



UNIVERSITETI POLITEKNIK I TIRANËS
FAKULTETI I INXHINIERISË MATEMATIKE & INXHINIERISË FIZIKE
DEPARTAMENTI I INXHINIERISË FIZIKE

DISERTACION

për mbrojtjen e gradës shkencore “*Doktor i Shkencave*”

Analiza e sinjaleve nga qarqe elektronike që operojnë në
mënyrë kaotike dhe përdorimi i tyre për sigurinë e
komunikacionit

Kandidati
Joan JANI

Udhëheqësi
Prof. Dr. Partizan MALKAJ

Tiranë

2015



UNIVERSITETI POLITEKNIK I TIRANËS
FAKULTETI I INXHINIERISË MATEMATIKE & INXHINIERISË FIZIKE
DEPARTAMENTI I INXHINIERISË FIZIKE

DISERTACION

Paraqitur nga **Joan JANI**

për mbrojtjen e gradës shkencore “*Doktor i Shkencave*”

TEMA:

Analiza e sinjaleve nga qarqe elektronike që operojnë në
mënyrë kaotike dhe përdorimi i tyre për sigurinë e
komunikacionit

Mbrohet më datë/...../..... para jurisë

1. Prof. Dr. Pëllumb BERBERI Kryetar
2. Prof. Asoc. Ligor Nikolla Anëtar
3. Prof. Asoc. Luigj Gjoka Anëtar
4. Prof. Dr. Dritan Spahiu Anëtar - Oponent
5. Prof. Dr. Lulëzim Hanelli Anëtar - Oponent

Dedikuar familjes

Falenderime

Dëshiroj të falenderoj të gjithë ata që më kanë ndihmuar në realizimin e këtij punimi për kontributin e vyer të tyre. Në rradhë të parë dëshiroj të falenderoj udhëheqësin shkencor Prof. Dr. Partizan Malkaj, për kohën e dedikuar dhe për udhëzimet e shumta dhe të çmuara, pa ndihmën e tij ky punim nuk do të ishte realizuar.

Dëshiroj të falenderoj kolegët e mi të cilët kanë qenë gjithnjë të gatshëm për të dhënë kontributin me këshillat e tyre, si dhe të gjithë stafin akademik të Departamentit të Fizikës për bashkëpunimin e frytshëm.

Gjithashtu, falenderoj Fakultetin e Inxhinierisë Matematike dhe Inxhinierisë Fizike për mbështetjen dhe ndihmën e vazhdueshme gjatë kërkimit tim shkencor.

Një falenderim i veçantë edhe për Departamentin e Fizikës së Universitetit të Athinës ku janë kryer një pjesë e madhe e matjeve pjesë e këtij punimi shkencor, në veçanti Prof. Dr. Georgios Tombras.

Në fund dëshiroj të falenderoj të gjithë ata që kanë dhënë kontributin e tyre moral në hartimin e këtij punimi, veçanërisht familjen time.

Të gjithë personat e cituar në këtë faqe kanë pasur një rol të rëndësishëm në këtë punim dhe suksesin e tij, por cdo gabim apo pasaktësi është thjesht përgjegjësi e imja.

Abstrakti në Shqip

Në këtë punim studiohen disa qarqe që veprojnë në mënyrë kaotike si dhe bëhet analiza e tyre. Në fillim paraqitet një hyrje e shkurtër tek sistemet dinamike, përkufizohen madhësitë që i karakterizojnë dhe prezantohet aparati matematikor për studimin e tyre i cili do përdoret në disertacion. Dukuria e kaosit shfaqet në sisteme dinamike, përkufizohet kaosi dhe eksponenti Lyapunov i cili karakterizon një sistem dinamik si sistem kaotik. Në vazhdim bëhet një hyrje tek metoda e analizës së serive kohore jo lineare do përdoret për të studiuar dinamikën e qarqeve elektronike. Në pjesën e dytë paraqiten qarqe elektronike që operojnë në mënyrë kaotike. Jepen rezultatet e simulimit dhe të implementimit laboratorik të qarkut Chua. Propozohen dy qarqe të cilat mund të përdoren si burime kaosi dhe kryhet analiza e serive kohore që merren nga ato. Më tej studiohet mënyra e sinkronizimit Pecora dhe Carroll në varësi me raportin sinjal zhurmë dhe në lidhje me dobësimin e sinjalit midis qarkut e transmetimit dhe qarkut marrës. Në fund kryhet një studim i aplikimit i kaosit për sigurinë e informacionit duke përdorur qarkun Chua. Metodatat të cilat analizohen janë maskim me kaos (Chaotic Masking (CMA)), modulim me kaos (Chaos Modulation (CMO)) dhe Chaos Shift Keying (CSK).

Fjalët kyçe: sisteme dinamike, kaos, kaos në qarqe elektronike, llogaritja e eksponentin Lyapunov, qarku Chua, sinkronizimi, Chaotic Masking (CMA), Chaos Shift Keying (CSK) dhe Chaos Modulation (CMO)

Abstract in English

In this study we analyze the behavior of some electronic circuits which operate in a chaotic manner. At first we present a brief introduction to dynamical systems, defined sizes that characterize those systems and the tools that will be used later in dissertation. The phenomenon of chaos appears in dynamic systems, we will define chaos and Lyapunov exponent which characterizes a dynamic system as chaotic system. In addition, we give an introduction to the methods of non linear time series analysis used to study the dynamics of these electronic circuits. In the second part are presented electronic circuits that operate in a chaotic manner. The results of the simulation and laboratory implementation of Chua circuit are given. We have proposed two circuits that can be used as sources of chaos and performed the analysis of time series received. Further study of synchronization using the method proposed by Pecora and Carroll depending on signal to noise ratio and about weakening the signal transmission between the transmitter and receiver. At the end of a survey of the application of chaos in information security is done using Chua's circuit. We have analyzed the methods of Chaotic Masking (CMA), modulation of Chaos Chaos Modulation (CMO) and Chaos Shift Keying (CSK).

Keywords: dynamic systems, chaos, chaos in electronics, Lyapunov exponent, Chua's circuit, synchronization, Chaotic Masking (CMA), Chaos Shift Keying (CSK) dhe Chaos Modulation (CMO)

Përmbajta

Falenderime	iii
Abstrakti në Shqip	iv
Abstrakt in English	v
Figurat	xi
Tabelat	xii
 I Pjesa e parë	 1
1 Hyrja	2
1.1 Motivimi	2
1.2 Qëllimi i punimit	4
1.3 Metodologjia e punimit	5
1.4 Struktura e punimit	5
 2 Sistemet jolineare dinamike	 8
2.1 Sistemet dinamik	8
2.2 Përshkrimi matematikor i sistemeve dinamike	10
2.3 Bifurkimi	17
2.3.1 Bifurkimi Hopf	18
2.3.2 Bifurkimi i palosjes	19
2.3.3 Bifurkim i menjëhershëm	19
2.4 Sisteme dinamike dhe kaos	19
2.5 Kalimi në kaos	21
2.5.1 Kalimi në kaos me dyfishimin e periodës (period doubling)	22
2.5.2 Kalimi në kaos nëpërmjet shkëputjes (intermittency)	22
2.5.3 Shembulli i bifurkimit në logistic map	23
2.6 Eksponenti Lyapunov	25

2.6.1	Shembulli i bifurkimit dhe i kaosit	26
3	Seritë kohore	28
3.1	Paraqitja e serive kohore	28
3.2	Metodat e analizave të serive kohore	29
3.3	Rindërtimi i hapësirës fazore	29
3.4	Zgjedhja e vonesës τ	32
3.4.1	Llogaritja e autokoleracionit	32
3.4.2	Informacioni i përbashkët	33
3.5	Dimensioni i ngulitur m (emdedded dimendion)	35
3.5.1	Të afërmit e rremë	36
3.6	Spektri i Fuqisë	37
II	Pjesa e dytë	39
4	Prania e kaos-it në qarqet elektronike	40
4.1	Qarku i Chua-s	40
4.1.1	Modeli matematikor i qarkut të Chua's	42
4.1.2	Realizimi i rezistencës jo lineare	44
4.1.3	Realizimi i qarkut të Chua's në Multisim	48
4.1.4	Simulimi me MATLAB të qarkut Chua	52
4.1.5	Realizimi laboratorik i sistemit	53
4.2	Qarku kaotik me një transistor	56
4.2.1	Komponentët e qarkut	58
4.2.2	Simulimi dhe implementimi i qarkut	59
4.2.3	Regjistrimi i të dhënave	60
4.3	Zona aktive e kundërt	62
4.3.1	Analiza kohore e sinjalit të daljes	63
4.3.2	Rindërtimi i hapësirës fazore	68
4.4	Llogaritja e eksponentit Lyapunov	70
4.4.1	Studimi i kontrollit të kaosit	74
4.5	Një qark kaotik me dy tranzistor	74
4.6	Analiza kohore e sinjalit të daljes	75
4.7	Konkluzione	78
5	Sinkronizimi	80
5.1	Paraqitja teorike	80

5.2	Sinkronizimi i qarkut të Chuas	81
5.3	Studimi sipas raportit sinjal mbi zhurmë	82
5.4	Studimi sipas dobësimit të sinjalit	84
6	Kriptografia në komunikime dixhitale duke përdorur kaos	91
6.1	Maskim me kaos - Chaos Masking (CMA)	92
6.1.1	Realizimi i kaotik masking	92
6.2	Modulimi me sinjal kaotik - Chaos Modulation (CMO)	94
6.2.1	Realizimi i modulimit me sinjal kaotik CMO	95
6.3	Chaos Shift Keying (CSK)	96
6.3.1	Realizimi i sistemit CSK	97
6.4	Konkluzionet	99
7	Përfundimet	100
7.1	Konkluzionet	100
7.2	Puna në vazhdimësi	101
	Bibliografia	102

Figurat

2.1	Prezantimi grafik i sistemit	9
2.2	Portreti fazor për lavjerësin me fërkim [1]	14
2.3	Shëmbull e një sistemi konservativë dhe sistemi me humbje [1]	17
2.4	Bifurkimi Hopf	18
2.5	Bifurkimi i menjëhershëm në sistemin Duffing [2]	20
2.6	Paraqitja e bifurkimit në logistic map.	24
2.7	Llogaritja e eksponentit Lyapunov në logistic map.	24
2.8	Paraqitja grafike e eksponentit Lypunov për dy trajektore të cilat janë afër me njëra tjetrën	25
3.1	Paraqitja grafike e rindërtimit të hapësirës fazore [3]	30
4.1	Qarku i Chua-s i cili studiohet në këtë kapitull	41
4.2	Rezistenca jo-lineare N_R që është parametri kryesor i paraqitjes të dukurisë së kaosit.	41
4.3	Realizimi i rezistencës jolineare të qarkut Chua [4]	44
4.4	Realizimi i qarkut të plotë Chua [4]	47
4.5	Qarku elektronik i cili përdoret për të simuluar sistemin e Chua-s . . .	48
4.6	Hapësira fazore e atraktorit të Chua-s pas simulimit me $R_2 = 1.72$. . .	49
4.7	Atraktori i plotë i sistemit të Chua-s i cili realizohet me rezistencën $R_2 = 1.9 k\Omega$	49
4.8	Singali kaotik që merret në C_2 pas simulimit me rezistencën $R_2 = 1.9 k\Omega$	50
4.9	Singali kaotik që merret në C_1 pas simulimit me rezistencën $R_2 = 1.9 k\Omega$	50
4.10	Hapësira fazore e llogaritur me metoda numerike	53
4.11	Sinjalet kaotike që prodhohen nga sistemi i Chua-s	54
4.12	Diferencat që shfaqen në v_1 kur ndryshohen kushtet fillestare.	54
4.13	Karakteristika	55
4.14	Rezultati i realizimit në laborator të qarkut.	56
4.15	Realizimi i atraktorit të plotë të qarkut të Chua-s	57

4.16 Sinjali real kaotik që merret midis skajeve të kondensatorit C_2	57
4.17 Spektri i fuqis të sinjalit kaotik të prodhuar nga qarku i Chuas.	58
4.18 Skema elektronike e qarkut kaotik ku transistori vepron në zonën aktive të kundërt	59
4.19 Implementimi laboratorik i qarkut të prezantuar në figurën 4.18.	60
4.20 Simulimi i qarkut të figurës 4.18.	61
4.21 Simulimi i te sinjalit të daljes $V_c(t)$ me hollësi më të madhe.	62
4.22 Figura në oshiloskopit pas implementimit të qarkut të laborator.	63
4.23 Sinjali i përfituar nga oshiloskopi dixhital.	64
4.24 Paraqitja grafike e karakteristikave të transistorit BJT [5].	65
4.25 Rezultati i llogaritjes së informacionit të përbashkët.	65
4.26 Llogaritja e autokorelacionit të serisë kohore	67
4.27 Përqindja e të afërmeve të rremë (FNN) në lidhje me dimensionin e ngulitur m , përpara (vija e zezë) dhe pas (vija e kuqe) e reduktimit të zhurmës	68
4.28 Hapësira fazore e marrë nga oshiloskopi.	69
4.29 Projektioni në dy dimensione e hapësirës fazore të rikonstruktuar.	69
4.30 Llogaritja e eksponentit Lyapunov maksimal sipas metodës Rosenstein	70
4.31 Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 13 Volts$	71
4.32 Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 13 Volts$	71
4.33 Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 10 Volts$	72
4.34 Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 10 Volts$	72
4.35 Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 11.5 Volts$	73
4.36 Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 11.5 Volts$	73
4.37 Qarku i propozuar si burim i sinjaleve kaotike	75
4.38 Seria kohore e sinjalit $V_c(t)$ ashtu siç llogaritet nga simulimi	76
4.39 Informacioni i përbashkët në lidhje me 4.37	77

4.40 Llogaritja e shumatorit të korrelacionit (correlation sum) në lidhje me logaritmin e distancës	79
4.41 Llogaritja e derivatit të shumatorit të korrelacionit për të gjetur dimensionin e korrelacionit.	79
5.1 Mënyra e sinkronizimit të qarkut të Chuas	81
5.2 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=11dB	85
5.3 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=5dB	85
5.4 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=-14dB	86
5.5 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=-19dB	86
5.6 Mënyra e sinkronizimit të qarkut të Chuas	87
5.7 Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 0\Omega$	88
5.8 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 0\Omega$	88
5.9 Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 3.5 k\Omega$	89
5.10 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 3.5 k\Omega$	89
5.11 Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 10 k\Omega$	90
5.12 Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 10 k\Omega$	90
6.1 Bllok skema e sistemit me maskim kaotik (CMA)	92
6.2 Sinjalet për metodën maskim me kaos	93
6.3 Sinjalet për metodën maskim me kaos	94
6.4 Bllok skema e sistemit CMO	95
6.5 Sinjalet për metodën CSK	96
6.6 Chaos Shift Keying (CSK)	97
6.7 Sinjalet për metodën CSK	98
6.8 Sinjalet për metodën CSK	98
7.1 Laboratori i elektronikës në Departamentin e Fizikës të Universitetit të Athinës në Greqi	127

Tabelat

2.1	EkspONENTËT Lyapunov të gjendjeve të mundshme të një sistemi dinamik.	26
4.1	Tabela e plotë e kompetenteve që u përdorën për qarkun e Chua's.	51
4.2	Vlerat fillestare për zgjidhjen e ekuacioneve.	52
4.3	Informacioni i përbashkët në lidhje me vonesën τ	66
4.4	Autokorelacioni në lidhje me vonesën τ	66
5.1	Vlerat e SNR dhe ekuacionet e drejtëzës që lidhin v_{11} dhe v_{12}	84
1	Të dhënat e serisë kohore nga qarku me një tranzistor	118
2	Të dhënat e serisë kohore nga qarku me dy tranzistor	119

Pjesa I

Pjesa e parë

Kapitulli 1

Hyrja

Jetojmë në një botë të pasigurt e cila bazohet në komunikimin në distanca të largëta. Arritjet e reja në fushën e telekomunikacionit kanë sjellë ndryshime të mëdha jo vetën në mënyrën e komunikimit midis njerëzve por kanë ndryshuar dhe tregun ekonomik botëror. Tashmë i njëjti artikull, nëpërmjet internetit, mund ti ofrohet çdo qytetari në çdo vend të botës që ai jeton. Ky ndryshim i tregut me një fjale quhet "Globalizëm". Në këtë botë të globalizuar siguria në transmetimin e mesazheve është çështje primare. Për këtë arsye kriptografia e mesazheve është një domosdoshmëri. Por sa i sigurtë duhet të ndihet përdoruesi i një sistemi transmetimi kur çdo ditë fuqia kompjuterike rritet, duke vënë në dyshim sigurinë e sistemeve kriptografike? Në këtë kapitull hyrës paraqitet arsyeja e përzgjedhjes së kësaj fushe kërkimi shkencor.

1.1 Motivimi

Kriptografia është përdorur që nga lashtësia dhe deri në ditët tona kryesisht në sistemet moderne të transmetimit të informacionit.

Kriptografia moderne është aplikuar në çdo sistem i cili transmeton informacione të rëndësishëm, si informacion ushtarak, informacion financiar, informacion bankar ose të dhëna personale dhe përdor si bazë teorinë e numrave të mëdhej. Hipoteza

ekzistuese, e cila është marrë e mirëqënë, është se fuqia kompjuterike nuk mund të faktorizojë në një kohë relativisht të shkurtër numra të mëdhenj. Fakt ky i vërtetë deri diku, por me zhvillimin e teknologjisë kompjuterike fuqia e kompjuterit është gjithmonë në rritje.

Nga ana tjetër, përveç rritjes së fuqisë kompjuterike duhet përmendur dhe fusha e re e kompjuterave kuantikë. Këta bazohen në vetitë kuantike të elektroneve. Teknologjia e sotme e elektronikës bazohet në veprimin e elektroneve nën ndikimin e fushës. Kompjuterat kuantikë sigurojnë fuqi kompjuterike marramendëse. Si pasoj të gjitha sistemet e sigurisë së transmetimit të përdorura deri tani janë të pa sigurta, pasi duke përdorur një kompjuter kuantik të gjitha kodet mund të thyhen në një kohë shumë të shkurtër. [6]

Kjo e fundit është një risi teknologjike e cila ka sjellë skepticizëm rreth kriptografisë tradicionale të bazuar tek faktorizimi i numrave të mëdhej. Kështu është e domosdoshme të prezantohen sisteme të reja për të garantuar sigurinë e komunikimeve. Deri tani janë bërë dy propozime nga komuniteti shkencor, i pari ka të bëjë me kriptografinë kuantike, ku përdoren vetitë kuantike të fotoneve. Metoda e dytë, e propozuar është metoda e kriptografisë duke përdorur sinjale kaotike.

Kaosi është një veti e sistemeve jolineare. Këtu ecuria e sistemit varet shumë nga kushtet fillestare. Një ndryshim i vogël tek kushtet fillestare mund të shkaktojë një ndryshim në ecurinë e sistemit. Në këtë mënyrë një vëzhgues i jashtëm mund të karakterizojë këto si sisteme rastësore. Këto sisteme mund të implementohen dhe në qarqe elektronike. Atëherë, kaosi i shfaqur në këto sisteme vëzhgohet nga një vrojtues i jashtëm si një sinjal rastësor. Në realitet ky sinjal rastësor mund të rigjenerohet nëpërmjet procedurës së sinkronizimi të qarqeve.

Duke konsideruar faktet e sipër përmendura, mund të propozohet një sistem i cili përdor sinjale kaotike të gjeneruar nga një qark elektronik i posatshëm, këto sinjale përdoren si zhurmues (chirper) për të ruajtur mesazhin e transmetuar. Ky mesazh

nuk mund të lexohet nga një përgjues se deshifrimi i tij nuk mund të bëhet nga një program kompjuterik, pasi është krijuar mbi vetitë jolineare të qarqeve elektronike. Nga ana tjetër, tek sistemi marrës, një qark elektronik me të njëjtat komponentë si tek sistemi i transmetimit gjeneron një sinjal identik me sinjalin zhurmues. Kështu duke hequr sinjalin kaotik nga sinjali i marrë përfitohet mesazhi i transmetuar.

Së fundi, duhet thënë se fusha e zgjedhur e kërkimit është një ndërthurje e elektronikës, e programimit, e sistemeve jolineare si dhe e matematikës së aplikuar. Kjo fushë si ndërdisiplinore motivoj më shumë autorin pasi ndërthurja e shumë disiplinave kërkon aftësi dhe njohuri mbi fusha të ndryshme të kërkimit shkencor.

1.2 Qëllimi i punimit

Qëllimi i këtij studimi është që të prezantohen dhe të krahasohen karakteristikat dhe performancat e sistemeve kriptografike të bazuar në qarqe kaotike.

Në fillim, propozohen qarqe që mund të përdoren si burime kaotike. Prezantohen rezultatet e simulimeve të tyre dhe rezultatet pasi ato janë implementuar në laborator. Diskutohet cili nga këto sisteme mund të përdoret për një sistem komunikimi me qëllim kriptografinë e sinjalit.

Në vazhdimësi vlerësohen sisteme të sinkronizimit në një sistem kriptografie si dhe studiohet sinkronizimi i sistemit në lidhje me zhurmën që shfaqet në kanal. Së fundmi prezantohen rezultatet e simulimeve dhe llogaritjeve të probabilitetit të gabimit të sistemit në lidhje me zhurmën.

Për të realizuar këtë studim janë përdorur programe kompjuterike të cilat simulojnë sistemet jo lineare. Në këtë mënyrë u bë e mundur analiza dhe arritja e përfundimeve mbi efikasitetin e këtyre sistemeve.

1.3 Metodologjia e punimit

Për të kryer këtë punim, si fillim puna nisi në laborator për krijimin e qarqeve jo-lineare. Për ta bërë këtë u përdorën programe të simulimit të qarqeve elektronike dhe pastaj realizimi laboratorik i tyre. Në laborator matjet janë kryer duke përdorur osiloskopi dixhital Agilent. Ky përveç prezantimit në ekran të sinjalit të matur mundëson dhe rruajtjen e sinjalit në një skedar për procesim të mëtejshëm.

Pas marrjes së sinjalit dalës, përdoret metoda e analizës të serive kohore, kryhet rindërtimi i hapësirës fazore sipas metodës Takens dhe karakterizohet në qoftë se sinjali i marrë është sinjal kaotik apo jo. Metoda e përdorur, përshkruhet hollësisht në kapitujt në vazhdim. Algoritmat e metodës janë implementuar në gjuhën e programimit MATLAB, dhe parashtrohen në fund të punimit.

Pasi kryhet analiza e qarqeve të cilat do operojnë si burime të sinjaleve kaotike, propozohet mënyra se si mund të arrihet sinkronizim i tyre. Sinkronizimi studiohet duke kryer simulimin në gjuhën MATLAB. Testohet varësia e sistemit nga raporti sinjal zhurmë dhe nga dobësimi i sinjalit.

Së përfundim, testohet efikasiteti i sistemit, duke simuluar komunikimin e tij në kushte të ndryshme të cilësisë së kanalit. Për të kryer këtë studim u përdorën simulime të qarqeve elektronike në MULTISIM dhe në MATLAB.

1.4 Struktura e punimit

Ky punim është strukturuar në shtatë kapituj. Përmbajtja e çdo kapitulli prezantohet në vijim:

Kapitulli 1: Kapitulli i parë është kapitulli hyrës i punimit të doktoraturës. Në këtë kapitull prezantohet arsyeja që nxiti autorin për të lëvruar më thellë këtë fushë studimi. Në vazhdimësi paraqitet qëllimi i punimit dhe metodologjia që u ndoq mbi

kryerjen e tij. Ky kapitull përfundon me paraqitjen e strukturës së punimit dhe përbajtën e çdo kapitulli.

Kapitulli 2: Në këtë kapitull jepen bazat teorike të sistemeve jolineare si dhe përshkrimi i tyre matematikor. Në vazhdim jepet përkufizimi i hapësirës fazore si dhe i bifurkimit që shfaqët në të. Parashtrohen rastet e bifurkimeve që shfaqen në sisteme elektronike si dhe përkufizimi i sistemeve kaotike të cilat do të jenë tema kryesore e punimit. Duke përfunduar kapitullin shpjegohet se si një sistem dinamik mund të kalojë në veprime kaotike.

Kapitulli 3: Në këtë kapitull paraqitet metoda e analizës së serive kohore, përkufizimet e tyre dhe paraqitet baza matematikore e procedurave që aplikohen për ti karakterizuar ato. Analiza jolineare e serive kohore përdoret për të vërtetuar nëse qarqet elektronike të cilat do të paraqiten në kapitujt në vazhdimësi so të shfaqin dukurinë e kaos-it.

Kapitulli 4: Në kapitullin e katërt paraqiten tre qarqe të cilët operojnë në mënyrë kaotike. Qarku i pari i cili studiohet është qarku Chua i cili është realizuar në laborator dhe është simuluar me anë të programit Multisim. Paraqiten rezultate të qarkut Chua të realizuar në MATLAB, i cili do të përdoret për të studiuar sinkronizimin e tij. Në vazhdimësi paraqiten dy qarqe kaotike të propozuara nga autori ku kryhet dhe analiza e serive kohore të tyre për të vërtetuar prezencën e kaos-it. Në fund të kapitullit jepen konkluzionet e arritura nga analiza e bërë në keto qarqe.

Kapitulli 5: Në kapitullin e pestë studiohet sinkronizimi i qarkut Chua. Për të kryer këtë studim u përdor modeli i qarkut në gjuhën MATLAB dhe programi i simulimeve të qarqeve elektronike Multisim. Studiohet sinkronizimi në lidhje me ra-

portin sinjal zhurmë dhe sinkronizimi i qarkut në lidhje me dobësimin e sinjalit.

Kapitulli 6: Në kapitullin e gjashtë paraqitet mënyra se si dukuria e kaosit mund të përdoret për të realizuar sigurinë e komunikacionit. Studiohen dy metoda të ndryshme se si mund të realizohet ky qëllim me anë të qarkut Chua. Këto sisteme janë Chaos Macking (CM) dhe Chaos Shift Keying (CSK). Kryhet simulimi i këtyre dy metodave duke përdorur qarkun Chua si burim kaosi dhe paraqiten rezultatet e arritura nga studimi i tyre.

Kapitulli 7: Në kapitullin e shtatë dhe të fundit të disertacionit paraqiten konkluzionet e arritura nga studimi i kryer. Gjithashtu paraqitet dhe puna në vazhdimësi.

Kapitulli 2

Sistemet jolineare dinamike

Në këtë kapitull jepen bazat teorike të sistemeve jolinear dhe përshkrimi i tyre matematikor. Jepet përkufizimi i hapësirës fazore dhe të bifurkimit që shfaqët në to si dhe rastet e bifurkimeve që shfaqen në sisteme elektronike. Në vazhdimësi jepet përkufizimi i sistemeve kaotike të cilat janë dhe tema kryesore e punimit. Dhe si përfundim të kapitullit shpjegohet se si një sistem dinamik mund të kaloj në veprime kaotike.

2.1 Sistemet dinamik

Një nga konceptet elementare që shfaqet në fizikë është koncepti i sistemit. Sipas një përkufizimi të përgjithshëm, *një sistem është një bashkësi objektësh të cilat karakterizohen nga një bashkëveprim ose raport reciprok [7].*

Një sistem mund të jetë i hapur ose i mbyllur, me kriter bashkëveprimin e tij me mjedisin e jashtëm. Funkcioni i tij i zakonshëm është që të bëj një transformim mbi të dhënat e hyrjes dhe të kthejë rezultatet në dalje. Nga një vështrim matematikor, mund të karakterizojmë si sistem një njesi, e cila në çdo çast kohor t , merr një hyrje $x(t)$ dhe prodhon në dalje $y(t)$ (fig. 2.1). Në përgjithësi supozohet që hyrjet të cilat jepen në sistem janë pjesë e një bashkësie X , kurse daljet e tij janë pjesë e një bashkësie Y . Në



Figura 2.1: Prezantimi grafik i sistemit

rastin e përgjithshëm dalja e sistemit në çdo çast kohor t , nuk varet vetëm nga vlera që ka tek hyrja $x(t)$ në çastin t por dhe nga vlerat e kaluara.

Një sistem dinamik, karakterizohet nga një bashkësi gjëndjesh të mundshme, dhe nga një ligj i cili lidh situatën aktuale me situatat para-ardhëse. Ky ligj quhet *deterministik* në qoftë se mundëson përcaktimin e situatës aktuale vetëm me njohurinë e situatave paraardhëse. Në qoftë se ky përcaktim nuk është i mundur atëherë sistemi është stokastik ose rastësor.

Një diferencim i dytë i cili mund të përdoret mbi sistemet fizike, ka të bëjë me frekuencën e aplikimit të ligjit të ndryshimit të situatës. Në qoftë se ndryshimi aplikohet vetëm në çaste diskrete, atëherë sistemi quhet sistem dinamik diskret (*diskrete time dynamical system*) dhe evolucioni i tij kohor përshkruhet nga ekuacione diferencash. Në qoftë se çasti kohor tenton zeron, atëherë sistemi quhet *sistem dinamik i vazhdueshëm* (*continuous time dynamical system*) dhe evolucioni i tij përshkruhet nga ekuacione diferenciale. Në qoftë se koha nuk shfaqet tek ekuacionet të lëvizjes së sistemit, sistemi quhet *autonom* (*autonomous*), përndryshe sistemi quhet *jo-autonom* (*non autonomous*) [8].

Nga analiza e mësipërme është bërë e qartë se ekuacionet diferencial - ose ekuacionet e diferencave për sistemet diskrete - janë mjeti kryesor për studimin e ecurisë kohore të sistemeve dinamike. Këto ekuacione mund të jenë lineare ose jo-lineare. Si rrjedhojë një sistem dinamik mund të karakterizohet si *linear* kur ekuacionet që e përshkruajnë janë lineare dhe *jo-linear* kur ndodh e kundërta [9].

Vetia kryesore e sistemeve linear është *mbivendosja*, ose *vetia e linearitetit* (*superposition principle*) [7]. Sipas këtij parimi kombinimi linear i dy zgjidhjeve të cilat

janë linearisht të pavarura është prapë zgjidhje e sistemit. Kjo do të thotë që në qoftë se një sistem dinamik me një përmasë i cili varet nga koha dhe dy zgjidhjet linearisht të pavarura të tij $g(x, t)$ dhe $h(x, t)$, atëherë edhe kombinimi linear i tyre $\alpha * g(x, t) + \beta * h(x, t)$, ku α dhe β janë konstante, është zgjidhje e sistemit. Parimi i mbivendosjes lejon ndarjen e sistemit në nën-sisteme më të vogla, gjetjen e zgjidhjes në secilën prej tyre, dhe mbivendosjen e këtyre zgjidhjeve për gjetjen e zgjidhjes së gjithë sistemit.

Në sistemet jolineare -të cilët në ekuacionet e lëvizjes së tyre variablat që i përshkruajnë paraqiten në një formë jo lineare - parimi i mbivendosjes nuk funksionon, dhe si pasojë nuk mund ta ndajmë këtë sistem në nënsisteme. Kjo është arsyeja pse nuk ekziston një mënyrë analize e përgjithshme e këtyre sistemeve jo lineare, fakt që bën të vështirë studimin e tyre.

Shumica e sistemeve fizike janë jo lineare. Por për shkak të vështirësisë në studim përdoret një procedurë për linearizimin e tyre [10]. Kjo procedurë përben heqjen e disa elementeve jo linear, kështu që sistemi me një lloj afërsie të konsiderohet linear. Sigurisht që ky thjeshtësim çon në zgjidhje të përafërta por të cilat përshkruajnë sjelljen e sistemit me saktësi të mjaftueshme.

2.2 Përshkrimi matematikor i sistemeve dinamike

Evoluimi kohor i një sistemi dinamik, mund të përshkruhet duke përdorur një sistem ekuacionesh diferenciale, numri i ekuacioneve është i barabartë me gradat e lirisë, domethënë me numrin e variablave të pavarura që përshkruajnë situatën e sistemit. Në qoftë se supozohen N ekuacione të tillë, atëherë evoluimi kohor i këtij sistemi do të paraqitet grafikisht në një hapësirë gjeometrike me N dimensione, R^N , që quhet *hapësira fazore* (phase space), dhe në shumicën e rasteve përshkruhet nga gjeometria Euklidiane. Vetia karakteristike e kësaj hapësire, është se çdo pikë e saj - e cila korrespondon në një vektor $\vec{X}(t)$ me N komponentë - përshkon totalisht situatën e sistemit

në çastin kohor t .

Në një përshkrim më gjeometrik, hapësira fazore përkufizohet nëpërmjet përdorimit të një bashkësi prej N akse, të cilët janë pingul me njëri tjetrin dhe përshkruajnë plotësisht situatën e sistemit. Duhet të theksohet se nuk ekziston një ligj i cili tregon mënyrën e ndërtimit të hapësirës fazore, por kjo bazohet nga parametrat e problemit në secilin rast. Për shembull në rastin e një pike materiale që lëviz në mënyrë të njëtrajtshme, hapësira fazore do të jetë dy-dimensionale ku aksi i parë do prezantojë shpejtësinë v dhe i dyti kohën t [11]. Por nuk ekziston asnjë kundërshtim në qoftë se zgjidhet pozicionin r dhe impulsi p .

Në rastin e një sistemi dinamik të vazhdueshëm, vektori i situatës $\vec{X}(t)$ që përshkruan situatën e sistemit në çastin kohor t do të jetë:

$$\vec{X}(t) = (x_1(t), x_2(t), x_3(t), \dots, x_N(t)) \quad (2.1)$$

kurse për sisteme diskrete, komponentët e vektorit varen vetëm nga vlerat diskrete të kohës t_n

$$\vec{X}(t_n) = (x_1(t_n), x_2(t_n), x_3(t_n), \dots, x_N(t_n)) \quad (2.2)$$

Një përkufizim tjetër matematikor që vektori i situatës $\vec{X}(t)$ është zgjidhje të ekuacionit diferencial të tipit të mëposhtëm

$$\frac{d\vec{X}(t)}{dt} = \vec{F}(\vec{X}, t) \quad (2.3)$$

i cili siç është thënë më parë, mund të transformohet në një sistem N ekuacionesh të rendit të parë. Ku sistemi i ekuacioneve do të ketë formën e mëposhtme:

$$\begin{aligned}\frac{dx_1}{dt} &= f_1(x_1, x_2, \dots, x_N) \\ \frac{dx_2}{dt} &= f_2(x_1, x_2, \dots, x_N) \\ &\vdots \\ \frac{dx_N}{dt} &= f_N(x_1, x_2, \dots, x_N)\end{aligned}$$

ku $\vec{F}(\vec{X}, t)$ është një *funksion vektorial* me parametra $(f_1, f_2, \dots, f_N)$. Duke supozuar që gjendja fillestare e sistemit përshkruhet nga vektori $\vec{X}(t_0) \equiv \vec{X}(t)|_{t=t_0}$, atëherë sistemi mund të karakterizohet si *deterministik*, ku problemi i kushteve fillestare:

$$\frac{d\vec{X}(t)}{dt} = \vec{F}(\vec{X}, t) \quad \vec{X}(t_0) \equiv \vec{X}(t)|_{t=t_0} \quad (2.4)$$

ka një zgjidhje të vetme. Sipas teoremës së unicitetit të zgjidhjes (*local existence and continuity theorem*) [9], në qoftë se $\vec{f}(\vec{x}, t)$ është i vazhdueshëm sipas kohës dhe respekton kushtin e Lipschitz

$$\|\vec{f}(\vec{x}, t) - \vec{f}(\vec{y}, t)\| \leq L|\vec{x} - \vec{y}| \quad (2.5)$$

në një zonë rrethuese të pikës $\vec{x}_0 = x_0^1, x_0^2, \dots, x_0^N$ e tillë që $\forall \vec{x}, \vec{y} \in B = \{\vec{x} \in R^n \mid \|\vec{x} - \vec{x}_0\| \leq r\} \quad \forall t \in [t_0, t_1]$, ekziston një $\delta > 0$, kështu që ekuacioni $\dot{\vec{x}} = \vec{F}(\vec{x}, t)$ me $\vec{X}(t_0) = \vec{X}_0$, ka vetëm një zgjidhje në intervalin $[t_0, t_0 + \delta]$.

Nga ana tjetër, sistemet dinamike diskrete, përshkruhen nga një ekuacion diferen-cash ose ekuacion rekurencash që ka formën e përgjithshme

$$\vec{X}_{n+1} = \vec{F}(\vec{X}_n) \quad (2.6)$$

e cila në analogji të plotë me rastin e mësipërm mund të analizohet në një sistem

ekuacionesh të tipit

$$\begin{aligned} x_1(t_{n+1}) &= f_1(x_1(t_n), x_2(t_n), \dots, x_N(t_n)) \\ x_2(t_{n+1}) &= f_2(x_1(t_n), x_2(t_n), \dots, x_N(t_n)) \\ &\dots \quad \dots \quad \dots \\ x_N(t_{n+1}) &= f_N(x_1(t_n), x_2(t_n), \dots, x_N(t_n)) \end{aligned}$$

ku përsëri, funksioni $\vec{F}$ është një funksion vektorial me parametra $(f_1, f_2, \dots, f_N)$.

Duke supozuar një pikë në hapësirën e fazës, $\vec{x}_0 \in D$, përkufizohet trajektoria pozitive e përshkrimit $\vec{F}$ nga pika $\vec{x}_0$, si sekuençë e pikave $(\vec{x}(k))_{k \geq 0}$, kështu që $\vec{x}_k = \vec{F}^k(\vec{x})$, ku

$$F^k = \underbrace{F \circ F \circ \dots \circ F}_{k \text{ herë}} \quad k \in N \quad (2.7)$$

Më shpesh paraqitja $\vec{F}$ është e kthyeshme, mund të përkufizohet dhe *trajektoria negative* të pikës $\vec{x}_0$, nga marrëdhënia $\vec{F}(\vec{x}_k) = \vec{x}_{k+1}$, për çdo numër të plot k më të vogël se zero, e cila është e barazvlefshme me ekuacionin e mëparshëm, në qoftë se $\vec{F}^{-k} = (\vec{F}^{-1})^k$, $\forall k > 0$. Trajektoria negative e pikës $\vec{x}_0$, simbolizohet me $(\vec{x}_k)_{k \in \mathbb{Z}}$. [12]

Bashkësitë e trajektoreve të cilat janë zgjidhje të ekuacioneve të lëvizjes së një sistemi dinamik, paraqiten grafikisht në portretizon fazor (phase portrait) të sistemit. Ky portret mund të ndërtohet, duke vizatuar trajektoret për një bashkësi të kushteve fillestare dhe në mënyrë të tillë që të mbulohet e gjitha hapësira fazore. Ekzistojnë shumë mënyra më të cilat mund të mund të riprodhohet këtë figurë, një nga më të njohurat është metoda izokline (isocline method). Për të kuptuar përdorimin e kësaj metode, duhet të përkufizohet pjerrësia e trajektores në çdo pikë $\vec{x}$ të hapësirës fazore, e cila për rastin e dy dimensioneve jepet nga shprehja:

$$s(\vec{x}) = \frac{f_2(x_1, x_2)}{f_1(x_1, x_2)} \quad (2.8)$$

Duke supozuar ekuacion 2.8 $s(\vec{x}) = c$, është e kuptueshme se marrëdhënia e mësipërme përkufizon një kurbë në planin (x_1, x_2) , gjatë së cilës, trajektorët e sistemit kanë pjerrësi c . Kjo do të thotë se çdo herë që një trajektore tenton atë kurbë në një pikë, pjerrësia e trajektores në atë pikë është e barabartë me c . Ajo që duhet të bëhet për të krijuar hapësirën fazore të sistemit, është vizatimi i kurbës $s(\vec{x}) = c$, dhe gjatë kësaj, të vizatohet pjesë të vogla të cilat do të jenë paralele midis tyre, që do të kenë pjerrësi të barabartë me c , dhe drejtimi i tyre do të përcaktohet nga shenja e funksioneve $f_1(\vec{x})$ dhe $f_2(\vec{x})$ në pikën $\vec{x}$. Kjo procedurë përsëritet disa herë për vlera të ndryshme të c -së, kështu që hapësira fazore të mbushet nga një bashkësi e kurbave të tilla. Në vazhdimësi, duke filluar nga pika fillestare $\vec{x}_0$, vizatohet trajektoria që fillon nga ajo pikë, duke lëvizur përgjatë drejtëzave të vogla nga një kurbë izokline në tjetrën. Në figurë 2.2 paraqitet portreti i fazave për lavjerësin e thjeshtë me fërkim.

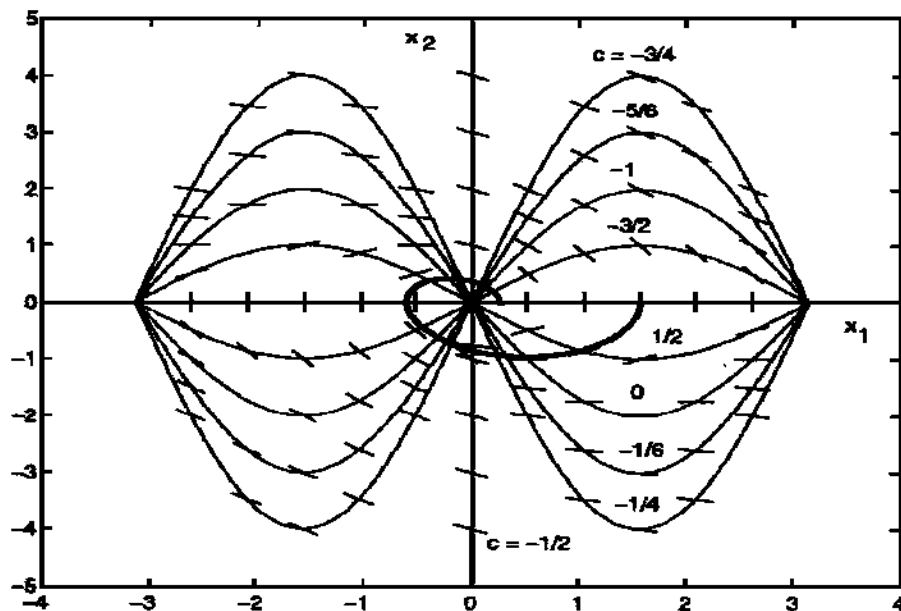


Figura 2.2: Portreti fazor për lavjerësin me fërkim [1]

Nuk është e vështirë të vihet re se në në figurën 2.2, dy trajektore të sistemit në

hapësirën fazore nuk kryqëzohen kurrë midis tyre. Kjo cilësi karakterizon çdo trajektore, e cila evoluon në hapësirën fazore duke mos u kryqëzuar kurrë me veten e saj. Kjo veti përshkruhet nga teorema e mos kryqëzimit të trajektores së sistemit (no intersection property) [9], [11], e cila është e pritshme, për shkak se çdo sistem në natyrë është deterministik dhe i bindet ligjit shkak-pasojë. Ashtu siç u përmënd dhe më sipër, gjendja e sistemit në çdo çast kohor, përshkruhet nga një pikë në hapësirën fazore. Kjo do të thotë se mënyra e evoluimit të sistemit në kohë varet plotësisht nga pozicioni aktual i sistemit në hapësirën fazore.

Në qoftë se supozojmë që kjo veti nuk ekziston domethënë që është e mundshme që dy trajektore të takohen në të njëjtën pikë të hapësirës fazore, atëherë në atë pikë, dy trajektoret do të karakterizoheshin nga të njëjtat vlerat për sa i përket variablave të sistemit dhe derivateve të tyre. Gjithsesi, nga kjo pikë evoluimi kohor i tyre do të ishte i ndryshëm. Kjo do të thotë se në qofte se sistemi ndodhet në të njëjtat kushte fillestare, do të ndjekë dy trajektore të ndryshme, ose ndryshe i njëjti shkak do të jepte pasoja të ndryshme. Kjo nuk mund të ndodhi në një sistem deterministik, ashtu siç janë të gjitha sistemet në natyrë, sepse do të kishte shkelje të marrëdhënie shkak - pasoje, sipas të cilës i njëjti shkak do të çoj gjithmonë në të njëjtën pasojë.

Një tjetër mënyrë për të vërtetuar vetinë e më sipërme, është më ndihmën e teoremës së zgjidhjes unike. Vërtet, në qoftë se funksionet $f_i(x)$ ($i = 1, 2, \dots, n$) të cilat përshkruajnë evoluimin kohor të sistemit dinamik në një hapësirë me n përmasa, janë të vazhdueshme sipas parametrave të tyre, të cilët janë edhe variablat që karakterizojnë gjendjen e këtij sistemi, atëherë nga çdo pikë e hapësirës fazore, do të kalojë vetëm një zgjidhje, domethënë një trajektore e vetme.

Duke përdorur përkufizimin e hapësirës fazore, mundet të klasifikojmë sistemet dinamike në dy kategori: në sistemet konservative (*conservative systems*) ku energjia e plotë qëndron konstante gjatë evoluimit kohor të tij dhe në sistemet me humbje (*dissipative systems*) evoluimi kohor i tyre karakterizohet midis të tjerave dhe nga hum-

bja e energjisë së përgjithshme, e cila me kalimin e kohës konvertohet në nxehtësi (shembull karakteristik i tij është lavjerësi më shuarje) [11]. Për të klasifikuar një sistem si konservativ ose jo, duhet të vëzhgojmë mënyrën e ndryshimit të një pjese të hapësirës fazore, gjatë evoluimit kohor të tij. Ashtu siç dihet nga fizika, trajektoret të cilat përshkruajnë sistemet në hapësirën fazore, kanë një lidhje me vlera karakteristike të energjisë së tij. Kjo do të thotë se, në qoftë se supozojmë një zonë të kësaj hapësire, kështu që $M \subset D$, e cila përmban një bashkësi nga pika, kjo zonë në sistemet konservative do të qëndrojë konstante me kalimin e kohës, përkundrazi në sistemet jo konservative, ajo zonë do të zvogëlohet deri sa të arrijë në formë gjeometrike e cila mund të përmbajë një ose më shumë pika. Në varësi të dimensionit në të cilën përkufizohet hapësira fazore, kjo zonë e hapësirës fazore mund të jetë një drejtëz, një sipërfaqe e planit, një volum ose një superstruktura me N përmasa. Në çdo rast mund të llogaritet volumi i kësaj strukture duke përdorur integralin Riemann.

$$V(M) = \int_M dx \quad dx = dx_1 dx_2 \dots dx_n \quad M \subset D \quad (2.9)$$

Meqenëse pikat të cilat përfshihen brenda volumit $V(M)$, lëvizin në hapësirën fazore gjatë aplikimit të paraqitjes F , volumi i superstrukturës e cila përmban këto pika, nuk ngelet konstant, por pëson dhe ai ndryshim në lidhje me kohën. Në qoftë se simbolizojmë me $M_k = F^k(M)$, zonën e hapësirës fazore e cila krijohet nga aplikimi nga paraqitja $\vec{F}$ mbi hapësirën M , k herë, dhe me $V_k = V(M_k)$, hapësirën e zonës M_k , vërtetohet se në çastin kohor $k+1$, volumi i kësaj zonë M_{k+1} , do jepet nga marrëdhënia

$$V_{k+1} = \int_{M_k} \left| \det \left(\frac{\partial \vec{F}}{\partial x}(x) \right) \right| dx \quad (2.10)$$

Ku $(\partial \vec{F})/(\partial x)(x)$, është matrica Jakobiane (Jacobian matrix) e paraqitjes $\vec{F}$ duke e llogaritur në pikën $\vec{x}$. Kjo matric përkufizohet si një matricë katrore me përmasa $N \times N$, ku N është dimensionin e hapësirës fazore, çdo element i kësaj matricë llogaritet

nga $a_{ij} = (\partial \vec{f}_i) / \partial x_j(x)$.

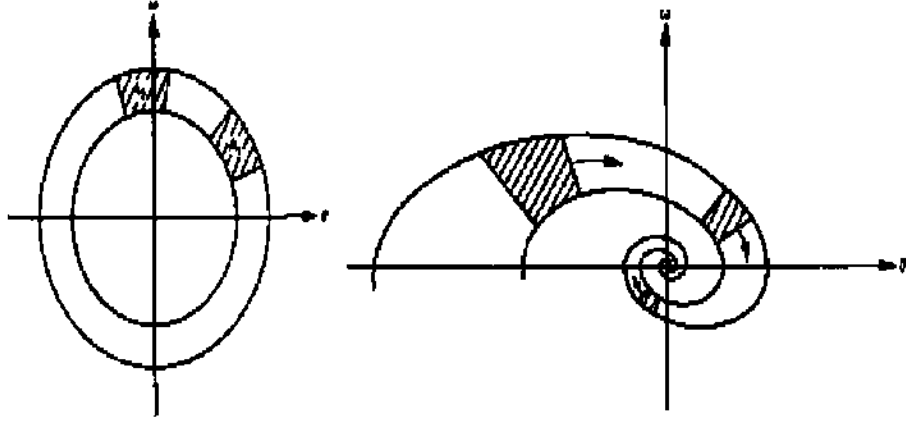


Figura 2.3: Shëmbull e një sistemi konservativë dhe sistemi me humbje [1]

Nga ekuacioni 2.10 mund të vërtetohet se në qoftë se zbatohet marrëdhënia:

$$\left| \det \left(\frac{\partial \vec{F}}{\partial x}(x) \right) \right| dx = 1 \quad (2.11)$$

sistemi është konservativ dhe karakterizohet nga ruajtja e volumit të zonës M në lidhje me kohën, domethënë do të jetë $V_{+1} = V_k$. Përndryshe në qoftë se:

$$\left| \det \left(\frac{\partial \vec{F}}{\partial x}(x) \right) \right| dx < 1 \quad (2.12)$$

kemi zvogëlim të këtij vëllimi me kalimin e kohës i cili shkon në një pikë të hapësirës fazore. Në këtë rast kemi marrëdhënien $V_{k+1} < V_k$ dhe sistemi karakterizohet si sistem jo konservativ.

2.3 Bifurkimi

Supozojmë sistemin e ekuacioneve diferenciale të sistemeve sipas një parametri μ :

$$\frac{d\vec{X}(t)}{dt} = \vec{F}(\vec{X}, \mu) \quad (2.13)$$

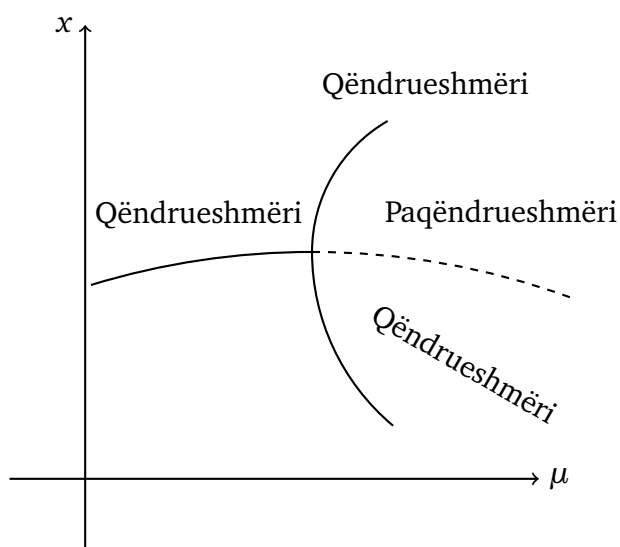


Figura 2.4: Bifurkimi Hopf

i cili varet nga parametri μ . Pikat e ekuilibrit, për të cilat matrica

$$a_{ij} = \left(\frac{\partial \vec{f}_i}{\partial x_j} \right)(x)$$

ka vlera vetjake të barabartë me zero, quhen si pikat e bifurkimit (bifurcation points) [13]. E thënë ndryshe, pikat e bifurkimit, janë vlerat e parametrave μ për të cilat ndryshon topologjia e hapësirës fazore dhe si rrjedhojë edhe sjellja e gjithë sistemit. Sot nga teoria janë të njohura disa grupe bifurkimi, të cilat parashtrohen në vazhdimësi.

2.3.1 Bifurkimi Hopf

Bifurkimi ose degëzimi Hopf shfaqet kur një pikë ekuilibri ndryshon nga i qëndrueshme në të paqëndrueshme dhe si rezultat lind një cikle limit i ri. Atëherë pjesa e qëndrueshme bëhet e paqëndrueshme dhe dy degë të reja të qëndrueshme krijohen. Në qarqet elektronike ky degëzim është lehtësisht i vrojtueshëm.

2.3.2 Bifurkimi i palosjes

Bifurkimi i palosjes (fold), rezulton kur një trajektore përkufizohet në një kanal të ngushtë. Si rezultat i këtij bifurkimi është shfaqja e dukurisë të shkëputjes (intermittency) dhe të krizës së brendshme (interior crisis). Në gjendjen e shkëputjes një sistem ndodhet midis gjendjes me periodë të gjatë dhe një relativisht të shkurtër me ndryshime të menjëhershme [14]. Një trajektore e qëndrueshme dhe një e paqëndrueshme afrohen midis tyre, me ndryshimin e parametrut të bifurkimit. Në krizën e brendshme madhësia e atraktorit në hapësirën fazore rritet menjëherë pasi parametri kalon për një vlerë kritike.

Bifurkimi i palosjes është më i njohuri në sistemet që shfaqin shumë atraktorë. Një shembull tipik i qarqeve elektronike, në të cilën shfaqet ky bifurkim është qarku Schmitt Trigger.

2.3.3 Bifurkim i menjëhershëm

Kur shfaqet dyfishimi i periodës (period doubling), atëherë bifurkimi quhet i menjëhershëm (flip bifurcation). Ky rast shfaqet vetëm kur zgjidhjet e sistemit të ekuacioneve diferenciale janë periodike. Atëherë në pikën e bifurkimit, një trajektore periodike me period T ndryshon në një tjetër me periodë $2T$. Një rast ku ndodh bifurkimi i menjëhershëm është tek sistemi Duffing.

2.4 Sisteme dinamike dhe kaos

Një nga vetitë kryesore të sistemeve dinamike, është parimi deterministik që ka të bëjë me evoluimin e tyre në kohë. Një sistem dinamik mund të konsiderohet si deterministik, vetëm kur gjendja e tij varet nga gjendjet e mëparshme. Në bazë të këtij përkufizimi arrihet konkluzioni që një sistem dinamik duke filluar nga e njëjta pikë do të përshkruajë gjithmonë të njëjtën trajektore.

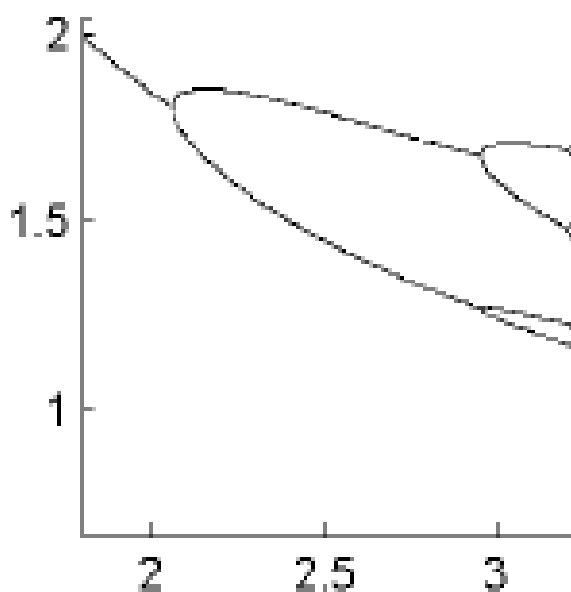


Figura 2.5: Bifurkimi i menjëhershëm në sistemin Duffing [2]

Ka raste kur në sistemet deterministike karakteristika e mësipërme nuk shfaqet. Një shembull tipik janë fenomenet meteorologjike, që edhe pse ndodhen brenda në një sistem deterministik është e pamundur të parashikohen në mënyrë afatgjate. Pa mundësia e parashikimit është karakteristikë që shfaqet në këto sisteme dhe përkufizohet si ndjeshmëri ndaj kushteve fillestare (sensitivity to initial conditions) [15].

Në bazë të këtij parimi në qoftë se një sistem fillon të evoluoj në kohë duke filluar nga kushte fillestare që kanë një diferencë të vogël, atëherë trajektorët e tij do divergjojnë nga njëra tjetra, dhe kështu evoluimi i tij kohor, do të jetë tërësisht ndryshe. Kjo është arsyeja pse keto sisteme të cilat janë të njohura si sisteme kaotike (chaotic systems) në fillim u karakterizuan si sisteme stokastike (stochastic systems) ose rastësore (random).

Një përkufizim i sistemeve kaotike është dhënë në një konferencë prestigjioze ndërkombëtare të organizuar nga Shoqëria Mbretërore (Royal Society) në Londër në vitin 1986.[16]

"Kaos është veprimi stokastik që shfaqet në një sistem deterministik."

Duke përmbledhur faktet e parashtruar më sipër, arrijmë në konkluzionin se një

sistem dinamik që të konsiderohet si sistem kaotik, duhet te karakterizohet nga tre kushte [8]:

- Të shfaqe sjellje aperiodike në lidhje me kohën (aperiodic time-asymptotic behavior). Kjo veti konsiston në shfaqjen e trajektoreve në hapësirën fazore, të cilat nuk duhet të shkojnë drejt pikave të caktuar ose në trajektore periodike. Për më tepër këto trajektore duhet të jenë të kufizuara (bounded), domethënë të ndodhen në një hapësirë të kufizuar të hapësirës fazore dhe të mos shtrihen deri në infinit.
- Të jetë deterministik, domethënë të mos ketë komponentë rastësor. Duke vendosur këtë përkufizim, sigurohet që në qoftë se vëzhgohen veprime të cilat mund të konsideroheshin si rastësore, atëherë ato në realitet burojnë në karakterin kaotik të sistemit dhe jo në faktorë rastësor, si për shembull zhurma.
- Të karakterizohet nga ndjeshmëria ndaj kushteve fillestare. Kjo do të thotë se dy trajektore të cilat fillojnë nga pika të afërta, largohen eksponencialisht në lidhje me kohën. Ky fakt nënkupton, ashtu siç do parashtrohet në vazhdimësi, ekzistencën e një eksponenti pozitiv Lyapunov.

Prezantimi i vetive kryesore të cilat karakterizojnë një sistem kaotik, na lejon të studiojmë mënyrat me anë të të cilave bëhet i mundur kalimi i sistemit nga një situatë jo kaotike në një situatë kaotike. Ky kalim bëhet nëpërmjet shumë mekanizmave të cilat emërtohen procedura tranzicioni në kaos (chaos transition mechanisms ose routes to chaos).

2.5 Kalimi në kaos

Çdo bifurkim mund të çojë sistemin drejt veprimit kaotik në qoftë se shfaqet në mënyrë të përsëritshme me ndryshimin e parametrin të degëzimit. Ku lloj kalimi në

kaos është shumë i rëndësishëm, sepse shumë herë nga të dhënat eksperimentale është e vështirë të kuptohet nëse sistemi vepron në mënyrë kaotike ose veprimi ndodh për shkak të zhurmës [17].

2.5.1 Kalimi në kaos me dyfishimin e periodës (period doubling)

Për herë të parë kjo dukuri u studiua teorikisht nga Mitchell Feigenbaum [18]. Kur ndodhin një seri nga degëzime të njëpasnjëshme të dyfishimit të periodës me ndryshimin e parametrut të degëzimit, atëherë sistemi hyn në gjendje kaotike. Për të ndodhur kjo është e domosdoshme një seri e pafundme e dyfishimit të periodës, që çon në një sistem trajektoria e të cilit ka një periodë infinite që zë një spektër të gjerë frekuencash. Dyfishimi i periodës është një mënyra më e zakonshme për kalimin e sistemit në një gjendje kaotike dhe përshkruhet matematikisht nga disa konstante të cilat nuk varen nga forma e ekuacioneve diferenciale.

2.5.2 Kalimi në kaos nëpërmjet shkëputjes (intermittency)

Kalimi në kaos nëpërmjet degëzimit të palosjes shfaqet me shumë mënyra, keto mënyra kanë si karakteristik të përbashkët kalimin e menjëhershëm nga një gjendje normale në atë kaotike. Mënyra më e zakonshme e shfaqjes së këtij kalimi në kaos është nëpërmjet shkëputjes (intermittency), rast i studiuar nga Manneville dhe Pomeau [19].

Në këtë rast, menjëherë pas bifurkimit trajektoria karakterizohet nga intervale të gjata të veprimit normal (laminar phases) dhe nga disa çaste veprimesh të parregullta. Perioda e lëkundjeve të sistemit është afërsisht e njëjtë me atë para bifurkimit. Për vlerën kritike të parametrut të degëzimit μ , për të cilën sistemi shkon në gjendje kaotike, intervalet e veprimit normal bëhen më të shkurtra ndërsa veprimet e parregullta shfaqen më shpesh.

2.5.3 Shembulli i bifurkimit në logistic map

Në vitin 1976 biologu Australian Robert May publikoi një artikull ku përshkruhet ecuria e popullsisë së një specie në një mjedis kompetitivë [20]. Popullsia e një specie mund të përshkruhet nga ekuacioni i mëposhtëm:

$$x_{n+1} = \alpha x_n(1 - x_n) \quad (2.14)$$

ku x_n është një numër midis zeros dhe njëshit, dhe përfaqëson raportin e popullsisë ekzistuese në vitin n me popullsinë maksimale, kurse α është një numër pozitiv që tregon raportin e riprodhimit.

Siç mund të konstatohet kur popullsia është e vogël riprodhimi është relativisht i madh. Përkundrazi kur popullsia është relativisht e madhe aftësia për riprodhim kufizohet për arsye të antagonizmit dhe të burimeve të kufizuara të mjedisit.

Më poshtë bëhet një analizë e parametrin α , duke ndryshuar parametrin α vëzhgojmë ecurinë e popullsisë (fig 2.6). Në qoftë se $0 \leq \alpha \leq 1$ atëherë popullsia do zhduket dhe nuk varet nga numri i saj fillestar. Në qoftë se $1 \leq \alpha \leq 2$ atëherë popullsia do të arrijë vlerën $\frac{\alpha-1}{\alpha}$. Për vlera $2 \leq \alpha \leq 3$ popullsia do të arrijë prapë të njëjtën vlerë por duke u luhatur rreth kësaj vlere për disa herë.

Në qoftë se vlera e parametrin α do jetë midis $3 \leq \alpha \leq 1 + \sqrt{6} \approx 3.44949$ pothuajse për çdo vlerë që do të kenë kushtet fillestare, popullsia do të luhetet midis dy vlerave të cilat varen nga vlera e parametrin α . Për vlera $3.44949 \leq \alpha \leq 354409$ si vihet re edhe nga Figura (2.6) për çdo vlerë fillestare të popullsisë do të ketë një luhatje midis katër vlerave. Në qoftë se vlera e parametrin α vazhdon të rritet atëherë numri i vlerave që mund të marrë popullsia behet 8, 16, 32 dhe në vazhdimësi.

Por një ndryshim mbi vlerën $\alpha > 3.56995$ do të ketë si pasoj futjen e sistemit në operim kaotik. Tani nuk mund të jetë i mundur dallimi i periodës se lëkundjes, dhe një ndryshim shume i vogël i vlerave fillestare të popullsisë mund të ndryshojë shume

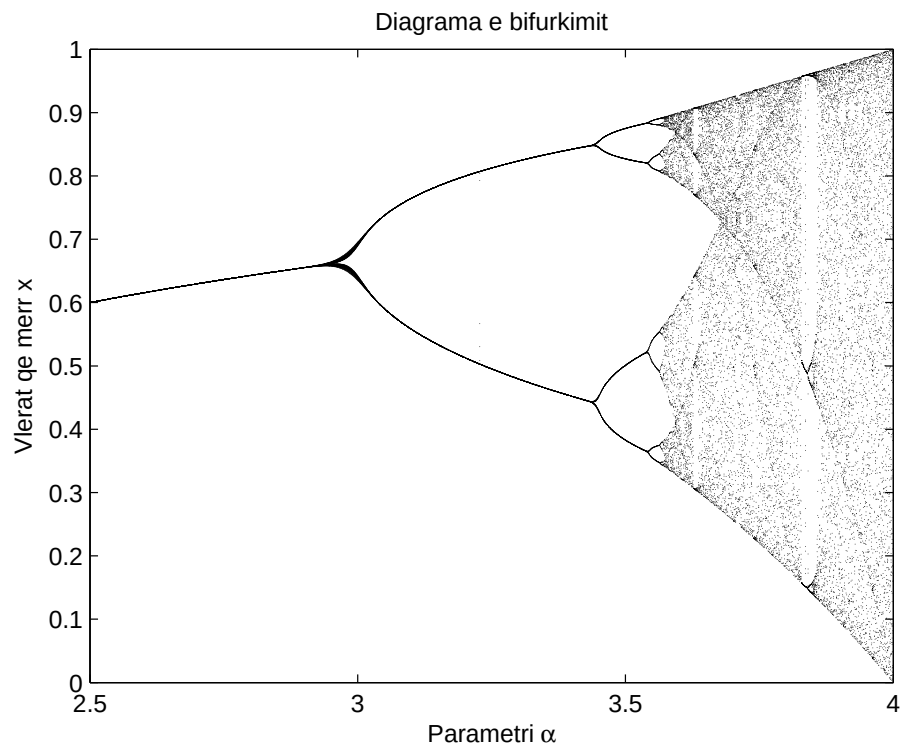


Figura 2.6: Paraqitja e bifurkimit në logistic map.

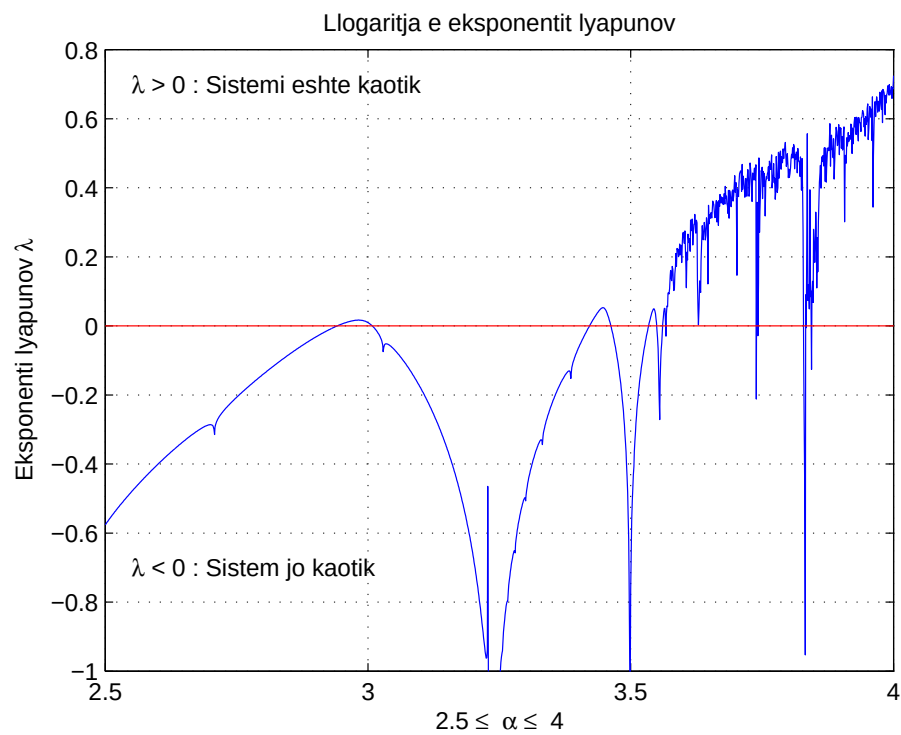


Figura 2.7: Llogaritja e eksponentit Lyapunov në logistic map.

vlerat përfundimtare që ajo merr.

2.6 Eksponenti Lyapunov

Tregues të cilët lidhen me ndjeshmërinë ndaj kushteve fillestare dhe qëndrueshmërinë ose jo të trajektoreve janë propozuar për qëllimin e matjes së shkallës së kaosit në sisteme të ndryshme. Një madhësi që lidhet me qëndrueshmërinë e gjendjeve të rregullta, kaotike ose gjysëm periodike është dhe eksponenti Lyapunov (Lyapunov Exponent) [21].

Eksponenti Lyapunov është një tregues i veprimit kaotik të një sistemi dinamik dhe lidhet me shmangien e trajektoreve të një atraktori në hapësirën fazore. Domethënë, eksponentët Lyapunov të një prezantimi përbëjnë një tregues të ndjeshmërisë ndaj kushteve fillestare, karakteristik kjo e veprimit kaotik në sistemet dinamike.

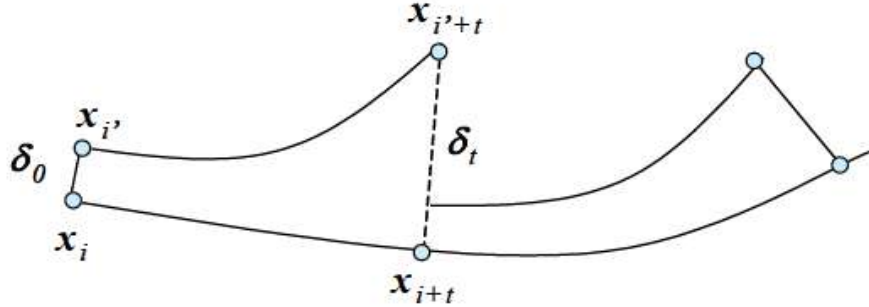


Figura 2.8: Paraqitja grafike e eksponentit Lyapunov për dy trajektore të cilat janë afër me njëra tjetrën

Në rastin e një prezantimi njëdimensional eksponenti Lyapunov, i cili simbolizohet me λ , llogaritet menjëherë. Në qoftë se një sistem mund të evoluojë në kohë dhe dy gjendje fillestare të ndryshme x dhe $x + \delta_0$, atëherë pas kohës t divergjenca e dy trajektoreve do të jetë:

$$\delta_t \cong \delta_0 e^{\lambda t} \quad \text{për } t \rightarrow \infty \quad (2.15)$$

ku, eksponenti Lyapunov λ tregon vlerën mesatare të shmangjes. Në qoftë se eksponenti λ është negativ, atëherë të dyja trajektoret do të konvergjojnë dhe ecuria e sistemit nuk do të çojë në kaos. Në qoftë se λ është pozitiv, atëherë trajektoret e afërta do të divergjojnë dhe ecuria e sistemit është e ndjeshme ndaj kushteve fillestare e cila çon në një operim kaotik të sistemit.

Si pasojë, eksponenti Lyapunov është një tregues i ritmit të hapjes ose të mbylljes të atraktorit në hapësirën fazore.

Gjendja	Eksponenti Lyapunov	
Gjendje ekuilibri	$\lambda_1 = 0$	$0 > \lambda_1 \geq \dots \geq \lambda_n$
Rreth limit	$\lambda_1 = 0$	$0 > \lambda_2 \geq \dots \geq \lambda_n$
Toroid	$\lambda_1 = \lambda_2 = 0$	$0 > \lambda_3 \geq \dots \geq \lambda_n$
Kaos	$\lambda_1 > 0$	$\sum_{i=1}^n \lambda_i < 0$

Tabela 2.1: Eksponentët Lyapunov të gjendjeve të mundshme të një sistemi dinamik.

2.6.1 Shembulli i bifurkimit dhe i kaosit

Më poshtë paraqitet një shembull se si llogaritet eksponenti Lyapunov për rastin e logistic map. Ashtu siç u tha më përpara logistic map është një sistem dinamik me një variabël i cili shprehet me anë të marrëdhënies 2.14. Në ekuacionin e mëposhtëm prezantohet formula me anë të së cilës llogaritet eksponenti Lyapunov:

$$\lambda = \frac{1}{N_t} \sum_{j=1}^N \ln \frac{\delta_{t,j}}{\delta_{0,j}} \quad (2.16)$$

Sipas marrëdhënies 2.16, eksponenti Lyapunov mund të llogaritet si vlera mesatare e raporteve të diferencave ashtu siç paraqitet më poshtë:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{dx_{n+1}}{dx_n} \right|$$

Duke aplikuar metodën e më lart përmëndur për të dhënat që kemi nga logistic map merret diagrama e figurës (2.7). Në këtë diagram paraqitet eksponenti Lyapunov

në lidhje me parametrin α . Në këtë diagram vihet re se kur parametri α ka vlerë $\alpha < 3.56995$ atëherë vlera e eksponentit Lyapunov është negative dhe sistemi nuk është në gjendje kaotike. Për vlera më të mëdha atëherë ai kalon në veprim kaotik. Kjo mund të vihet re dhe tek figura (2.6) ku shohim se bifurkimi në atë pik ka çuar sistemin në kaos.

Kapitulli 3

Seritë kohore

Në këtë kapitull paraqitet metoda e analizës së serive kohore, përkufizimi i serive kohore dhe paraqiten bazat matematikore të proceduarve që aplikohen për ti karakterizuar ato. Analiza jolineare e serive kohore përdoret për të vërtetuar në qoftë se qarqet elektronike të cilat paraqiten në kapitujt në vazhdim shfaqin dukurinë e kaos-it.

3.1 Paraqitja e serive kohore

Në shumicën e studimeve të fenomeneve që ndodhin në natyrë mundohemi të krijojmë modele të cilët shprehin lidhjen e madhësive që na interesojnë me madhësi të tjera. Këto modele mund të ndërtohen nga njohuritë që ekzistojnë rreth problemit i cili studiohet, domethënë nga marrëdhëniet që ekzistojnë midis madhësive, dhe quhen modele të parimeve themeltare (*first principles*).

Por në disa raste këto marrëdhënie nuk janë të njohura, atëherë studimi bazohet në vëzhgimet e këtyre madhësive dhe kryesisht matjeve. Këto modele bazohen tek eksperiencia dhe quhen modele të krijuara nga të dhënat (*empirical or data driven models*). Trajtimi i problemit nuk kërkon njohuri të thellë të tij, por analiza bazohet ekskluzivisht mbi të dhënat që kemi marrë. Si pasojë do kushtëzohemi në të dhënat e marra në kohë, domethënë në *serin kohore*. Objekti është analiza e serive kohore, që

konsiston në përdorimi e metodave të cilat na mundësojnë të studiojmë mekanizmin (procedurë rastësore ose sistem dinamik) nga i cili prodhohen ato, për të gjetur karakteristikat e tij, të ndërtojmë modelin dhe të bëjmë parashikime të ecurisë kohore të tij, domethënë të gjejmë vlerat pasardhëse të serisë kohore.

3.2 Metodat e analizave të serive kohore

Një seri kohore $\{x_i\}$ për $i = 1, 2, 3 \dots N$ mund të supozohet si rrjedhojë nga një sistem dinamik si vrojtimi x_i të çdo pike $\vec{s}_i$ të trajektores të sistemit, domethënë:

$$x_i = h(\vec{s}_i) \quad (3.1)$$

ku h është ekuacioni i projektimit $h : \mathbb{R}^d \mapsto C$ e cila quhet edhe *funksioni i vëzhgimit* (observation function). Në shumicën e rasteve seritë kohore janë zgjidhje të ekuacioneve diferenciale edhe pritjet të jenë të vazhdueshme në kohë. Sipas përkufizimit 3.1 seritë kohore janë diskrete, atëherë mëren kampione me një kohë kampionimi τ_s (sampling time) kështu që koha që korespondon në një vëzhgim x_i është it_s [22].

Duhet theksuar që ashtu siç në çdo matje që kryhet në një sistem edhe në sistemet dinamike ekzistojnë zhurma.

$$x_i = h(\vec{s}_i) + w_i \quad (3.2)$$

ku w_i mund të konsiderohet zhurma gaussiane, e cila nuk ka korrelacion me x_i por as me $\vec{s}_i$. [23]

3.3 Rindërtimi i hapësirës fazore

Nga përkufizimi i serisë kohore 3.1 u vu re se seria kohore është një vrojtım njëdimensional i një sistemi shumëdimensional. Ajo që kërkohet në analizën e serive kohore është të rindërtohet hapësira fazore në të cilën shfaqen të gjitha veçoritë e tërhe-

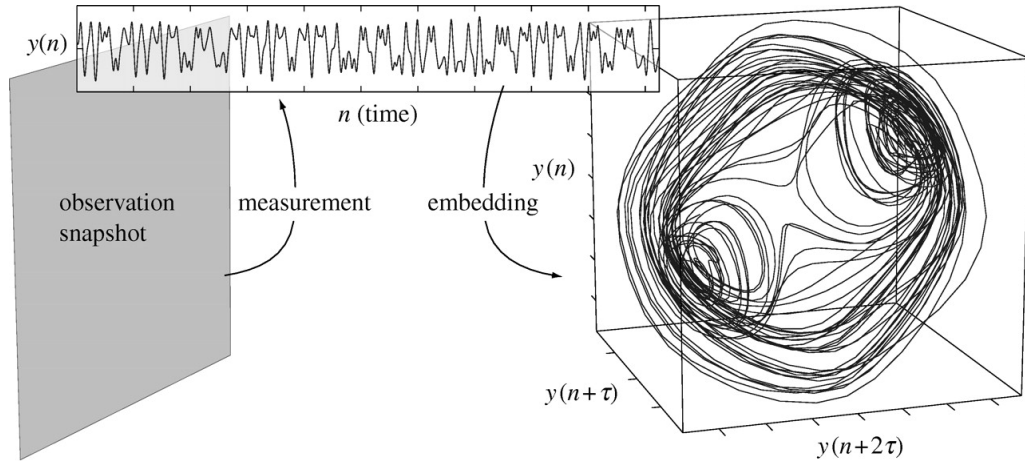


Figura 3.1: Paraqitja grafike e rindërtimit të hapësirës fazore [3]

qësit (attractor). Kjo është diçka e pamundur matematikisht, por nga ana tjetër ekziston mundësia për të rindërtuar një hapërire fazore e cila do të kthejë vrojtimin $\mathbb{R}$ në $\mathbb{R}^d$. Hapat e kësaj procedure shpjegohen më poshtë dhe do përdoren për të analizuar seritë kohore të mara nga qarqet të cilat do të paraqiten në kapitujt në vazhdim.

Teorema e Takens-it mundëson krijimin e një hapësire fazore, duke plotësuar disa kushte, me dimension m në të cilin trajektoret e rindërtuara $\{x_i\} \in \mathbb{R}^m$ nga seria kohore $\{x_i\}$, në të cilin tërheqësit (attractor) i rindërtuar ka të njëjtat veçori me tërheqësin origjinal. Kështu dhe sistemi dinamik i rindërtuar $x_{i+1} = \vec{F}(x_i)$ ka të njëjtat karakteristika me sistemin dinamik fillestar $s_{i+1} = f(s_i)$. [24]

Për tu rindërtuar hapësira fazore sipas teoremës së Takens, duhet të plotësohet kushti $m \geq 2D + 1$, ku D është dimensionin i fraktalitetit të tërheqësit (attractor) dhe m është dimensionin e hapësirës fazore të rindërtuar (fig. 3.1). Kjo ka ardhur si pasojë se dimensionin m i hapësirës fazore të rindërtuar nuk do të jetë mjaft i madh, atëherë tërheqësit (attractor) do të shfaqet me kryqëzime (intersections) dhe nuk do të jetë topologjikisht i barabartë me tërheqësin fillestar. Thekësohet se sistemet dinamike nuk mund të kenë dy ose më shumë zgjidhje për të njëjtin kushtin fillestar, kështu që dy trajektore nuk mund të takohen. [25]

Duhet të theksohet se në teoremën Takens, supozohet se seritë kohore duhet të

jenë pa zhurmë dhe të kenë një gjatësi kohore infinite. Në realitet këto kushte nuk plotësohen asnjëherë dhe rezultatet që dalin pas rikonstruksionit të hapësirës fazore mund të konsiderohen vetëm si të përafërta. [24]

Procedura e rikonstruksionit të hapësirës fazore behet me krijimin e pikave $\vec{x}_i \in \mathbb{R}^m$ nga seria kohore njëdimensionale $\{x_i\}$ për $i = 1, 2, \dots, N$. Metoda më e thjeshtë për tu bërë kjo është metoda e vonesave (methods of delay) dhe pikat x_i prodhohen nga:

$$\vec{x}_i = [x_i, x_{i-\tau}, \dots, x_{i-(m-1)\tau}] \quad (3.3)$$

ku m është *dimensioni i përfshirë* (embedding dimension) i hapësirës fazore e rindërtuar dhe tregon numrin e matjeve të serisë kohore për të krijuar një pikë, dhe ku τ është *vonesa* (delay), e cila përcakton diferencën kohore të matjeve të serisë kohore për të krijuar një vektor $\vec{x}_i$. Dritarja kohore që përcakton informacionin e kaluar nga seria kohore në çdo vektor $\vec{x}_i$ të hapësirës fazore të rindërtuar jepet nga:

$$\tau_w = (m - 1)\tau \quad (3.4)$$

ku τ_w quhet dhe dritarja e Theiler-it (Theifler Window) [26]. Për një rikonstruksion të saktë nuk duhet që kjo dritare të jetë shumë e vogël, ndryshe nuk do të përdoret informacion i mjaftueshëm, por njëkohësisht as shumë i madh, se ndryshe do të shfaqet informacion i panevojshëm.

Për një rindërtim sa më të saktë të hapësirës fazore duhen zgjedhur vlera të përshtatshme për parametrat m dhe τ . Në paragrafët në vazhdim prezantohen disa metoda për vlerësimin e këtyre parametrave.

3.4 Zgjedhja e vonesës τ

Zgjedhja e vonesës τ për rindërtimin e hapësirës fazore, është shumë e rëndësishme për suksesin e metodës, një zgjedhje e gabuar e vonesës τ do të çonte në një hapësirë fazore të gabuar e cila nuk do të përmbajnte të gjithë informacion. Si hap i parë duket i arsyeshëm për zgjedhjen e hapësirës fazore τ , vlera të vogla për të marrë trajektore të zbutura. Në qoftë se parametri τ është shumë i vogël atëherë, vlerat e njëpasnjëshme eksperimentale do të jenë të përafërta dhe do të jenë shumë afër në diagonalen kryesore të hapësirës fazore [8]

3.4.1 Llogaritja e autokoleracionit

Nga teoria e sinjaleve është e ditur se shkalla e korrelacionit r midis dy $x(t)$ dhe $y(t)$, llogaritet nga funksioni i korrelacionit (correlation function):

$$r = \frac{\overline{(x - \bar{x})(y - \bar{y})}}{\sigma_x \sigma_y} \quad (3.5)$$

ku simboli $\bar{x}$ shpreh vlerën mesatare të serisë kohore $x(t)$, kurse σ_x dhe σ_y janë devijimet standarte të dy serive kohore të cilat llogariten nga marrëdhëniet:

$$\sigma_x = \sqrt{\overline{(x - \bar{x})^2}} \quad \sigma_y = \sqrt{\overline{(y - \bar{y})^2}} \quad (3.6)$$

Në qoftë se si $y(t)$ merret seria kohore $x(t + \tau)$, e cila përmban kampione të $x(t)$ të cilët janë spostuar në kohë τ , atëherë funksioni i korrelacionit përkufizohet midis dy casteve të ndryshme të së njëjtës seri kohore, dhe quhet funksioni i autokorrelacionit (autocorrelation function) dhe jepet nga:

$$r(\tau) = \frac{\sum_{k=1}^N x(k)x(k + \tau)}{\sum_{k=1}^N |x(k)|^2} \quad (3.7)$$

Funksioni $r(t)$ ashtu siç jepet nga ekuacioni (3.7) merr vlerën e tij maksimale kur

$\tau = 0$. Mund të vërtetohet se në qoftë se seria kohore ka prejardhje nga një sistem kaotik ose rastësor atëherë forma e përgjithshme e $r(\tau)$ do të jetë:

$$r(\tau) = \alpha e^{-\tau/T} \quad (3.8)$$

ku α është vlera maksimale e autokorrelacionit e cila korenspondon për vlerën $\tau = 0$, kurse parametri T quhet koha e autokorrelacionit (autocorrelation time). Praktika e cila përdoret për zgjedhjen e parametrin τ është që ai të bëhet i barabartë me $\tau = T$, atëherë $r(\tau) = \alpha e^{-\tau/\tau} = \alpha/e$ kështu që vlera e optimale e vonesës kohore është kur vlera e autokorrelacionit bëhet $(1/e)$ e vlerës fillestare. [27]

3.4.2 Informacioni i përbashkët

Ndryshe nga funksioni i autokorelacionit i cili mat vartësinë lineare (linear dependence) të të dhënave të serisë kohore, funksioni i informacionit të përbashkët (mutual information) jep mundësinë e matjes të marrëdhënieve më të përgjithshme, e cila mund të aplikohet edhe në rastin e sistemeve dinamike.

Më konkretisht informacioni i përbashkët na lejon të përafërsojmë saktësinë e parashikimit të vlerës të $x(t + \tau)$ kur është e ditur vlera $x(t)$, dhe nga kjo pikëpamje, mat shkallën e korrelacionit midis këtyre dy kampioneve.

Për të përkufizuar informacionin e përbashkët le të supozojmë një seri kohore X me vlera $x_1, x_2, \dots, x_n$ dhe të prezantohet $P_x(x_1), P_x(x_2), \dots, P_x(x_n)$ probabiliteti i shfaqjes së tyre. Në këtë rast, entropia (entropy) H e sistemit do të përkufizohet si: [28]

$$H(X) = - \sum_{i=1}^n P_x(x_i) \log(P_x(x_i)) \quad (3.9)$$

Duke supozuar një seri kohore $Y = X(t + \tau)$, vlerat e të cilës $y_1, y_2, \dots, y_n$ janë marrë me një vonesë kohore τ nga seria kohore X (janë domethënë $y_i(t) = x_i(t + \tau)$ për $i = 1, 2, \dots, n$), atëherë mund të përkufizojmë informacionin e përbashkët si

një tregues të varësisë të serisë kohore Y , nga seria kohore X dhe anasjelltas. Për të llogaritur informacionin e përbashkët nga seritë kohore X dhe Y bëhen hapat e mëposhtme. Në fillim përkufizohet madhësia:

$$\begin{aligned} H(Y|x_i) &= - \sum_{j=1}^n P_{y|x}(y_j|x_i) \log[P_{y|x}(y_j|x_i)] \\ &= - \sum_{j=1}^n \frac{P_{xy}(x_i, y_j)}{P_x(x_i)} \log \left[\frac{P_{xy}(x_i, y_j)}{P_x(x_i)} \right] \end{aligned} \quad (3.10)$$

ku në marrëdhënien e mësipërme, $P_{y|x}(y_j|x_i)$ është probabiliteti i marrjes së vlerës y_j nga seria kohore Y duke ditur se në të njëjtin çast, seria kohore X ka vlerën x_i . Duke mbledhur probabilitetet e mësipërme për çdo x_i , do të kemi:

$$H(Y|X) = \sum_{i=1}^n P_x(x_i) H(Y|x_i) \quad (3.11)$$

ose e shprehur në një formë tjetër

$$H(Y|X) = \sum_{i=1}^n \sum_{j=1}^n P_{xy}(x_i, y_j) \log \left[\frac{P_{xy}(x_i, y_j)}{P_x(x_i)} \right] \quad (3.12)$$

që është pasiguria totale që ka të bëjë me procedurën e matjes së serisë kohore Y , kur është e dhënë seria X .

Mund të vërtetohet se:

$$H(Y|X) = H(X, Y) - H(Y) \quad (3.13)$$

ku $H(X, Y)$ jepet nga relacioni

$$H(X, Y) = \sum_{i=1}^n \sum_{j=1}^n P_{xy}(x_i, y_j) \log[P_{xy}(x_i, y_j)] \quad (3.14)$$

është pasiguria që ka të bëjë me probabilitetin (joint probability), kryhen matje në të

njëjtën kohë të serive kohore X dhe Y . Në rastin kur seritë kohore X dhe Y nuk kanë lidhje midis tyre kemi marrëdhënien:

$$H(X, Y) = H(X) + H(Y) \quad (3.15)$$

Informacioni i përbashkët (mutual information), përkufizohet si madhësia e informacionit që përfitohet nga seria kohore Y nga matja e serisë kohore X dhe anasjelltas, dhe jepet nga marrëdhënia:

$$I(X, Y) = H(Y) - H(Y|X) = H(Y) + H(X) - H(X, Y) = I(Y, X) \quad (3.16)$$

ose duke u bazuar nga (3.14), (3.12) dhe (3.15) nga

$$I(X, Y) = \sum_{i=1}^n \sum_{j=1}^n P_{xy}(x_i, y_j) \log \frac{P_{xy}(x_i, y_j)}{P_x(x_i)P_y(y_j)} \quad (3.17)$$

Sepse seria kohore $Y(t)$ ka një vonesë kohore τ nga seria $X(t)$, kuptohet se funksioni i informacionit të përbashkët $I(X, Y)$ është në varësi të vonesës kohore τ , domethënë është $I = I(\tau)$. Minimumi i informacionit të përbashkët $I(X, Y)$ tregon se kampionet e serisë Y dhe X , janë të pavarura midis tyre. Atëherë zgjedhim si vlerën optimale të vonesës kohore τ , atë vlerë që korespondon me minimumin e parë të informacionit të përbashkët [29].

3.5 Dimensioni i ngulitur m (emdedded dimendion)

Dimensioni i ngulitur m (emdedded dimension) përkufizon numrin e matjeve që bëhen komponent të vektorit të rindërtuar. Teorema Takens jep kushtin e nevojshëm për shmangejen e kryqëzimeve të atraktorit. Ky kush nuk është i mjaftueshëm dhe si rrjedhojë dimensionin m duhet të jetë sa më i vogël. Në qoftë se do të dinim dimensionin d të hapësirës Euklidiane në të cilën ndodhet atraktori, për dimensionin

e ngulitur m' duhet të plotësohet kushti:

$$2D + 1 \geq m' \geq d \quad (3.18)$$

Por sepse nuk janë të njohura d dhe D atëherë nuk ekzistojnë të dhëna për zgjedhjen e m . Një metodë e cila përdoret për gjetjen e m' është metoda e të afërmeve të remë (method of false nearest neighbors, FNN). Më poshtë prezantohet metoda e të afërmeve të remë për gjetjen e dimensionit të ngulitur. [30]

3.5.1 Të afërmit e rremë

Një atraktor, si dhe çdo objekt tjetër gjeometrik, karakterizohet nga dimensionin e tij në hapësirën Euklidiane e cila përmban atraktorin (për shembull për hapësirën e rindërtuar është dimensionin e ngulitur (embedded dimension m)). Një metodë që përdoret për të gjetur dimensionin m , bazohet në studimin e karakteristikave gjeometrike të atraktorit, gjatë ndërtimit të tij në hapësira fazore duke rritur dimensionin e tyre. Ashtu siç u tha dhe më sipër në qoftë se dimensionin do të jetë i vogël atëherë atraktori do të takoj veten e vet, që do të thotë se pika të atraktorit real do të shfaqeshin në pozicione shumë të afërta, kur në realitet ato ndodhen shumë larg midis tyre. Dimensionin e ngulitur m (embedded dimension) do të jetë ai që zvogëlon përqindjen e fqinjëve të rremë (FNN) në më pak se 0.1%. Përqindja e të afërmeve të remë llogaritet nga marrëdhënia më poshtë:

$$P = \frac{\|\vec{X}_i(m+1) - \vec{X}_j(m+1)\|}{\|\vec{X}_i(m) - \vec{X}_j(m)\|} \quad (3.19)$$

Metoda të ndryshme janë përdorur për të diferencuar zhurmën nga një sinjal kaotik deterministik. Një nga metodat që përdoren më shumë është ajo e paraqitjes së shpërndarjes së të afërmeve më të afërt. Kjo paraqitje grafike bën të mundur dallimin midis zhurmës nga matejet dhe të sinjalit kaotik deterministik. [31]

3.6 Spektri i Fuqisë

Mënyra më e thjeshtë për të karakterizuar një sinjal i cili prodhohet nga një sistem dinamik, si periodik ose kaotik, është duke përdorur spektrin e fuqisë (power spectrum) [32]. Spektri i fuqisë është katror i amplitudës të transformimit Fourier të serisë kohore të sinjalit. Transformimi Fourie i sinjalit $x(t)$ jepet nga marrëdhënia më poshtë:

$$X(\omega) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T x(t) e^{-j\omega t} dt \quad (3.20)$$

dhe spektri i fuqisë jepet nga marrëdhënia:

$$S(\omega) = |X(\omega)|^2 = \lim_{T \rightarrow \infty} \frac{1}{T} \left| \int_0^T x(t) e^{-j\omega t} dt \right|^2 \quad (3.21)$$

Rastet e spektrit dallohen në lidhje me gjendjen e sistemit dhe pasqyrohen më poshtë:

- Në rastin kur sinjali është periodik, atëherë spektri i fuqis përmban maksimume të dallueshme që korrespondojnë me frekuencën themeltare ω_0 të zgjidhjes periodike dhe të harmonikëve me frekuencë më të lartë. Spektri i fuqis ndryshon në bifurkimet e dyfishimit të periodës dhe atëherë krijohet një maksimum me frekuencë $\omega/2$. E njëjta gjë ndodh edhe për çdo bifurkim tjetër.
- Për sinjalin pseudoperiodik, spektri i fuqisë përbëhet përsëri nga maksimume të dallueshme që në këtë rast korrespondojnë në të gjitha frekuencat që përmbajnë sinjalin.
- Për sinjalet periodike spektri i fuqis është i vazhdueshëm dhe shoqërohet nga maksimumet e frekuencave dominuese.

Gjithashtu duhet theksuar se pavarësisht nga dobia e tyre, spektrat e fuqisë nuk duhet të përdoren si e vetmja mënyrë për të verifikuar sjelljen e një sistemi dinamik.

Më konkretisht për sa i përket karakteristikave të sistemeve kaotike mundet që spektri i vazhdueshëm i fuqisë të shfaqet për arsye të prezencës së zhurmës në sinjal.

Pjesa II

Pjesa e dytë

Kapitulli 4

Prania e kaos-it në qarqet elektronike

Dekadën e fundit po tregohet një interes i madh në fushën e dinamikës të qarqeve elektrike dhe elektronike jo-lineare. Qarqet elektrike dhe elektronike janë një grup sistemesh ku vëzhgimet dhe matjet mund të bëhen lehtësisht. Specifikisht për projektuesit dhe për shkencëtarët jepet mundësia e simulimit të operimit të këtyre sistemeve duke përdorur programe kompjuterike, si SPICE.

Prania e dukurisë së kaosit në qarqet elektronike është vërtetuar eksperimentalisht. Në këtë kapitull paraqitet qarku i Chua-s i cili u realizua me një topologji të re dhe u prezantua në vitin 1983 [33]. Gjithashtu paraqiten dhe disa qarqe jolineare të cilat u propozuan nga autori.

4.1 Qarku i Chua-s

Qarku i Chua-s, i cili prezantohet në figurën 4.1 është një qark jolinear i cili ende është objekt i studimi [34]. Qarku përbëhet nga katër komponentë linearë, (dy kondensator, një bobinë dhe një rezistencë) dhe një rezistencë jo lineare e cila quhet diodë Chua e cila mund të realizohet në laborator duke përdorur komponentë të thjeshtë elektronik.

Rezistenca jo-lineare është parametri kryesor i operimit të qarkut në mënyrë kaotike.

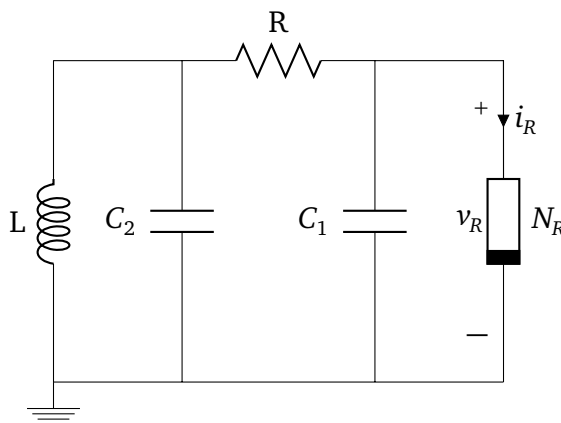
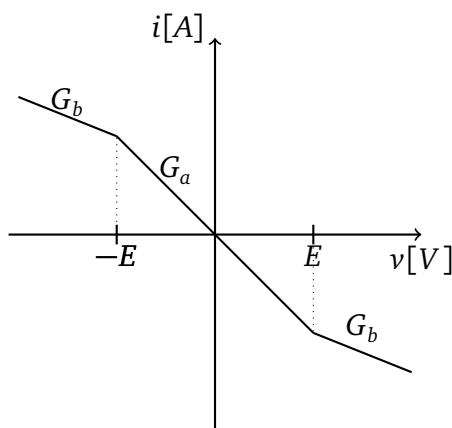


Figura 4.1: Qarku i Chua-s i cili studiohet në këtë kapitull

Karakteristika e rezistencës jolineare shfaqet në figurën 4.2. Siç mund të shihet edhe nga figura 4.1 qarku i Chua-s nuk është gjë tjetër se një oshilator RLC pa prezencën e rezistencës jolineare. Rezistenca jolineare përbëhet nga pjesë lineare ashtu siç shihet edhe në figurën 4.2.


 Figura 4.2: Rezistenca jo-lineare N_R që është parametri kryesor i paraqitjes të dukurisë së kaosit.

Në realitet diferenca e potencialit midis skajeve të kondensatorit C_1 është gjithmonë me e vogël se sa E , fakt i cili duhet marrë parasysh në projektimin e karakteristikes $v - i$. Supozojmë se vlerat e parametrave janë zgjedhur me këtë mënyrë, që drejtëza e ngarkesës, e cila ka pjerrësi $-1/R$, të takohet me karakteristikën në tre pika, kështu që qarku të ketë tre pika ekuilibri. Pika e parë do të jetë në fillimin e boshteve, me përçueshmëri negative G_a dhe dy pikat e tjerë do të jenë në pjesën e jashtme me

përçueshmëri negative G_b . Të tre pikat e ekuilibrit janë të pa qëndrueshme sepse korrespondojnë me pika të përçueshmërisë negative.

4.1.1 Modeli matematikor i qarkut të Chua's

Në këtë paragraf do të paraqitet ndërtimi i ekuacioneve diferenciale të cilat përshkruaj sjelljen e qarkut Chua. Në vazhdimësi do të paraqitet rezultatet e simulimit nga programi i simulimeve të qarqeve elektrtonike Multisimi dhe do kryhet krahasimi i kësaj zgjidhje me zgjidhjen numerike të ekuacioneve duke përdorur programin MATLAB.

Duke aplikuar rregullat e Kirkofit te qarku i figurës 4.1 merren ekuacionet diferenciale 4.1 të cilat përshkruajnë dinamikën e qarkut[35].

$$\begin{aligned} C_1 \frac{dv_1}{dt} &= \frac{v_2 - v_1}{R} - h(v_1) \\ C_2 \frac{dv_2}{dt} &= \frac{v_1 - v_2}{R} + i_L \\ L \frac{di_L}{dt} &= -v_2 \end{aligned} \quad (4.1)$$

Ku v_1 nënkupton diferencën e potencialit midis skajeve të kondensatorit C_1 , v_2 diferencën e potencialit midis kondensatorit C_2 , i_L korrenti që përshkruan bobinën, C_1 dhe C_2 janë kapacitet e kondensatorëve përkatës. Duhet theksuar që $h(v_1)$ është rezistenca jolineare e qarkut.

Karakteristika tension-rrymë e kësaj rezistence paraqitet në Fig. 4.2 dhe shprehet nga ekuacioni (4.2):

$$h(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \quad (4.2)$$

ku G_a dhe G_b janë pjerrësitë përkatëse të pjesës së brendshme dhe të jashtme, ashtu siç paraqiten tek Figura 4.13, të cilat në rastin tonë janë negative kurse me E tregohen

pikat e dallimit [34].

Pikat e ekuilibrit të qarkut do të llogariten sipas zgjidhjes së ekuacioneve

$$\frac{di_L}{dt} = 0 \quad (4.3)$$

$$\frac{dv_2}{dt} = 0 \quad (4.4)$$

$$\frac{dv_1}{dt} = 0 \quad (4.5)$$

ekuacionet (4.3), (4.4) dhe (4.5) mund të shkruhen duke marrë parasysh (4.1)

$$0 = \frac{v_2 - v_1}{R} - h(v_1) \quad (4.6)$$

$$0 = \frac{v_1 - v_2}{R} + i_L \quad (4.7)$$

$$0 = -v_2 \quad (4.8)$$

dhe përfundimisht rezulton se $v_2 = 0$ dhe që :

$$i_L = -\frac{1}{R}v_1 \quad (4.9)$$

$$h(v_1) = -\frac{1}{R}v_1 \quad (4.10)$$

Kjo procedurë është e barasvlershme me analizën *DC* të qarkut, në të cilën supozojmë kondensatorët si qark të hapur, kurse bobinën si qark të mbyllur. Ekuacionet (4.9) dhe (4.10) përkufizojnë drejtëzën e ngarkesës e cila ka pjerrësi negative $G = -1/R$ por njëkohësisht duhet të plotësohen edhe marrëdhëniet (4.2) kështu që pikat e ekuilibrit mund të dalin edhe nga ekuacionet diferenciale (4.1) ose mënyrë grafike duke përdorur figurën 4.2.

4.1.2 Realizimi i rezistencës jo lineare

Ekzistojnë shumë mënyra për të ndërtuar një rezistencë negative, njëra nga këto është lidhja e tre rezistencave pozitive në një burim tensioni i kontrolluar nga tension (Voltage-Controlled Voltage Source VCVS). Një qarkë i tillë është i realizueshëm nëpërmjet një amplifikatori operacional. [4]

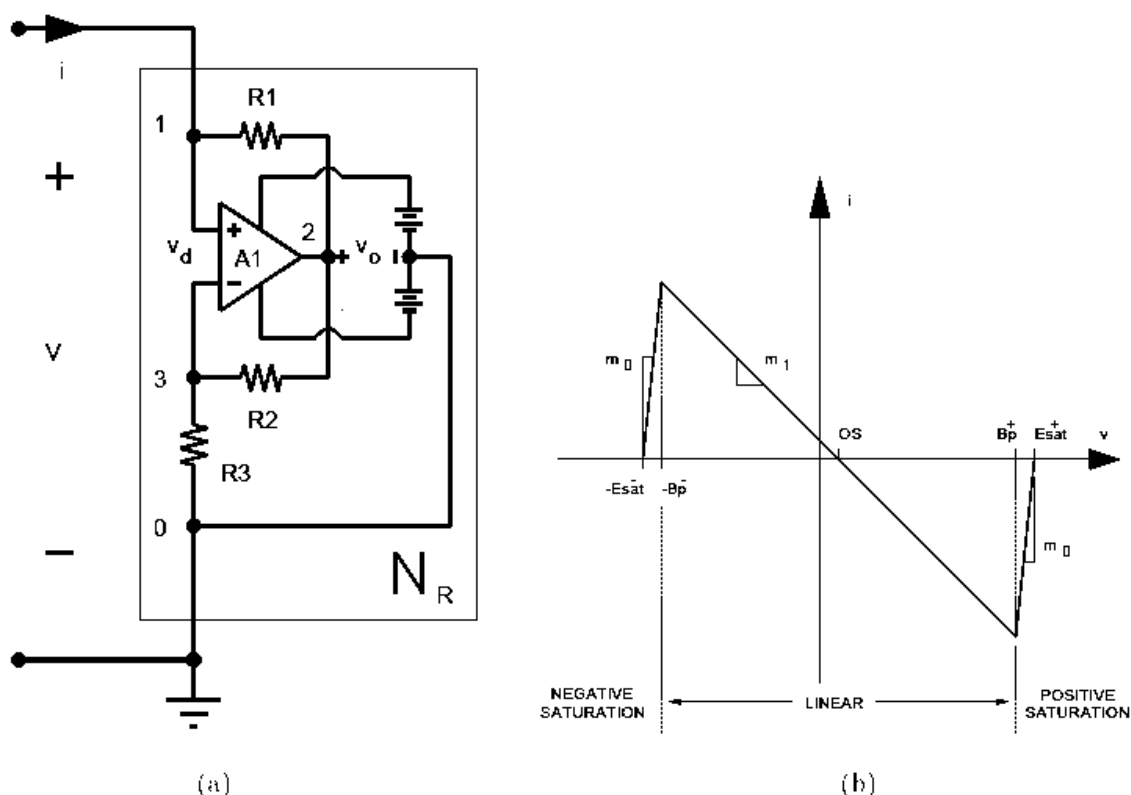


Figura 4.3: Realizimi i rezistencës jolineare të qarkut Chua [4]

Aplikohet ligji i parë i Kirkofit për nyjen (1) e paraqitur në figurë 4.3, për arsye të rezistencës të madhe të hyrjes të amplifikatorit operacional rryma që futet në të supozohet barabartë me zero, atëherë do kemi:

$$i = \frac{1}{R_1}(v - v_o) \quad (4.11)$$

Aplikohet ligji i dyte i Kirkofit për konturin 1-3-0-1 dhe kemi:

$$v = v_d + \left[\frac{R_3}{R_2 + R_3} \right] v_o \quad (4.12)$$

Duke ditur që për amplifikatorin operacional ekziston marrëdhënia:

$$v_o = Av_d \quad (4.13)$$

Atëherë nga ekuacionet 4.13 dhe 4.12 do të jetë:

$$\begin{aligned} v &= \frac{v_o}{A} + \left[\frac{R_3}{R_2 + R_3} \right] v_o \\ &= \frac{(R_2 + R_3)}{A(R_2 + R_3)} v_o + \left[\frac{A}{A} \frac{R_3}{R_2 + R_3} \right] v_o \\ &= \left[\frac{R_2 + (A + 1)R_3}{A(R_2 + R_3)} \right] v_o \end{aligned}$$

ose ndryshe

$$v_o = \left[\frac{A(R_2 + R_3)}{R_2 + (A + 1)R_3} \right] v \quad (4.14)$$

dhe duke zvendësuar ekuacioni e mësipërm tek ekuacioni 4.11 do të kemi:

$$\begin{aligned} i &= \frac{1}{R_1} \left(v - \left[\frac{A(R_2 + R_3)}{R_2 + (A + 1)R_3} \right] v \right) \\ &= \frac{1}{R_1} \frac{R_2 + (1 + A)R_3 - A(R_2 + R_3)}{R_2 + (1 + A)R_3} v \\ &= \frac{R_2 + R_3 + AR_3 - AR_2 - AR_3}{[R_2 + (1 + A)R_3]} v \\ &= \left[\frac{(1 - A)R_2 + R_3}{R_1[R_2 + (1 + A)R_3]} \right] v \end{aligned}$$

Për amplifikatorët operacional dimë se A është shumë i madhë, atëherë gjejmë limitin e shprehjes së mësipërme për $A \rightarrow \infty$

$$i \approx - \left[\frac{R_2}{R_1 R_3} \right] v$$

Dhe për më tej në qoftë se zgjidhet $R_1 = R_2$ atëherë:

$$i \approx -\frac{1}{R_3}v$$

Kur amplifikatori operacional ndodhet në saturim pozitiv

Amplifikatori operacional ndodhet në saturim(ngopje) kur:

$$v_d \geq \frac{E_{sat}^+}{A}$$

Sipas ekuacionit të mësipërm dhe eq:nr2 duke marrë parasysh se $v_o = E_{sat}^+$ do të kemi :

$$\begin{aligned} v &\geq \frac{E_{sat}^+}{A} + \frac{R_3}{R_2 + R_3} E_{sat}^+ \\ &\geq \frac{R_2 + (1 + A)R_3}{A(R_2 + R_3)} E_{sat}^+ \end{aligned}$$

Dhe pika e thyerjes do të jetë:

$$B_p^+ = \frac{E_{sat}^+}{A} + \frac{R_3}{R_2 + R_3} E_{sat}^+$$

Kur amplifikatori operacional ndodhet në saturim negativ

Amplifikatori operacional ndodhet në saturim(ngopje) kur:

$$v_d \leq \frac{E_{sat}^-}{A}$$

Sipas ekuacionit të mësipërm dhe eq:nr2 duke marrë parasysh se $v_o = E_{sat}^-$ do të

kemi :

$$\begin{aligned} v &\leq \frac{E_{sat}^-}{A} + \frac{R_3}{R_2 + R_3} E_{sat}^- \\ &\leq \frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} E_{sat}^- \end{aligned}$$

Dhe pika e thyerjes do të jetë:

$$B_p^- = \frac{E_{sat}^-}{A} + \frac{R_3}{R_2 + R_3} E_{sat}^-$$

Për të ndërtuar rezistenca negative e paraqitur në figurën 4.2 për të krijuar tre pika të paqëndrueshme duhen përdorur një konfigurim me dy rezistenca të paraqitura në qarkun 4.3 në lidhje paralele. Qarku i plotë paraqitet në figurën ??.

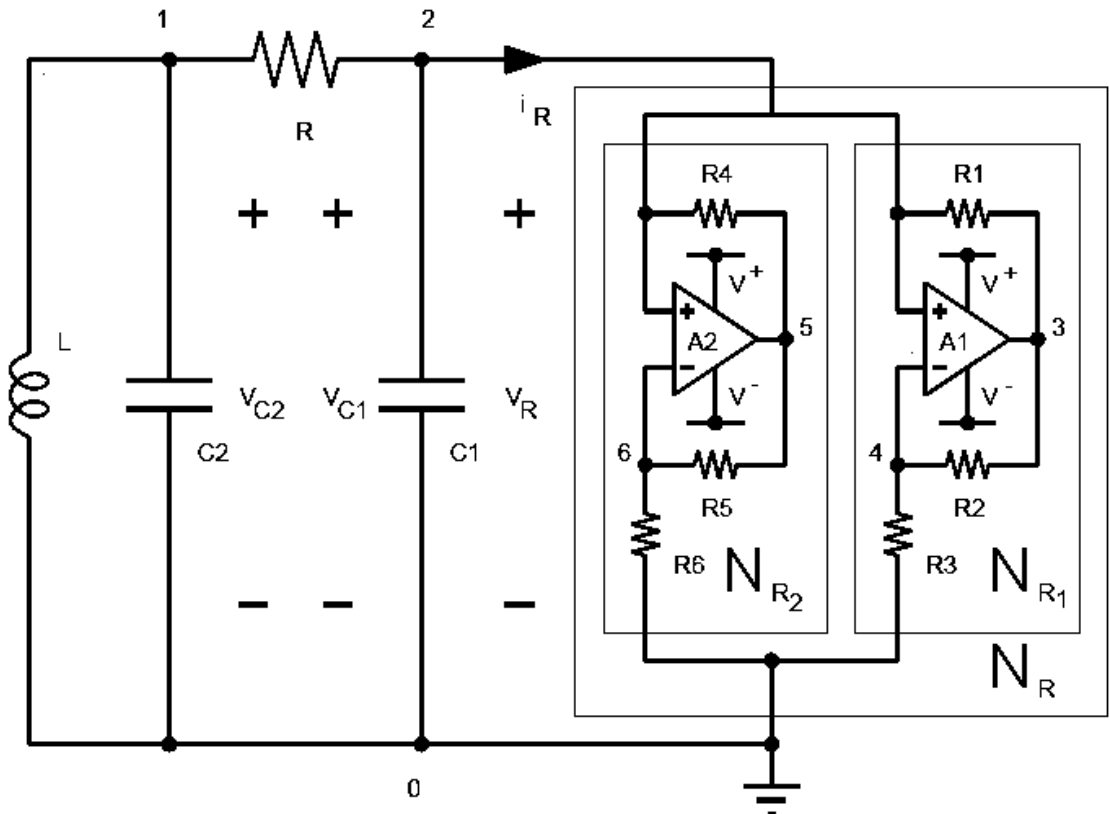


Figura 4.4: Realizimi i qarkut të plotë Chua [4]

4.1.3 Realizimi i qarkut të Chua's në Multisim

Pasi është bërë analiza teorike e qarkut të Chua-s, paraqitet simulimi i tij i cili u bë i mundur duke përdorur dy metoda të ndryshme.

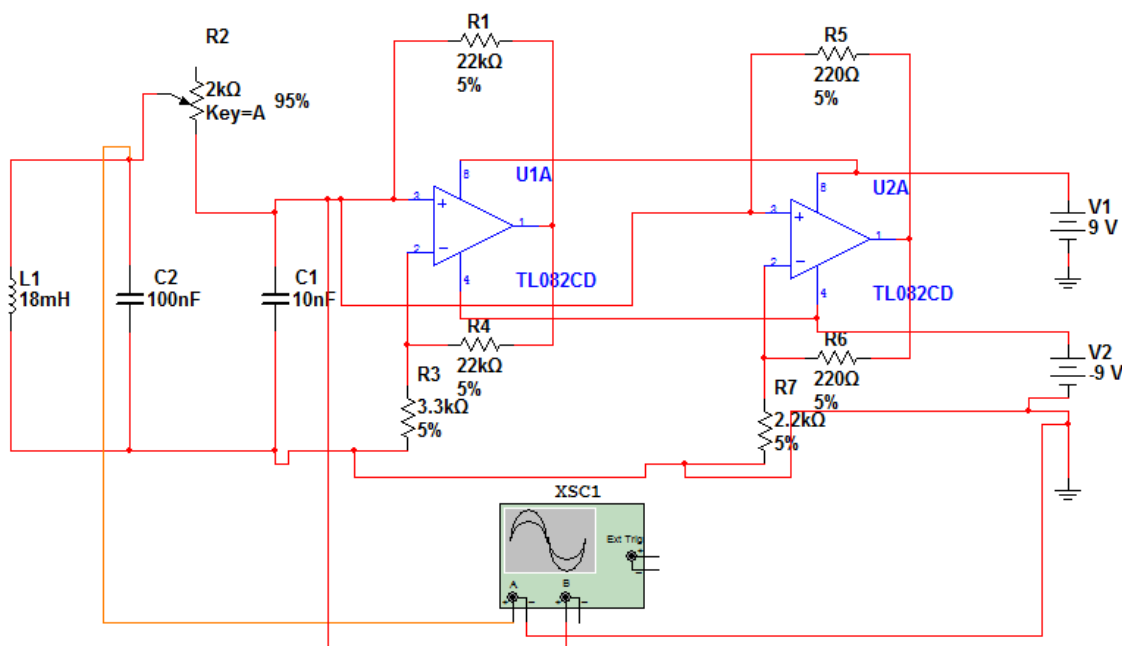


Figura 4.5: Qarku elektronik i cili përdoret për të simuluar sistemin e Chua-s

Si fillim u përdor programi kompjuterik Multisim i cili përdoret për simulime të qarqeve elektronike dhe në vazhdimësi mjedisi programues MATLAB i cili ka të integruar procedurë të integritit numerik dhe të zgjidhjes së ekuacioneve diferenciale. Programi Multisim ofron një implementim të qarkut me mënyra që i përafrohen botës reale dhe si rezultat është shumë i thjeshtë për tu përdorur.

Skema elektronike që u përdor tregohet në figurën 4.5. Për të krijuar rezistencën jolineare është përdorur amplifikatori operacional (TL082) të cilat ofrojnë një përforcim të madh dhe zhurma të cilën prodhojnë është e ulët [36].

Komponentët që janë zgjedhur për të realizuar simulimin e qarkut paraqiten tek tabela 4.1.

Duhet të theksohet se qarku i Chua-s është një qark autonom, kjo do të thotë që nuk duhet ndonjë sinjali i jashtëm që ai të operojë në mënyrë kaotike. Ajo që na intereson

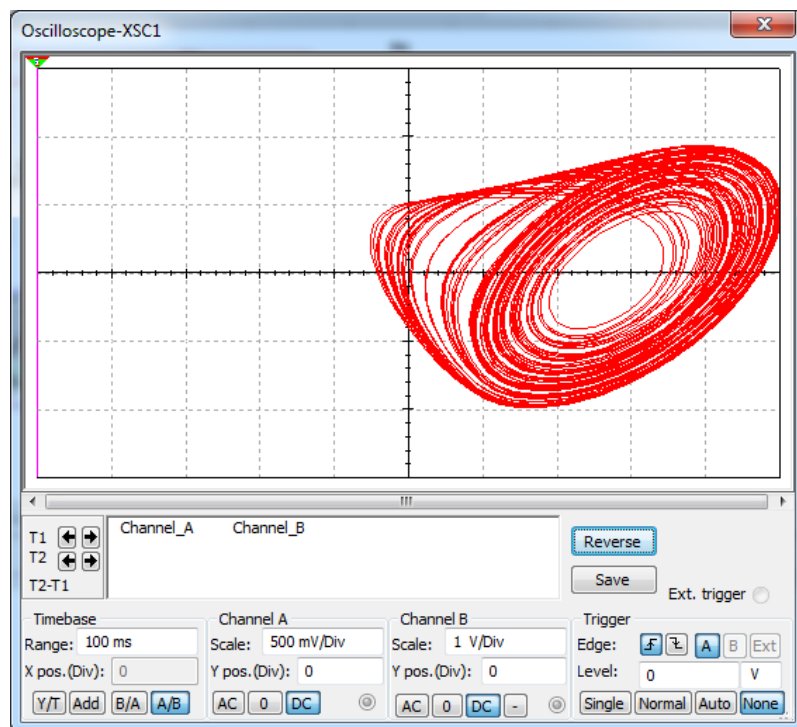


Figura 4.6: Hapësira fazore e atraktorit të Chua-s pas simulimit me $R_2 = 1.72$

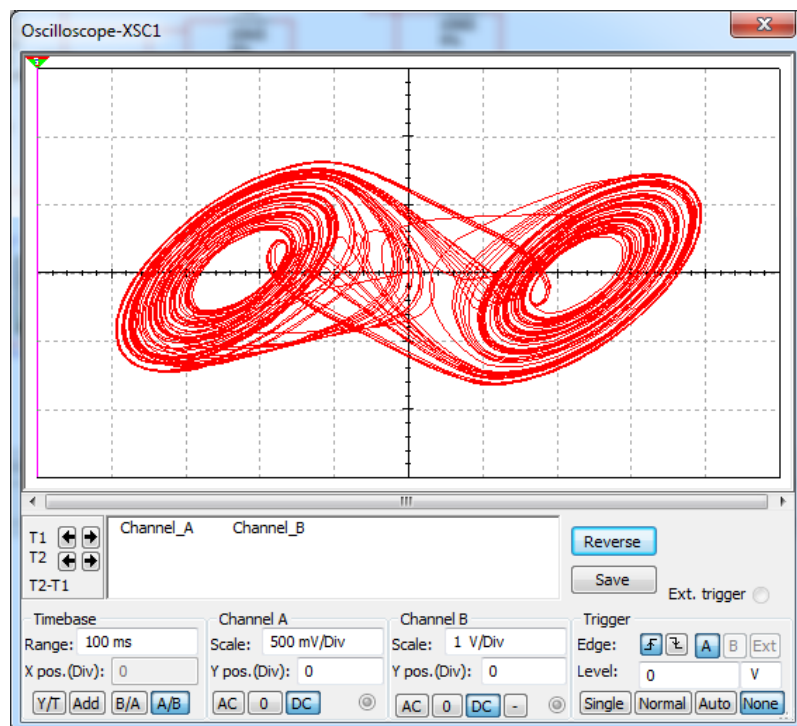


Figura 4.7: Atraktori i plotë i sistemit të Chua-s i cili realizohet me rezistencën $R_2 = 1.9 k\Omega$

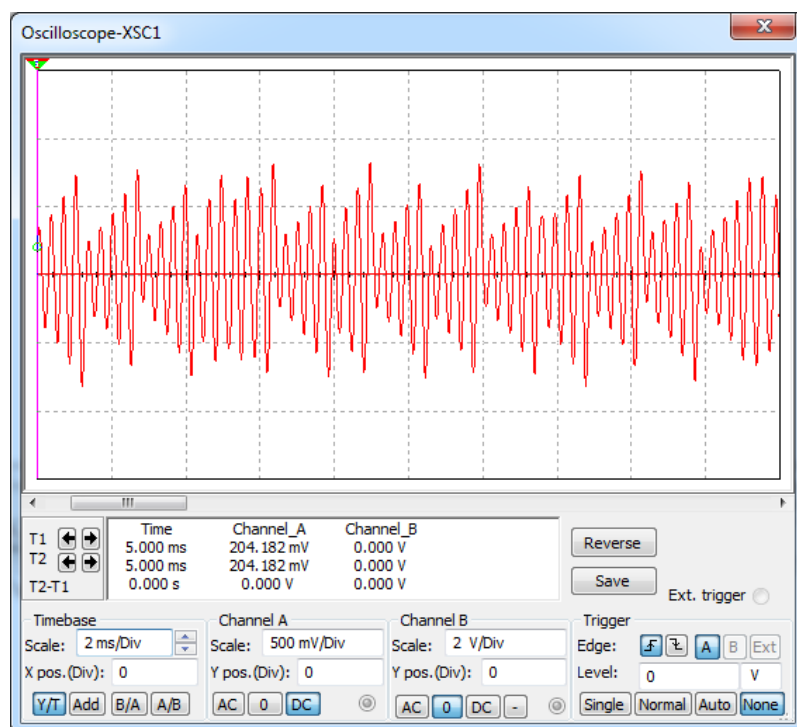


Figura 4.8: Singali kaotik që merret në C_2 pas simulimit me rezistencën $R_2 = 1.9 k\Omega$

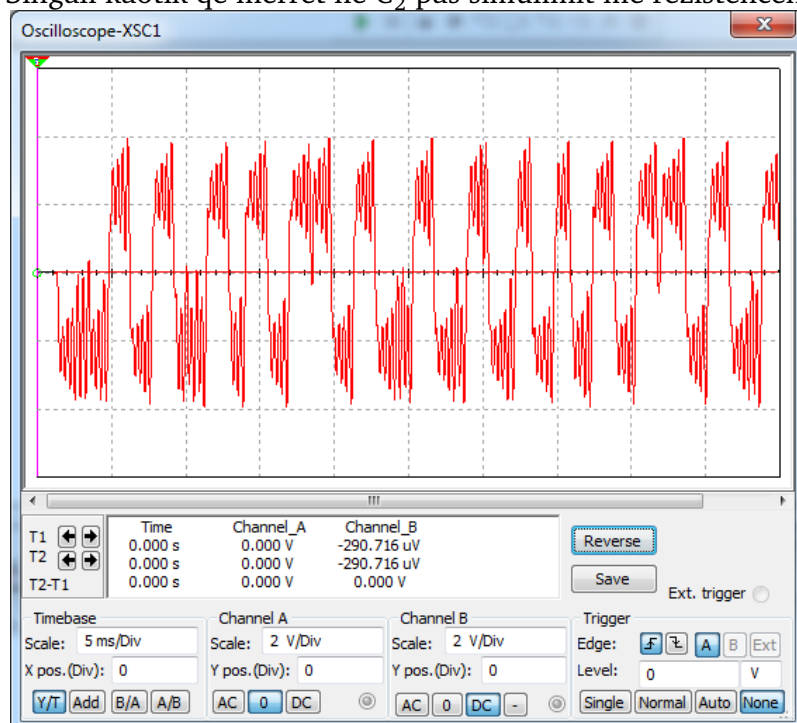


Figura 4.9: Singali kaotik që merret në C_1 pas simulimit me rezistencën $R_2 = 1.9 k\Omega$

Emri	Tipi	Vlera	Toleranca
C_1	Kondensator	10 nF	$\pm 5\%$
C_2	Kondensator	100 nF	$\pm 5\%$
L	Bobinë	18 mH	$\pm 10\%$
R_1	Rezistencë	22 k Ω	$\pm 5\%$
R_2	Potensiometër	Varied	$\pm 5\%$
$S R_3$	Rezistencë	3.3 k Ω	$\pm 5\%$
R_4	Rezistencë	22 k Ω	$\pm 5\%$
R_5	Rezistencë	220 Ω	$\pm 5\%$
R_6	Rezistencë	220 Ω	$\pm 5\%$
R_7	Rezistencë	2.2 k Ω	$\pm 5\%$

Tabela 4.1: Tabela e plotë e kompetenteve që u përdorën për qarkun e Chua's.

është të marrim të dhëna për diferencën e potencialit midis skajeve të kondensatorëve C_1 dhe C_2 . Prandaj te dy kanalet e oshiloshkopit (A dhe B) lidhen respektivisht me dy kondensatorët C_1 dhe C_2 . Duhet të vihet re se oshilatori i Chua-s përshkruhet nga tre variabla të pavarur (v_1 , v_2 dhe i_L) kështu dhe hapësira fazore e tij do të jetë një hapësirë fazore me tre përmasa, atëherë në oshiloskop do marrim një projektim të kësaj hapësire tredimensionale në dy dimensione.

Kontrolli i dukurisë së kaosit në këtë qark bëhet nëpërmjet potenciometrit R_2 . Kemi vënë re që qarku operon në mënyrë kaotik kur raporti i kondensatorit është midis 0.86 dhe 0.95, kjo do të thotë një rezistencë $R_2 = 1,72 \Omega$ deri $1,9 k\Omega$.

Në figurën 4.6 kemi rezultatin e parë të simulimit. Këtu paraqitet se kur rezistenca e potenciometrit është $R_2 = 1,72 k\Omega$ atëherë në oshiloskop paraqitet vetëm një anë e atraktorit. Duke rritur rezistencën e potenciometrit atëherë shfaqet dhe rrotulla e dyte e atraktorit e cila paraqitet në figurën 4.7, kjo figurë realizohet për vlerën $R_2 = 1.9 k\Omega$

Në figurat 4.6 dhe 4.7 është paraqitur hapësira fazore e sistemit. Për qëllimet e kriptografisë të këtij punimi duhet të tregohen dhe sinjalet kohore. Keto sinjale paraqiten tek figura 4.8. Në këtë figurë merret sinjali vetëm nga kanali A i oschiloskopit, i cili i përket diferencës së potencialit midis skajeve të kondensatorit C_2 pra të variablës v_2 sipas ekuacioneve (4.1).

4.1.4 Simulimi me MATLAB të qarkut Chua

Për të zgjidhur ekuacionet diferenciale të paraqitura në (4.1) përdoret mjedisi programues MATLAB. Në këtë program janë integruar metoda të integritit numerik dhe të zgjidhjes së ekuacioneve diferenciale. Për të zgjidhur ekuacionet diferencial të sistemit të Chua-s përdoret funksioni ODE45 i cili është aplikimi i metodës Runge-Kutta i optimizuar për programin MATLAB.

Realizimi i kodit paraqitet në shtojcën përkatëse ku jepen dhe shpjegimet përkatëse nepërmjet komenteve. Pas realizimit të modelit kompjuterik në gjuhën MATLAB u bë e mundur zgjidhja e ekuacioneve duke vendosur kushtet fillestare përkatëse. Kushtet fillestare të përdorura paraqiten tek tabela 4.3 si më poshtë.

Përshkrimi	Simboli	Vlera	Toleranca
Diferenca e potencialin në C_1	v_1	0, 1V	0%
Diferenca e potencialin në C_2	v_2	0 V	0%
Rryma që përshkruan bobinën L	i_L	0 mA	0%

Tabela 4.2: Vlerat fillestare për zgjidhjen e ekuacioneve.

Vlerat e sistemit në fillim tentojnë drejt zeros por nuk janë zero, ndryshe nuk mund të kishim ecuri të sistemit.

Mbi këtë sistem mund të tregohet dhe një nga cilësitë karakteristike të sistemeve kaotike, ndjeshmëria e tyre nga kushtet fillestare që quhet ndryshe efekti i fluturës. Duke mos ndryshuar asgjë tek sistemi meren tre raste të veçanta zgjidhjeje duke ndryshuar kushtet fillestare. Fillimisht sistemi i Chua-s zgjidhet për vlera fillestare $v_1 = 0.1, v_2 = 0, i_L = 0$ si rasti i parë, në rastin e dytë $v_1 = 0.2, v_2 = 0, i_L = 0$ dhe në rastin e tretë $v_1 = 0.3, v_2 = 0, i_L = 0$. Të gjitha rezultatet vendosen në figurën 4.12 aty mund të vihet re se në fillim të tre grafikët fillojnë nga e njëjta pikë por më tej me ecurinë e kohe ndahen. Kjo tregon që një ndryshim i vogël i kushteve fillestare sjell një ndryshim të madh tek rezultatet e sistemit.

Nuk duhet të harrohet që keto rezultate kanë ardhur si pasojë e zgjidhjes konkrete të sistemit të ekuacioneve diferencial dhe jo nga një sistem rastësor. Në këtë mënyrë

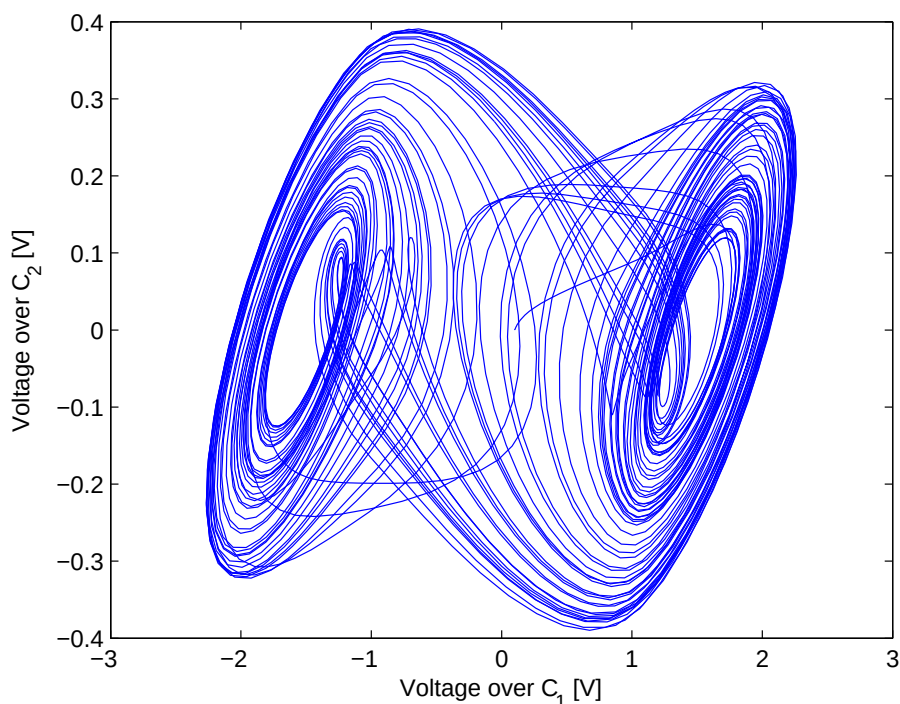


Figura 4.10: Hapësira fazore e llogaritur me metoda numerike

mund të vërtetohet përkufizimi i dytë mbi sistemet kaotike që kaosi është veprimi stokastik që shfaqet në një sistem deterministik.

Përveç analizës që u bë mbi veprimin e qarkut të Chua-s një tjetër rezultat vjen edhe nga paraqitja grafike e rezistencës jo lineare. Në figurën 4.13 paraqitet rezistenca jolineare, pjese përbërëse e qarkut në studim.

Në grafikun e paraqitur në figurën 4.13 duhet të vihet se rezistenca është negative pasi pjerrësia e karakteristikes $V-i$ është negative. Drejtëza jolineare përbëhet nga tre drejtëza lineare, me pjerrësi G_a për pjesën e brendshme dhe G_b për pjesën e jashtme. I njëjti rezultat arrihet edhe në programin e simulimit elektronik.

4.1.5 Realizimi laboratorik i sistemit

Realizimi laboratorik u bë i mundur në mjediset e Departamentit të Fizikës, të Universitetit të Athinës në laboratorin e Elektronikës, Telekomunikacionit dhe Automatikës. Në këtë laborator u bë i mundur realizimi në plaket elektronike të qarkut

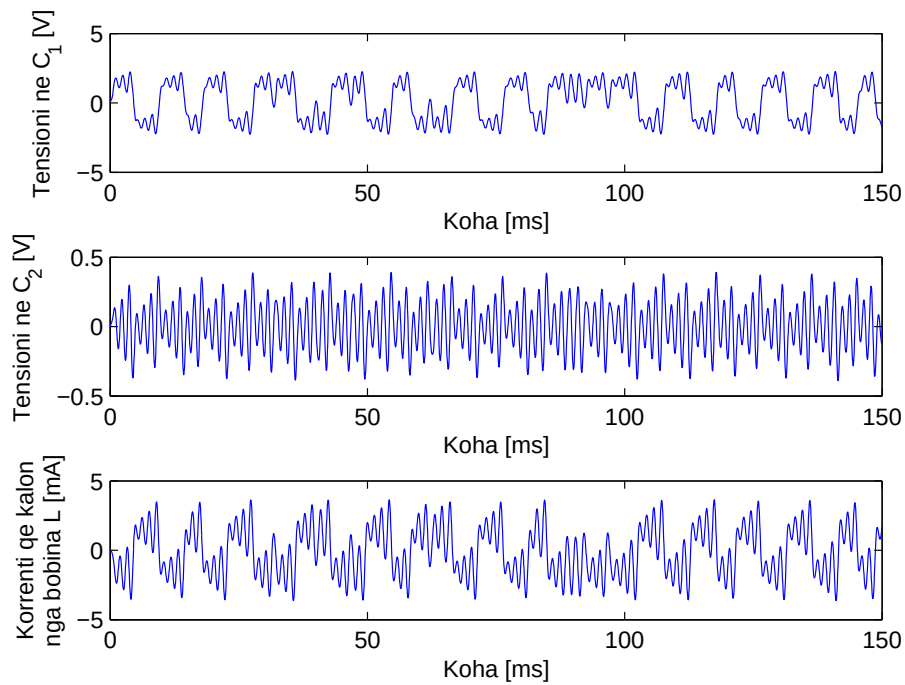


Figura 4.11: Sinjalet kaotike që prodhohen nga sistemi i Chua-s

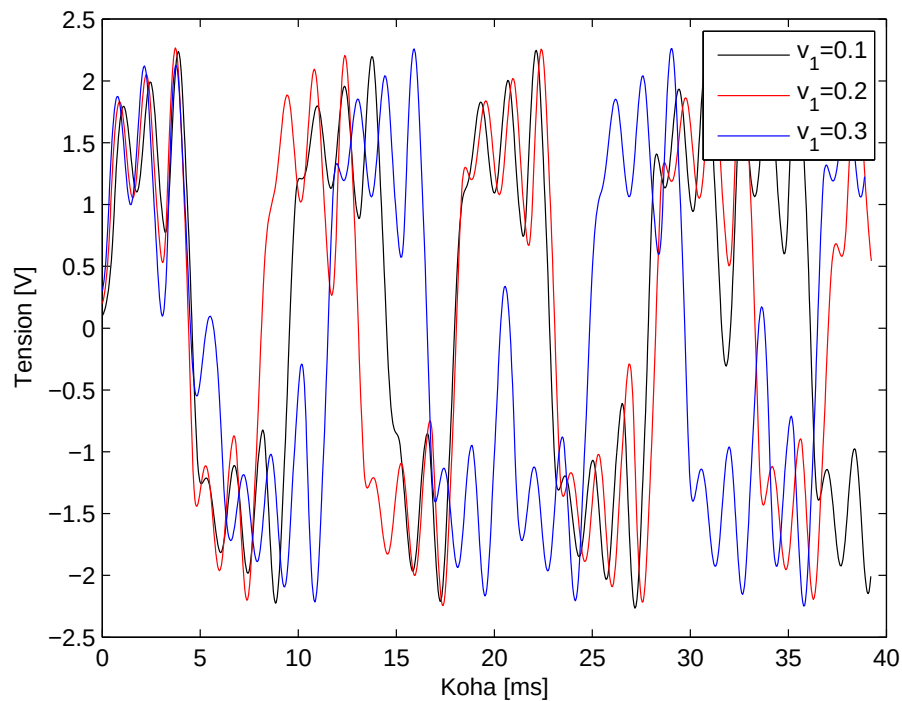


Figura 4.12: Diferencat që shfaqen në v_1 kur ndryshohen kushtet fillestare.

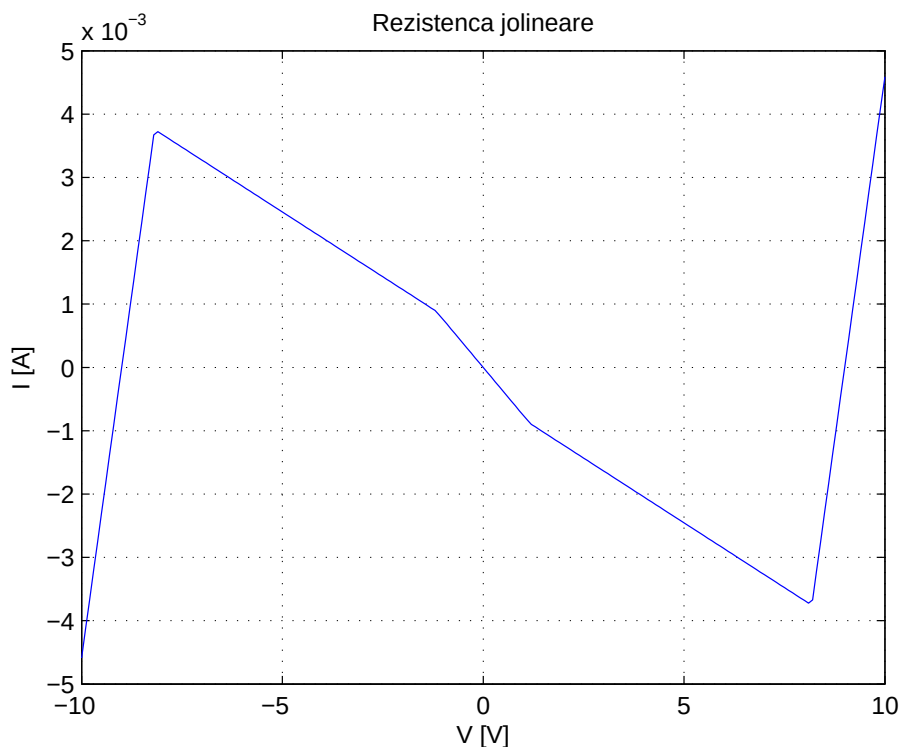


Figura 4.13: Karakteristika

dhe kryerja e matjeve duke përdorur sisteme matëse bashkëkohore dhe të kompjuterizuara.

Proçedura për të vëzhguar hapësirat fazore të atraktoreve është e njëjta me atë që u përdor edhe për simulimin e tyre në Multisim. Fillimisht potenciometri vendoset në një pozicion të tillë që rezistenca të jetë e vogël por jo zero. Shumë ngadalë rritet rezistenca e potenciometrit deri sa qarku të fillojë të operojë në mënyrë kaotike. Në këtë moment merret vetëm një anë e atraktorit të Chua-s e që paraqitet në figurën 4.14. Figura 4.14 korrespondon me figurën 4.7 e cila është rezultati i simulimit me programin Multisim.

Si përfundim theksojmë se qarku i Chua-s i propozuar që në vitin 1980, është ende teme studimi. Sepse kur u propozua ky qark, të dhënat nuk mund të analizoheshin plotësisht për arsye se fuqia kompjuterike nuk ishte e mjaftueshme. Tashmë është vënë re një interes botëror për studimin më të hollësishëm të vetive dinamike që paraqiten në këtë qark. Nga ana tjetër duhet theksuar dhe interesi ndërdisiplinor mbi këtë qark

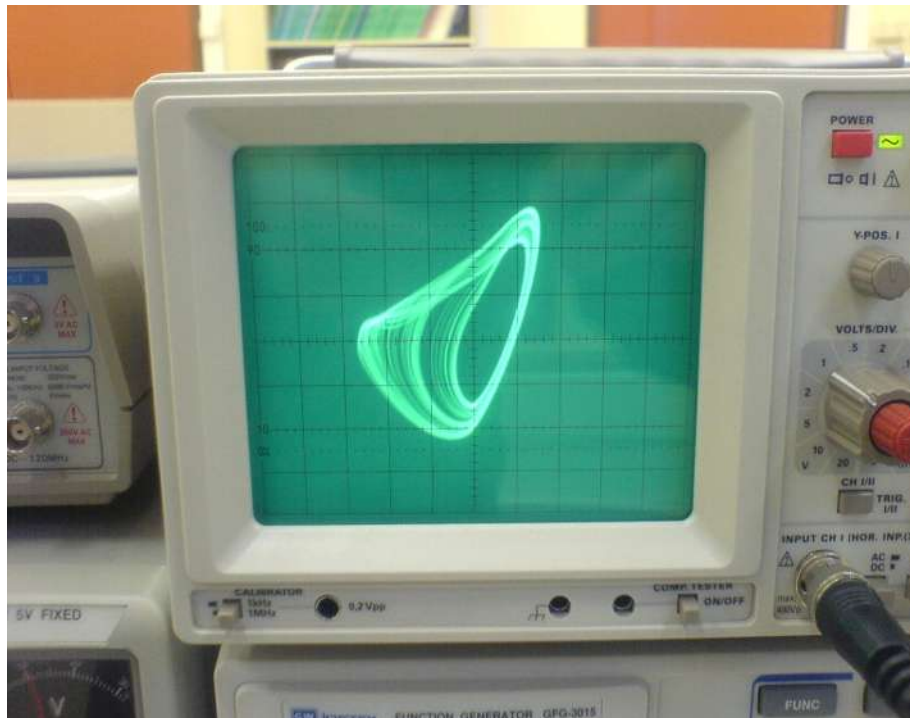


Figura 4.14: Rezultati i realizimit në laborator të qarkut.

pasi për studimin e tij duhen njohuri të sistemeve dinamike aftësi në fushën e elektronikës dhe sigurisht analizimi i të dhënave kërkon njohuri edhe në fushën e programimit.

4.2 Qarku kaotik me një transistor

Përveç qarkut të Chuas i cili është paraqitur dhe është analizuar më sipër, mund të realizohen qarqe që paraqesin një veprim kaotik me topologji me të thjeshtë. Keto qarqe, kryesisht përbëhen nga një rezistencë (L), një bobine (R) dhe një transistor (T), që në literature paraqiten si qarqe (RTL). Keto kanë një përparësi kundrejt qarkut të Chuas se mund të realizohen me më pak komponentë elektronikë. Ky fakt ul ndjeshëm koston e krijimit të një sistemi komunikacioni i cili përdor kriptografi kaotike.

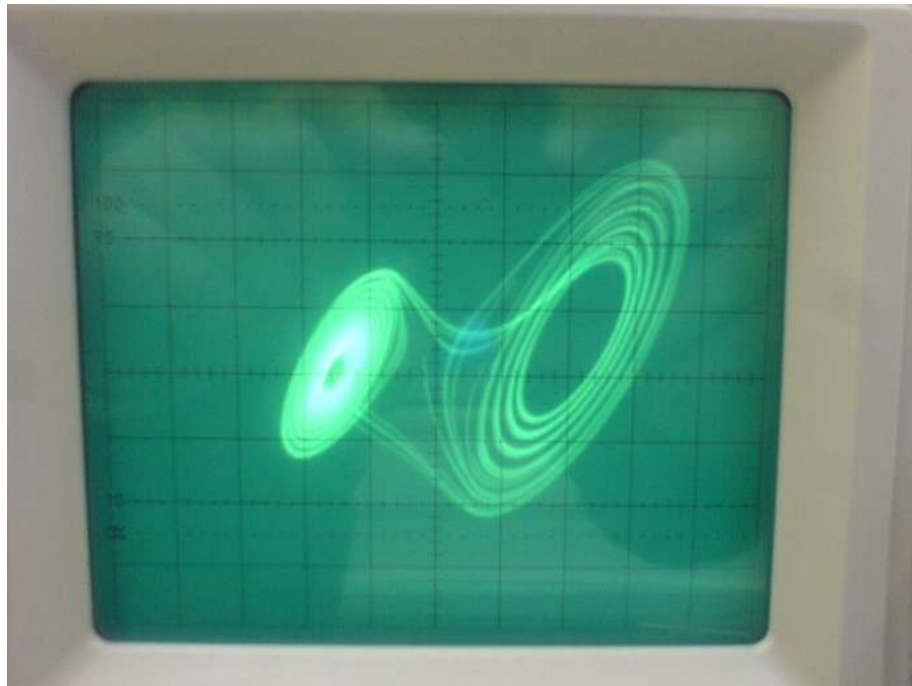


Figura 4.15: Realizimi i atraktorit të plotë të qarkut të Chua-s

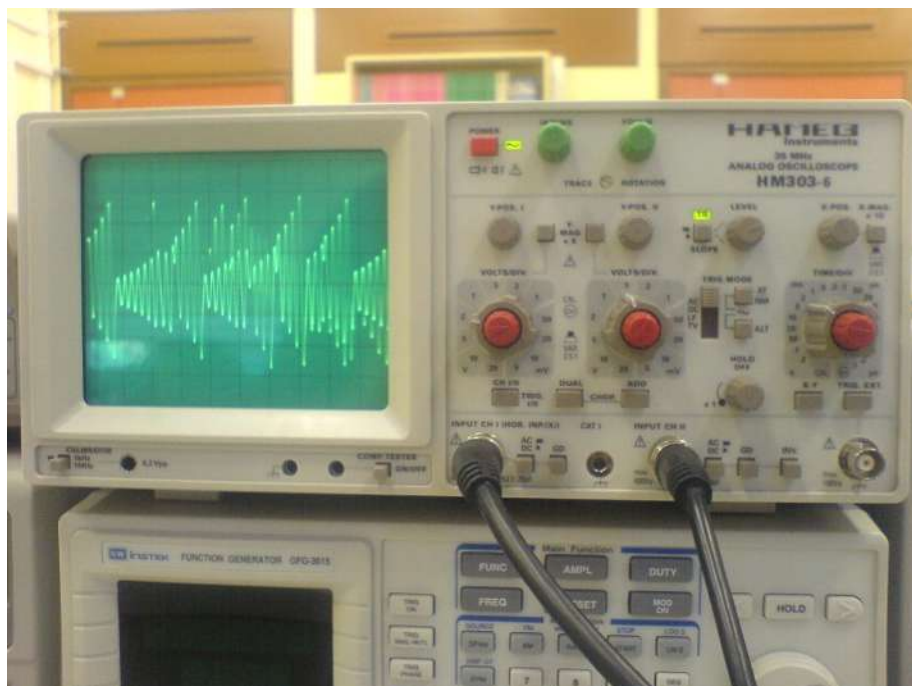


Figura 4.16: Sinjali real kaotik që merret midis skajeve të kondensatorit C_2

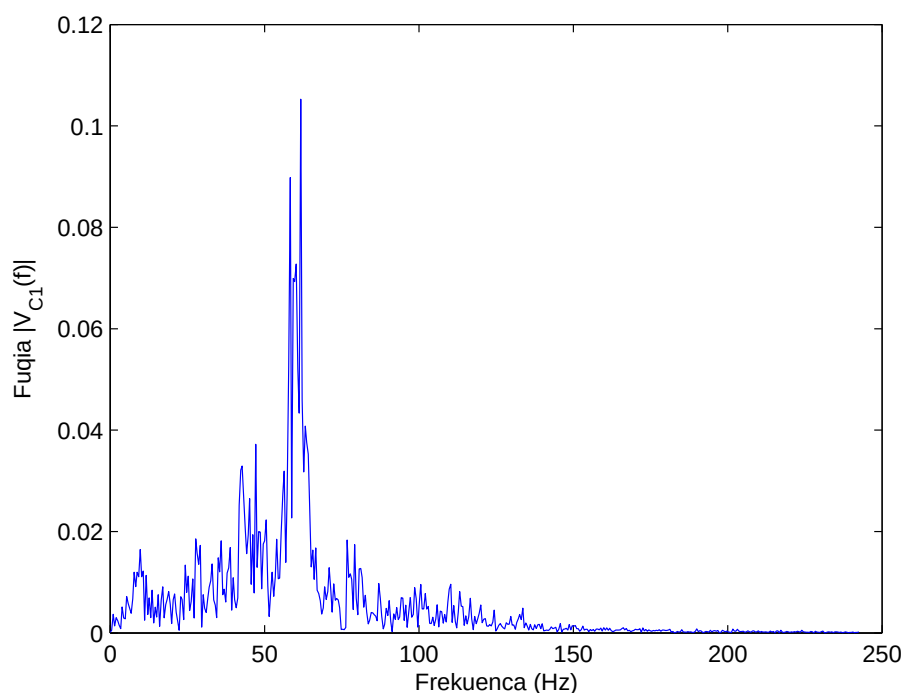


Figura 4.17: Spektri i fuqis të sinjalit kaotik të prodhuar nga qarku i Chuas.

4.2.1 Komponentët e qarkut

Qarku i plote u realizua në laborator paraqitet tek figura 4.18. Siç mund të vihet re, qarku përmban një transistor bipolar (BJT) BCD107BP, i tipit nnp i lidhur me emiter të përbashkët, rezistenca në emiter është $R_2 = 33\Omega$, kurse në kolektor është lidhur rezistencë $R_1 = 3,3k\Omega$.

Hyrja e qarkut është lidhur me një gjenerator sinjalesh i cili prodhon një sinjal sinusoidal me amplitudë $V_o = 13V$ i cili kalon nëpërmjet një bobine $L = 55\mu H$. Qarku ushqehet edhe burimi i tensionit $V_1 = 12V$. Si në figurën 4.18.

Këtu studiohet veprimi i qarkut duke marrë sinjalin e daljes në kolektorin e transistorit $V_c(t)$, nëpërmjet rezistencës së tokëzuar R_1 . Tensioni $V_c(t)$ ka lidhje me rrymën e kolektorit, i cili është faktor kryesor i qarkut, sepse nëse në qark shfaqet veprim kaotik atëherë sinjali do të tregoj veti kaotike.

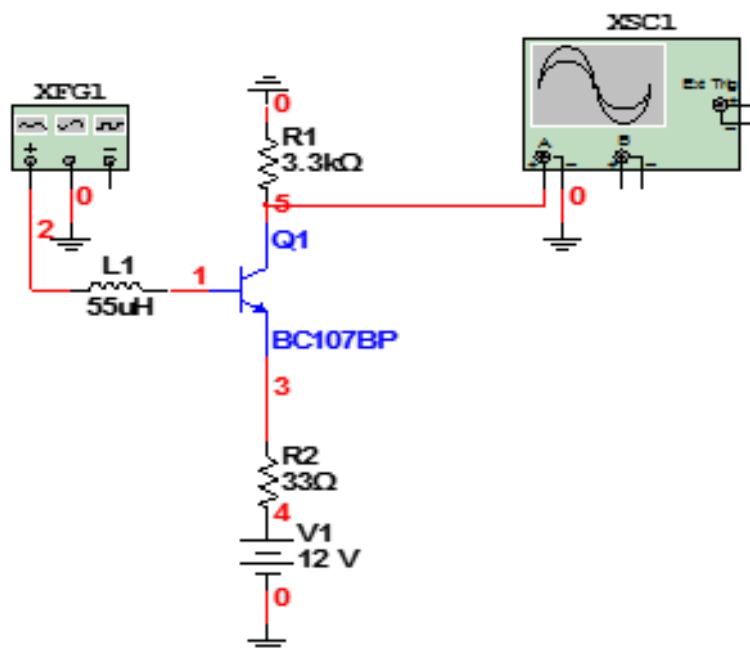


Figura 4.18: Skema elektronike e qarkut kaotik ku transistori vepron në zonën aktive të kundërt

4.2.2 Simulimi dhe implementimi i qarkut

Simulimi i qarkut të paraqitur në figurën 4.18 kryhet duke përdorur programin MULTISIM të kompanisë National Instruments. Ky program njihet botërisht për saktësinë e tij në kryerjen e simulimeve elektronike. Për sinjal sinusoidal me amplitudë $V_o = 13\text{ V}$ dhe frekuencë $f_1 = 3\text{ kHz}$ merret sinjali tensioni në kolektorin e transistorit $V_c(t)$ i cili prezantohet tek figura 4.20.

Vihet re se gjatë gjysëm periodës pozitive sinjali i marë i përket një sinjali sinusoidal, kurse gjatë gjysëm periodës negative vihen re disa oshilime me frekuencë të madhe. Me më shumë hollësi keto oshilime mund të shihen tek figura 4.21. Përveç oshilimeve me frekuencë vihet re dhe një lloj zhurme kur tensioni sinjal bëhet nga negativ në pozitiv.

Për të vërtetuar në qoftë se ndodh e njëjta gjë edhe në realitet u realizua qarku në laborator. Në figurë 4.19 paraqitet qarku ashtu siç u realizua në laborator.

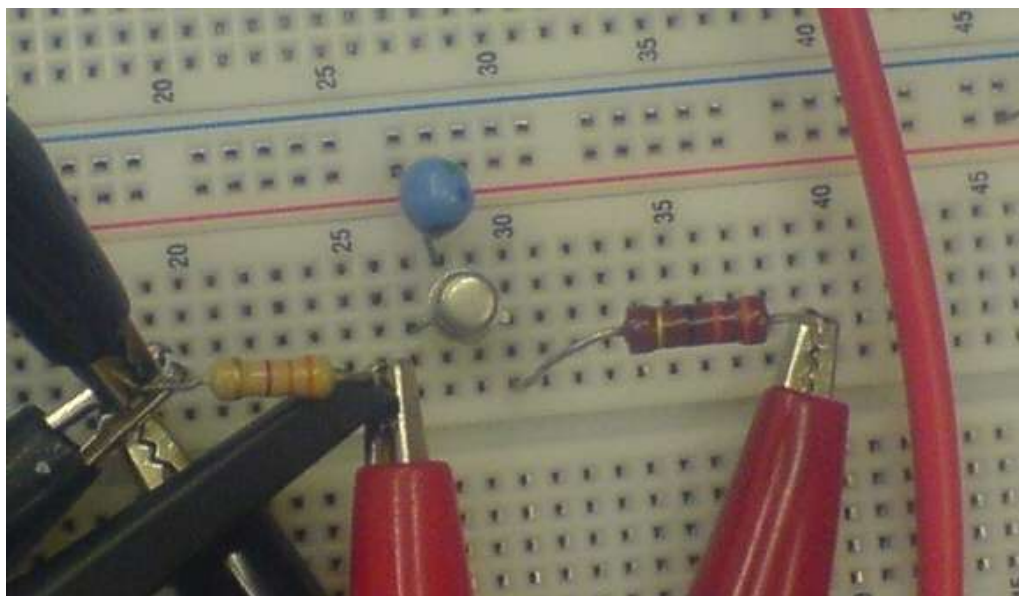


Figura 4.19: Implementimi laboratorik i qarkut të prezantuar në figurën 4.18.

4.2.3 Regjistrimi i të dhënave

Në figurën 4.22 paraqitet sinjali i marrë nga oshiloskopi dhe, duhet vrojtuar ngjashmëria e tij me rezultatet e simulimit të paraqitura tek figura 4.21.

Duke parë daljen e qarkut ashtu siç ajo paraqitet tek implementimi i tij laboratorik duhet theksuar ngjashmëria që ajo ka me simulimin. Ashtu siç shihet gjatë gjysmës të periodës negative sinjali i hyrjes paraqitet i defomuar për arsye të aplikimit të DC tensionit V_1 nëpërmjet rezistencës R_2 në emiterin e transistorit dhe për arsye të polarizimit negativ të takimit bazë - emiter duke qenë se takimi bazë - kolektor qëndron i polarizuar pozitivisht. 4.22

Në vazhdimësi duhet bërë rindërtimi i hapësirës fazore duke kryer analizën e serisë kohore që përfitohet nga oshiloskopi. Nga oshiloskopi analog një gjë e tillë është e pamundur pasi ai nuk mund të ruajë të dhëna. Për këtë arsye u përdor oshiloskopi dixhital për marjen e sinjalit dalës.

Në figurën 4.23 vëzhgojmë sinjalin e daljes dhe mund të marrim disa të dhëna paraprake për sa i përket karakteristikave të saj. Treguesi 1 i cili ndodhet në pjesën e poshtme nga ana e majtë prezanton nivelin e tokëzimit të oshiloskopit (GRD), i cili

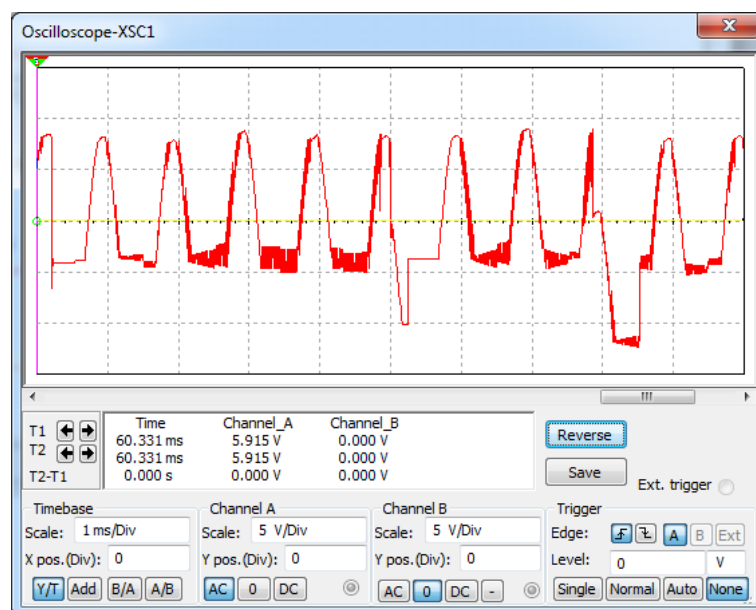


Figura 4.20: Simulimi i qarkut të figurës 4.18.

tregon nivelin 0V. Oshiloskopi përdoret në DC mode, kështu ne në oshiloskop marrim dhe komponentin alternativ (AC) por edhe komponentin e vazhduar (DC) të sinjalit. Çdo ndarje në boshtin Y korrespondon në 2V. Vlera më e madhe e tensionit është 12V sa është dhe tensioni V_1 . Sinjali tregon të ketë saturim në 4V atje ku ndodhin dhe oshilimet kaotike të cilat do të vërtetohen në paragrafet në vazhdim. Çdo ndarje në boshtin X korrespondon në $200\mu s$. Ashtu siç tregohet në figurë perioda është $T = 3,1 ms$.

Për të kryer analizën jo lineare të serisë kohore merren 2000 kampione të sinjalit dalës me frekuencë kampionimi $\Delta t = 0,5\mu s$. Të dhënat e sinjalit ruhen në memorien e oshiloskopit dhe për ti marrë ato përdoret programi kompjuterik MATLAB i cili është lidhur me oshiloskopin.

Para së të kalojmë në analizën e serisë kohore në paragrafin në vazhdimësi paraqitet analiza e zonës aktive e kundërt.

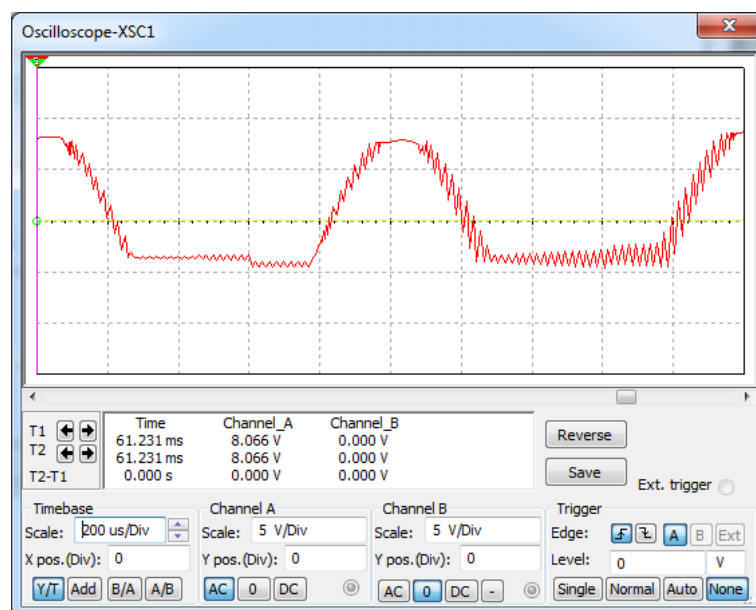


Figura 4.21: Simulimi i te sinjalit të daljes $V_c(t)$ me hollësi më të madhe.

4.3 Zona aktive e kundërt

Kjo menyrë operimi të një transistori BJT quhet si operim në zonën aktive të kundërt. Një prezantim grafik të zonave të operimit të transistorit paraqitet tek figura 4.24.

Zona e veprimit aktiv e kundërt shfaqet kur diferenca e potencialit midis bazë dhe emiterit është negativ:

$$V_{BE} < 0 \quad (4.15)$$

dhe kur diferenca e potencialit midis bazës dhe kolektorit është pozitiv:

$$V_{BC} > 0 \quad (4.16)$$

Zona e veprimit të kundërt ka aplikime në qarqe të logjikës dixhitale por edhe në qarqe analoge. [37]

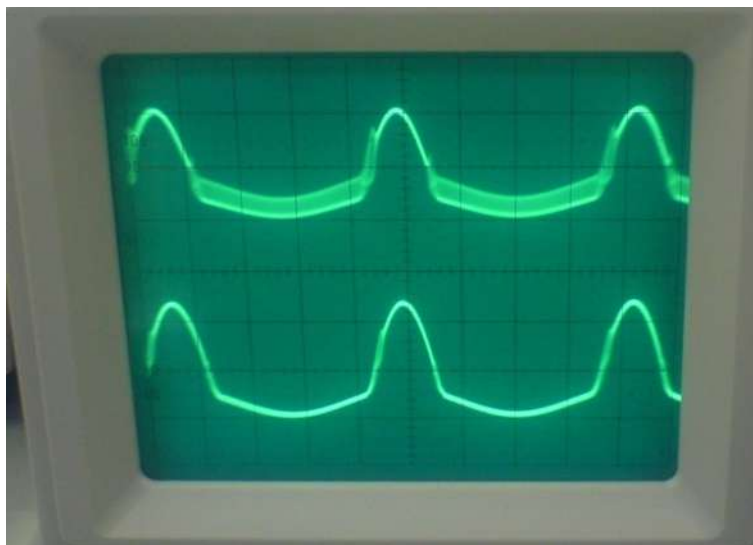


Figura 4.22: Figura në oshiloskopit pas implementimit të qarkut të laborator.

4.3.1 Analiza kohore e sinjalit të daljes

Për një madhësi skalare siç është seria kohore në rezistencën e kolektorit ku $V_C(t) = V_t$, ku $t = 1, 2, 3, \dots, N$, hapësira fazore mund të rindërtohet duke përdorur metodën e vonesave. Ideja kryesore e kësaj metode është që zhvillimi i secilës variabël varet nga variablat më të cilat ajo bashkëvepron. [38]. Këto informacione mund të llogatiten nga ecuria e vlerave që ato morrën.

$$X = V_t, V_{t-\tau}, V_{t-2\tau}, \dots, V_{t-(m-1)\tau} \quad (4.17)$$

ku τ është vonesa kohore dhe m dimensionimi i ngulitur ashtu siç ato u përkufizuan në paragrafin e përparshëm. Për analizën e serisë kohore duhet të përdoret paketa e analizës së serive kohore jo lineare TISEAN (nonlinear Time Series Analysis) [22]. Për prezantimin e rezultateve dhe për automatizimin e procedurave janë ndërtuar dhe rutina të posatshme në MATLAB.

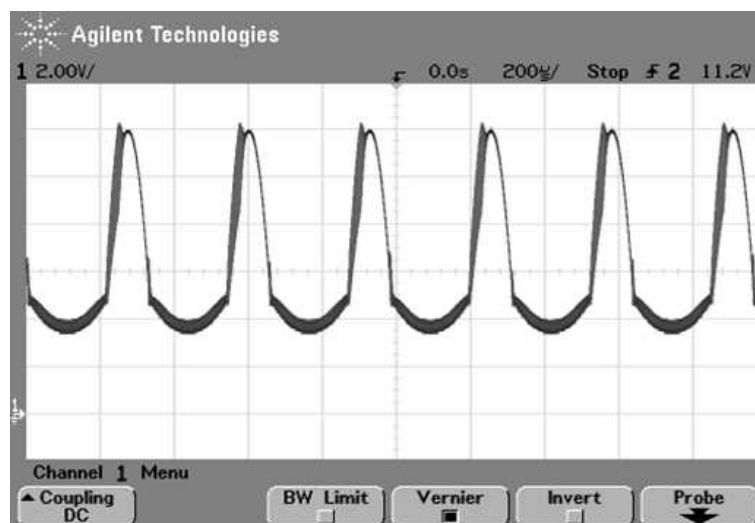


Figura 4.23: Sinjali i përfituar nga oshiloskopi dixhital.

Llogaritja e informacionit të përbashkët

Për të llogatitur informacionin e përbashkët përdoret kodi i cili paraqitet tek shtojcat. Një tjetër mënyrë për të llogaritur informacionin e përbashkët është duke përdorimi i programit “mutual.exe” të paketës TISEAN. [39]. Vihet re se sa më e vogël të jetë ngjashmëria midis serive $X(t)$ dhe $X(t - \tau)$ aq më e vogël do të jetë dhe vlera e informacionit të përbashkët.

Në figurën 4.25 vihet re se minimumi i parë i informacionit të përbashkët paraqitet diku midis vlerave 0 dhe 10. Në tabelën 4.3 paraqiten rezultatet e llogaritjes së informacionit të përbashkët në këtë interval. Vihet re se minimumi i parë merret kur vlera e vonesës është e barabartë me $\tau = 4$

Llogaritja e autokorelacionit

Llogaritja e autokorelacionit tregon shkallën e korelacionit midis serisë kohore $X = X(t)$ dhe serisë kohore $Y = X(t - \tau)$. Llogaritja e këtij koeficienti bëhet me anë të ekuacionit 3.7

Për të llogaritur autokorelacionin e një serie kohore, mund të përdoret proram i “autocor.exe” i paketës TISEAN ose kodi MATLAB i cili li paraqitet në shtojcë. Llogaritja

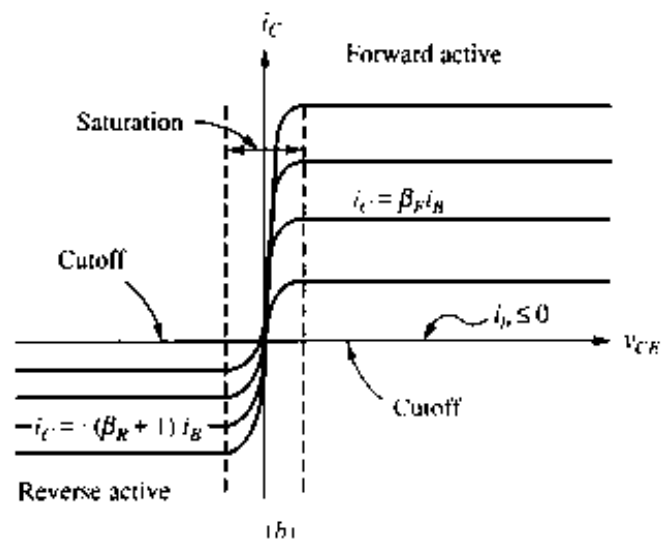


Figura 4.24: Paraqitja grafike e karakteristikave të transistorit BJT [5].

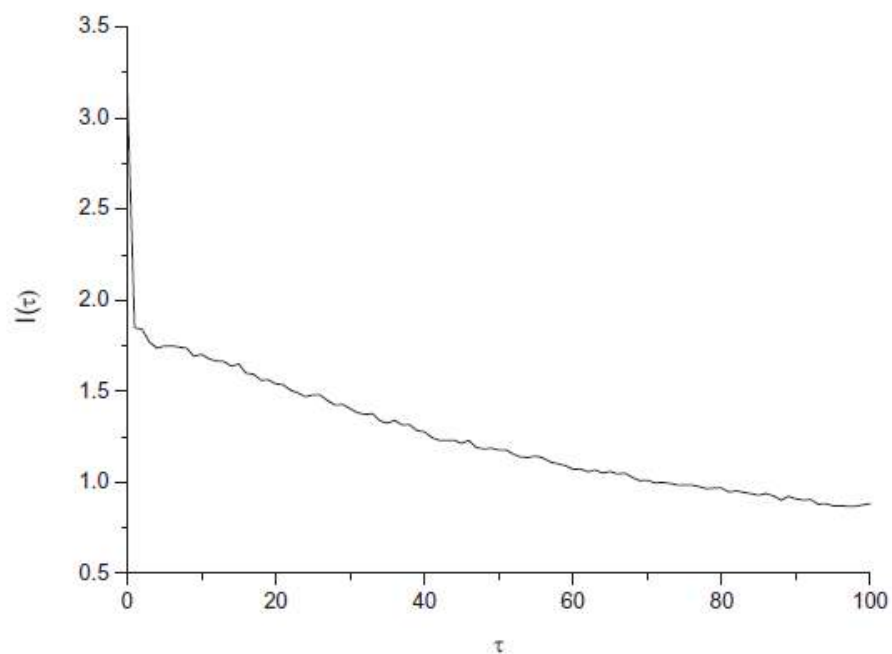


Figura 4.25: Rezultati i llogaritjes së informacionit të përbashkët.

Vonesat τ	Informacioni i përbashkët
0	2,17426377608017
1	1,27661324047168
2	1,26773668387991
3	1,21627841567891
4	1,20045669773559
5	1,20415004755149
6	1,20388672237182
7	1,19777466220207
8	1,19744680756947
9	1,16633531986132
10	1,17398848995359

Tabela 4.3: Informacioni i përbashkët në lidhje me vonesën τ

e autokorelacionit të serisë kohore për vlera të ndryshme të vonesës τ ka si qëllim specifikimit e dritares Thiler (Theiler window). [40] Sipas metodës duhet që vlera e vonesës τ e cila na dha minimumin e parë të informacionit të përbashkët të jetë e njëjta brenda ketij intervali i quajtur ndryshe Theiler window.

Ashtu siç shihet tek figura 4.26 autokorelacioni nuk shkon shpejt drejt zeros, por kjo ndodh kur vonesa kohore të bëhet e barabartë me $\tau = 150$. Dritarja Theiler do të jetë e barabartë me vonesën e cila na jep $1/e$ të vlerës fillestare të autokorelacionit. Për rastin tonë autokorelacioni fillestar kur $\tau = 0$ është i barabartë me 1 sepse në këtë rast $X = Y$.

Më poshtë paraqiten vlerat (Tabela 4.4) e llogaritjes së autokorelacionit për vlera të përafërta me $1/e = 0.368$ të vlerës fillestarë.

Vonesat τ	Autokorelacioni r
94	0,390334698246421
95	0,380828890903791
96	0,371373540621757
97	0,361620111126137

Tabela 4.4: Autokorelacioni në lidhje me vonesën τ

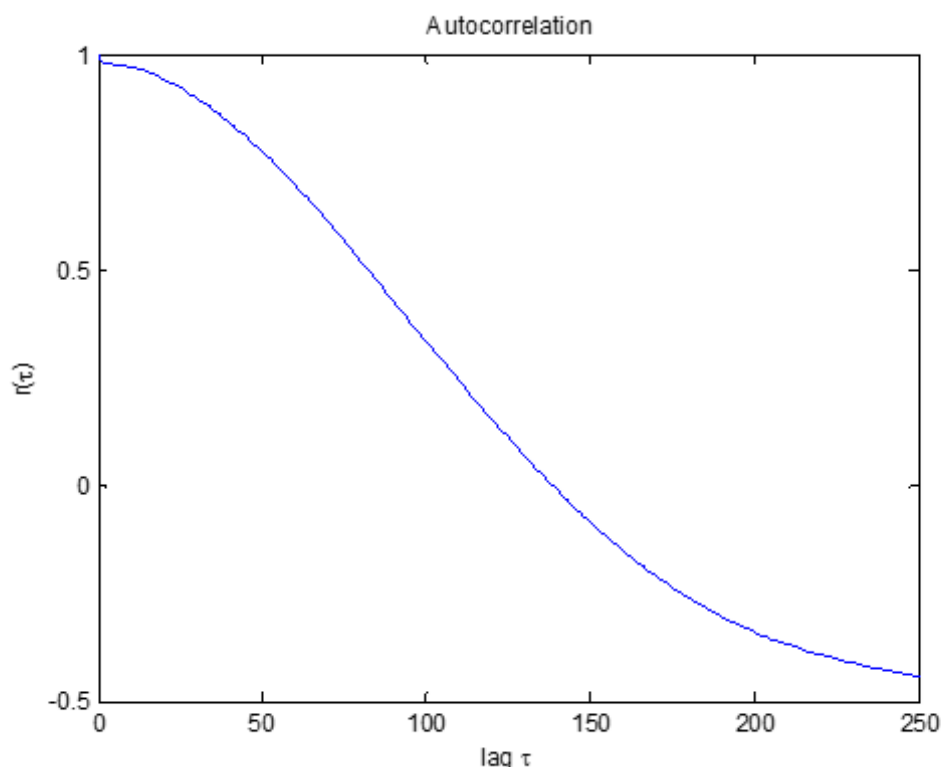


Figura 4.26: Llogaritja e autokorelacionit të serisë kohore

Llogaritja e të afërmve të rremë

Për të gjetur dimension e ndërfutur përdoret metoda e të afërmve të rremë e cila është paraqitur në paragrafin përkatës. Para se të bëhet llogaritja e të afërmve të rrëmë bëhet heqja e zhurmës së sinjalit, sepse prezenca e zhurmës ndikon të llogaritja e sakte të rezultatit. Heqja e zhurmës behet me metodën *locally projective nonlinear noise reduction* [41]. Programi i cili kryen këtë veprimin është “ghkss.exe” i paketës TISEAN.

Në figurën 4.27 paraqitet përqindja e të afërmve të rremë në lidhje me dimensionin e ngulitur. Si një një zgjedhje optimale e dimensionit të ndërfutur, merret ajo vlerë për të cilën përqindja e të afërmve të rremë është më e vogël se 1%. Kjo ndodh për $m = 5$.

Tek figura 4.27 vija me ngjyrë të kuqe prezanton llogaritjen e të afërmve të rremë pas reduktimit të zhurmës kurse vija e zezë prezanton rezultatin e llogaritjes për vlerat

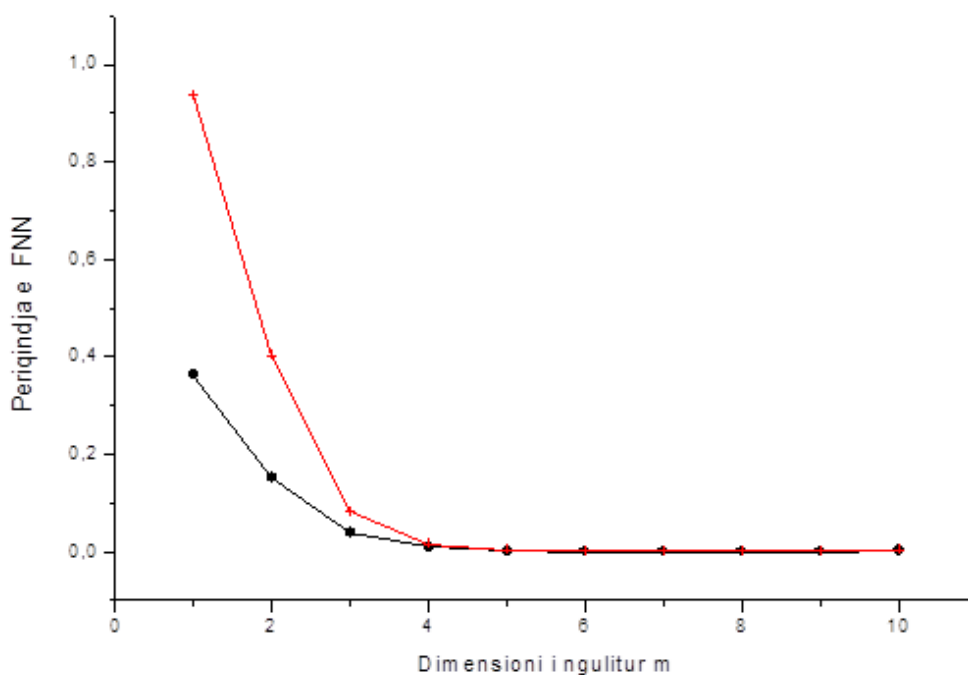


Figura 4.27: Përqindja e të afërmeve të rremë (FNN) në lidhje me dimensionin e ngulitur m , përpara (vija e zezë) dhe pas (vija e kuqe) e reduktimit të zhurmës

origjinale.

4.3.2 Rindërtimi i hapësirës fazore

Duke u bazuar tek analiza e bërë më sipër bëhet rikonstrukcioni i hapësirës fazore. Në bazë të vonesës τ dhe të dimensionit të ndërfutur m krijohet një matricë me N rreshta, sa janë dhe kampionet e serisë kohore dhe me m shtylla. Çdo rresht prezanton vektorin e një pike të trajektores.

Paraqitja grafike e hapësirës fazore të rindërtuar dhe projeksioni dy dimensionale i saj prezantohen tek figura 4.29. Kjo figurë mund të krahasohet me figurën konkrete të hapësirës fazore të marrë nga oshiloshkopi e paraqitur në 4.28.

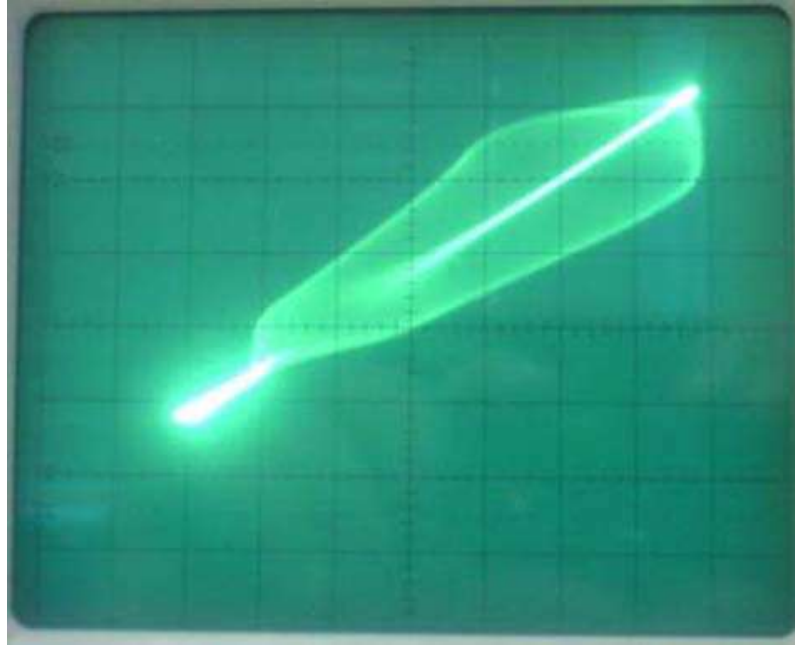


Figura 4.28: Hapësira fazore e marrë nga oshiloskopi.

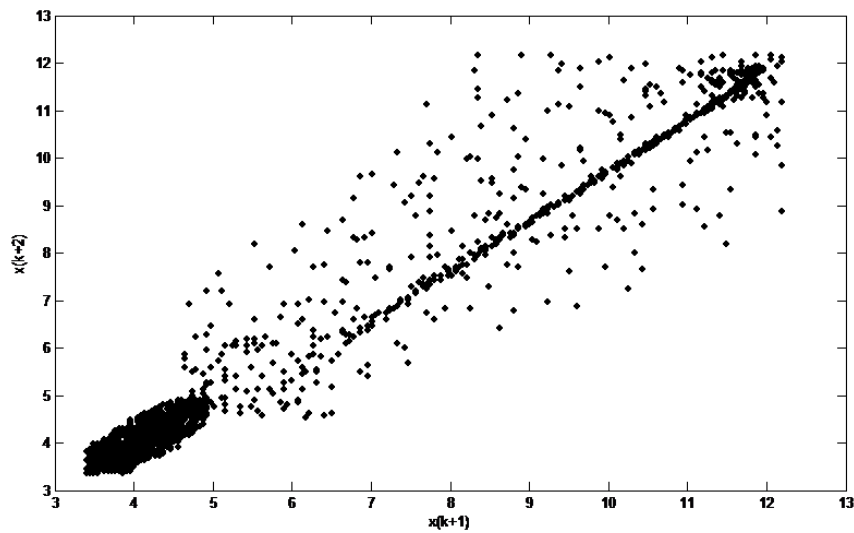


Figura 4.29: Projektioni në dy dimensione e hapësirës fazore të rikonstruktuar.

4.4 Llogaritja e eksponentit Lyapunov

Hapi tjetër në analizën e serisë kohore është llogaritja e eksponentit Lyapunov më të madh. Për llogaritjen e këtij eksponenti përdoret metoda e propozuar nga Rosenstein e përshtatshme për seri kohore të vogla [42].

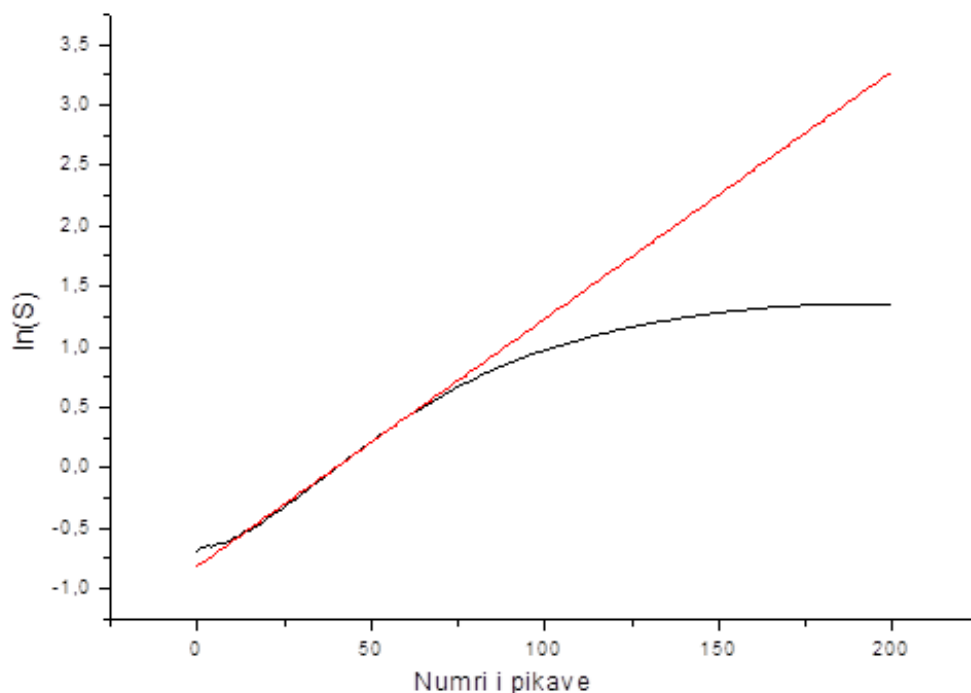


Figura 4.30: Llogaritja e eksponentit Lyapunov maksimal sipas metodës Rosenstein

Llogaritja e eksponentit Lyapunov më të madh është e rëndësishme për të vërtetuar veprimin kaotik të sistemit. Ashtu si sistemi evoluon në kohë trajektoria e tij do të konvergjojë ose do të divergjojë. Eksponenti Lyapunov është një tregues i karakteristikave kaotike të sistemit, në qoftë se eksponenti është pozitiv atëherë sistemi do të ketë sjellje kaotike.

Nga të dhënat u llogarit që eksponenti Lyapunov më i madh është $\lambda_{max} = 0.02048$ për dimensionin e ngulitur $m = 5$. Në figurën 4.30 paraqitet logaritmi i shumës së pikave të trajektore. Atëherë, qarku i cili studiohet paraqet sjellje kaotike. Mund të shihet, që pas 200 pikave logaritmi konvergjon në vlerën 1,5. Eksponenti Lyapunov është pjerrësia e drejtëzës e cila tenton më mirë kurbën e shumës.

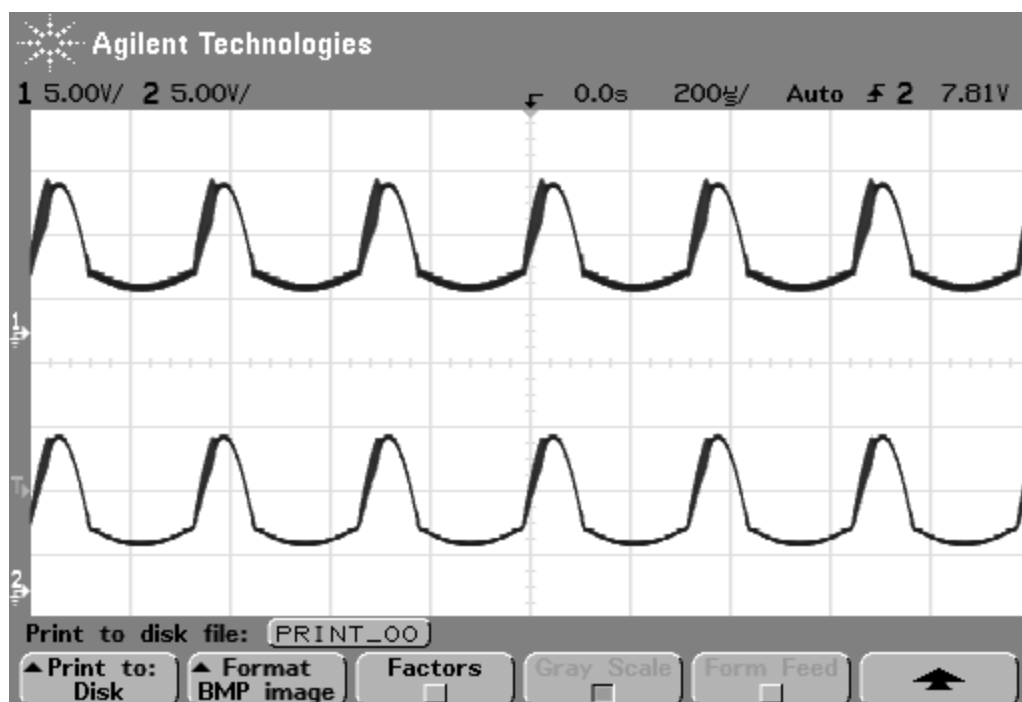


Figura 4.31: Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 13 \text{ Volts}$

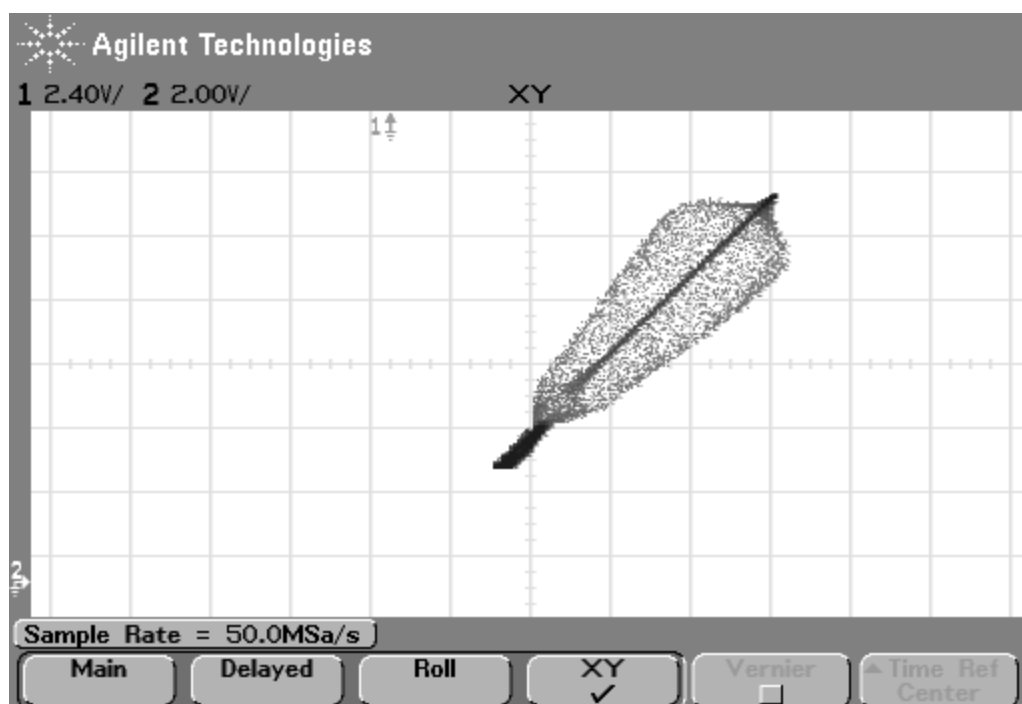


Figura 4.32: Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 13 \text{ Volts}$

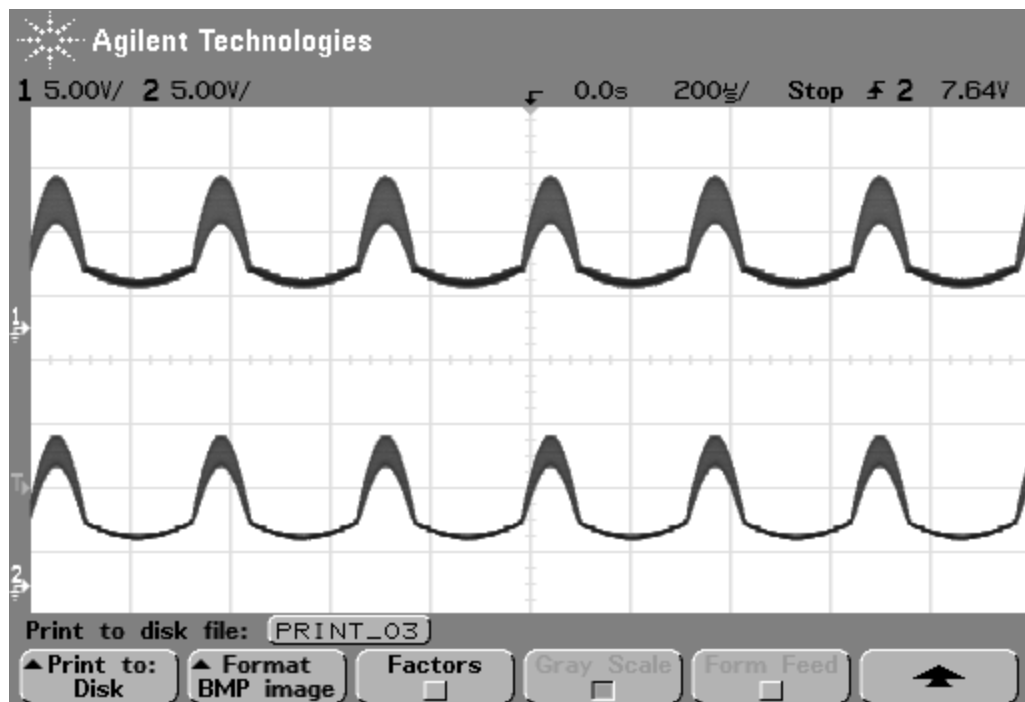


Figura 4.33: Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 10 \text{ Volts}$

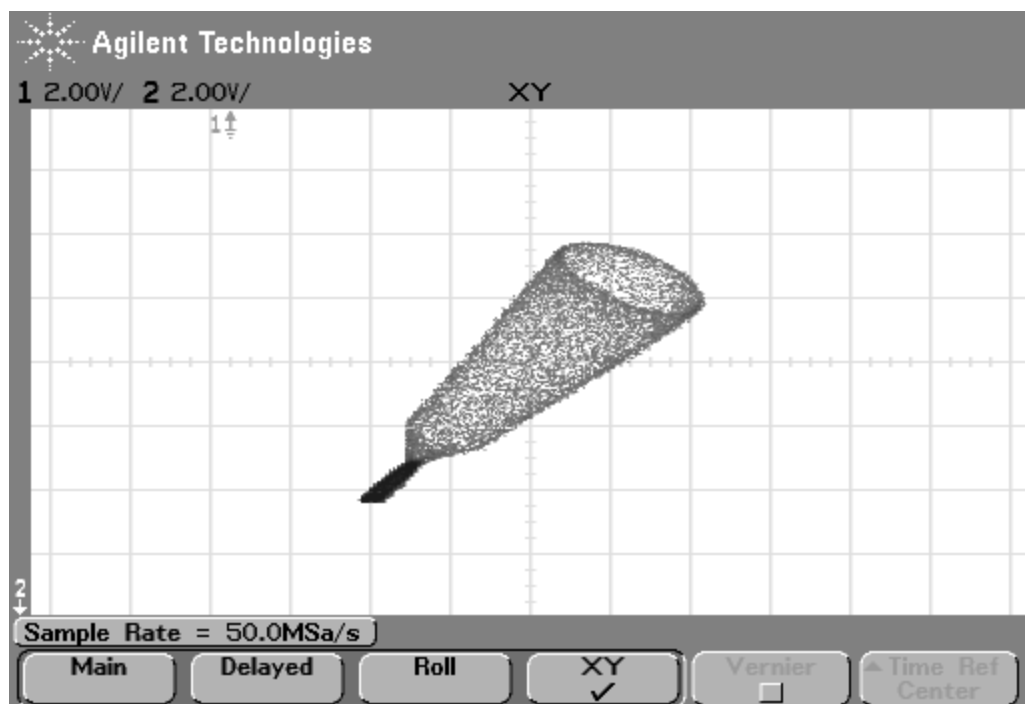


Figura 4.34: Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 10 \text{ Volts}$

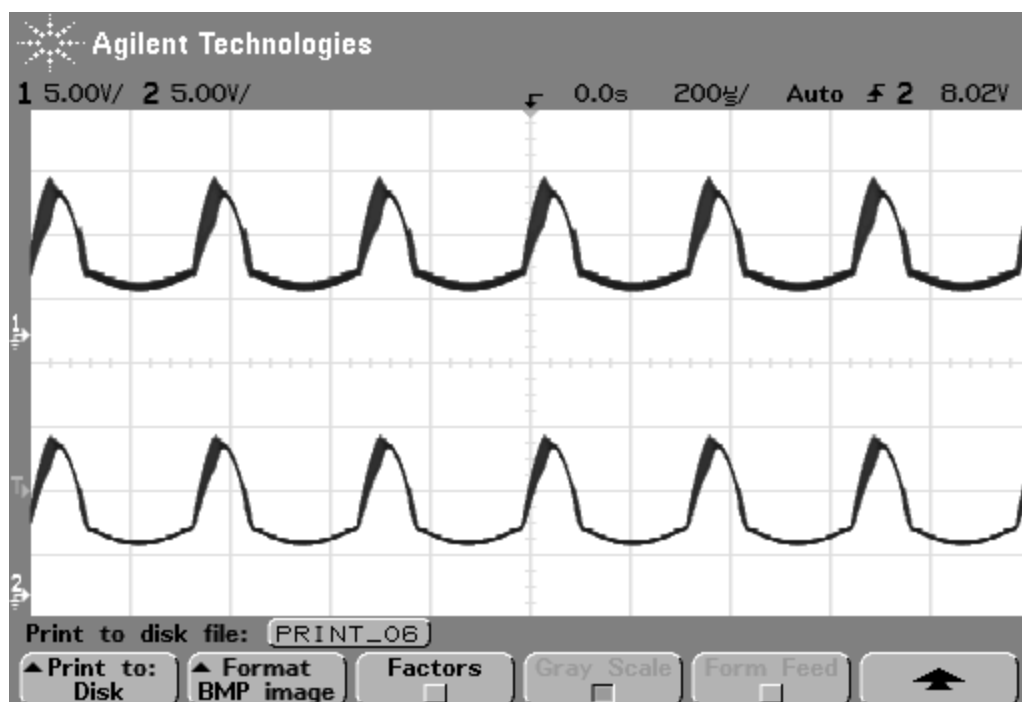


Figura 4.35: Sinjali dalës dhe sinjali hyrës (poshtë) dhe sinjali dalës lartë nga oshiloskopi dixhital Agilent kur sinjali hyrës ka amplitudë $V_0 = 11.5 \text{ Volts}$

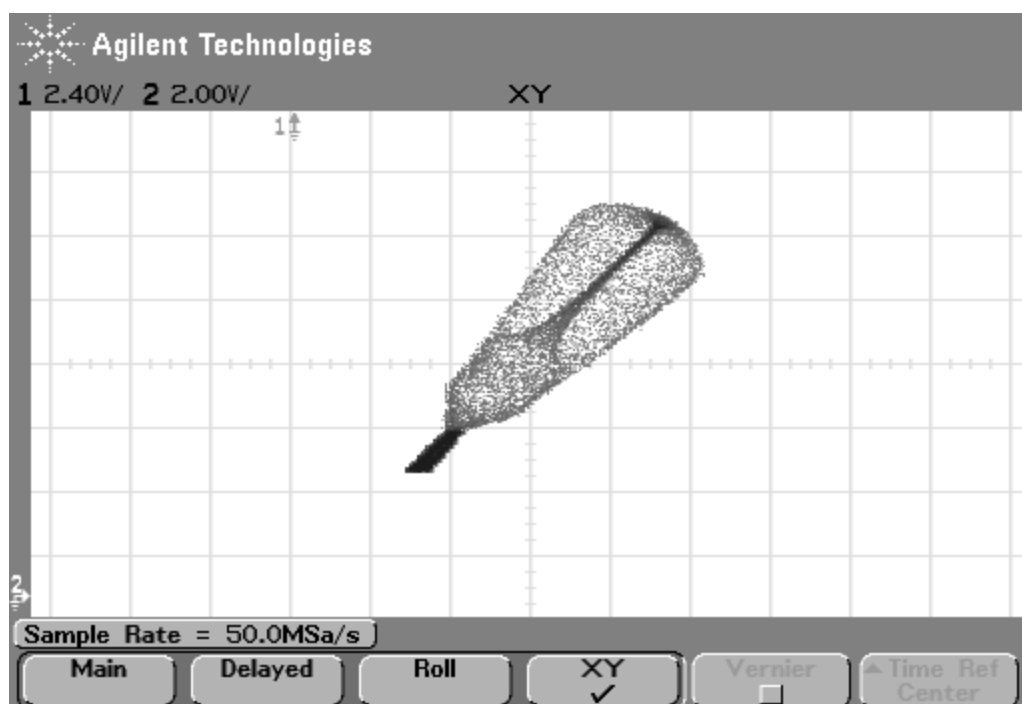


Figura 4.36: Hapësira fazore e gjeneruar nga oshiloskopi dixhital Agilent në XY mode kur sinjali hyrës ka amplitudë $V_0 = 11.5 \text{ Volts}$

4.4.1 Studimi i kontrollit të kaosit

Duke tentuar të arrijmë kontrollin e sinjalit kaotik kryhet studimi i varësisë së formës gjeometrike të atraktorit me sinjalin hyrës. Për këtë qëllim janë marrë disa raste kur amplituda e sinjalit sinusoidal i cili aplikohet tek hyrja e qarkut jo linear ndryshon nga $V_0 = 10\text{ Volts}$ në $V_0 = 11.5\text{ Volts}$ dhe $V_0 = 13\text{ Volts}$.

Në figurat 4.31, 4.33 dhe 4.35 paraqitet sinjali dalës dhe sinjali hyrës në qark kur amplituda e hyrjes është $V_0 = 13\text{ Volts}$, $V_0 = 10\text{ Volts}$ dhe $V_0 = 11.5\text{ Volts}$ respektivisht. Ajo që vihet re është se qarku ka ndikim tek sinjali hyrës (poshtë) pasi nuk merret pjesa e vlerave negative të sinjalit. Tek sinjali dalës paraqiten disa oshilime të frekuencave të larta të cilat analiza e serive kohore vërteton se janë sinjale kaotike.

Në figurat 4.32, 4.34 dhe 4.36 paraqitet hapësira fazore e qarkut kur amplituda e hyrjes është $V_0 = 13\text{ Volts}$, $V_0 = 10\text{ Volts}$ dhe $V_0 = 11.5\text{ Volts}$ respektivisht. Ashtu siç tregohet edhe tek figura 4.29 kemi një ngjashmëri midis hapësirës fazore të rindërtuar sipas metodës së vonesave me hapësirën fazore të marrë nga oshiloskopi.

4.5 Një qark kaotik me dy tranzistor

Një qark tjetër i propozuar është ai i paraqitur në figurën 4.37. Qarku përmban dy tranzistor BJT, një BC107BP (të tipit npn) dhe një të tipit BC177AP (të tipit pnp), në një konfiguracion me emiterin e përbashkët. Rezistenca e lidhur në kolektorin e tranzistoreve është $R_1 = R_2 = 30\Omega$ dhe rezistenca midis emiterit të çdo tranzistori dhe burimit të tensionit është $R_2 = 3.0\text{ k}\Omega$. Qarku është lidhur me një burim të rrymës alternative, i që prodhon një sinus me amplitudë V_0 i cili kalon në bazën e tranzistorit nëpërmjet një bobine $L = 55\mu\text{H}$. Qarku ushqehet nga dy burime të tensionit DC një $V_{cc} = 12\text{ V}$ dhe $V_3 = -12\text{ V}$

Qarku i cili paraqitet tek figura 4.37 është simuluar nëpërmjet programit MultiSim, i cili është një program i aprovuar gjerësisht për simulimin e qarqeve elektronike. Një

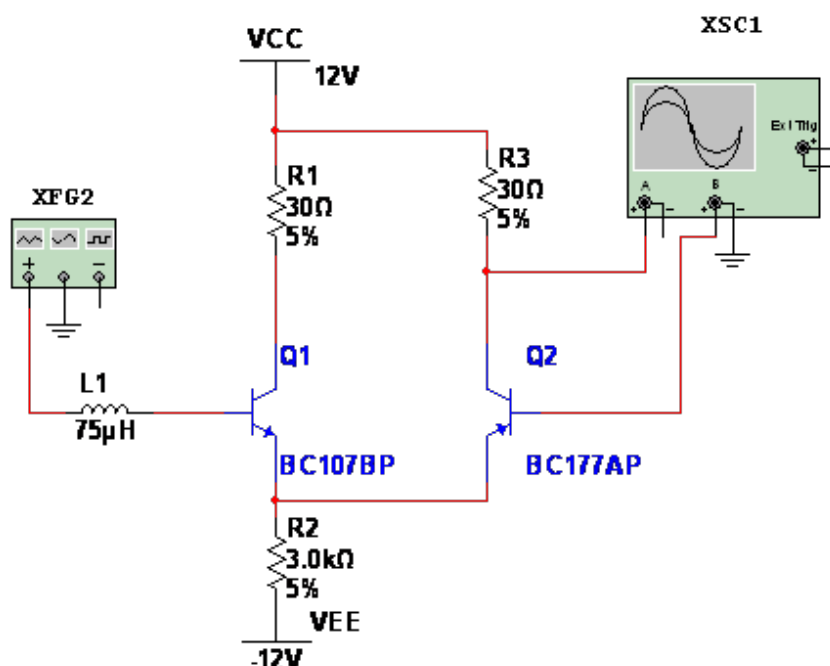


Figura 4.37: Qarku i propozuar si burim i sinjaleve kaotike

tjetër faktor, për zgjedhjen e programit të mësipërm është fakti që ofron një implementim të qarkut shumë afër realitetit.

Pas simulimit në figurën 4.38 paraqitet sinjali V_c i marrë në kolektorin e tranzistorit, i cili varet nga rryma që përshkruan kolektorin $i_c(t)$ dhe është një parametër i rëndësishëm, kur qarku kalon në veprim kaotik.

4.6 Analiza kohore e sinjalit të daljes

Aplikohet metoda e analizës së serive kohore të qarqeve jo lineare për të rindërtuar hapësirën fazore dhe për të kryer llogaritjet e eksponentit Lyapunov i cili do të tregojë prezencën ose jo të kaosit. Kjo metodë është paraqitur në kapitullin përkatës.

Si hap i parë është llogaritja e informacionin të përbashkët për të gjetur vonesën kohore τ . Vonesa kohore τ është ajo që na jep minimumin e parë të informacionit të përbashkët.

Për rastin konkret, pasi është kryer simulimi i qarkut të dhënat ruhen në një skedar

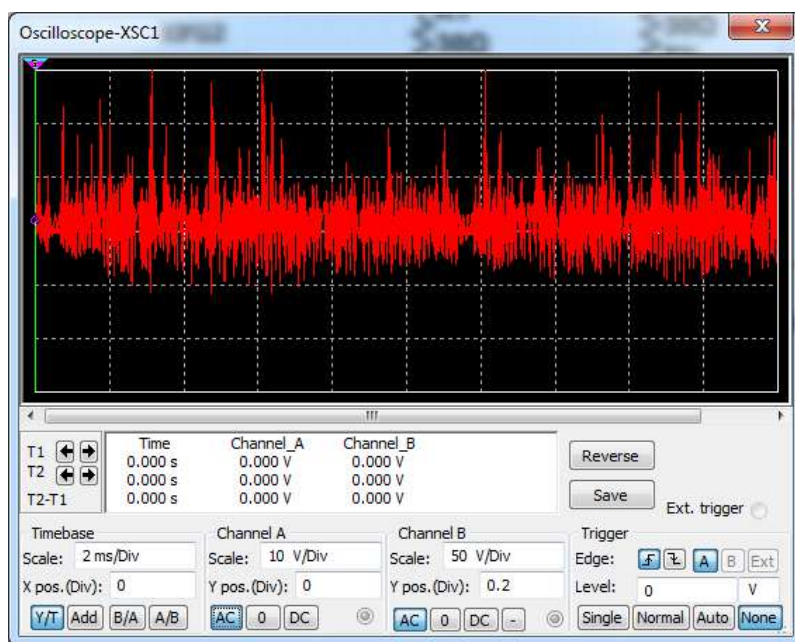


Figura 4.38: Seria kohore e sinjalit $V_C(t)$ ashtu siç llogaritet nga simulimi

.dat. Në vazhdimësi të dhënat përpunohen me anë të programit kompjuterik MATLAB dhe duke përdorur disa procedura të paketës TISEAN.

Llogaritja e informacionit të përbashkët

Për të llogaritur informacionin e përbashkët përdoret kodi i paraqitur në shtojcën përkatëse. Rezultati pas llogaritjes së informacionit të përbashkët në lidhje me vonesën kohore τ paraqitet tek figura 4.39.

Sipas llogaritjes minimumi i parë i informacionit të përbashkët korespondon me vonesën $\tau = 5$ në serinë kohore.

Llogaritja e shumatorit i korrelacionit

Për të analizuar sinjalin kaotik të propozuar në këtë qark përdoret metoda e shumatorit të korrelacionit (correlation sum)[43]. Kjo metodë është aplikuar në raste të tjera kur seria kohore vjen nga një qark i thjeshtë elektronik [44].

Le të supozohet një atraktor i cili përbëhet nga x_i pika dhe përkufizojmë proba-

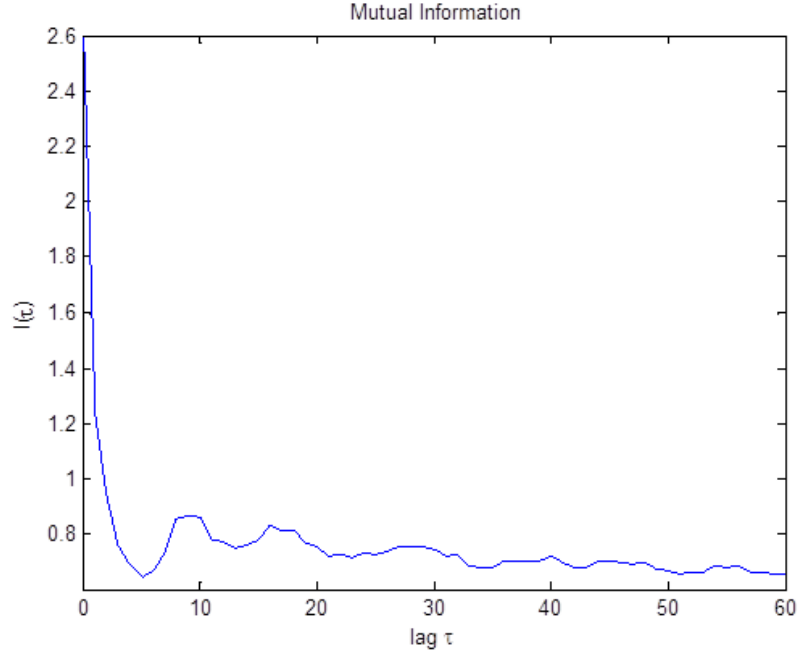


Figura 4.39: Informacioni i përbashkët në lidhje me 4.37

bilitetin $P((x_i - x_j) < r)$ distanca e dy pikave në hapësirën fazore.

Për një bashkësi pikash $\{x_i\}$, $i = 1, \dots, N$ të trajektores në hapësirën fazore të rindërtuar nga të dhënat e serisë kohore, llogaritet shumatori i korrelacionit (correlation sum) $C(r)$.

$$C(r) = \frac{1}{N_{\text{çifte}}} \sum_{\substack{l=1 \\ j=l+W}}^N H(r - \|\vec{X}_l - \vec{X}_j\|) \quad (4.18)$$

Ku funksioni $H(x)$ është funksioni Heaviside:

$$H(x) = \begin{cases} 0 & \text{kur } x \leq 0 \\ 1 & \text{kur } x > 0 \end{cases}$$

dhe llogaritja e numrit të çifteve të serisë kohore llogaritet nga funksioni më poshtë.

$$N_{\text{çifte}} = \frac{2}{(N - m + 1)(N - m + W + 1)} \quad (4.19)$$

Shumatori llogarit të gjitha çiftet e mundshme (x_i, x_j) të cilat kanë distancë me të

vogël se r . Për $N \rightarrow \infty$ dhe $r \rightarrow 0$ llogaritet dimensioni i korrelacionit:

$$\nu = \frac{d \log C(r)}{d \log r} \quad (4.20)$$

Për të karakterizuar një sistem nga dimensioni i korrelacionit ν duhet llogaritur shumatori i korrelacionit për disa vlera të ndryshme të dimensionit të ngulitur m . Pritet se dimensioni i korrelacionit ν në lidhje me dimensionin e ngulitur ν do të jetë si në vazhdim: Për vlera të vogla të m , rindërtimi i atraktorit nuk do të jetë i mjaftueshëm, dhe ν do të rritet në lidhje me m .

Për vlera më të mëdha në segmentin linear të gjitha vlerat do të tentojnë një vlerë të caktuar.

4.7 Konkluzione

Të tre qarqet e realizuara në laborator janë qarqe që veprojnë në mënyrë kaotike. Qarku i parë i prezantuar është qarku Chua dhe veprimi i tij kaotik u vërtetua në laborator por edhe me simulim duke përdorur programin Multisim.

Në vazhdimësi paraqiten dy qarqe të propozuara nga autori si qarqe që operojnë në mënyrë kaotike. Prezenca e kaosit u vërtetua nga përpunimi i serisë kohore.

Përparësia e qarqeve të propozuara është thjeshtësia e realizimit të tyre. Sigurisht që thjeshtësia e tyre ka lidhje dhe me koston sepse qarqet e propozuara përbëhen nga pak komponentë relativisht të lira.

Nga ana tjetër qarqet e propozuara duhet të funksionojnë me një burim rryme alternative të jashtme, fakt i cili rrit koston dhe kompleksitetin e realizimit të tyre. Janë bërë përpjekje për implimentimin e një sistemi ku dy qarqe ose me një tranzistor ose me dy të sinkronizohen, duke dhënë të njëjtën sinjal AC. Si përfundim sinkronizimi nuk u arrit dhe për këtë arsye vazhdon të studiohet rasti i sinkronizimit të dy qarqeve Chua.

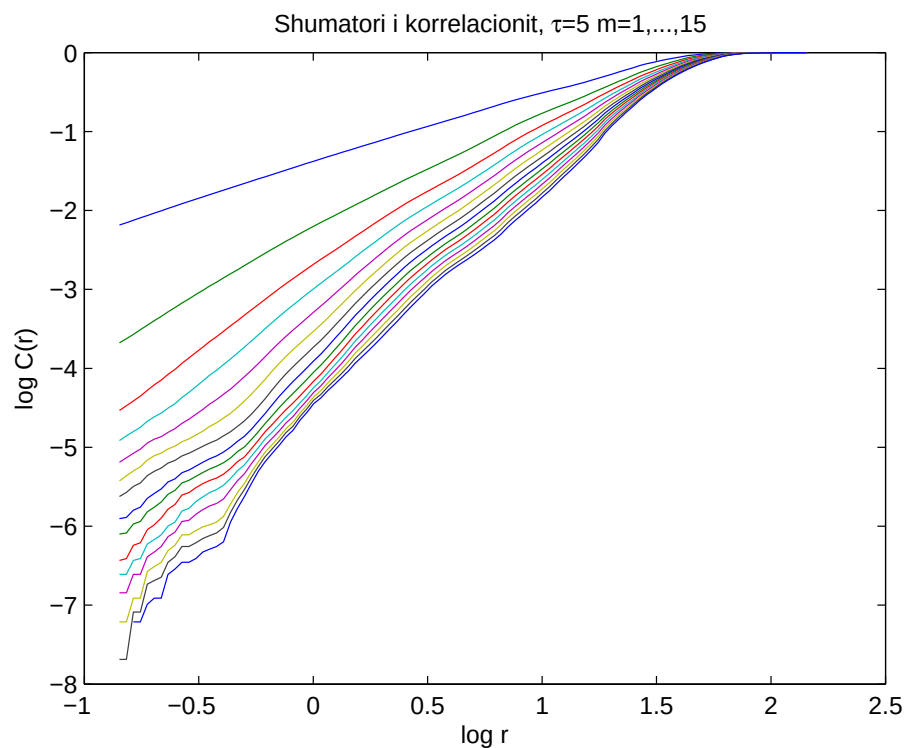


Figura 4.40: Llogaritja e shumatorit të korrelacionit (correlation sum) në lidhje me logaritmin e distancës

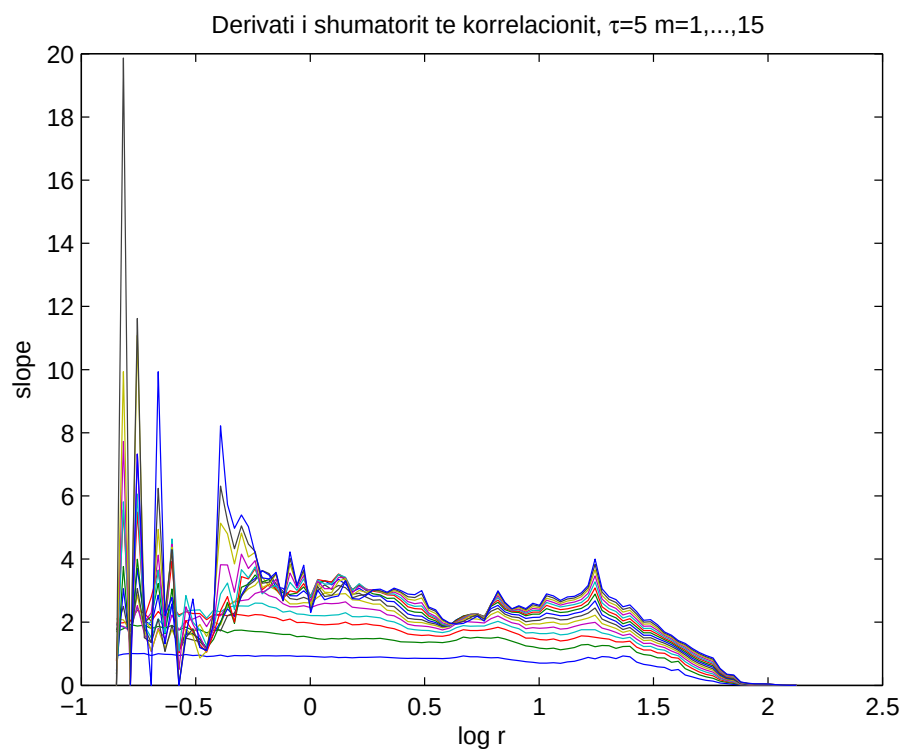


Figura 4.41: Llogaritja e derivatit të shumatorit të korrelacionit për të gjetur dimensionin e korrelacionit.

Kapitulli 5

Sinkronizimi

Sinkronizimi është një nga problemet kryesore në projektimin e një sistemi telekomunikacioni.

Sistemet kaotike janë të ndjeshëm ndaj kushteve fillestare dhe divergjojnë në mënyrë eksponenciale. Edhe në qoftë se ekziston një diferencë sadopak e vogël në kushtet fillestare, dy sisteme identike mund të operojnë në mënyrë krejtësisht të ndryshme. Sinkronizimi i dy ose me shumë sistemeve, është një dukuri në të cilën keto sisteme shfaqin të njëjtin veprimtar duke përdorur një sinjal referencë.

5.1 Paraqitja teorike

Një nga metodat që janë studiuar më shumë për sinkronizimin e qarqeve kaotike është metoda Pecora dhe Carroll [?]. Ata supozuan një sistem autonom me n përmasa, i cili përshkruhet nga ekuacioni

$$\frac{dx}{dt} = f(x(t)) \quad (5.1)$$

Ata propozuan zbërthimin e sistemit fillestar në dy nënsisteme kështu që matrica e gjëndjeve është:

$$x = \begin{bmatrix} x_p \\ x_s \end{bmatrix} \quad (5.2)$$

ku nënsistemi P sistemi primar i cili konsiderohet si sistemi udhëzues dhe S është sistemi sekondar. Atëherë:

$$\begin{cases} \dot{x}_p = g(x_p, x_s) \\ \dot{x}_s = h(x_p, x_s) \end{cases} \quad (5.3)$$

Në përgjithësi është propozuar krijimin e një kopje të sistemit primar i cili udhëzohet nga sinjali x_p që vjen nga sistemi primar. Në qoftë se diferenca $\Delta x_R = x_s - x_R$ tenton zeron për $T \rightarrow \infty$ atëherë sinjalet e prodhuara nga sistemi primar dhe sekondar janë asimptotë midis tyre, domethënë janë të sinkronizuara.

Kjo metodë është aplikuar gjerësisht në sisteme të ndryshme kaotike.

5.2 Sinkronizimi i qarkut të Chuas

Në kapitullin paraardhës u prezantua qarku i Chuas. Në këtë kapitull propozohet një mënyrë sinkronizimi i këtij qarku si dhe rezultatet.

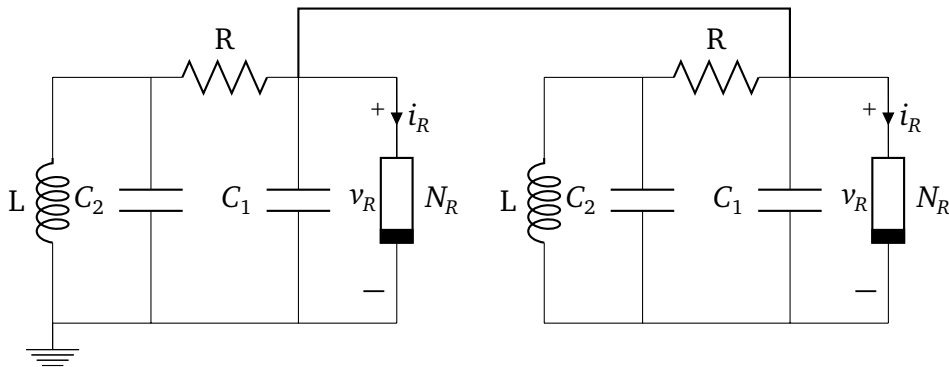


Figura 5.1: Mënyra e sinkronizimit të qarkut të Chuas

Mënyra e sinkronizimit e propozuar nga metoda Pecora-Carroll paraqitet tek figura 5.6. Në këtë rast të dy tensionit v_1 tek kondensatori i qarkut primar vendosen mbi

kondensatorin e qarkut sekondar. Kështu që $v_{11} = v_{12}$. Për rastin në studim ekuacionet e qarkut Chua për sistemin primar do të jenë si më poshtë:

$$\begin{aligned} C_{11} \frac{dv_{11}}{dt} &= \frac{v_{21} - v_{11}}{R} - h(v_{11}) \\ C_{21} \frac{dv_{21}}{dt} &= \frac{v_{11} - v_{21}}{R} + i_{L1} \\ L_1 \frac{di_{L1}}{dt} &= -v_{21} \end{aligned} \quad (5.4)$$

dhe ekuacionet diferenciale të qarkut sekondar:

$$\begin{aligned} C_1 \frac{dv_{12}}{dt} &= \frac{v_{22} - v_{12}}{R} - h(v_{12}) \\ C_2 \frac{dv_{22}}{dt} &= \frac{v_{12} - v_{22}}{R} + i_{L2} \\ L \frac{di_{L2}}{dt} &= -v_{22} \end{aligned} \quad (5.5)$$

Kushtet fillestare dhe kushti për të sinkronizuar qarqet janë:

$$\begin{aligned} v_{11} &= v_{12} \\ v_{21} &= v_{22} = 0 \\ i_{L1} &= i_{L2} = 0 \end{aligned} \quad (5.6)$$

5.3 Studimi sipas raportit sinjal mbi zhurmë

Sistemi i paraqitur në ekuacionet 5.4 dhe 5.5 duke marrë parasysh kushtet fillestare 5.6 zgjidhet duke përdorur metodën Euler me hap integrimi të vogël. Për të studiuar sinkronizimin e qarkut merren raste të ndryshme të cilësisë të sinjalit.

Cilësia e sinjalit matet nga raporti sinjal mbi zhurmë. Zhurma gjenerohet duke përdorur komandën *randn()* në sistemin MATLAB, e cila gjeneron numra rastësorë me shpërndarje normale. Vlera mesatare e shpërndarjes është $\bar{x} = 0$ dhe devijimi

standard i saj është $\sigma = 1$. Sinjali i sinkronizimit në qarkun sekondar do të jetë:

$$v_{11} = v_{12} + n$$

ku n është sinjali i zhurmës. Raporti sinjal mbi zhurmë llogaritet nga ekuacioni i mëposhtëm [?]:

$$SNR = \frac{P_{sinjali}}{P_{zhurme}} \quad (5.7)$$

ku $P_{sinjali}$ është fuqia e sinjalit dhe P_{zhurme} është fuqia e zhurmës. Fuqia e një sinjali $x(t)$ llogaritet nga

$$P = \frac{1}{T} \int_0^{\infty} x^2 dt$$

por për rastin e simulimit përdoret marrëdhënia e mëposhtme për arsye se sinjali i simuluar është diskret:

$$P = \frac{1}{N} \sum_{n=1}^N x_n^2$$

i cili shprehet në decibel si më poshtë:

$$SNR_{dB} = 10 \log \left(\frac{P_{sinjali}}{P_{zhurme}} \right) \quad (5.8)$$

atëherë, për të studiuar sinkronizimin e qarkut primar dhe sekondar merren rezultatet e ndryshme për nivele të ndryshme të raportit sinjal zhurmë.

Si fillim marrim rastin kur zhurma është shumë e vogël në raport me sinjalin. Në qoftë se në sinjal nuk ka zhurmë, atëherë SNR tenton infinitin, ky rast nuk është real prandaj nuk studiohet. Në rastin e parë marrim një sinjal prej $SNR = 11.9dB$ dhe simulohet sistemi i përshkruar në ekuacionet 5.4 dhe 5.5. Në figurën 5.2 paraqitet tensioni në kondensatorin C_1 të sistemit primar me atë të sistemit sekondar. Vihet re që është që sistemi është i sinkronizuar, domethënë kemi një marrëdhënie $v_{21} = v_{22}$, ashtu siç pritej nga teoria.

Në vazhdimësi kryhet simulimi i sistemit për një vlerë tjetër të raportit sinjal mbi

zhurmë. Në këtë rast $SNR = 5dB$, rezultati i simulimit paraqitet tek figura 5.3. Këtu kemi përsëri sinkronizim por shohim që në figurë kemi disa devijime nga rezultati prej 0.3%.

Në vazhdimësi studiohen rastet kur $SNR = -11dB$ ku rezultati i simulimit paraqitet tek figura 5.4 dhe $SNR = -19dB$ në figurën 5.5. Vlera negative e raportit sinjal mbi zhurmë tregon se fuqia e sinjalit është më e madhe se sa fuqia e zhurmës. Në keto dy raste të studiuara kemi prishjen e sinkronizimit. Si rezultat për të përdorur qarkun në një sistem kriptografie duhet që raporti sinjal mbi zhurmë të jetë pozitiv.

Për të parë më mirë sinkronizimin në varësi kryhet regresi linear midis vlerave të tensionit tek qarku primar dhe tek ai sekondar ashtu siç u tha dhe më përpara pritet që të ekzistojë një marrëdhënie $y = x$ ose ndryshe $v_{11} = v_{12}$. Në tabelën e mëposhtme paraqiten vlerat e ekuacionit të drejtëzës për çdo rast të raportit sinjal mbi zhurmë bashkë me koeficientin e përcaktueshmërisë R^2 .

SNR	Ekuacini i drejtëz midit v_{21} dhe v_{22}	R^2
11 dB	$v_{22} = 1.0001v_{21} - 0.0001$	1.0000
5 dB	$v_{22} = 1.0002v_{21} - 0.0001$	1.0000
-14 dB	$v_{22} = 0.99155v_{21} + 0.002481$	0.9975
-19 dB	$v_{22} = 1.0058v_{21} + 0.0233$	0.9898

Tabela 5.1: Vlerat e SNR dhe ekuacionet e drejtëzës që lidhin v_{11} dhe v_{12}

Vihet re se me rritjen e zhurmës koeficienti i përcaktueshmërisë zvogëlohet. Në rastet e komunikimeve duhet që sinkronizimi të jetë absolut, sepse sistemet janë të ndjeshëm ndaj kushteve fillestare dhe një ndryshim i vogël mund të shkaktoj prishjen e sinkronizimit. Si përfundim konkluzion raporti sinjal mbi zhurmë duhet të jetë gjithmonë pozitiv që të arrihet sinkronizimi i dy qarqeve.

5.4 Studimi sipas dobësimit të sinjalit

Një tjetër studim i sinkronizimit të dy qarqeve Chua kryhet në lidhje me dobësimin e sinjalit. Ky studim simulon dobësimin e sinjalit kur ai transportohet në distanca të

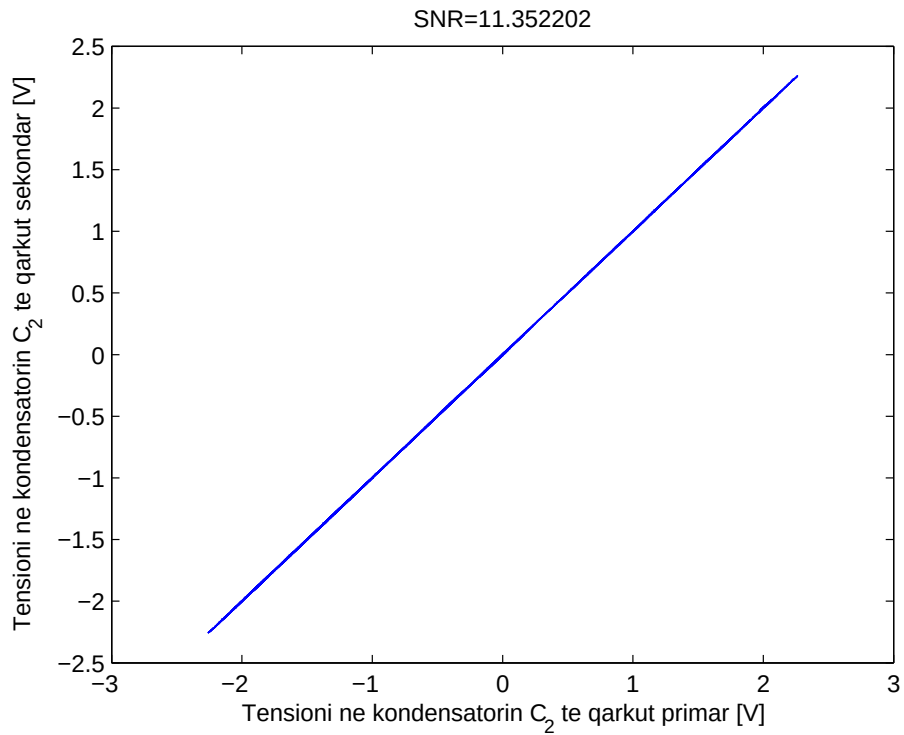


Figura 5.2: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=11dB

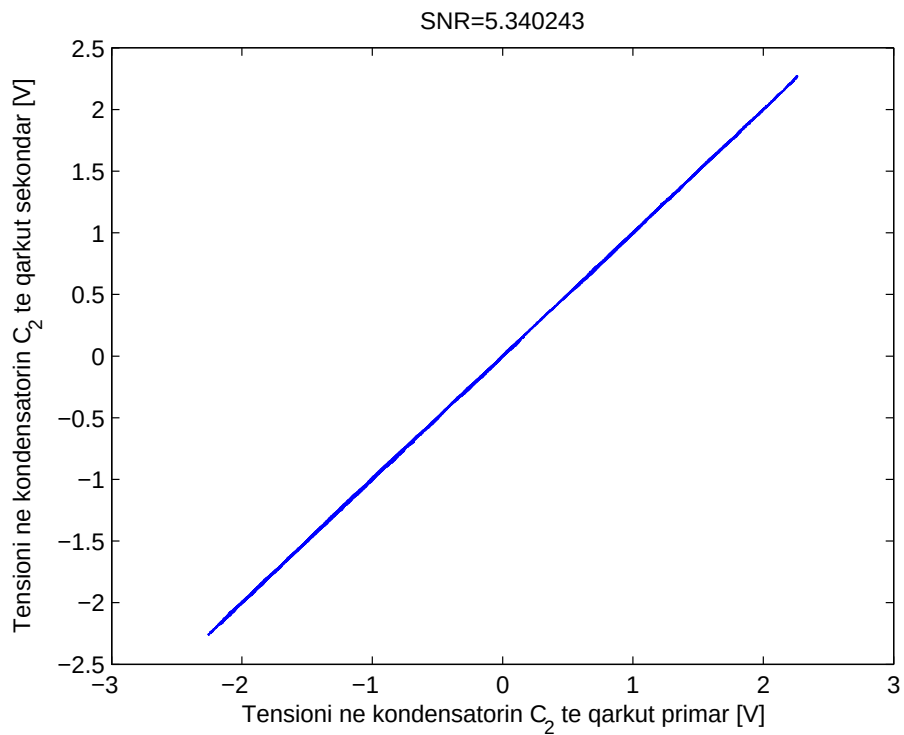


Figura 5.3: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=5dB

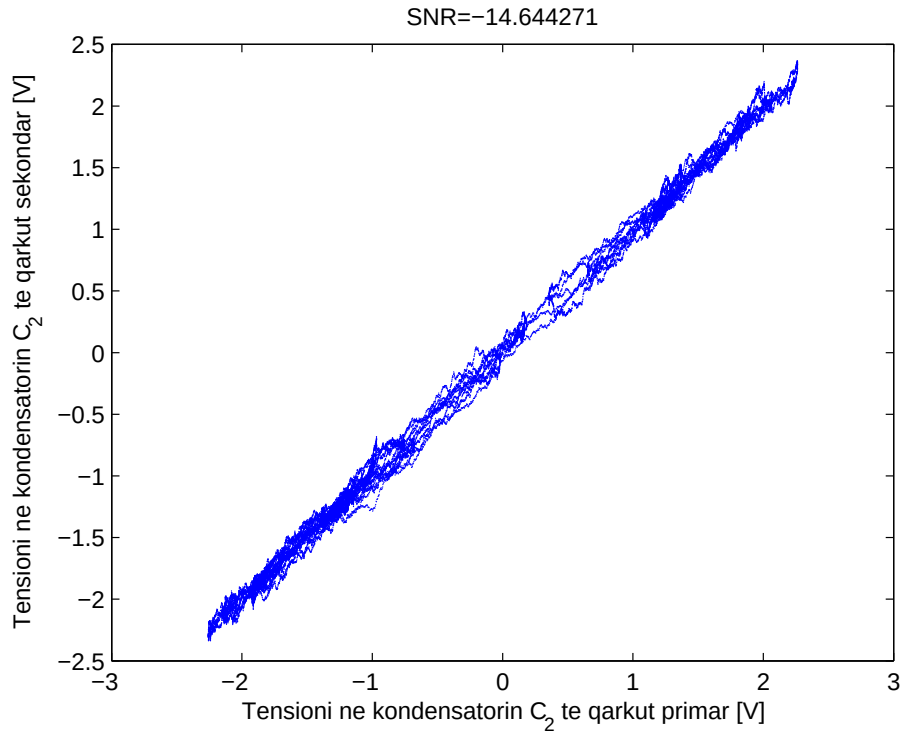


Figura 5.4: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=-14dB

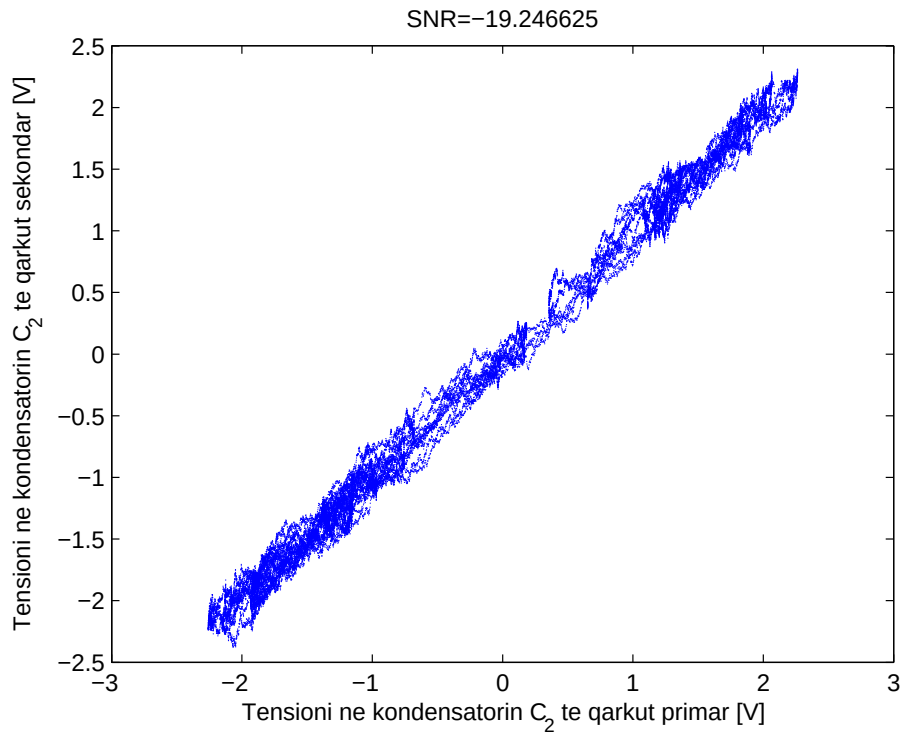


Figura 5.5: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur sinjali ka SNR=-19dB

largëta. Atëherë në këtë rast nuk plotësohet kushtin $v_{12} = v_{11}$ por do kemi një 5.4 dhe 5.5 në këtë rast kushtet fillestare do të jenë:

$$\begin{aligned} v_{22} &= v_{21} = 0 \\ v_{12} &= v_{11} - i_s R \\ i_{L1} &= i_{L2} = 0 \end{aligned} \quad (5.9)$$

Në figurën 5.6 paraqitet qarku i realizuar në Multisim për kryerjen e simulimit. Një rezistencë R_v është vendosur midis qarkut primar dhe atij sekondar.

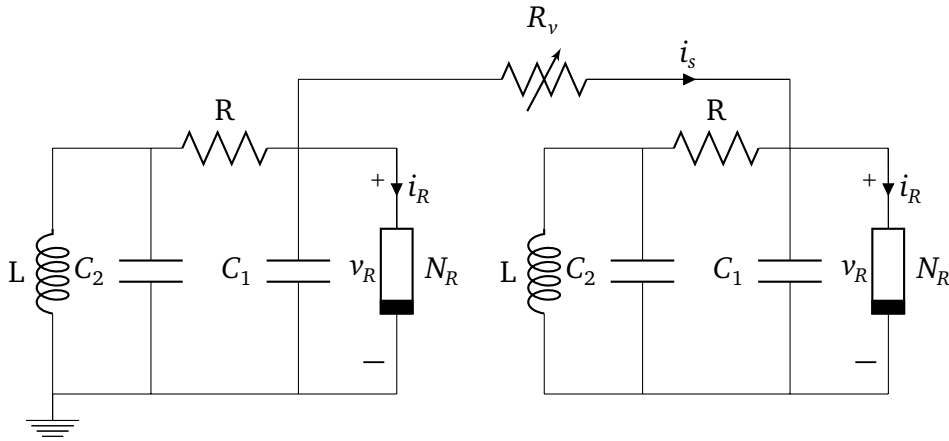


Figura 5.6: Mënyra e sinkronizimit të qarkut të Chuas

Në figurë 5.7 paraqitet hapësira fazore kur rezistenca në linjën e transmetimit është $R_v = 0\Omega$, dhe në figurën 5.8 paraqitet sinkornizmi midis tensionit në kondensatorin C_1 të sistemit sekondar në varësi të atij primar. Për rastin kur $R_v = 3.5 k\Omega$ rezultatet paraqiten në figurat 5.9 dhe 5.10 dhe për rastin kur $R_v = 10 k\Omega$ në figurat 5.11 dhe 5.12.

Ashtu siç mund të shihet në figurat përkatëse kemi prishjen e sinkronizimit kur rezistenca në linjën e transmetimit të sinjalit të sinkronizimit bëhet $R_v = 10 k\Omega$. Kjo tregon se sinkronizimi varet nga distanca për arsye se sa më e madhe të jetë distanca aq me e madhe do të jetë edhe linja që transmeton sinjalin e sinkronizimit.

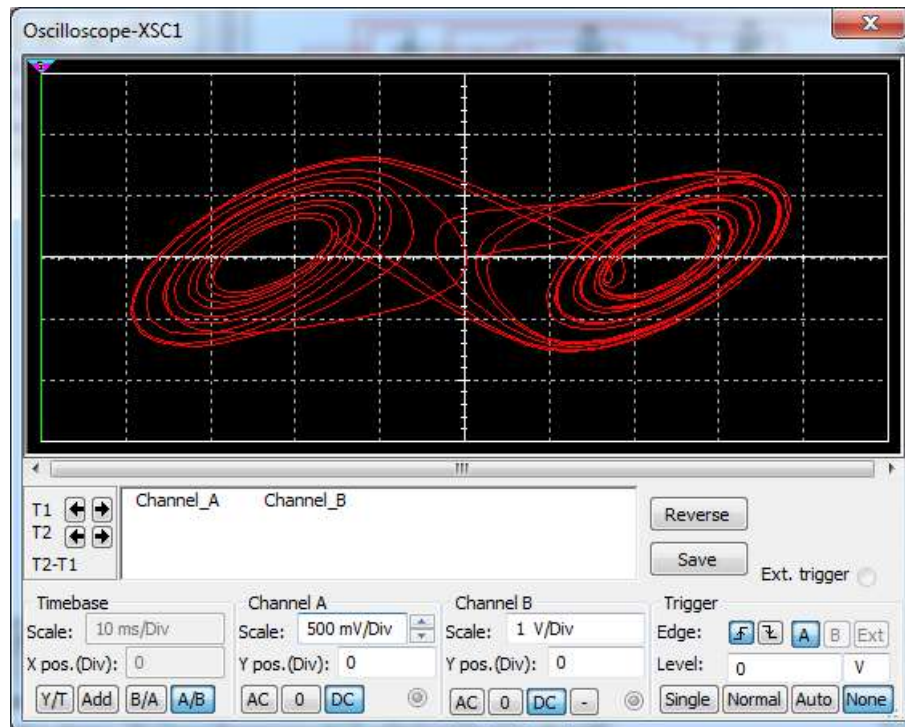


Figura 5.7: Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 0 \Omega$

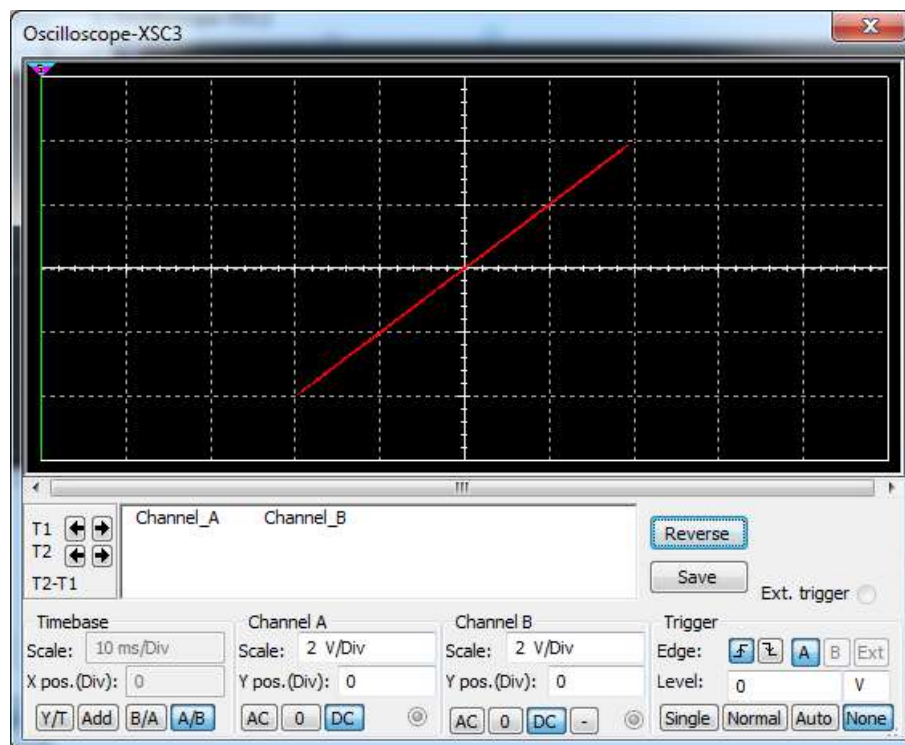


Figura 5.8: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 0 \Omega$

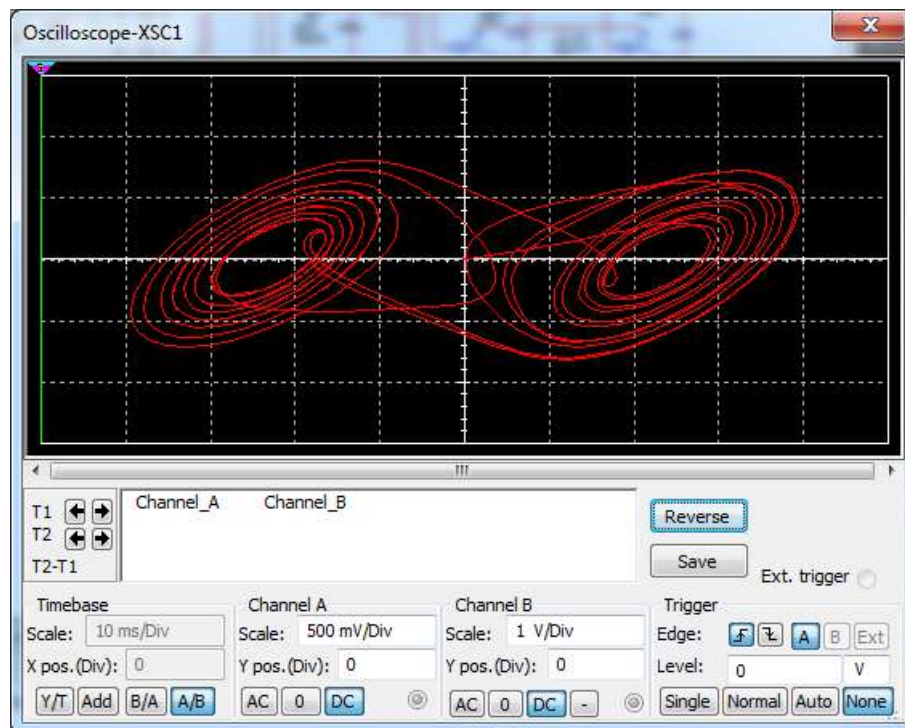


Figura 5.9: Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 3.5 \text{ k}\Omega$

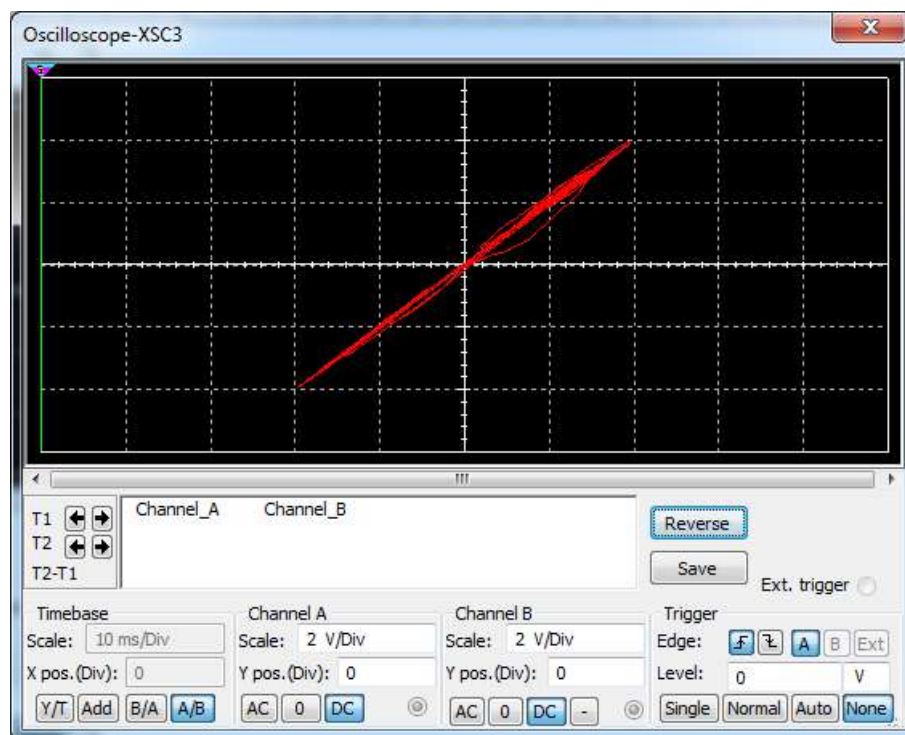


Figura 5.10: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 3.5 \text{ k}\Omega$

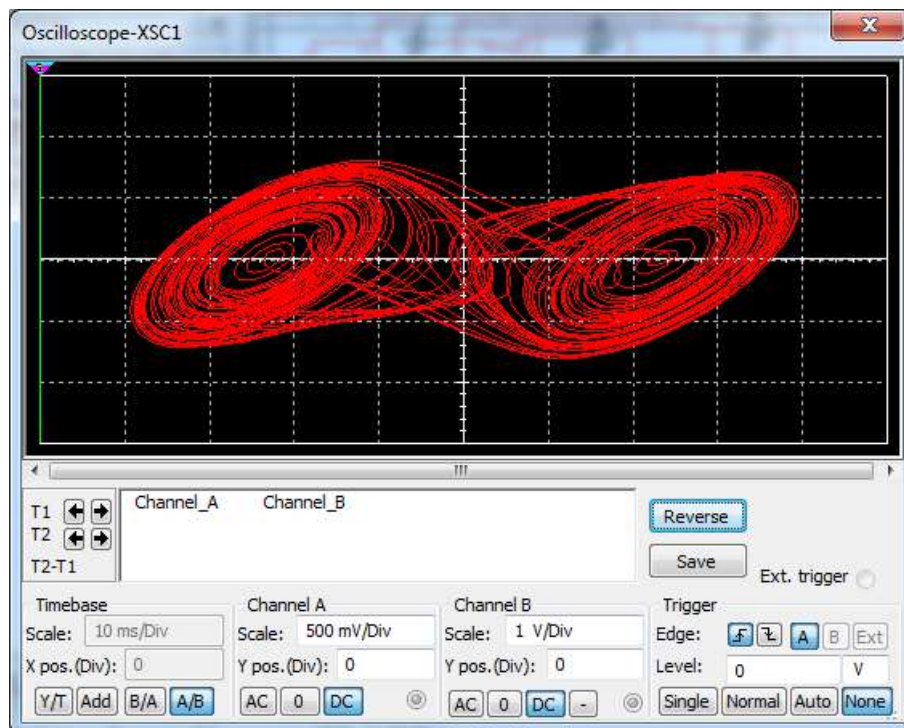


Figura 5.11: Paraqitja e hapësirës fazore të qarkut Chua për $R_v = 10\text{ k}\Omega$

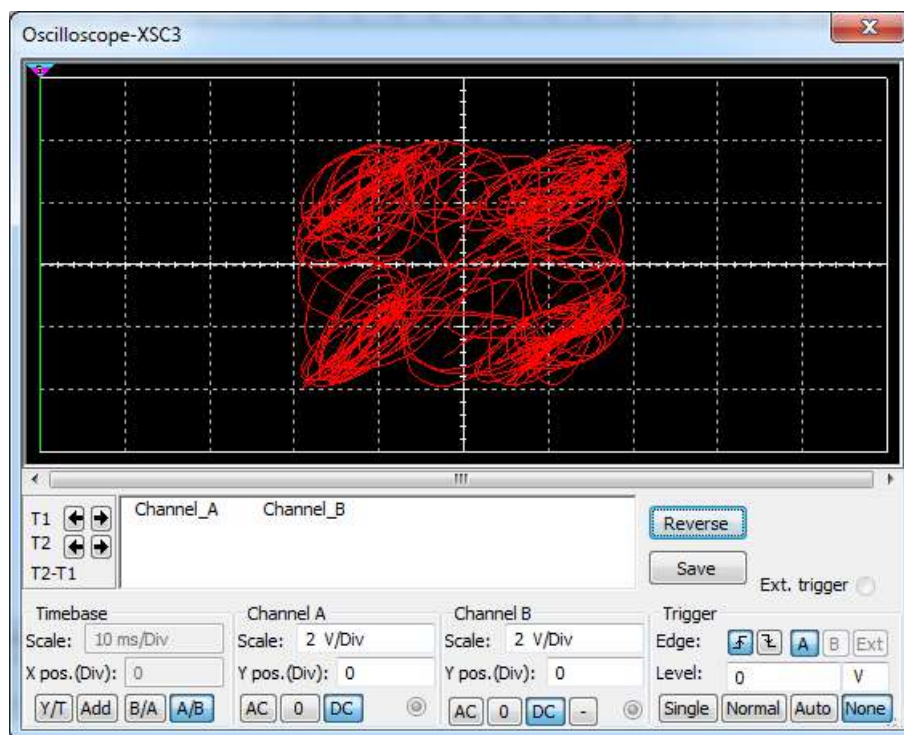


Figura 5.12: Tensioni në kondensatorin C_2 të sistemit sekondar në varësi të atij primar kur $R_v = 10\text{ k}\Omega$

Kapitulli 6

Kriptografia në komunikime dixhitale duke përdorur kaos

Në këtë kapitull analizohet aplikimi i kaos-it për qëllime kriptografike. Teknologjia që paraqitet në këtë kapitull ka të bëjë me përdorimin e një metode analoge të kriptografisë për të anashkaluar vështirësitë e metodave dixhitale. Teknika që parashtrohet në këtë kapitull ka të bëjë me kodimin analog kaotik dhe deshifrimin e tij. Mesazhet, për tu transmetuar kodohen duke përdorur kaosin e gjeneruar nga një burim i cili i analizua në kapitujt e mëparshëm. Çelësi i komunikimeve kaotike është sinkronizimi i kaosit, çështje e diskutuar më lart. Në komunikimet e tilla një mesazh bashkohet me një sinjal mbajtës kaotik dhe ky sinjal transmetohet, duke hequr nga sinjali i cili u transmetua sinjalin kaotik mesazhi deshifrohet saktësisht.

Në këtë kapitull paraqiten metodat e kriptografisë kaotike të cilat janë propozuar nga literatura. Këto sisteme janë maskim me kaos - Chaos Masking (CMA), modulimi me sinjal kaotik - Chaos Modulation (CMO), dhe Chaos Shift Keying (CSK). Kryhet simulimi i këtyre dy metodave duke përdorur qarkun Chua si burim kaosi.

Paraqiten bllok skemat e secilës metodë dhe kryhet një simulim i kodimit dhe i dekodimit duke përdorur programin MATLAB dhe duke përdorur si burim kaosi qarkun Chua. Nga rezultate e simulimit nxirren konkluzione për përparësitë dhe

mangësitë e secilës metodë.

6.1 Maskim me kaos - Chaos Masking (CMA)

Në figurën 6.1 paraqitet bllok skema e një sistemi kodimi maksim me kaos. Mesazhi i shkurtër $m(t)$ bashkohet me një mbajtës kaotik $x(t)$ në sistemin e transmetuesit, në kanal transmetohet sinjali $x(t) + m(t)$. Sistemi marrës është i njëjtë me sistemin e transmetimit dhe operojnë të dy me të njëjtat parametra. Vetëm sinjali kaotik rigjen-erohet tek sistemi marrës.

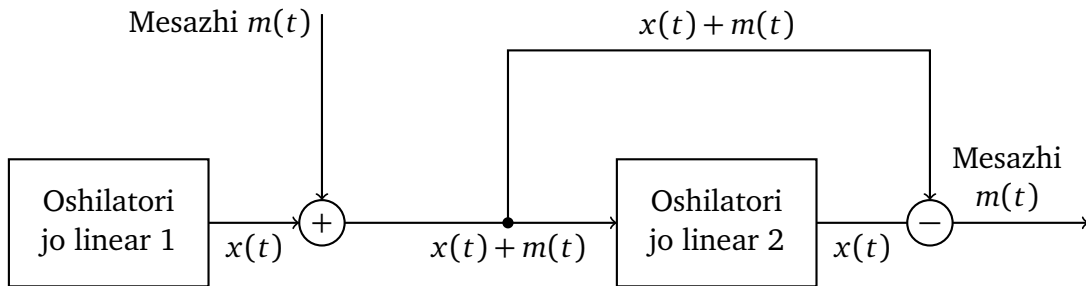


Figura 6.1: Bllok skema e sistemit me maskim kaotik (CMA)

Në vazhdimësi, mesazhi $m(t)$ dekodohet duke hequr sinjalin kaotik $x(t)$ nga sinjali i marrë $x(t) + m(t)$. Për të fshehur mesazhin me siguri brenda në kaos (përdorimi si “maskë”) dhe të dekodohet me cilësi të lartë, amplituda e tij duhet të jetë e vogël krahasuar me sinjalin kaotik. Në shumicën e rasteve fuqia e mesazhit është më pak se sa 1% e fuqisë mesatare të sinjalit kaotik. [?]

6.1.1 Realizimi i kaotik masking

Në vazhdimsi paraqitet një sistem kriptografie sipas metodës maskim me kaos te paraqitur në figurën 6.1. Sistemi është bazuar tek qarku Chua. Përdoret sinjali kaotik që merret nga kondensatori C_1 (fig 6.2), ashtu siç shihet në figurë sinjali ka vlera midis 3V dhe -3V. Atëherë për të fshehur mesazhin përdoret një sinjal që merr vlera -0.1 V

për vlerën llogjike '0' dhe 0.1 V për vlerën llogjike '1'. Ky mesazh i shtohet sinjalit kaotik dhe mbledhja e këtyre është sinjali i cili do të transmetohet.

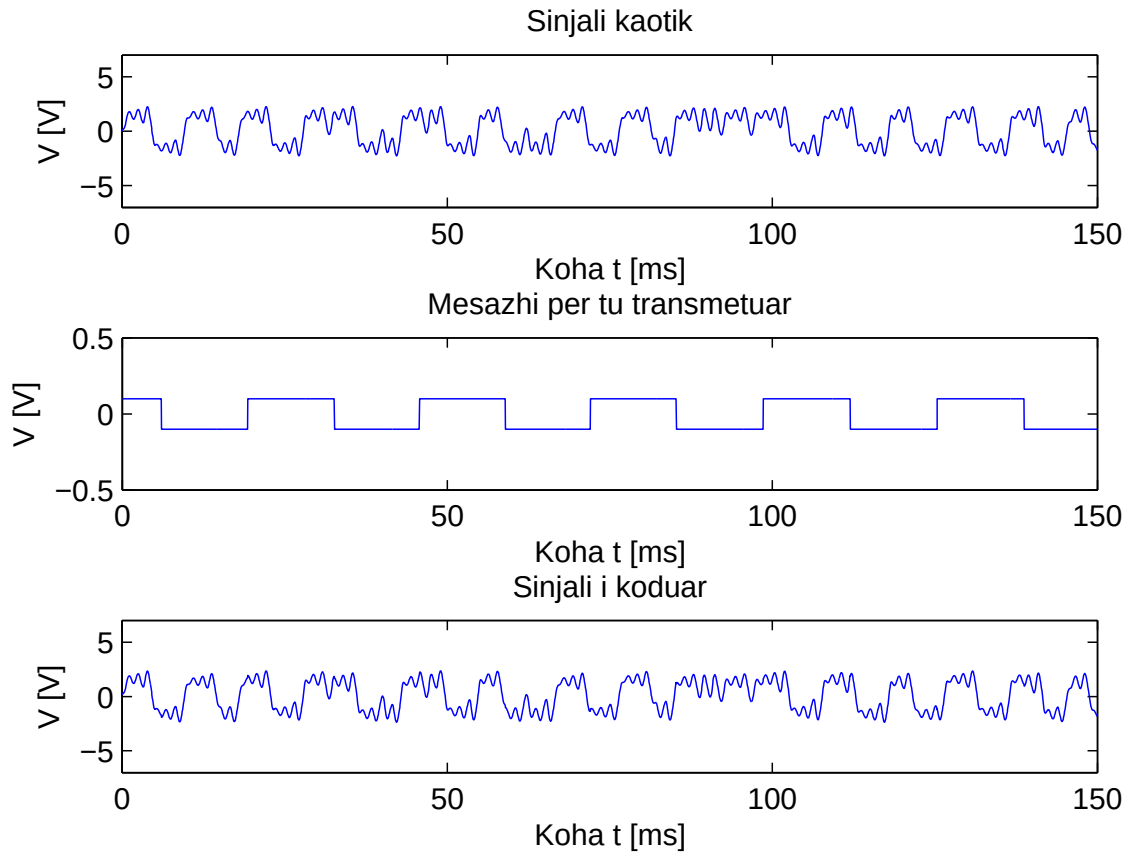


Figura 6.2: Sinjalet për metodën maskim me kaos

Për të deshifruar sinjalin e transmetuar është i nevojshëm sinkronizimi perfekt midis sistemit marrës dhe atij transmetues. Në 6.3 paraqitet rezultati si simulimit të dekodimit sipas sistemit CMA. Ajo që vihet re është se sinjali është jarzakonisht i ndjeshëm në lidhje me zhurmën e kanalit. Për se ashtu siç u përmend më sipër fuqia e duhet të jet më pak se sa 1% të sinjalit kaotik, bën këtë skeme të vështirë për tu realizuar.

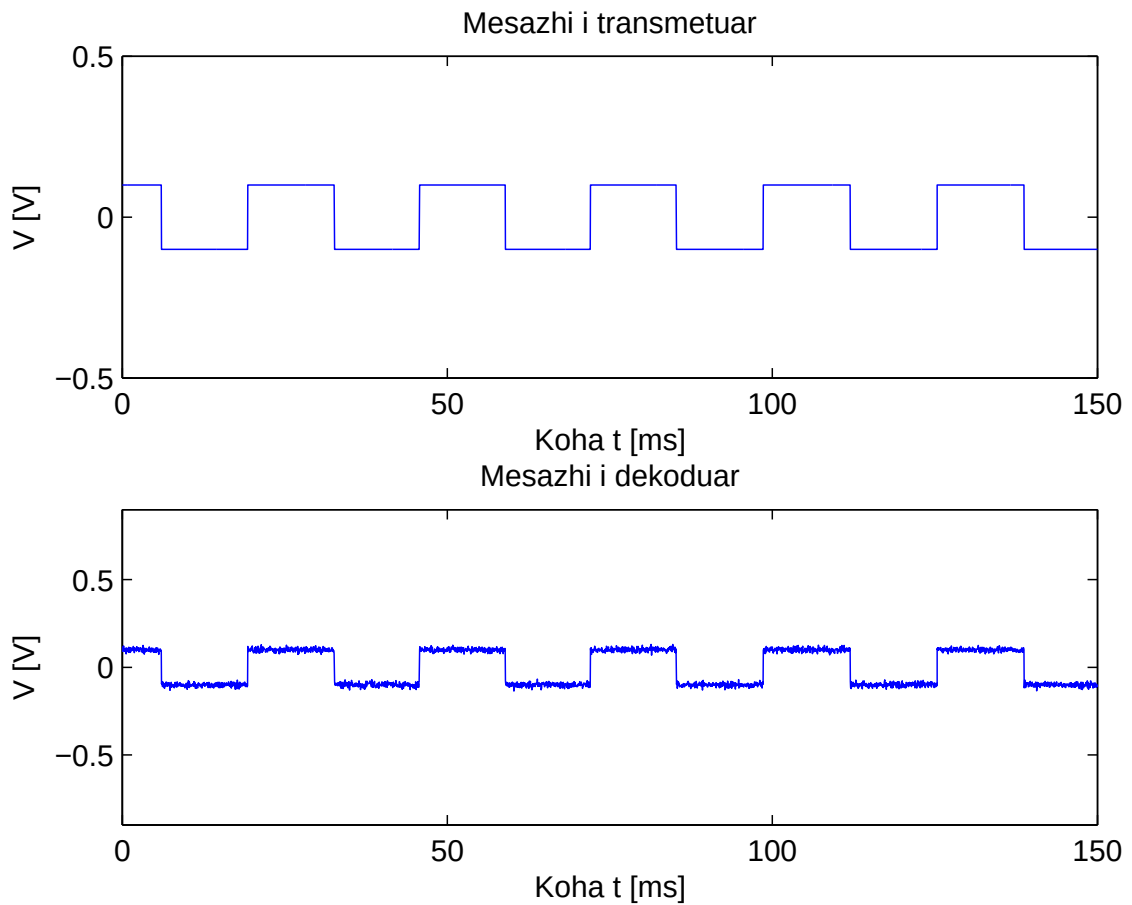


Figura 6.3: Sinjalet për metodën maskim me kaos

6.2 Modulimi me sinjal kaotik - Chaos Modulation (CMO)

Në figurën 6.6 paraqitet sistemi CMO, në këtë rast dhe sinjali kaotik por edhe mesazhi për transmetim krijojnë një lëkundje të re të sistemit jo linear. Kështu që ndryshe nga sistemi CMA në këtë rast mesazhi për transmetim mund të mos jetë i vogël. Sistemi i transmetimit dhe sistemi marrës përshkruhen matematikisht nga të njëjtat ekuacione diferenciale kështu arrihet sinkronizimi kaotik, dhe në dalje arrihet një sinjal totalisht i sinkronizuar me atë të transmetuesit. Edhe pse metoda ngjan me metodën CMA, në thelb është teknikë e ndryshme. Ashtu siç tregohet edhe tek figura 6.2, mesazhi bashkohet me mbartësin kaotik dhe të dy sinjalet krijojnë një

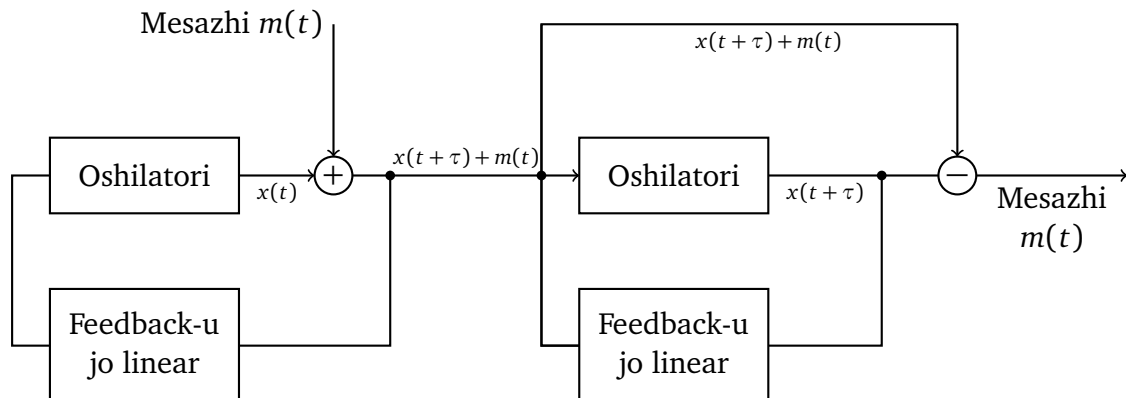


Figura 6.4: Bllok skema e sistemit CMO

gjendje kaotike, ndryshe nga ajo fillestare. Sistemi CMO, përdor një sistem feedback me vonesë si gjenerator kaosi. Sinjali i ri kaotik jepet nga $x(t + \tau) = f(x(t) + m(t))$, pas një vonesë kohore τ , ku f është funksioni jo linear i sistemit. Ky sinjal i ri bashkë me mesazhin $x(t + \tau) + m(t + \tau)$ transmetohen nga sistemi. Pasi transmetues dhe marrësi janë sisteme lineare identike, lëkundja kaotike $x(t + \tau) = f(x(t) + m(t))$ rigjenerohet totalisht në sistemin marrës (sinkronizim kaotik). Me heqjen e sinjalit të sinkronizuar kaotik $x(t + \tau)$ nga sinjali $x(t + \tau) + m(t + \tau)$ i cili u transmetua, është i mundur dekodimi i mesazhit i cili u transmetua. Në disa raste, mesazhi dekodohet me pjestim të sinjalit të transmetuar me sinjalin e sinkronizuar në marrje. Nga ana e kodimit dhe të dekodimit të mesazhit, metoda CMO nuk imponon asnjë kufizim në lidhje me amplitudën që duhet të kenë mesazhi, për arsye të krijimit të gjendjeve të reja në sistemet jo lineare (nga bashkimi i sinjalit mbartës dhe të mesazhit). Duhet theksuar, se në rastet kur gjatësia e mesazhit bëhet e madhe atëherë niveli i sigurisë në transmetimin e të dhënave ulet. Për këtë arsye, edhe me teknikat e metodës CMO, amplituda e mesazhit duhet të jetë e vogël.[?]

6.2.1 Realizimi i modulimit me sinjal kaotik CMO

Për të kryer realizimin e modulimit me sinjal kaotik kryhet simulimi i sistemit Chua me anë të metodës që është prezantuar më parë. Sinjalet kaotik të përfituara nga

simulimi rruhen në një skedar dhe përdoren për të simuluar sistemin CMO. Për të prezantuar grafikisht sinjalet e kodimit CMO krijohet një sinjalt dixhital i cili është dhe mesazhi për transmetim $m(t)$ dhe përfitohet krijohet sinjali i vonuar kaotic $x(t + \tau)$ nga sinjali kaoti $x(t)$ nëpërmjet një vonuesi. Të dy sinjalet bashkohen dhe krijojnë sinjalin $x(t + \tau) + m(t)$ i cili dhe transmetohet në kanal.

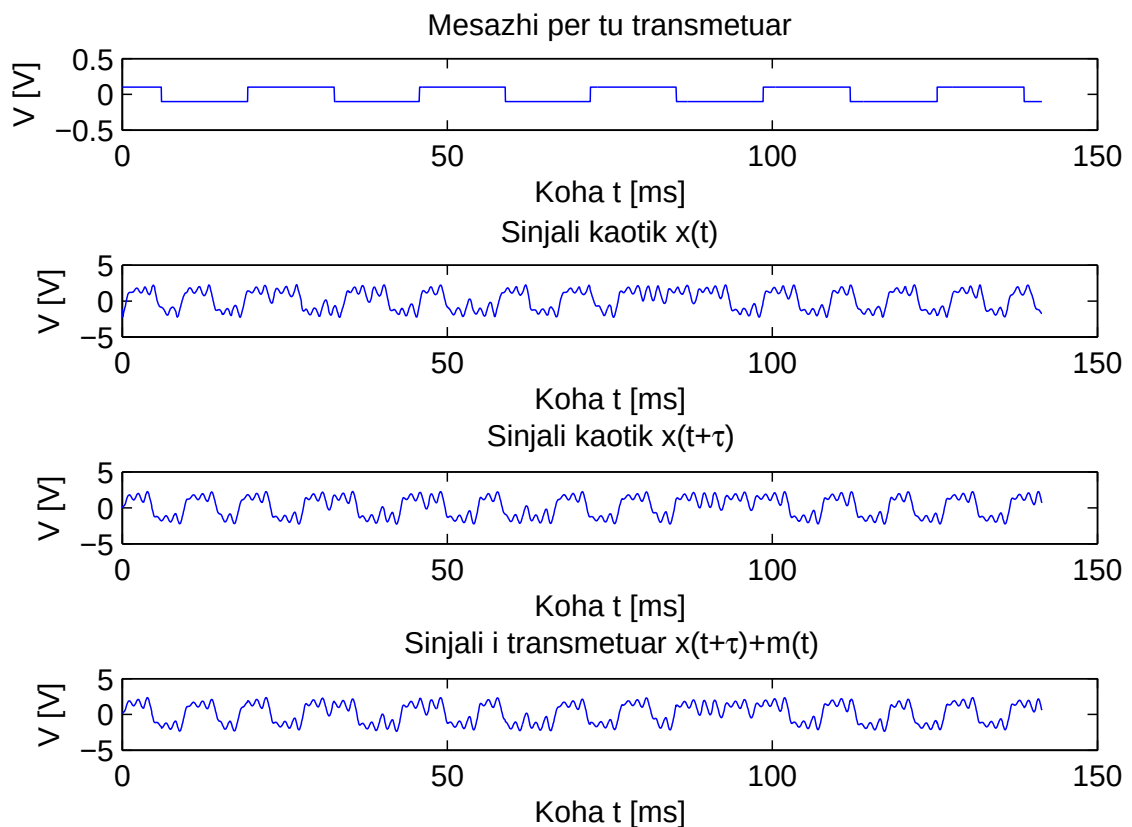


Figura 6.5: Sinjalet për metodën CSK

6.3 Chaos Shift Keying (CSK)

Metoda CSK praqitet grafikisht në figurën 6.6. Sipas kësaj metode, prodhohen dy sinjale kaotike $x_1(t)$ dhe $x_2(t)$ në sistemin e transmetuesit. Në bazë të mesazhit dixhital bëhet zgjedhja me çelësin e sinjalit kaotik që duhet të transmetohet në çdo rast, kështu që transmetohet sinjali $x_1(t)$ për vlerën logjike “0” dhe $x_2(t)$ për vlerën logjike

“1”. Në sistemin e marrësit secila nga këto gjendje detektohet me teknikën e sinkronizimit kaotik. Diferenca midis dy gjendjeve kaotike në sistemin CSK duhet të jetë e vogël, ndryshe një mesazh mund të analizohet dhe të thyhet. Gjatë sinkronizimit kaotik në sistemet jo lineare, koha që duhet për tu sinkronizuar marrësi me transmetuesin është i fundme. Kështu që duhet të parashikohet dhe përgjigja impulsive e sinjaleve në çështjen praktike të sistemeve CSK.

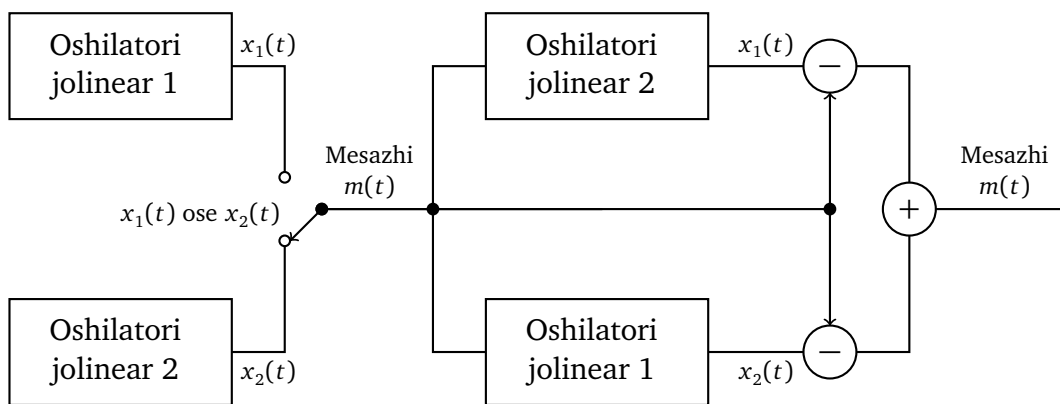


Figura 6.6: Chaos Shift Keying (CSK)

6.3.1 Realizimi i sistemit CSK

Për të krye simulimin e kësaj metode përdoren dy qarqe Chua të pavarura. Në këtë mënyrë përfitohen dy sinjalet e nevojshme $x_1(t)$ dhe $x_2(t)$ të nevojshme për të implementuar sistemin. Përdoret sinjali kaotik që merret nga kondensatori C_1 nga dy qarqe të pavarura. Këto sinjale janë gjeneruar nga simulimi i kryer më përpara për vlera të ndryshme të kushteve fillestare. Ashtu siç është thënë në kapitullin e paraqitjes të sistemeve jolineare, një ndryshim i kushteve fillestare do të ketë si pasojë dy rezultate të ndryshme. Kjo vihet re në figurën 6.7 ku sinjali $x_1(t)$ nuk është i njëjtë me sinjalin $x_2(t)$.

Ashtu siç u tha dhe në paraqitjen e sistemit CSK më përpara kur transmetohet sinjali $x_1(t)$ për vlerën logjike “0” dhe $x_2(t)$ për vlerën logjike “1”. Rezultatet e simulimit

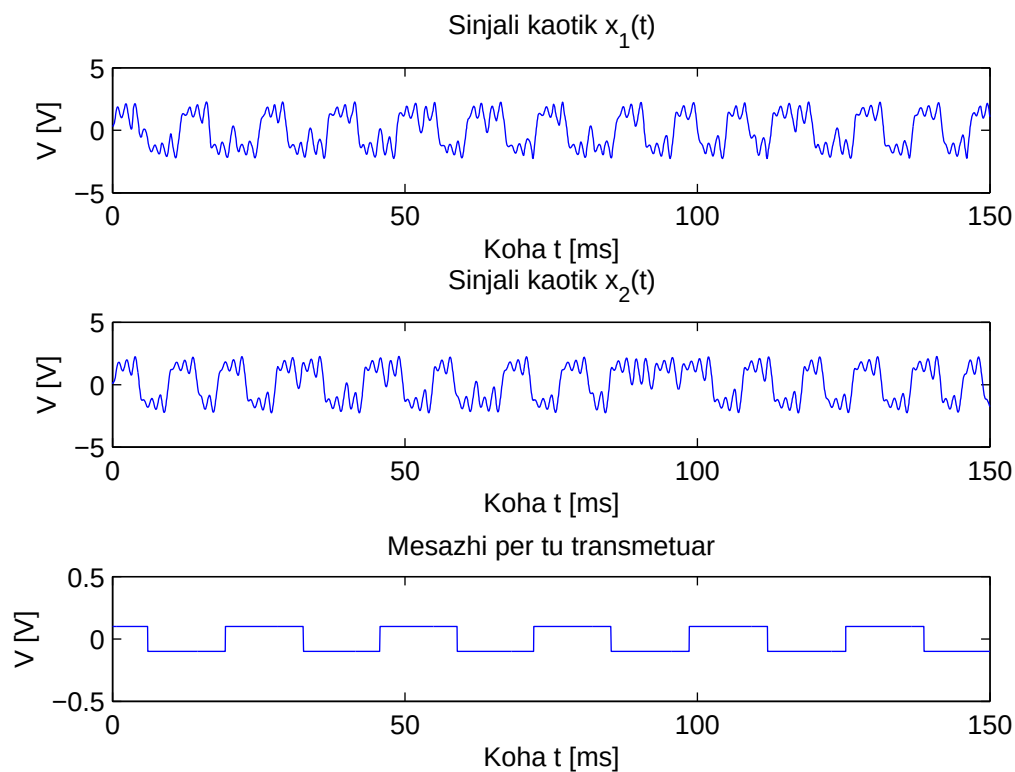


Figura 6.7: Sinjalet për metodën CSK

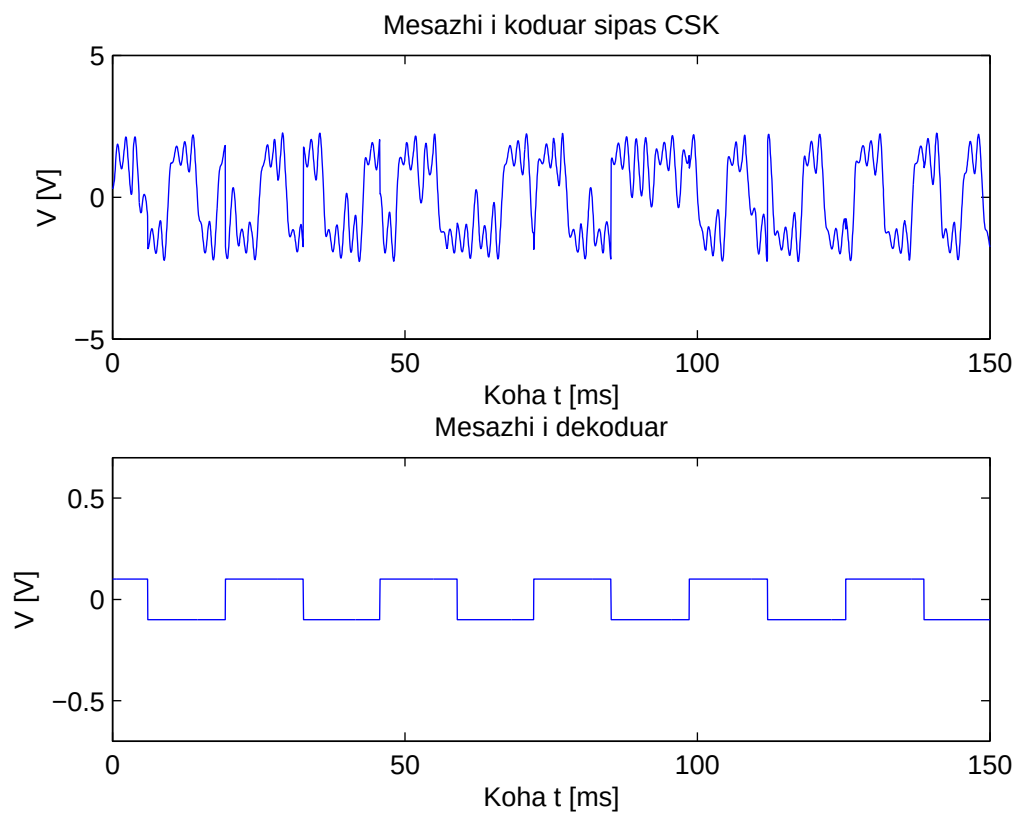


Figura 6.8: Sinjalet për metodën CSK

të këtij sistemi paraqiten tek figura [6.8](#)

6.4 Konkluzionet

Nga analiza e bërë më sipër mund të themi se maskimi me kaos i mesazhit është metoda më e thjeshtë për të implementuar. Lind pyetja cila nga metodat e mësipërme është më e "mira" për ty përdorur. Kjo është një pyetje relativisht e vështirë për ty përgjigjur. Sistemi CMO është sistemi i cili siguron fshehjen më të mirë të mesazhit por nga ana tjetër është shumë i ndjeshëm ndaj gabimeve. Nga ana tjetër sistemi CSK ka më shumë rrezik për transmetimin e sinjalit por dekodimi i tij bëhet më lehtë. Atëherë, duhen bërë disa marrëveshje paraprake për sa i përket disavantazheve të çdo metode kështu që të arrihet përfitimi maksimal i metodave të transmetimit kaotik.

Kapitulli 7

Përfundimet

Më kapitullin e fundit të disertacionit paraqiten konkluzionet e punimit. Me sigurinë që punimi do të ketë vazhdimësi parashtrohet edhe puna në vazhdimësi.

7.1 Konkluzionet

Në këtë studim janë paraqitur qarqe kaotike të cilat operojnë në mënyrë kaotike. U propozuan dy qarqe të cilët u studiuan me anë të analizës jo lineare të serive kohore dhe u llogarit eksponenti Lyapunov për to. U realizua në laborator qarqu i Chuas dhe u vërtetua prezenca e kaosit në atë. U propozuan dy qarqe relativisht të thjeshta për prodhimin e sinjaleve kaotike. Për të marrë kaosin nga këto qarqe është e nevojshme vendosja në hyrje të tyre e një sinjali sinusoidal. Në vazhdimësi u studiua dhe mënyra se si mund të kontrollohet kaosi.

U krye modelimi i qarkut Chua në programin MATLAB. U krye simulimi i qarkut në programin e simulimeve të qarqeve elektronike Multisim dhe u vërtetua se rezultatet e mara nga të dy modelet janë shumë afër me realitetit. Kjo jepën një përparësi në studimin e këtij qarku se anashkalon problemet që mund të shfaqet nga sinjale të padëshirueshme gjatë realizimit laboratorik të tij.

U studiua sinkronizimi në lidhje me raportin sinjal zhurmë dhe në lidhje me dobësimin

e sinjalit. U gjet se për të patur sinkronizim midis dy qarqeve duhet që ato të lidhen në një konfiguracion master-slave. Raporti i sinjalit mbi zhurmë duhet të jetë pozitiv për të patur sinkronizimin. U gjet se sinkronizimi arrihet kur dobësimi i sinjalit që përdoret për sinkronizim duhet të jetë i vogël në mënyrë që të kemi dy qarqe të cilat punojnë në mënyrë të pavarur dhe prodhojnë kaos.

Në bazë të analizës që u krye më sipër implementohen metodat e kriptografisë kaotike në shtresën fizike. Simulohen metodat e maskimit me kaos dhe të modulimit kaotik.

7.2 Puna në vazhdimësi

Duke marrë parasysh të gjitha tematikat dhe problemet që u parashtruan në kapitujt e mëparshëm, në vazhdimësi mund të kryhet një studim më i thellë të parametereve të sistemit. Duhet realizuar sistemi duke përdorur elektronikë RF dhe duhet të merret parasysh modulimi i sistemit.

Një propozim është implementimi i këtij parimi në transmetim me fibra optike. Për këtë duhet të studiohen qarqe fotonik të cilat janë jo linear dhe të shikohet nëse këto mund të prodhojnë kaos. Në vazhdimësi mund të vlerësohet mundësia e transmetimit i këtyre sinjaleve në fibra optike. Një problem tjetër inxhinierik është në qoftë se ky sistem mund të implementohet në sistemet aktuale të transmetimit me fibra optike.

Një nga propozimet është të studiohet kompleksiteti i kaos-it nëpërmjet entropisë dhe të dimensionit të tij. Kjo do të thotë, gjetjen e prehjes së artë midis BER-it (Bit Error Rate), kështu që me cilësinë e komunikimit të duhur të arrihet siguria maksimale gjatë kriptografisë.

Bibliografia

- [1] J. Robert H., *Dynamics of Physical Systems*. Dover Civil and Mechanical Engineering, Dover Publications, 2012.
- [2] P. Saha, D. S. A. Ray, and A. R. Chowdhury, “Multistability in a single system with hidden attractors-theory and experiment,” *International Journal of Physics*, vol. 2, no. 6, pp. 217–225, 2014.
- [3] D. Chelidze and M. Liu, “Reconstructing slow-time dynamics from fast-time measurements,” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 366, no. 1866, pp. 729–745, 2008.
- [4] M. P. Kennedy, “Robust op amp realization of chua’s circuit,” *Frequenz*, vol. 46, no. 3-4, pp. 66–80, 1992.
- [5] D. Neamen, *Semiconductor physics and devices: basic principles*. McGraw-Hill Series in Electrical and Computer Engineering, McGraw-Hill, 2003.
- [6] A. Politi, J. C. F. Matthews, and J. L. O’Brien, “Shor’s Quantum Factoring Algorithm on a Photonic Chip,” *Science*, vol. 325, p. 1221, Sept. 2009.
- [7] K. T. Alligood, T. D. Sauer, J. A. Yorke, and J. D. Crawford, “Chaos: An Introduction to Dynamical Systems,” *Physics Today*, vol. 50, 1997.
- [8] R. C. Hilborn, *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. oxford university press Oxford, 2000.

- [9] H. Khalil, *Non Linear Systems*, Prentice Hall. Prentice Hall, 1996.
- [10] M. Ababneh, M. Salah, and K. Alwidyan, "Linearization of Nonlinear Dynamical Systems: A Comparative Study," *Jordan Journal of Mechanical & Industrial Engineering*, no. 5, pp. 1–5, 2011.
- [11] I. Chatzidimitriou, *Theoretical Mechanics, Volume A*. Yahoudi Yapouli Editions, 1994.
- [12] N. Berglund, "Geometrical theory of dynamical systems," *arXiv preprint math/0111177*, 2001.
- [13] G. Contopoulos, "Order and chaos in general," in *Order and Chaos in Dynamical Astronomy*, pp. 11–376, Springer, 2002.
- [14] M. J. Ogorzalek, *Chaos and complexity in nonlinear electronic circuits*. World Scientific, 1997.
- [15] E. Glasner and B. Weiss, "Sensitive dependence on initial conditions," *Nonlinearity*, vol. 6, no. 6, p. 1067, 1993.
- [16] I. Stewart, *Does God Play Dice? The New Mathematics of Chaos*. Wiley-Blackwell, 2002.
- [17] M. P. Kennedy, "Basic concepts of nonlinear dynamics and chaos," *Circuits and Systems Tutorials*, pp. 289–313, 1996.
- [18] M. J. Feigenbaum, "Quantitative universality for a class of nonlinear transformations," *Journal of statistical physics*, vol. 19, no. 1, pp. 25–52, 1978.
- [19] P. Manneville and Y. Pomeau, "Intermittency and the lorenz model," *Physics Letters A*, vol. 75, no. 1, pp. 1–2, 1979.
- [20] R. M. May *et al.*, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

- [21] A. A. Tsonis, "Chaos from theory to applications plenum press," *New York*, 1992.
- [22] H. Kantz and T. Schreiber, *Nonlinear time series analysis*, vol. 7. Cambridge university press, 2004.
- [23] P. E. McSharry and L. A. Smith, "Better Nonlinear Models from Noisy Data: Attractors with Maximum Likelihood," *Physical Review Letters*, vol. 83, p. 11, Nov. 1999.
- [24] F. Takens, "Detecting strange attractors in turbulence," *Dynamical systems and turbulence, Warwick 1980*, 1981.
- [25] D. Kugiumtzis, B. r. Lillekjendlie, and N. Christophersen, "Chaotic time series. Part I. Estimation of some invariant properties in state-space," *Modeling, Identification and Control: A Norwegian Research Bulletin*, vol. 15, no. 4, pp. 205–224, 1994.
- [26] J. Theiler, "Estimating fractal dimension," *Journal of the Optical Society of America A*, vol. 7, p. 1055, June 1990.
- [27] A. M. Albano, J. Muench, C. Schwartz, A. Mees, and P. Rapp, "Singular-value decomposition and the grassberger-procaccia algorithm," *Physical Review A*, vol. 38, no. 6, p. 3017, 1988.
- [28] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.
- [29] A. Fraser and H. Swinney, "Independent coordinates for strange attractors from mutual information," *Physical review A*, 1986.
- [30] M. Berthold and D. J. Hand, *Intelligent data analysis: an introduction*. Springer Science & Business Media, 2003.

- [31] T. Aittokallio, M. Gyllenberg, J. Hietarinta, T. Kuusela, and T. Multamäki, “Improving the false nearest neighbors method with graphical analysis,” *Physical Review E*, vol. 60, no. 1, p. 416, 1999.
- [32] J. Eckmann and D. Ruelle, “Ergodic theory of chaos and strange attractors,” *World Scientific Series on Nonlinear Science Series A*, vol. 16, pp. 365–404, 1995.
- [33] L. Chua, L. Kocarev, K. Eckert, and M. Itoh, “Experimental chaos synchronization in Chua’s circuit,” *... of Bifurcation and Chaos*, 1992.
- [34] M. Kennedy, “Three steps to chaos. II. A Chua’s circuit primer,” *Circuits and Systems I: Fundamental Theory and ...*, vol. 40, no. 9211603, 1993.
- [35] T. Matsumoto, L. Chua, and S. Tanaka, “Simplest chaotic nonautonomous circuit,” *Physical Review A*, 1984.
- [36] G. Description, “TL082 Wide Bandwidth Dual JFET Input Operational Amplifier Wide Bandwidth Dual JFET Input Operational Amplifier,” *Journal of Vegetation Science*, vol. 8, pp. 463–474, 1995.
- [37] R. C. Jaeger and T. N. Blalock, *Microelectronic circuit design*, vol. 97. McGraw-Hill New York, 1997.
- [38] H. D. Abarbanel, R. Brown, and J. B. Kadtke, “Prediction in chaotic nonlinear systems: Methods for time series with broadband fourier spectra,” *Physical Review A*, vol. 41, no. 4, p. 1782, 1990.
- [39] R. Moddemeijer, “A statistic to estimate the variance of the histogram-based mutual information estimator based on dependent pairs of observations,” *Signal Processing*, vol. 75, no. 1, pp. 51–63, 1999.

- [40] J. Theiler, S. Eubank, A. Longtin, B. Galdrikian, and J. D. Farmer, “Testing for nonlinearity in time series: the method of surrogate data,” *Physica D: Nonlinear Phenomena*, vol. 58, no. 1, pp. 77–94, 1992.
- [41] R. Hegger, H. Kantz, and T. Schreiber, “Practical implementation of nonlinear time series methods: The tisean package,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 9, no. 2, pp. 413–435, 1999.
- [42] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, “A practical method for calculating largest lyapunov exponents from small data sets,” *Physica D: Nonlinear Phenomena*, vol. 65, no. 1, pp. 117–134, 1993.
- [43] P. Grassberger and I. Procaccia, “Measuring the strangeness of strange attractors,” *Physica D: Nonlinear Phenomena*, vol. 9, pp. 189–208, Oct. 1983.
- [44] M. Halias and G. Tombras, “Time series cross prediction in a single transistor chaotic circuit,” *Chaos, Solitons & Fractals*, vol. 41, no. 3, pp. 1167–1173, 2009.

Lista e konferencave dhe revistave të botuara nga doktoranti.

Publikuar në revista shkencore (4)

1. "Evaluating the synchronization of a chaotic encryption scheme using different channel parameters", **Joan Jani**, Malkaj, Partizan, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 10, Issue 1, Ver. II (Jan - Feb. 2015) [link](#)
2. "Simulation of Chua's non linear circuit and his application in chaotic encryption", **Joan Jani**, Malkaj, Partizan, Open Journal of Modelling and Simulation SCIRP, ISSN Print: 2327-4018
3. "Numerical Calculation Of Lyapunov Exponents In Various Nonlinear Chaotic Systems", **Joan Jani**, Malkaj, Partizan, International Journal Of Scientific & Technology Research VOLUME 3, ISSUE 7, JULY 2014 ISSN 2277-8616 [link](#)
4. "Sisteme jo-lineare dhe prezenca e kaosit në ato", **Joan Jani**, Revista Shkencore Logos, Vellimi 2, 2014, Tirane, Albania, ISSN: 2308-2208

Prezantuar në konferenca shkencore (6)

1. "Simulation of performance of a chaotic encryption scheme based on Chua's circuit", **Joan Jani**, P. Malkaj, *EDIS - Publishing Institution of the University of Zilina*, (Vol. 3, p. 293), (ARSA 2014), Slovakia [link](#)
2. "Evaluation Of Performance Of Chaotic Masking Encryption Scheme", **Joan Jani**, Partizan Malkaj, *International Conference on "New Technologies and Applications in Medicine"* (NTAM 2014), November 2014, Tirana, Albania
3. "Applications Of Chaotic Dynamics In Electrocardiogram Signals", **Joan Jani**, Alvin Asimi, Partizan Malkaj, *International Conference on "New Technologies and Applications in Medicine"* (NTAM 2014), November 2014, Tirana, Albania
4. "Simulation and implementation of the Chua's chaotic oscillator", **Joan Jani**, P. Malkaj, *International Conference on Research and Education in Natural Sciences*, (RENS 2013), November 2013, Shkodër, Albania
5. "Nonlinear time series analysis of an externally triggered double transistor chaotic circuit", **Joan L. Jani**, P. Malkaj, *International Conference on "Research and Education - Challenges Toward future"* (ICRAE 2013), May 2013, Shkodër, Albania [link](#)
6. Blind estimation of SNR in medical images, **Joan Jani**, Partizan Malkaj, Niko Hyka, *The 8th General Conference of Balkan Physical Union*, Constanta, Romania, ISBN: 978-606-598-181-2

Shtojcat

A. Kodi për të krijuar bifurkimin ne Logistic Map dhe llogaritjen e eksponentit Lyapunov

Kodi i mëposhtëm u përdor për të krijuar për të krijuar figurën e bigurkimit të paraqitjes logjistike 2.6. Në të njëjtin kod bëhet dhe llogaritja e eksponentit Lyapunov, rezultatet paraqitet tek figura 2.7.

```
clear;clc;close all;

% Parametrat e programit
N=4000;
M=100;
x=ones(N,1)*0.0001;
a=zeros(1,N);
lyap=zeros(1,N);

for j=1:N

    a(j)=j/1000;
    for i=1:M
        % Kodi per te ndertuar bifurkimin e
        x(j,i+1)=a(j)*x(j,i)*(1-x(j,i));

        % Kodi per te llogaritur eksponentin Lyapunov
        lyap(j)=lyap(j)+log(abs(a(j) - 2*a(j)*x(j,i+1)));
    end

    lyap(j)=lyap(j)/M;

end

plot(x)
%% Kodi per te krijuar grafikun e logistik map
figure

plot(a,x(:,end-40:end),'k.','MarkerSize',0.8)
title('Diagrama e bifurkimit')
xlabel('Parametri \alpha')
ylabel('Vlerat qe merr x')
axis([2.5 4 0 1])

% Kodi per rruajtjen e grafikeve
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 IJSTR_map.eps
close;

% Kodi per te krijuar grafikun e eksponentit Lyapunov
figure

plot(a,lyap);
title('Llogaritja e eksponentit lyapunov')
ylabel('Eksponenti lyapunov \lambda')
xlabel('2.5 \leq \alpha \leq 4')
```

```

axis([2.5 4 -1 0.8])
hold on
plot(zeros(1,length(a)), 'r')
grid on
text(2.55,0.7, '\lambda > 0 : Sistemi eshte kaotik');
text(2.55,-0.7, '\lambda < 0 : Sistem jo kaotik');

% Kodi per rruajtjen e grafikeve
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 IJSTR_lyap.eps
close;

```

B. Kodi për të krijuar grafikun e rezistencës jolinear

Kodi i mëposhtëm u përdor për të krijuar figurën 4.13

```
clc;clear;close all;
x=-10:0.1:10;

% Kodi i cili thërrët funksionin e
for i=1:length(x)
    g(i)=hfun(x(i));
end

% Komandat për të krijuar grafikun
plot(x,g)
xlabel('V [V]')
ylabel('I [A]')
title('Rezistenca jolineare')
grid on

% Kodi për të krijuar figurën dhe për ta rruajtur atë në ...
    formatin eps
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 chara_sim.eps
close;
```

Funksioni i rezistencës jo linear

Më poshtë paraqitet kodi i cili simulon rezistencën jolineare të paraqitur në ekuacionin 4.2

```
% Funksioni për rezistencën jolinear
function g = hfun( x )
% x: Tensioni në hyrje

%% Te dhënat e qarkut
    R1 = 220;
    R2 = 220;
    R3 = 2200;
    R4 = 22000;
    R5 = 22000;
    R6 = 3300;

% Burimi DC
    Esat = 9;
    E1 = R3/(R2+R3)*Esat;
    E2 = R6/(R5+R6)*Esat;

    m12 = -1/R6;
    m02 = 1/R4;
    m01 = 1/R1;
    m11 = -1/R3;
```



```

m1 = m12+m11;

if (E1>E2)
    m0 = m11 + m02;
else
    m0 = m12 + m01;
end

mm1 = m01 + m02;
Emax = max([E1 E2]);
Emin = min([E1 E2]);

if abs(x) < Emin
    g = x*m1;
elseif abs(x) < Emax
    g = x*m0;
    if x > 0
        g = g + Emin*(m1-m0);
    else
        g = g + Emin*(m0-m1);
    end
elseif abs(x) ≥ Emax
    g = x*mm1;
    if x > 0
        g = g + Emax*(m0-mm1) + Emin*(m1-m0);
    else
        g = g + Emax*(mm1-m0) + Emin*(m0-m1);
    end
end
end
end

```

C. Kodi per te simuluar qarkun Chua

Më poshtë paraqitet kodi që bën të mundur simulimin e qarkut të Chuas duke zgjidhur ekuacionet diferenciale të tij. Në vazhdimësi jepen dhe komandat për krijimin e figurave 4.10, 4.11, 4.12 dhe 4.17

```
clear;close all;
%% Simulimi i qarkut Chua sipas funksionit ode45

% Eshte perdorur funksioni ode45 per te zhgjidhur ekuacionet ...
%   diferencial
[t,y] = ode45(@Chua,[0 150],[0.1 0 0]);
% Ndryshimi i kushteve fillestrare
[t2,y2] = ode45(@Chua,[0 150],[0.2 0 0]);
[t3,y3] = ode45(@Chua,[0 150],[0.3 0 0]);

%% Figura per krijimin e hapësirës fazore
figure
plot(y(:,1),y(:,2))
xlabel('Voltage over C_1 [V]')
ylabel('Voltage over C_2 [V]')
grid

%% Kondanda per te marre figure ne forme .eps
%set(gcf, 'PaperPositionMode', 'auto');
%print -depsc2 chualsim.eps
%close;

N=900;
figure
plot(t(1:N),y(1:N,1),'k')
hold on
plot(t2(1:N),y2(1:N,1),'r')
plot(t3(1:N),y3(1:N,1),'b')
xlabel('Koha [ms]')
ylabel('Tension [V]')
title('');
legend('v_1=0.1','v_1=0.2','v_1=0.3')
hold off

%% Kondanda per te marre figure ne forme .eps
% set(gcf, 'PaperPositionMode', 'auto');
% print -depsc2 chuasim_chaos.eps
% close;

%% Figura e sinjaleve te marra nga qarku
figure
subplot(3,1,1)
plot(t,y(:,1));
ylabel('Tensioni ne C_1 [V]')
xlabel('Koha [ms]')
subplot(3,1,2)
plot(t,y(:,2));
```

```

ylabel('Tensioni ne C_2 [V]')
xlabel('Koha [ms]')
subplot(3,1,3)
plot(t,y(:,3));
ylabel({'Korrenti qe kalon'; 'nga bobina L [mA]'})
xlabel('Koha [ms]')

%% Kondanda per te marre figure ne forme .eps
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 chua2sim_time.eps
close;

%% FFTL: Transformimi fourier i sinjalit
Fs=1/(t(2)-t(1));
L=length(y);
NFFT = 2^nextpow2(L); % Next power of 2 from length of y
Y = fft(y(:,2),NFFT)/L;
f = Fs/2*linspace(0,1,NFFT/2+1);

% Plot single-sided amplitude spectrum.
figure
plot(f(1:500),2*abs(Y(1:500)))
title('Spektri fuqis te sinjalit nga qakut')
xlabel('Frekuenca (Hz)')
ylabel('Fuqia |V_{C1}(f)|')

%% Kondanda per te marre figure ne forme .eps
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 chuaSpectr.eps
close;

```

D. Kodi për të studiuar sinkronizimin e qarkut Chua

Më poshtë paraqitet kodi që bën të mundur simulimin e qarkut të Chuas duke zgjidhur ekuacionet diferenciale të tij.

```
clear;clc; close all

% Kushtet fillestare per qarkun Primar
x = 0.7;
y = 0;
z = 0;

% Kushtet fillestare per qarkun Sekondar
x2 = 0.7;
y2 = 0;
z2 = 0;

dt=0.0005; %s

%Implementimi i metodes Euler
for i=1:50000

    % Parametrat per qarkun primar
    alpha = 15.6;
    beta = 28;
    m0 = -1.143;
    m1 = -0.714;

    % Per funksioni jo linear i qarkut te primar
    h = m1*x+0.5*(m0-m1)*(abs(x+1)-abs(x-1));

    % Parametrat per qarkun sekondar
    xdot = (alpha*(y-x-h))*dt;
    ydot = (x - y+ z)*dt;
    zdot = (-beta*y)*dt;

    % Per funksioni jo linear i qarkut te primar
    h2 = m1*x+0.5*(m0-m1)*(abs(x2+1)-abs(x2-1));

    %Zbatimi i metodes Euler
    xdot2 = (alpha*(y2-x2-h2))*dt;
    ydot2 = (x2 - y2+ z2)*dt;
    zdot2 = (-beta*y2)*dt;

    x=x+xdot;
    y=y+ydot;
    z=z+zdot;

    % Shtimi i zhurmes ne qark me ane te funksionit randn()

    % 0.05 -> SNR=11
    % 0.1 -> SNR=5
    % 0.5 -> SNR=-8
```

```

% 1 -> SNR=-14
% 2 -> SNR=-19

S=4;
Noise(i)=S*randn(1,1);

% Lidhja e qarkut primar dhe atij sekondar me shtimin e ...
% zhurmes
x2=x2+xdot2;
y2=y + Noise(i);
z2=z2+zdot2;

xx(i)=x;
yy(i)=y;
zz(i)=z;

xx2(i)=x2;
yy2(i)=y2;
zz2(i)=z2;
end

% Llogaritja e fuqis se sinjalit
Ps=sum(yy.^2)/length(xx);
% Llogaritja e fuqis se zhumes
Pn=sum(Noise.^2)/length(Noise);

% Logaritja e
SNR=10*log10(Ps/Pn);

% Krijimi i figurave
str = sprintf('SNR=%f',SNR);
plot(xx,xx2,'.','MarkerSize',0.5)
title(str)
xlabel('Tensioni ne kondensatorin C_1 te qarkut primar [V]');
ylabel('Tensioni ne kondensatorin C_1 te qarkut sekondar [V]');

% Kodi i cili perdoret per te rruajtur figuren ne cilesi te larte

% set(gcf, 'PaperPositionMode', 'auto');
% print -depsc2 SNR11.eps
% close;
%% Kodi per te llogaritur ekuacionin e drejtzes
p = polyfit(xx,xx2,1)
yfit = polyval(p,xx);
yresid = xx2 - yfit;
SSresid = sum(yresid.^2);
SStotal = (length(xx2)-1) * var(xx);
rsq = 1 - SSresid/SStotal
%% Llogaritja e gabimit relativ dhe devijimit standart
error=mean(abs(xx-xx2)/abs(xx));
std(abs(xx-xx2));
yfit = p(1) *xx + p(2);

%% Llogaritja e transformimit Fourier

```

```

% Fs=1/dt;
% Y=fft(xx);
% Y=abs(Y);
% plot(Y);
% title('Spektri fuqis te sinjalit nga qakut')
% xlabel('Frekuenca (Hz)')
% ylabel('Fuqia |V_{C1}(f)|')
% axis([0 250 0 2000])

```

E. Të dhënat nga qarku me një tranzistor

Më poshtë paraqiten të dhënat nga qarku i figurës [4.18](#)

9.624	7.187	9.937	9.624	6.937	9.812	9.062	9.312	7.124
7.562	7.937	9.437	9.312	9.437	9.562	6.624	9.374	8.437
9.499	7.999	6.562	6.624	7.624	6.374	8.874	8.749	8.874
8.437	7.937	6.437	8.312	6.124	6.499	6.062	6.312	6.499
8.499	6.937	6.812	7.562	7.937	5.749	7.874	7.937	6.124
5.687	5.499	7.749	6.562	5.312	7.624	5.312	6.749	5.624
6.187	5.124	7.187	7.124	5.312	4.874	5.749	4.937	6.124
6.687	6.624	4.562	4.937	5.874	6.374	6.124	4.687	5.624
4.374	5.437	5.124	4.499	5.124	4.749	4.812	4.624	4.499
4.499	4.562	4.749	4.624	4.499	4.562	4.499	4.749	4.499
4.749	4.437	4.562	4.499	4.624	4.499	4.624	4.687	4.687
4.562	4.499	4.374	4.624	4.624	4.312	4.374	4.312	4.374
4.624	4.562	4.562	4.374	4.312	4.562	4.374	4.312	4.312
4.499	4.312	4.312	4.249	4.562	4.312	4.562	4.437	4.249
4.562	4.562	4.187	4.187	4.187	4.499	4.249	4.499	4.249
4.249	4.312	4.437	4.374	4.312	4.374	4.062	4.124	4.249
4.062	4.437	4.062	4.062	4.249	3.937	4.062	4.312	3.937
3.999	4.437	4.374	4.437	3.937	3.937	3.999	4.249	4.249
4.249	3.874	4.062	4.124	3.937	4.124	4.312	4.249	3.937
3.874	3.937	3.937	3.937	3.812	3.812	3.812	4.124	4.249
4.187	3.812	4.249	3.937	3.812	3.874	4.187	4.249	3.749
4.187	3.749	4.124	3.999	4.124	4.062	4.249	4.062	3.749
3.874	3.687	3.624	3.687	3.687	3.874	3.749	3.812	3.874
3.937	4.124	4.062	3.874	3.999	3.749	4.062	3.937	3.687
3.999	3.562	3.624	3.874	3.999	3.687	3.937	3.624	3.937
3.812	3.562	3.874	3.562	3.562	3.687	3.937	3.999	3.937
3.562	3.437	3.499	3.562	3.499	3.624	3.874	3.499	3.687
3.562	3.562	3.812	3.562	3.499	3.812	3.749	3.749	3.437
3.749	3.499	3.624	3.499	3.437	3.562	3.437	3.437	3.812
3.437	3.437	3.437	3.812	3.437	3.562	3.437	3.812	3.562
3.687	3.749	3.624	3.562	3.499	3.312	3.624	3.687	3.437
3.312	3.499	3.437	3.624	3.812	3.374	3.812	3.499	3.499
3.374	3.437	3.437	3.437	3.499	3.812	3.499	3.374	3.437
3.374	3.812	3.374	3.562	3.687	3.374	3.749	3.437	3.437
3.499	3.437	3.499	3.624	3.812	3.312	3.374	3.374	3.562
3.437	3.437	3.437	3.437	3.687	3.562	3.437	3.562	3.624
3.437	3.374	3.499	3.812	3.749	3.437	3.624	3.624	3.562
3.437	3.499	3.437	3.812	3.749	3.437	3.499	3.687	3.374
3.499	3.812	3.687	3.437	3.437	3.437	3.437	3.437	3.687
3.437	3.874	3.812	3.562	3.499	3.499	3.437	3.437	3.874

Tabela 1: Të dhënat e serisë kohore nga qarku me një tranzistor

G. Të dhënat nga qarku me dy tranzistor

Më poshtë paraqiten të dhënat nga qarku i figurës [4.37](#)

11.793	11.796	11.803	11.814	11.823	11.838	11.855	11.879
11.903	11.926	11.955	11.982	12.020	12.054	12.102	12.153
12.206	12.264	12.319	12.380	12.437	12.505	12.569	12.660
12.770	12.963	13.323	13.733	14.136	14.556	14.961	15.375
15.766	16.160	16.524	16.886	17.213	17.533	17.812	18.081
18.306	18.516	18.656	18.704	18.768	18.833	18.888	18.926
18.942	18.931	18.891	18.822	18.723	18.593	17.111	18.794
18.667	18.558	14.896	18.730	18.701	18.668	18.644	18.568
14.851	15.881	18.644	18.637	18.632	18.620	18.593	18.501
11.796	16.376	18.678	18.609	18.680	18.596	18.645	18.559
18.595	18.499	18.502	11.357	14.160	18.722	18.730	18.738
18.730	18.726	18.703	18.683	18.640	18.594	13.278	14.591
18.683	18.698	18.681	18.682	18.651	18.623	18.563	11.304
15.662	18.843	18.737	18.822	18.702	18.766	18.627	18.657
15.321	11.251	18.501	18.667	18.484	18.628	18.437	18.550
18.294	11.162	18.725	18.884	18.650	18.806	18.538	18.574
12.341	16.527	18.585	18.720	18.514	18.636	17.435	11.071
18.760	19.015	18.737	18.967	18.676	18.852	18.271	10.963
18.929	19.211	18.863	19.133	18.755	18.902	12.742	16.874
18.750	18.978	18.629	10.906	18.933	19.296	18.907	19.236
18.853	19.153	18.646	10.797	18.837	19.226	18.768	19.138
18.649	18.900	15.762	10.737	19.691	20.028	19.504	19.866
19.269	19.505	11.926	20.960	20.461	20.768	20.299	20.503
19.934	10.807	21.220	21.517	21.010	21.316	20.714	20.962
11.863	21.937	21.527	21.794	21.405	21.588	21.119	10.895
22.042	22.322	21.870	22.151	21.619	21.806	16.328	10.813
22.714	23.005	22.487	22.798	22.229	22.466	21.753	10.739
24.221	24.460	23.827	24.097	23.447	23.685	22.870	23.005
11.889	23.802	23.316	23.562	23.098	23.262	22.756	22.768
21.852	14.338	23.346	23.441	22.906	23.043	22.486	22.597
21.857	21.799	11.650	25.617	25.296	25.395	25.066	25.067
24.663	24.532	24.003	23.687	22.785	22.075	11.371	32.511
31.633	31.231	30.523	29.872	28.691	27.854	19.683	33.006
33.650	33.496	32.986	32.652	31.682	30.877	29.705	28.897
27.872	27.064	25.430	24.381	22.948	21.545	38.569	34.025
31.807	29.720	27.884	26.434	24.855	22.712	11.581	34.069
32.009	30.834	29.474	28.048	26.482	15.583	36.275	35.066
33.888	32.968	31.450	29.687	27.721	25.934	23.905	11.231
25.278	33.256	31.687	30.586	29.406	28.169	13.154	34.517
33.898	33.526	32.970	32.334	31.132	30.075	28.347	34.945

Tabela 2: Të dhënat e serisë kohore nga qarku me dy tranzistor

H. Komandat për përpunimi e të dhënave nga qarku me dy tranzistor

```
clear;clc;close all;
% uiopen('C:\Users\igiann\Documents\MATLAB\CHAOS.DAT',1)
% Hapja e te dhenave te rruatjtuara ne skedarin
fid = fopen('Paper_ICAER_2013.scp','r');
tline = fgetl(fid);

while ~feof(fid)
    tline = fgetl(fid);
    if (tline=='-')
        break
    end
end

% Komandat per leximin e skedarit dhe krijimit te matrices DATA
while ~feof(fid)
    tline = fgetl(fid);
    temp = textscan(fid, '%f %f %f');
    DATA(:,1)=temp{1};
    DATA(:,2)=temp{2};
    DATA(:,3)=temp{3};
end
fclose(fid);

% Komandat per te rruajtur te dhenat e serise kohore
textable=vec2mat(DATA(:,3),8);
[n,m]=size(textable);
fileID = fopen('exp.txt','w');

for i=1:40
    for j=1:m-1
        fprintf(fileID,'%0.3f &', textable(i,j));
    end
    fprintf(fileID,'%0.3f \\\ \n',textable(i,m) );
end
fclose(fileID);

%figure
% plot(DATA(:,3));
% xlabel('Samples');
% ylabel('V_b[Volts]');
%% Llogaritja e informacionit te perbashket
%plot(DATA(:,1),DATA(:,2));
cd .././Analysis

[mutM] = mutualinformation(DATA(2:10000,3), 60, 15, '', 'c');
%Kodi per krijimin e te dhenave
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 D:/Dropbox/PhD/Thesis/Figures/ICRAE_mutual.eps
close;
```

```

%% false nearest
falsenearest(DATA(:,3),5,10,'Mutual information')
%% Autocorrelation
autocorrelation(DATA(1:10000,3), 5, '', 'd')
%% Corelation dimension
correlationdimension(DATA(2:10000,3),5,15,'',3,1,10)
%% Phase space reconstruct
v = DATA(1:1000,2);
dv = derive(v, 0.001);
%XM = embeddelays(DATA(1:1000,3), 3, 5);
plot(v(1:size(dv)),dv);

```

I. Simulimi i metodës Chaotic Masking CM

```
%% Simulimi i kaotik masking
clear;clc;close all;
% Importimi i serise kaotike
load data
[n,m]=size(data);
% Krijimi i mesazhit
for i=1:n
    if(mod(round(i/300),2)==0)
        x(i)=0.1;
    else
        x(i)=-0.1;
    end
end
% Komanda per kaotik masking
Y=data(:,2)+x';

% Afishimi i sinjaleve
subplot(3,1,1)
plot(data(:,1),data(:,2))
axis([ 0 150 -7 7])
title('Sinjali kaotik')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(3,1,2)
plot(data(:,1),x)
axis([ 0 150 -0.5 .5])
title('Mesazhi per tu transmetuar')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(3,1,3)
plot(data(:,1),Y)
xlabel('Koha t [ms]')
title('Sinjali i koduar')
axis([0 150 -7 7])
ylabel('V [V]');

% Komandat per rruajtjen e figures
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 D:\Dropbox\PhD\Thesis\Figures\masking.eps
% close;

%% Komandat per dekodimin e komunikacionit
% 0.1 -
% 0.2 -
% Zhurma
Noise= 0.01*randn(size(data(:,2)));
x_rek=Y-data(:,2)+Noise;
SNR=10*log10(sum(Y.^2)/sum(Noise.^2))
```

```

subplot(2,1,1)
plot(data(:,1),x)
axis([0 150 -0.5 0.5])
xlabel('Koha t [ms]')
ylabel('V [V]');
title('Mesazhi i transmetuar')
subplot(2,1,2)
plot(data(:,1),x_rek)
xlabel('Koha t [ms]')
axis([0 150 -0.9 0.9])
ylabel('V [V]');
title('Mesazhi i dekoduar')

set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 D:\Dropbox\PhD\Thesis\Figures\masking2.eps
% close;

```

J. Simulimi i metodës CMO

```
% Simulimi i kaotik masking
clear;clc;close all;
% Importimi i serise kaotike
load dataCMO
[n,m]=size(dataCMO);

for i=1:n
    if(mod(round(i/300),2)==0)
        x(i)=0.1;
    else
        x(i)=-0.1;
    end
end
figure

subplot(4,1,1)
plot(dataCMO(1:end-200,1),x(1:end-200))
axis([0 150 -0.5 0.5])
title('Mesazhi per tu transmetuar')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(4,1,2)
plot(dataCMO(1:end-200,1),dataCMO(201:end,2))
title('Sinjali kaotik x(t)')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(4,1,3)
plot(dataCMO(1:end-200,1),dataCMO(1:end-200,2))
title('Sinjali kaotik x(t+\tau)')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(4,1,4)
plot(dataCMO(1:end-200,1),dataCMO(1:end-200,2)+x(1:end-200))
title('Sinjali i transmetuar x(t+\tau)+m(t)')
xlabel('Koha t [ms]')
ylabel('V [V]');

set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 D:\Dropbox\PhD\Thesis\Figures\CMO.eps
% close;
```

K. Simulimi i metodës CSK

```
%% Simulimi i CSK
clear;clc;close all;
% Importimi i serise kaotike
load dataCSK
[n,m]=size(dataCSK);

% Krijimi i mesazhit
for i=1:n
    if(mod(round(i/300),2)==0)
        x(i)=0.1;
        % Kodi per modulimin e sinjalit
        moduleCSK(i)=dataCSK(i,5);
    else
        x(i)=-0.1;
        % Kodi per modulimin e sinjalit
        moduleCSK(i)=dataCSK(i,2);
    end
end

% Afishimi i sinjaleve
subplot(3,1,1)
plot(dataCSK(:,1),dataCSK(:,5))
axis([ 0 150 -5 5])
title('Sinjali kaotik x_1(t)')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(3,1,2)
plot(dataCSK(:,1),dataCSK(:,2))
axis([ 0 150 -5 5])
title('Sinjali kaotik x_2(t)')
xlabel('Koha t [ms]')
ylabel('V [V]');
subplot(3,1,3)
plot(dataCSK(:,1),x)
axis([ 0 150 -0.5 .5])
title('Mesazhi per tu transmetuar')
xlabel('Koha t [ms]')
ylabel('V [V]');

%% Kondanda per te marre figure ne forme .eps
set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 CSKsingals.eps
close;

figure
subplot(2,1,1)
plot(dataCSK(:,1),moduleCSK)
title('Mesazhi i koduar sipas CSK')
xlabel('Koha t [ms]')
axis([ 0 150 -5 5])
```

```

ylabel('V [V]');
subplot(2,1,2)
plot(dataCSK(:,1),x)
title('Mesazhi i dekoduar')
xlabel('Koha t [ms]')
ylabel('V [V]');
axis([ 0 150 -0.7 .7])

set(gcf, 'PaperPositionMode', 'auto');
print -depsc2 CSKmodule.eps
close;

```

L. Laboratori ku u kryhen matjet

Më poshtë paraqitet laboratori ku u krye pjesa eksperimentale.



Figura 7.1: Laboratori i elektronikës në Departamentin e Fizikës të Universitetit të Athinës në Greqi