DELAVNICE IZ KRIPTOGRAFIJE

(občasno vključujejo tudi računalniško varnost ali teorijo kodiranja)

FMF–KRIPTOGRAFIJA 1998

1)	BAN	Vladimir	Kvantni računalnik
2)	DOLINAR	Gregor	Reševanje kongruenc in Riemanova hipoteza
3)	Luževič	Peter	Nahrbtniški kriptosistemi in LLL algoritem
4)	POVH	Janez	Generatorji pseudonaključnih števil
5)	ŠEGA	Gregor	Testiranje praštevilskosti in Karmichaelova števil
6)	ŽIBERT	Janez	Simetrični sistem IDEA in linearna analiza

FMF–KRIPTOGRAFIJA 1999

1)	BARBIČ	Jernej	tetje točk na eliptični krivulji
2)	BRŽAN	Irena	Kartice zdravstvenega zavarovanja
3)	FLAJS	Andrej	Generator naključnih števil
4)	IVANEC	Desider	Kriptografski slovar pojmov
5)	JEREB	Mojca	DNK računanje
6)	KOCAN	Peter	Faktorizacija z eliptičnimi krivuljami
7)	KOMAR	Mojca	Prodaja sistemov za varnost podatkov
8)	KAPŠ	Mateja	Zgodovina kriptografije
9)	MEDVED	Mario	Zaščita naše domače strani
10)	MARKOVČIČ	Maja	Slovenska zakonodaja in kriptografija
11)	MIKLAVIČ	Štefko	Algoritmi za potenciranje
12)	NASTRAN	Vanja	Echelon
13)	NOVAK	Tadej	Psevdonaključna zaporedja bitov
14)	PEČAR	Martin	Vizualna kriptografija
15)	PERKO	Urban	Kleptografija - študij varne kraje informacij
16)	PRAPROTNIK	Matjaž	Zgoščevalna funkcija SHA-1
17)	ŠIJANEC	Tina	NSA in računska moč
18)	TONEJC	Jernej	Izboljšanje množenja za določene tipe EC
19)	TROŠT	Matjaž	Brezžični telefoni
20)	VUK	Miha	CA in standard 509
21)	ZUPAN	Eva	Mehanski stroji za faktorizacijo

FRI–KIRV 2000

1)	BENEDIK	Hubert	Hitro odkrivanje potenc praštevil
2)	CEFERIN	Tomo	Izvoz kriptografske tehnologije, patenti
3)	DOBROVOLJC	Andrej	Microsoft CryptoAPI - Kriptografski programski vmesnik
4)	HRASTOVEC	Marko	Ali je kupovanje preko interneta varno - www.eon.si
5)	KAVŠEK	Branko	
6)	KOLMANIČ	Robert	Stanje v Sloveniji na področju pametnih kartic.
7)	KOTNIK	Samo	Elektronsko bančništvo v sloveniji
8)	LEBEN	Roni	Analiza varnosti sistema GSM
9)	MASTEN	Mitja	Kakšno zaščito imajo naše banke
10)	NENEZIC	Vitomir	Slovenska zakonodaja na področju kriptografije in rač. varnosti
11)	NOVAK	Damjan	Twofish
12)	PIVK	Aleksander	Elektronski plačilni sistemi
13)	ROŽANEC	Alenka	Varovanje računalniških sistemov s poudarkom na zaščiti DB
14)	ŠKOF	Ivan	IDEA
15)	ŠKULJ	Janez	Kerberos
16)	TRAMPUŠ	Matej	SSL
17)	VERHOVŠEK	Roman	Javanska kriptografska knjižnica
18)	VESTER	Boštjan	Blowfish
19)	VIČIČ	Jernej	Digitalni vodni žig - digital watermark

FRI-KIRV 2002

1)	BAŠA	Vigor	Biometrija
2)	GOLOUH	Mitja	Vloga nadzora pri računalniški varnosti
3)	GROM	Matej	Varnost protokola Bluetooth
4)	JEREB	Franci	IPsec protokol v VPN omrežjih
5)	KUSTER	Robert	RNG(LFSR)/CRC
6)	MOČNIK	Jaka	E-volitve
7)	OBLAK	Boštjan	HMAC
8)	PERME	Marko	Digitalni denar
9)	POR	Luka	OpenSSL in certifikati
10)	SPINDLER	Matej	XTR kriptosistem
11)	STAJDUHAR	Ivan	DS in timestamping: Digitalni dokumenti danes
12)	STORMAN	Iztok	IPSEC/802.11b, 802.1x/UMTS
13)	UNK	Miha	Varnost mreznih naprav
14)	ZAPLOTNIK	Tomaž	Kriptografske hash funkcije
15)	ZUPAN	Janez	RNG/ključi in testi linearnosti

FMF–KITK 2003

1)	BIZJAK	Maja	Zgodovina kodiranja
2)	BREZNIK	Kristija	Elementarni dokaz praštevilskega izreka
3)	BRLOGAR	Aljoša	Dokazi brez razkritja znanja
4)	DAKSKOBLER	Blaž	Praštevilo je v P
5)	GOLJEVŠČEK	Luka	Differential power analysis
6)	IPŠA	Simona	Enigma in Purple (WWII)
7)	JERMAN	Nataša	Otroška kriptografija
8)	KIRN	Meta	Kripto-popul3
9)	KOCBEK	Primož	Kleptografija (Študij varne kraje informacij)
10)	KOMELJ	Andrej	OPEN SSL in EC
11)	KOŠIČ	Janja	Kripto-popul2
12)	KRALJ	Katarina	Fish in Tunny
13)	MAHNIČ	Jana	Konvolucijske kode
14)	MLEKUŽ	Patrik	Prehod med bazami
15)	OŽEK	Matej	WEP, 802.11i
16)	REŠČIČ	Miha	EC implementation
17)	STANEK	Maruša	Normalne baze
18)	STRAŽAR	Anja	Dokazi brez razkritja znanja
19)	ŠIRCELJ	Karin	Kripto-popul1
20)	TOLA	Špela	Kripto-krožek
21)	TOMAŠ	Tatjana	Identifikacijska števila in črtne kode
22)	URLEP	Matjaž	Varna domača stran
23)	VUKSANOVIC	Miloš	Simetrične sifre
24)	ZADRAVEC	Aleš	Vizualna kriptografija in Hadamardjeve matrike
25)	ZEMAN	Mirjana	Psevdo-naključna zaporedja
26)	ŽELJKO	Jure	Razcep polinomov
27)	ŽIBRAT	Simon	Časovne oznake

FRI–KIRV 2004

1)	ALFIREVIC	Igor	Hash funkcije
2)	BRESKVAR	Gorazd	WEP, 802.11i?
3)	DOLENC	Boštjan	Napadi na RNG
4)	DRNOVŠČEK	Slavko	Slepi podpis
5)	GLAVIC	Boris	Standard XML - XAdES
6)	JANEŽIČ	Damjan	Uporabnost monostne identifikacije za varno e-poslovanje
7)	JERIČ	Borut	Metode preklicevanja certifikatov
8)	KLJUN	Matjaž	Hackerji
9)	KOS	Ludvik	Digitalna poštna znamka
10)	KOVAČ	Jure	Brezkontaktne sc
11)	KRALJ	Primož	Glasbena gesla
12)	MAHKOVEC	Žiga	Analiza RNG v Linuxu
13)	PAVLIČ	Tomaž	Digitalni denar
14)	PRAPROTNIK	Matjaž	CC LFSR
15)	REBOLJ	Gregor	Kriptoanaliza SIM kartice?
16)	SKUBIC	Ales	Varna soba
17)	TOMAŠEVIČ	Denis	Poarni zid v OpenBSD
18)	VIDRIH	David	E-glasovanje
19)	ZDEŠAR	Blaž	Mentalni poker

FRI–KIRV 2006

1)	HITI	Tomaž	Varnost gesel in dinamična gesla
2)	KEJŽAR	Marko	Družina zgoščevalnih funkcij SHA
3)	KERŠNIK	Jelena	Kriptosistem XTR
4)	KRMELJ	Jernej	Elektronske dražbe
5)	ŠTIMEC	Aleš	Diferenčna analiza električne aktivnosti
6)	TURK	Boris	Faktorizacija - algoritem številskega rešeta
7)	ZUPANČIČ	Tadej	Pregled varnosti pri komunikaciji z GSM

IŠRM–KITK 2008

1)	ERMENC	Rok	Dokazi brez razkritja znanja
2)	JANEŽ	Tadej	SE:crypto-engine, digitalni denar
3)	MUHIČ	Andrej	EC DLP
4)	KOŠMERLJ	Aljaz	Zgoščevalne funkcije
5)	NOSE	Peter	NTRU, EC štetje točk
6)	PAŠČINSKI	Uros	McEliece shema za podpis
7)	SIPOŠ	Ruben	TPM
8)	ŠUBELJ	Lovro	Vizualna kriptografija
9)	TRAMPUŠ	Mitja	Mentalni poker
10)	VIDALI	Janos	Skupinski podpisi
11)	ŽBONTAR	Jure	Pametne kartice
12)	ŽAGAR	Lan	Testiranje hadrwerskega RNG

FRI–KIRV 2008

1)	ANŽIN	Matej	AES - konkretna implementacija?
2)	ČERNIVEC	Aleš	Infrastruktura javnih ključev (PKI)
3)	FAJT	Radivoj	Wireless (brez WEB) in IPSec
4)	GLAD	Damjan	Lamportov podpis
5)	JUŽNA	Jernej	RC4
6)	KASTELIC	Marko	Družina zgoščevalnih funkcij SHA-2
7)	MAVER	Jan	Anonimnost podatkovnih baz
8)	MUNDA	Davor	Analiza PRNG v Linux
9)	POREKAR	Jan	Varnost dolgoročne hrambe
10)	RAZORŠEK	Grega	Nepropustnost kriptografskih naprav
11)	SOLIČ	Mirko	Digitalni denar
12)	STAJDOHAR	Miha	Dokazi brez razkritja znanja
13)	STARC	Iztok	Varnost brezkontaktih kartic
14)	TOPLAK	Marko	Zakonodaja na področju računalniške varnosti
15)	IMŠIROVIC	Denis	Požarni zid v OpenBSD

IŠRM–KITK 2009

1)	BLAGUS	Neli	Sim kartice
2)	BOGATAJ	Polona	Zgodovina kripto - Colossus
3)	KOŠMERL	Marko	Network security
4)	KOZINA	Simon	Časovni žigi
5)	MAČEK	Tina	Črtne kode
6)	MOŠKON	Sašo	Brezkontaktne kartice
7)	PEVEC	Darko	Poštna znamka
8)	POLAJNAR	Matija	Sidechannel attacks
9)	PUGELJ	Mitja	Turbo kode
10)	RADOVIC	Marija	KeeLoq
11)	STARC	Janez	Dokazi brez razkritja znanja
12)	VIDMAR	Kaja	Kid-crypto
13)	TOLIC	Andrej	HMAC

IŠRM–KITK 2010

1)	AMBROŽIČ	Martin	Pollardova ro metoda za razcep
2)	KRNC	Matjaž	Hadamardove matrike
3)	LIST	Ivo	E-volilne sheme
4)	PURGAJ	Janko	Kvantni digitalni podpis
5)	ROJKO	Mateja	Deljenje skrivnosti
6)	ŠKOFIC	Nejc	Kvantni prstni odtis
7)	STARIČ	Anže	Časovni žigi
8)	VELKAVRH	Gaja	Varnostna območja
9)	ŽITNIK	Slavko	RFID
10)	NOVAK	Matija	SET
11)	PEROVŠEK	Matic	Implementacija PRNG v FPGA
12)	UGRIN	Matej	Kriptografski protokoli

FRI–KIRV 2010

1)	BEŠTEK	Mate	TinyECC za brezžična senzorska omrežja
2)	SKALE	Primož	Varovanje splatnih strani (HTTPS)
3)	Škoberne	Nejc	Lokalizirana spletna baza zgoščenih vrednosti