Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

LKRV

LABORATORIJ ZA KRIPTOGRAFIJO IN RAČUNALNIŠKO VARNOST

London
Barcelona
Torino
Trento
Eindhoven
Campinas, SP
Hefei
Pohang
Sendai
Osaka
Madison, WI
Worcester, MA
Waterloo, ON

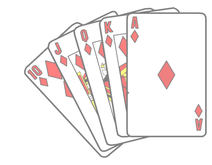
Raziskovalna področja

Ukvarjamo se s kriptografijo in računalniško varnostjo, diskretno matematiko, teorijo kodiranja ter statističnim načrtovanjem. Imamo izkušnje z uporabno kriptografijo, posebno s kriptosistemi z javnimi ključi (npr. eliptične krivulje), kriptografskimi protokoli in njihovo implementacijo v omejenem okolju (npr. pametnih karticah).

Raziskujemo tudi na področju algebraične kombinatorike (razdaljno regularni grafi, asociativne sheme, končne geometrije, kode, kvantni sprehodi ipd.)

Anonimizacija

Miselni poker



E-učenje

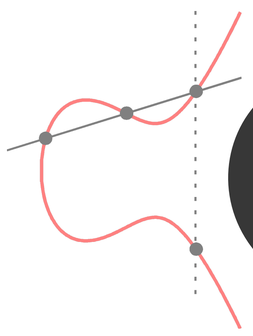
Naključnost

Verjetnost in statistika

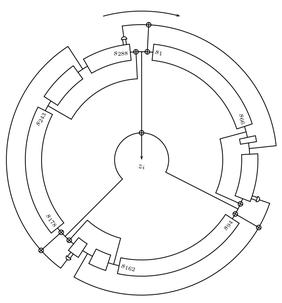
Pametne kartice

#hacking

Eliptične krivulje



Tokovne šifre



Kriptografija

Protokoli

Računalniška varnost

Gesla

@friCA
Certifikatna agencija

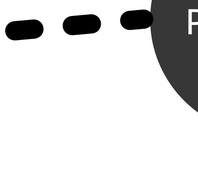
Zgoščevalne funkcije

Asociativne sheme

Grafi

Kode

Geometrije



Algebraična kombinatorika

Članki

P. Nose: Security weaknesses of a signature scheme and authenticated key agreement protocols,
Inf. Process. Lett. 114 (2014)

A. Jurišić in J. Vidali: Extremal 1-codes in distance-regular graphs of diameter 3,
Des. Codes Cryptogr., 65 (2012)

P. Nose, Security weaknesses of authenticated key agreement protocols,
Inf. Process. Lett. 111 (2011)

A. Jurišić in J. H. Koolen, Classification of the family AT4(qs,q,q) of antipodal tight graphs,
J. Combin. Theory (A) 118 (2011)

J. Vidali, P. Nose in E. Pašalić: Collisions for variants of the BLAKE hash function,
Inf. Process. Lett. 110 (2010)

Društvo kriptologov
Zagreb
Beograd
St. Peterburg
Netanya