UDK621.3:(53+54+621+66), ISSN0352-9045 Informacije MIDEM 37(2007)1, Ljubljana

KAOTIČNI KRIPTOGRAFSKI SISTEM Z UPORABO VEZIJ FPGA

Bojan Jarc, Matej Šalamon

Univerza v Mariboru, Fakulteta za elektrotehniko računalništvo in informatiko, Maribor, Slovenija

Kjučne besede: kriptografski sistemi, kaos, digitalni filtri, vezja FPGA.

Izvleček: *V naslednjem prispevku predstavljamo kaotični kriptografski sistem in možnost njegove strojne izvedbe. Jedro kriptografskega sistema predstavljata multipomična šifrirna oz. dešifrirna funkcija (enačbe 2, 3, 4) in generator psevdo-kaotične sekvence (slika 3), realiziran z digitalnim sitom drugega reda. Razmeroma enostavna struktura in izvajanje preprostih matematičnih operacij (seštevanje, odštevanje, množenje s skalarjem) dopuščajo strojno realizacijo sistema, ki omogoča hitro delovanje. Kriptografski sistem sestavlja šifrirno in dešifrirno vezje (slika 5). Pri njegovi realizaciji smo uporabili 16 bitno aritmetiko s stalno vejico in vezje FPGA XC3S500E družine Spartan-3E. Enota odprtega sporočila je bila 16 bitna. Pri načrtovanju smo uporabili kombinirani grafični opis in opis z visokonivojskim jezikom VHDL (slika 6). Maksimalna frekvenca ure, pri kateri je bila inverznost med operacijo šifriranja in dešifriranja še zagotovljena, je znašala 25 MHz (sliki 8 a, b). Pri 7-kratni (N=7) ponovitvi šifrirne funkcije je bila maksimalna frekvenca šifriranja 3,125 MHz. Ocenili smo tudi hitrost delovanja sistema pri uporabi drugih vezij FPGA (tabela 1). Ugotovili smo, da bi lahko z vezji družine Virtex 4 dosegli hitrost šifriranja 77,71 MHz pri N=1.*

Chaotic Cryptographic System Using FPGA Circuits

Key words: cryptographic systems, chaos, digital filters, FPGA circuits.

Abstract: *In this paper we present a chaotic cryptographic system and its hardware realization. The core of chaotic cryptographic system is a multi-shift cipher (eq. 2, 3) or decipher (eq. 4) and pseudo-chaotic sequence generator (fig. 3), realized with second order digital filter. Relatively simple structure and executions of simple mathematical functions (addition, subtraction, scalar multiplication) allows us to use a hardware realization, suitable for high frequencies. A chaotic cryptographic system is composed of cipher and decipher circuit (fig. 5). For its realization we have used 16 bit fixed point arithmetic and FPGA XC3S500E circuit of Spartan 3E family. Plaintext digits was 16 bit long. At designing stage we have used combined schematic and language VHDL description approach (fig. 6). Maximum clock frequency at which cipher and decipher were inversive was 25 MHz (fig. 8 a, b). Choosing the multi-shift function repetition number N = 7, allows us to encrypt the plaintext with frequency 3,125 MHz. Performance was estimated for other FPGA circuits (table 1). For Virtex 4 FPGAs we've achieved maximal clock frequency 77,71 MHz at N = 1..*

1. Uvod

Nekoč zgolj zanimiv fenomen deterističnega kaosa, je postal v zadnjem desetletju tudi praktično uporaben. Na področju digitalnih komunikacijskih sistemov je apliciran v različnih kompresijskih, šifrirnih in modulacijskih gradnikih, potrebnih pri prenosu informacij. Znani so npr. različni načini pretvorbe informacijskega signala v kaotičnega na oddajni strani in izločitev informacijskega signala iz kaotičnega na sprejemni strani. Med najpomembnejše sodijo: kaotično maskiranje, kaotično preklapljanje in kaotična modulacija.

Med leti 1990 in 1995 je bil cilj številnih raziskav, razviti sistem, ki bo omogočal modulacijo in šifriranje s pomočjo enega samega kaotičnega sistema. Ob tem sta se formirali dve različni raziskovalni področji: področje kaotične modulacije in kaotična kriptografija /1/.

Kriptografija je matematična disciplina, ki s ukvarja z varnostjo informacij, šifriranjem, avtentičnostjo in avtorizacijo. Z njo so običajno povezani: simetrični blokovni šifrirni sistemi, generatorji naključnih števil, tokovni šifrirni sistemi in asimetrični šifrirni sistemi oziroma šifrirni sistemi z javnim ključem /4/.

Apliciranje kaosa v kriptografiji oziroma pojav ti. kaotičnih kriptografskih sistemov se je pojavilo z odkritjem možnosti sinhronizacije kaotičnih oscilacij identičnih kaotičnih sistemov /3/. Sinhronizacija dveh identičnih kaotičnih sistemov je uspešna, če je mogoče, kljub njuni hiperobčutljivosti na začetne pogoje, zagotoviti njuno identično kaotično oscilira-nje. Sinhroniziranost kaotičnih sistemov na šifrirni in dešifrirni strani je namreč potreben pogoj za reverzibilnost oddajne in sprejemne strani kaotičnega kriptografskega sistema.

Kaotični sistemi se v kriptografiji uporabljajo kot generatorji naključnih števil za generiranje kriptografskih ključev in za naključno inicializacijo posameznih spremenljivk v kriptografskih algoritmih. Z odkritjem obstoja kaosa v digitalnih sistemih se v kriptografiji pojavlja vse več psevdo-kaotičnih sistemov. Ti sistemi imajo končno število različnih stanj, zato lahko generirajo le navidezno naključne oziroma psevdo-kaotične sekvence števil, ki so sicer periodične, periode ponavljanja pa so običajno zelo velike.

V prispevku predstavljamo kaotični kriptografski sistem, v katerem smo za generiranje naključnih sekvenc uporabili kaotično digitalno sito II. reda, za šifrirno in dešifrirno funkcijo pa posebno multipomično funkcijo. Opis digitalnega sita kot generatorja psevdo-naključnih sekvenc je opisan v drugem poglavju. Tretje poglavje je namenjeno opisu predlaganega šifrirnega in dešifrirnega algoritma, ki omogoča ti. tokovno šifriranje in dešifriranje. Implementacija celotnega

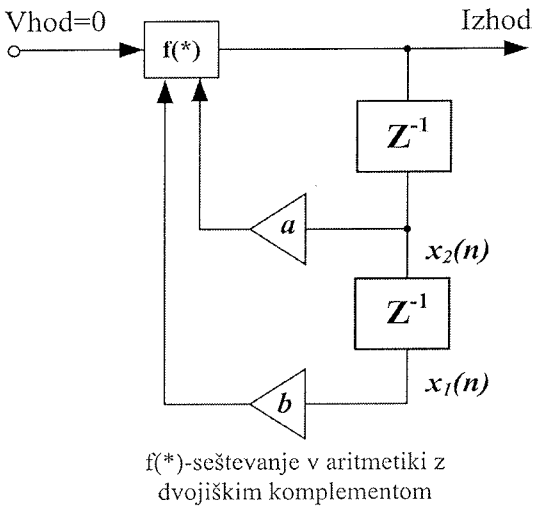
kriptografskega sistema v vezju FPGA je opisana v četrtem poglavju, peto poglavje pa opisuje rezultate meritev.

2. Generator psevdo-kaotične sekvence

Generator naključnih sekvenc je zraven šifrirne in dešifrirne funkcije najpomembnejši del vsakega kriptografskega sistema. Resnično naključne sekvence je mogoče dobiti le s pomočjo naključnih fizikalnih procesov kot je npr. metanje kovanca, termični šum na uporu ali Zener diodi itd. Med nje se pogosto uvrščajo tudi kaotični procesi, z značilno deterministično naključnostjo. Ker naključni procesi niso ponovljivi, z njimi ni mogoče zagotoviti potrebne reverzibilnosti šifrirnega in dešifrirnega algoritma, saj sta za njo potrebna dva popolnoma enaka vira naključnih sekvenc.

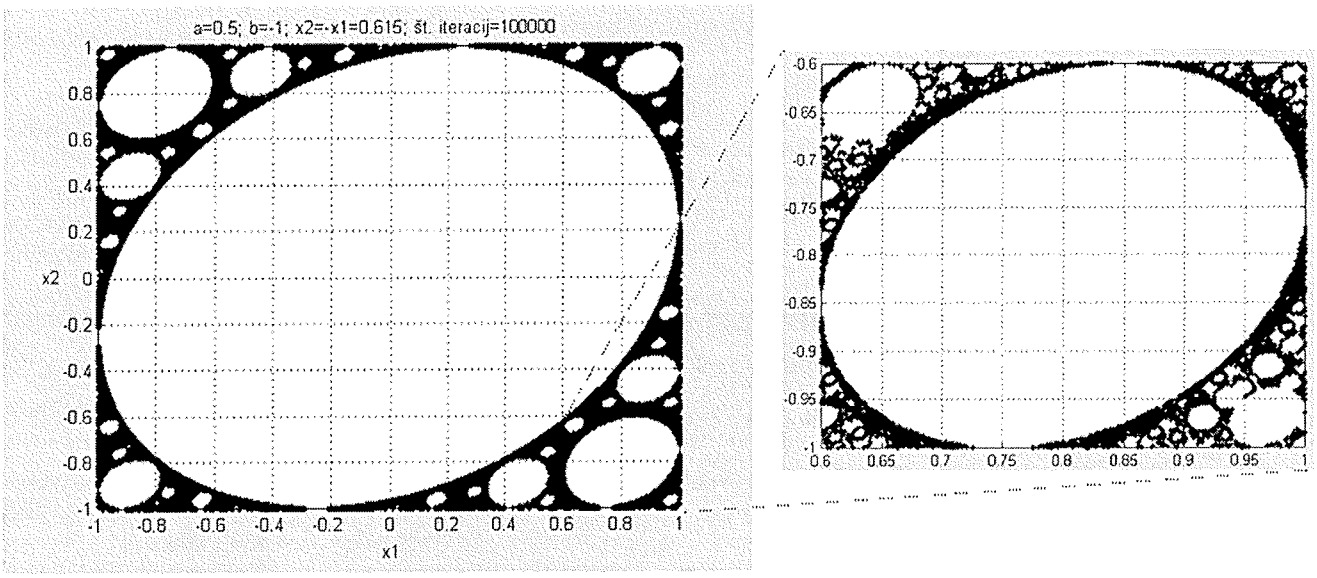
Večina današnjih kriptografskih sistemov uporablja generatorje psevdo-naključnih sekvenc. Ti lahko zaradi končnega števila različnih stanj, generirajo le navidez naključna oziroma psevdo-naključna zaporedja števil. Takšna zaporedja so sicer periodična, njihova perioda pa zelo velika[1] in običajno vnaprej izračunljiva. Psevdo-naključne sekvence z majhno periodo za šifrirne namene niso primerne, saj omogočajo hitro razkritje tajnega ključa. Zelo znan je preprost način generiranja psevdo-naključnih sekvenc s pomičnimi registri in povratno zanko LFSR[2] /4/.

Med psevdo-naključne sekvence se velikokrat uvrščajo tudi psevdo-kaotične sekvence /5/, čeprav je med njimi kar nekaj razlik /6/. V generatorju psevdokaotičnega signala poteka hiperobčutljiv iterativni proces, na osnovi katerega se generira psevdokaotična sekvenca števil, ki je paradoksalno urejeno neurejena. Kaotično naključni proces je namreč v primerjavi s povsem naključnim procesom bolj urejen oziroma manj naključen. Urejeno neurejenost potrjujejo urejene fraktalne podobe, ki pri resnično naključnih procesih ne obstajajo.



Slika 1: Nelinearni model digitalnega sita drugega reda.
Fig. 1: Second order digital filter nonlinear model.

Eden izmed sistemov, ki se lahko obnaša kaotično, je tudi digitalno sito II. reda. Čeprav je njegovo obnašanje natančno obravnavano v prispevkih /7/, na tem mestu omenimo le nekatere pomembnejše ugotovitve, ki bodo omogočile lažje razumevanje, v nadaljevanju predstavljenega, kaotičnega kriptografskega sistema. Slika 1 prikazuje nelinearni model digitalnega sita II. reda, ki se lahko ob določenih pogojih obnaša kaotično.



Slika 2: Kaotična trajektorija.
Fig. 2: Chaotic trajectory.

1 *Periode psevdo-naključnih sekvenc, uporabljenih v kriptografskih sistemih znašajo 2^{256} in več.*

2 *LFSR- Linear Feedback Shift Registers.*

Za to morajo biti izpolnjeni naslednji pogoji /7/:

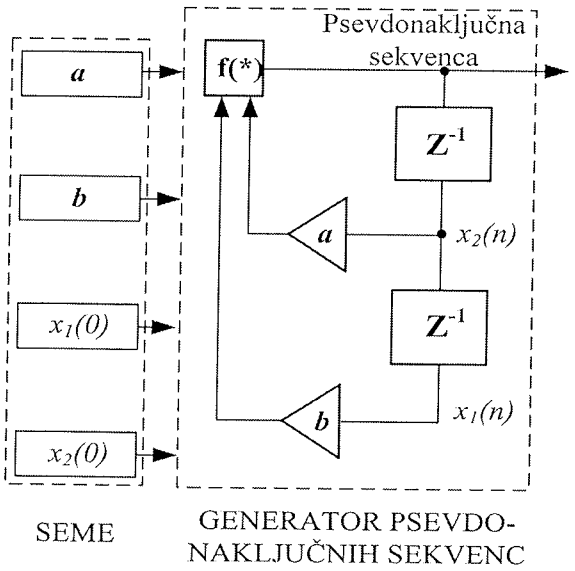
- na vhodu mora biti ničelni signal;
- koeficienta *a* in *b* morata biti izbrana tako, da sistem deluje na robu stabilnosti;
- za začetni stanji $x_1(0)$ in $x_2(0)$ morata veljati:

$$x_1(0) = -x_2(0) = x_0 > \frac{1}{2}\cdot(2-a)^{1/2} = 0{,}612372435695... \quad (1)$$

Kaotično obnašanje sita predstavlja trajektorija, ki v ravnini x_1-x_2 opisuje fraktalno geometrijo elips. Takšna trajektorija je prikazana na sliki 2. Dobili smo jo na osnovi simulacije 16-bitne strukture pri naslednjih parametrih sita: a=0,5; b=-1; $x_2(0)$= -$x_1(0)$=0,615.

V primeru 16-bitne strukture je število vseh različnih stanj oziroma vrednosti spremenljivk x_1 in x_2 2^{16} = 65536. Te vrednosti se pojavljajo psevdo-naključno. Velikost period je spremenljiva in odvisna od začetnega stanja spremenljivk stanj x_1 in x_2 ter števila bitov, s katerimi spremenljivki predstavimo.

Predstavljeno digitalno sito lahko v kaotičnem režimu delovanja uporabimo kot generator psevdo-naključne sekvence (slika 3), ki je generirana na osnovi začetnih stanj spremenljivk x_1 in x_2 ter koeficientov *a* in *b*. Te vrednosti predstavljajo seme oziroma začetno stanje za algoritem, ki opisuje delovanje sita.



Slika 3: Generator psevdo-kaotičnih sekvenc.
Fig. 3: Pseudo-chaotic stream generator.

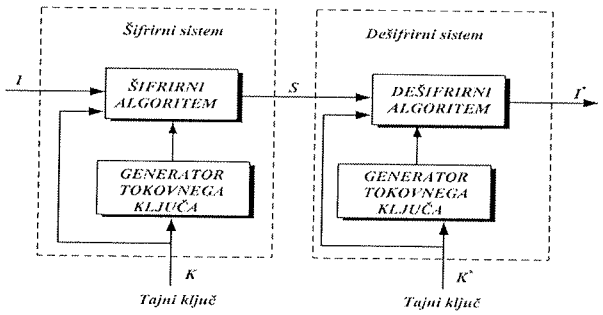
3. Kaotični kriptografski sistem

Klasičnim kriptografskim sistemom se v zadnjih nekaj letih pridružujejo novi kaotični kriptografski sistemi, ki temeljijo na fenomenu determinističnega kaosa oziroma na zelo preprostih, vendar hiperobčutljivih iterativnih postopkih. Ker je področje determinističnega kaosa še precej neraziskano, je razumljivo, da je tudi t.i. kaotična kriptografija relativno nov subjekt raziskav, vezana na metode in standarde, ki so šele v razvojni fazi. Danes zasledimo tako tokovne kot blokovne kaotične kriptografske sisteme.

V tokovnih simetričnih šifrirnih sistemih so generatorji psevdonaključne sekvence uporabljeni kot generatorji tokovnega ključa, kar pomeni, da se šifriranje odprtega sporočila izvaja bit za bitom, in sicer tako, da se tokovni ključ kombinira z biti odprtega sporočila. Ti sistemi so zelo hitri in izvajajo šifriranje manjših enot odprtega sporočila, kot je npr. bit ali znak (8-bitov) v datoteki, točka v digitalni sliki itd.

Druga vrsta šifrirnih sistemov so blokovni. Pri teh se odprto sporočilo razdeli na tako dolge bloke, kot jih zahteva algoritem[3], nato pa se biti posameznega bloka, v skladu s šifrirnim algoritmom, premeščajo in kombinirajo s tajnim ključem, generiranim z generatorjem naključnih sekvenc.

V nadaljevanju obravnavamo tokovni kaotični kriptografski sistem, ki temelji na multipomični šifrirni/dešifrirni funkciji. Tokovni ključ je generiran s pomočjo prej predstavljenega kaotičnega digitalnega sita. Blokovna shema celotnega kriptografskega sistema je prikazana na sliki 4.



Slika 4: Blokovna shema kriptografskega sistema.
Fig. 4: Cryptographic system block scheme.

Šifriranje odprtega sporočila *I* se izvaja postopoma po korakih (slika 5). *N*-ti vzorec odprtega sporočila *i*(*n*) in psevdonaključne vrednosti *k*(*n*), se s pomočjo tajnega ključa *K* in posebne nelinearne, rekurzivne, multipomične funkcije, pretvori v šifriran vzorec tajnopisa *s*(*n*). Multipomično šifrirno funkcijo /8/ opisuje enačba:

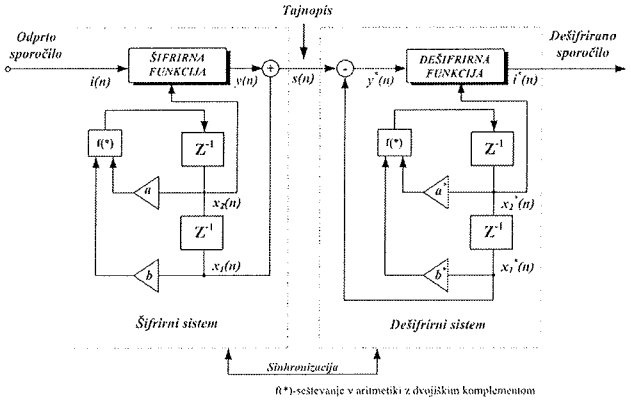
$$s(n) = \underbrace{f_1(...f_1(f_1}_{N}(i(n), \underbrace{k(n)), k(n)),...k(n))}_{N} + k(n+1) \quad (2)$$

pri čemer je *N* poljubno število iteracij nelinearne funkcije f_1:

$$f_1(x,k) = \begin{cases} (x+k)+2\cdot h & -2\cdot h \le (x+k) \le -h \\ (x+k) & -h \le (x+k) \le h \\ (x+k)-2\cdot h & h \le (x+k) \le 2\cdot h \end{cases} \quad (3)$$

Tajni ključ sestavlja več vrednosti: koeficienta sita *a* in *b*, začetni stanji $x_1(0)$ in $x_2(0)$, število iteracij multipomične šifrirne funkcije *N* in parameter *h*.

3 *Več sto kilo bajtov.*



Slika 5: Podrobnejša shema kriptografskega sistema.
Fig. 5: Detail scheme of cryptographic system.

Šifrirna funkcija $y(i(n))$ bo bijektivna, če bo vrednost spremenljivke h izbrana tako, da bosta x in k vedno znotraj intervala $(-h, h)$. Samo v tem primeru bo obstajal tudi inverzni - dešifrirni algoritem, ki ga lahko v skladu z oznakami na sliki 5 opišemo z naslednjo dešifrirno funkcijo:

$$i^*(n) = \underbrace{f_1(...f_1(f_1(y^*(n), \underbrace{-x_2^*(n)), -x_2^*(n)), ..., -x_2^*(n)}_{N})}_{N} \quad (4)$$

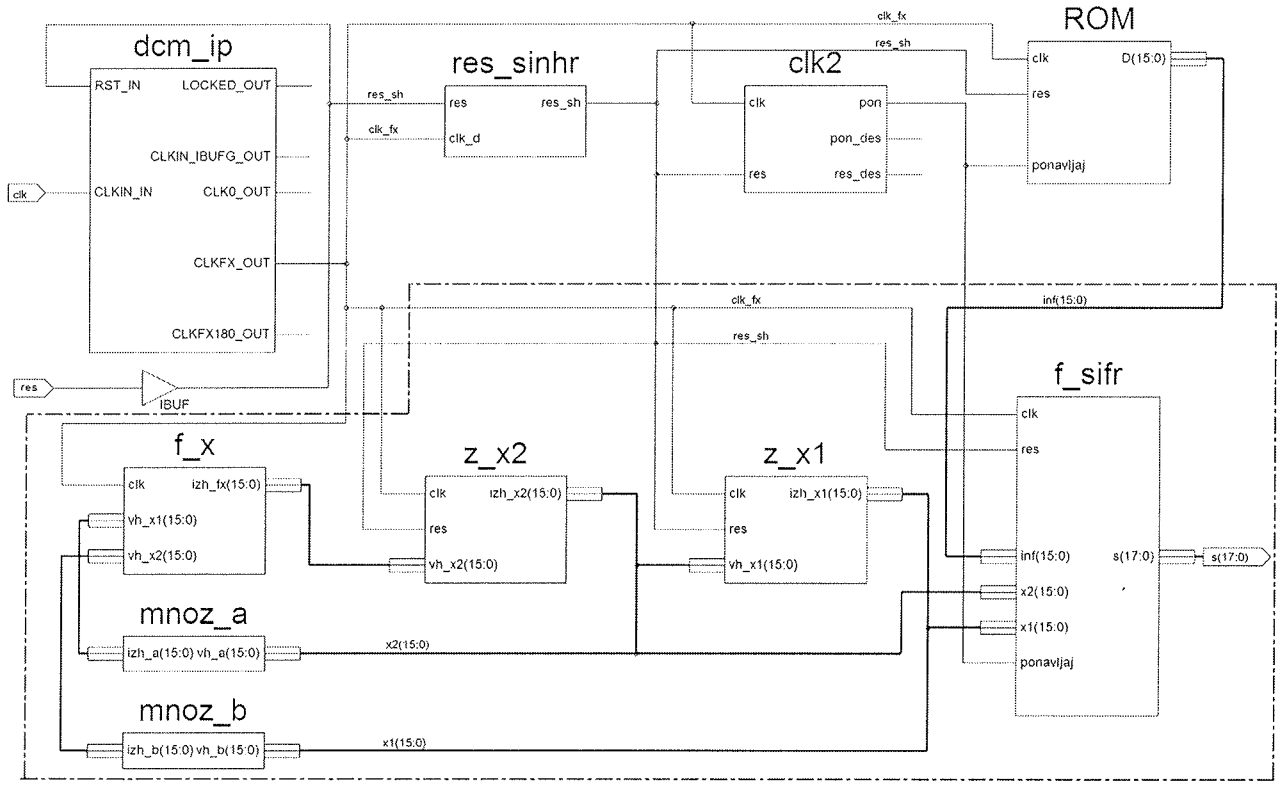
Ker sta šifrirna in dešifrirna funkcija rekurzivni, bo za izračun posamezne vrednosti $y(n)$ oziroma $i^*(n)$ potreben določen čas, ki bo odvisen od izbranega števila iteracij N.

4. Implementacija kriptografskega sistema

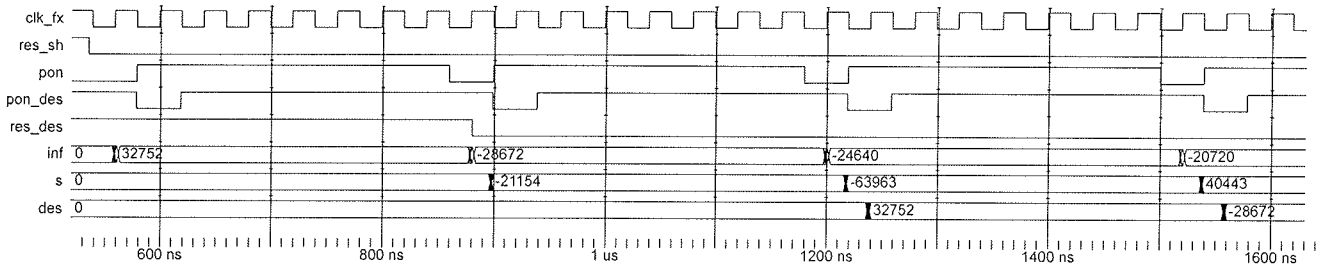
Kriptografski sistem je mogoče implementirati s pomočjo programa, ki se izvaja na računalniku ali s strojno opremo. V našem primeru smo se odločili za realizacijo s polji programirljivih logičnih vezij (vezja FPGA) in aritmetiko s fiksno vejico. Implementirali smo 16-bitno strukturo.

Današnja vezja FPGA ponujajo, razen osnovnih logičnih elementov, bistveno kompleksnejše gradnike: množilnike, bloke za digitalno procesiranje signalov pa tudi procesorje. Iz slike 1 je razvidno, da sta najkompleksnejši enoti generatorja psevdo-kaotičnih sekvenc, množilnika. Ker pa sta multiplikatorja, a = 0,5 in b = -1, je realizacija obeh množenj enostavna, in sicer z vezjem za pomik binarne besede v desno in vezjem za tvorjenje dvojiškega komplementa. Tako realiziran generator psevdo-kaotičnih sekvenc bo sposoben v eni periodi urinega signala generirati novo psevdo-kaotično število.

Čim krajše razvojno obdobje, možnost enostavne nadgradnje sistema in spremembe tajnega ključa narekujejo načrtovanje z uporabo visokonivojskega jezika. Podjetje XILINX predstavlja enega izmed vodilnih proizvajalcev in ponuja širok spekter vezij FPGA. Razen visoko zmogljivih (družina Virtex), ponuja tudi srednje zmogljiva vezja (družina Spartan). Hkrati je prosto dostopna osnovna verzija načrtovalskega orodja ISE. Orodje ISE podpira opis vezij z vi-



Slika 6: Izvedbena struktura šifrirnega sistema v vezju FPGA.
Fig. 6: FPGA realization block scheme of cipher circuit.



Slika 7: Simulirani časovni odzivi kriptografskega sistema izvedenega v vezju FPGA.
Fig. 7: Simulated waveforms of cryptographic system realized in FPGA circuit.

sokonivojskim jezikom (VHDL, Verilog, ...), shematski opis in opis s pomočjo diagrama stanj. Skupaj z logičnim simulatorjem ModelSim, omogoča osnovno funkcionalno preverjanje delovanja vezja in časovno simulacijo.

Kriptografski sistem smo realizirali s pomočjo razvojne plošče Spartan-3E /9/. Jedro razvojne plošče predstavlja vezje XC3S500E družine Spartan-3E. Poleg klasičnih gradnikov (logična vrata, logične celice, pomnilnik RAM, ...), so v XC3S500E na voljo tudi množilniki 16×16 bitov, ki pa jih naše vezje ne izkorišča. Za opis vezja smo uporabili kombiniran pristop z visokonivojskim jezikom VHDL in shematskim opisom. Zaradi enostavnejše primerjave z osnovno blokovno shemo (glej sliko 5), smo vezje razdelili na osnovne enote, kot to prikazuje slika 6.

Na sliki 6 je šifrirni sistem obkrožen s prekinjeno črto. Posamezni bloki so predstavljeni z naslednjimi imeni:

- *mnoz_a*, *mnoz_b*: moženje s konstantama *a* in *b*, izvedeno s pomikom vsebine za bit v desno (*mnoz_a*) in s tvorjenjem dvojiškega komplementa (*mnoz_b*);
- *z_x1*, *z_x2*: zakasnilna elementa;
- *f_x*: seštevanje v aritmetiki z dvojiškim komplementom;
- *f_sifr*: multipomična šifrirna funkcija;
- *dcm_ip*: generator signala ure z delitvijo signala zunanje ure *clk*;
- *res_sinhr*: vezje za reset;
- *clk2*: generator krmilnih signalov;
- *ROM*: pomnilnik z odprtim sporočilom.

Vodila znotraj šifrirnega sistema, kot tudi enota (beseda) odprtega sporočila *inf* (slika 6), so 16 bitna. Enota tajnopisa *s* je zapisana z 18 biti. Da hitrosti delovanja šifrirnega sistema ne bi omejevale vhodno/izhodne enote razvojne plošče, je odprto sporočilo *inf* dolžine 5500 besed, shranjeno v pomnilniku tipa ROM (slika 6) in se ponavljajoče pošilja šifrirnemu sistemu. Splošno gledano, sta lahko začetni stanji $x_1(0)$ in $x_2(0)$ zakasnilnih elementov *z_x1* in *z_x2* poljubni, z enačbo (1) določeni vrednosti. V našem primeru smo ju zapisali v dvojiškem komplementu s 16 bitno besedo in sicer z $B179_{16}$ (-0,6135) in $4E87_{16}$ (0,6135). Število iteracij *N* šifrirne funkcije (enačbi 2 in 3) določa blok *clk2*, s pomočjo kontrolnega signala *pon*. Posamezna iteracija šifriranja se izvede v eni periodi ure *clk_fx*. Šifriranje z nelinearno funkcijo (3) se ponavlja dokler signal *pon* ostaja na nivoju logične enice. S postavitvijo signala *pon* na nivo logične ničle se beseda tajnopisa *s* prenese na izhod in zajame novo vrednost odprtega sporočila *inf*.

Pravilnost delovanja šifrirnega sistema smo preverili s pomočjo dešifrirnega sistema, ki smo ga realizirali v istem vezju FPGA. Njegova struktura je podobna strukturi šifrirnega sistema na sliki 6, zato je podrobneje ne bomo opisovali. V realnem okolju sta šifrirni in dešifrirni sitem običajno dislocirani napravi. Da kriptografski sistem deluje pravilno, je potrebno pred pošiljanjem tajnopisa poskrbeti za sinhronizacijo generatorjev psevdo-kaotičnih sekvenc ter varno izmenjavo tajnega ključa. Ključ sestavlja podatek o številu iteracij multipomične šifrirne funkcije ter vrednosti začetnih stanj $x_1(0)$ in $x_2(0)$. Načrtovanje vezja za sinhronizacijo in varno izmenjavo tajnega ključa ni predmet naših raziskav, zato smo sinhronizacijo zagotovili kar s pomočjo signalov *res_des*, *pon_des* in *clkfx180_out* (slika 6). Navedeni signali predstavljajo reset, kontrolni signal iteracij in uro dešifrirnega sistema. Izbrali smo tajni ključ in ga uporabili na šifrirnem in dešifrirnem sistemu. Simulirane časovne poteke signalov, z upoštevanimi zakasnitvami povezav in elementov, prikazuje slika 7.

Označbe signalov so naslednje:

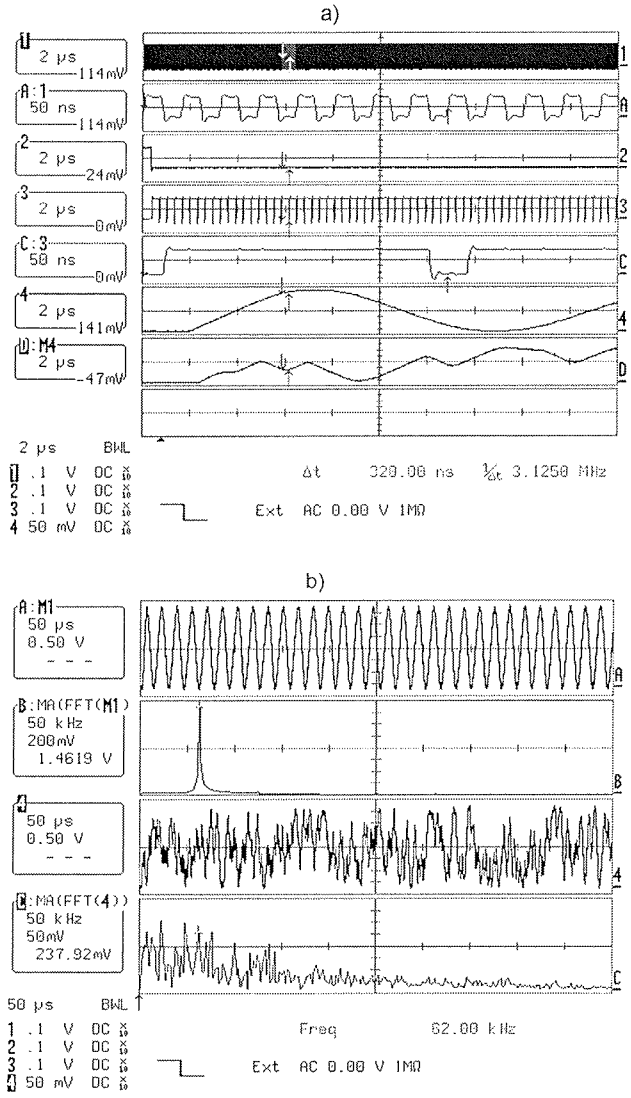
- *clk_fx*: signal ure, s pomočjo fazne zanke sintetiziran iz *clk*;
- *res_sh*: z uro *clk_fx* sinhroniziran asinhroni reset *res*;
- *pon*, *pon_des*: krmilna signala šifrirnega in dešifrirnega sistema, ki določata število ponovitev multipomične funkcije;
- *inf*: oprto sporočilo;
- *s*: tajnopis;
- *des*: dešifrirano odprto sporočilo.

Za izbrano vezje FPGA XC3S500E-4 smo uspeli zagotoviti inverznost med operacijo šifriranja in dešifriranja do frekvence ure f_{clk_fx} = 25MHz. Frekvenco ure omejujejo časovne zakasnitve elementov in povezav v vezju FPGA. Če je število ponovitev multipomične šifrirne funkcije $N > 1$, se frekvenca šifriranja odprtega sporočila ustrezno zmanjša. Na sliki 7 je prikazan primer za $N = 7$, kjer je šifriranje besede odprtega sporočila trajalo 320 ns oz. s frekvenco

3,125 MHz. Enak čas je potreben tudi za dešifriranje (signal *des* na sliki 7).

5. Rezultati meritev

Pravilno delovanje vezja potrjujejo rezultati meritev. Čeprav lahko šifriramo poljubne podatke kot so tekst, digitalizirani avdio ali video signal, smo delovanje kriptografskega sistema preverili s pomočjo šifriranja in dešifriranja sinusnega signala. Digitalizirane vrednosti smo zapisali v pomnilnik ROM (slika 6). Primerjavo med odprtim sporočilom in tajnopisom smo izvedli s pomočjo 12 bitnega serijskega DA pretvornika LTC2624, ki je na voljo na razvojni plošči. Sliki 8 a) in b) prikazujeta izmerjene odzive.



Slika 8: Rezultati meritev: a) Časovni odzivi šifrirnega sistema. b) Časovna poteka tajnopisa in dešifriranega odprtega sporočila, ter njuna amplitudna spektra.

Fig. 8: Measured waveforms: a) Cypher circuit waveforms. b) Waveforms Simulated waveforms of cryptographic system realized in FPGA circuit.

Slika 8 a) prikazuje: časovni potek signala ure *clk_fx*, izsek signala *clk_fx*, signal *res_sh*, signal *pon*, izsek signala *pon*, odprto sporočilo *inf* (sinusni signal) in tajnopis *s*. Slika 8 b) prikazuje dešifrirano sporočilo (potek A), njegov amplitudni spekter (potek B), časovni potek šifriranega signala (potek 4) in njegov amplitudni spekter (potek C). V amplitudnem spektru šifriranega signala ni mogoče prepoznati oprtega sporočila.

Maksimalna dopustna frekvenca delovanja kriptografskega sistema je veliki meri odvisna od razmestitve elementov, dolžine povezav v vezju FPGA in od izbranega vezja FPGA oz. tipičnih zakasnitev logičnih blokov ter povezav. V procesu načrtovanja običajno uporabljamo postopke avtomatskega razmeščanja in povezovanja na katere lahko vplivamo. S vhodnimi parametri in z določitvijo časovnih omejitev, ki jih morajo izpolnjevati elementi vezja in povezave, lahko vplivamo na doseženo maksimalno frekvenco delovanja. Tako smo s postopkom Fmax /10/ poiskali vhodne nastavitve algoritmov avtomatskega razmeščanja in povezovanja, ki maksimirajo hitrost delovanja šifrirnih, vezij realiziranih na petih različnih platformah. Rezultate prikazuje tabela 1.

Družina	Vezje FPGA	Frekv. [MHz]
Spartan 3E	XC3S500E-4	39,44
Spartan 3E	XC3S400-5	39,83
Virtex 2P	XC2VP2-7	57,62
Virtex 4	XC4VLX25-12	77,23
Virtex 4	XC4VFX12-12	77,71

Tabela 1. Predvidene maksimalne frekvence delovanja šifrirnega vezja glede na izbrano vezje FPGA.
Table 1. Expected maximum clock frequency of cipher circuit depending on chosen FPGA circuit.

Maksimalne frekvence delovanja smo le ocenili, saj dejanskega delovanja nismo preizkusili. Najvišji hitrosti delovanja lahko pričakujemo v primeru uporabe vezij družine Virtex 4. Najnovejše družine Virtex 5 nismo preizkusili, saj je razvojno orodje ISE WebPack ne podpira.

6. Zaključek

V prispevku smo predstavili kaotični kriptografski sistem in možnost njegove strojne realizacije. Šifrirni in dešifrirni sistem sestavljata multipomična šifrirna oz. dešifrirna funkcija in generator psevdo-kaotičnih sekvenc, realiziran s kaotičnim digitalnim sitom. Oba sistema smo izvedli v istem vezju FPGA družine Spartan 3E. Struktura šifrirnega sistema je bila 16 bitna.

Bistvena prednost predlagane strojne izvedbe pred programsko, je hitrost izvajanja šifrirnega in dešifrirnega algoritma. Za generiranje psevdo-kaotične vrednosti je potrebna le ena perioda urinega signala. V našem primeru sta bili

operaciji šifriranja in dešifriranja še inverzni, če je bila frekvenca ure 25 MHz. Maksimalna frekvenca šifriranja je odvisna predvsem od števila ponovitev multipomične šifrirne oziroma dešifrirne funkcije. S pomočjo postopka Fmax pa smo ocenili, da bi lahko pri uporabi vezij družine Virtex 4, frekvenco ure povečali na 77,71MHz.

Programirljivost vezij FPGA omogoča enostavno spremembo števila bitov strukture kaotičnega sistema in dolžino tajnega ključa. Uporaba daljših enot šifriranja ne bi vplivala na hitrost šifriranja, ampak le na kompleksnost sistema, saj bi se povečal uporabljen delež razpoložljivih logičnih blokov v vezju FPGA.

7. Literatura

/1/ N. Masuda, G. Jakimoski, K. Aihara, L. Kocarev: *Chaotic Block Ciphers: From Theory to Practical Algorithms*, IEEE Transaction Circuits and Systems-I: letnik 53, št. 6, junij 2006, str. 1341-1352.

/2/ T. Stojanovski, L. Kocarev: *Chaos-Based Random Number Generators-Part I: Analysis,* IEEE Transaction Circuits and Systems-I: Fundamental Theory and Applications, letnik 48, št. 3, marec 2001, str. 281-288.

/3/ L. M. Pecora, T. L. Carroll: *Synchronization in Chaotic Systems,* Physical Review Letters, letnik 64, št. 8, 1990, str. 821-824.

/4/ B. Schneier: Applied *Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*, John Wiley & Sons, New York, 1996.

/5/ Greg M. Bernstein, Michael A. Lieberman: *Method and apparatus for generating secure random numbers using chaos*, US Patent No. 5007087, april 1991.

/6/ Gernot Kubin: *What Is a Chaotic Signal ?*, IEEE Workshop on Nonlinear Signal and Image Processing, Greece, 20 - 22. junij, 1995, http://poseidon.csd.auth.gr/Workshop/papers/.

/7/ M. Šalamon, T. Dogša: *Nevarnost kaosa v digitalnem situ drugega reda*, Inf. MIDEM, letnik 30, št. 1, marec 2000, str. 37-42.

/8/ T. Yang, C. W. Wu, L. O. Chua: *Cryptography Based on Chaotic Systems*, IEEE Transaction Circuits and systems-I: Fundamental theory and applications, letnik 44, št.5, maj 1997, str. 469-472.

/9/ Xilinx, Inc.: *Spartan-3E Starter Kit Board User Guide*, UG230 (v1.0) March 9, 2006.

/10/ H. Patel: *Synthesis and Implementation Strategies to Accelerate Design Performance*, Xilinx, Inc., July, 2005.

Doc. dr. Bojan Jarc
Doc. dr. Matej Šalamon

oba UNIVERZA V MARIBORU
FAKULTETA ZA ELEKTROTEHNIKO,
RAČUNALNIŠTVO IN INFORMATIKO
2000 Maribor, Smetanova 17, Slovenija
e-mail: *bojan.jarc@uni-mb.si, matej.salamon@uni-mb.si*

Prispelo (Arrived): 20.12.2006 *Sprejeto (Accepted):* 30.03.2007