UDK: 681.3.067(047)=861
COSATI: 09-02, 17-02, 14-07

Arhitektura mikroprocesorskog modula za kriptozaštitu datoteka na personalnim računarima

Mr Srđan Atanasijević, dipl.inž.[1)]

Analizira se problem zaštite tajnosti podataka na savremenim personalnim računarima. Kao rezultat analize predlaže se arhitektura mikroprocesorskog modula koja ispunjava postavljene konstrukcijske zahteve.

Ključne reči: **Zaštita tajnosti podataka, kriptografske metode, arhitektura računara, PC mikroračunari.**

Korišćene oznake i simboli

M – otvoren tekst,
E – šifrovan tekst,
T_k – kriptografska transformacija,
k – ključ za kriptovanje,
T_k^{-1} – inverzna kriptografska transformacija - dešifrovanje
L_{max} – maksimalna dužina pseudoslučajnog niza
n, m – dužine šift registara
GPSN – generator pseudoslučajnih brojeva

U v o d

RAZMATRA se zaštita, pre svega, ličnih podataka korisnika PC mikroračunara kao i podataka koje u svom radu stvara manji tim pojedinaca zaposlenih u lokalnoj računarskoj mreži i koji učestvuju u kreiranju radne dokumentacije. Stepen primenjene zaštite treba da se ograniči na vreme trajanja poslovnog procesa, odnosno vreme tajnosti kreiranih dokumenta je prirodom primene vremenski ograničeno. Posle nekog vremena (npr. nekoliko meseci) tajnost dokumenata nije više imperativ, jer se rezultati rada publikuju, tj. rezultat poslovnog procesa je vidljiv.

Postupak kriptografske zaštite treba da bude jednostavan, a tehnika transparentna za korisnika. Korisnici treba da se pridržavaju procedure koja ih svojom kompleksnošću ne sputava u radu.

Arhiva u kojoj se čuvaju kriptovani podaci je centralizovana - čuvaju se ili lični dokumenti ili dokumenti sa kojima radi manji tim u lokalnoj mreži, tako da su za primenu pogodne simetrične kriptografske metode.

Radi veće brzine procesa kriptovanja kao i fizičkog odvajanja kriptografskog algoritma od operativnog sistema korisnika, poželjna je hardverska implementacija algoritma.

U grupi simetričnih kriptografskih metoda pogodnih za jednostavnu hardversku implementaciju izdvajaju se *sekvencijalni simetrični šifarski* sistemi. *Sekvencijalni simetrični šifarski* sistemi koriste jednostavan princip, a to je sumiranje po modulu dva niza slučajnih brojeva (koji čine ključ) sa nizom informacija koje se štite. Sigurnost sistema zasniva se na kvalitetu niza slučajnih brojeva.

Kako je cena uređaja presudan faktor za širu primenu u ovako definisanom okruženju primene, potrebno je da uređaj bude što jednostavnije konstrukcije, znači jeftin, a ipak da bude robustan, pouzdan, prenosiv na različite operativne sisteme, efikasan i brz.

Kriptografski algoritmi pogodni za hardversku implementaciju: generator pseudoslučajnih brojeva po modelu Marsaglia- McLaren

Kvalitet niza slučajnih brojeva: kvalitet kriptografije

Kriptografija je tehnika [1] kojom se čitljiv, otvoren, tekst (M) koji treba štititi, transformiše u nečitljiv - šifrovan tekst (E), kriptografskom transformacijom izabranom iz skupa transformacija - šifara (T) na osnovu parametara - ključa kriptosistema (K), a kasnije primena inverzne transformacije (T^{-1}) nad šifrovanim tekstom (E) daje ponovo otvoren (izvorni) tekst (M).

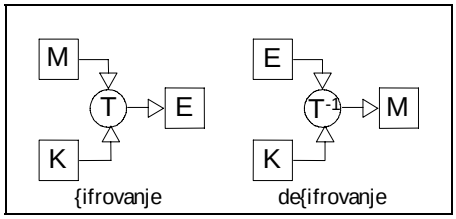
Tako jednačina za šifrovanje teksta glasi:

$$E = T_K(M) \tag{1}$$

a za dešifrovanje:

$$M = T_K^{-1}(E) \tag{2}$$

Grafički prikaz ove tehnike je dat na sl.1.



Slika 1. Grafički prikaz tehnike kriptografije

Kriptografske metode pogodne za primenu u ovakvim slučajevima su metode zasnovane na beskonačnim

[1)] Viša tehnička škola, 34000 Kragujevac, Španskih boraca 8

slučajnim nizovima, koje se u teoretskom i praktičnom smislu smatraju apsolutno tajnim [1-4]. Kao generatori ovakvih nizova mogu da se koriste razni elektronski elementi (diode, tranzistori, i dr.) kod kojih se kao izvor slučajnosti koriste šumovi. Dodatnom opremom signal šuma se pretvara u slučajan niz koji se "sabira" po nekom modulu (obično 2) sa otvorenim tekstom, a na izlazu se dobija šifrovani niz. Međutim, ovakva oprema nema praktičnu upotrebu u svakodnevnom životu. Pored toga, da bi se šifrovan tekst dešifrovao potrebno je da se ceo ključ, slučajan niz, čuva u posebnoj datoteci, što ovu tehniku čini glomaznom i u praksi teško ostvarivom.

Da bi se ova dobra ideja učinila pogodnom za praktičnu primenu, neophodno je koristiti slučajan niz, koji se može relativno lako stvoriti, a restaurisati po volji. Naravno, to više neće biti potpuno slučajan niz (jer je kontrolabilan) pa će se nazvati pseudoslučajni niz (PSN).

Osnovni zahtev, koji se postavlja pred PSN, jeste da ima što duže periode ponavljanje sekvence, da ima veliki broj različitih perioda i da ima karakteristike koje neznatno odstupaju od karakteristika pravih slučajnih nizova. Da bi se to postiglo, potrebno je da PSN ispuni sledeće zahteve [4,5]:

- PSN mora da ima uniformnu raspodelu,
- sukcesivno pojavljivanje "0" i "1" mora da bude što kraće,
- rezultati svih relevantnih testova nad PSN moraju da budu što sličniji rezultatima testova slučajnog binarnog niza.

Posebno interesantna i perspektivna klasa generatora PSN-a izuzetno pogodna za primenu u oblasti kriptozaštite podataka, obrađena je u velikom broju radova [3-6], a to su nelinearni generatori PSN-a (NGPSN) tipa Marsaglia-MacLarena (MMGPSN) [4].

U [4 i 5] detaljno su ispitane statističke osobine odabranih tipova MMGPSN-a sa sedam aspekata: Hi-kvadrat test (Pirsonov), test Romanovskog, test Kolmogorova, BLOK test, frekvencijski test, poker test i test sakupljača (collector).

Na osnovu dobijenih rezultata, komparativnom analizom, najbolje karakteristike pokazao je MMGPSN sa davačem u obliku memorijskog polja (RAM). Ovaj generator je izabran kao osnova za konstrukciju modula za kriptografiju podataka na PC mikroračunaru.

U vreme završetka izrada ovog projekta, dr Mihaljević je [6] objavio postupak kriptoanalize poruka kriptovanih korišćenjem Marsaglia-MacLaren algoritma.

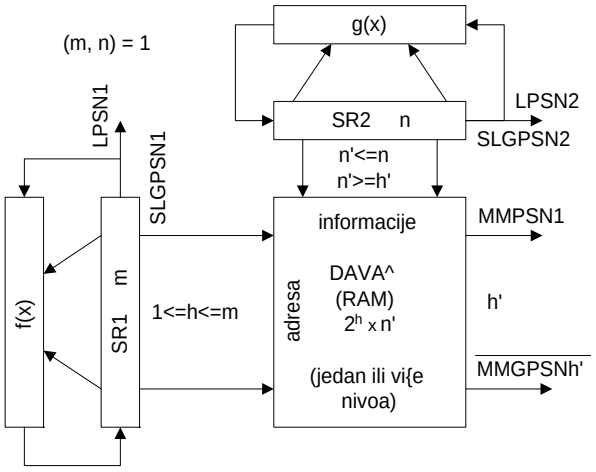
To znači, da se modul zasnovan na ovom algoritmu ne može koristititi za zaštitu informacija koje zahtevaju najviši stepen tajnosti, ali je i dalje veoma upotrebljiv u svakodnevnoj primeni, što i jeste cilj projekta.

Klasa generatora Marsaglia- MacLaren: generator na bazi primene RAM memorije

Generatori pseudoslučajnih nizova (PSN) zasnovani na modelu koji su predložili Marsaglia i MacLaren, smatraju se najefikasnijim generatorima PSN-a [4]. Ovi generatori su jednostavni, pouzdani, efikasni, ekonomični, brzi i moguća je jednostavna kontrola rada elemenata u konfiguraciji generatora [8].

Ovaj tip generatora je nelinearan, jer svaki generator ima jedan ili više nelinearnih elemenata. Za rad u polju binarnih brojeva, što je predmet interesovanja ovog rada, nelinearni elementi su različiti mešači (multiplekseri, JK bistabili) kao i razni davači: memorije (RAM), registri itd.

MMGPSN na bazi primene RAM memorije (davač) (MMGPSND) sastoji se, najčešće, od dva linearna generatora PSN (SLGPSN) i jednog davača kao što je prikazano na sl.2. Najpovoljnije, s aspekta jednostavnosti i efikasnosti, je da se za pobudne generatore koriste SLGPSN, a kao davač memorija (RAM), [4].



Slika 2. Opšta blok šema MMGPSND (MMGPSNRAM)

Cela konfiguracija prikazana na sl.2 može biti upotrebljena kao jedan pobudni generator, koji generiše adresu ili informaciju za neki davač na drugom nivou što znači da se može formirati MMGPSN u više nivoa. Međutim, analizom MMGPSND pokazano je [4,5] da je i MMGPSND sa jednim nivoom dovoljno dobar za širok spektar primena, te će se takav model MMGPSND koristiti kao baza za projektovanje generatora PSN-ova u kriptomodulu.

Ovakav sklop funkcioniše na sledeći način:

SLGPSN2, koji daje PSN uniformnih brojeva kao informaciju za glavno memorijsko polje (tok označen kao informacioni simboli). SLGPSN1, čijim izlazom se prozivaju memorijske lokacije glavnog memorijskog polja (tok označen kao adresni simboli). Na osnovu postavljene adrese prvo se iščitava prozvana memorijska lokacija glavnog memorijskog polja, a zatim se u tu lokaciju unosi novi broj, generisan pomoću SLGPSN2.

Za praktičnu primenu ovakvog koncepta potrebno je da se identifikuju parametri generatora koji utiču na kvalitet izlazne sekvence, a to su:

- *maksimalna dužina sekvence* bez ponavljanja, koja se izračunava po formuli:

$$L_{\max} = \left(2^n - 1\right) \cdot \left(2^m - 1\right) \tag{3}$$

pri čemu su *m i n* dužine registara SR1 i SR2,

- *veličina RAM memorije* koja utiče na broj različitih izlaznih nizova (ključeva) koji se generišu,
- *početna stanja* registara i RAM memorije,
- *dozvoljene vrednosti* funkcija povratnih veza $f(x)$ i $g(x)$,

Model hardverske implementacije algoritma: prilagođenje zahtevima PC korisnika

Na osnovu analize opisane u [2] postavljeni su sledeći parametri konfiguracije generatora (oznake su prema sl.2):

- veličina SR1 je (m=8) 8 bita
- početno stanje SR1

- broj adresnih ulaza, odnosno veličina RAM memorije je 128 bita
- veličina SR2(n) je od n=3 do n=15, odnosno pošto (m,n)=1, n uzima vrednost iz skupa $n\in\{3,5,7,9,11,13,15\}$
- početno stanje SR2 je sa logičkom jedinicom u prvoj ćeliji (1000...)
- raspored 6 (h-1) adresnih ulaza u RAM sa SR1 od 7 (m-1) preostalih pošto se sa prvog bistabila SR1-1 izlaz vodi na adresni ulaz RAM-a A0
- parametar smetnje S
- $f(x)$
- $g(x)$

U praksi je potrebno da se zadovolje sledeći konstrukcijski uslovi:

- početna stanja SR1 i SR2 moraju biti različita od nule;
- broj XOR elemenata u povratnoj vezi $f(x)$ i $g(x)$ mora da bude neparan;
- konfiguracija povratne veze $f(x)$ i $g(x)$ mora da obuhvata i poslednji m-ti odnosno n-ti stepen;
- $f(x)$ i $g(x)$ treba da budu primitivni polinomi;
- prvih S bitova na izlazu generatora ne smeju da se mešaju sa bitovima izvornog fajla koji se štiti.

Funkcionalni opis arhitektura modula za kriptografiju: modul baziran na PC ISA sabirnici

Osnovne funkcije, koje podsistem za kriptografsku zaštitu datoteka na PC mikroračunaru treba da obavi, jesu:

- šifrovanje datoteka u realnom vremenu,
- dešifrovanje datoteka,
- mogućnost rada u programskom i prekidnom režimu rada,
- maskiranje grešaka nastalih u radu i
- dojava otkaza vitalnih funkcionalnih blokova.

Posebni zahtevi ostvareni u konstrukciji sa stanovišta funkcionalnosti primene su:

- *pouzdanost* u radu, koja se postiže maskiranjem grešaka upotrebom tehnike povećanja redudancije tzv. TMR (*Triplicated Modular Redudancy*) [8] maskiranjem greške u radu (*fault masking*) jednog od kritičnih funkcionalnih blokova,
- *dojava otkaza* jednog od kritičnih funkcionalnih blokova na osnovu čega se preduzimaju procedure za proveru ispravnosti šifrovane datoteke,
- *prenosivost,* koja se ogleda u "otvorenosti" za ugradnju na sve modele PC mikroračunara bez obzira na proizvođača,
- *mobilnost,* što znači da se po potrebi može evakuisati iz PC mikroračunara kao dodatni vid osiguranja zaštite,
- *zatvorenost* podsistema, koja je ostvarena realizacijom algoritma generisanja PSN-a kao i šifrovanje hardverski čime se povećava i brzina šifrovanja,
- *fleksibilnost* ostvarena programskim modelom, koji omogućuje različite aplikativne nadgradnje podsistema uz povećanje njegove upotrebljivosti i
- *niska cena* modula jer je izgrađen od jeftinih TTL komponenata, kao što su brojači, registri, logička kola i sl.

Osnovna funkcija podsistema za kriptografiju je da na osnovu komande izdate spolja, od strane CPU-a, izvrši zadatak - šifrovanje datoteke. Taj zadatak ovaj podsistem mora obaviti brzo, pouzdano i efikasno.

Geneza arhitekture podsistema za kriptografiju:

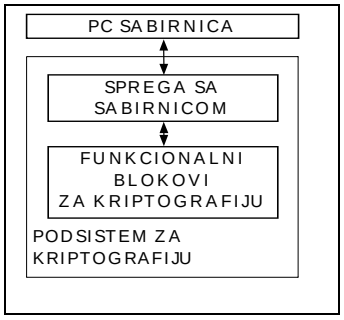
Geneza arhitekture podsistema za kriptografsku zaštitu datoteka na PC mikroračunaru prikazaće se u tri koraka metodologijom hijerarhijske dekompozicije - *odozgo na dole* (*top-down*). U prvom koraku prikazaće se veza podsistema sa arhitekturom PC mikroračunara. Drugi korak predstavlja analizu osnovnih gradivnih blokova podsistema, a treći korak pojednostavljeni blok-dijagram sa svim bitnim elementima arhitekture podsistema. Četvrti korak, najniži nivo hijerarhijske dekompozicije, nivo funkcionalnih elemenata, biće prikazan u sledećem članku istoga autora, u kome će biti detaljno izložena konstrukcija podsistema.

Podsistem za kriptografiju lociran je na PC ISA kartici tako da će se nazivati i *kriptomodulom*. Podsistem za kriptografiju sastoji se od sprege sa PC ISA sabirnicom i funkcionalnih blokova, opisanih u daljnjem tekstu, koji obavljaju proces kriptografije. Sabirnička sprega upravlja radom funkcionalnih blokova za kriptografiju. Skup komandi, koje se koriste da izvrše inicijalizaciju uređaja ili transakciju prenosa šifrovanog teksta, zovu se rutine za spregu (*device driver*). Rad podsistema za kriptografiju, posle inicijalizacije, odvija se samostalno.

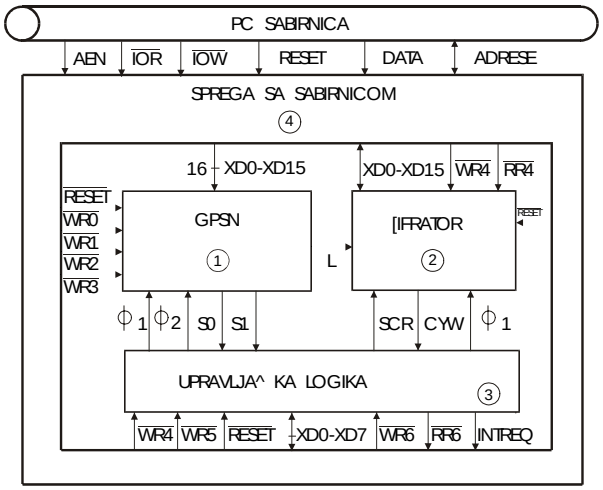
Prvi korak u procesu kriptografije predstavlja prenos reči otvorenog teksta od strane PC-mikroračunara ka podsistemu i iniciranje operacije šifrovanja. Posle izvršene operacije šifrovanja reči otvorenog teksta, aktivira se operacija prenosa ka PC-mikroračunaru, za koju je odgovorna logika sabirničke sprege. Na najvišem nivou apstrakcije arhitekture podsistema razlikuju se dve funkcije:

- funkcija šifrovanja i
- funkcija prenosa (transfer u dva smera i to u smeru od PC-a - reči otvorenog teksta, a u smeru ka PC *sabirnici* reči šifrovanog teksta).

Na sl.3 je prikazana veza kriptouređaja i PC mikroračunara preko sabirničke sprege.



Slika 3. Veza podsistema za kriptografiju sa PC sabirnicom



Slika 4. Funkcionalni blokovi modulaza kriptografiju

U drugom koraku geneze arhitekture prikazni su osnovni funkcionalni blokovi kriptomodula, a to su (sl.4):

1. **GPSN**: generator pseudoslučajnog niza po metodi MMGPSND izloženoj u tekstu.
2. **ŠIFRATOR:** funkcionalni blok za šifrovanje jedne reči (16 bita) otvorenog teksta sa delom niza PSN-a koji sukcesivno, u komadima od po 16 bita, stiže u šifrator iz GPSN-a i šifruje sumiranjem po modulu 2 (reč otvorenog teksta - datoteke),
3. **UPRAVLJAČKA LOGIKA**: funkcionalni blok za generisanje upravljačkih signala, signala vremenskog vođenja ϕ_1 i ϕ_2, te statusni i upravljački registar.
4. **SABIRNIČKA SPREGA**: funkcionalni blok, koji je odgovoran za dekodiranje adrese registara kartice, za baferovanje upravljačkih signala i signala sabirnice podataka.

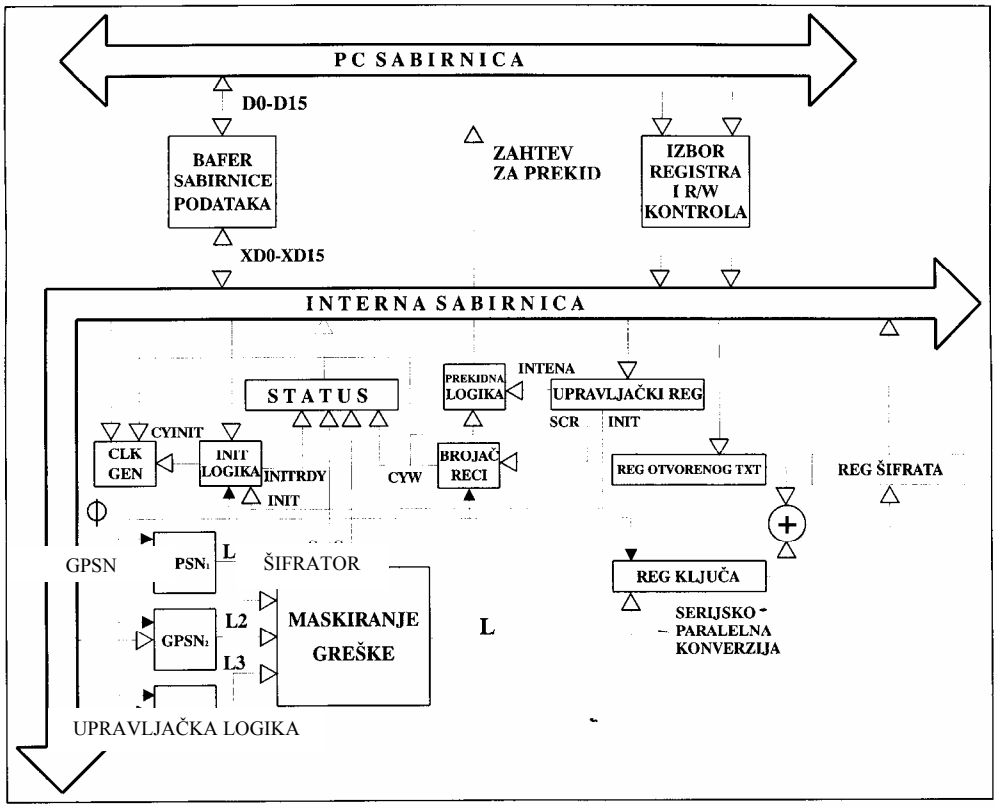
Funkcionalni blok GPSN (broj ⅠⅠ na sl.4) predstavlja generator PSN po modelu MMGPSND, opisanom u prethodnom poglavlju. Funkcija generisanja PSN-a je sa stanovišta pouzdanosti i sigurnosti kriptografije kritična, tako da bi greška na jednom bitu PSN mogla imati katastrofalne posledice pri netačnom dešifrovanju polaznih datoteka, posebno izvršnih. To je funkcionalni blok visoke pouzdanosti projektovan po principima TMR, što znači da je otkaz pojedinog funkcionalnog dela transparentan za korisnika, a ukoliko dođe do greške pri generisanju bita šifrata greška se automatski ispravlja, jer je primenjena tehnika glasanja "dva od tri". Dojava otkaza pojedinačne funkcije bloka obavlja se preko statusnih bitova S_0 i S_1 i prosleđuje se upravljačkoj logici modula, koja inicira procedure dalje obrade otkaza.

Funkcionalni blok ŠIFRATOR (broj ⅡⅠ na sl.4) ima ulogu šifrovanja. U ovaj funkcionalni blok stižu sukcesivno: reči fajla koji se štiti i bitovi PSN kojim se štiti fajl. Nakon serijsko-paralelne konverzije dela PSN-a sumiranjem po modulu dva, formira se reč šifrovanog fajla. Tada se dojavljuje upravljačkoj logici da je šifrovanje jedne reči završeno (signal CYW) koja dalje inicira proces prenosa.

Funkcionalni blok označen kao UPRAVLJAČKA LOGIKA (broj ⅡⅡ na sl.4) odgovoran je za upravljanje i vremensko vođenje podsistema.

Funkcionalnim blokom SABIRNIČKA SPREGA (broj na sl.4) ostvareno je povezivanje i prilagođavanje signala modula sa signalima ISA AT sabirnice.

Na sl.5 je prikazan treći korak u genezi arhitekture



Slika 5. Pojednostavljeni blok-dijagram podsistema za kriptografiju

sistema, pojednostavljeni blok-dijagram podsistema za kriptografiju sa svim bitnim elementima arhitekture.

U okviru funkcionalnog bloka GPSN, označenim sa 1 na sl.4, nalaze se:

- tri generatora pseudoslučajnog niza ($GPSN_1$, $GPSN_2$, $GPSN_3$) i
- logika za maskiranje grešaka, maskiranje i dojavu otkaza (MASKIRANJE GREŠKE).

Ulazne signale u ovaj funkcionalni blok čine:

- baferovani signali sabirnice podataka kojima se inicijalizuju registri generatora,
- signali vremenskog vođenja, generator takta,
- upravljački signali za upis u registre generatora.

Izlazni signali iz funkcionalnog bloka GPSN su:

- signali indikacije otkaza (S_0 i S_1) i
- PSN označen sa L.

U okviru funkcionalnog bloka ŠIFRATOR (br.2 na sl.4) nalaze se:

- registar otvorenog teksta u koji se pre starta šifrovanja upisuje reč iz datoteka koja se šifruje (REG OTVORENOG TXT) - prvi operand,
- registar reči ključa (REG KLJUČA), koji vrši serijsko-paralelnu konverziju ulaznog PSN-a, te je registar drugog operanda u operaciji šifrovanja,
- brojač bitova reči (BROJAČ REČI), koji odbrojava 16 bita reči ključa pri konverziji iz serijskog PSN-a u REG KLJUČA označavajući signalom CYW kraj jednog ciklusa konverzije,
- registar šifrovane reči (REG ŠIFRATA), u koji se smešta rezultat operacije sumiranja po modulu dva operanada smeštenih u registre: registar otvorenog teksta (REG OTVORENOG TXT) i registar reči ključa (REG KLJUČA).

Ulazni signali u ovaj funkcionalni blok su:

- baferovani signali sabirnice podataka kojima se upisuje reč otvorenog teksta,
- signali vremenskog vođenja, generatora takta,
- upravljački signali za upis i čitanje iz registara,
- upravljački signal SCR kojim se omogućuje proces šifrovanja.

Izlazni signali iz funkcionalnog bloka ŠIFRATOR su:

- CYW kojim se označava kraj serijsko paralelne konverzije
- baferovani signali sabirnice podataka kojima se prenosi šifrovana reč.

U okviru funkcionalnog bloka UPRAVLJAČKA LOGIKA (br.3 na sl.4) nalaze se:

- upravljački registar (UPRAVLJAČKI REG),
- statusni registar (STATUS),
- logika za inicijalizaciju (INIT LOGIKA),
- generator signala vremenskog vođenja (CLK GEN),
- logika za generisanje prekida (PREKIDNA LOGIKA).

Ulazni signali u ovaj funkcionalni blok su:

- baferovani signali sabirnice podataka kojima se postavlja registar logike za inicijalizaciju podsistema i upisuju signali u upravljački registar i
- upravljački signali za upis/čitanje u registre.

Izlazni signali iz funkcionalnog bloka su:

- signali generatora takta ϕ_1 i ϕ_2 i
- baferovani signali sabirnice podataka kojima se prenosi stanje statusnog registra.

U okviru funkcionalnog bloka SABIRNIČKA SPREGA (br. 4 na slici 4) nalaze se:

- baferi sabirnice podataka (BAFER SABIRNICE PODATAKA) i
- adresni dekoderi za registre podsistema kao i logika za čitanje, pisanje i inicijalizaciju registara logike podsistema.

Funkcionisanje arhitekture

Funkcionisanje arhitekture modula za kriptografiju biće izloženo prikazom redosleda aktivnosti koje se vrše u fazi inicijalizacije i izvršavanja procesa kriptografske zaštite datoteka.

Posle startovanja procesa kriptografije, modul za kriptografiju obavlja aktivnosti kriptografske zaštite prolazeći kroz tri faze:

- fazu tzv. softverskog RESET-a modula,
- fazu postavljanja na definisane početne vrednosti (tzv. SETUP) logike modula i
- fazu šifrovanja datoteke.

Kraj procesa kriptografije može biti, (status upisan u statusni registar):

- regularno, proces je izvršen korektno i
- potencijalnom greškom, što znači da je došlo do otkaza nekog od generatora.

Prva faza u startovanju uređaja predstavlja dovođenje svih komponenata u poznato početno stanje. To je faza softverskog RESET-a logike i obavlja potpuno iste aktivnosti kao i POWER-ON RESET logike modula. Redosled aktivnosti u toku faze softverskog RESET-a modula za kriptografiju, posle upisa upravljačke reči RESET ($00) u upravljački (UPRAVLJAČKI REG) registar su:

- onemogućenje izlaza iz logike za generisanje prekida (*tree state*),
- blokira se izlaz oscilatora - CLK GEN-a,
- onemogućuje se rad logike ŠIFRATOR-a,
- postavlja se na nulu stanje svih registara i brojača i
- upisuju se odgovarajuće statusne reči za RESET u statusni registar ($00).

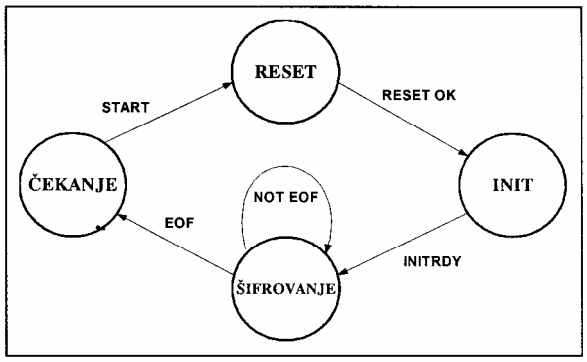
Rezultat prve faze je dovođenje logike modula na poznate početne vrednosti. U drugoj fazi (označenoj sa init na sl.6) vrši se postavljanje vrednosti stanja svih registara, brojača i RAM memorija na vrednosti zadatog ključa, odnosno postavljanje GPSN-a na zadato početno stanje. Posle upisa odgovarajuće komandne reči u upravljački registar (INIT), može da se krene sa sledećim aktivnostima:

- postavljanjem vrednosti $f(x)$ i $g(x)$ na zadate vrednosti,
- postavljanjem početnog stanja registra SR_1 na zadatu vrednost,
- postavljanjem funkcije adresnog mešača,
- postavljanjem vrednosti brojača za određivanje dužine trajanja prelaznog procesa i
- startom uređaja − postavljaju se vrednosti RAM-a GPSN-a tokom zadatog prelaznog procesa.

Rezultat ove faze, tj. kraj uspešno obavljene inicijalizacije upisuje se u statusni registar: signal INITRDY, a bitovi S0 i S1 ne opisuju stanje greške jer su početna stanja RAM memorija tri GPSN u trenutku uključenja postavljena proizvoljno.

Ukoliko su prve dve faze uspešno okončane - sklop je spreman za kriptografiju. Faza kriptografske zaštite fajlova (faza šifrovanje na sl.6) može se odvijati na dva načina:

- pod *programskim* upravljanjem ili
- u *prekidnom* režimu.



Slika.6. Dijagram stanja modula za kriptografiju

Ako se radi sa prekidima, onda bi prvi korak bilo omogućavanje izlaza iz logike za generisaanje prekida i instalacija prekidnog programa (detalji će biti izloženi u poglavlju o softveru).

U upravljački registar upisuje se komandna reč SCR čime je omogućena logika ŠIFRATOR-a, a zatim:

- upisom reči otvorenog teksta iz datoteke koji se štiti startuje se proces kriptografije,
- iz GPSN stiže PSN serijski (linija L) i ulazi u logiku za serijsko-paralelnu konverziju.

Posle 16 taktova signala vremenskog vođenja (CLK), upisana je jedna reč od 16 bita PSN-a i logika za brojanje bita (BROJAČ REČI) generiše signal CYW koji stopira generator takta (CLK GEN), upisuje u statusni registar bit CYW koji označava da je jedna reč šifrovanog teksta spremna za prenos (u prekidnom režimu rada logika za generisanje prekida generiše prekid). Izlazi iz registra koji čuvaju vrednost ključa (REG KLJUČA), zajedno sa izlazima registra koji sadrži vrednost reči otvorenog teksta (REG OTVORENOG TXT) sumiraju se po modulu dva, a rezultat vodi na ulaze registra u kome se privremeno čuva rezultat šifrovanja (REG ŠIFRATA). Kada CPU ustanovi da je reč spremna za transfer inicira se operacija čitanja šifrovane reči, a posle čitanja inicira se operacija prenosa sledeće reči izvorne datoteke koja se šifruje. Posle upisa nove reči u registar prvog operanda operacije šifrovanja (REG OTVORENOG TXT), sklop za brojanje 16 bita koji čine reč ključa (BROJAČ REČI) se postavlja na 0, omogućuje se izlaz iz generatora takta (CLK GEN) i proces šifrovanja teče sve dok se ne dođe do kraja izvorne datoteke (signal EOF na sl.6).

Posle završenog šifrovanja, modul se nalazi u stanju očekivanja novog zadatka (faza čekanje na sl.6). Nakon ponovnog startovanja podsistema, ceo ciklus se ponavlja.

Zaključak

Razmatranjem primenjivosti generatora PSN-a tipa Marsaglia-MacLaren na definisani predmet primene − kriptozaštita datoteka na PC mikroračunaru − izvršen je izbor konfiguracije generatora koji je najprimenjiviji u rešavanju iznetog problema. Prilikom izbora parametara konfiguracije vodilo se računa da modul za kriptografiju zadovolji potrebe zaštite tajnosti podataka većine korisnika PC opreme. Proračunat je maksimalan broj različitih ključeva (nizova) koje generator sa izabranim parametrima može proizvesti po modelu koji su teoretski ponudili Marsaglia i MacLaren. Pri tome je uočeno da se za izabrane promenjive parametre konfiguracije generatora, može povećati broj različitih izlaznih nizova čime se protivniku otežava identifikacija niza ključa. To se postiže na taj način što se prvih *m* bitova (proizvoljnih jer su rezultat početnog stanja memorije) upisuje na početak zaštićenog fajla, a pošto se generator dovede u kontrolisano početno stanje, počne sa šifrovanjem izvornog fajla. Pravi ključ, koji se prenosi i čuva, čine izabrani parametri konfiguracije generatora i dopunski parametar kojim se u izlaznom, šifrovanom nizu, određuje početak stvarnog zaštićenog teksta.

Literatura

[1] PETROVIĆ,S., ĆIRIĆ,V. *Zaštita podataka u automatizovanim informacionim sistemima.* Naučna knjiga, Beorad, 1986.

[2] ATANASIJEVIĆ S. *Mikroprocesorski modul za kriptografsku zaštitu datoteka na personalnim računarima.* magistarski rad, Elektrotehnički fakultet, Beograd, 1997.

[3] GOLIĆ,J., SAVIĆ,Z. *Zaštita informacionih sistema.* TVA KOV Beograd, 1992.

[4] NOVINC,Ž. *Prilog sintezi i analizi generatora PSN.* doktorska disertacija, Elektrotehnički fakultet, Zagreb, 1991.

[5] KOVAČ,S. *Analiza i primena generatora PSN u zaštiti tajnosti podataka.* seminarski rad, Elektrotehnički fakultet, Beograd, 1993.

[6] MIHALJEVIĆ,M. *A Correlation Attack on the Binary Sequence Generators with Time-Varying Output Function.* Advances in Cryptology - ASIACRYPT ‘’94, Lecture Notes in Computer Science, 1995, vol.917, p.67-79.

[7] MARSAGLIA,G., MACLAREN,M.D. Uniform Random Number Generators. *Journal of the Association for Computing Machinery.* January, 1965, vol.12, no.1, p.83-89.

[8] BREUER,A.M., FRIEDMAN,A.D. Diagnosis & Reliable Design of Digital Systems. *Computer Science Press*, 1976.

[9] OBRADOVIĆ,M. i dr. *Zaštitno kodovanje sa statističkim prepoznavanjem oblika.* Vojnoizdavački zavod, Beograd, 1989.

[10] SCHNEIER,B. *Applied Cryptography – Protocols, Algorithms and Source sode in C.* John Wiley and Sons, 1994.

[11] JANKOVIĆ,R. Multimikroprocesorski računarski sistem za transakcionu obradu poruka u realnom vremenu (I)-postavka problema, geneza i funkcionisanje arhitekture. *Naučnotehnički pregled*, 1990, vol.40, no.2, p.3-13.

[12] HWANG,K., BRIGS,F. *Computer architecture and parallel processing.* McGraw-Hill Book Company, 1984.

[13] MENEZES,A., P VAN OORSCHOT, VANSTONE,S. *Handbook of Apllied Cryptography.* CRC Press, 1996.

Rad primljen: 2.2.2000.god.