

# SEMINARAS

**2015 sausio 5 d. 11:00, SRL-I 427 kab.**

*Rita Palivonaitė*

## Chaotinė vizualinė kriptografija

Vizualinė kriptografija – tai kriptografijos šaka, kuri leidžia vizualinę informaciją užkoduoti sudėtingais kompiuteriniais algoritmais, tačiau šios informacijos iššifravimui užtenka žmogaus regos sistemos. Dinaminė vizualinė kriptografija (DVK) – alternatyvus vaizdų kodavimo metodas, kurio pagrindas yra ne statinė dviejų (ar n) užkoduotų skaidrių (ar geometrinio muaro vaizdų) superpozicija, o laike vidurkintas geometrinis muaras. Tai vieno vaizdo metodas, kuomet slaptas vaizdas išryškėja jį virpinant pagal harmoninį dėsnį iš anksto nusakyta kryptimi pagal tiksliai parinktą svyravimų amplitudę. Ši sritis dar nėra pilnai išnagrinėta, ypač kalbant apie saugesnes schemas bei praktinį DVK pritaikymą. Eksperimentinis DVK vykdymas reikalauja generuoti harmoninius virpesius, tačiau netiesinės sistemos, net ir sužadintos harmoniniais virpesiais, gali virpėti chaotiškai. Vienas iš pristatomų darbų – išvesti teoriniai sąryšiai ir realizuota kompiuterinė chaotinės vizualinės kriptografijos schema. Taip pat pristatoma deformuojamoji vizualinė kriptografija, bei padidinto saugumo DVK schemas. Tačiau kalbant apie realaus pasaulio eksperimentus, praktinis DVK įgyvendinimas – sudėtinga užduotis, nes slaptą vaizdo dekodavimo ekspozicijos laikas neturi tęstis ilgai, nes žmogaus akis matomą vaizdą vidurkina akimirksniu. Todėl efektyviam eksperimentiniam chaotinės vizualinės kriptografijos įgyvendinimui pristatomas įrankis trumpoms laiko eilutėms segmentuoti.

**Kviečiame dalyvauti.**

**Seminaro sekretorius A. Bugajev**