SEMINARIUM
MATEMATYKA DYSKRETNA

wtorek, 16 maja 2023 r., godz. 12:30, s. 612 C-7

Konstrukcja algorytmu kryptograficznego opartego na grafach

Łukasz Jęda
WMS AGH

Idea konstrukcji szyfru bazującego na rezultatach dynamiki symbolicznej pojawiła się w wielu istniejących pracach, np. Kotulskiego i Szczepańskiego [1]. Wyniki w dziedzinie dynamiki symbolicznej wskazują nieskracalne przestrzenie przesunięć, w których zbiór słów zakazanych tworzy język regularny (ang. *irreducible sofic shifts*) jako potencjalną bazę do budowy szyfru. Przestrzenie te charakteryzują się m.in.:

- ekspansywnością,
- chaotycznością w sensie Devaneya,
- dodatnią entropią topologiczną.

Te właściwości czynią wspomniane systemy dobrą podstawą do projektowania szyfrów. Przestrzenie te są reprezentowane za pomocą silnie spójnych etykietowanych digrafów (dokładniej: tworzą je generowane na ich bazie dwustronnie nieskończone ciągi etykiet) [2, 3].

Prezentowany kryptosystem jest symetryczny, wykorzystujący w procesie szyfrowania i deszyfrowania digraf przejść i dwa klucze. Pierwszy klucz odpowiada za sterowanie procedurą szyfrowania, drugi ma za zadanie wprowadzić do wejściowego tekstu jawnego szum, by utrudnić złamanie szyfru oraz odkrycie pierwszego klucza. Digraf zawiera wierzchołki odzwierciedlające możliwe stany kryptosystemu, pomiędzy którymi system „przechodzi" w procesie szyfrowania i deszyfrowania wiadomości (tzn. system w dowolnym momencie znajduje się w pewnym określonym stanie i pod wpływem szczególnych warunków następuje jego przeniesienie się do innego stanu).

[1] Z. Kotulski, J. Szczepański, Discrete chaotic cryptography, *annalen der physik (adp)*, DOI 10.1002/andp.19975090504 (1997), s. 381–394.

[2] M. Béal, F. Fiorenzi, D. Perrin, A Hierarchy of Irreducible Sofic Shifts, *Mathematical Foundations of Computer Science 2004* T. 3153, Lecture Notes in Computer Science (LNSC), Berlin 2004, s. 611–622.

[3] P. Oprocha, Algorithmic Approach to Devaney Chaos in Shift Spaces, *Fundamenta Informaticae* 87 (2008) s. 435–446.