SIMULACIJA DEFEKATA OSNOVNOG KOLA KONTROLNE LOGIKE NSDDL METODA

Milena Stanojlović, Elektronski fakultet, Univerzitet Niš, milena@venus.elfak.ni.ac.rs
Dragiša Milovanović, Elektronski fakultet, Univerzitet Niš, dragisa.milovanovic@elfak.ni.ac.rs

Sadržaj – *U radu će biti predstavljeno dinamičko NILI kolo (Dnor) koje čini osnovu NSDDL (No Short-circuit current Dynamic Differential Logic) kriptografskog metoda. Pošto ulazi u sastav kontrolne logike kao i samih kriptovanih ćelija veoma je važno ispitati pouzdanost ovakvog kola. Upravo iz ovih razloga biće uvedeni defekti tipa prekid i kratkak spoj radi ispitivanja njegovog logičkog ponašanja.*

1. UVOD

Kako je zloupotreba podataka sve učestalija pojava postalo je neophodno razviti nove metode, kako u softveru tako i u hardveru, radi zaštite podataka. Domen istraživanja ovog rada je primena kriptografskog metoda u hardveru zasnovanom na primeni standardnih ćelija radi projektovanja integrisanog kriptografskog sistema otpornog na napade preko sopednih kanala (*Side Channel Attack* – SCA) [1], [2]. Pod bočnim napadom podrazumeva se svaki pokušaj neovlašćenog otkrivanja sadržaja šifrovane poruke koji je zasnovan na merenju fizičkih parametara u kriptografskom sistemu. Kao fizički parametri mogu se izdvojiti elektromagnetno zračenje, potrošnja energije, talasni oblici signala kao i ostale veličine i fenomeni koji mogu da pomognu dešifrovanje kripto ključa. Praktično u ovaj skup ulaze svi merljivi fizički fenomeni čija analiza pomaže potencijalnom napadaču da otkrije sadržaj zaštićenih informacija. Uobičajen je termin da informacije "otiču kroz bočne kanale". Jedan od osnovnih izvora curenja informacija iz integrisanih kriptografskih sistema prouzrokuje korelacija između talasnih oblika struje napajanja i aktivnosti integrisanog kola. Zato je razvijeno više metoda koji imaju za cilj da ujednače promenu struje napajanja tako što će je učiniti nezavisnom od promene logičkih stanja u digitalnom kolu.

Nakon dužeg proučavanja različitih metoda, primenljivih u hardveru, za zaštitu podataka izabran je jedan koji zadovoljava postavljene kriterijume. Dakle, metod za odbranu od bočnih napada koji koristi predefinisane strukture iz biblioteke standardnih ćelija poznat je pod nazivom NSDDL (*No Short-circuit current Dynamic Differential Logic*) [3].

Dalje u radu, posebna pažnja biće posvećena testiranju Dnor kola na kome je zasnovan pomenuti metod. Namernim uvodjenjem defekata kratkih spojeva i prekida u ispravno kolo pratiće se izlazni signal kao i struja napajanja za svaki defekt zasebno pri određenim kombinacijama ulaznih signala. Broj simulacija zavisiće od broja defekata koji se testiraju. Za ovakav način testiranja autori su se opredelili iz razloga ustanovljavanja testne sekvence, odnosno uspešnosti testa gde se na taj način određuje što veća pokrivenost defekata datom sekvencom. Ovim se može pokazati da jedan test pokriva više defekata što znatno ubrzava proces testiranja. Pored ispitivanja logičke funkcije kola veoma je bitno i porediti struje napajanja ispravnog i kola sa defektom. Kod CMOS tehnologije jednosmerna struja napajanja je veoma mala s obzirom da su, u ustaljenom stanju, svi tranzistori neprovodni [4]. Upravo iz ovog razloga struja ne bi trebalo da zavisi od ulazne reči. Kada defekt postoji u kolu vrlo je verovatno da će se preslikati u promenu pomenute struje. Ovo je korisno jer se umesto stanja na nekom primarnom izlazu može posmatrati jednosmerna vrednost mirne struje napajanja (I_{DDQ}). Poredjenjem struja napajanja ispravnog i kola sa defektom uočava se razlika na osnovu koje se detektuje neispravnost [5].

Da bi se otkrile sve neispravnosti, pored logičkog testiranja, javila se potreba za I_{DDQ} testiranjem o čemu će biti reči u narednim poglavljima.

Rezultati simulacije dobijeni su korišćenjem *ELDO* simulatora u okviru *Mentor Graphics Design Architect* alata. Izabrana tehnologija za projektovanje je TSMC035.

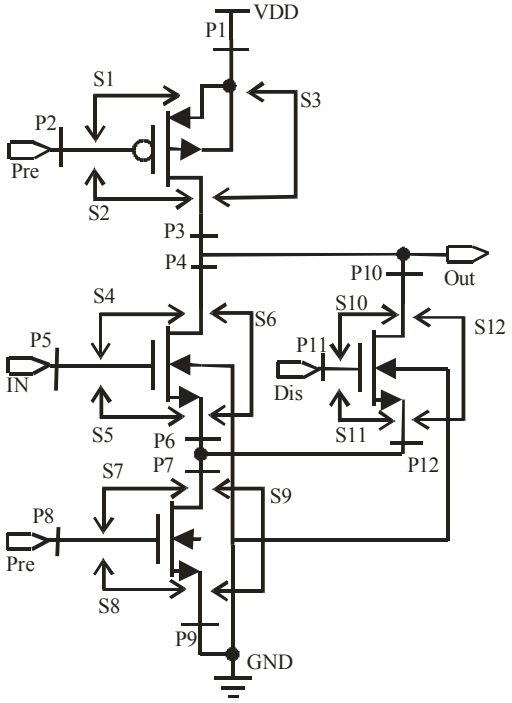
2. NAČINI TESTIRANJA KOLA SA DEFEKTOM

A. Logička simulacija defekata

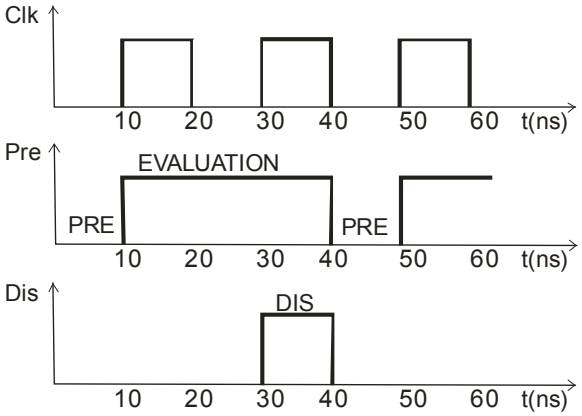
Kada se radi simulacija na logičkom nivou, defekt se modeluje kao logički element. Da bi se obavila simulacija defekata potrebno je da se odredi skup defekata koji se simulira. Nakon toga potrebno je uneti defekt u kolo kako bi se sagledalo prostiranje efekta defekta kroz isto. Model defekta može da sadrži novu funkciju logičkog elementa, promenu kašnjenja ili oba. Generisanje modela defekta treba da bude takvo da omogući preslikavanje skupa kvarova logičkog elementa u tabicu istinitosti. Polazeći od električne šeme i pobudnih signala, u vremenskom domenu, obavljajući električnu analizu dobiće se novi rezultati koji čine novu tablicu stanja. Konkretno, u radu će se razmatrati Dnor kolo u koje se unose defekti, pojedinačno, jedan za drugim. Na slici 1. prikazana je električna šema sa označenim defektima, kola koje se testira. Dvanaest defekata je tipa permanentan kratak spoj i označeni su sa S_i, i=1, 2,...,12 dok je ostalih dvanaest permanentan prazan hod i označeni su sa P_j, j=1, 2,...,12 [5].

Neispravan rad kola može se ustanoviti posmatranjem signala u mernoj tački koji se razlikuje od vrednosti signala u ispravnom kolu. Zato je potrebno generisanje testnog signala koji će to da obezbedi. Na ulazne priključke Dnor kola dovodi se testna sekvenca. Kako Dnor kolo ima tri različita priključka, IN, Pre i Dis, to znači da je maksimalan broj ulaznih kombinacija osam. Zbog specifičnog odnosa ulaznih signala koji mora biti ispoštovan, a što se može videti sa slike 2, ispitivaće se samo šest ulaznih kombinacija. U tabeli 1 oznakom U_l, l=1, 2,..,8 predstavljeno je osam kombinacija. Odnos ulaznih signala određuje rad kola, što znači da se kombinacije U_7=001 i U_8=101 nikada neće javiti na portovima testiranog kola. Za testne sekvence od U_1 do U_6 posmatra se izlaz kako ispravnog tako i kola sa defektom. Bitovi sekvence U_l dovode se na ulaze IN, Pre i Dis respektivno. Signali PRE i DIS, u toku pripremne faze, su u stanju logičke 0. Izvršna faza nastaje kada PRE signal dostigne logičku jedinicu. Faza pražnjenja traje dokle god su i PRE i DIS signali u stanju logičke jedinice [3]. Ovo je jako bitno jer se ovakvo kolo primenjuje u algoritmu za kriptovanje kod koga su presudni kontrolni signali. Testiranje ovakvog kola, specifične namene, ima veliki značaj u daljem

projektovanju. Kako se kriptografski metod oslanja na ispravan rad Dnor kola tako je neophodno ispitati sve mogućnosti koje mogu dovesti do suprotnog. Upravo iz ovog razloga autori su se odlučili za iscrpan test. Rezultati simulacija biće predstavljeni u narednom odeljku.



Slika 1. Prikaz fizičkih defekata u Dnor kolu



Slika 2. Talasni oblici kontrolišućih signala kod NSDDL

Tabela 1. Kombinacije ulaznih signala

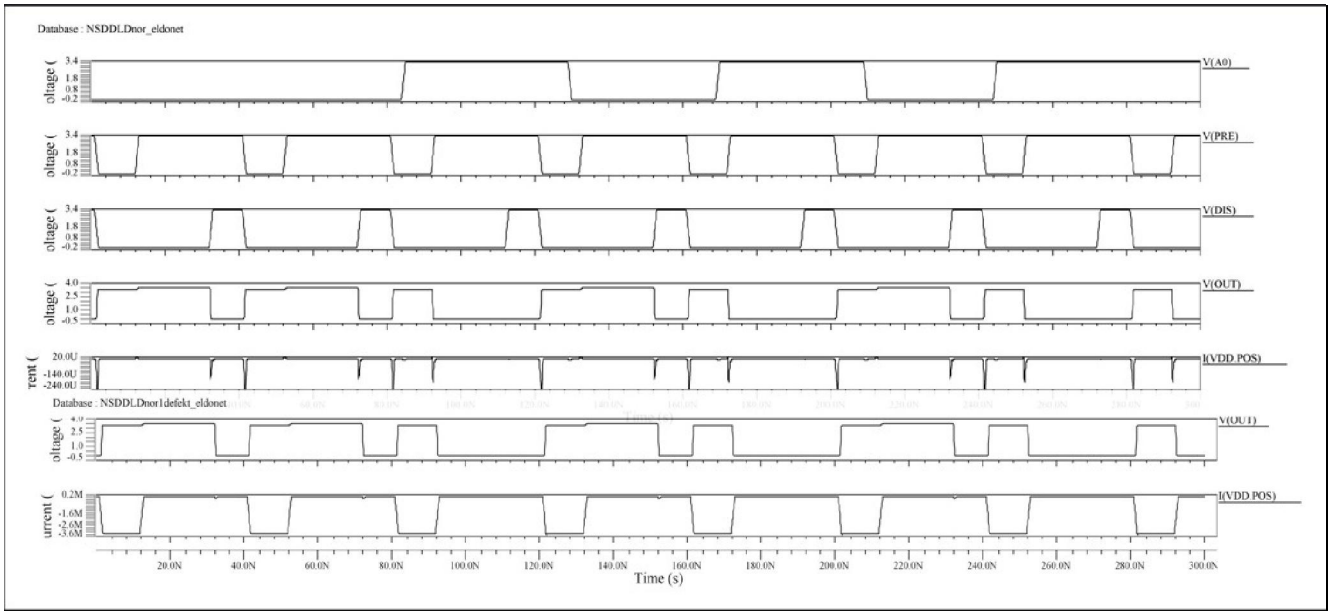
	IN	Pre	Dis
U1	0	0	0
U2	0	1	0
U3	0	1	1
U4	1	0	0
U5	1	1	0
U6	1	1	1
U7	0	0	1
U8	1	0	1

B. Osnove I_{DDQ} testa za digitalna kola

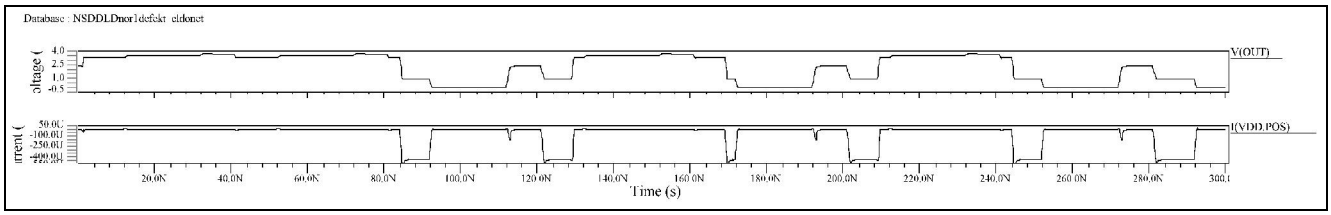
Testiranje bazirano na struji napajanja predstavlja odličnu dopunu testiranju logičke funkcije kola. Pored posmatranog logičkog stanja na primarnom izlazu od velikog je značaja vrednost jednosmerne struje napajanja I_{DDQ}. Uočavanjem razlike izmedju vrednosti struja napajanja ispravnog i kola sa defektom dolazi se do zaključka da u kolu postoji neka neispravnost. Ovakvo testiranje je bitno jer se može desiti da se talasni oblici kola sa defektom ne razlikuju od talasnih oblika ispravnog kola. To je jedan od osnovnih razloga zašto je I_{DDQ} testiranje veoma korisno i ima veliku primenu. I_{DDQ} testiranje digitalnih kola može se obaviti na tri različita načina. Prvi način podrazumeva merenje I_{DDQ} za svaki testni vektor. Ovaj način testiranja je veoma koristan prilikom testiranja prototipova. Rezultati simulacije ispravnog kola predstavljeni su za svaki vektor koji to obezbeđuje. Iako se smatra da je merenje struje napajanja za svaki pobudni vektor nepraktično, zbog velikog broja merenja, autori su se opredelili baš za ovaj način testiranja. Razlog je taj što se testiranje vrši za šest testnih vektora, jer kolo ima mali broj ulaza. Pored toga može se desiti da neki defekti ostanu netestirani što nikako nije poželjno iz razloga konkretne primene ovog kola. Ovo je dovoljan razlog da opravda zašto je rađen iscrpan test. Drugi način I_{DDQ} testiranja je selektivno merenje struje napajanja. Tada se pomenuta sruja meri samo za određene testne vektore. Treći način je dodatno I_{DDQ} testiranje. U ovom slučaju razvijaju se posebni (dodatni) testni signali koji su isključivo namenjeni I_{DDQ} testiranju. Ovo testiranje se obavlja nakon funkcionalnog testiranja. Kao što je ranije pomenuto, kod CMOS integrisanih kola jednosmerna struja napajanja je veoma mala kada je tranzistor u stanju mirovanja, odnosno kada je u stacionarnom režimu. Ukoliko kolo pokazuje značajno povećanje I_{DDQ}, onda se smatra da je u kolu došlo do defekta. Potrebno je odrediti graničnu vrednost te struje koja će pokazati da li je kolo ispravno ili ne. Određivanje ovog praga je od velikog značaja, u smislu da loše određen prag vodi ka nerealnom broju ispravnih, odnosno neispravnih kola. Ovo može dovesti do loše procene vrednosti prinosa i profita [5], [6], [7], [8].

3. REZULTATI SIMULACIJA

Kako su ovde ispitivani defekti tipa permanentan kratak spoj kao i permanentan prazan hod u tabeli 2 prikazani su rezultati pokrivenosti ovih defekata. Bitno je napomenuti da se ovakva vrsta defekata svrstava u grupu fizičkih defekata. Za svaki defekt koji je unet u kolo obavljena je simulacija uzimajući u obzir svaku testnu sekvencu. To znači da su izvršene dvadeset i četiri analize kola sa defektom i jedna analiza ispravnog kola. Posmatranjem dobijenih talasnih oblika i poređenjem sa talasnim oblicima ispravnog kola došlo se do zaključka da se neki defekti ne preslikavaju na izlaz kola. Defekti S_1 i P_2 ne utiču na promenu funkcije kola. Sa slike 3 može se videti da su četvrti i šesti vremenski dijagrami identični, gde prvonavedeni predstavlja izlaz ispravnog, a drugonavedeni izlaz kola sa defektom S_1. U ovm slučaju, kao i u prethodno navedenom, talasni oblici izlaznog napona ne otkrivaju defekt u kolu tako da mogu ostati neopaženi. Kada se pogledaju dijagrami struja ispravnog i kola sa defektom, odnosno peti i sedmi dijagram, respektivno može se zaključiti da to nije slučaj. Poređene su izmerene struje, za svaku ulaznu kombinaciju oba kola, čija razlika ukazuje da kolo ima određene nepravilnosti. Kriterijum na osnovu kojeg je donošena odluka da li u kolu postoji defekt je ta da struje neispravnog kola promeni za 10% u odnosu na struju ispravnog kola. Na slici 4. prikazan je uticaj defekta S_{11} na oblik izlaznog napona kola kao i struje napajanja.



Slika 3. Talasni oblici ispravnog (1-5) i kola sa defektom S_1 (6 i 7)



Slika 4. Talasni oblici napona i struje kola sa defektom S_{11}

Tabela 1. *Detekcija defekata u Dnor kolu*

	Detektovani defekti posmatranjem struje napajanja (IDDQ)	**Detektovani defekti posmatranjem izlaznog napona (UIZ)**
U1	S1, S2, S4, S5, S9, S10, P1, P3, P8, P10	S2, S4, S10, P1, P3
U2	S2, S3, S7, S8, S9, S10, S11, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12	S4, S6, S10, S12, P1, P3, P5, P11
U3	S2, S3, S4, S6, S8, S10, S11 S12, P1, P2, P3, P4, P5, P6, P8, P9, P10, P11, P12	S2, S3, S7, S8, S10, S11, P7, P8, P9, P10, P11, P12
U4	S2, S3, S4, S5, S7, S8, S9, S11, P1, P2, P3, P4, P5, P6, P7, P8, P9, P10	S2, S7, S8, S9, S10, S11, P1, P3
U5	S1, S2, S3, S5, S7, S8, S9, S10, S11 P1, P2, P3, P4, P5, P6, P7, P8, P9, P11, P12	S2, S3, S4, S5, S7, S8, P4, P5, P6, P7, P8, P9
U6	S2, S3, S4, S5, S7, S8, S10, S11, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12	S2, S3, S4, S5, S7, S8, S10, S11, P7, P8, P9

Ovo je samo jedan od defekata koji narušavaju logičku funkciju kola, međutim, ne mogu svi dijagrami biti prikazani. U tabeli 2. sortirani su rezultati na osnovu kojih se može videti da se I_{DDQ} testiranjem otkriva veći broj defekata, ali ne i svi. Defekti detektovani logičkim testiranjem, a koji ujedno pripadaju skupu defekata dobijenog I_{DDQ} testiranjem su oni koji se ispoljavaju kada se na ulaze kola dovode testne sekvence U_1 i U_6. Za sve ostale sekvence I_{DDQ} testiranje daje veći skup defekata kome pripadaju i defekti dobijeni logičkom simulacijom. Ovo je odličan pokazatelj da je za sigurno testiranje neophodno uključiti više različitih metoda tastiranja, naravno, ukoliko je to moguće. Bitno je naglasiti da je za detekciju defekta uzet u obzir i pad napona izlaznog signala koji ne odgovara ni jednoj logičkoj vrednosti. Maksimalan broj detektovanih defekata za jednu testnu sekvencu, kada se obave oba načina testiranja, je dvadeset i jedan. To se postiže kada se na ulaze kola dovedu sekvence U_3 i U_5. Ove dve testne sekvence ne otkrivaju iste vrste defekata. To znači da ove dve sekvence čine minimalni testni skup. Ove dve sekvence omogućuju testiranje svakog defekta. Sekvenca U_3 prestavlja esencijalni test kada se obavlja I_{DDQ} testiranje jer se jedino njime pokrivaju defekti S_6 i S_{12}. Ako se pogledaju skupovi defekata dobijeni pomoću testova iz minimalnog testnog skupa može se zaključiti da je

dovoljno obaviti samo I_{DDQ} testiranje kako bi bili pokriveni svi defekti u kolu. Ovakav postupak je iscrpan i ne preporučuje se kao metod za određivanje minimalnog testnog skupa kod složenih kola.

4. ZAKLJUČAK

U ovom radu simulirano je kolo koje čini osnovu metoda za hardversku odbranu od DPA bočnih napada na kripto-sistem. Zbog velike uloge ovog kola u kriptografskom metodu bitna je i njegova pouzdanost. Iscrpnim analizama došlo se do zaključka da je za detektovanje svih defekata dovoljno primeniti dve testne sekvence i to U_3 i U_5. Logičkim testiranjem detektuje se znatno manji broj defekata u odnosu na broj postignut I_{DDQ} testiranjem. Tako da se I_{DDQ} testiranju može pripisati veća efikasnost. Ovo saznanje će uticati na smenjenje vremena potrebnog za testiranje.

ZAHVALNOST

Rezultati prikazani u ovom radu ostvareni su u okviru projekta TR 32004 koji je finansiran od strane Ministarstva nauke Republike Srbije.

LITERATURA

[1] P. M. Petković, M. Stanojlović, V. B. Litovski "*Design of side-channel-attack resistive criptographic ASICS*", Forum BISEC 2010, Zbornik radova druge konferencija o bezbednosti informacionih sistema, Beograd, Srbija, Maj 2010, pp 22-27.

[2] M. Stanojlović, P. Petković: *Strategies Against Side-Channel-Attack*, Proceedings of the Small Systems Simulation Symposium 2010, Niš, 12-14 February, 2010, pp. 86-89, ISBN 987-86-6125-006-4

[3] J. Quan and G. Bai, "*A new method to reduce the side-channel leakage caused by unbalanced capacitances of differential interconnections in dual-rail logic styles*", 2009 Sixth International Conference on Information Technology: New Generations, DOI 10.1109/ITNG.2009.185, pp. 58-63

[4] V. Litovski: "*Projektovanje elektronskih kola*", DGIP Nova Jugoslavija, Vranje, 2000.

[5] V. Litovski: *Osnovi testiranja elektronskih kola*, Elektronski fakultet, Niš, 2009, ISBN 978-86-85195-71-6

[6] D. Milovanović, V. Litovski: *Fault Models of CMOS Circuits*, Microelectronics and Reliability, Vol.34, No5, May, 1994, 883-896

[7] M. Sokolović, D. Stevanović, P. Petković: *Projektovanje za IDDQ testiranje u SoC*, Zbornik radova LII konferencije ETRAN, Palić, 08.06-12.06., 2008, EL2.3-1-4, ISBN 978-86-80509-63-1

[8] D. Milovanović, V. Litovski,: *Fault Models of CMOS Circuits*, Microelectronics and Reliability, Vol.34, No5, May, 1994, 883-896

Abstract – The dynamic NOR circuit (Dnor) that represent the basis cell of NSDDL (No Short-circuit current Dynamic Differential Logic) cryptographic method will be presented in this paper. Since Dnor is the major part of NSDDL control logic, reliability of this circuit will be tested. For this reason defects like breakage and short circuits will be inserted in to the Dnor cell in order to analyse its logical behavior.

IMULATION OF DEFECTS IN BASIC CIRCUIT FOR NSDDL METHOD CONTROL LOGIC

Milena Stanojlović, Dragiša Milovanović