

1. Niederreiter H., On the distribution of pseudorandom numbers generated by the linear congruential method, III, Math. Comp., 30 (1976), 571-597.

Contact information

Pavel Varbanets
Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua