D flip-flop ćelija otporna na bočne napade analizom struje napajanja

Milena Stanojlović

Apstrakt—**Sadržaj kriptovanih informacija u digitalnim elektronskim sistemima štiti se uvođenjem specifičnih algoritama koji treba da otežaju otkrivanje šifre. Zaštita se uglavnom fokusira na definisanje kompleksnog ključa čije otkrivanje zahteva ispitivanje dovoljno velikog broja kombinacija. Što je vreme za iscrpljivanje svih kombinacija duže, zaštita je bolja. Međutim, otkrivanje ključa može značajno da se olakša ukoliko se sem logičkog stanja sistema prate i ostale njegove karakteristike. Najčešće se u tu svrhu koristi analiza potrošnje, odnosno struje napajanja. Neovlašćeno prikupljanje takvih informacija o radu kripto-sistema naziva se "bočni napad" (Side Channel Attack - SCA). U ovom radu opisane su karakteristike D flip-flop ćelije realizovane u CMOS tehnici koja pokazuje izuzetnu otpornost na bočne napade, tako što maskira informaciju o korelaciji između struje napajanja i stanja u kolu. Radi se o primeni NSDDL metoda (No Short-circuit current Dynamic Differential Logic). Karakteristike ove ćelije upoređene su pri različitim uslovima rada sa standardnom D flip-flop ćelijom kako bi se procenila njena imunost na bočni napad analizom struje napajanja. Predviđa se da ova ćelija bude deo kripto sistema ugrađenog u električno brojilo kako bi se zaštitili podataci o registrovanju potrošnje električne energije.**

Ključne reči—**SCA; DPA; CMOS; kriptografija; potrošnja.**

I. UVOD

Sa pojavom velikog interesovanja za analizu struje napajanja došlo je do razvoja velikog broja hardverskih metoda za zaštitu uređaja od SCA (Side Channel Attacks), odnosno bočnih napada [1]. Posmatranjem dinamike potrošnje elektronskog kriptosistema može se doći do dodatnih informacija o radu sistema čime se olakšava otkrivanje željenih informacija. Kao najatraktivniji metod za analizu struje napajanja pokazao se DPA (Differential Power Analysis). Takođe često korišćeni metodi napada na kriptosistem su SPA (Simple Power Analysis), EMA (Electromagnetic Analysis) kao i vremenska analiza [2]. SCA napadi se sa pravom mogu okarakterisati kao veoma moćno sredstvo koje napadačima pomaže u potrazi za tajnim ključem. Korelacija između ulaznih podataka i informacija dobijenih pomoću pomenutih analiza, može dovesti do otkrivanja tajnog ključa. Dodatne informacije o ponašanju elektronskog kriptosistema mogu značajno da smanje broj kombinacija neophodnih za otkrivanje šifre.

Osnovni način zaštite od DPA sastoji se u razbijanju korelacije između aktivnosti kola i potrošnje. U tu svrhu koriste se dve tehnike. Jedna je zasnovana na maskiranju odstupanja potrošnje od pobude tako što se unose lažne informacije (često uz korišćenje generatora pseudoslučajnih brojeva). Druga se svodi na prikrivanje informacije o srednjoj vrednosti potrošnje tako što je potrošnja nezavisna od aktivnosti kola. Svi metodi svode se na povećanje hardvera uvođenjem simetričnih diferencijalnih struktura uz dodatak kontrolne logike. Ove strukture imaju udvostručen broj ulaza i izlaza u odnosu na standardna rešenja. Suština zaštite svodi se na pobudu komplementarnim signalima: pravim i lažnim. Njihov je zadatak da na izlazima (pravom i lažnom) uvek izazovu komplementarnu promenu, i to tako da ne postoji neutralni događaj. Dakle, svaka ulazna sekvenca izaziva promenu na izlazu što prouzrokuje promenu struje napajanja. Povećan je hardver, povećana je potrošnja, ali je sakrivena informacija o zavisnosti potrošnje od promene stanja signala u sistemu.

Ovaj rad prikazuje iskustva koja su stečena u LEDA laboratoriji Elektronskog fakulteta Univerziteta u Nišu na fizičkom nivou implementacije zaštite prenosa podataka od SCA. U narednom poglavlju biće opisan NSDDL (No Short-circuit current Dynamic Differential Logic) metod [3] korišćen u odbrani od SCA. Takođe biće objašnjena primena NSDDL metoda kako kod kombinacionih tako i kod sekvencijalnih ćelija. Kao primer kombinacione ćelije biće razmatrana invertorsko/baferska ćelija. Treće poglavlje bavi se problematikom projektovanja sekvencijalne D flip flop ćelije. U ovom poglavlju staviće se akcenat na važnost zaštite podataka po cenu povećanja hardverske strukture.

Otpornost projektovanih ćelija meri se stepenom maskiranja uticaja sadržaja ulaznih reči na promenu struje napajanja u kripto-sistemu. Rezultati simulacije dobijeni su korišćenjem ELDO simulatora u Mentor Graphics alatu za projektovanje integrisanih kola. Izabrana tehnologija za projektovanje je TSMC035.

II. NSDDL METOD

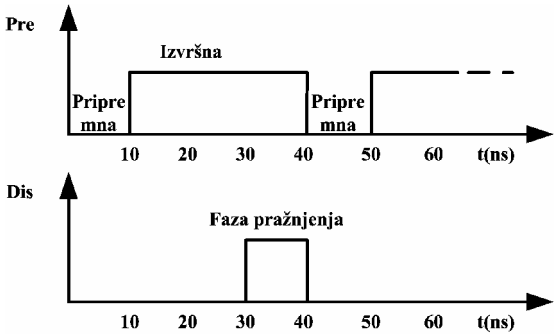
NSDDL (No Short-circuit current Dynamic Differential Logic) metod zasnovan je na logici koja se izvršava u tri različite faze: pripremnoj (Precharge), izvršnoj (Evaluation) i fazi pražnjenja (Discharge). Preteča NSDDL metoda je TDPL (Three-Phase Dual-Rail Pre-Charge Logic) [4] metod kod koga je uvođenjem treće faze postignuto da se u toku njenoog trajanja svi kondenzatori u kolu prazne. Na sličnom pricipu zasniva se i NSDDL metod kod koga je pražnjenje kondezatora postignuto primenom dinamičkog NOR (Dnor) kola. Ovim kolom ostvarena je minimizacija struje kratkog

Milena Stanojlović - LEDA laboratorija, Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, kao i Inovacioni centar naprednih tehnologija, Dragise Cvetkovica 28a, 18000 Niš, Srbija (e-mail: milena@venus.efak.ni.ac.rs)

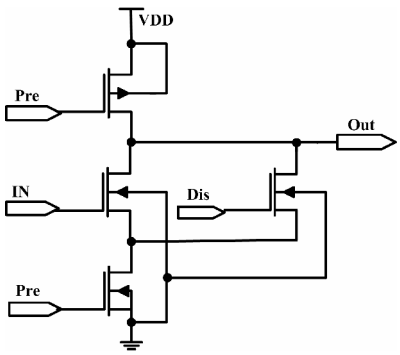
spoja u CMOS kolu. Dnor kolo je sastavni deo kako kontrolne logike tako i samih ćelija. Dakle, pored pripremne i izvršne faze uvedena je i faza pražnjenja kondenzatora (dis-charge). Prednost ovog metoda u odnosu na WDDL (Wave Dynamic Differential Logic) [5] ogleda se u imunosti na neuparenost opterećenja na pravom i lažnom izlazu. Kada je reč o ćelijama projektovanim TDPL metodom filozofija je u potpunosti drugačija u odnosu na NSDDL metod. NSDDL metod zasnovan je na primeni standardnih logičkih ćelija u kombinaciji sa Dnor ćelijom dok TDPL metod zahteva potpuno projektovanje svake ćelije.

A. Kombinaciona logika

Kada je reč o kombinacionoj logici treba reći da stanja izlaza u izvršnoj fazi zavise isključivo od stanja koja su na ulazima kriptovane ćelije. U pripremnoj fazi svi izlazni signali nalaze se u stanju logičke jedinice dok se u fazi pražnjenja svi signali nalaze u stanju logičke nule. Ovakav način rada obezbeđuje već pomenuto Dnor kolo. Kontrolni signali koji upravljaju radom Dnor kola prikazani su na slici 1 dok je samo kolo prikazano na slici 2.

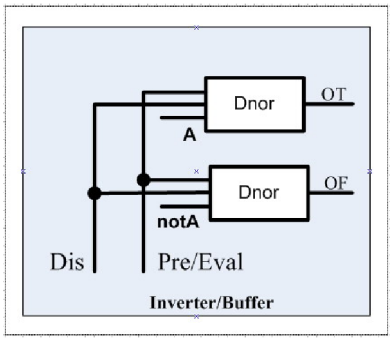


Sl. 1. Vremenski dijagram kontrolnih signala Dnor ćelije



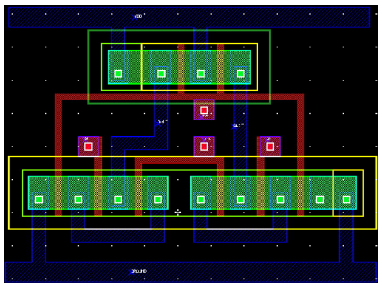
Sl. 2 Prikaz šeme Dnor ćelije

U većini slučajeva kada se projektuju kriptovane ćelije komplementarna svojstva pravih i lažnih izlaza ne ostvaruju se samo komplementarnim ulaznim signalima nego i komplementarnim strukturama. Strukture se spajaju prema *De Morgan*-ovim pravilima pa sledeće strukture I, ILI, NI, NILI, XOR i XNOR su uparene sa svojim komplementarnim strukturama [6]. Ovo nije slučaj kada se govori o invertoru ili multiplekseru gde su strukture iste, samo su ulazni signali komplementarni [7]. Kao primer primene identičnih struktura za pravi i lažni izlaz predstavićemo invertorsko/bafersku (INV/BUFF) ćeliju čija je blok šema prikazana na slici 3. Na ulaze se dovode komplementarni signali A i notA. Na izlazu ćelije generišu se dva izlazna signala označena sa OT (Output True) i OF (Output False). Signal OT predstavlja pravi izlaz (invertovani A signal), dok OF predstavlja lažni izlaz. U slučaju da se radi o baferskoj ćeliji izlazi OT i OF menjaju značenje.



Sl. 3. Blok šema INV/BUFF NSDDL ćelije otporne na bočne napade

Tokom izvršne faze pravi izlaz invertorske ćelije ima vrednost komplementa ulaznog signala, a lažni se poklapa sa stanjem ulaznog. Ukoliko se radi o baferu, ukrštaju se signali OT i OF. Ovo praktično znači da se funkcija invertovanja u NSDDL logici svodi na ukrštanje pravih i lažnih signala. Izgled lejauta INV/BUFF kola prikazan je na Slici 4.



Sl. 4. Lejaut INV/BUFF ćelije otporne na bočne napade

Da bi se procenila imunost NSDDL ćelije na DPA napad upoređene su promene energije pri promenama ulaznih signala klasične invertorske (INV) ćelije sa NSDDL INV/BUFF ćelijom. Rezultati su sistematizovani u Tabeli I. Dinamička potrošnja energije iskazana je kroz integral struje napajanja tokom jednog ciklusa promene ulaznih signala shodno jednačini (1).

$$E = V_{DD} \int_0^T i_{DD}(t) \cdot dt. \qquad (1)$$

Kada se posmatra klasična INV ćelija obuhvaćen je isti vremenski interval, T, koji je potreban NSDDL ćeliji da obavi sve tri faze rada.

Kao mera otpornosti digitalne ćelije na bočne napade posmatra se relativna srednja razlika potrošnje energije, odnosno vrednost standardne devijacije i standardne devijacije normalizovane sa prosečnom potrošnjom energije. S obzirom da se u slučaju INV/BUFF ćelije radi samo o dve moguće

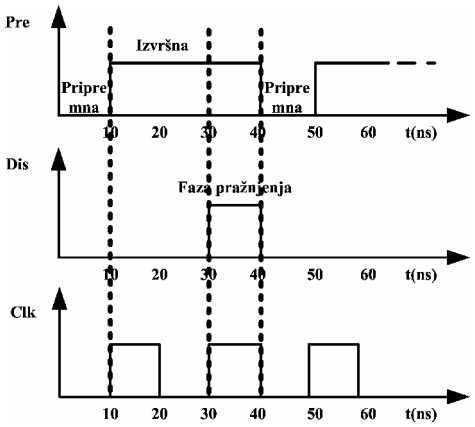
promene stanja ulaznog signala, nepotrebno je statistički obrađivati dva podatka. Zato ćemo posmatrati samo relativnu srednju razliku energije, koja je označena sa δE u Tabeli 1. Očigledno je značajno povećana uniformnost potrošnje koja ovu ćeliju kvalifikuje kao otpornu na bočne napade DPA tipa. Sa stanovišta parametra δE otpornost je povećana 98,9 puta.

TABELA I

	E_{CLASIC}[J]	E_{NSDDL}[J]
E_{max}[J]	-2.217E-13	-1.328E-12
E_{min}[J]	-2.482E-13	-1.329E-12
E_{av}[J]	-2.349-13	-1.329E-12
δE	11.275	0.114

B. Sekvencijalna logika

Za razliku od kombinacionih kola, stanja izlaznih signala sekvencijalnih kola u izvršnoj fazi zavise još i od signala takta. Veoma je bitno odrediti kada će se on pojaviti u odnosu na signale Pre i Dis. Na slici 5 prikazan je međusobni odnos ovih signala prema preporuci autora ovog metoda [3].

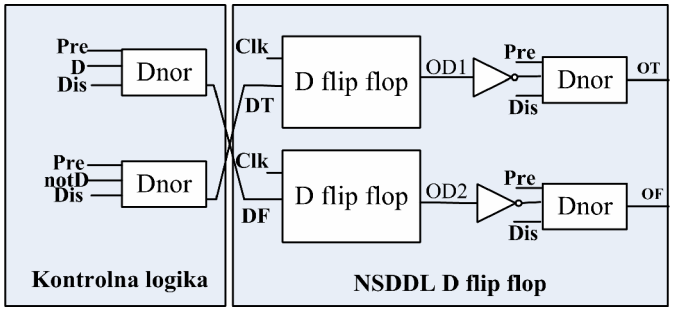


Sl. 5. Preporučeni vremenski dijagram signala takta u odnosu na signale Pre i Dis

Kod sekvencijalnih kola bitno je da se informacija upiše u memorijsi element pre početka izvršne faze kako bi se prava informacija prenela na izlaz tokom izvršne faze. Ovoj problematici, na primeru projektovanja D fip flopa, biće posvećen naredni odeljak.

III. PROJEKTOVANJE D FLIP FLOPA

Standardna procedura projektovanja NSDDL ćelije zahteva dupliranje hardvera i primenu Dnor ćelija. Slika 6 prikazuje blok dijagram D flip flop ćelije. Ako se primeni ova struktura rastuća ivica klok signala mora se javiti samo u toku izvršne faze. To znači da signal takta mora imati duplo duže trajanje nego što je preporučeno dijagramom sa slike 5 za ovaj metod kriptovanja. NSDDL metod zahteva kontrolu kako ulaznih tako i izlaznih signala korišćenjem Dnor ćelija. Prava vrednost ovih signala javlja se za vreme trajanja izvršne faze. U tom periodu potrbna je rastuća ivica klok signala kako bi se prava vrednost ulaznog signala upisala u memorijski element. Do problema dolazi kada ulazni signal menja svoju vrednost u odnosu na njegovu vrednost u prethodnoj izvršnoj fazi. Problem vremenske usklađenosti signala ilustruje slika 7. gde se jasno vidi promena vrednosti izlaznog signala u izvršnoj fazi. Isprekidanim linijama, u signalima OT i OF, docrtano je do kada bi signal trebalo da drži vrednost uzetu sa početka izvršne faze označene sa IZVR na datoj slici. Dakle, ovde trpi izlazni signal koji menja svoju vrednost u periodu kada bi trebalo da bude konstantan. Do ovoga dolazi zbog promena signala OD1 u pomenutom periodu. Ova odstupanja od pravila koja nalaže NSDDL metod odražavaju se na struju napajanja koja je napadačima glavni izvor informacija. Sa druge strane upis prave informacije u memorijski element moguć je jedino tokom izvršne faze pa se, shodno tome, rastuća ivica takta javlja u ovom periodu. Ova dva uslova: da se ulazni signal mora upisati u memorijski element u toku izvršne faze i to da taj isti signal prosleđen na izlaz mora imati konstantnu vrednost tokom cele izvršne faze jednostavno nisu ostvariva.

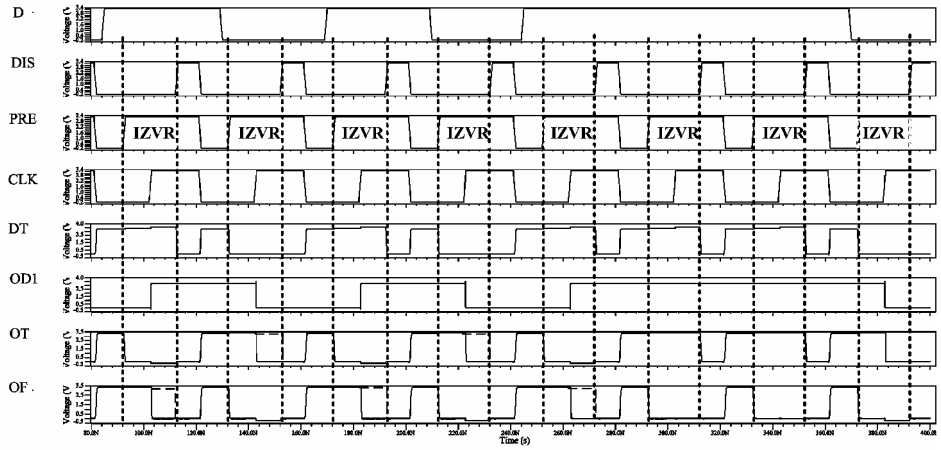


Sl. 6. Blok šema D flip flop NSDDL ćelije

Ovim smo pokazali da struktura sa slike 6 nije prihvatljiva, pa je neophodno novo rešenje. Posmatranjem dinamičke potrošnje energije iskazane kroz integral struje napajanja pokazuje se ranjivost ove ćelije. Integral je posmatran tokom obe ivice taktnog signala kada ulazni signal miruje što obuhvata jedan operacioni ciklus. Otpornost na DPA kvantifikuje se preko maksimalnog relativnog odstupanja energije od srednje vrednosti, odnosno vrednost standardne devijacije i standardne devijacije normalizovane sa prosečnom potrošnjom energije (veličine označene sa δE, σ i NSD u Tabeli II). Može se videti da je NSD parametar za kriptovanu ćeliju oko pet puta manje u odnosu na nezaštićenu ćeliju. Ako se uzme u obzir da naše iskustvo pakazuje da gornja granica ovog parametra ne bi trebalo da bude veća od 1.5% onda se može reći da je ova ćelija ranjiva i nedovoljno pouzdana.

TABELA II

	$E_{CLASICDFF}$[J]	$E_{NSDDLDFF}$[J]
E_{max}[J]	-7.86E-13	-3.79E-12
E_{min}[J]	-1.78E-12	-4.39E-12
E_{av}[J]	-1.17E-12	-4.14E-12
δE	-55.78	-13.73
σ	4.01E-13	2.85E-13
NSD	-34.32	-6.96



Sl. 7. Vremenski dijagrami probne verzije D flip flop NSDDL ćelije

Rešenje koje se nameće kao jedino moguće je da se svaki D fip flop realizuje kao *master slave* struktura na koju mogu da se primene kontrolni signali prikazani na slici 5. Ovo je neophodno kako bi se na prednju ivicu takta u *master* sekciju upisala prava vrednost ulaznog signala u toku trajanja izvršne faze, a na opadajuću ivicu ta vrednost prenela u *slave*. Ovim se stvaraju željeni uslovi da se u pripremnoj fazi dešavaju promene ulaznog signala. Shodno tome u izvršnoj fazi ulazni signal ima konstantnu vrednost tokom celog njenog trajanja. Nevezano za ovu problematiku *master slave* D flip flop ćelija isprojektovana ranije zbog ranijih potreba primene [8]. Rezultati za kriptovanu NSDDL Master Slave D flip flop ćeliju su daleko bolji tako da NSD iznosi minimalnih 0.149%.

IV. ZAKLJUČAK

U ovom radu razmatrano je projektovanje NSDDL D flip flop sekvencijalne ćelije otporne na bočne napade. Dobijeni rezultati pokazali su da ćelija projektovana standardnim NSDDL postupkom ne garantuje dovoljnu bezbednost od bočnih napada DPA tipa. To pokazuje normalizovana vrednost standardne devijacije, NSD, parametar koji je usvojen kao kriterijum za odluku da li je ćelija dovoljno pouzdana ili ne. Da bi se ćelija smatrala pouzdanom sa stanovišta SCA, NSD parametar ne bi trebalo da ima veću vrednost od 1.5%. Zato je zaključeno da se umesto klasičnog D flip flopa koristi Master Slave struktura. Kod ove strukture NSD parametar iznosi 0.147%. Naredni cilj je da se redizajnira MS struktura u cilju smanjenja hardvera.

ZAHVALNICA

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

LITERATURA

[1] V. Lomné, A. Dehaboui, P. Maurine, L. Torres, M. Robert, "Side Channel Attack"', in B. Badrignans, J. L. Danger, V. Fischer, G. Gogniat, L. Torres, "Security Trends for FPGA", Springer Netherlands, pp. 47-72, 2011

[2] J. J.Quisquater, "Side channel attacks", State-of-the-Art, Rep, October 2002.

[3] J. Quan and G. Bai, "A new method to reduce the side-channel leakage caused by unbalanced capacitances of differential interconnections in dualrail logic styles", Sixth Int. Conf. on Information Technology: New Generations, pp. 58-63, 2009

[4] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti,"Three- Phase Dual-Rail Pre-Charge Logic". In: Goubin, L., Matsui, M. (eds.) CHES 2006.LNCS, vol. 4249, pp. 232–241. Springer, Heidelberg (2006).

[5] K. Tiri and I. Verbauwhede, "Place and Route for Secure Standard Cell Design", CARDIS'04, pp. 143-158, 2004.

[6] M. Stanojlović andP. Petković,"Resistance of XOR/XNOR NSDDL Cell to Side Channel Attack", Proc. of Small System Simulation Symposium, Niš, Serbia, pp. 141-144 Febryary, 2012..

[7] M. Stanojlović and P. Petković,"Design and Simulation of Multiplexer Cell Resistant to Side Channel Attacks", IX Simposium on Industrial Electronics INDEL, Banja Luka, B&H, pp. 50-54, November, 2012.

[8] P. Petković, and M. Stanojlović: Hardverska zaštita od napada na kripto-sistem zasnovana na primeni ćelija koje maskiraju informaciju o potrošnji, Zbornik LV konferencije ETRAN, Banja Vrućica, BiH, 06.06.-09.06., 2011, EL 3.5,

ABSTRACT

Content of an encrypted data in digital systems is protected by utilizing specific algorithms which should harden decrypting. Protection is usually based on complex keys which require hacker to examine large number of combinations in order to break the key. Longer the time to try each bit combination provides better protraction. However, time for key breaking may be significantly reduced if, besides logical states, other characteristics of the signal are observed. Commonly, analysis of power consumption i.e. power supply current time profile are used for this purpose. Unauthorized collecting of such information about crypto system behavior is called Side Channel Attack (SCA). This paper presents custom designed D flip-flop (DFF) CMOS standard cell which provides remarkably good SCA resistance. This is achieved by masking the correlation between power supply current and logic states of the circuit. No Short-circuit current Dynamic Differential Logic (NSDDL) method is implemented. Characteristics of the cell are compared with standard, not encrypted, DFF cell under various operational conditions in order to prove SCA resistance. Designed encrypted cell will be the part of more complex crypto system for power consumption metering and it should increase overall system's data security.

D flip-flop cell resistant to power supply current side channel attacks

Milena Stanojlović