PROJEKTOVANJE WDDL ĆELIJA OTPORNIH NA BOČNE NAPADE

Milena J. Stanojlović, Elektronski fakultet, Univerzitet Niš, milenastanojlovic@yahoo.com
Predrag M. Petković, Elektronski fakultet, Univerzitet Niš, predrag.petkovic@elfak.ni.ac.rs

Sadržaj – *U ovom radu razmatrani su kriptografski algoritmi, primenjeni u hardveru, koji štite curenje informacija iz uređaja, takozvanih bočnih kanala. Važne informacije, kao što su tajni ključevi, mogu se otkriti posmatranjem potrošnje, merenjem elektromagnetnog zračenja, analizom talasnih oblika itd. Ove vrste napada nazivaju se bočnim napadima (side-channel attacks (SCA)). Postoji nekoliko tehnika napada pomoću kojih se na osnovu analize potrošnje mogu otkriti željene informacije. Jedna od njih je DPA (Differential power analysis) tehnika na osnovu koje je izvedena kontramera u cilju zaštite informacija. Za odbranu od ovakvih napada korišćena je WDDL (Wave Dynamic Differential Logic) tehnika kao odličan predstavnik klase DPL (Dual-rail with Pre-charge Logic) kola.*

1. UVOD

Zaštita podataka predstavlja danas izuzetno važan problem čije rešavanje je izazvalo veliko interesovanje kako u svetu nauke tako i u svakodnevnom životu. Finansijske transakcije, e-trgovina, e-pošta, e-bankarstvo i drugi oblici razmene poverljivih podataka koji se odvijaju preko mobilne telefonske mreže ili interneta imaju za posledicu porast broja osetljivih transakcija bez fizičkog prisustva. Takav način poslovanja i razmene podataka otvorio je apetite za zloupotrebom poverljivih podataka koji se prenose kroz javne mreže. Zaštita podataka zasnovana je prevashodno na algoritamskim rešenjima. Prva linija odbrane koristi složene višebitne šifre. Razbijanje ovakvih šifara, jednostavnim softverskim alatima, postaje otežano i zahteva mnogo vremena. Duže lozinke i sofisticirani algoritmi kodiranja kao rezultat daju veći broj kombinacija, pa samim tim i bolju zaštitu. Moglo bi se reći da se problem zaštite može rešiti upravo povećanjem broja kombinacija. Međutim, vrednost skrivenih podataka se enormno povećava. Ovo inspiriše potencijalne napadače da ulažu dosta novca i pameti kako bi došli do željenih informacija [1]. Primarni način predstavlja čitanje osnovnih digitalnih podataka koji se razmenjuju u mreži. Sekundari način predstavlja prikupljanje ostalih tipova informacija o radu harvera, koje se mogu klasifikovati kao *sporedni podaci*. Pokazalo se naime, da analiza potrošnje kriptografskog hardvera može pomoći u razotkrivanju šifre. Neki od metoda koji omogućavaju lakše razbijanje šifara poznati su kao SPA (*Simple Power Analysis*), DPA (*Differential Power Analysis*) i EMA (*Electromagnetic Analysis*) [2]. Zajedničko za sve ove metode je analiza sporednih informacija koje "cure" iz fizički implementiranog hardvera. Prikupljanje tih informacija nikako ne može da se desi slučajno zato zahteva korišćenje posebne opreme. Očigledno mora da postoji jasna *namera* da se do takvih podataka dođe. Zato se ovakve aktivnosti nazivaju *napadom*, a s obzirom da se radi o napadu na sporedne izvore informacija, oni se karakterišu kao *bočni napadi*. U daljem tekstu oni će se označavati skraćenicom *SCA* koja potiče od engleskog termina *Side Channel Attack*. Postoje različite taktike *napada* odnosno načina za prikupljanja sporednih podataka. Među njima se prepoznaju napad indukovanjem greške, napad preko praćenja vremena događaja ili napada pomoću sonde [2].

Cilj ovog rada je da prouči neke od strategija u borbi protiv bočnih napada zasnovanih na adaptaciji hardvera. Autori su posebno zainterosovani za primenu u zaštiti podataka u sistemu za upravljanje prenosom i naplatom električne energije [3]. Osnovni predmet istraživanja predstavlja razvoj ASIC kola koje sprečava curenje podataka zasnovano na analizi promene struje napajanja. Planira se projektovanje biblioteke standardnih logičkih ćelija otpornih na bočne napade. Projektovanje ovakvih ćelija predmet je istraživanja u LEDA laboratoriji na Elektronskom fakultetu u Nišu. Upravo iz tih razloga, posmatrano sa implementacione tačke gledišta, a u sferi naših interesovanja biće razmatrana arhitektura poznata kao WDDL (Wave Dynamic Differential Logic) [4]. Razmatraće se uticaj nesimetričnog opterećenja i promene napona napajanja na otpornost kola na DPA napade.

Zato će u narednom poglavlju biti opisane poznate strategije odbrane od SCA. Posebna pažnja biće posvećena opisu WDDL kola u trećem poglavlju. Četvrto i peto poglavlje daju prikaz rezultata simulacije kojima se sagledava uticaj nesimetričnog opterećenja i promene napona napajanja WDDL AND ćelije na ranjivost prema SCA.

2. STRATEGIJE ODBRANE OD SCA

Tehnike napda kao što su EMA i analize potrošnje zahtevaju korišćenje različitih tipova sondi. U ovim slučajevima izvor dobijanja informacija je struja curenja CMOS kola (I_{DD}). Curenje predstavlja promenu u struji napajanja I_{DD} ulsed svake uzastopne promene stanja u CMOS kolu. Svaka promena sa 0 na 1 predstavlja process prenosa određene količine naelektrisanja od V_{DD} na izlaznu kapacitivnost. Takođe svakom promenom stanja sa 1 na 0 ova izlazna kapacitivnost se prazni prema masi. Iznos naelektrsajna koje se pri ovim prmenama stanja prenese direktno je srazmeran broju kapacitivnosti koje treba napuniti i isprazniti. Za nekoga ko ima elementarno znanje o digitalnim kolima prethodno navedena činjenica je od izuzetne važnosti. Naime, praćenje digitalnih signala na ulazu u kolo uz monitoring struje napjanja I_{DD} postaje moćan alat za otkrivanje ponašanja posmatranog digitalnog kola ili sistema. Cilj je da se uspostavi korelacija između ponašanja kola i promene struje napajanja, odnosno snage. U tom slučaju može se identifikovati uneta šifra koju kolo *prepoznaje* kao očekivani ključ.

Mere zaštite se mogu razvrstati u zavisnosti od nivoa na kome se izvode i to kao mere na arhitekturskom, algoritamskom ili na nivou gejtova. Mogu se realizovati pomoću tri metodologije i to: *zavaravanje, maskiranje* i *zaslepljivanje*.

Zavaravanje se primenjuje na algoritamskom nivou kao često menjanje tajnog ključa kako bi se izbegla mogućnost pronalaženje korelacije.

Maskiranje podrazumeva dodatne logičke operacije kako bi se pokrio protok pravih podataka. Moguće ih je izvoditi na algoritamskom i nivou gejtova. Međutim, ova tehnika se može "razbiti" većim brojem analiza potrošnje kola.

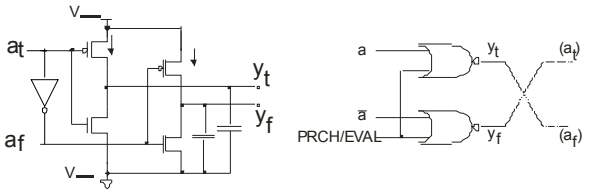
Zaslepljivanjem se postiže nezavisnost protoka podataka od potrošnje kola. U osnovi postoje dva načina da se ovo postigne:

- Zadržavanjem konstantne potrošnje kola u vremenu, što zahteva ubacivanje posebnih analognih modula; time je potrošnja značajno uvećana u odnosu na standardni pristup.
- Forsiranjem ćelije da u svakom logučkom prelazu ima isti talasni oblik snage potrošnje kola.

Druga klasa metoda poznata je kao DPL (*Dual-rail with Pre-charge Logic*) [5]. Kod ove tehnike svi signali se udvostručavaju tako što se pored ispravnog (*true*) generiše i lažni (*false*) signal. Pored toga, ćeluija radi u dva režima: pripremnom (*pre-charge*) i izvršnom (*evealuation*). Režim rada određen je specifičnim taktnim signalom. Tokom pripremne faze oba izlaza dovode se na stanje logičke nule. Tokom izvršne faze uvek samo jedan od izlaza menja stanje. WDDL ćelija je dobar primer korišćenja DPL tehike [4]. Ona može da se realizovati standardnim CMOS procesom. Njihovom opisu posvećen je naredni odeljak.

3. WDDL

WDDL ćelije projektuju se sa ciljem da izbrišu korelaciju između potrošnje kola i protoka podatka. Da bi radile na principu DPL logike, potrebno je da pri svakoj kombinaciji ulaznih signala obezbede promenu stanja ili na pravom ili lažnom izlazu tokom izvršne faze.U slučaju invertora to znači da svaka promena na izlazu mora da ima isti uticaj na I_{DD}. Ovo je moguće ukoliko je invertor realizovan sa dva standardna invertora napajanih iz istog V_{DD} izvora. Taj slučaj je pirkazan na Sl. 1.a.

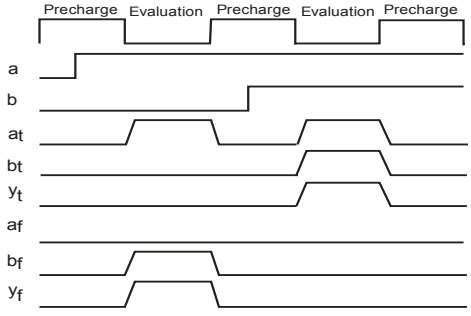


a) b)

Sl.1. *WDDL invertor a) generička šema, b)praktična realizacija*

Indeksi t i f na slici 1.a odnose se na prave (*true*) i lažne (*false*) signale respektivno. Znajući da je $\boldsymbol{a_f}$=NOT($\boldsymbol{a_t}$) može se zaključiti da će svaka promena na $\boldsymbol{a}$=$\boldsymbol{a_t}$ za isto opterećenje na izlazima $\boldsymbol{y_t}$ i $\boldsymbol{y_f}$, uzrokovati istu promenu I_{DD}.

Međutim, za ostale tipove logičikh ćelija nije dovoljno jednostavno udvosturčiti hardver. Svaka ćelija mora imati svoju dualnu ili komplementarnu ćeliju. Ovo znači da za svaki pravi izlaz za koji važi da je $\boldsymbol{y_t}$=$\boldsymbol{a_t}$ ¤ $\boldsymbol{b_t}$, treba obezbediti njegov komplementarni lažni izlaz $\boldsymbol{y_f}$=NOT($\boldsymbol{y_t}$)=NOT($\boldsymbol{a_t}$) * NOT($\boldsymbol{b_t}$). Pri tome simboli ¤ i * označavaju osnovnu i dualnu logičku operaciju.



Sl.2. Talasni oblici *WDDL* AND ćelije

Tokom trajanja pripremne faze svi signali su postavljeni na nizak logički nivo, dok se za vreme trajanja izvršne faze izlazi postavljaju na odgovarajuće logičke nivoe. Zbog ovakve logike ćelija invertora nije realizovana kao na slici 1.a već kao na Sl. 1.b . Istovetna arhitektura se koristi za generisanje talasnih oblika pravih i lažnih signala koji pobuđuju svaku WDDL ćeliju ($\boldsymbol{a_t}$ i $\boldsymbol{a_f}$ dobijaju se od signala $\boldsymbol{a}$; $\boldsymbol{b_t}$ i $\boldsymbol{b_f}$ od signala $\boldsymbol{b}$).

Na slici 2 prikazani su talasni oblici sledećih signala u redosledu odozgo nadole: „pre-charge/evaluation“signal, ulazni signali a i b, na osnovu njih generisani ulazni signali a_t i b_t, signal na pravom izlazu y_t, signali generisani na lažnim ulazima a_f i b_f i signal na lažnom izlazu y_f. Izlazni signali odgovaraju WDDL ćeliji koja obavlja logičku AND funkciju na izlazu y_t.

U slučaju da ulazni signali ne dolaze u istim vremenskim trenucima WDDL arhitektura, implementirana sa NAND ćelijama, generisaće gličeve koje mogu uočiti napadači. Istovremeno to će proizvesti curenje informacije i čitava arhitektura postaće ranjiva. Zbog toga se WDDL realizuje jedino „pozitivnim“ gejtovima (AND i OR), a ne negativnim (NAND i NOR). Ukoliko bi se reailzacija izvodila „negativnom“ logikom (gejtovima) neophodno bi bilo forsiranje ulaza gejtova ka V_{DD} umesto ka masi za vreme pripremne faze. U tom slučaju uvodi se modifikacija koja omogućava ovakv način rada i poznata je kao DSDRL (*Dual Spacer Dual Rail Logic*) [6].

Treba napomenuti da je WDDL pristup pouzdan samo ukoliko su opterećenja u slučaju pravih i lažnih izalza uravnotežena. U suprotnom, javlja se disbalans promene struje I_{DD} usled razlika u vremenskom odzivu lažnog i pravog izlaza koji ugrožava sam WDDL koncept [7].

Glavna prednost WDDL koncepta u odnosu na druge predstavlja jednostavna realizacija na bazi standaranih ćelija. Prema tome dovljno je koristiti standardne alate za rutiranje. Nažalost ovakvi alati nisu optimizovani u smislu simetriranja veza. Tako da se nameće problem rutiranja simetričnih veza postojećim algoritmima za povezivanje koji današnji alati nude. Do sada je razvijeno nekoliko algoritama za simetrično rutiranje [7].

U narednom poglavlju biće prezentovan uticaj neuparenog opterećenja na mogućnost bočnog napada preko struje napajanja.

4. OTPORNOST WDDL ĆELIJE NA SCA PRI NEUPARENOM OPTEREĆENJU

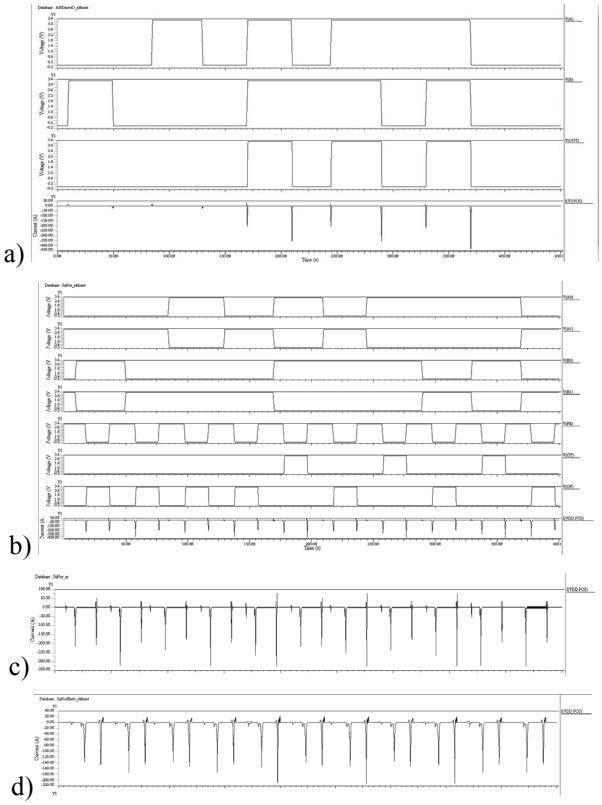
Otpornost WDDL ćelija na bočne napade preko struje napajanja ispitaćemo na primeru jedne AND ćelije implementirane WDDL tehnikom (WDDL AND). Ćelija je projektovana u TSMC CMOS035 tehnologiji. Cilj je da se uporede promene struje napajanja pri simetričnom i više nesimetričnih kapacitivnih opterećenja Na osnovu dobijenih rezultata treba utvrditi granicu dopuštene asimetrije.

Da bi se ilustrovale prednosti WDDL AND u odnosu na standardnu AND ćeliju (SR AND), najpre će se pri istim uslovima simulirati ponašanje standardne AND ćelije projektovane u istoj tehnologiji.

Sl. 3a prikazuje talasne oblike napona na ulazima a i b, kao i napona na izlazu SR AND ćelije. Dijagram na dnu slike 1.a prikazuje talasni oblik struje napajanja. Očigledno je da postoji korelacija između stuje napajanja i pobudnih napona. Najveća I_{DD} postoji pri promeni oba ulazna signala sa 1 na 0.

Na Sl. 3b prikazani su vremeski dijagrami karakterističnih

signala za WDDL AND ćeliju. Odozgo nadole prikazani su talasni oblici signala a, NOTa, b, NOTb, takta precharge/enable, y_t, y_f i struje napajanja. Oba izlaza vezana su za kapacitivno opterećenje istih vrednosti.



Sl.3 *Vremenski dijagrami za: a) SR AND ćeliju, b)WDDL AND ćeliju sa uparenim opterećenjem, c)WDDL AND napad sa V_{DD} = 2.4V, d) WDDL AND napad sa V_{DD} = 4.2V*

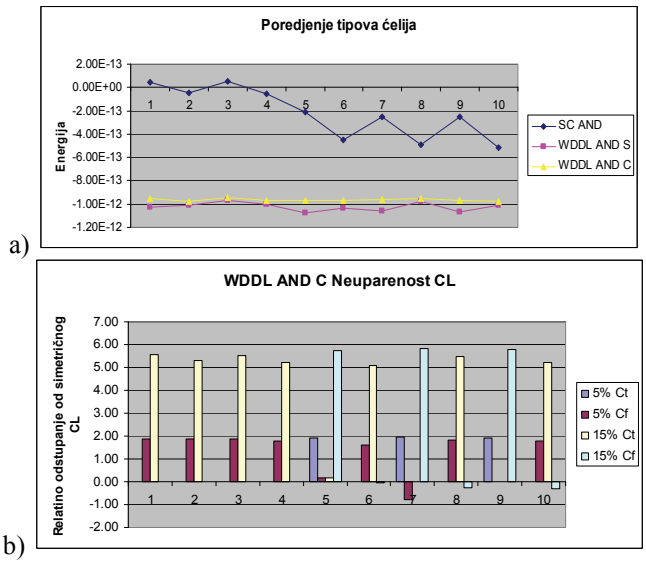
Poređenjem talasnih oblika struje I_{DD} sa Sl. 3a i 3b očigledno je da su pikovi kod WDD AND ćelije češći jer se javljaju pri svakoj ivici taktnog signala, ali da je razlika između maksimalnih vrednosti struje mnogo manja nego u slučaju SR AND ćelije. Time se izgubila informacija o korelaciji između I_{DD} i promene stanja na ulazima kola.

To je posledica promena na lažnom izazu (dijagram iznad I_{DD}) koja se javlja samo kada na pravom izlazu (treći dijagram od dna) nema promene stanja. Uočava se da lažni izlaz menja stanje i za kombinacije ulaza 0-0 i 1-1 koje za SR AND izazivaju neutralni događaj. Ukoliko se postigne da oblik I_{DD} bude identičan za svaku moguću kombinaciju ulaznih signala, može se reći da ne postoji curenje informacije o stanju izlaza ćelije. Kako je integral struje I_{DD} pogodana mera curenja informacije biće korišćen i kao mera ocene valjanosti projektovane ćelije. Praktično, dinamika snage napajanja je praćena na isti način kako bi to potencijalni SCA napadač radio analizom potrošnje kola.

U slučaju SR AND ćelije na osnovu poređenja vrednosti integrala struje napajanja pri promeni stanja na izlazu 0-1 sa onim dobijenim za promenu 1-0 uočava se značajna razlika. Ona može da se koristi za prepoznavanje promene ulaznih signala, tako da se kaže da ona predstavlja tzv. *potpis u snazi* (*power signature*).

Kod WDDL AND ćelije (Sl. 3b) vidi se da je ovaj potpis veoma *nečitak* jer ne postoji velika razlika u talasnim oblicima I_{DD} pri različitoj kombinaciji ulaznih signala. Kao mera razlike, međsobno se porede vrednosti integrala struje napajanja za sve kombinacije ulaznih signala tokom izvršne faze. Rezultati *čitljivosti* potpisa za SC AND i dve WDDL AND ćelije upoređeni su na Sl. 4a pri deset karakterističnih promena ulaznih signala. Pri tome, jedna WDDL AND ćelija projektovana je na bazi standardnih ćelija (WDDL AND S), dok su u drugoj, dimenzije tranzistora modifikovane sa ciljem da se postigne bolja simetrija potrošnje struje (*custom designed* WDDL - WDDL AND C).

Očigledno da pri neutralnim događajima koji odgovaraju prednjoj i zadnjoj ivici signala *B* dok je signal *A* u stanju 0 i obrnuto (videti Sl. 3a i Sl.3b) ne postoji promena značajnija energije kod SC AND ćelije (prelazi označeni sa 1, 2, 3 i 4 na sl. 4a i 4b). Kombinacije ulaznih reči koje izazivaju promenu izlaznog signala dovode do veće promene energije. Pri tome, kao što je očekivano, promena izlaznog signala sa 0 na 1 zahteva veću energiju od promene sa 1 na 0.



Sl.4 *a) Poređenje apsolutnog odstupanja energije od srednje vrednosti SC AND, WDDL AND S i WDDL AND C ćelija b)Relativno odstupanje energije WDDL AND C ćelije pri neuparenom opterećenju od 5% i 15%*

Observabilnost korelacije snage i aktivnosti kola može da se iskaže parametrom *relativno maksimalno odstupanje energije* definisanim sa (1).

$$\delta = \left| \frac{E_{\max} - E_{\min}}{E_{sr}} \right| \quad , \qquad (1)$$

Gde su E_{max}, E_{min} i E_{sr} maksimalna minimalna i srednja vrednost energije za različite kombinacije ulaznih signala, respektivno.Velike vrednosti parametra δ odgovaraju većoj korelaciji između ponašanja kola i potrošnje. To znači da je *čitljivost potpisa* direktno proporcionalna oscilacijama u energiji, a ne apsolutnoj vrednosti energije. U slučaju SC AND, WDDL AND S i WDDL AND C ćelija δ iznosi 257.64%, 10.68% i 3.35% respektivno.

S obzirom na ranije izneto zapažanje da neuparenost opterećenja na parvom i lažnom izlazu smanjuje otpornost WDDL AND ćelije na SCA, od interesa je porceniti do kog iznosa neuparenost ovih opterećenja može da se toleriše. Zato je urađen set simulacija pri različitim vrednostima kapacitivnog opterećenja. Konkretno, analizirana je WDDL AND C ćelija za neuparneost kapacitvnog opterećenja od 5% i 15%. Dobijeni rezultati relativnog odstupanja energije u odnosu na slučaj sa simetričnim opterećenjem sistematizovani su u na Sl.4.b. Posebno su razmotreni slučajevi kada je uvećana kapacitivnost na pravom (C_t) i lažnom izlazu (C_f).

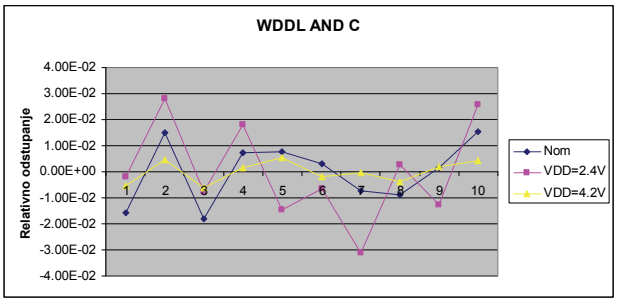
Pretpostavljajući da je dinamika čitljivosti potpisa u odnosu na idealan slučaj od 10% dovoljna za registrovanje posmatranog curenja, može se zaključiti da je prihvatljiv prag neuparenosti za ovu ćeliju do 20%.

5. OTPORNOST WDDL NA PROMENU V_{DD}

U ovom poglavlju razmatran je uticaj defekata koje može uneti potencijalni napdač kako bi smanjio otpornost na SCA WDDL ćellije. Naime, posmatranjem ponašanja kola prilikom namerno unetog defekta, napadač može pronaći validna stanja izlaza.

Jedan od parametara koji potencijalni npadač može da menja i time unese defekt u kolo, jeste napon napajanja V_{DD}. Ovakvi napadi su simulirani pri promeni napona napajanja u oba smera u odnosu na standardni napon napajanja za TSMC CMOS035 tehnologiju koji iznosi 3.3V.

Razmatrana su dva slučaja: smanjenje V_{DD} na 2,4V i povećanje na 4.2V. Dobijeni talasni oblici I_{DD} prikazani su na slikama 3.c i 3.d za V_{DD-}=2.4V i V_{DD+}=4,2V respktivno. Poređenje relativnog odstupanja energije od srednje vrednosti prikazano je na Sl. 5. Može se uočiti da se kombinacije ulaznih signala označene brojevima 5 i 7 lakše uočavaju kada se V_{DD} obori na 2.4V. Istovremeno, očigledno je da povećanje V_{DD} na 4.2V bolje sakriva korelaciju između snage i pobudnih signala. To potvrđuje i parametar δ koji u slučaju V_{DD}=2.4V iznosi 5.94% dok za V_{DD}=4.2V iznosi samo 1.13%.



Sl.5 *Poređenje relativnog odstupanja energije od srednje vrednosti za WDDL AND C ćeliju za različite vrednosti napona napajanja*

6. ZAKLJUČAK

U ovom radu prezentovane su neke od kontramera za zaštitu od SCA. Konkretno ispitana je AND ćelija čija je topologija realizovana primenom WDDL topologije. Projektovane su WDDL AND ćelije. Jedna je realizovana na bazi standardnih ćelija iz biblioteke TSMC CMOS 035mm, dok su u drugoj dimenzije tranzistora modifikovane kako bi se povećela simetričnost odziva na pravom i lažnom izlazu. Zabeležena je tri puta povećana osetljivost na SCA nego u slučaju primene standardnih bibliotečkih ćelija. Pored toga analizirana je otpornost na bočne napade sa stanovišta uparenosti opterećenja na pravom i lažnom izlazu kola. Takođe je ispitivan uticaj promene napona napajanja na osetljivost WDDL AND ćelije na SCA napade.

Ostvareni rezultati pomoćiće prilikom donošenja odluke o izboru tipa zaštite od SCA koja bi bila najprikladnija za implementaciju u integrisanom merača potrošnje električne energije ali i za sve druge primene u kojima je neophodna zaštita podataka koji se prenose preko javnih komunikacionih mreža.

ZAHVALNICA

Ovaj rad je podržan od strane Ministarstva nuke i tehnološkog razvoja republike Srbije u okviru projekta TR 11007.

LITERATURA

[1] P. Kocher and J. Jaffe and B. Jun, “Differential Power Analysis,” in Proceedings of CRYPTO’99, ser. LNCS, vol. 1666. Springer-Verlag, 1999, pp. 388–397.

[2] Jean-Jacques Quisquater, Side channel attacks State-of-the-Art, Report, Oct. 2002. Avilable on: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf [Pristupljeno 15.12.2009.].

[3] Litovski, V., Petković, P.: Why The Power Grid Needs Cryptography?, Electronics, Vol. 13, No. 1, Banja Luka, June, 2009, pp. 30-36.

[4] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” in DATE’04. IEEE Computer Society, February 2004, pp. 246–251, Paris, France.

[5] Rajesh Velegalati, Securing Light Weight Cryptographic Implementations on FPGAs Using Dual Rail with Pre-Charge Logic, PhD Thesis, George Mason University, Fairfax, VA, 2009, Available on http://digilib.gmu.edu:8080/bitstream/1920/5623/1/Velegalati_Rajesh.pdf, [Accessed on March 2010].

[6] Danil Sokolov, Julian Murphy, Alexander Bystrov, and Alex Yakovlev. Design and Analysis of Dual-Rail Circuits for Security Applications. IEEE Transactions on Computers, 54(4):449–460, 2005. ISSN 0018-9340.

[7] Sylvain GUILLEY Sumanta CHAUDHURI Laurent SAUVAGE Tarik GRABA Jean-Luc DANGER Philippe HOOGVORST Vinh-Nga VONG Maxime NASSAR Florent FLAMENT, Shall we trust WDDL? in Future of Trust in Computing, Berlin : Germany (2008), pp. 1-8, DOI : 10.1007/978-3-8348-9324-6_22.

Abstract - This contribution discusses cryptographic algorithm in hardware that protects the information leaks out of the device through so called „side channels“. Attacks on crypto-processors are based on analyses of the leaked data are known as side-channel attacks (SCA). Important information, such as secret keys, can be obtained by observing the power consumption, the electromagnetic radiation, the timing information etc. There are several types of protection and some will be discussed in this paper. Special attention is paid to Wave Dynamic Differential Logic (WDDL) that was evaluated in terms of load symmetry on an example.

DESIGNING WDDL CELLS RESISTENT TO SCA

Milena Stanojlović, Predrag Petković