HARDVERSKA ZAŠTITA OD NAPADA NA KRIPTO-SISTEM ZASNOVANA NA PRIMENI ĆELIJA KOJE MASKIRAJU INFORMACIJU O POTROŠNJI

Predrag Petković, *Elektronski fakultet, Univerzitet Niš*, predrag.petkovic@elfak.ni.ac.rs
Milena Stanojlović, *Elektronski fakultet, Univerzitet Niš*, milena@venus.elfak.ni.ac.rs

Sadržaj – *Uobičajeni način za neovlašćeno otkrivanje sadržaja kriptovanih informacija svodi se na postupke zasnovane na kombinatorici koja omogućava otkrivanje šifre. Složeni kriptografski algoritmi imaju za cilj da onemoguće/otežaju ispitivanje mogućih kombinacija u realnom vremenu. Dodatne informacije o ponašanju elektronskog kripto-sistema mogu značajno da smanje broj kombinacija neophodnih za otkrivanje šire. Prikupljanje takvih informacija predstavlja "bočni napad"(Side Channel Attack - SCA). Najčešći oblik ovih napada svodi se na analizu potrošnje elektronskog kriptosistema. Da bi se napadi ovog tipa onemogućili neophodno je u kripto-sistem uvesti dodatnu hardversku zaštitu. Metodi hardverske zaštite svode se na razbijanje korelacije između aktivnosti kola i potrošnje. Konkretno u ovom radu razmatrane su osobine sekvencijalnih digitalnih ćelija baziranih na primeni NSDDL (No Short-circuit current Dynamic Differential Logic) metoda.*

1. UVOD

Za prenos digitalnih podataka najčešće se koriste postojeće fizičke veze koje su sastavni deo javnih komunikacionih mreža. Izuzetak ne predstavlja ni prenos poverljivih podataka. Poverljive informacije štite se kriptovanjem, odnosno, korišćenjem ključeva koji su poznati samo ovlašćenim korisnicima. Značaj informacija sadržanih u kriptovanim porukama provocira neovlašćene i zainteresovane korisnike javnih komunikacionih mreža da otkriju njihov sadržaj. Svaki neovlašćeni pokušaj pristupa kriptovanim sadržajima tretira se kao napad na kriptografski sistem. Uobičajeni način za neovlašćeno otkrivanje sadržaja kriptovanih informacija svodi se na postupke zasnovane na kombinatorici koja omogućava otkrivanje šifre. Složeni kriptografski algoritmi imaju za cilj da onemoguće, odnosno, otežaju ispitivanje mogućih kombinacija u realnom vremenu. Dodatne informacije o ponašanju elektronskog kripto-sistema mogu značajno da smanje broj kombinacija neophodnih za otkrivanje šire. Prikupljanje takvih informacija predstavlja "*bočni napad*" (*Side Channel Attack* - SCA).

Posmatranjem dinamike potrošnje elektronskog kripto-sistema može se doći do dodatnih informacija o radu sistema čime se olakšava razotkrivanje šifre. Najefikasniji metodi napada na kripto-sistem jesu SPA (Simple Power Analysis), DPA (Differential Power Analysis) i EMA (Electromagnetic Analysis) [1].

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 opisani najčešće korišćeni metodi bočnog napada. Treći deo rada opisuje metode hardverske zaštite od DPA napada. Autori su posebno zainterosovani za hardversku zaštitu podataka u sistemu za upravljanje prenosom i naplatom električne energije [2, 3]. Sa tim ciljem istraživački tim LEDA laboratorije razvija biblioteku CMOS ćelija koje su *otporne* na DPA napade. Otpornost se meri stepenom maskiranja uticaja sadržaja ulaznih reči na promenu struje napajanja u kripto-sistemu. U fokusu našeg interesovanja je NSDDL *(No Short-circuit current Dynamic Differential Logic)* metod [4], i zato će njegovom opisu biti posvećeno četvrto poglavlje ovog rada. U tom kontekstu biće opisano projektovanje NSDDL kombinacionih ćelija na primeru NAND kola, dok je projektovanje Master Slave D flip-flop NSDDL ćelije opisano su petom poglavlju. Rezultati simulacije dobijeni su korišćenjem *ELDO* simulatora u *Mentor Graphics Design Architect* okruženju. Za crtanje lejauta korišćen je *Mentor Graphics ICstudio alat,* dok je za *DRC (Design Rule Check), LVS (Leyout Versus Schematics) i PEX (Parasitic extraction)* zadužena *Calibre*. Izabrana tehnologija za projektovanje je TSMC035.

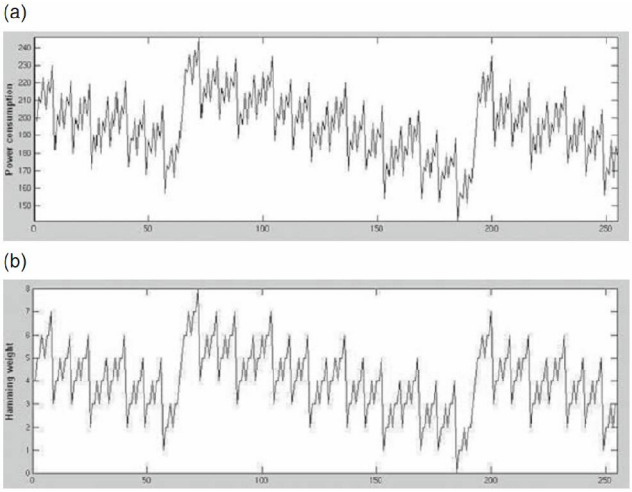
2. TEHNIKE BOČNOG NAPADA ZASNOVANE NA ANALIZI POTROŠNJE

Promena struje napajanja (IDD) predstavlja veoma važan dodatni izvor informacija o ponašanju kriptografskog sistema. Do nagle promene IDD dolazi u CMOS kolima samo prilikom promene logičkih stanja. Tokom promena sa 0 na 1, pune se izlazne kapacitivnosti od VDD preko pMOS mreže. Pri promenama stanja sa 1 na 0 one se prazne prema masi. Ovome treba dodati i struje kratkog spoja tokom intervala u kome vode i pMOS i nMOS tranzistori. Napadaču su poznati pobudni podaci, ali ne može da pristupi tačkama u kojima bi mogao da registruje odziv. Jedini izvor informacija o ponašanju kola jeste aktivnost izražena kroz promenu struje napajanja. Ipak i sama informacija o potrošnji kola u korelaciji je sa aktivnošću kola, te omogućava brže otkrivanje kriptografskog ključa. U najefikasnije tehnike napada, bazirane na analiziranju potrošnje kola, spadaju SPA i DPA.

SPA- je tehnika napada pri kojoj napadač vezuje otpornik redno sa VDD ili GND pinom i osciloskopom prati potrošnju. Dobijene podatke poredi sa informacijom o ponašanju sistema pri poznatoj pobudi na ulazu. Jedan od načina jeste da se upoređuje zapis o potrošnji dobijen napadom sa rastućom sekvencom bitova sa različitim brojem nenultih bitova (Hammingova težina) ili razlikom u broju nenultih bitova između dva susedna koda (Hamminogovo rastojanje) dobijenim istom sekvencom. Slika 1.a ilustruje merenu potrošnju na smart kartici pri kombinacijama $x[0, 255]$. Slika 1.b pokazuje Hammingovo rastojanje za operaciju (184)XOR(x). Očigledna je sličnost oba dijagrama iz koje se zaključuje koju operaciju obavlja sistem i pri kojoj kodiranoj reči.

DPA – predstavlja veoma moćno sredstvo napada. Njime mogu da se otkriju dve važne informacije. Najpre, u kome se delu sekvence promene napajanja nalazi kriptovana informacija, a zatim i da se otkrije sadržaj skrivene informacije. DPA se zasniva na statističkoj obradi prikupljenih podataka. Važnu osobinu DPA napada predstavlja mogućnost da se primeni na otkrivanje dela ključa. Na taj način značajno se smanjuje broj pokušaja

neophodan za otkrivanje celog ključa. Ovo ilustruje primer razbijanja 128-bitne AES šifre. Naime, za otkrivanje ključa od jednog bajta potrebno je 256 kombinacija. DPA napadom moguće je razgraničiti 16 bajtova u 128-bitnom ključu, tako da se ceo ključ može dešifrovata samo sa 256x16=4096 DPA napada.



Slika 1. SPA Napad: a)Mereni podaci o potrošnji na smart kartici b) Hammingovo rastojanje pri operaciji (184)XOR(x), za x [0,…,255], (preuzeto iz [1])

Sve standardne strukture digitalnih logičkih ćelija ranjive su na SCA napade. Kada je u pitanju napad preko analize potrošnje (SPA, DPA), napadača interesuje srednja vrednost potrošnje tokom određene aktivnosti kola. Kao što se sa Slike 1 vidi, informacija o razlici u potrošnji između dve pobudne reči očigledno otkriva aktivnost kola. Kako su se ovakvi napadi pokazali veoma produktivnim, porastao je motiv za proučavanje tehnika kojima se povećava imunost kripto sistema na ovakve napade. Mere zaštite primenjuju se na svim nivoima projektovanja: na arhitekturskom, algoritamskom ili na nivou gejtova. Principi hardverske zaštite od DPA opisani su u narednom odeljku

3. HARDVERSKA ZAŠTITA OD DPA

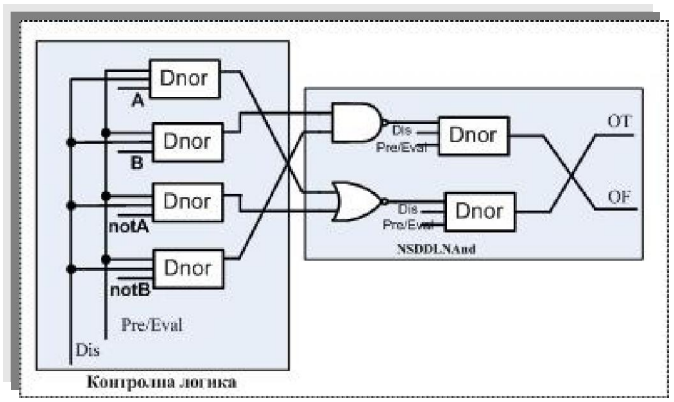
Osnovni način zaštite od DPA sastoji se u razbijanju korelacije između aktivnosti kola i potrošnje. U tu svrhu koriste se dve tehnike. Jedna je zasnovana na maskiranju odstupanja potrošnje od pobude tako što se unose lažne informacije (često uz korišćenje generatora pseudoslučajnih brojeva). Druga se 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 promena ulaznog signala izaziva promenu na bar jednom izlazu. Dakle, uvek postoji promena struje napajanja. Povećan je hardver, povećana je potrošnja, ali je sakrivena informacija o zavisnosti potrošnje od promene stanja signala u sistemu.

Najznačajniji predstavnik ovog pristupa poznat je pod nazivom WDDL (*Wave Dynamic Differential Logic*) [4] WDDL koristi DPL *(Dual-rail with Pre-charge Logic)* logiku tako što pri svakoj kombinaciji ulaznih signala obezbedi promenu stanja ili na pravom ili na lažnom izlazu. Ćelije rade naizmenično u pripremnoj (*pre-charge*) i izvršnoj (*evaluation*) fazi. Tokom pripreme, svi izlazi (pravi i lažni) dovode se u stanje logičke 1. Tokom izvršne faze uvek samo jedan (pravi ili lažni) izlaz menja stanje. Time se obezbeđuje samo jedan logički događaj po ciklusu. Osnovni nedostatak WDDL ćelije ogleda se u osetljivosti na nebalansirano opterećenje diferencijalnih izlaza. Naime, u savremenim kolima dominantan uticaj na kašnjenje signala imaju veze, a ne logičke ćelije. S obzirom da je WDDL zasnovan na primeni diferencijalnih simetričnih signala, svaka asimetrija kvari njihove karakteristike. WDDL metod implementiran na FPGA pokazuje ranjivost usled nesaglasnosti struja punjenja/pražnjenja stadardnih komplementarnih logičkih ćelija (I i ILI). Mnogo bolji rezultati postignuti su realizacijom u ASIC tehnologiji sa redizajniranim dimezijama tranzistora u pMOS i nMOS mrežama [3].

Uvođenjem treće faze, tokom koje se svi kondenzatori u kolu prazne, realizovana je TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*) logika [5]. Na sličnom pricipu zasnovana je NSDDL (*No Short-circuit current Dynamic Differential Logic*) logika [6] čijem su opisu i implementaciji posvećeni naredni odeljci ovog rada.

4. NSDDL METOD

NSDDL metod zasnovan je na logici koja se izvršava u tri različite faze. Pored pripremne i izvršne faze uvedena je i faza pražnjenja kondenzatora (*dis-charge*). Prednost ovog metoda u odnosu na WDDL ogleda se u imunosti na neuparenost opterećenja na pravom i lažnom izlazu. Ovo je postignuto primenom dinamičkog NOR kola kojim se minimizuje uticaj struje kratkog spoja u CMOS kolu. Ono je sastavni deo kako kontrolne logike tako i samih ćelija. Rad NSDDL kola objasniće se na primeru NAND ćelije prikazane na slici 2.

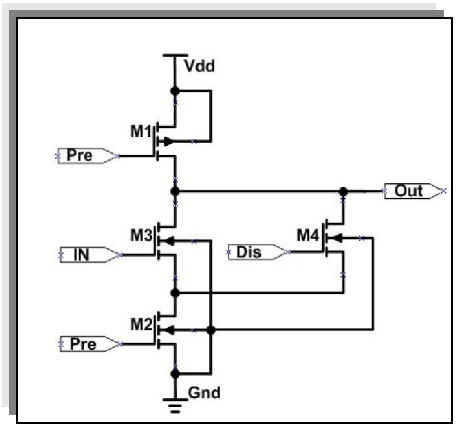


Slika 2. Logička struktura NSDDL NAND/AND2 ćelije

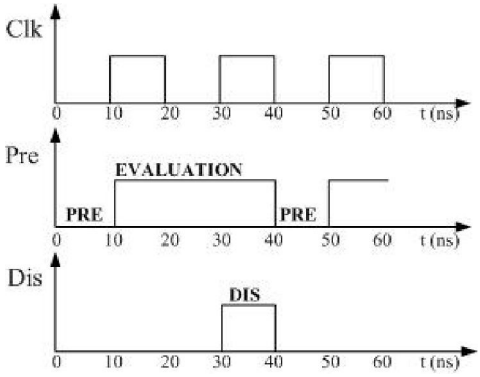
Princip dupliranja hardvera uvođenjem komplementarnih ćelija u ovom slučaju realizuju NAND i NOR kolo. Ključnu ulogu u radu NSDDL ćelije igra dinamičko NOR kolo, označeno sa Dnor na Slici 3. Preko njega se dovode pravi i komplementarni ulazni signali. Pored ulaznih Dnor kolo zaduženo je i za kontrolu izlaznih signala OT i OF.

Slika 4 ilustruje talasne oblike kontrolišućih signala. Tokom pripremne faze signali PRE i DIS su u stanju logičke 0, tako da tranzistor M1 vodi, dok su ostali tranzistori zakočeni. Time se izlaz dovodi u stanje logičke jedinice,

nezavisno od stanja ulaznog signala, IN. Izvršna faza počinje kada signal PRE dostigne logičku jedinicu. Tada su M1 i M4 zakočeni, M2 vodi, a stanje na ulazu IN kontroliše tranzistor M3. Ukoliko je signal IN na nivou logičke 0, M3 ne vodi, tako da izlaz zadržava stanje 1. Ukoliko je ulaz IN na nivou 1, M3 vodi tako da, preko M2 koji vodi, izlazni signal prelazi u stanje 0. Očigledno je da se na izlazu ostvaruje funkcija invertovanja ulaznog signala. Faza pražnjenja nastaje kada su i PRE i DIS signal u stanju logičke jedinice. Tada je M1 zakočen, a M2 i M4 vode, tako da izlazni signal postaje (ostaje) 0 nezavisno od stanja ulaznog signala. Tokom pripremne faze izlazni signal uvek uzima visoki, a tokom faze pražnjenja niski logički nivo.



Slika 3. Električna šema Dnor kola



Slika 4. Talasni oblici kontrolišućih signala kod NSDDL

Kao što se iz prethodnog vidi, hardver je značajno uvećan u odnosu na standardno NAND kolo. Postavlja se pitanje da li je to bilo vredno truda. Da bi se procenila imunost NSDDL ćelije na DPA napad upoređene su promene energije pri promenama ulaznih signala klasične NAND ćelije sa NSDDL NAND ćelijom. Rezultati su sistematizovani u Tabeli I. Ponašanje je analizirano pri promenama ulaznih signala prikazanim u kolonama. Dinamička potrošnja energije iskazana je kroz integral struje napajanja tokom jednog ciklusa promene ulaznih signala koji u slučaju klasične NAND ćelije obuhvata isti vremenski interval koji je potreban NSDDL ćeliji da obavi sve tri faze rada. Kao mera otpornosti na SCA posmatra se relativna srednja razlika potrošnje energije, odnosno vrednost standardne devijacije i standardne devijacije normalizovane sa prosečnom potrošnjom energije. Ove tri veličine označene su sa δE, σ и NSD u vrstama 14, 15 и 16. Očigledno da je postignuta značajna uniformnost potrošnje čime se NSDDL ćelija kvalifikuje kao otporna na DPA napade. Sa stanovišta NSD parametra otpornost je povećana 94,52 puta.

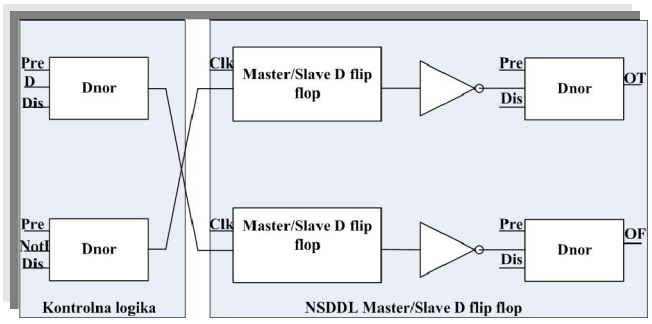
Veoma slični rezultati postignuti su i za druge kombinacione ćelije. Što se tiče sekvencijalnih kola, raspored sve tri faze rada ostaje isti, ali se mora dotatno uskladiti sa signalom takta. Naredno poglavlje opisuje projektovanje MS D flip-flop ćelije (MSDff) primenom NSDDL metoda.

Tabela I

R.br.	A	B	E_{NANDc} [J]	E_{NSDDL} [J]
1	0	0->1	4.667E-14	-2.806E-12
2	0	1->0	-4.788E-14	-2.771E-12
3	0->1	0	4.905E-14	-2.779E-12
4	1->0	0	-5.344E-14	-2.744E-12
5	0->1	0->1	-6.905E-13	-2.753E-12
6	1->0	1	-6.502E-13	-2.820E-12
7	0->1	1	-6.173E-13	-2.773E-12
8	1	1->0	-7.276E-13	-2.790E-12
9	1	0->1	-6.558E-13	-2.742E-12
10	1->0	1->0	-7.600E-13	-2.764E-12
11	E_{max} [J]		4.91E-14	-2.74E-12
12	E_{min} [J]		-7.60E-13	-2.82E-12
13	E_{av} [J]		-4.11E-13	-2.77E-12
14	δE [%]		196.98	2.81
15	σ [fJ]		337.7	24.31
16	NSD[%]		82.23	0.87

5. SEKVENCIJALNA NSDDL KOLA

Blok šema NSDDL MSDff ćelije prikazana je na Slici 5.

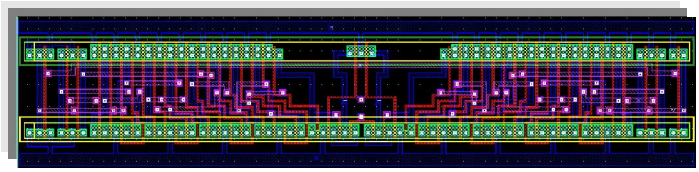


Slika 5. Blok šema NSDDL Master/Slave D flip flop ćelije otporne na bočne napade

Da bi se obavio jedan operacioni ciklus koji sadrži pripremnu, izvršnu i fazu pražnjenja potrebna su dva taktna signala Za transfer ulaznog signala na izlaz MSDff potrebna su dva operaciona ciklusa. Zato je potrebno da kriptovani MSDff radi sa duplo većom frekvencijom takta u odnosu na standardni M/S D flip flop. Izlaz iz kriptovane ćelije vodi se preko bafera i Dnor ćelija čime se obezbeđuje siguran rad bez curenja informacija.

S obzirom da su svi metodi iz pomenute grupe zaštite od bočnih napada zasnovani na primeni simetričnih struktura, posebna pažnja pri projektovanju NSDDL ćelija posvećena je

fizičkom uparivanju simetričnih delova. Lejaut NSDDL MSDff prikazan na Slici 6 ilustruje navedeni pristup.



Slika 6. Lejaut NSDDL M/S D flip flop ćelije otporne na bočne napade

Otpornost na bočne napade ove ćelije verifikovana je na sličan način kao što je urađeno za NSDDL NAND ćeliju. Rezultati simulacije sistematizovani su u Tabeli II.

Tabela II

D	Clk	Q_{n-1}	Q_n	$E_{classic}$ [pJ]	E_{NSDDL} [pJ]
0	0->1	0	0	-0.9604	-10.296
0	1->0	0	0		
0->1	0	0	0	-0.0450	-10.339
1	0->1	0	0	-1.467	-10.312
1	1->0	0	1		
1	0->1	1	1	-0.9082	-10.316
1	1->0	1	1		
1->0	0	1	1	-0.2052	-10.303
0	0->1	1	1	-1.683	-10.293
0	1->0	1	0		
E_{max} [pJ]				-0.0445	-10.29
E_{min} [pJ]				-1.683	-10.34
E_{av} [pJ]				-0.8781	-10.31
δE [%]				186.5	0.448
σ [fJ]				598.46	15.41
NSD[%]				68.152	0.149

Dinamička potrošnja energije iskazana je kroz integral struje napajanja tokom obe ivice taktnog signala kada ulazni signal miruje (interval od dva operaciona ciklusa), odnosno jedan operacioni ciklus kada se menja samo signal D. Kao u slučaju kombinacionih ćelija, za 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). Maksimalno relativno odstupanje svedeno je od 186,5% na svega 0,448%. Sa stanovišta parametra NSD otpornost je povećana za više od 457 puta.

4. ZAKLJUČAK

NSDDL Master/Slave D flip flop predstavlja sekvencijalnu ćeliju u biblioteci digitalnih ćelija otpornih na bočne napade. Projektovano je u CMOS tehnologiji TSMC 0,35um korišćenjem Mentor Graphics projektantskih alata. Dobijeni rezultati pokazali su da ovako projektovana ćelija, gledano iz bezbedonosnog ugla, ima odlične karakteristike. To upućuje na dobar odabir metoda za kriptovanje u hardveru. Nedostatak ovakvih metoda za kriptovanje je povećana potrošnja usled dodavanja hardvera. Međetim, kada se uzme u obzir sigurnosni aspekt i važnost očuvanja podataka ovakav podatak se zanemaruje.

ZAHVALNOST

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

LITERATURA

[1] Koc, Cetin Kaya (Ed.) *Cryptographic Engineering*, Springer, 2009.

[2] 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.

[3] M. Stanojlović, P. Petković, "Hardware based strategies against side-channel-attack implemented in WDDL", *Electronics*, Vol. 14, No. 1, Banja Luka, June, 2010, pp. 117-122

[4] Danger, J.-L. Guilley, S. Bhasin, S. Nassar, M., Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors, *Proc. of International Conference on Signals, Circuits and Systems SCS'2009*, Djerba, Tunisia, November 5-8 2009, pp. 1-8

[5] 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)

[6] 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.

Abstract – The usual method for the unauthorized disclosure of encrypted information is reduced to the proceedings based on combinatorics, which allows detection of code. Complex cryptographic algorithms are designed to prevent / hamper investigation of possible combinations in real time. Information about the behavior of e-crypto-system can significantly reduce the number of combinations necessary to discover beyond. Collecting such information is a "side-attack" (Side Channel Attack -SCA). The most common form of attack is reduced to the power analysis of consume electronic cryptosystem. In order to prevent attacks of this type is necessary in the crypto-system to introduce additional hardware protection. Hardware protection methods are reduced to breaking the correlation between circuit activities and spending. Specifically this paper analyses the properties of digital cells based on the implementation NSDDL (No Short-circuit current Dynamic Differential Logic) method.

HARDVARE PROTECTION AGAINST ATTACKS ON CRYPTO-SYSTEM BASED ON THE IMPLEMENTATION OF CELLS THAT MASKED INFORMATION ABOUT CONSUMPTION

Predrag Petković, Milena Stanojlović