UNIVERZITET CRNE GORE

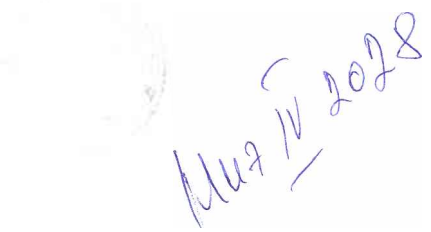
ELEKTROTEHNIČKI FAKULTET

Milena Đukanović

TEHNIKE SIDE-CHANNEL NAPADA NA HARDVER PAMETNE KARTICE I HARDVERSKE MJERE ZAŠTITE

- Doktorska teza -

Podgorica, 2012. godina



PODACI I INFORMACIJE O DOKTORANTU

Ime i prezime: **Milena Đukanović**

Datum i mjesto rođenja: **08.06.1983. godine, Podgorica, Crna Gora**

Naziv završenog postdiplomskog studijskog programa i godina završetka: **Elektronika, magistarski rad odbranjen 10.12.2007. godine**

INFORMACIJE O DOKTORSKOJ DISERTACIJI

Naziv doktorskih studija: **Doktorske studije elektrotehnike**

Naziv teze: **Tehnike side-channel napada na hardver pametne kartice i hardverske mjere zaštite**

Fakultet na kojem je disertacija odbranjena: **Elektrotehnički fakultet, Podgorica**

UDK, OCJENA I ODBRANA DOKTORSKE DISERTACIJE

Datum prijave doktorske teze: **05.10.2009. godine**

Datum sjednice Senata Univerziteta na kojoj je prihvaćena teza: **11.02.2010. godine**

Komisija za ocjenu podobnosti teze i kandidata:

Prof. dr Radovan Stojanović

Prof. dr Veselin Ivanović

Prof. dr Vladan Vujičić

Mentor: **Prof. dr Vladan Vujičić**

Komisija za ocjenu doktorske disertacije:

Prof. dr Alessandro Trifiletti

Prof. dr Vladan Vujičić

Prof. dr Dejan Vukobratović

Komisija za odbranu doktorske disertacije:

Prof. dr Igor Đurović

Prof. dr Vladan Vujičić

Prof. dr Alessandro Trifiletti

Prof. dr Veljko Milutinović

Prof. dr Zoran Mijanović

Datum odbrane: 21.06.2012. godine

Datum promocije: _____

Izražavam zahvalnost svom mentoru Prof. dr Vladanu Vujičiću na svesrdnoj i dragocjenoj pomoći, ukazanom povjerenju i korisnim savjetima pri izradi doktorske teze.

Posebnu zahvalnost dugujem Prof. dr Alessandro Trifiletti-ju i Prof. dr Giuseppe Scotti-ju sa Università La Sapienza di Roma, Dipartimento di Ingegneria Elettronica, Centro Studi Giorgio Barzilai, na pruženoj mogućnosti da se bavim naučno-istraživačkim radom na pomenutoj instituciji i intezivnoj saradnji tokom rada na tezi.

Milena Đukanović

SADRŽAJ

REZIME

U radu je analizirana najefikasnija klasa napada na pametne kartice u protekloj deceniji (*side-channel* napadi), koja se zasniva na slabostima u hardverskoj implementaciji algoritma i eksploatiše informacije koja "cure" iz kriptografskog uređaja u toku izvršavanja algoritma. Među njima najmanje proučavani napadi baziraju se na analizi statičke disipacije snage i struja curenja u hardveru. Njihova aktuelnost dobija na značaju sa primjenom novih tehnologija zbog dominantnog udijela statičke disipacije snage u ukupnoj snazi disipacije, a samim tim i odlučujućeg uticaja na performanse dizajna pametne kartice. Iz tog razloga izvršena je analiza i implementacija nove tehnike pasivnih napada na 65nm-sko CMOS kriptografsko jezgro, koja je bazirana na analizi struja curenja hardvera pametne kartice – tzv. CLA (*Correlation Leakage Analysis*) napad. Istraživanja su obuhvatila takođe i analizu uticaja *intra-die* procesnih varijacija na efektivnost ovog napada. CLA napadi su se pokazali izuzetno uspješnim na značajnom broju testnih uzoraka CMOS kriptografskog uređaja, čime se pokazalo da CMOS tehnologija ne predstavlja dovoljno dobru mjeru zaštite protiv CLA napada.

Značajan dio rada posvećen je i analizi adekvatnih mjera zaštite u odnosu na CLA napade na hardver pametne kartice. U tom smislu, razmatrana je i veoma aktuelna hardverska mjera zaštite na tranzistorskom nivou bazirana na TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*) logici, koja je prvobitno kreirana kao vrlo efikasna protivmjera napadima baziranim na analizi dinamičke disipacije snage i dinamičkih struja, tzv. DPA (*Differential Power Analysis*) napadima. U tu svrhu je modelovan CLA napad na 65nm-sko TDPL kriptografsko jezgro sa uzimanjem u obzir *intra-die* procesnih varijacija, a dobijeni rezultati su upoređeni sa prethodno dobijenim rezultatima za CLA napad na 65nm-sko CMOS kriptografsko jezgro.

Na kraju, prikazana je i zavisnost struja curenja od implementirane tehnologije (90nm-ska i 65nm-ska), tipa tranzistora (h-tip i l-tip), temperature (0°C, 25°C, 50°C, 75°C, 100°C), tipa podataka (ulazni ili izlazni podaci), itd. Takođe, izvršena je komparacija 65nm-ske CMOS i TDPL logike putem faktora NCD (*Normalized Current Deviation*) i NSD (*Normalized Standard Deviation*) sa aspekta njihove efikasnosti kao mjera zaštite od CLA napada.

ABSTRACT

This work analyzes the most efficient class of attacks on smart cards in the last decade (side-channel attacks), that is based on weaknesses in the hardware implementation of encryption modules and exploits the information that "leak" from crypto-core devices while executing the algorithm. The least studied among them are the attacks based on analysis of static power consumption and leakage currents in the hardware. Their actuality brings on importance with the use of new technologies where static power consumption plays major part in overall power consumption and therefore decisive influence on design peroformances of smart cards. For that reason, analysis and implementation of passive attack's new technique on 65-nm CMOS crypto-core, which is based on analysis of leakage currents in the hardware of smart card - so-called CLA (*Correlation Leakage Analysis*) attack. Influence of *intra-die* process variations on efectiveness of this attack has also been included in research. CLA attacks have proven to be extremely successfull on significant number of test samples of CMOS crypto-cores, thus proved that CMOS technology does not represent a countermeasure enough durable against CLA attacks.

Significant part of thesis is dedicated to analysis of adequate countermeasures regarding CLA attacks on smart card's hardware. In this respect, a current countermeasure at transistor level based on TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*) logic has been considered, originally created as a very efficient countermeasure for attacks based on analysis of dynamic power consumption and dynamic currents, so-called DPA (*Differential Power Analysis*) attacks. For this purpose, a CLA attack on 65-nm TDPL crypto-core has been modeled, with taking into account *intra-die* process variations. These results have been compared with the previously obtained results for CLA attack on 65-nm CMOS crypto-core.

Finally, dependence of leakage currents on implemented technology (90-nm and 65-nm), transistor type (h-type and l-type), temperature (0°C, 25°C, 50°C, 75°C, 100°C), data type (input or output data), etc. is presented. Also, a comparison of 65-nm CMOS and TDPL logics through factors NCD (*Normalized Current Deviation*) and NSD (*Normalized Standard Deviation*) was done from the aspect of their efficiency as a CLA attacks' countermeasure.

I Uvod

Tehnike pasivnih napada (*Side-Channel Attacks*) na hardver čip-kartice i mjere zaštite od takvih napada su predmet intenzivnih istraživanja u protekloj deceniji. Aktuelnost teme potvrđena je i brojnim projektima sponzorisanim od Evropske unije (okvirni projekti FP6, FP7) koji se upravo bave analizama i simulacijama pasivnih implementacionih napada, kao i kreiranjem hardvera koji će biti otporan na ove napade.

Najrasprostranjenija i najpoznatija među čip-karticama je pametna kartica (*smart card*) koja u sebi sadrži integrisani čip kojim se značajno podiže nivo sigurnosti, jer omogućava ugradnju kriptografskih algoritama i primjenu širokog skupa zaštitnih mehanizama. Njene najveće prednosti su male dimenzije, prenosivost, višekratna upotrebljivost, raznolikost funkcionalnosti i sigurnost. U odnosu na svoju konkurenciju pametne kartice imaju prednost upravo zbog sigurnosti, iako ne postoji pametna kartica za koju možemo reći da je u potpunosti sigurna. Međutim, sa adekvatnim dizajnom i zaštitnim mehanizmima pametne kartice se mogu smatrati relativno sigurnim sistemima, sa minimalnim rizikom za uspješnost napada.

Najefikasnija klasa napada na pametne kartice u protekloj deceniji zasniva se na slabostima u hardverskoj implementaciji algoritma, a posebno interesantni su pasivni napadi koji se popularno zovu i *side-channel* napadi, jer eksploatišu informaciju koja "curi" iz kriptografskog uređaja u toku izvršavanja algoritma. Najefektniji i najviše proučavani *side-channel* napadi ostvareni u praksi i publikovani do sada su napadi bazirani na analizi dinamičke disipacije snage i dinamičkih struja, kao i elektromagnetnom zračenju kriptografskog jezgra. Najmanje proučavani pasivni napadi baziraju se na analizi statičke disipacije snage i struja curenja, a shodno tome oni su do sada rijetko i veoma oskudno razmatrani u literaturi. Aktuelnost analize pasivnih napada baziranih na analizi statičke disipacije snage i struja curenja dobija na značaju s obzirom da sa novim tehnologijama (90nm-ska, 65nm-ska, 45nm-ska) statička disipacija snage ima dominantan udio u ukupnoj snazi disipacije, a samim tim i odlučujući uticaj na performanse dizajna pametne kartice.

Stoga su se, sa primjenom novih tehnologija, javili realni razlozi i potrebe za istraživanja mogućnosti realizacije pasivnih napada baziranih na analizama ovih parametara. Upravo će se doprinos ove disertacije ogledati u analizi i implementaciji nove tehnike pasivnih napada koja je bazirana na analizi struja curenja hardvera pametne kartice, kao i pronalaženju efikasnih mjera zaštite hardvera pametne kartice od tih napada.

Disertacija se sastoji od ukupno osam poglavlja. Nakon uvoda, u drugom poglavlju su objašnjeni principi i ciljevi kriptografije, data je istorija kriptografije i kriptoanalize, navedena je i objašnjena podjela kriptografskih algoritama. Opisane su fizičke i električne karakteristike pametnih kartica i klasifikacija istih prema vrsti čipa, načinu prenosa podataka i mehanizmu pristupa.

U trećem poglavlju su definisane sigurnosne komponente pametne kartice i izvršena je klasifikacija napada na pametne kartice. Detaljno je opisana najefikasnija klasa napada na pametne kartice u protekloj deceniji - *side-channel* napadi, kao i tipovi *side-channel* napada: napadi bazirani na analizi snage (*Power Analysis Attacks*), vremenskoj analizi (*Timing Analysis Attacks*), analizi elektromagnetnog zračenja (*Electromagnetic Analysis Attacks*), analizi grešaka (*Fault Analysis Attacks*).

U četvrtom poglavlju je napravljen pregled postojećih mjera zaštite kriptografskih jezgara pametnih kartica (algoritamskih i hardverskih) od *side-channel* napada baziranih na analizi snage (struje). Hardverske mjere zaštite, koje su od posebnog interesa za ovaj rad, klasifikovane su prema uključenom nivou implementacije hardvera - na nivou sistema, kola ili tranzistora. Nalaženje adekvatnog rješenja u hardverskim mjerama zaštite pametnih kartica od pasivnih napada baziranih na analizi struja curenja hardvera, analiziraće se kroz implementaciju i testiranje novih logičkih stilova, kao što je TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*).

Peto poglavlje se bavi procjenom zavisnosti struja curenja od implementirane tehnologije, temperature i *Hamming*-ove težine ulaznih podataka. U tu svrhu izvršena je komparacija struja curenja za CMOS logička kola koja su implementirana u 90nm-skoj i 65nm-skoj tehnologiji, pri čemu je uzeto u obzir pet različitih temperatura. Takođe, prikazana je i zavisnost struja curenja od *Hamming*-ove težine ulaznih podataka u *bit-sliced* strukturama (registrima) dizajniranim u 65nm-skoj CMOS tehnologiji.

U šestom poglavlju je detaljno objašnjena procedura vršenja napada baziranog na analizi struja curenja CLA (*Correlation Leakage Analysis*), koji eksploatiše simulirane i izmjerene vrijednosti struje curenja kriptografskog uređaja sa ciljem nalaženja tajnog ključa. Radi boljeg razumijevanja suštine funkcionisanja, kao i preciznije simulacije CLA napada u eksperimentalnim uslovima, analiziran je uticaj procesnih varijacija na rezultate napada. Kroz detaljne analize pokazaće se da procesne varijacije ne utiču na uspješnost CLA napada na 65nm-sko CMOS kriptografsko jezgro i stoga se mogu zanemariti.

Kako se CLA napad pokazao uspješnim na CMOS kriptografsko jezgro, u sedmom poglavlju izvršena je analiza jedne od najnovijih i najperspektivnijih hardverskih mjera zaštite na tranzistorskom nivou - TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*) logike, koja je prvobitno kreirana kao protivmjera napadima baziranim na analizi dinamičke disipacije snage i dinamičkih struja - DPA (*Differential Power Analysis*) napadima. Izvršena je komparacija CMOS/TDPL logike, koje koriste l-tip tranzistora u 65nm-skoj tehnologiji. Putem faktora NCD (*Normalized Current Deviation*) i NSD (*Normalized Standard Deviation)* ove logike su poređene sa aspekta njihove efikasnosti kao mjere zaštite od CLA napada. Takođe, modelovan je CLA napad na 65nm-sko TDPL kriptografsko jezgro sa uzimanjem u obzir procesnih varijacija. Ti rezultati biće upoređeni sa prethodno dobijenim rezultatima za CLA napad na 65nm-sko CMOS kriptografsko jezgro.

U osmom poglavlju je izvršena analiza postignutih rezultata korišćenjem tehnike CLA napada na CMOS i TDPL kriptografsko jezgro, a dati su i predlozi za promjene i poboljšanja iste.

U disertaciji je data literatura sa 122 korišćene reference.

Kao prilog doktorskom radu, dati su dodaci A i B u kojima se nalaze Matlab i OCEAN kodovi za realizaciju CLA napada na CMOS i TDPL kriptografsko jezgro. Takođe, dati su šematski prikazi složenijih struktura CMOS i TDPL kola koji su realizovani u Cadence softveru.

Sastavni dio rada predstavlja i priloženi CD, koji sadrži sve kodove i fajlove potrebne za izvršenje CLA napada na CMOS i TDPL kriptografsko jezgro, šematske prikaze djelova kriptografskih jezgara, rezultate običnih i *Monte Carlo* simulacija struja curenja.

II Karakteristike pametnih kartica

Tehnologija danas, više nego ikad, određuje društvo u kojem živimo. Ulazi u sva područja ljudske djelatnosti, stvara nove vrste poslova i uzrokuje evoluciju društva. Jedan izum objedinjuje i simbolizuje ove promjene, a to je računar. Prvi računari izvodili su nekoliko računskih operacija, a današnji izvode 3D animacije, izvršavajući pritom mnogobrojne paralelne operacije velikom brzinom. Razvoj poluprovodničke industrije omogućio je da se veličina računara sa prostora jedne sobe spusti na površinu od nekoliko kvadratnih milimetara. Time je stvoren prostor za razvoj novih tehnologija. Jedna od njih je i pametna kartica (*smart card*).

§ *II.1 Istorija pametnih kartica*

Korijeni današnjih pametnih kartica sežu do 1950. godine i *Diners* kluba koji je proizveo prvu plastičnu karticu i počeo da je koristi kao sredstvo plaćanja i identifikacije vlasnika kao člana ekskluzivne grupe ljudi [1]. Tada se paralelno na tržištu pojavljuju *Visa* i *MasterCard*, ali je zbog neovlašćenog miješanja potreba klijenata i banke bilo neophodno napraviti karticu koja bi se "čitala" uz pomoć nekog uređaja. Tako se pojavila kartica sa magnetnom trakom koja je omogućila digitalizaciju podataka. Međutim, kako se uz pomoć određenih uređaja moglo pristupiti ovoj kartici i vršiti upisivanje, čitanje i brisanje podataka, trebalo je doraditi karticu dodavanjem centralne infrastrukture za verifikaciju i obradu podataka. Inače, ovaj tip kartice je bio u znatno većoj upotrebi u SAD-u u odnosu na Evropu. Jedno rješenje je bilo jačanje serverskih karakteristika, a drugo prebacivanje dijela aktivnosti sa servera na klijenta. Opredjeljujući se za drugo rješenje, Evropske zemlje su uvele u upotrebu karticu sa integrisanim kolom (*Integrated Circuit Card - ICC*) [2].

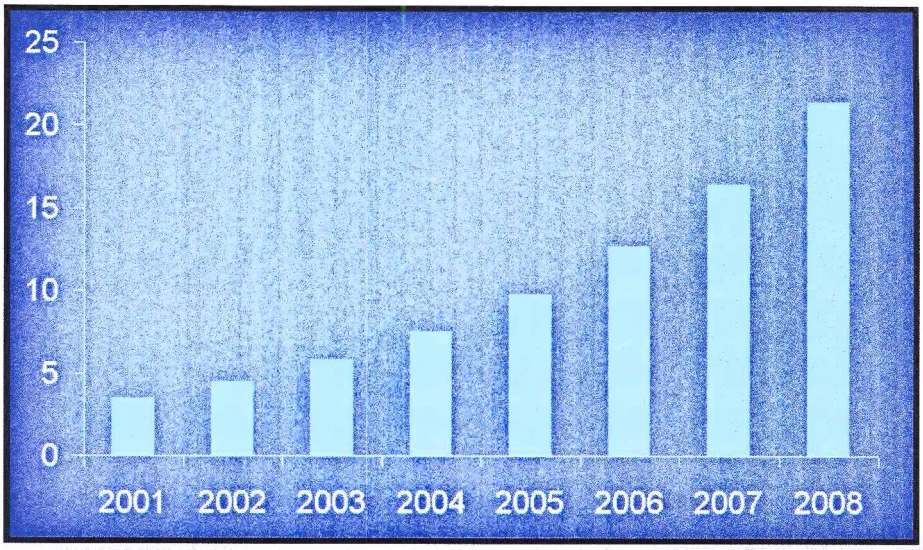
Tri čovjeka se navode kao mogući izumitelji pametnih kartica: Nijemac *Jürgen Dethloff*, Japanac *Kunitaka Arimura* i Francuz *Roland Moreno*. Prva komercijalna primjena

pametne kartice započinje 1984. godine u Francuskoj kada telefonska industrija PTT (*Postal and Telecommunications services agency*) izdaje prvu telefonsku karticu kao sredstvo plaćanja u javnim telefonskim govornicama. Novu revoluciju pametne kartice doživljavaju sredinom 1990-ih uvođenjem GSM (*Global Standard for Mobile Telecommunications*) standarda u mobilnu telefoniju [3]. GSM specifikacija podijeljena je u dva dijela, prvi dio opisuje osnovne funkcionalne karakteristike, dok drugi dio opisuje interfejs i logičku strukturu kartice. Originalno, ova specifikacija je bila napravljena za mobilnu telefonsku mrežu. Kada se pametna kartica počela koristiti u mobilnim telefonima kao SIM (*Subscriber Identification Modul*) modul identifikacije pretplatnika, dio GSM standarda postao je i standard pametnih kartica. Najzaslužnije organizacije za razvoj pametnih kartica su organizacije poput EMV (*Europay International, Mastercard International & Visa*) koje su kreirale i istoimeni standard za pametne kartice [4]. Ovaj standard pokriva elektromehaničke karakteristike, protokole, podatke, instrukcije koje su povezane sa bankarskim transakcijama. Cilj EMV specifikacije je da svi sistemi za plaćanje dijele iste POS (*Points of Sales*) terminale čime se osigurava da pametne kartice budu kompatibilne sa bankarskim transakcionim sistemima.

Od ranih 1990-ih pa sve do danas pametne kartice napreduju i mijenjaju svoju funkcionalnost i područja primjene. Inter-operabilnost, standardizacija i razvoj su izazovi postavljeni današnjim pametnim karticama. Ti izazovi nijesu jednostavni - uz pomoć industrije javljaju se inovativna rješenja koja spajaju nove tehnologije, poput interaktivne televizije, pametnih mobilnih telefona, ručnih digitalnih organizatora, elektronskih novčanika i interneta. Dokumentovati noviju istoriju pametnih kartica (od 1999. godine do danas) nije jednostavno. Na tržištu svakim danom ima sve više rješenja za različite primjene pametne kartice. Prihvatanje i primjena tehnologije pametnih kartica razlikuje se od zemlje do zemlje i nacionalni sistemi još uvijek nijesu kompatibilni.

Usljed zahtjeva na sve široj primjeni pametnih kartica, javlja se potreba za bržim razvojem kartičnih aplikacija (Slika 2.1). Sigurnosni zahtjevi se neprestano mijenjaju, nema proizvođača pametnih kartica koji može reći da je njegov proizvod otporan na sve postojeće (buduće) napade. Pristup sigurnosti pametnih kartica sve više se okreće standardizaciji. Prepoznavanje opasnosti, njihova specifikacija i mjere zaštite implementirane prema standardima, znatno će pojednostaviti korišćenje i razumijevanje s jedne strane, a otežati gubitak informacija s druge. Sigurnosna evaluacija rješenja koje obuhvata prethodno

navedene karakteristike, prati cjelokupni razvoj pametne kartice od faze ideje do nalaženja adekvatnog rješenja. Nezavisnost proizvođača mikromodula pametnih kartica i proizvođača kartičnih operacionih sistema uzrokovaće niže cijene kartičnih sistema. Od pametnih kartica se u budućnosti očekuje raširena upotreba na svim područjima ljudskih djelatnosti, objedinjavanje više usluga na jednoj kartici i lakše poslovanje uz maksimalnu sigurnost.



Slika 2.1 – Broj prodatih pametnih kartica u svijetu izražen u milijardama

§ *II.2 Tipovi pametnih kartica*

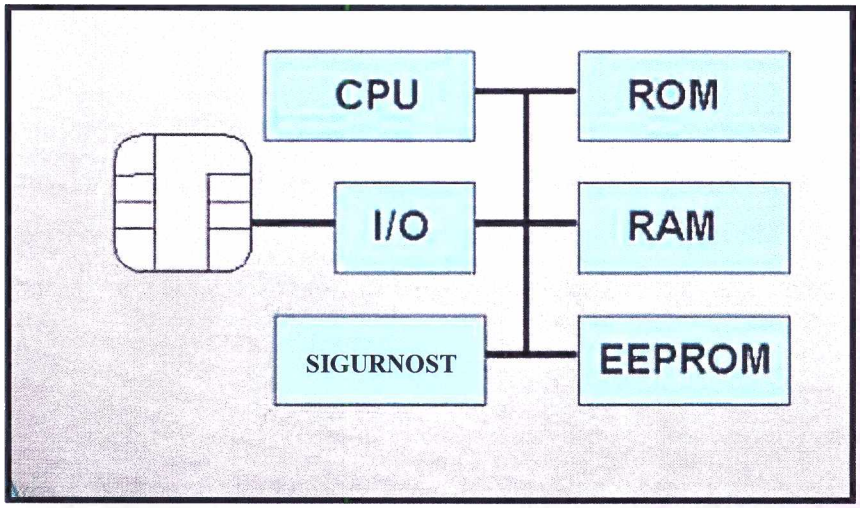
Postoje četiri osnovne vrste pametnih kartica: memorijske, mikroprocesorske, kartice sa kripografskim procesorom i beskontaktne pametne kartice [5]. Osim njih postoje i hibridne kartice koje ujedinjuju oba tipa kartica (kontaktne i beskontaktne), kao i napredne pametne kartice kojima nije potreban ni spoljašnji izvor energije, zbog čega im je nivo sigurnosti dodatno povećan.

- Memorijske kartice sadrže EEPROM (*Electrically Erasable Programmable Read Only Memory*) i ROM (*Read Only Memory*) memoriju, kao i adresnu sigurnosnu

logiku, ali ne sadrže mikroprocesor niti operativni sistem koji ih kontroliše. Najjednostavniji dizajn ovih kartica podržava logiku koja onemogućava pisanje i brisanje podataka. Složeniji dizajn nudi mogućnost ograničenog pristupa kod čitanja podataka sa kartice. Memorija može sadržati samo statičke podatke (kao što su razni identifikatori, imena i sl.) ili podatke za koje nije potrebna dinamička enkripcija. Tipične aplikacije sa memorijskim karticama su telefonske kartice sa "plaćanjem unaprijed" (*prepaid*), kao i kartice za zdravstveno osiguranje.

Besprocesorski čipovi koji se nalaze unutar kartica posjeduju tvrdo-ožičenu logiku (*hard wired logic*) kojom se kontroliše pristup kartici. Upravljanje pristupom je izvedeno postavljanjem unutrašnjeg prekidača (*on/off switch*) baziranog na upoređivanju PIN-a (*Personal Identification Number*) i zapisa u zaštićenoj memoriji u unutrašnjosti kartice. Nakon što test PIN-a uspješno prođe, prekidač je postavljen u *on* poziciju i podaci su raspoloživi za korišćenje. Bitovi mogu biti tretirani kao zasebni ili grupisani tako da formiraju oktalni ili heksadecimalni zapis. Bez obzira na to da li se koristi tvrdo-ožičena logika ili ne, operacija pristupanja podacima na čipu i izvođenje ulazno/izlaznih operacija su pod nadzorom domaćina (*host*). Svaki proizvođač implementira svoje čipove na drugačiji način, pa se nakon umetanja u čitač mora ispitati da li je pametna kartica ispravna. Na primjer, programska podrška domaćina će preko čitača izvršiti nekoliko testova nad karticom, a prvi podrazumijeva slanje zahtjeva kojim se saznaje vrsta kartice. Ako je na kartici ugrađen procesor, ona će odgovoriti ATR (*Answer To Reset*) signalom i ostatak komunikacije se znatno pojednostavljuje. Ako pak kartica ne odgovori na zahtjev, znači da je u pitanju obična memorijska kartica. Komunikacija je složenija, jer prije doticanja identifikacijskog bajta potrebno je obaviti i neke druge radnje. Prva od njih je detektovanje ispravnog mehanizma za komunikaciju sa memorijskim čipom. Čitači tu detekciju sprovode tako što šalju različite zahtjeve kartici, sve dok ne dobiju odgovor koji određuje mehanizam kojim će se komunicirati sa memorijskim čipom. Iz toga se može zaključiti da se memorijske kartice mogu koristiti samo u okruženjima za koja je unaprijed poznato da podržavaju taj tip kartice, jer u suprotnom aplikacija ne reaguje na umetanje kartice u čitač.

- Arhitektura mikroprocesorskih kartica uključuje komponente kao što su centralna procesorska jedinica CPU (*Central Process Unit*) ili procesor, RAM (*Random Access Memory*), ROM i EEPROM (Slika 2.2) [6]. Procesor omogućava unos informacija u memoriju i njihovu zaštitu, čitanje podataka iz memorije kartice i obavljanje instrukcija. Nakon što se procesor priključi na napajanje, umetanjem kartice u čitač, čip unutar kartice postaje mali računar. Za upravljanje, pametna kartica koristi operativni sistem koji se takođe nalazi na kartici, poznatiji kao SCOS (*Smart Card Operating System*) koji je jedinstven za svaki čip ili proizvođača kartice. Takođe, operativni sistem se često naziva i ROS (*Reader Operating System*). Operativni sistem je obično smješten unutar ROM memorije, dok CPU koristi RAM za radnu memoriju, a većina podataka je spremljena u EEPROM memoriji. Empirijsko pravilo kod silikona za pametne kartice govori o tome da RAM zahtijeva četiri puta veći prostor od EEPROM memorije, dok EEPROM zahtijeva četiri puta više prostora od ROM memorije.



Slika 2.2 – Arhitektura mikroprocesorskih kartica

- Iako su tehnički u istoj kategoriji kao i mikroprocesorske kartice, kartice sa kriptografskim koprocesorom se od njih razlikuju u cijeni i funkcionalnosti [7]. Algoritmi kriptovanja služe da obezbijede sigurnost pametnim karticama i ugrađeni su

u hardveru mikroprocesorskih kartica. Pošto oni zahtijevaju računanje sa velikim cijelim brojevima, arhitekturi pametnih kartica dodaje se kriptografski koprocesor. Na taj način vrijeme potrebno za složene operacije smanjeno je na nekoliko stotina mikrosekundi. Koprocesori uključuju dodatnu aritmetičku jedinicu, čime se znatno podiže cijena pametne kartice. Uvođenje kriptografskog koprocesora povećava cijenu kartice za 50-100%, ali se ta cijena postepeno smanjuje povećanom proizvodnjom kartica. Uprkos većoj cijeni, koprocesor donosi velike prednosti računarskoj i mrežnoj sigurnosti, a omogućava da privatni ključ nikad ne napušta karticu. Sigurnost predstavlja kritičan faktor u operacijama kao što su digitalni potpis, autentifikacija i neporicanje. Povećanjem snage i funkcionalosti osnovnih procesora moguće je da kriptografski koprocesori uskoro više neće biti nužno potrebni. Osim intenzivnih matematičkih algoritama, postoje i algoritmi koji koriste eliptičke krive (*elliptic curve technology*). Eliptičke krive koriste se u kriptosistemima sa javnim ključem, kao i u algoritmima za kreiranje digitalnog potpisa. Upotrebom eliptičkih krivih postiže se isti nivo sigurnosti pri znatno manjoj dužini ključa od dužine ključa u algoritmima (npr. RSA) gdje se one ne koriste.

- Beskontaktne pametne kartice umjesto kontakata na površini kartice upotrebljavaju neku vrstu beskontaktnog spoja [8], [9]. Kartica se mora približiti na određenu udaljenost od čitača, zavisno od vrste tehnologije koja se koristi. Nakon toga čitač preko induktivnog (transformator) ili kapacitivnog spoja usmjerava električnu energiju ka kartici čime se vrši njeno aktiviranje.

- Hibridne pametne kartice (*combo smart cards*) posjeduju mogućnost rada kao kontaktne i beskontaktne kartice, a uz to imaju na sebi i magnetsku traku, pa podržavaju tehnologiju s jednodimenzionalnim ili dvodimenzionalnim bar kodom [10]. Ta svojstva omogućavaju kartici široko područje upotrebe i multi-aplikativno korišćenje .

- Do sada opisane kartice su pasivne, jer za svoj rad zahtijevaju spoljašnji izvor napajanja i terminal (čitač). Ta ograničenja dosta utiču na njihovu prikladnost za neke tipove aplikacija. Na primjer, svaki terminal mora osiguravati dostupnost, ali i

zadovoljavajući nivo sigurnosti u odnosu na potencijalne napade na sistem. Ti nedostaci su doveli do razvijanja aktivnih pametnih kartica treće generacije, koje su poznatije pod imenom napredne pametne kartice (*super smart cards*) [11].

Napredne pametne kartice sadrže LCD (*Liquid Crystal Display*) monitor, tastaturu i naslon koji se nalaze na samoj površini kartice. Mogu funkcionisati kao potpuno zasebne jedinice (*standalone units*) ili se mogu priključiti na računar kontaktima na svojoj površini. Nedostatak naprednih pametnih kartica je visoka cijena u poređenju sa drugim vrstama pametnih kartica, poteškoće kod usklađivanja sa ISO standardima i male dimenzija tastature na kartici. Glavna prednost naprednih pametnih kartica je *off-line* funkcionalnost samo-vrednovanja (*self-validating*). Za razliku od pasivnih kartica kojima je potreban izvor napajanja, napredne pametne kartice se mogu koristi uvijek i svugdje, a zajedno sa ugrađenim programima za vrednovanje PIN-a i ostalih sigurnosnih sistema, postižu vrlo visok nivo zaštite postojećeg sistema pametnih kartica.

§ II.3 Fizičke i električne karakteristike pametnih kartica

Najvažnije karakteristike pametnih kartica definišu ISO (*International Organization for Standardization*) standardi. ISO 7816 standard opisuje pametnu karticu [12].Tačan naziv za ovaj standard je "*Indentification cards – Integrated circuit cards with contacts*". Postoji nekoliko djelova ISO 7816 standarda:

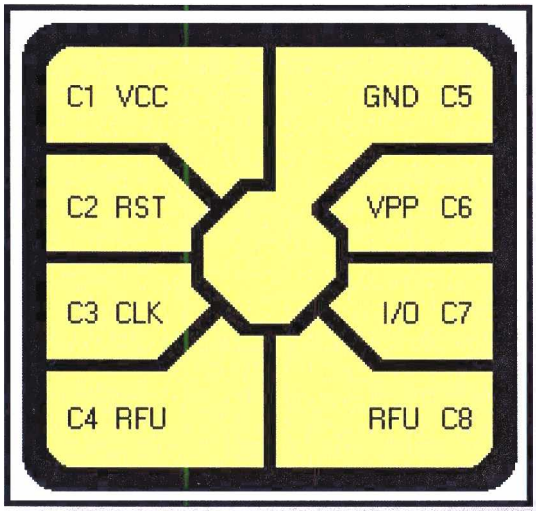
- ISO/IEC 7816-1 – opisuje fizičke karakteristike kao što su dimenzije pametne kartice, materijal od kog je napravljena pametna kartica i otpornost pametne kartice na spoljašnje uticaje, pod koje spadaju ultraviolentno zračenje, temperatura, sila savijanja, snaga elektromagnetnog polja, količina statičkog elektriciteta, itd. Neki materijali od kojih se danas izrađuju pametne kartice i neka njihova svojstva prikazani su u Tabeli II.1. Takođe, prema ovom standardu postoje tri formata pametnih kartica identifikovana kao *ID-1* (85.60mm×53.98mm×0.76mm), *ID-00* (66.00mm×33.00mm×0.76mm), *ID-000* (25.00mm×15.00mm×0.76mm), među kojima su popularniji *ID-1* i *ID-000* formati.

Tabela II.1 – Karakteristike materijala od kojih se izrađuju pametne kartice

Materijal	PC	PVC	ABS
Ime	polikarbonat	polivinil-hlorid	acryl-butadien-styrol
Pretpostavljeni životni vijek	>10 godina	2-5 godina	oko 4 godine
Mehanička svojstva	Izdržljiv na hemijske agense i visoke temperature, ali osjetljiv na mehanička oštećenja	Osjetljiv na visoke temperature	Teško prima boje
Temperaturni opseg	-40°C do 120°C	-5°C do 65°C	-25°C do 80°C
Područja upotrebe	identifikacija	kreditne kartice	SIM moduli
Biološka štetnost	ništa poznato	potrebno ga je kontrolisano odlagati, jer sadrži hlorid	za sada nijesu poznati negativni uticaji na zdravlje, ali sadrži karcinogeni benzen

- ISO/IEC 7816-2 – određuje dimenzije i lokaciju kontakata na pametnoj kartici, kao i funkciju i poziciju određenog kontakta. Kontaktna pločica na površini pametne kartice koja je spojena sa izvodima ugrađenog čipa pametne kartice ima osam kontakata koji su označeni od C1 do C8 (Slika 2.3).

  C1 (*VCC*) i C5 (*GND*) kontakti rezervisani su za napajanje čipa koje se obično kreće od 1.8V (klasa C) do 5.5V (klasa A). Naravno, ovi naponi napajanja se mogu razlikovati od napona napajanja tranzistora na čipu čija vrijednost zavisi od naprednosti tehnologije koja je korišćena pri izradi čipa. C2 (*RST*) kontakt služi za slanje reset signala mikroporcesoru kartice, dok C3 (*CLK*) kontakt osigurava ispravan takt rada mikroprocesora kartice i čitača. C6 (*VPP*) je kontakt za napajanje koji se ranije koristio za programiranje kartice, a C7 (*I/O*) služi za transfer podataka. C4 (*RFU*) i C7 (*RFU*) su kontakti rezervisani za inovacije i proširenja u budućnosti.



Slika 2.3 – Raspored kontakata pametne kartice

- ISO/IEC 7816-3 – opisuje električne signale i protokole prenošenja signala između pametne kartice i CAD (*Card Acceptance Device*) uređaja. Veći dio ovog standarda važan je za proizvođače CAD uređaja i za programere koji žele da uspostave komunikaciju sa pametnom karticom shodno ovom standardu. Ovim standardom se deklarišu naponski nivoi, jačine struje i periodi trajanja signala, a opisuju se i osnovni protokoli komunikacije između pametne kartice i čitača.

- ISO/IEC 7816-4 – određuje cijelu logičku strukturu pametne kartice, naredbe, protokole za komunikaciju, a posebno:

    - sadržaj poruka, naredbi i odgovora poslatih od strane CAD uređaja prema kartici i obrnuto
    - strukturu i sadržaj bajtova koje šalje pametna kartica kao odgovor na *reset* signal
    - strukturu datoteka i podataka
    - metode pristupa datotekama i podacima na kartici
    - metode za sigurnu komunikaciju

- ISO/IEC 7816-5 – opisuje brojni sistem za prikaz identifikatora aplikacija, tzv. AID-a (*Application IDentifiers*). Svaki AID se sastoji iz dva dijela. Prvi dio je identifikator registrovanog davaoca aplikacije RID (*Registered Application Provider IDentifier*) koji se sastoji od 5 bajtova koji su jedinstveni. Drugi dio je promjenljive dužine do 11 bajtova koji omogućava RID-u identifikaciju specifične aplikacije.

- ISO/IEC 7816-6 – ovaj dio ISO 7816 standarda opisuje podatke, uključujući kompleksne elemente podataka koji treba da budu kompatibilni kada je u pitanju razmjena podataka. Ovaj standard identifikuje sljedeće karakteristike svakog elementa podatka: identifikator, naziv, opis i referencu, format i kodiranje. Izgled svakog elementa podatka je opisan onako kako se vidi na interfejsu, između interfejsa uređaja i interfejsa pametne kartice.

- ISO/IEC 7816-7 – opisuje strukturalni jezik SCQL (*Structured Card Query Language*) za upite prema kartici i inter-operabilnost komandi različitih proizvođača. Takođe, specificira standardne metode za održavanje i preuzimanje podataka iz baze podataka, a sadrži i definicije formata podataka.

- ISO/IEC 7816-8 – opisuje komande i mehanizme za bezbjednost podataka pametne kartice. Uključuje komande za upravljanje bezbjedonosnim mehanizmima ugrađenim u pametnu karticu, a može još uključiti i tehnike kriptovanja podataka.

- ISO/IEC 7816-9 – opisuje komande i mehanizme za upravljanje pametnim karticama (kontaktnim i beskontaktnim), kao što su npr. izrada i brisanje korisničke datoteke. Ove komande pokrivaju čitav životni vijek kartice, tako da neke komande mogu da se izdaju i prije nego li se kartica personalizuje ili nakon što istekne vijek trajanja kartice. Dodatak ovom dijelu standarda čini opis učitavanja podataka u memoriju kartice, u smislu provjere prava na učitavanje podataka i zaštite unesenih podataka.

- ISO/IEC 7816-10 – opisuje izvor napajnja, snagu, jačinu struje, strukturu i trajanje signala, kao i strukturu ATR odgovora na *reset* u komunikaciji pametne kartice sa nekim drugim uređajem, na primjer terminalom.

- ISO/IEC 7816-11 – provjerava ispravnost ličnih podataka koristeći biometrijske mehanizme implementirane u pametnoj kartici.

- ISO/IEC 7816-12 – opisuje operativne uslove za pametne kartice koje imaju podržan USB-ICC (*Universal Serial Bus – Integrated Circuit Card*) interfejs. Opisani su električni signali, strukture podataka, protokoli A i B za prenos podataka, status i tipovi grešaka, itd.

- ISO/IEC 7816-15 – specificira aplikaciju unutar pametne kartice koja sadrži informacije o kriptografskoj funkcionalnosti. Ovaj dio ISO 7816 standarda definiše uobičajenu sintaksu i format kriptografskih informacija i mehanizama, a podržava sljedeće funkcije pametne kartice: skladištenje mnogobrojnih primjera kriptografskih informacija u kartici, upotrebu i pronalaženje kriptografskih informacija, upotrebu različitih mehanizama autentifikacije, mogućnost ugradnje više kriptografskih algoritama u kartici (pri čemu podjela kriptografskih algoritama i njihova pogodnost nijesu predmet istraživanja ovog standarda).

Pored prethodno navedenih djelova ISO 7816 standarda, postoji još čitava paleta ISO standarda koja reguliše svojstva pametnih kartica. Tim standardima su definisane karakteristike pametne kartice od njene boje i površine do provodnosti materijala od kog je sačinjen čip pametne kartice. Isto tako postoji čitava paleta standarda koja reguliše svojstva čitača pametnih kartica. Takođe, postoje i mnogi ne-ISO standardi među kojima su najpoznatiji već objašnjeni standardi EMV i GSM (Poglavlje II.1), kao i mnogi drugi standardi: PC/SC (*Personal Computer/Smart Card*), HIPAA (*Health Insurance Portability and Accountability Act*), biometrijski ANSI-INCITS (*American National Standard Institute-InterNational Committee for Information Technology Standards*), itd, koji se odnose na definisanje i standardizaciju ove kompleksne problematike [13].

§ II.4 Pametne kartice kao kriptografski uređaji

Da bi sljedeća poglavlja o napadima na hardver pametne kartice (Poglavlje III) i hardverskim mjerama zaštite (Poglavlje IV) bila razumljiva, potrebno je poznavati pojam kriptografskog uređaja. Komponente kriptografskog uređaja mogu biti implementirane ili na razdvojenim čipovima ili na jednom jedinom čipu. Ukoliko su implementirane na razdvojenim čipovima, čipovi moraju biti montirani na PCB (*Printed Circuit Board*) ploči. Odgovarajuća pakovanja za ove čipove su na primjer DIP (*Dual In-line Package*) pakovanje ili PLCC (*Plastic-Leaded Chip Carrier*) pakovanje [14]. Primjer kriptografskih uređaja sa jednim čipom, koji je montiran ispod vidljivih kontakata, upravo su pametne kartice.

Kriptografski uređaji sastoje se iz nekoliko komponenti. Svaka od tih komponenti ima određenu funkciju, kao što su enkripcija podataka ili čuvanje kriptografskih ključeva. Komponente u kriptografskim uređajima se mogu podijeliti u dvije grupe. Komponente prve grupe izvode kriptografske operacije, na primjer digitalna kola koja izvode operacije enkripcije. Komponente druge grupe rukuju podacima kriptografskih operacija, na primjer neizbrisiva NVM (*Non-Volatile Memory*) memorija koja čuva podatak - ključ enkripcije. Neke od najznačajnijih komponenti tipičnog kriptografskog jezgra pametne kartice su [15]:

- *kriptografski softver* – Softverska kriptografska rješenja su ograničena sa stanovišta brzine centralnog procesora računara, efikasnosti prenosa podataka, arhitekture računarskog sistema, operativnog sistema, realizacije sistemskih funkcija i drugih faktora. Rješenja zaštite na nivou softvera posjeduju bezbjedonosne nedostatke, pošto se senzitivne kriptografske funkcije izvršavaju u okruženju potencijalno nebezbjednih operativnih sistema.

- *kriptografski hardver* – Hardverski kriptografski moduli, realizovani u vidu kriptografskih koprocesora, predstavljaju bitnu karakteristiku savremenih rješenja zaštite pametnih kartica. Kriptografski hardver obezbjeđuje zaštitu bezbjednosno kritičnih podataka, kao što su kriptografski ključevi, korisničke šifre i privatni

algoritmi zaštite. Ovo je ujedno i najznačajnija komponenta hardvera pametne kartice, kada su u pitanju analize tehnika *side-channel* napada, kojima će se baviti ova disertacija.

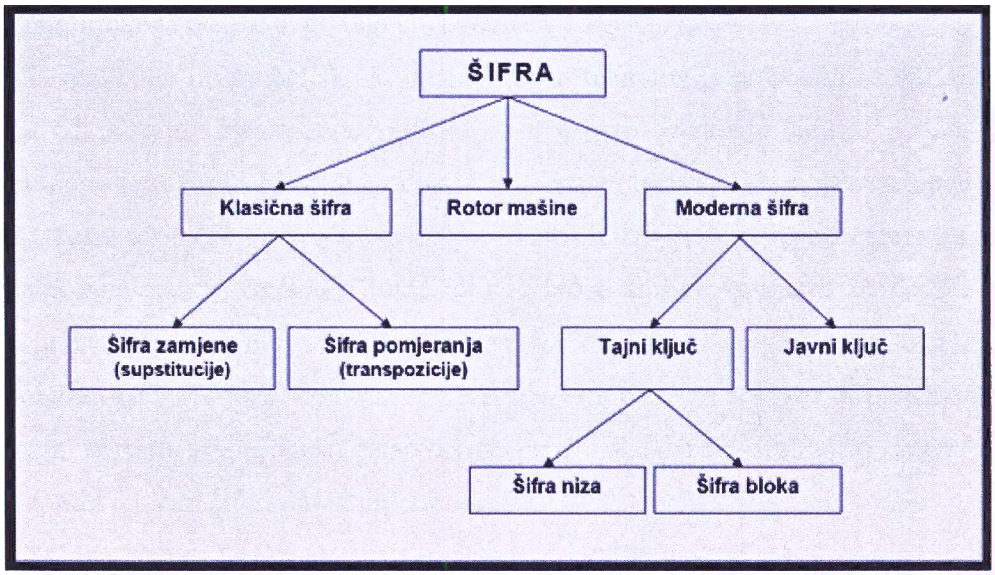
- *memorija* – Hardver pametne kartice posjeduje tri tipa memorije: ROM memoriju, RAM memoriju i NVM memoriju. ROM memorija je namijenjena za smještanje operativnog sistema pametne kartice, a njen kapacitet u pametnim karticama obično iznosi od 4kB do 96kB. RAM memorija služi za privremeno smještanje promjenljivih u toku izvršenja kriptografskih procedura ili rutina operativnog sistema, a njen kapacitet je svega nekoliko kilobajta. NVM memorija se koristi za implementaciju onih memorija čiji se sadržaj pamti i nakon prestanka napajanja pametne kartice, a to su najčešće EEPROM memorije. Za upisani podatak se garantuje trajnost čuvanja zapisa od 10 godina. Ukupan broj upisa na određenu lokaciju je limitiran i iznosi oko 100 000. Vrijeme upisa je znatno duže od vremena čitanja.

- *interfejs* – Ova komponenta obezbjeđuje transfer podataka do i od hardvera pametne kartice. Kriptografske aplikacije implementirane u hardveru pametne kartice nameću posebne zahtjeve interfejsu. Od krucijalnog je značaja da interfejs zaštiti osjetljive podatke, kao što je ključ (šifra) kriptografskog uređaja, od neautorizovanog spoljašnjeg pristupa.

§ II.4.1 Razvoj moderne kriptografije

Da bi razumjeli kako funkcionišu kriptografski uređaji, potrebno je razumjeti način funkcionisanja kriptografskih algoritama. Kriptografija, nauka o sigurnosti podataka, obuhvata široko istorijsko razdoblje – od starih Egipćana do današnjih dana [16]. Prve metode kriptovanja zasnivale su se na šiframa supstitucije, a zatim i na šiframa transpozicije. Današnje metode kriptovanja se po *Kerckhoff*-ovom principu zasnivaju na upotrebi ključa, koji uz pomoć logičkih operacija nad binarnim zapisom podataka kriptuje datu poruku (Slika 2.4).

Ključ je najvažniji dio u kriptovanju i dekriptovanju poruka. Zaštita kriptovane poruke zavisi od zaštite ključa, a ne od zaštite algoritma. U zavisnosti od načina korišćenja ključa, razvile su se dvije klase algoritama - simetrična i asimetrična klasa. Osnovna razlika je u tome da simetrični algoritmi koriste isti ključ za enkripciju i dekripciju neke poruke, ili se ključ za dekripciju može lako izvesti iz originalnog ključa za enkripciju koji mora biti tajan. Sigurnost komunikacije zavisi od toga koliko sigurno učesnici komunikacije čuvaju taj ključ. Asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju poruke, a još se nazivaju i algoritmima sa javnim ključem (*public-key algorithms*) ili algoritmima za razmjenu ključeva. Razlog ovakvom nazivu je taj što je ključ za enkripciju javan, tako da svako može da enkriptuje poruku, ali je ključ za dekripciju tajan (privatan), tako da samo ovlašćeni primalac može dekriptovati poruku.



Slika 2.4 – Podjela kriptografskih algoritama prema upotrebi ključa

Tek su se razvojem računara otvorile mogućnosti implementacije složenih algoritama koji bi bili nezamislivi u doba metoda supstitucije, transpozicije, elektromehaničkih mašina. Prvim većim napretkom u komjuterskom dobu smatra se razvoj IBM-ovog (*International Business Machines*) algoritma Lucifer, 1970. godine pod vođstvom *Dr. Horsta Feistela* [17]. Nacionalni biro za standarde u SAD-u, NBS (*National Bureau of Standards*), uočava potrebu

za standardom zaštite podataka i nakon konsultacija sa Agencijom za nacionalnu bezbjednost u SAD-u, NSA (*National Security Agency*), 15. marta 1973. godine otvara službeni konkurs. Međutim, pokazalo se da nijedna od pristiglih prijava za kandidata nije ispunjavala stroge kriterijume konkursa, pa se otvara novi konkurs 27. oktobra 1974. godine. Na ovom konkursu je IBM prijavio algoritam DEA (*Data Encryption Algorithm*), razvijen na osnovama algoritma Lucifer. Algoritan DEA je 1976. godine proglašen standardom kriptovanja i preimenovan je u DES (*Data Encryption Standard*), pri čemu je njegova službena oznaka glasila FIPS 46. On je reafirmisan kao standard 1983. godine, a zatim uz određena poboljšanja i 1988. godine (FIPS 46-1), 1993. godine (FIPS 46-2), kao i 1999. godine (FIPS 46-3) [18]. Ova posljednja verzija DES algoritma poznata je pod nazivom Triple DES algoritam i ujedno je jedina verzija DES algoritma koju je Nacionalni institut za standarde, NIST (*National Institute for Standards and Technology*), odobrio za kriptovanje povjerljivih vladinih informacija do 2030. godine [19].

Sa razvojem informacijsko-komunikacionih tehnologija pokazalo se da DES više ne može na odgovarajući način zadovoljavati rastuće potrebe zaštite tajnosti podataka. Taj je problem postao kritičan 1990-ih godina kada "na velika vrata" u široku upotrebu ulazi Internet. Zato je 1997. godine NIST pokrenuo inicijativu za pronalaženje korisnije i pouzdanije zamjene za DES. Pri tome, cilj je bio definisati zamjenu za DES koja će se koristiti u svrhe postizanja zadovoljavajućeg stepena informacione sigurnosti u civilnim informatičkim aplikacijama i komunikacijama tijela i institucija državne uprave SAD-a, ali i u nevladinom sektoru. Na taj način će novi enkripcijski standard postati opšti *de facto* standard u SAD-u, ali i u međunarodnim razmjerama.

Na izboru za novi enkripcijski standard 2000. godine za pobjednika je izabran algoritam Rijndael koji je nazvan po prezimenima svojih tvoraca *Vincent Rijmen*-a i *Joan Daemen*-a [20]. Nakon što je izabran da bude zamjena za DES algoritam, preimenovan je u AES (*Advanced Ecryption Standard)* algoritam. AES je zvanično proglašen službenim enkripcijskim standardom u SAD-u, 26. maja 2002. godine, pri čemu je dobio službenu oznaku FIPS 197. Kao takav i danas je važeći. NIST je kao svoje razloge odabira Rijndael-a naveo vrlo dobro ponašanje u hardverskoj i softverskoj implementaciji u različitim uslovima, odličan *key-setup* (pozicija ključa u kriptografskom algoritmu i njegove karakteristike) i niske memorijske zahtjeve. U 2006. godini AES je proglašen za najpopularniji i najčešće korišćeni simetrični algoritam kriptovanja. Precizno govoreći, AES se razlikuje od Rijndael-a jer koristi

fiksnu dužinu bloka od 128 bita, dok Rijndael koristi promjenljivu dužinu bloka od 128, 192 ili 256 bita. Dužina ključa je promjenljiva za oba algoritma (128, 192 ili 256 bita). Za AES standard kriptovanja, pored Rijndael algoritma prijavljeni su sljedeći simetrični algoritmi, nabrojani po abecednom rasporedu: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, SAFER+, Serpent, Twofish.

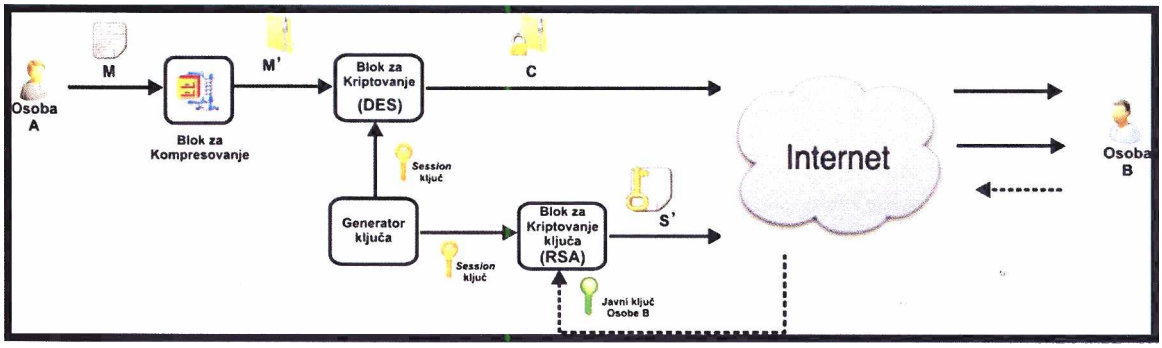
Paralelno sa razvojem simetričnih algoritama razvija se i zamisao o kriptografiji javnih ključeva koju su javnosti predstavili *Whitfield Diffie* i *Martin Hellman* kroz svoj rad "Novi pravci u kriptografiji" koji je objavljen 1976. godine [21]. U to vrijeme je za standard kriptovanja postojao DES sa 64-bitnim ključem. Diffie i Hellman su svoj rad zaključili primjedbom: "Vještina u razbijanju kodova je uvijek bila na strani profesionalaca, ali je inovacija, posebno izumi novih metoda kriptovanja, dolazila od strane amatera."

Inspirisani radom *Diffie*-a i *Hellman*-a, a inače sami u potpunosti početnici u kriptografiji, *Ronald R. Rivest*, *Adi Shamir* i *Leonard M. Adleman* su kreirali RSA algoritam, koji je naziv dobio po inicijalima svojih tvoraca. RSA predstavlja praktični kod sa javnim ključevima koji se mogao koristiti i za kodiranje poruka i za digitalni potpis, a bazirao se na složenosti faktorizacije velikih brojeva [22]. Rad je objavljen 1977. godine u časopisu "Scientific American". U članku u kojem je opisan RSA nalazila se i ponuda da se pošalje potpuna tehnička specifikacija svakome ko pošalje adresiranu kovertu sa plaćenom poštarinom. Došlo je na hiljade takvih koverata iz cijelog svijeta. U Centralnoj obavještajnoj agenciji (*CIA*) u SAD-u je prigovoreno zbog slanja te specifikacije u inostranstvo, pa je distribucija RSA algoritma jedno vrijeme zaustavljena. Tvorci RSA algoritma nijesu bili upoznati sa odredbom o tajnosti patenata, pa su rad objavili prije prijave za međunarodni patent.

Primarna prednost asimetričnih algoritama je ta što se privatni ključ ne mora slati ni pokazivati bilo kome, što nije slučaj kod simetričnih algoritama gdje se tajni ključ mora poslati učesniku komunikacije, što za sobom povlači rizik otkrivanja podataka tokom njihovog slanja. Ova karakteristika za sobom povlači veliko smanjenje broja ukupno potrebnih ključeva. U sistemu u kome komunicira milion korisnika, potrebno je samo dva miliona ključeva, dok bi u slučaju korišćenja simetričnog kriptovanja bilo potrebno bar 500 milijardi ključeva. Dalja prednost asimetričnih algoritama je mogućnost kreiranja digitalnog potpisa. Značajna mana asimetričnih algoritama je ta što su po svojoj prirodi sporiji (oko 100 puta u odnosu na simetrične algoritme), tj. imaju ogromne zahtjeve ka procesorskim

resursima, pa se zato koriste u radu sa manjim izvornim podacima (kratkim porukama). Najpoznatiji asimetrični algoritmi pored RSA algoritma su ElGamal, Diffie-Hellman, KEA (*Key Exchange Algorithm*), RPK (*Raike Public Key*), Rabin, Blum-Goldwasser, Menezes-Vanstone.

Imajući u vidu da upotreba simetrične i asimetrične kriptografije pati od izvjesnih nedostataka, javlja se potreba za sistemima koji kombinuju najbolje pojedinačne karakteristike oba sistema - hibridni kriptosistemi. Princip rada ovih sistema se ogleda u sljedećem: izvorni tekst se kriptuje generisanim ključem simetričnog algoritma (prethodno je u nekim slučajevima poželjno izvršiti i dodatnu kompresiju, ukoliko se radi o velikom dokumentu), a zatim se generisani ključ kriptuje primaočevim javnim ključem. Postupak dekripcije cijele poruke se ostvaruje obrnutim redosljedom operacija: primalac prvo dekriptuje poruku pomoću svog tajnog ključa i na taj način pronalazi simetričan ključ koji koristi da bi poruku vratio u svoj izvorni oblik. Za generisanje simetričnog (*session*) ključa koristi se generator pseudo-nasumičnih brojeva u kombinaciji sa raznim korisnikovim unosima u toku procesa generisanja. Na ovaj način se postižu zavidne performanse sistema za kriptovanje, jer se asimetrično kriptuje samo kratak simetrični ključ, a ne cijela, velika poruka. Primjer uspješnog hibridnog kriptosistema je PGP (*Pretty Good Privacy*) programski paket [23] za kriptovanje podataka koji je formirao *Phill Zimmerman* 1991. godine (Slika 2.5).



Slika 2.5 – Postupak kriptovanja pomoću PGP algoritma [24]

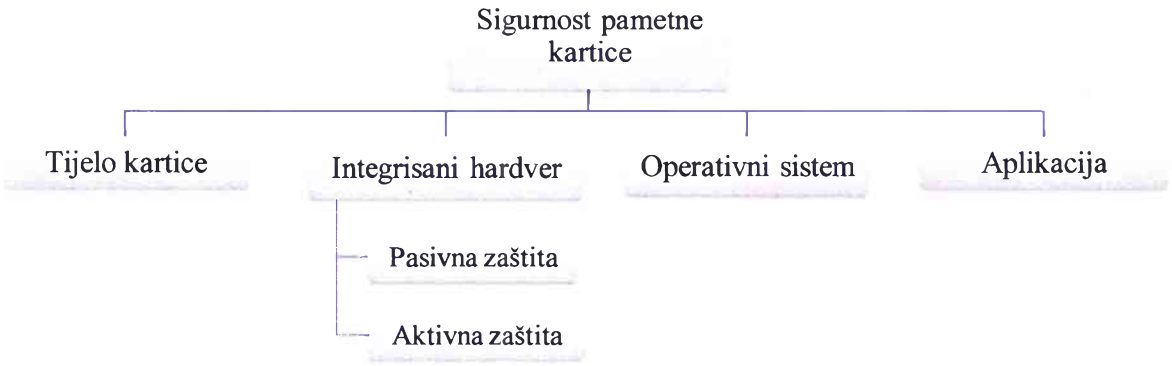
§ II.5 Zaključci

U ovom poglavlju hronološki je prikazan razvoj pametnih kartica i područja njihove primjene. Izvršena je podjela pametnih kartica prema vrsti čipa, kao i prema načinu prenosa podataka i mehanizmu pristupa. Objašnjeni su djelovi ISO 7816 standarda, koji definišu najvažnije karakteristike pametnih kartica, kao što su dimenzije pametne kartice, materijal od koga je napravljena pametna kartica, otpornost pametne kartice na spoljašnje uticaje, dimenzije, funkciju i lokaciju kontakata na pametnoj kartici, električne signale i protokole prenošenja signala između pametne kartice i čitača, itd.

Kriptografski uređaj definisan je kroz neke od najznačajnijih komponenti tipičnog kriptografskog jezgra: kriptografski softver, kriptografski hardver, memorija i interfejs. U cilju boljeg razumijevanja kriptografskog uređaja, prikazan je način funkcionisanja kriptografskih algoritama. Takođe, izvršena je podjela kriptografskih algoritama u zavisnosti od načina upotrebe ključa. Navedene su osnovne razlike između simetričnih i asimetričnih algoritama, kao i njihove prednosti i mane. Objašnjeni su i sistemi koji kombinuju najbolje pojedinačne karakteristike oba sistema - hibridni kriptosistemi.

III Side-channel napadi na hardver pametne kartice

Najvažnije svojstvo pametne kartice je da obezbijedi sigurno okruženje za podatke i ugrađene programe. Kada se ne bi zahtijevao dovoljno značajan trud da se pročitaju podaci sa pametne kartice, ona se ne bi mnogo razlikovala od diskete. Gotovo je nemoguće konfigurisati kompletan sistem (pametnu karticu) tako da ima savršenu sigurnost protiv raznih tipova napadača i napada. Četiri komponente definišu sigurnost pametne kartice (Slika 3.1). Prva komponenta je *tijelo kartice* (*card body*) u kojoj je usađen mikrokontroler. Bezbjednosne karakteristike koje se nalaze na tijelu kartice nijesu vidljive isključivo primjenom odgovarajućih čitača pametnih kartica, već i ljudskim okom. To u principu nije karakteristika pametnih kartica, ali je karakteristika ostalih tipova kartica. Preostale sigurnosne komponente: *integrisani hardver* (*chip hardware*), *operativni sistem* (*operating system*) i *aplikacija* (*application*) štite podatke i programe koji se nalaze u mikrokontroleru pametne kartice [25].



Slika 3.1 – Klasifikacija komponenti sigurnosti pametne kartice

Bezbjednost pametne kartice zagarantovana je samo ukoliko su sve komponente prisutne, a njihovi mehanizmi odbrane funkcionišu ispravno. Ako se pametna kartica koristi u okruženju gdje nije izložena vlasničkoj verifikaciji, komponenta *tijelo kartice* nije obavezna. Ostale tri komponente koje su nezavisne od tijela kartice, neophodne su u pogledu fizičke i

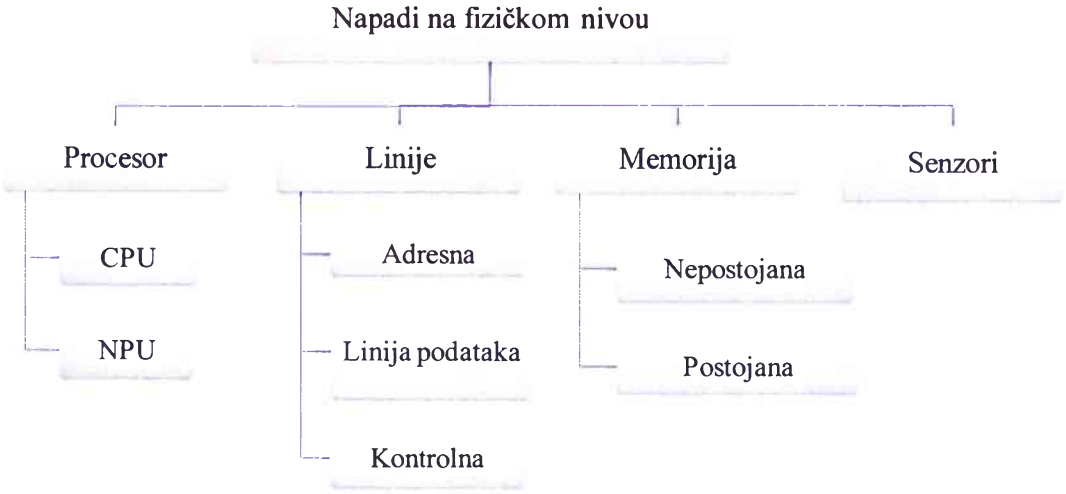
logičke sigurnosti pametne kartice u odnosu na napade. Ako bilo koja od ovih komponenti ne ispuni postavljene zahtjeve, pametna kartica više nije sigurna, s obzirom na to da su ove tri komponente spregnute logičkom AND relacijom. Činjenica da je pametnu karticu potrebno zamijeniti novom nakom isteka roka validnosti, pruža mogućnost proizvođačima pametnih kartica da se upoznaju sa posljedicama aktuelnih napada na iste i na taj način ugrade u narednoj generaciji pametnih kartica naprednije mjere zaštite.

§ *III.1 Klasifikacija napada na pametne kartice*

Postoji nekoliko različitih pristupa sistematičnoj klasifikaciji napada na pametne kartice [26], ali cilj je uvijek isti - otkriti skrivene ključeve (*secret keys*) unutar kriptografskih uređaja. Jedan od ovih pristupa razlikuje napade na socijalnom, fizičkom i logičkom nivou. U praksi takođe postoje i napadi koji predstavljaju različite kombinacije pomenutih. Na primjer, napad na fizičkom nivou može da pripremi realne uslove i sredstva za napad na logičkom nivou, što je slučaj sa diferencijalnim napadom baziranim na analizi grešaka (*differential fault analysis attack*).

Napadi na pametne kartice na socijalnom nivou su napadi koji su primarno usmjereni ka ljudima koji rade sa pametnim karticama: čip i softver dizajnerima koji rade za proizvođače pametnih kartica ili dalje u životnom ciklusu kartice – vlasnicima pametnih kartica. Ovi napadi baziraju se na organizacionim mjerama, a mogu uključivati dijelom i tehničke mjere.

Napadi na pametne kartice na fizičkom nivou zahtijevaju tehničku opremu (mikroskop, laserski rezač, mikromanipulatori, hemijska oprema za rezanje) iz razloga što je neophodno omogućiti fizički pristup hardveru mikrokontrolera pametne kartice (Slika 3.2). Ovi napadi mogu biti statički, što podrazumijeva da se ne vrši napajanje mikrokontrolera, ili dinamički, kada mikrokontroler djeluje. Za vrijeme statičkog napada ne postoji vremensko ograničenje u okviru koga napadač mora izvršiti napad, za razliku od dinamičkog napada kada je neophodno da napadač ima dovoljno brzu i kvalitetnu opremu za dobijanje i procjenjivanje podataka.



Slika 3.2 – Klasifikacija meta napada na fizičkom nivou na mikrokontroler pametnih kartica

Najefikasnija grupa napada je na logičkom nivou. Primjer logičkog napada je tzv. napad grubom silom (*brute force attack*) - metoda probijanja kriptografskog algoritma sistematskim pokušavanjem velikog broja mogućih ključeva [27]. Ovaj napad je postao poznat nakon probijanja 56-bitnog DES algoritma 1998. godine, za šta je mašini napravljenoj da odradi ovaj napad (tzv. *Deep Crack*) bilo potrebno nešto više od 4 dana. Smatra se da je 128-bitni ključ dovoljno siguran od *brute force* napada na simetrične kriptografske algoritme. Naime, u slučaju 128-bitnog ključa svaka od 2^{128} kombinacija mora biti isprobana. Iako bi rješenje vjerovatno bilo pronađeno nakon što bi se isprobalo pola od mogućih kombinacija, s obzirom na red veličine u kojem je izraženo potrebno vrijeme da bi računar isprobao sve moguće kombinacije, to ne igra veliku ulogu.

Logički napadi uključuju i napade koji eksploatišu razne greške u operativnom sistemu pametne kartice ili trojanske konje u izvršnom kodu aplikacije pametne kartice, kao i kriptoanalitičke napade. Naime, vremenom su se metode i tehnike na bazi kriptoanalize drastično promijenile, odnosno uznapredovale uporedo sa sve složenijim metodama zaštite kriptografskih algoritama. Probijanje kriptografskog algoritma označava da je poznat postupak otkrivanja tajnih informacija (ključeva) koje se mogu iskoristiti za dekripciju

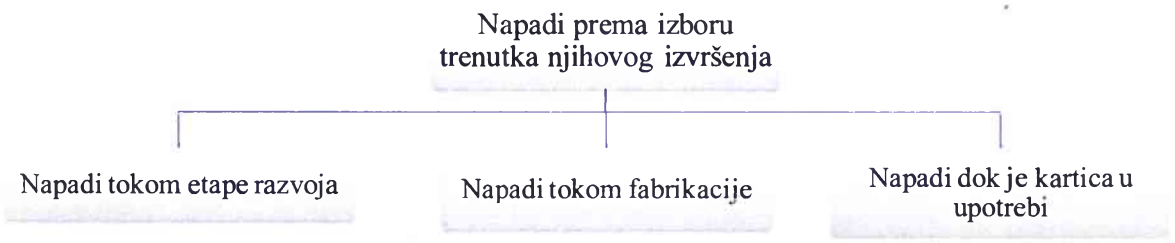
kriptovane poruke. Kriptoanaliza se može sprovesti nagađanjem ključa ili korišćenjem informacija o sistemu koji se napada. Osnovne vrste kriptoanalize uključuju:

- samo kriptovani tekst (*cyphertext*) – napadač ima pristup samo skupini kriptovanih poruka,
- poznati nekriptovani tekst (*known-plaintext*) – napadač ima skupinu kriptovanih poruka za koje poznaje odgovarajuće izvorne poruke,
- izabrani (ne)kriptovani tekst (*chosen-plaintext/ciphertext*) – napadač može otkriti (ne)kriptovane poruke koje odgovaraju skupini (ne)kriptovanih poruka po njegovom vlastitom izboru,
- prilagodljivi izabrani nekriptovani tekst (*adaptive chosen-plaintext*) – poput prethodnog, osim što napadač može izabrati sljedeću nekriptovanu poruku na temelju informacija koje je prikupio u prethodno opisanom načinu dekripcije,
- napad odgovarajućim ključem (*related-key attack*) – poput izabranog (ne)kriptovanog teksta, osim što napadač može otkriti kriptovane poruke kriptovane pomoću dva različita ključa. Pri tome, ključevi nijesu poznati napadaču, ali poznat je odnos među njima.

Sljedeći način klasifikacije napada na pametne kartice je prema izboru trenutka kada će se izvršiti napad. Prema fazama životnog ciklusa pametne kartice, koje su definisane prema ISO standardu 10202-1 [28], izvršena je klasifikacija napada u odnosu na tri intervala: razvoj, proizvodnja i upotreba kartice (Slika 3.3). Napadi za vrijeme razvoja pametne kartice odnose se na dizajn sistema, razvoj čipa, razvoj operativnog sistema i generaciju aplikacija. Izraz "proizvodnja" koristi se u kontekstu generalno svih procesa koji učestvuju u proizvodnji hardvera. To pokriva cijeli asortiman procesa počev od fabrikacije tankih pločica poluprovodnog materijala (*wafer*) od strane proizvođača pametnih kartica do personalizacije pametnih kartica i njihovog slanja vlasnicima. Upotreba kartice odnosi se na period kada se pametna kartica nalazi "u rukama" vlasnika.

Dalja klasifikacija napada na pametne kartice karakteristična za mikroprocesorske pametne kartice i ostale čip-kartice podrazumijeva invazivne (*invasive*), poluinvazivne (*semi-invasive*) i neinvazivne (*non-invasive*) napade [29].

- Invazivni (aktivni) napadi su najjača grupa napada koja zahtijeva da se mikroprocesor ukloni iz pametne kartice i direktno napadne na fizički način. Ova klasa napada može, makar u teoriji, ugroziti sigurnost bilo kog sigurnog mikroprocesora. Ovi napadi podrazumijevaju skupocjenu opremu kako bi se bezbjedno izdvojio čip iz kartice i zahtijevaju relativno veliko vrijeme da bi se dobili traženi rezultati. Iz tog razloga se smatra da su ovi napadi najčešći i najrealniji u domenu proizvođača pametnih kartica i istraživača u vrhunski opremljenim laboratorijama. Primjer jednog ovakvog napada mogao bi se realizovati postavljanjem sondi na linijama među blokovima čipa, nakon čega bi napadač posmatranjem informacija koje se šalju od bloka do bloka, mogao da otkrije skrivenu informaciju. Svega nekoliko radova postoji na temu invazivnih napada, a među najznačajnijima su [30], [31] i [32].

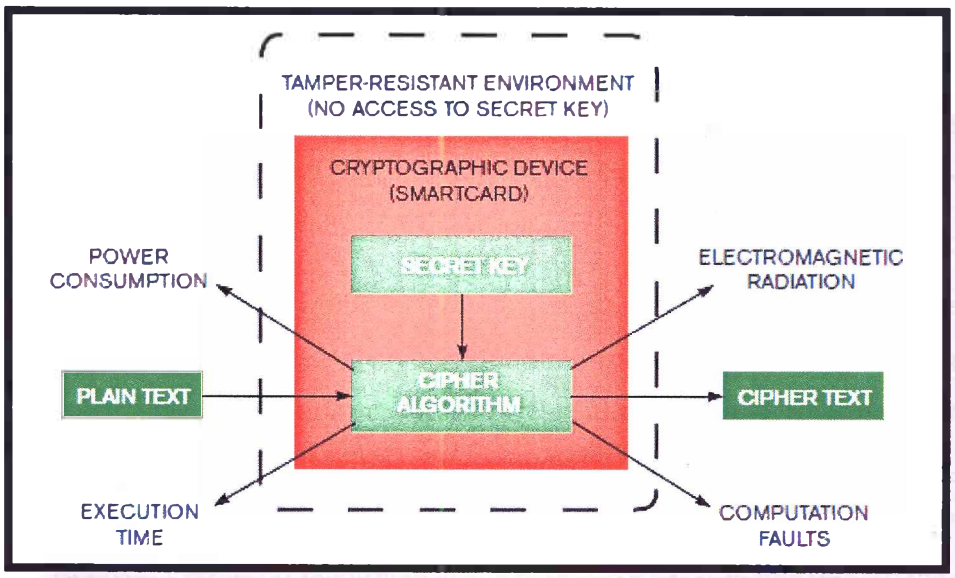


Slika 3.3 – Klasifikacija "tajminga" mogućih napad

- Poluinvazivni napadi zahtijevaju od pametne kartice da površina čipa bude dostupna napadaču koji će pokušati da ugrozi sigurnost kartice bez direktnog modifikovanja čipa. Cilj ovih napada je obično iščitavanje sadržaja memorijskih ćelija i uspješan napad na ovu temu publikovan je u [33]. Svakako, cilj poluinvazivnih napada je da se izazovu greške u kriptografskom uređaju. Primjer poluinvazivnog napada je analiza elektromagnetnog zračenja korišćenjem specijalne sonde, ili pak izazivanje grešaka u izvršenju algoritma pomoću laserskog ili bijelog svijetla [34]. Poluinvazivni napadi ne zahtijevaju tako skupocjenu opremu kao invazivni napadi. Međutim, opet je potreban relativno ogroman napor da bi se izveo jedan ovakav napad. Jedan od

komplikovanijih zadataka u poluinvazivnim napadima predstavlja lociranje tačne pozicije za izvršenje napada na površini pametne kartice i zahtijeva veliko vrijeme i iskustvo. Najrazumljivija publikacija na temu poluinvazivnih napada predstavlja doktorska teza *Skorobogatov*-a [32].

- Neinvazivnim (pasivnim) napadima napadač dolazi do skrivene informacije analizom izmjerene fizičke veličine: snaga disipacije, dinamičke struje, struje curenja, vrijeme izvršavanja algoritma, elektromagnetno zračenje, itd, ali pritom ne uzrokuje nikakve modifikacije na pametnoj kartici, tj. sigurnosni mikroprocesor i tijelo pametne kartice oboje ostaju netaknuti (Slika 3.4). Ovi napadi se još popularno zovu i *side-channel* napadi, jer eksploatišu informaciju koja "curi" iz kriptografskog uređaja u toku izvršavanja algoritma. Većina neinvazivnih napada se može izvršiti uz pomoć opreme koja je relativno jeftina, pa iz tog razloga ova vrsta napada predstavlja najveću realnu prijetnju sigurnosti kriptografskih jezgara pametnih kartica.



Slika 3.4 – *Side-channel* informacija [35]

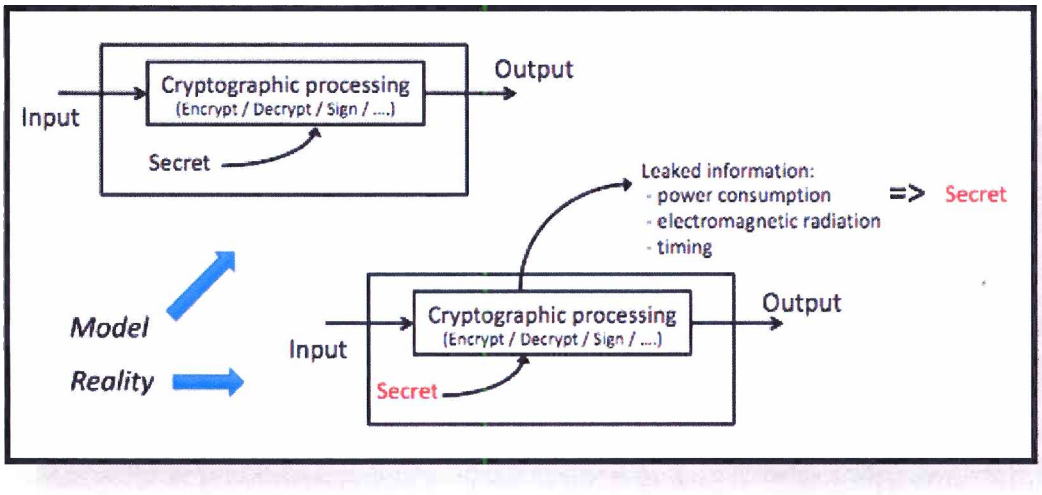
§ III.2 Opis side-channel napada

Oblast kriptografije ima viševjekovnu istoriju. Algoritmi i protokoli se formulišu i reformulišu kako bi se izborili za povjerljivost i integritet podataka, autentifikaciju entiteta i autentifikaciju poruka. Oblast klasične kriptoanalize koristi matematičke tehnike za razbijanje kriptografskih struktura, međutim sa *Kocher*-ovom publikacijom iz 1996. godine [36] gdje se prvi put pominju *side-channel* napadi, postalo je jasno da nije dovoljno obezbijediti teorijsku sugurnost ugrađenih algoritama, već je od velike važnosti i sigurnost njihove implementacije.

Side-channel napadi su najefikasnija klasa napada na kriptografski hardver pametnih kartica u posljednjoj deceniji [37], [38]. Ovi napadi eksploatišu činjenicu da fizičke veličine koje je moguće izmjeriti van pametne kartice i koje se zovu *side-channel* informacije, zavise od tajnog ključa (*secret key*) unutar kriptografskog uređaja. Ovo svakako ne znači da je moguće direktno otkriti tajni ključ mjereći side-channel informaciju. Uglavnom se u side-channel napadu izlazna vrijednost iz "bočnog kanala" koristi kako bi izračunavanje ključa bilo kompjuterski izvodljivo. Nekad se može desiti da je rezultat *side-channel* napada sveden na uži izbor mogućih vrijednosti ključa i u tom slučaju ključ se nalazi izvođenjem već pomenutog, direktnog nasumičnog napada (*brute-force attack*).

Osnovna ideja *side-channel* napada je da se svo raspoloživo znanje o hardveru pametne kartice iskoristi za građenje modela *side-channel* izlaza iz kriptografskog uređaja. To znanje obično podrazumijeva informacije o implementiranom kriptografskom algoritmu, kao i znanje o tehnologiji koja je korišćena za integrisanje kriptografskog hardvera. Napad je uspješniji što je napadač bolje postavio model *side-channel* izlaza. Generalno ne bi trebalo da predstavlja problem saznati u kojoj je tehnologiji hardver izrađen, kao ni koji je kriptografski algoritam implementiran, jer se te informacije mogu naći u knjizi sa specifikacijama koju publikuje prozvođač pametnih kartica. Ovakve knjige često sadrže i druge informacije koje mogu biti od koristi za napadača. Na primjer, bilo kakva informacija o arhitekturi uređaja pomaže napadaču da unaprijedi svoj model *side-channel* izlaza. Ta informacija može biti neki od parametara dizajna poput veličine registara ili protok podataka. Takođe, model *side-*

channel izlaza koji kreira napadač ne mora biti visoko sofisticiran i komplikovan. Naprotiv, u do sada publikovanim napadima ovi modeli imaju krajnje jednostavnu formu. Za bilo koji model koji se može iskoristiti u *side-channel* napadu, obavezno je da jedan od ulaznih parametara modela bude ključ ili neki segment ključa. Činjenica da izlaz napadačevog modela zavisi od ključa je upravo njegova najvažnija osobina. Ova zavisnost između izlaza i ključa unutar modela treba da bude jednaka zavisnosti između fizičkog (stvarnog) *side-channel* izlaza i ključa koji je smješten u kriptografskom uređaju, pri istim ulaznim podacima (Slika 3.5).



Slika 3.5 – Građenje stvarnog modela *side-channel* izlaza [39]

Pošto je napadač konstruisao model *side-channel* napada i uvjerio se da poznaje sve potrebne parametre za napad, može početi sa izvršenjem samog napada. Koraci jednog takvog napada šematski su prikazani na Slici 3.6.

Da bi se otkrio ključ u kriptografskom uređaju napadač pravi hipotezu o ključu ili dijelu ključa, nakon čega treba utvrditi da li je hipoteza ispravna ili ne. Obično je takva hipoteza vezana za *Hamming*-ovu težinu dijela ključa ili pak za vrijednost određenih bitova ključa, iako hipoteza ključa nije limitirana na ove karakteristike. Inače, *Hamming*-ova težina nekog niza predstavlja ukupan broj simbola koji su različiti od nule, a tipičan slučaj je niz

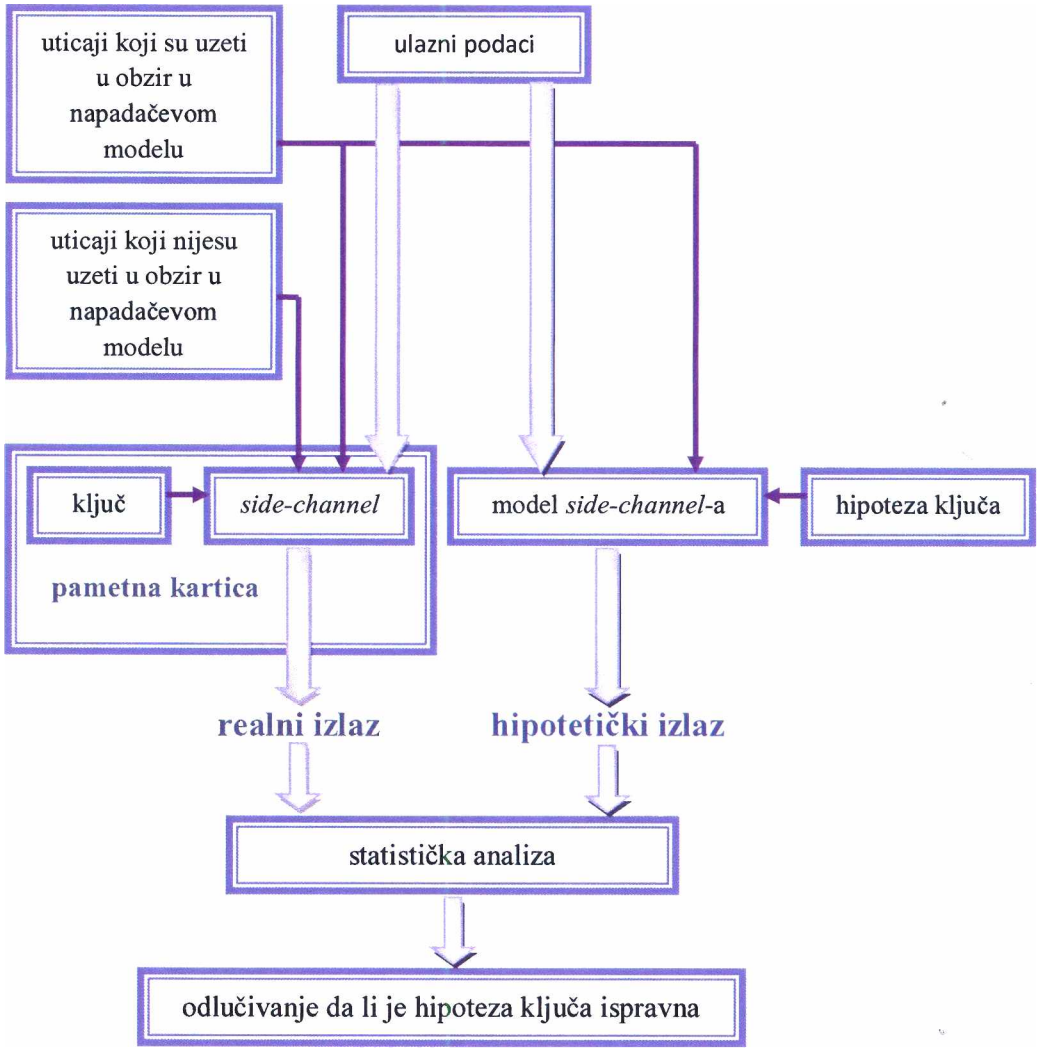
bitova gdje *Hamming*-ova težina označava broj jedinica. Pored pojma *Hamming*-ove težine, često se koristi i pojam *Hamming*-ove udaljenosti (*Hamming distance*) koja kod dva niza jednake dužine predstavlja broj pozicija u kojima su odgovarajući simboli različiti. U teoriji informacija i kodova upotrebom gore navedenih pojmova mogu se definisati uslovi koje određeni kod (npr. *Hamming*-ov kod) mora zadovoljiti kako bi se koristio za detekciju i korekciju greške pri prenosu poruka.

Dakle, kako bi se utvrdila tačnost hipoteze napadač će upotrijebiti svoj model *side-channel* izlaza i stvarni *side-channel* izlaz iz kriptografskog uređaja. Osnovna ideja napada sastoji se iz sljedećih koraka:

- izmjeriti *side-channel* izlaz iz uređaja,
- izračunati hipotetički *side-channel* izlaz, koristeći konstruisani model *side-channel* napada i hipotezu ključa zajedno sa svim ulaznim parametrima koje napadač poznaje.

Ono što napadač dobija na ovaj način su pravi *side-channel* izlaz iz uređaja i hipotetički *side-channel* izlaz dobijen korišćenjem modela *side-channel* napada koji je osmislio sam napadač. Svakako, samo poređenjem ove dvije vrijednosti napadač ne može dobiti odgovor da li je hipoteza ključa tačna ili ne. Potrebno je izračunati *side-channel* izlaze koristeći već konstruisani model *side-channel* napada, ali za alternativnu vrijednost ključa. Alternativna hipoteza ključa je ništa drugo do hipoteza da ključ nema vrijednost koju je imao u prethodno upotrijebljenoj hipotezi ključa. Na primjer, napadač može napraviti hipotezu da dva najniža bita ključa imaju vrijednost 11. Alternativna hipoteza ključa bi bila da dva najniža bita ključa imaju vrijednosti 00, 01 ili 10. Koristeći model s*ide-channel* napada potrebno je izračunati hipotetičke *side-channel* izlaze za ove tri vrijednosti ključa. Važno je shvatiti da je alternativna hipoteza ključa kompleksnija ukoliko je više alternativa prvobitnoj hipotezi ključa. Ako se hipoteza ključa sastoji iz N bita, onda se alternativna hipoteza ključa sastoji od $2^N - 1$ kombinacija nula i jedinica koje se mogu pojaviti u binarnoj riječi od N bita, isključujući samu hipotezu ključa. Tek nakon što je napadač izmjerio pravu vrijednost *side-channel* izlaza iz uređaja kao posljedicu napada, a zatim izračunao i izlazne vrijednosti modela *side-channel* napada bazirane na hipotezi ključa i alternativnoj hipotezi ključa, napadač može početi da provjerava da li je hipoteza ključa ispravna. Poređenje stvarnog *side-channel* izlaza sa izlazima baziranim na hipotezi ključa i alternativnoj hipotezi ključa vrši se

statističkim diferencijalnim metodama. Razlog tome je što se u praksi model *side-channel* napada pokazuje prilično nesavršenim, jer ne uzima u obzir mnogobrojne uticaje na stvarni *side-channel* izlaz iz uređaja (npr. razni oblici električnog šuma). Prema tome, jednostavno poređenje izmjerenog *side-channel* izlaza iz uređaja i *side-channel* izlaza napadačevog modela *side-channel* napada nije moguće.



Slika 3.6 – Šematski prikaz izvršnih koraka *side-channel* napada

Različite statističke metode koje se koriste u *side-channel* napadima gotovo uvijek zahtijevaju od napadača da izmjeri *side-channel* izlaz iz kriptografskog uređaja više puta. Što

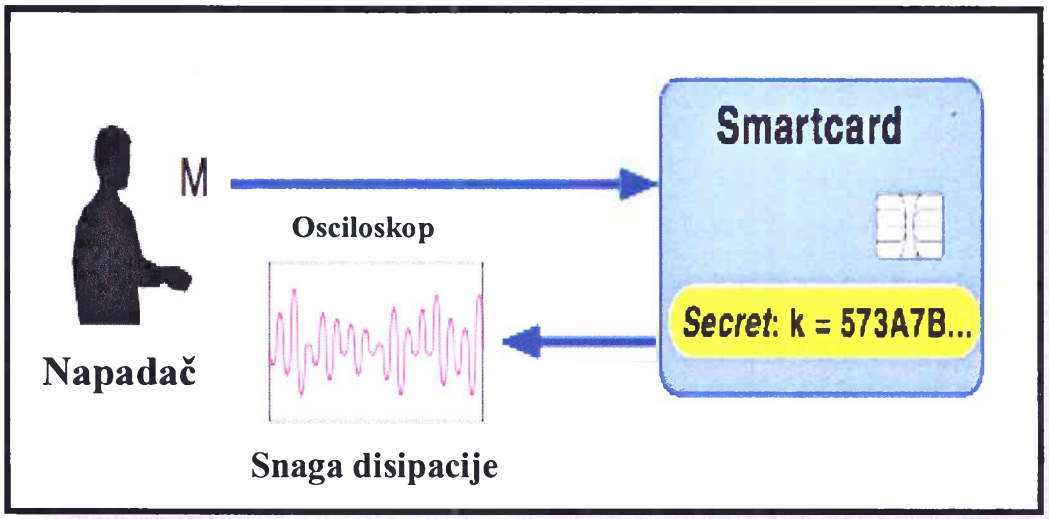
je više mjerenja izvršeno, statističke metode korišćene u napadu više pomažu da se kompenzuju aproksimacije koje je napadač napravio u svom modelu napada. *Side-channel* napad smatra se uspješnim ukoliko je napadač uspio da otkrije ključ unutar kriptografskog uređaja sa razumnim brojem mjerenja *side-channel* izlaza iz kriptografskog uređaja.

§ III.2.1 Power Analysis Attacks

Do ovog trenutka najefektniji *side-channel* napadi, ostvareni u praksi i publikovani u ogromnom broju su napadi bazirani na analizi utrošene snage kriptografskog uređaja, tzv. PAA (*Power Analysis Attacks*). Snaga digitalnih kola je izuzetno bitna tema. Disipacija snage determiniše da li čip treba da se rashladi ili ne, determiniše tip napajanja, a u slučaju kriptografskih uređaja determiniše da li uređaj može biti napadnut ili ne. Mogućnost izvođenja PAA napada po prvi put pominje *Kocher* u svom radu, koji se zapravo bavi analizom napada baziranih na analizi vremena izvođenja određenih kriptografskih operacija [40]. Naime, *Kocher* naglašava da lažna izvršavanja dodata kriptografskom algoritmu u vidu praznih petlji (*empty loops*) istovremeno mogu biti dobra protivmjera napadima baziranim na analizi vremena, ali i laka meta napadima baziranim na analizi snage. Razlog tome je što prikupljeni tragovi snage će se izuzetno razlikovati za djelove algoritma koji predstavljaju prazne petlje i stvarne kriptografske operacije, pa napadaču neće biti teško da razdvoji ove segmente i na taj način iskoristi tragove snage upotrebljivog dijela algoritma za PAA napade.

U *New York Times*-u 1998. godine predstavljeni su novi rezultati *Kocher*-ovog istraživanja vezanog za napade bazirane na analizi snage kriptografskih uređaja [41]. Jedan od zapanjujućih rezultata naznačio je da je za neke kriptografske uređaje, prikupljeni trag snage samo jedne kriptografske operacije dovoljan da bi se otkrila vrijednost čitavog ključa usađenog u hardveru pametne kartice. *Kocher* i njegov tim su došli do još značajnijeg zaključka – ispitujući po jedan prikupljeni trag za svaku od 1000 testiranih pametnih kartica uspjeli su da otkriju skriveni ključ (*secret key*) svake od njih. Pošto je *Kocher* objavio sve tehničke detalje ovih otkrića [42], postalo je jasno da napadi bazirani na analizama snage predstavljaju ozbiljnu prijetnju sigurnosti hardvera pametnih kartica (Slika 3.7).

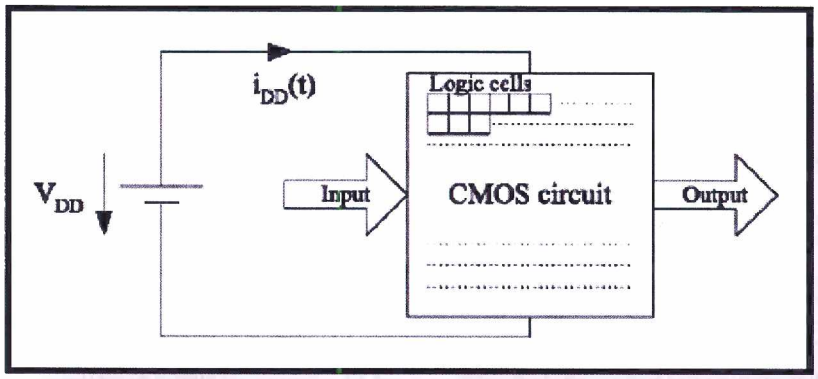
U cilju boljeg pojašnjenja koncepta napada zamislimo kriptografske elektronske uređaje koji crpe struju iz izvora napajanja tokom određene operacije. Intenzitet struje zavisi od putanje koju struja prati u uređaju, tj. od složenosti kriptografske operacije. Da bi se snimio strujni tok, koristi se tzv. *sniffer*, uređaj koji se ponaša kao standardni čitač pametnih kartica, ali koji osim što napaja karticu, vrši konverziju struje napajanja u napon koji se može prikazati na osciloskopu. Obično je napon napajanja pametne kartice konstantan, pa je razlika između napada baziranih na analizi snage i napada baziranih na analizi struje konstantan faktor. U daljem dijelu rada, u poglavljima V, VI i VII, biće posebno analizirani napadi bazirani na analizi struje curenja kriptografskog jezgra, kao i mjere zaštite hardvera protiv tih napada.



Slika 3.7 – Napad baziran na analizi snage hardvera pametne kartice [43]

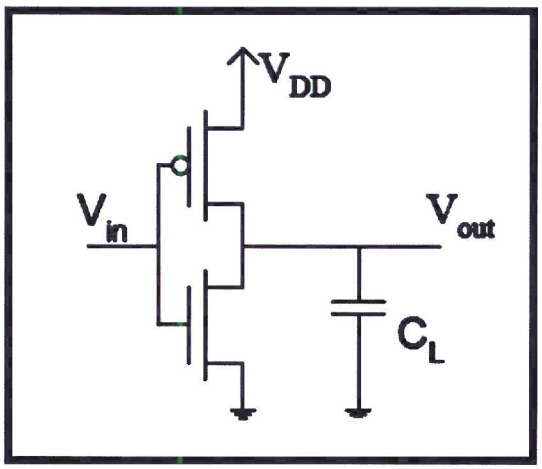
Hardver većine pametnih kartica je implementiran u CMOS (*Complementary Metal-Oxid-Silicon*) tehnologiji, a struje i disipaciju snage kriptografskog uređaja je najlakše objasniti na primjeru CMOS invertora koji je reprezentativan i za ostala CMOS kola. Razlikujemo dinamičku disipaciju snage invertora koja nastaje zbog prelaznih struja, kao i

zbog punjenja i pražnjenja parazitnih kapacitivnosti i statičku disipaciju snage invertora koja nastaje zbog struja curenja (Slika 3.8) [44].



Slika 3.8 – Disipacija snage u CMOS kriptografskom uređaju [45]

Dva su glavna uzroka relativno velikoj dinamičkoj disipaciji snage: postojanje direktne struje od V_{DD} do mase tokom trajanja prelaznog procesa kada oba MOSFET-a provode i struja koje potiču od punjenja i pražnjenja izlaznih parazitnih kapacitivnosti. Na taj način imamo ukupnu dinamičku snagu disipacije invertora koja se sastoji od: P_{dp} (oko 15% ukupne dinamičke *disipacije* snage) i P_{dyn} (oko 85% ukupne dinamičke disipacije snage), respektivno.



Slika 3.9 –CMOS invertor

Istorijski, primarni doprinos disipaciji snage u CMOS kolima pripisivan je punjenju i pražnjenju parazitnih kapacitivnosti, tj. dinamičkoj disipaciji snage. Međutim, sa novim tehnologijama čije su širine kanala od 90nm i manje, povećava se uticaj statičke disipacije na potrošnju i performanse dizajna. To omogućava napade na hardver pametnih kartica bazirane na analizi struja curenja koja protiče kroz zakočeni mosfet: kada je vrijednost ulaznog signala V_{in} logička 0 provodi P-kanalni MOSFET invertora, a N-kanalni MOSFET je zakočen, dok je situacija obrnuta kada je V_{in} logička 1 (Slika 3.9). Ukupnu snagu disipacije CMOS invertora računamo kao sumu statičke i dinamičke disipacije snage [46] :

$$P = P_{stat} + P_{dp} + P_{dyn} = V_{DD} I_{leak} + V_{DD} I_{peak} \frac{t_r + t_f}{2} f + C_L V_{DD}^2 f \qquad (3.1)$$

U ovoj jednačini t_r i t_f predstavljaju uzlazno (*rise)* i silazno (*fall)* vrijeme ulaznog signala, tj. označavaju brzinu promjene signala na ulazu invertora, f je učestanost signala koja se dovodi na ulaz invertora, I_{leak} je struja curenja, I_{peak} je dinamička struja, C_L je vrijednost izlazne kapacitivnosti.

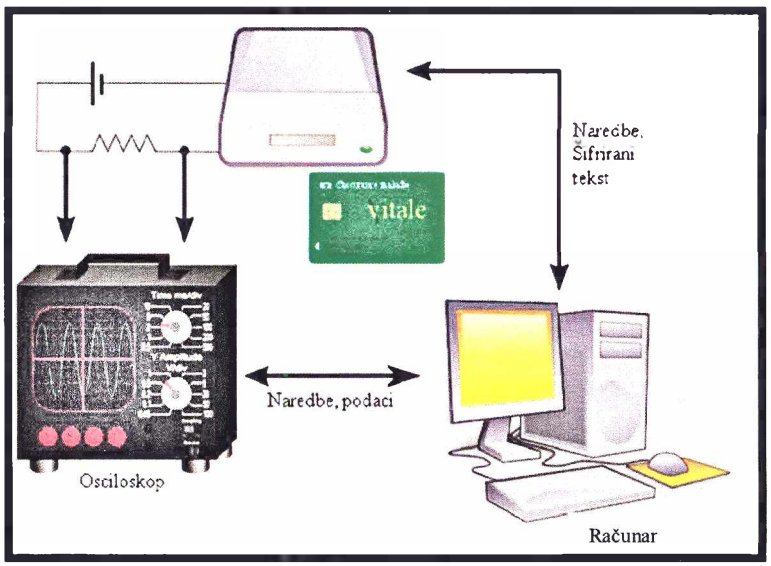
Ukupna disipacija snage u kriptografskim uređajima zavisi od broja logičkih ćelija i kola u uređaju, konekcija među njima i činjenice na koji način su te ćelije i kola izgrađeni. Ove karakteristike su rezultat odluka o dizajnu na sistemskom nivou (ukupna sistemska arhitektura, upotrijebljeni algoritmi, *hardware/software* razdvajanje, itd.), arhitektonskom nivou (specifična implementacija hardverskih ili softverskih komponenti), ćelijskom nivou (dizajn logičkih ćelija), tranzistorskom nivou (poluprovodnička tehnologija upotrijebljena za implementaciju MOS tranzistora u logičkim ćelijama).

Oprema za izvođenje napada baziranih na analizi snage kriptografskog uređaja obično se sastoji od nekoliko komponenti koje su međusobno povezane (Slika 3.10) [45].

Komponente koje sadrži mjerna oprema (*measurment setup*) su:

- *kriptografski uređaj* – Ovo je uređaj pod napadom. Obično ima interfejs za komuniciranje sa PC-em. Ovaj interfejs se može iskoristiti za slanje komandi uređaju od strane PC-a, nakon čega uređaj enkriptuje poslate podatke i vraća rezultate nazad PC-u.

- *generator takta* (*clock generator*) – Kriptografski uređaji se napajaju eksternim generatorom takta. Pametne kartice se napajaju taktom brzine do 4MHz.
- *izvor napajanja* – Kriptografski uređaji se napajaju i eksternim izvorom napajanja. Napajanje pametnih kartica vrši čitač pametnih kartica. Takav jedan čitač obično obezbjeđuje napajanje od 5V, 3V ili 1.8V umetnutoj pametnoj kartici.
- *mjerno kolo ili EM (electromagnetic) sonda* – Disipacija snage kriptografskog uređaja se može mjeriti direktno, ubacivanjem mjernog kola između izvora napajanja i kriptografskog uređaja ili indirektno putem EM sonde.
- *digitalni osciloskop* – Signal disipacije snage obezbijeđen od strane mjernog kola ili EM sonde mora biti snimljen. Uglavnom se to radi pomoću digitalnog osciloskopa. Moderni osciloskopi mogu biti kontrolisani sa daljine od strane PC-a putem GPIB (*General-Purpose Interface Bus*) interfejsa ili Ethernet interfejsa. Na taj način snimljeni tragovi snage mogu biti prenijeti PC-u.
- *personalni kompjuter* – PC kontroliše svu opremu u ovom procesu i čuva izmjerene tragove snage. Svaki savremeni PC ima dovoljno izvršne snage da komunicira sa kriptografskim uređajem i osciloskopom. Dakle, nema posebnih zahtjeva za ovu komponentu opreme.



Slika 3.10 – Potrebna oprema za izvođenje napada baziranog na analizi snage kriptografskog uređaja

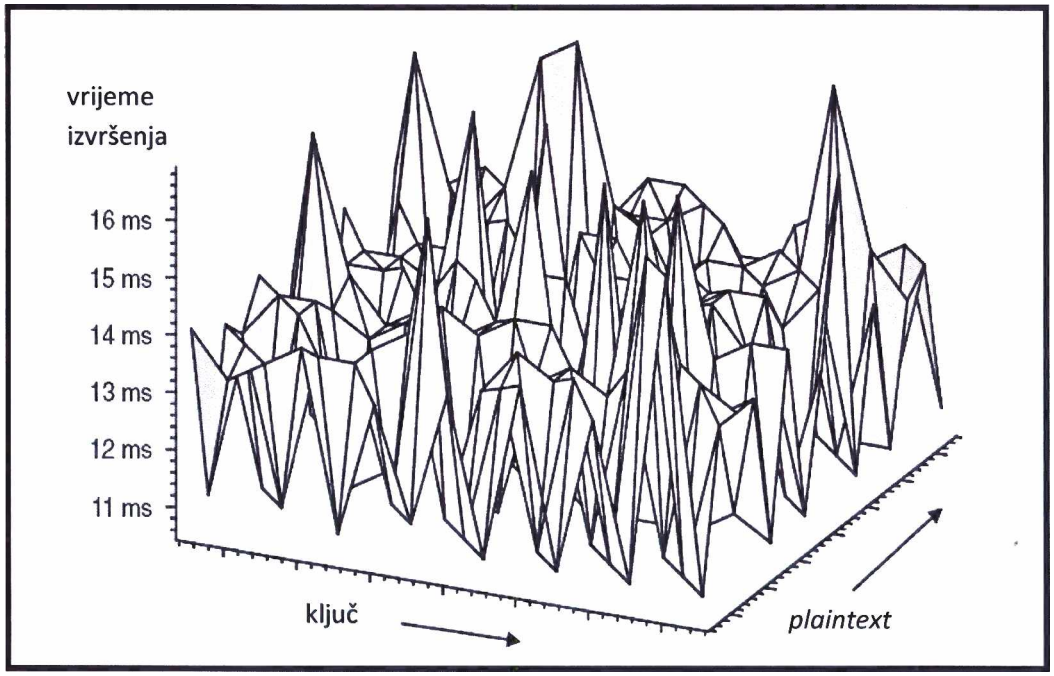
Najjednostavniji tip napada baziran na analizi snage kriptografskog uređaja je SPA *(Simple Power Analysis Attack)* napad. Po riječima *Kocher*-a, SPA je tehnika koja se sastoji od direktne analize izmjerene disipacije snage tokom kriptografskih operacija [36]. Drugim riječima, napadač pokušava da otkrije ključ manje-više direktno iz traga snage. Ovo čini SPA napad velikim izazovom u praksi. Često, potrebno je imati detaljno znanje o implementiranom kriptografskom algoritmu u uređaju koji je napadnut. Dalje, ukoliko je dostupan samo jedan trag snage, kompleksnim statističkim metodama potrebno je izdvojiti signal.

Dakle, cilj SPA napada je da otkrije skriveni ključ kada postoji mali broj tragova snage, tj. za mali broj ulaznih podataka. U ekstremnom slučaju, napadač pokušava otkriti ključ samo na osnovu jednog traga snage. Da bi se napravila razlika između normalnog i ekstremnog SPA pokušaja, razlikujemo SPA napad baziran na jednom snimku (*single-shot SPA attack*) i SPA napad baziran na više snimaka (*multiple-shot SPA attack*). U *single-shot* SPA napadima samo jedan trag snage može biti snimljen, dok u *multiple-shot* SPA napadima može biti snimljeno više tragova snage. U *multiple-shot* SPA napadima može se mjeriti disipacija snage za iste vrijednosti ulaznog podatka ili za različite vrijednosti ulaznog podatka. Prednost posjedovanja tragova za iste vrijednosti ulaznog podatka je ta što se može smanjiti šum računanjem srednje vrijednosti tragova. Pored razlika u izvršenju *single-shot* i *multiple-shot* mjerenja, principi SPA napada su uvijek isti. Napadač mora biti u poziciji da mjeri i nadgleda disipaciju snage napadnutog kriptografskog uređaja. U napadnutom kriptografskom uređaju, ključ mora imati (direktno ili indirektno) veiliki uticaj na disipaciju snage.

§ *III.2.2. Timing Analysis Attacks*

Napadi bazirani na vremenskoj analizi eksploatišu činjenicu da algoritmi sa promjenljivim vremenom izvršenja omogućavaju otkrivanje skrivenih podataka i to iz razloga što vrijeme potrebno za izvršenje kriptografskog algoritma u pametnoj kartici zavisi od vrijednosti ključa [39] (Slika 3.11). Ovi različiti vremenski periodi izvršenja algoritma mogu biti uzrokovani uslovnim skokovima u algoritmu, raznim optimizacionim tehnikama, neefikasnošću keš memorije (*cache misses*). Za razliku od napada baziranih na analizi snage,

djelovanje ovih napada nije ograničeno samo na pametne kartice. Pokazalo se da napadi bazirani na vremenskoj analizi ne moraju djelovati isključivo na hardver, već generalno na softverske sisteme i mrežno bazirane kriptosisteme [47].



Slika 3.11 – Primjer zavisnosti kriptovanih podataka u DES algoritmu od ulaznih podataka

Sigurnost aplikacije pametne kartice temelji se na tajnosti ključeva upotrijebljenih u kriptografskim algoritmima. Terminal se mora ovjeriti uz pomoć tajnog ključa da bi mogao pametnom karticom izvršiti određene akcije. Autorizacija terminala od strane pametne kartice predstavlja potencijalnu metu napada na njenu sigurnost. Naime, pametna kartica ovjerava terminal slanjem slučajnog broja, koji terminal kriptuje i vraća kartici. Zatim pametna kartica izvodi istu enkripciju i upoređuje rezultat sa vrijednošću dobijenom od terminala. Ako je rezultat poređenja pozitivan, onda je terminal uspješno ovjeren i prima odgovarajući povratni kod. Početna tačka napada je analiza vremenskog intervala koji počinje slanjem kriptovanog broja kartici, a završava se primanjem odgovarajućeg povratnog koda. Nivo šuma kriptografskog algoritma određuju vremenske razlike u trajanju procesa kriptovanja ili

dekriptovanja zavisno od ulaznih vrijednosti, originalnog teksta i tajnog ključa. Što su te vremenske razlike veće, nivo šuma je veći. Očigledan način odbrane od ove vrste napada je implementacija algoritma sa konstantnim vremenom izvršavanja. Kako je ovaj napad poznat već relativno dugo vremena, sve aktuelne pametne kartice koriste bešumne kriptografske algoritme (*noise-free*) kod kojih vrijeme potrebno za enkripciju i dekripciju podataka ne zavisi od ulaznih podataka. Time se sprečava gore navedeni napad. Programski kod pisan za ovakav algoritam je znatno duži iz razloga što putanja kroz program mora imati istu dužinu za sve moguće kombinacije originalne riječi i ključa, pa se se za referentnu vrijednost uzima najduži mogući put po kojoj se ravnaju sve ostale kombinacije. Takođe, mana bešumnih algoritama je da su uvijek sporiji od svoje bučne verzije.

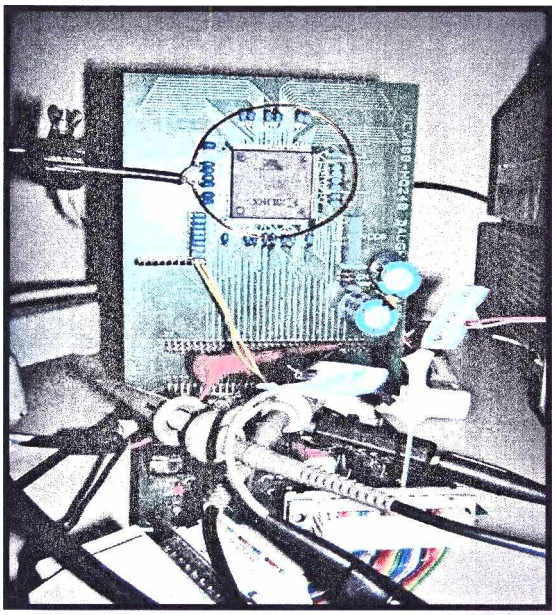
Gotovo sve moderne implementacije kriptografskih uređaja su otporne na napade bazirane na vremenskoj analizi, što znači da su ovakvi napadi nemogući ako se izvode sami. Ukoliko se informacija o vremenu kombinuje sa drugim *side-channel* informacijama, postoji opasnost za sigurnost pametne kartice. Na primjer, informacija o vremenu se može iskoristiti da bi se locirali određeni djelovi algoritma.

Kod nekih pametnih kartica dodatna sigurnost se postiže dodavanjem brojača za svaki postojeći ključ u kriptografskom uređaju koji broji neuspjele pokušaje identifikacije ključa, tako da se može izvršiti samo ograničeni broj neuspješnih identifikacija. Kad brojač pokušaja dosegne maksimalnu vrijednost blokira se svaki dalji pokušaj identifikacije.

§ *III.2.3. Electromagnetic Analysis Attacks*

U *side-channel* napadima, mjerljivi fizički kvantiteti kao što su disipacija snage, vrijeme i elektromagnetno zračenje se analiziraju radi izdvajanja skrivenih informacija iz kriptografskog uređaja bez razbijanja samog algoritma. Svaki komad hardvera troši određenu snagu, zahtijeva vrijeme za izvođenje raznih operacija i stvara elektromagnetno zračenje, pri čemu je svaka od nabrojenih performansi upotrijebljena ili proizvedena u skladu sa potrebama ili karakteristikama različitih hardverskih blokova za izgradnju kriptografskog uređaja. Već je

rečeno da iz procesuiranih podataka cure informacije. U Poglavlju III.2.1 objašnjena je zavisnost podataka od disipacije snage, dinamičke struje, struje curenja. Po prirodi stvari, kada struja protiče kolom, stvara se elektromagnetno polje. Postoji nekoliko prednosti u izvođenju napada baziranom na analizi elektromagnetnog zračenja u odnosu na napade bazirane na analizi dispacije snage, dinamičkih struja i struja curenja. Prva prednost je ta što se sam napad može izvesti sa distance, za razliku od mjerenja disipacije snage gdje je neophodna povezanost sa kriptografskim uređajem. Druga prednost je ta što se napadač može fokusirati na određeni dio kriptografskog uređaja.



Slika 3.12 – Segment mjerne opreme za elektromagnetne analize

Prvi publikovani radovi u ovoj oblasti odnose se na autore *Quisquater*-a i *Samyde*-a [48], kao i *Gandolfi*-a, *Mourtel*-a i *Olivier*-a [49]. *Quisquater* i *Samyde* pokazali su da je moguće mjeriti elektromagnetno zračenje pametne kartice. Oprema korišćena za njihova istraživanja sastojala se iz senzora u vidu jednostavnog ravnog kalema (*loop antenna*) (Slika 3.12), osciloskopa ili analizatora spektra i Faradejevog kaveza. Upravo je *Quisquater* uveo pojmove SEMA (*Simple Electromagnetic Analysis)* i DEMA (*Differential Electromagnetic*

Analysis). Rad [49] se odnosi na istraživanja uticaja kriptografskih algoritama DES, RES i COMP-128 na elektromagnetno zračenje pametne kartice. Naime, ovaj tim naučnika je analizirao izvodljivost EMA napada i uporedio njihovu efikasnost sa napadima baziranim na analizi snage, pri čemu je data prednost EMA napadima. Takođe, ovaj tim je došao do zaključka da se na osnovu elektomagnetnog zračenja mogu dobiti lokalne informacije iz hardvera pametne kartice i da se ta mjerenja, iako sa više šuma, mogu izvesti sa veće distance.

Prema *Agrawal*-u postoje dva tipa zračenja: namjeran i nenamjeran [50, 51]. Prvi tip je rezultat direktnog strujnog toka, dok drugi tip zračenja nastaje zbog raznih sprega, modulacija (AM, FM), itd. Pomenute publikacije [50, 51] bave se isključivo namjernim tipom zračenja, dok ogromna prednost EMA napada u odnosu na druge *side-channel* napade leži u mogućnosti istraživanja nenamjernog zračenja [52]. Preciznije govoreći, EMA napad koji se bazira na nenamjernom zračenju može iskoristiti *side-channel* informaciju koja se sastoji iz više kanala i on je poznat pod nazivom više-kanalski napad. Informacije iz tih kanala mogu biti istog tipa (npr. elektromagnetno zračenje detektovano i lokalizovano na različitim djelovima čipa) ili različitog tipa kada se stvaraju kombinovani napadi (EMA i PA: *side-channel* informacije o elektromagnetnom zračenju i snazi kriptografskog uređaja).

§ *III.2.4. Fault Analysis Attacks*

Prvi uspješan napad na pametne kartice baziran na analizi grešaka prezentovao je *Boneh* 1997. godine [53], a imao je za metu RSA (*Rivest Shamir Adleman*) algoritam sa javnim ključem. Generalno, interesovanje za napade na elektronske sisteme bazirane na analizi grešaka postoji još od otkrića iz 1975. godine da kosmički zraci imaju dovoljnu količinu energije da promijene stanja elemenata u elektronskim integrisanim kolima (sateliti, svemirske letjelice) što se ogleda kroz "flipovanje" (promjena vrijednosti) bita u memoriji elektronskih uređaja [54]. Prema klasifikaciji grešaka koju je izvršio sam *Boneh*, greške izazvane kosmičkim zracima pripadaju kategoriji kratkotrajnih grešaka koje se slučajno javljaju. Druga kategorija grešaka su latentne greške u vidu hardverskih ili softverskih "bagova" koje je teško locirati. Treća kategorija grešaka su greške ubačene u sistem

posredstvom napadača za šta je bilo neophodno da napadač aktivno i neautorizovano djeluje na hardver pametne kartice. Naime, uz određeni instrumentalni *set-up* pametna kartica je izložena fizičkom stresu u toku koga napadač ubacuje greške u memorijske ćelije ili neke druge strukturne elemente kriptografskog hardvera. Reakcija pametne kartice na ovaj fizički napad ogleda se u promjeni struje kroz memorijske ćelije, magistrale prenose drugačije signale, strukturni elementi se mijenjaju.

Napadi bazirani na analizi grešaka mogu eksploatisati iste na dva različita načina. Prvi način je da netačan rezultat, dobijen greškama u radu kriptografskog uređaja, napadač iskoristi za otkrivanje skrivenog ključa. Drugi način ne podrazumijeva direktno eksploatisanje netačnog rezultata, već samo informacije da li je u krajnjem rezultatu (*ciphertext*) došlo do greške ili ne.

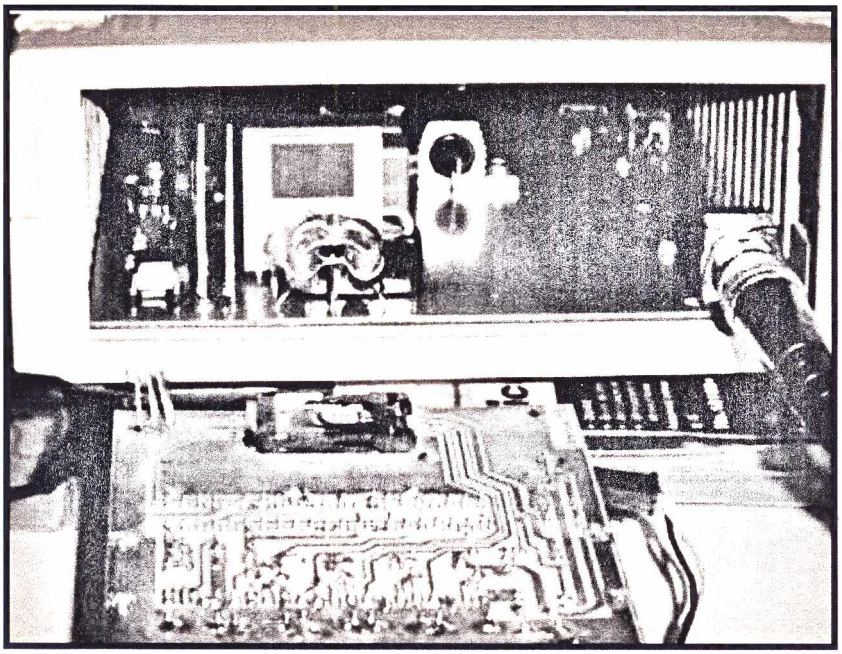
Neke od najpublikovanijih tehnika ubacivanja grešaka u hardver pametnih kartica su:

- *mijenjanje napona napajanja* – u toku izvršavanja algoritma može dovesti do toga da procesor pogrešno interpretira ili preskoči instrukciju.

- *promjena frekvencije spoljašnjeg takta* – može da dovede do pogrešnog čitanja podataka (kolo pročita vrijednost sa magistrale prije nego što je memorija uspjela da zaključi traženu vrijednost) ili preskoči izvršenje instrukcije (kolo počne da izvršava instrukciju $n+1$ prije nego što je mikroprocesor završio sa izvršavanjem instrukcije n)

- *temperatura* – proizvođači pametnih kartica definišu gornji i donji prag temperature u čijem okviru kola ispravno funkcionišu. Cilj napadača je prevazići temperaturni prag čime se mogu postići dva efekta: nasumična modifikacija RAM ćelija zahvaljujući procesu zagrijavanja i iskorišćavanje činjenice da se temperaturni pragovi operacija čitanja i pisanja ne podudaraju kod većine nepostojanih memorija. Podešavajući temperaturu čipa tako da je operacija pisanja nemoguća dok je operacija čitanja izvodljiva i obrnuto, mogu se izvršiti mnogobrojni napadi na hardver pametne kartice.

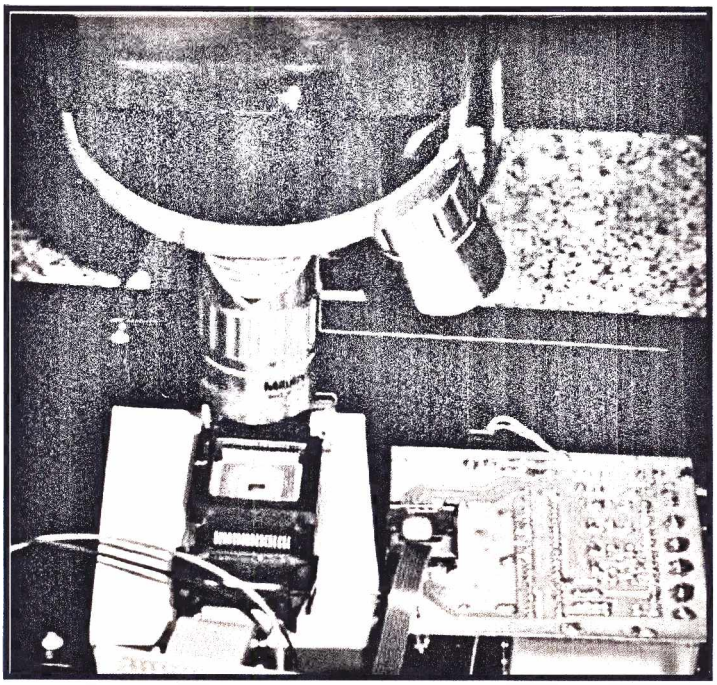
- *bijela svjetlost* – sva električna kola su osjetljiva na svjetlost zahvaljujući fotoelektričnom efektu. Indukovana struja može izazvati greške ukoliko je kolo izloženo intezivnoj svjetlosti u kratkom vremenskom periodu (Slika 3.13).



Slika 3.13 – Oprema za izazivanje greške bijelom svjetlošću [55]

- *x zraci i jonski snopovi* – takođe se mogu iskoristiti za izazivanje grešaka, iako je to jako rijetko. Njihova prednost je u tome što dozvoljavaju izvođenje napada baziranih na analizi grešaka bez prethodnog raspakivanja čipa.

- *laser* – efekat dobijen djelovanjem lasera na hardver pametne kartice sličan je efektu dobijenom korišćenjem bijele svjetlosti za izazivanje grešaka. Prednost je u tome što je laserom moguće napasti tačno određen, mali dio hardvera pametne kartice (Slika 3.14).



Slika 3.14 – Oprema za izazivanje greške laserom [55]

§ *III.3 Zaključci*

U ovom poglavlju su definisane sigurnosne komponente pametne kartice. Izvršena je klasifikacija napada na pametne kartice kroz nekoliko različitih pristupa. Za istraživanja izvršena u okviru doktorske teze, najznačajnija je podjela na invazivne, polu-invazivne i neinvazivne napade na hardver pametnih kartica. Objašnjena je i najefikasnija klasa neinvazivnih napada na pametne kartice u protekloj deceniji - *side-channel* napadi. Detaljno je objašnjena ideja *side-channel* napada kroz model *side-channel* napada, kao i koraci njegovog izvršenja. Prikazani su i objašnjeni tipovi *side-channel* napada: napadi bazirani na analizi snage (*Power Analysis Attacks*), vremenskoj analizi (*Timing Analysis Attacks*), analizi elektromagnetnog zračenja (*Electromagnetic Analysis Attacks*), analizi grešaka (*Fault Analysis Attacks*).

IV Mjere zaštite pametnih kartica od side-channel napada baziranih na analizi snage (struje)

Od trenutka kada su *side-channel* napadi bazirani na analizi snage (struje) počeli da predstavljaju realnu prijetnju sigurnosti čip-kartica, predloženo je obilje mjera zaštite istih. Cilj i namjena svake od ovih zaštitnih mjera, integrisanih u čipu pametne kartice je da snaga disipacije (struja) kriptografskog uređaja bude nezavisna od najznačajnijih podataka u kriptografskom uređaju (ulazni podaci, izlazni podaci, skriveni ključevi, itd.). Do danas je napisan značajan broj publikacija na temu različitih načina zaštite pametnih kartica od ovih napada. Svaka od postojećih zaštitnih mjera ima svoju cijenu koja zavisi od performansi ili veličine čipa/memorije čuvanog kriptografskog uređaja. Iz tog razloga, odluka o najadekvatnijoj mjeri zaštite za određeni kriptografski uređaj mora se donijeti za svaki uređaj individualno.

U ovom poglavlju je napravljen pregled vrsta mjera zaštite kriptografskih jezgara pametnih kartica od *side-channel* napada baziranih na analizi snage (struje). Generalno, podjela ovih mjera zaštite vrši se na algoritamske (softverske) i hardverske mjere zaštite.

§ *IV.1 Algoritamske (softverske) mjere zaštite*

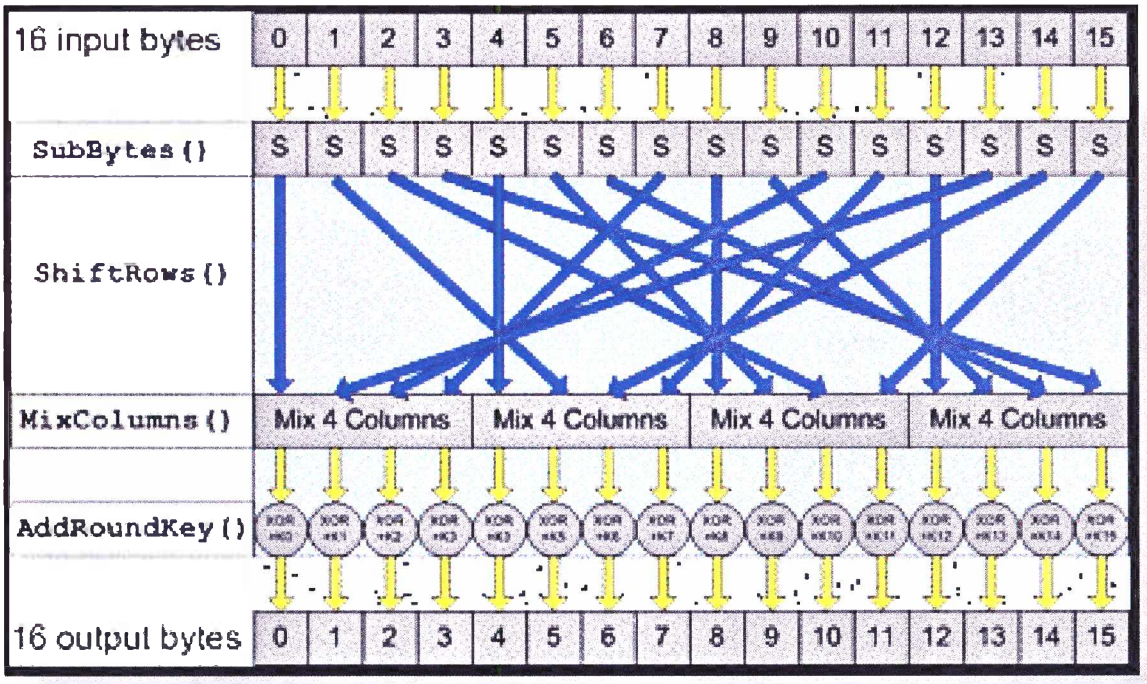
Napadi bazirani na analizi snage ili struje temelje se na elementarnim proračunima koji zavise od dijela skrivenog ključa, kao i ulaznog ili izlaznog podatka, za koje se pretpostavlja da su poznati. Do nedavno, većina ovih napada eksploatisala je specifične karakteristike softverski implementiranih kriptografskih algoritama, što je i dovelo do dizajniranja mjera zaštite na softverskom nivou.

Jedna od najuspješnijih softverskih tehnika za zaštitu kriptografskog uređaja/algoritma je maskiranje ulaznog podatka i svih međurezultata kako bi se "dekorelisala" bilo kakva

informacija dobijena kroz *side-channel* koja potiče od obrađenog tajnog podatka. Na primjer, ulazni podatak kriptografskog uređaja u simetričnim algoritmima se vodi na ulaz XOR kola zajedno sa nekim slučajnim podatkom (ili ključem) i na taj način transformiše u novi ulazni podatak. Napadač, ne znajući vrijednost slučajnog broja (ili ključa), nije u stanju da otkrije novi, maskirani ulazni podatak. Korišćeni slučajni broj se naziva maskom *m*, a sam proces zaštite podataka na ovaj način maskiranjem. Maska se generiše unutar kriptografskog uređaja i drugačija je kod svake nove algoritamske operacije, a oblik maske zavisi od operacija koje se koriste u određenom kriptografskom algoritmu. Podrazumijeva se da maska nije poznata od strane napadača. Takođe, postoje i odgovarajuće transformacije ulaznih podataka kod asimetričnih algoritama. Naime, maskiranje ovih podataka se bazira na aritmetičkim karakteristikama asimetričnih algoritama.

Maske u kriptografskim algoritmima se ne primjenjuju samo na ulazni podatak, već i na skrivene ključeve, kao i na rezultat enkripcije. Naravno, kako bi se kompenzovao efekat upotrebe maski tokom operacija algoritma i da bi se došlo do originalnog izlaznog podatka, potrebno je ukloniti masku nakon svih algoritamskih operacija. Tipična šema maskiranja definiše na koji se način podaci maskiraju i kako se maske upotrebljavaju, uklanjaju i mijenjaju kroz kriptografski algoritam.

Tipičan primjer maskiranja je maskiranje koraka AES simetričnog kriptografskog algoritma [56]. Standardna dužina ključa je 128 bita, ali za neke aplikacije potrebna dužina je 192 ili 256 bita. Ulazni podatak se smješta u matricu veličine 4x4 bajta koja se označava kao matrica stanja (*state*). Ključ se takođe predstavlja kroz matricu stanja, ali u zavisnosti od veličine ključa može biti 4×4, 4×6 ili 4×8 bajta. Takođe, od veličine ključa (stanja ključa) zavisi broj rundi koji će se izvršiti u AES algoritmu: 10, 12 ili 14, respektivno. Svaka runda se sastoji iz četiri različite operacije koje se izvode sljedećim redosljedom: *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey* (Slika 4.1). Na početku algoritma, prije svih rundi, vrši se *AddRoundKey* operacija, tj. XOR operacija između ulaznog podatka (*plaintext*) i početnog ključa (*key*). Takođe, potrebno je naglasiti da se posljednja runda razlikuje od ostalih po tome što ima jednu operaciju manje, nema *MixColumns* operaciju.



Slika 4.1 – Operacije u toku jedne runde izvršenja AES algoritma

Sve operacije, osim *SubBytes* operacije su linearne, tj. za njih važi da je $f(x + m) = f(x) + f(m)$. Posljedica ove karakteristike je prilično laka rekonstrukcija maske m nakon transformacije ili niza transformacija. Ostale karakteristike linearnih operacija u AES algoritmu su:

- *ShiftRows operacija* – ciklično pomjera bajtove ulijevo u svakom redu stanja za određeni broj pozicija. Nulti red se ne rotira, dok se ostali redovi rotiraju za $r - 1$ pozicija, pri čemu je $1 \leq r \leq 4$.
- *MixColumns operacija* – kombinuje četiri bajta svake kolone stanja tako da svaki bajt pojedinačno utiče na sva četiri izlazna bajta. Zajedno sa *ShiftRows* operacijom ova operacija obezbjeđuje difuziju algoritma i ukoliko je ona dobro izvedena promjena ulaznog bita bi trebala da promijeni svaki bit izlaza sa vjerovatnoćom *0.5*. Druga karakteristika operacija sigurnog algoritma je konfuzija koju obezbjeđuje upotreba S-kutije, kao u operaciji *SubBytes*.

- *AddRoundKey operacija* – izvršava XOR operaciju nad ključem runde i stanjem, pri čemu ključ runde označava ključ koji se koristi u trenutnoj rundi. Do njega se dolazi iz glavnog ključa kriptovanja (*cypher key*) upotrebom algoritma odabira ključa koji se sastoji iz dva dijela, ekspanzije ključa i odabira ključa runde. U svakoj rundi koristi se po jedan ključ koji se sastoji od 4 riječi (riječ=32 bita).

Kako je *SubBytes* operacija nelinearna bajt supstitucija, prilično je komplikovano obnoviti masku nakon *SubBytes* transformacije. Iz tog razloga *SubBytes* operacija predstavlja glavnu strukturnu jedinicu u AES algoritmu. Funkcija ove operacije je da zamijeni svaki bajt stanja koristeći 8-bitnu S-kutiju koja je jedinstvena za sve runde i koja se sastoji iz dva koraka:

- Svaki bajt stanja zamjenjuje se svojom recipročnom vrijednošću (*multiplicative inverse*) u konačnom polju GF (*Galois Field*) koje AES koristi za veći dio matematičkih operacija koje obavlja. GF je specijalna matematička konstrukcija gdje su operacije sabiranja, oduzimanja, množenja i dijeljenja redefinisane, a podaci mogu biti veličine samo do 8-bitnog broja (decimalne vrijednosti od 0 do 255). Rezultati svih ovih operacija u AES algoritmu kao rezultat takođe imaju 8-bitni broj.

- Dobijeni 8-bitni multiplikativni inverz se dalje transformiše uz pomoć tzv. fiksne afine transformacije koja je definisana kao:

$$b_i' = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i \qquad (4.1)$$

gdje je i=0,...,7 položaj bita, b_i`- izlazni bit, b_i – ulazni bit, c_i je i-ti bit konstantnog vektora C.

SubBytes transformacija implementirana je kao fiksna tabela. Samo maskiranje *SubBytes* operacije prikazano je kao $SubBytes(x + m) = SubBytes(x) + m'$. Da bi se ova operacija postigla sa fiksnom tabelom, potrebno je kreirati odgovarajuću tabelu *MaskedSubBytes* za masku m, kao što je prikazano sljedećim algoritmom [57]:

INPUT: m

OUTPUT: MaskedSubBytes(x XOR m) = SubBytes(x)XOR m,

1: for i = 0 to 255 do

2: MaskedSubBytes(iXOR m) = SubBytes(i)XOR m

3: end for

4: Return(MaskedSubBytes)

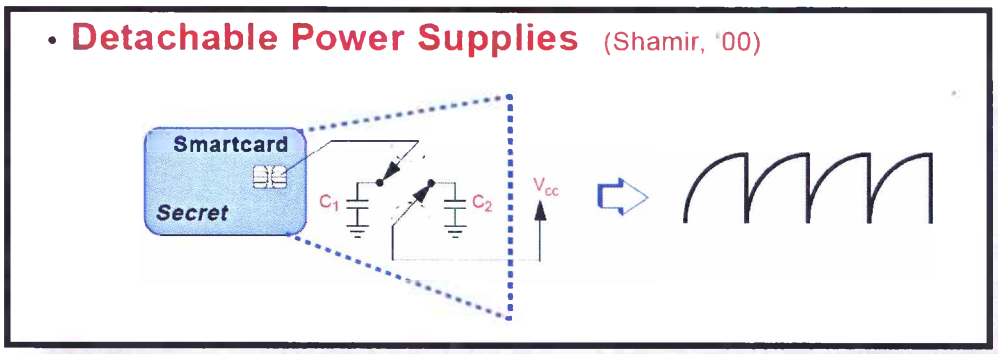
MaskedSubBytes tabela mora biti izračunata za svaku vrijednost maske m_i. Ako se koristi i različitih maski m, onda je složenost ove procedure i*256. Ako se obezbijedi da se iste maske m_i obnove prije *SubBytes* operacije u svakoj rundi, onda se iste i tabele mogu koristiti kroz sve AES kalkulacije. Proces uklanjnja maske se obavlja na sljedeći način: *SubBytes(x) = MaskedSubBytes(x XORm)XORm.*

§ *IV.2 Hardverske mjere zaštite*

Hardverske mjere zaštite su prilično intuitivne. Kako napadi bazirani na analizi snage (struje) zavise od procesuiranih podataka u kriptografskom uređaju, isti mogu biti spriječeni građenjem hardvera čija je snaga disipacije (struja) nezavisna od tih podataka. Klasifikacija hardverskih mjera zaštite vrši se u odnosu na angažovani nivo apstrakcije tokom automatizovanog elektronskog dizajna (*design flow*), pa prema tome razlikujemo mjere zaštite na nivou sistema, kola i tranzistora. U ovom poglavlju će biti opisani neki od primjera hardverskih mjera zaštite.

§ *IV.2.1 Mjere zaštite na nivou sistema (system-level countermeasures)*

Algoritamske mjere zaštite, kao i hardverske mjere zaštite nadalje prikazane u ovom poglavlju su takve da zahtijevaju od algoritma izvjesne promjene ili zahtijevaju promjene u implementaciji kriptografskog hardvera. Za razliku od njih, mjere zaštite na nivou sistema imaju takav pristup da generalno ne utiču na algoritamsku implementaciju.



Slika 4.2 – Mjere zaštite na nivou sistema bazirane na dodavanju kondenzatora

A. Shamir je našao način da disipacija snage uređaja bude nezavisna od ulaznih podataka dodajući kondenzatore postojećem dizajnu kriptografskog uređaja [58]. Osnovna ideja je upotrijebiti dva kondenzatora: jedan je povezan sa spoljašnjim naponom napajanja uređaja, dok je drugi povezan sa hardverom uređaja i vrši napajanje (Slika 4.2). Kada se kondenzator koji napaja kolo uređaja gotovo isprazni, kondenzatori zamijene uloge. Na taj način ova dva kondenzatora se periodično prekopčavaju: jedan se puni, dok drugi napaja kolo kriptografskog uređaja. Struja koju napadač mjeri u ovom slučaju je struja kroz kondenzator

C_2 koji nije povezan sa kriptografskim kolom uređaja i dobija se grafik struje koji nije od koristi za napad. Naravno, kapacitivnost kondenzatora treba da je dovoljno velika, a u *Shamir*-ovom radu predložena vrijednost kapacitivnosti je 0.1 μF. Postavlja se pitanje gdje se mogu smjestiti tako veliki kondenzatori, jer je izuzetno komplikovano implementirati tako velike kondenzatore u čipu. Postoji mogućnost smještanja kondenzatora van samog čipa, a u tijelu pametne kartice. Međutim, za uspješno izvođenje napada dovoljno je da napadač presječe kondenzatore i poveže čip direktno sa naponom napajanja. Ukoliko se kondenzatori ne mogu efikasno implementirati u čipu, tako da ne zauzimaju previše mjesta i ne komplikuju proces proizvodnje hardvera pametnih kartica, ova hardverska mjera neće pružiti visok nivo zaštite u praksi.

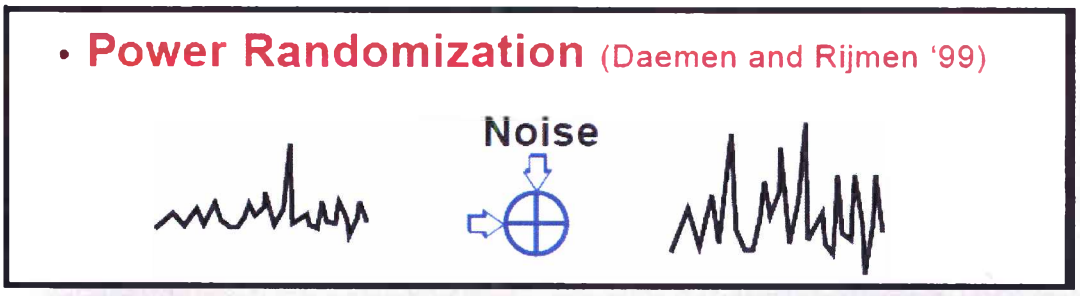
Sljedeća mjera zaštite je generisanje šuma tako da se izmjerene disipacije snage bitno razlikuju [36], [59]. Veličina koja definiše odnos signala i šuma *SNR* (*signal-to-noise ratio*) je odnos između komponente signala i komponente šuma u procesu mjerenja. Definicija *SNR*-a u okruženju napada baziranom na analizi snage je:

$$SNR = \frac{Var(P_{exp})}{Var(P_{sw.\ noise} + P_{el.\ noise})} \tag{4.2}$$

gdje je P_{exp} komponenta disipacije snage koja se može eksploatisati (*exploitable*), a varijansa $Var(P_{exp})$ definiše u kolikoj mjeri određena tačka na snimljenom tragu snage varira usljed eksploatisanog signala. To je ujedno i jedina komponenta koja sadrži relevantne informacije za napadača. Jasno je da što je veće *SNR*, lakše je detektovati P_{exp} u šumu. Šum je dat kroz sumu dvije komponente šuma: prekidačkog šuma $P_{sw.noise}$ i električnog šuma $P_{el.noise}$, dok varijansa njihovog zbira definiše u kolikoj mjeri varira tačka na snimljenom tragu šuma usljed generisanog šuma. Komponenta prekidačkog šuma $P_{sw.noise}$ je posljedica prekidačkog svojstva logičkih kola integrisanih u čipu pametne kartice i značajno zavisi od arhitekture kriptografskog jezgra. Komponenta električnog šuma $P_{el.noise}$ je nepoželjna komponenta šuma u aktivnim i pasivnim električnim komponentama kola, jer ograničava pojačanje i kvari kvalitet informacije koja se prenosi. Postoji više izvora električnog šuma u pametnim karticama: šum od izvora napajanja, šum od generatora takta, šum od električnog i elektromagnetnog zračenja komponenti na čipu, šum od analogno-digitalne konverzije koja se

izvodi na osciloskopu. Za sve ove izvore električnog šuma koji su karakteristični za mjerenja nad pametnom karticom postoje metode njihovog kontrolisanja i smanjenja.

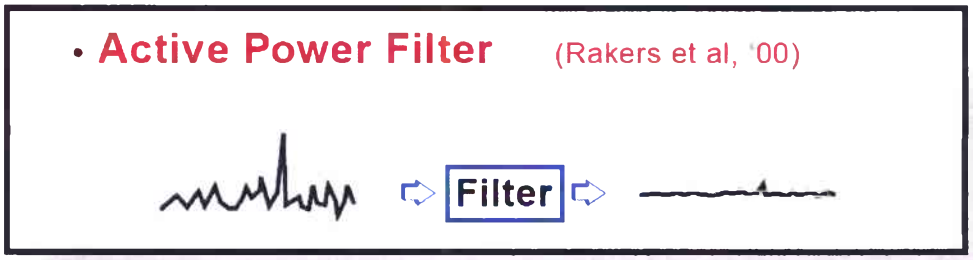
Generisani šum je uglavnom nekorelisan sa samim signalom (to se može postići dodavanjem bijelog šuma). Filtriranje nekorelisanog šuma postiže se usrednjavanjem prikupljenih tragova snage. Ukoliko je dodata veća količina šuma potrebno je obaviti ista mjerenja više puta, a nekada je nemoguće odstraniti sav šum i uspješno izvršiti napad (Slika 4.3). Generatori šuma su obično bazirani na generatorima nasumičnih brojeva i izvode nasumične prekidačke aktivnosti paralelno sa tekućim operacijama. Time se povećava komponenta $P_{sw.noise}$ i SNR je smanjen. Da bi se postigao ogroman uticaj na disipaciju snage, generatori nasumičnih brojeva moraju biti povezani sa mrežom velikih kondenzatora. Nasumično punjenje i pražnjenje ove mreže dovodi do šuma u disipaciji snage čime se otežava napad baziran na analizi disipacije snage. *Messerges* u radovima [60], [61] prezentuje nekoliko tehnika kako da se poboljša odnos signala i šuma, a *Daemen* i *Rijmen* testiraju i porede efikasnost ovih tehnika na svim kriptografskim algoritmima koji su bili kandidati za AES standard [62]. Takođe, bitno je shvatiti da SNR ne zavisi isključivo od kriptografskog uređaja, već i od mjerne opreme koja se koristi za napad. Ako mjera zaštite na nivou sistema smanji SNR za jedno izvedeno mjerenje, to ne podrazumijeva da će SNR biti smanjen za sva izvedena mjerenja.



Slika 4.3 – Mjere zaštite na nivou sistema bazirane na dodavanju šuma

Još jedna metoda smanjivanja *SNR*-a, tako da se približi vrijednosti 0 (jer ne postoji mjera zaštite kojom se može postići idealan uslov da je *SNR*=0) je da se postigne da varijansa $Var(P_{exp})$ ima malu vrijednost. Hardverski to se može ostvariti postavljanjem filtera između izvora napajanja kriptografskog uređaja i uređaja koji izvršava kriptografski algoritam (Slika 4.4) [63]. Cilj ove metode je da se ukloni komponenta snage disipacije koju je moguće eksploatisati. U praksi, disipacija snage se može filtrirati korišćenjem prekidačkih kondenzatora, izvora konstantne struje i raznih drugih uređaja koji regulišu disipaciju snage.

Pored navedenih mjera zaštite na nivou sistema, postoje i mjere koje podrazumijevaju izazivanje promjena u radu signala takta (*clock signal*) na više različitih načina [64], kao i umetanje nasumičnih lažnih (*dummy*) operacija tokom izvršavanja kriptografskog algoritma radi promjene vrijednosti disipacije snage koja se mjeri [65]. Za ove mjere zaštite koje utiču na vremensku dimenziju tragova snage (struje), od krucijalnog je značaja da napadači ne identifikuju tip zaštitne mjere.



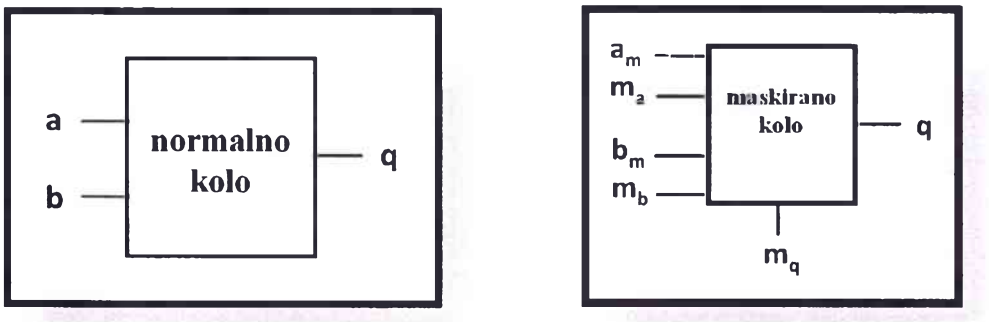
Slika 4.4 – Mjere zaštite na nivou sistema bazirane na dodavanju filtera

§ *IV.2.2 Mjere zaštite na nivou kola (gate-level countermeasures)*

Mjere zaštite na nivou kola podrazumijevaju maskiranje osnovnih logičkih kola (AND, XOR, itd.) unutar kriptografskih algoritama, kao i mnogih drugih algoritamskih

jedinica i blokova (sabirači, množači, ...). Mjere zaštite na nivou kola obuhvataju i različite procese maskiranja: nasumično kašnjenje (*random delays*), nasumično predpunjenje (*random precharging*), maskiranje linija (*masking buses*), zamke (*pitfalls*), itd. Dakle, u ovu kategoriju mjera zaštite spadaju i metode maskiranja prikazane u odjeljku IV.2.1, odnosno algoritamske mjere zaštite, ali koje su implementirane na nivou hardvera. U odnosu na algoritamske metode maskiranja, kod hardverskih metoda maskiranja mogući su kompromisi između veličine i brzine. Takođe, prednost mjera zaštite na nivou kola je ta što se mogu implementirati u digitalnom dizajnu uređaja koje predstavljaju prefabrikovane strukture koje se doradom prilagođavaju korisničkim zahtjevima (*semi-custom digital design*) u različitim tehnologijama i bibliotekama standardnih ćelija. Takođe, one se mogu primijeniti i kod postojećih kriptografskih IP (*Intellectual Property*) jezgara uz odgovarajuću modifikaciju njihovog RTL (*Register Transfer Level*) koda.

Karakteristično za proces maskiranja na nivou kola je nezavisnost od tipa implementiranog kriptografskog algoritma, štaviše taj proces može biti u potpunosti automatizovan upotrebom programa koji će konvertovati digitalno kolo u skup maskiranih kola. Osnovna ideja mjera zaštite na nivou kola je da u procesu maskiranja svaku vrijednost a koja se pojavljuje u digitalnom kolu predstavi sa dvije vrijednosti a_m i m_a. Vrijednost m_a predstavlja nasumičnu masku nezavisnu od vrijednosti a koja ima ravnomjernu distribuciju. Vrijednost maskiranja a_m izračunava se na sljedeći način: $a_m = a \oplus m_a$. Iz tog razloga u maskiranom digitalnom kolu, logička kola umjesto ulazne vrijednosti a uzimaju ulazni par (a_m, m_a) [66].



Slika 4.5 – a) Normalno kolo, b) Maskirano kolo

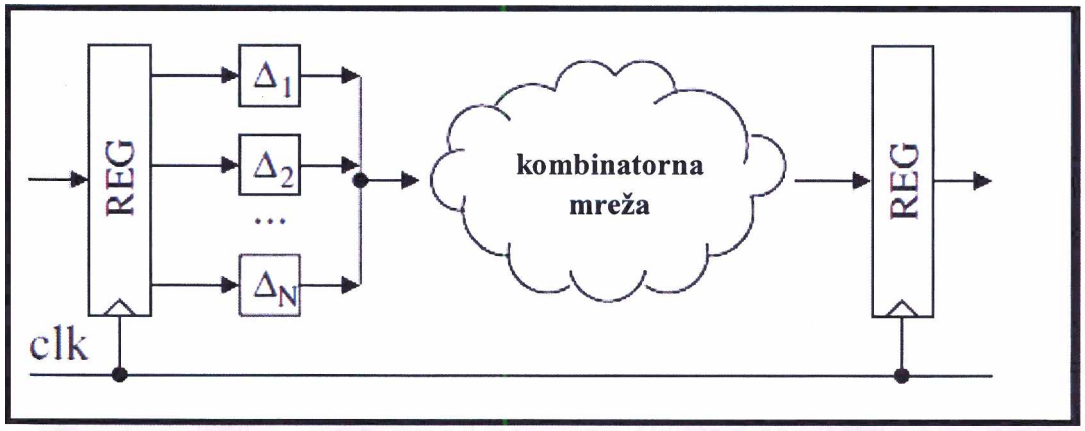
U normalnom digitalnom kolu izlazni signal q na osnovu ulaznih signala a i b se izračunava kao (Slika 4.5.a):

$$q = f(a, b) \tag{4.3}$$

U maskiranom digitalnom kolu, pored ulaznih signala, maskirani su i izlazni signali. To znači da imamo: $a_m = a \oplus m_a$, $b_m = b \oplus m_b$, $q_m = q \oplus m_q$, gdje su m_a, m_b i m_q nasumično generisane maske. Maskirano digitalno kolo izračunava izlazni signal q_m na osnovu ulaznih podataka a_m, m_a, b_m, m_b i m_q (Slika 4.5.b):

$$q_m = \tilde{f}(a_m, m_a, b_m, m_b, m_q) \tag{4.4}$$

Primjeri konstrukcije maski na više različitih načina za osnovna logičkih kola koja učestvuju u izgradnji djelova hardverski implementiranog kriptografskog algoritma dati su u [67], [68], [69].



Slika 4.6 – Umetanje nasumičnih kašnjenja ulaznim signalima

Još jedan primjer hardverske mjere zaštite na nivou kola je tehnika bazirana na umetanju nasumičnih kašnjenja ulaznih signala [70]. Dakle, svaki ulaz ka kombinatornoj

mreži se dovodi sa nasumičnim kašnjenjem Δ_i, $i=1,2,..N$ (Slika 4.6). Na taj način se umanjuje korelacija između procesuiranih podataka i disipacije snage (struje) u kriptografskom uređaju. Praktična implementacija ove metode zasniva se na upotrebi D flip-flopova sa nasumičnim kašnjenjem na koje se dovodi ulazni signal, a kod kojih vrijeme kašnjenja zavisi od nasumičnog bita R. Za kreiranje nasumičnog bita R koriste se generatori nasumičnih brojeva RNG (*random number generator*) koji su sastavni dio pametnih kartica. Mnogi radovi su publikovani na temu RNG modula [71], [72], [73], [74], [75].

Slična metoda je nasumično predpunjenje [76], [77]. Ovo podrazumijeva slanje nasumičnih brojeva kroz digitalno kolo kako bi se nasumično predpunile kombinatorne i sekvencijalne ćelije kola. U ovom procesu prave se duplikati sekvencijalnih ćelija, odnosno broj registara se udvostručuje. Duplikati registara se ubacuju između originalnih registara i kombinatornih ćelija uređaja. U toku prve periode takta, duplikati registara sadrže nasumične brojeve. Kako su ovi registri povezani sa kombinatornim ćelijama, izlazi ovih kombinatornih ćelija se nasumično predpune. U toku prelaska iz prve u drugu periodu takta, izlazi kombinatornih ćelija se smještaju u originalnim registrima koji sadrže srednju vrijednost algoritma koji se izvršava. Istovremeno, ove srednje vrijednosti se pomjeraju iz ovih registara u duplikate registara, čime se zamijenila uloga registara. U toku druge periode takta kombinatorne ćelije povezane su sa registrima koji sadrže srednje vrijednosti algoritma. Pri prelasku iz druge u treću periodu takta, opet dolazi do zamjene uloga registara i kombinatorne ćelije se ponovo predpune. Upotrebom ove metode, sva kombinatorna i sekvencijalna polja procesuiraju nasumične podatke u toku jedne periode takta, a srednje vrijednosti u toku druge, čime se maskira disipacija snage kriptografskog uređaja.

Još jedna metoda maskiranja, koja ima dugu tradiciju, je enkripcija linija u malim uređajima. Ona se odnosi na enkripciju podataka i adresnih linija koje povezuju procesor pametne kartice sa memorijom kriptografskih koprocesora. Algoritam enkripcije koji se koristi za enkripciju linija je uglavnom jednostavan: generiše se pseudo-nasumični ključ i upotrijebi u jednostavnom algoritmu maskiranja (jednostavnost podrazumijeva XOR operacije) [78], [79], [80].

U najnovijim istraživanjima vezanim za metode maskiranja, dokazano je da metode maskiranja nijesu najbolja vrsta zaštite, jer se kriptografski uređaji mogu i dalje efikasno napasti analizirajući glič eve generisane u kombinatornim mrežama gdje su primijenjene

metode maskiranja [81]. Inače, gličevi su netačne vrijednosti izlazne funkcije tokom kratkotrajnih stanja koja su posljedica kašnjenja i ne odgovaraju projektovanoj prekidačkoj funkciji. Naime, razlikujemo prelazni režim rada kombinatorne mreže od ustaljenog režima, koji se odvija od momenta promjene vrijednosti ulaznog signala do momenta smirivanja izlazne funkcije i određen je ukupnim kašnjenjem kroz kombinatornu mrežu.

§ *IV.2.3 Mjere zaštite na nivou tranzistora (transistor-level countermeasures)*

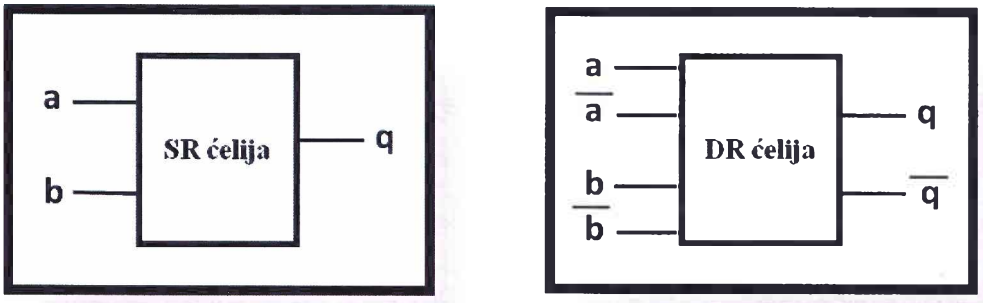
Mjere zaštite na nivou tranzistora nastale su kao odgovor na napade bazirane na analizi snage (*Power Analysis Attacks*). Osnovna ideja pri kreiranju mjera zaštite na nivou tranzistora je stvoriti kriptografski uređaj sačinjen od tranzistora koji su otporni na napade bazirane na analizi snage. Kako je ukupna snaga kriptografskog uređaja jednaka sumi snaga svih tranzistora u tom uređaju, onda će sam kriptografski uređaj biti otporan na napade bazirane na analizi snage ukoliko budu otporni i njegovi tranzistori. Hardverske mjere zaštite na tranzistorskom nivou zasnivaju se na prihvatanju novih logičkih familija kod kojih je disipacija snage nezavisna od procesuiranih podataka i izvedenih operacija. Ova nezavisnost se uglavnom postiže tako što je disipacija snage tranzistora (zatim i većih strukturnih jedinica) konstantna u svakoj periodi takta za sve procesuirane logičke vrijednosti. Nastale logičke familije mogu se dalje istraživati u smislu otkrivanja nezavisnosti nekih drugih parametara od procesuiranih podataka, kao što su dinamička struja ili struja curenja (posebno u najnovijim tehnologijama gdje vrijednosti struja curenja nijesu zanemarljive). Na taj način se može otkriti efikasnost logičkih familija i kada je kriptografski uređaj napadnut analiziranjem neke druge, ali takođe lako mjerljive *side-channel* informacije.

Tehnike koje se koriste za implementaciju logičkih ćelija zovu se logički stilovi. Najpopularniji logički stil za izgradnju logičkih ćelija, baziran na PMOS i NMOS tranzistorima je CMOS. U trenutku nastanka napada baziranih na analizi snage kriptografskog uređaja [36], kod statičke CMOS logike, koja je i danas podrazumijevani logički stil u bibiliotekama standardnih ćelija koje se koriste za izradu i ujedno zaštitu integrisanih kola,

statička disipacija snage je bila zanemarljiva, a dinamička disipacija snage je mjerljiva u slučaju promjene ulaza iz 1 u 0, odnosno izlaza iz 0 u 1. U slučaju promjene ulaza iz 0 u 1 dolazi do pražnjenja kondenzatora, a u slučajevim 0-0 i 1-1 nema disipacije snage. Upravo ovaj asimetrični režim disipacije snage daje potrebne informacije napadaču o načinu funkcionisanja kriptografskog uređaja i dozvoljava mu da otkrije skriveni ključ. Logički stil sa disipacijom snage nezavisnom od procesuiranih podataka ne otkriva takav vid informacije napadaču. Takav logički stil je DRP (*Dual-Rail Precharge*).

DRP logički stil kombinuje koncepte DR (*Dual-Rail*) logike i logike predpunjenja (*precharge logic*). Rezultirajuća funkcionalnost gradi temelj za logičke ćelije tako da imaju konstantnu disipaciju snage u svakoj periodi takta. Osim ove funkcionalsnoti, DRP ćelije i žice među njima moraju biti izgrađene na posebno balansiran način, kako bi se postigla konstantna disipacija snage.

U odnosu na SR (*Single-Rail*) logiku kod koje se logički signal a prenosi jednom žicom, DR logika koristi par žica za ovu namjenu (Sliak 4.7). U DR logici, jedna žica prenosi neinvertovani signal a, dok druga žica prenosi invertovani signal $\bar{a}$. Ovakav tip kodiranja poznat je pod nazivom - diferencijalno kodiranje. Dakle, validni logički signal je takav da dvije žice prenose komplementarne vrijednosti, tj. dok je jedna postavljena na vrijednost 1, druga je postavljena na vrijednost 0. Ove dvije žice DR žičanog para se često zovu komplementarnim žicama.



a) b)

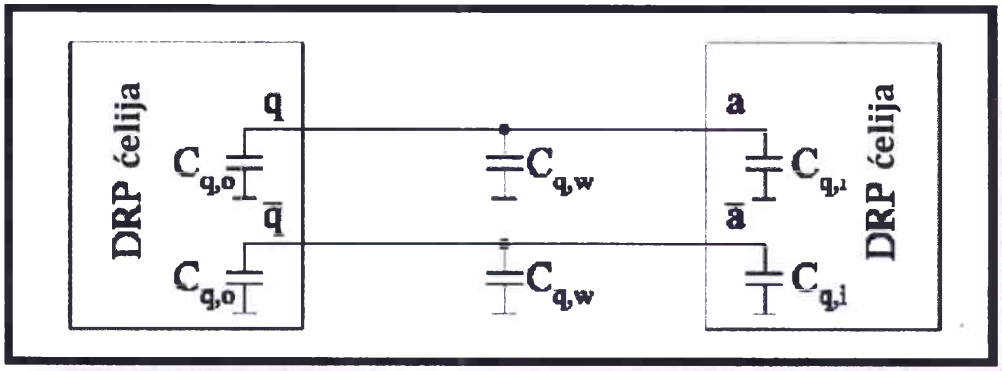
Slika 4.7 – a) SR ćelija sa dva ulaza, b) odgovarajuća DR ćelija sa dva ulaza

U logici predpunjenja svi logički signali alterniraju između tzv. vrijednosti predpunjenja i logičke vrijednosti koja se procesuira. Vrijednost predpunjenja iznosi ili 1 ili 0. Faza u kojoj se svi signali postavljaju na vrijednost predpunjenja zove se faza predpunjenja (*precharge phase*), dok faza u kojoj se svi signali postavljaju na svoje trenutne vrijednosti je faza evaluacije (*evaluation phase*). Obje ove faze kontrolisane su signalom takta. U većini slučajeva, logička vrijednost signala takta definiše fazu u kojoj se kolo trenutno nalazi. To znači da tokom jedne periode takta, signali prođu kroz fazu predpunjenja i fazu evaluacije.

Kombinacija DR logike i logike predpunjenja vodi ka DRP logici gdje su svi signali kodirani u vidu komplementarnih žica. Tokom faze evaluacije, vrijednosti na komplementarnim žicama postavljene su prema procesuiranim podacima na (0,1) ili (1,0). Kada je kolo prebačeno na fazu predpunjenja, vrijednosti na komplementarnim žicama su postavljene na vrijednost predpunjenja koja je ili 1 ili 0. Ako pretpostavimo da je vrijednost predpunjenja jednaka 0, a da prva polovina periode takta odgovara fazi evaluacije, onda će uvijek jedan od komplementarnih izlaza DRP ćelije izvoditi prelaze 0⟶1⟶0 tokom periode takta. Drugi komplementarni izlaz će svo to vrijeme iznositi 0. Ovo znači da DRP ćelija ima uvijek iste prelaze na svojim izlazima tokom svake periode takta. Ovi prelazi se pojavljuju ili kod izlaza q ili kod izlaza $\bar{q}$, zavisno od ulaznih vrijednosti. Upravo ovakvo funkcionisanje DRP ćelije omogućava konstantnu disipaciju snage.

U odnosu na probleme sa mjerama zaštite na nivou kola vezane za eksploataciju gličeva, DPR logika je nezavisna od uticaja gličeva, ali izgradnja dvije balansirane žice zahtijeva *full-custom* pristup čime se povećavaju troškovi dizajna i održavanja. Da bi razumjeli šta podrazumijeva balansiranje komplementarnih izlaza, potrebno je izanalizirati kapacitivna opterećenja na komplementarnim izlazima C_q i $C_{\bar{q}}$. Naime, ova opterećenja se sastoje iz tri dijela: izlazne kapacitivnosti DRP ćelije C_o, kapacitivnosti žice C_w koja spaja DRP ćeliju sa sljedećim DRP ćelijama i sume ulaznih kapacitivnosti C_i ovih ćelija. Na Slici 4.8 prikazana je situacija za oba komplementarna izlaza DRP ćelije q i $\bar{q}$ na koju se nadovezuje sljedeća DRP ćelija sa komplementarnim ulazima a i $\bar{a}$. Kako bi se balansirali C_q i $C_{\bar{q}}$, potrebno je balansirati sva tri dijela ovih kapacitivnih opterećenja. Kapacitivnosti $C_{q,o}$ i $C_{\bar{q},o}$ mogu se izbalansirati preciznim dizajniranjem DRP ćelija. To znači da oba izlaza moraju biti povezana sa istim brojem tranzistora koji imaju iste parametre (širina, itd.). Takođe, žice unutar ćelija koje se povezuju sa komplementarnim izlazima moraju imati istu kapacitivnost.

Na sličan način moguće je balansirati kapacitivnosti $C_{q,i}$ i $C_{\bar{q},i}$. Kod modernih tehnologija digitalnih kola, najveći doprinos izlaznim kapacitivnostima logičke ćelije daje C_w. Iz tog razloga najbitniji zadatak je balansiranje $C_{q,w}$ i $C_{\bar{q},w}$. To se postiže pravilnim raspoređivanjem i rutiranjem DRP ćelija. Predložena metoda raspoređivanja (*placing*) i rutiranja (*routing*) DRP ćelija na balansiran način zove se diferencijalno rutiranje [82] i ovom metodom se komplementarne žice rutiraju paralelno. Prototip čipa koji je implementiran koristeći ovu metodu prezentovan je u [83].



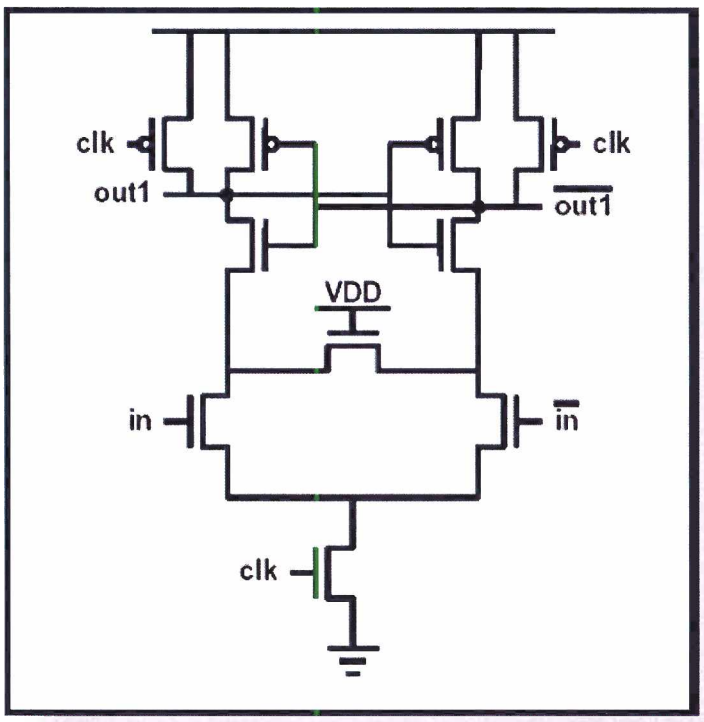
Slika 4.8 – Kapacitivnosti na komplementarnim izlazima DRP ćelije

Najefektivniji primjeri DRP logičkog stila su SABL (*Sense Amplifier Based Logic*), WDDL (*Wave Dynamic Differential Logic*), 3sDL (*3-state Dynamic Logic*), DSDR (*Dual-Spacer Dual-Rail Logic*) i najnovija *TDPL* (*Three-Phase Dual-Rail Precharge Logic*) logika.

SABL (*Sense Amplifier Based Logic*) ćelije su dizajnirane tako da je interna disipacija snage konstantna, a vrijeme evaluacije TOE (*Time Of Evaluation*) nezavisno od procesuiranih podataka, tj. SABL ćelije izračunavaju izlazne vrijednosti kao funkciju ulaznih vrijednosti, ali tek kada se svi ulazni signali postave na komplementarne vrijednosti [84]. Takođe, da bi disipacija snage bila konstantna potrebno je da i izlazni kondenzatori budu ekvivalentni. Posljedica ovakvog dizajna je velika otpornost na napade bazirane na analizi snage (struja) kriptografskog uređaja, ali implementacija SABL ćelija se mora izvršiti "od nule", tj. ne može se nadograditi na već kreiranu logičku ćeliju (Slika 4.9). U SABL kriptografskim uređajima

kombinatorna logika je povezana sa signalom takta i sve SABL ćelije se predpune istovremeno.

Prostorni zahtjevi za implementaciju SABL ćelija su minimum udvostručeni u odnosu na implementaciju CMOS ćelija. Takođe, disipacija snage SABL uređaja je značajno povećana, ali se ne može definisati generalni faktor tog uvećanja. Razlog tome je što uvećanje zavisi od mnogih različitih aspekata: veličine SABL uređaja, odnosa kombinatornih i sekvencijalnih ćelija u uređaju, statistike ulaznih podataka, itd. [85].



Slika 4.9 – SABL invertor

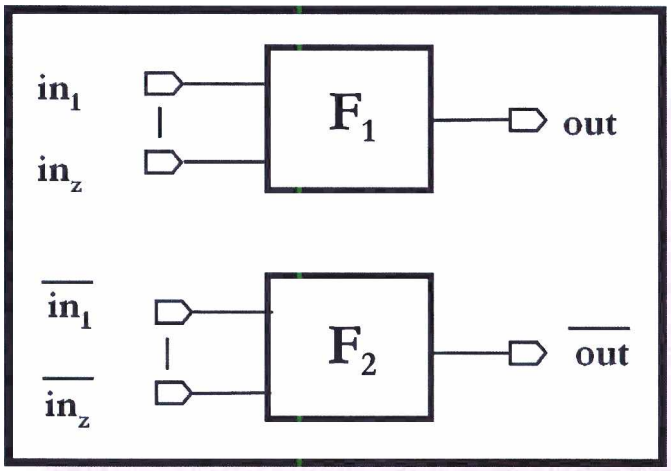
WDDL (*Wave Dynamic Differential Logic*) ćelije bazirane su na osnovama SR (*single-rail*) ćelija koje su na raspolaganju u postojećim bibliotekama standardnih ćelija [86]. Njihova struktura je znatno jednostavnija od SABL ćelija što vodi ka manjim WDDL uređajima. Njihova disipacija snage i vrijeme evaluacije su zavisni od procesuiranih podataka,

a njihova prednost je što mogu biti realizovani i u FPGA (*Field Programmable Gate Arrays*) tehnologiji [84].

U WDDL uređajima, samo sekvencijalne ćelije su povezane sa signalom takta i samo se one predpune i evaluiraju u isto vrijeme. Zato se vrijednost predpunjenja, kao i komplementarne vrijednosti dobijene WDDL ćelijama kreću kao talas (*wave*) kroz kombinatornu logiku WDDL uređaja, po čemu je ona i dobila ime [87].

Na Slici 4.10 prikazana je opšta struktura kobinatorne WDDL ćelije, koja se znatno razlikuje od strukture sekvencijalne WDDL ćelije. Kombinatorna WDDL ćelija sastoji se iz dva kola koja realizuju *Boole*-ove funkcije F_1 i F_2 koje zadovoljavaju sljedeću jednačinu:

$$F_1(in_1, \dots, in_z) = \overline{F_2(\overline{in_1}, \dots, \overline{in_z})} \tag{4.5}$$



Slika 4.10 – Opšta struktura kombinatorne WDDL ćelije

Još jedan DRP logički stil je 3sDL (*3-state Dynamic Logic*) [88] kod kojeg je vrijednost napona predpunjenja $\frac{V_{DD}}{2}$. Na kraju faze evaluacije, uvijek jedan komplementarni izlaz je postavljen na $V_{DD,}$ a drugi na masu. U sljedećoj fazi predpunjenja, dvije

komplementarne žice su spojene i ukoliko imaju ista kapacitivna opterećenja, naponski nivo obje žice je postavljen na $\frac{V_{DD}}{2}$. Ovaj pristup štedi energiju. Još jedna specifičnost 3sDL logičkog stila je da se invertovani izlaz ćelije ne rutira kroz kolo, već se invertovanom izlazu dodaje kondenzator čija se kapacitivnost poklapa sa kapacitivnošću neinvertovanog izlaza (*dummy condensator*). Glavna mana ovakvog pristupa je da se uparivanje mora odraditi individualno za svaku ćeliju u kolu.

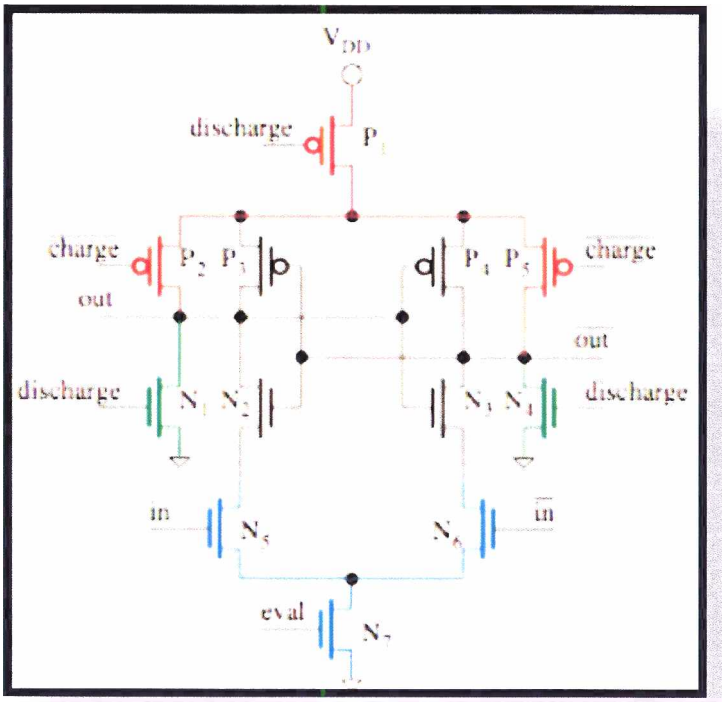
Specifičnost DSDR (*Dual-Spacer Dual-Rail*) logike je što se *dual-rail* žičani par u jednoj periodi takta predpuni na (0,0), a u sljedećoj periodi takta na (1,1) i tako naizmjenično [89], [90]. Na taj način je osigurano da komplementarni izlazni signali su prekidački u svakoj periodi takta (na početku *precharge* faze). Kao rezultat, disipacija snage logičkog kola tokom čitave periode takta nije pod uticajem eventualnog debalansa komplementarnih izlaza, tj. povezanosti izlaza sa različitim vrijednostima izlaznih kondenzatora.

TDPL (*Three-Phase Dual-Rail Precharge Logic*) logika je najmlađa od svih DRP logičkih stilova i svakako najmanje istražena. Iz tog razloga, a i zbog velikih potencijala u domenu hardverskih zaštitnih mjera kriptografskih uređaja od *side-channel* napada, ona je i jedna od bitnih tema ove doktorske disertacije (Poglavlje VII).

TDPL logiku karakterišu tri faze rada: faza predpunjenja (*precharge phase*), faza evaluacije (*evaluation phase*) i faza pražnjenja (*discharge phase*) [91]. Tokom faze predpunjenja izlazne linije opšteg logičkog kola se postavljaju na vrijednost V_{DD}, a tokom faze evaluacije jedna od njih se prazni do vrijednosti V_{SS} na osnovu vrijednosti ulaznog signala, dok se tokom faze pražnjenja prazni i druga izlazna linija.

Posljedica ovakvog funkcionisanja, s obzirom da su oba ulaza predpunjena do V_{DD} i ispražnjena do V_{SS}, pokazuje da TDPL logičko kolo ima konstantnu disipaciju snage tokom radnog ciklusa, nezavisno od toga da li su izlazna kapacitivna opterećenja izbalansirana. Upravo dodavanjem faze pražnjenja se balansira disipacija snage i oba izlazna signala mijenjaju svoju vrijednost tokom radnog ciklusa. Dakle, u odnosu na druge DRP logičke stilove, kod TDPL-a se ne mora voditi računa da izlazna kapacitivna opterećenja budu jednaka.

Ovakav koncept rada se može implementirati kao nadogradnja SABL logičke ćelije sa minimalnim povećanjem u prostoru kola. Na taj način SABL ćelije služe kao reper za izgradnju ekvivalentnih TDPL ćelija. Na Slici 4.11 prikazan je TDPL inverter koji je realizovan tako što su SABL inverteru dodata dva *pull-down* NMOS tranzistora (N_1, N_4) i jedan PMOS prekidač (P_1) kako bi se implementirala faza pražnjenja.

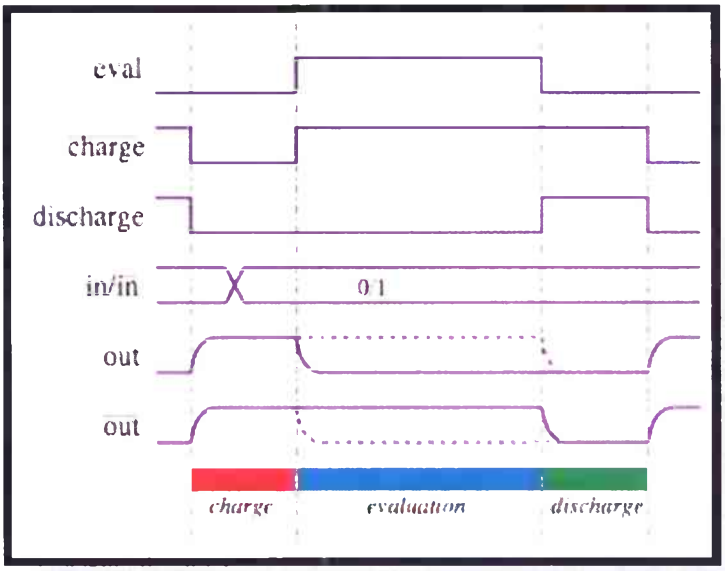


Slika 4.11 – TDPL inverter

Kao što se može vidjeti na vremenskom dijagramu rada TDPL invertera (Slika 4.12), izvode se sljedeće operacije:

- *charge* (*precharge phase*) – na početku svakog radnog ciklusa signal **discharge** ima vrijednost logičke 0, pa iz tog razloga dolazi do pražnjenja *pull-down* tranzistora (N_1, N_4), dok tranzistor P_1 provodi. Takođe, i signal $\overline{\textbf{charge}}$ ima vrijednost logičke 0, pa su obje izlazne linije predpunjene na V_{DD}.

- *evaluation* - tokom ove faze signal **eval** ima vrijednost logičke 1, a u zavisnosti od vrijednosti ulaznih podataka (**in**, $\overline{\textbf{in}}$), na uzlaznoj ivici signala **eval**, tranzistor N_7 provodi i na taj način dolazi do pražnjenja jednog od izlaznih signala (**out**, $\overline{\textbf{out}}$).
- *discharge* – na kraju svakod radnog ciklusa, signal **discharge** se aktivira kroz *pull-down* tranzistore (N_1, N_4) i ima vrijednost logičke 1, pa dolazi do pražnjenja i drugog izlaznog signala koji to nije odradio tokom faze evaluacije.



Slika 4.12 – Vremenski dijagram TDPL invertera

§ *IV.3 Zaključci*

Uvodni dio poglavlja obuhvata analizu postojećih algoritamskih i hardverskih mjera zaštite kriptografskih jezgara pametnih kartica od *side-channel* napada koji su bazirani na analizi snage (struje). Predstavljena je jedna od najuspješnijih softverskih tehnika za zaštitu kriptografskog uređaja/algoritma - maskiranje, a na primjeru AES algoritma prikazane su operacije i koraci maskiranja.

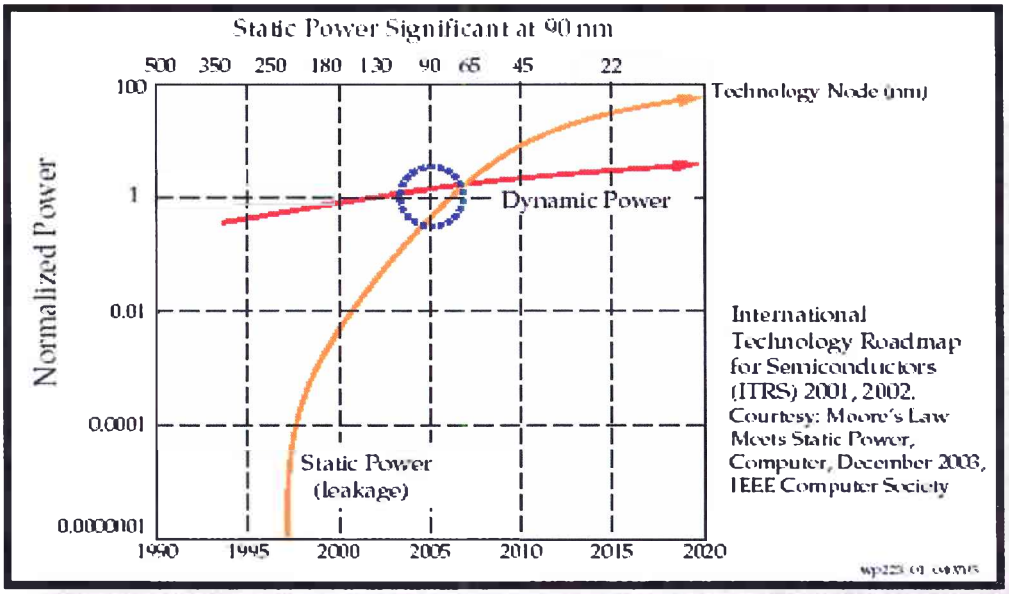
Hardverske mjere zaštite, koje su od posebnog interesa za ovaj rad, klasifikovane su prema uključenom nivou implementacije hardvera na mjere zaštite na nivou sistema, kola i

tranzistora. Za sva tri tipa hardverskih mjera zaštite navedene su najsavremenije tehnike koje se koriste u praksi. Posebna pažnja je posvećena mjerama zaštite na nivou tranzistora, jer se doprinos ove doktorske teze ogleda u testiranju i poređenju najpopularnijeg i najčešće implementiranog logičkog stila za izgradnju logičkih ćelija - CMOS, i najnovijeg DRP logičkog stila - TDPL. Objašnjeni su principi DRP logike sa podrobnim opisom najefektivnijih primjera DRP logičkog stila (SABL, WDDL, 3sDL, DSDR, TDPL).

V Zavisnost struje curenja od tehnologije, temperature i Hamming-ove težine ulaznih podataka

Članak *Gordon Moore*-a je imao nevjerovatan efekat na razvoj industrije [92]. Intenzivan razvoj računarskih komponenti i računarskih sistema doveo je do rasta proizvodnje koji se bliži eksponencijalnom. Značaj *Moore*-ovog zakona u proteklih 45 godina je neprikosnoven i do sada predstavlja najdugovječniju predikciju u industriji informacionih tehnologija. Dakle, prema ovom zakonu broj tranzistora koji se može smjestiti na kvadratni inč silicijuma duplira se svakih 18-24 mjeseca. Iako ovo jeste tumačenje grafikona iz originalnog članka, *Moore* nije bio skoncentrisan samo na prost broj tranzistora, odnosno na njihovu veličinu, već i na smanjenje troškova izrade samih tranzistora. Bilo da je u pitanju promjena tehnologije ili povećanje obima proizvodnje, krajnji efekat koji je *Moore* predvidio bio je usmjeren na pojavu jeftinih, sveprisutnih, moćnih tranzistora koji bi imali izuzetan uticaj na život i ljudsku djelatnost. Ovo razmišljanje utemeljilo je pravac razvoja elektronske industrije u ostatku XX i nadalje XXI vijeka.

Povećanjem broja tranzistora na čipu, njegova složenost raste istim tempom. Očekivano je da istim tempom raste i brzina kojom komponente rade, a kao posljedica i količina toplote koju one oslobađaju. Skaliranje dimenzija tranzistora propraćeno je većim strujama (statičkim i dinamičkim) i ujedno povećanjem disipacije snage, što zahtijeva skuplje pakovanje i rashladnu tehnologiju. Prilikom projektovanja CMOS integrisanih kola, pored optimizacija za velike brzine i male površine, neophodna je i optimizacija za malu potrošnju. Za tehnologije čije su širine kanala veće od 90nm dominantan uticaj ima utrošak snage u dinamičkim režimima, dok kod tehnologija sa širinom kanala od 90nm i manje, statička disipacija ima dominantan uticaj kako na potrošnju, tako i na performanse dizajna (Slika 5.1) [93]. U ovom poglavlju, upravo zbog navedenih karakteristika CMOS tehnologije, izvršićemo komparaciju dobijenih rezultata napada baziranih na analizama struje curenja (CLA) na CMOS kola integrisana u 90nm-skoj i 65nm-skoj tehnologiji.



Slika 5.1 – *ITRS* mapa za prikaz promjena dinamičke i statičke disipacije snage tokom godina [94]

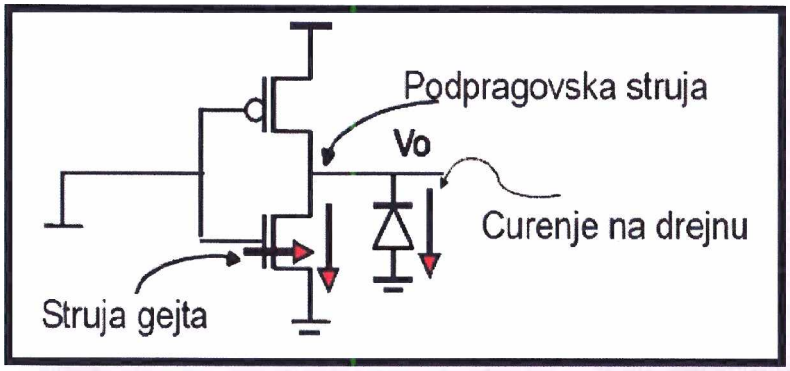
Istorijski, primarni doprinos disipaciji snage u CMOS kolima pripisivan je punjenju i pražnjenju parazitnih kapacitivnosti, tj. dinamičkoj disipaciji snage. Ova komponenta disipacije snage je proporcionalna kvadratu napona napajanja V_{DD}. Iz tog razloga, čip-dizajneri su u protekle dvije decenije na svake dvije godine u cilju najefikasnijeg smanjenja potrošnje snage, skalirali napon napajanja V_{DD} za faktor 0.7X. Da bi prekidačka frekvencija tranzistora ostala ista, potrebno je proporcionalno skalirati i napon praga provođenja tranzistora V_T (*threshold voltage*). Negativan efekat skaliranja napona praga V_T jeste eksponencijalni rast podpragovske struje curenja:

$$I_D = k_x \frac{W}{L} e^{\frac{V_{GS}-V_T}{nV_t}} \left(1 - e^{-\frac{V_{DS}}{V_t}}\right) \tag{5.1}$$

pri čemu je k_x konstanta koja zavisi od procesnih parametara, W i L predstavljaju širinu i dužinu kanala, V_{GS} je napon gejt-sors, V_{DS} je napon drejn-sors, n je različito od 1 (npr. $n \approx 1.5$), a V_t je termički napon ($V_t = kTq$).

Pokazuje se da 30-50% od ukupne disipacije snage, pa čak i više, u 90nm-skoj i 65nm-skoj CMOS integrisanoj tehnologiji potiče od struja curenja. Takođe, u aktuelnim CMOS tehnologijama podpragovska struja curenja je mnogo veća od ostalih komponenti struje curenja. Da bi skaliranje u CMOS tehnologiji bilo moguće, esencijalno je da dizajneri kola i arhitekte sistema razumiju izvore struja curenja, njihov uticaj na dizajn kola i sistema, kao i načine smanjenja tog uticaja. Sa druge strane, upravo te karakteristike struja curenja u nanometarskim tehnologijama, kao što su 90nm-ska i 65nm-ska CMOS tehnologija, omogućavaju da se informacije o njima iskoriste u kreiranju napada na kriptografska jezgra.

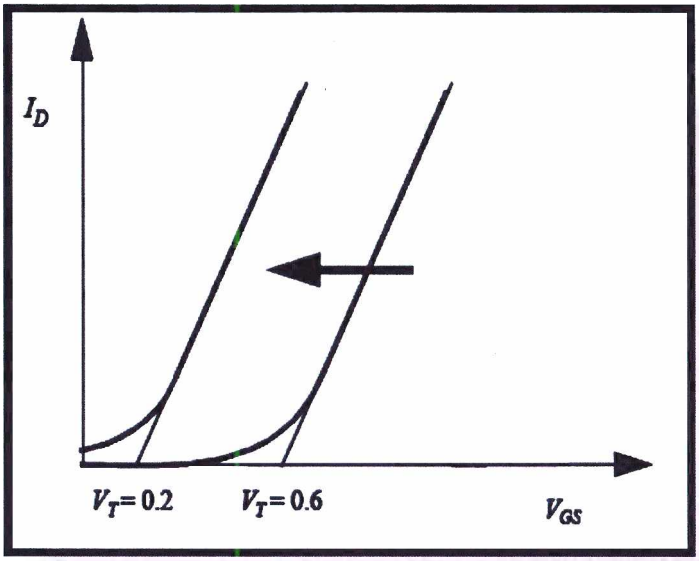
Tri su glavna izvora struje curenja (Slika 5.2) [95]:



Slika 5.2 – Izvori struje curenja

- podpragovska struja curenja (*subthreshold leakage)* – najznačajnija je komponenta struje curenja, jer je u aktuelnim CMOS tehnologijama ova komponenta znatno veća od ostalih. Podpragovska struja curenja se javlja usljed difuzije nosilaca između sorsa i drejna kada napon između gejta i sorsa V_{GS} dostigne tačku slabe inverzije, ali je još uvijek ispod napona praga V_T, gdje je dominantan drift nosilaca. Što je napon praga V_T bliži 0V, to je veća podpragovska struja curenja pri V_{GS} = 0V (Slika 5.3), a samim tim je veća i statička disipacija snage. Zapravo,

smanjujući V_T za 100mV uvećava se struja curenja za faktor 10. Takođe, struja curenja se uvećava smanjivanjem dužine tranzistora. Posljedica toga je da u čipu tranzistori, koji imaju manji napon praga provođenja i/ili dužinu usljed varijacija procesnih parametara, više doprinose porastu ukupne struje.



Slika 5.3 – Skaliranje napona praga povećava podpragovsku struju curenja kada je V_{GS} = 0V

- struja curenja na inverzno polarisanim spojevima *well-supstrat*-a *(junction leakage)* – je struja koja se javlja kada je tranzistor zakočen, i teče od sorsa ili drejna ka podlozi (*substrate*) kroz inverzno-polarisane (*reverse-biased*) diode. Npr. ako na ulaz invertora dovedemo logičku nulu, NMOS je zakočen, PMOS provodi, a izlazni napon je V_{DD}. Nakon toga, napon između drejna i podloge je jednak naponu napajanja V_{DD}, što rezultira strujom curenja kroz inverzno-polarisanu diodu. Veličina struje curenja kroz diodu veoma zavisi od temeperature (udvostručava se na svakih 5°C porasta temperature).

- struja tunelovanja kroz gejt *(gate direct tunneling leakage)* – je struja koja teče od tunela kroz sloj oksida do podloge i eksponencijalno raste sa smanjenjem debljine sloja oksida T_{OX} i napona napajanja V_{DD}. Za relativno malu debljinu oksida (oko 2-3nm), kada je V_{GS} = 1V, svako smanjenje T_{OX} za 0.2 nm dovodi do desetostrukog povećanja ove komponente struje. Što se tiče temperaturne zavisnosti, ova komponenta struje curenja se udvostručava na svakih 100°C. Način da se izbjegne veliki rast ove komponente struje, a zadrži kontrola gejta nad kanalom, jeste zamjena sloja izolatora – silicijum dioksida (SiO_2), koji se koristi u aktuelnim tehnologijama (još od 1960. godine). Ovaj izolator napravljen je od *high-k* dielektričnih materijala (materijali sa visokom dielektričnom konstantom) koji dozvoljavaju dalje smanjenje debljine oksida, a implementira se već u 45nm-skoj tehnologiji [96].

§ V.1 Komparacija struja curenja za CMOS kola projektovana u 90nm-skoj i 65nm-skoj tehnologiji

Najčešće korišćene tehnike za smanjenje struja curenja u CMOS kolima su kontrola vrijednosti ulaznog podatka, povećanje napona praga provođenja, isključivanje napona napajanja, itd. [97], [98], [99]. Tehnika kontrolisanja vrijednosti ulaznih podataka bazira se upravo na zavisnosti struja curenja u CMOS kolima od odgovarajućih vrijednosti na ulazima u CMOS kola [100], [101]. Ovdje će biti prikazana ta zavisnost i moguća kontrola struja curenja, kao i zavisnost od vrste korišćene tehnologije – 90nm-ske i 65nm-ske tehnologije.

Procjenu struja curenja u "stand-by" režimu za konkretan ulazni podatak moguće je dobiti simulacijom kola. Ukupan broj vrijednosti ulaznog podatka za kolo sa N ulaza je 2^N. Sva testirana CMOS kola implementirana su i simulirana u programu Cadence, koristeći standardne *Bsim4* modele h-tipa tranzistora [102] firme ST Microelectronics 90nm-ske i 65nm-ske tehnologije.

Tabela V.1 –Struja curenja kroz CMOS kola:

a) 90nm-ska tehnologija; b) 65nm-ska tehnologija

NOT Gate CMOS090 [A]					
A	T=0°	T=25°	T=50°	T=75°	T=100°
0	1.364n	3.19n	6.521n	11.98n	20.19n
1	238p	733.3p	1.895n	4.249n	8.489n
NAND2 Gate CMOS090 [A]					
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	168.5p	465.3p	1.1n	2.294n	4.327n
0	1	1.363n	3.19n	6.518n	11.97n	20.16n
1	0	1.02n	2.441n	5.089n	9.515n	16.3n
1	1	475.9p	1.466n	3.79n	8.498n	16.18n

a)

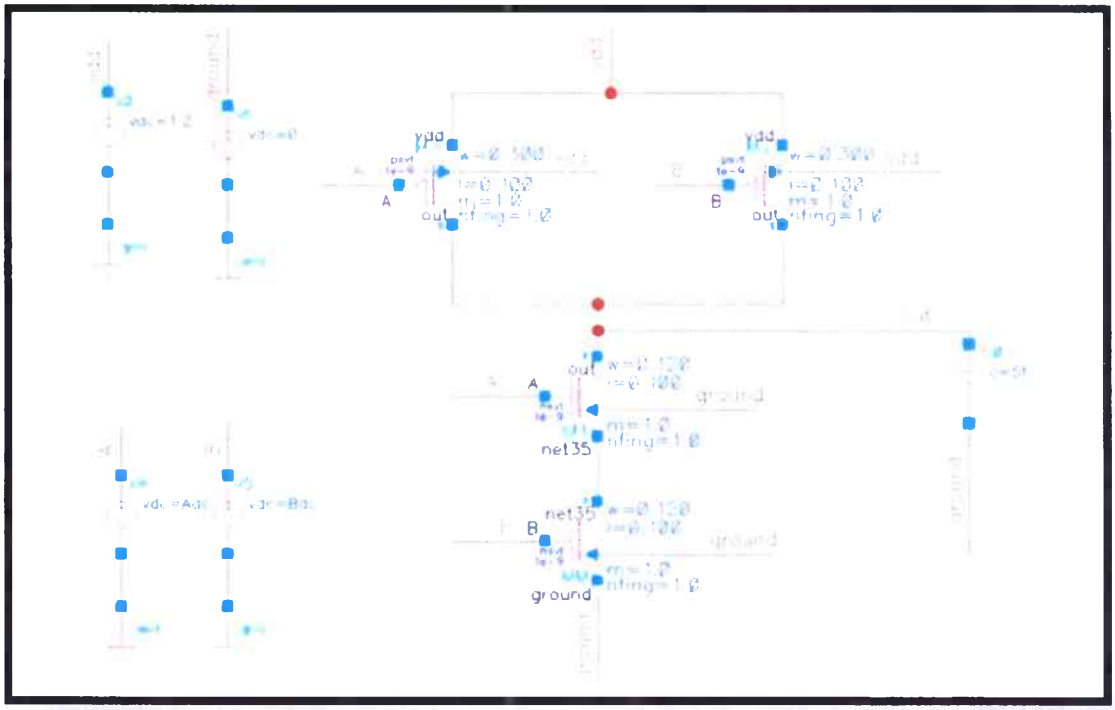
NOT Gate CMOS065 [A]					
A	T=0°	T=25°	T=50°	T=75°	T=100°
0	2.673n	2.986n	3.661n	6.571n	11.456n
1	0.134n	0.473n	1.407n	2.346n	4.896n
NAND2 Gate CMOS065 [A]					
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	2.372n	2.456n	2.591n	4.567n	9.987n
0	1	2.654n	2.982n	3.661n	6.787n	11.437n
1	0	2.52n	2.773n	3.297n	6.212n	11.102n
1	1	0.261n	0.94n	2.813n	4.315n	9.102n

b)

Za invertor i NAND2 kolo u 90nm-skoj tehnologiji korišćeni su sljedeći parametri: V_{DD} = 1.2V, L =100nm, širina NMOS tranzistora W_{NMOS} = 120nm, širina PMOS tranzistora W_{PMOS} =2.5 x 120nm = 300nm, C_L = 5fF. Parametri u 65nm-skoj tehnologiji su: V_{DD} = 1.2V, L =60nm, W_{NMOS} = 120nm, W_{PMOS} =2.5 x 120nm = 300nm, C_L = 5fF. Takođe, uzeto je u obzir pet različitih temperatura (0°, 25°, 50°, 75°, 100°) da bi se potvrdila visoka zavisnost struje curenja od temperature. Simulacije su vršene za NOT i NAND2 kola, a rezultati simulacija struja curenja prikazana su u Tabeli V.1.a).

Dakle, značajna zavisnost struja curenja od ulaznih vrijednosti potvrđena je podacima unutar Tabele V.1. Kada su u pitanju simulirane struje curenja invertora, primjećuje se da je struja curenja za ulaz 0 veća od struje curenja za ulaz 1 pri svakoj radnoj temperaturi kola, što je posljedica činjenice da je vrijednost napona V_T kod NMOS tranzistora niža u odnosu na PMOS tranzistor. Takođe, u Tabeli V.1.a) pokazuje se da je ta razlika u strujama curenja među ova dva ulaza određena faktorom 3-6, dok je taj faktor još veći u Tabeli V.1.b). Dalje se može primijetiti da je rast struja curenja u 90nm-skoj tehnologiji (npr. za ulaz 0 korespondentne struje curenja su 1.36, 3.19, 6.52, 11.98, 20.19) znatno veći u odnosu na 65nm-sku tehnologiju (npr. za ulaz 0 korespondentne struje curenja su 2.67, 2.98, 3.66, 6.57, 11.45). To je pokazatelj da je zavisnost struja curenja od radne temperature slabija za 65nm-sku tehnologiju u odnosu na 90nm-sku tehnologiju.

Prethodna razmatranja zavisnosti struja curenja od ulaznog podatka mogu se proširiti generalno na statička CMOS kola čije su *pull-up* (PMOS tranzistori) i *pull-down* (NMOS tranzistori) mreže sačinjene od paralelno i serijski povezanih tranzistora. Jedan od zaključaka je da ako se struje curenja poređaju u opadajućem redosljedu (za svaku testiranu temperaturu), ulazne logičke vrijednosti su poređane u istom redosljedu za svaku struju. Da bi se razumjela zavisnost struja curenja od ulaznih podataka, posmatrajmo slučaj dva serijski povezana NMOS tranzistora u kolu NAND2 (Slika 5.4). Uporedimo npr. slučaj kada je B=0 sa slučajem kada je B=1, pod pretpostavkom da je A=1: za B=0 struja curenja je veća nego za ulaz B=1, što je već primijećeno za kolo invertora. Slična razmatranja mogu se lako ponoviti i proširiti na veliki broj serijski povezanih tranzistora i dalje na veliki broj statičkih CMOS kola. Takodje, zapaža se da ako se za svaku radnu temperaturu struje curenja poređaju u opadajućem redosljedu, proizilazi da su i ulazne logičke vrijednosti poređane u istom redosljedu za svaku struju. To znači da npr. za NAND kolo sa dva bita ulaza, i za 90nm-sku i za 65nm-sku tehnologiju, logički ulaz 01 generiše maksimalnu struju curenja za sve vrijednosti temperatura [103]. Ovakav slijed je i logičan s obzirom na jednačinu za podpragovsku struju curenja u invertoru (5.1), gdje sa povećanjem temperature, tj. termičkog napona V_t (pri čemu je $V_{GSn} = 0\text{V}$ i $e^{-\frac{V_{DS}}{V_t}} \approx 0$) struja curenja I_D raste.



Slika 5.4 – Šema CMOS NAND2 kola implementiranog u 90nm-skoj tehnologiji

§ V.2 Zavisnost struja curenja od Hamming-ove težine

Značajna zavisnost struja curenja od ulaznog obrasca osnovnih logičkih kola je karakteristika koju je moguće eksploatisati kako bi se razumjela sveukupna struja curenja kompleksnijih logičkih struktura, kombinatornih i sekvencijalnih. Praktičan primjer kompleksne strukture koja se često susrijeće u realnim uređajima je primjer *bit-sliced* strukture, tj. strukture sa m-bitnim ulazima u kojoj se nalazi m identičnih replika jednog strukturnog kola. Primjeri ovakvih struktura su aritmetičko-logičke jedinice, registri, registarski fajlovi, itd.

U *bit-sliced* strukturama ukupna struja curenja jednaka je sumi struja curenja m-bitnih djelova, pri čemu razlikujemo struju curenja za ulazni bit 1 (I_L) i struju curenja za ulazni bit 0

(I_H). Kako je broj djelova sa strujom curenja kojoj odgovara logički ulaz 1 zapravo ekvivalentan *Hamming*-ovoj težini *w*, ukupna struja curenja $I_{leak.TOT}$ se može prikazati kao:

$$I_{leak.TOT} = w \cdot I_H + (m - w)I_L = w \cdot (I_H - I_L) + m \cdot I_L \qquad (5.2)$$

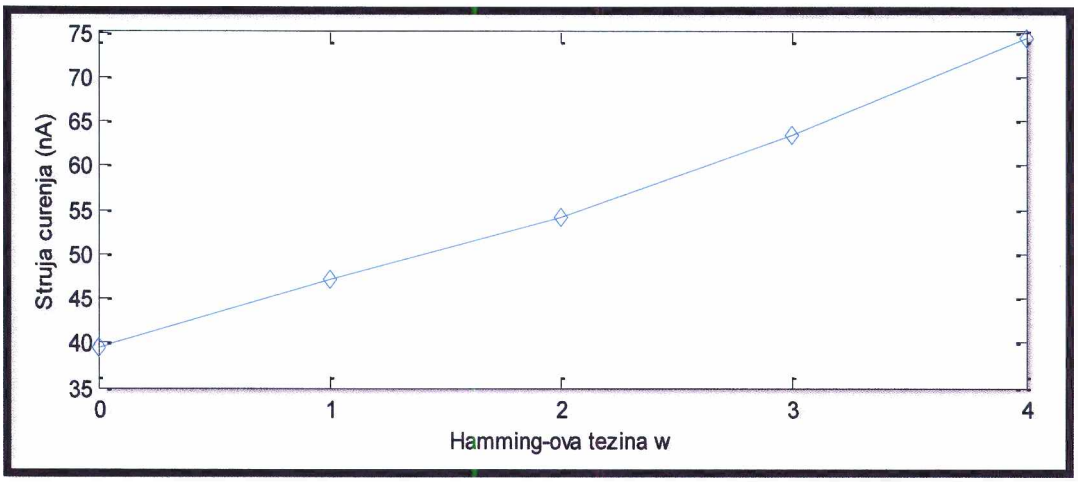
Iz ove jednačine se zaključuje da ukupna struja curenja u kolu linearno zavisi od *Hamming*-ove težine *w* ulazne riječi, a ne od specifične vrijednosti svakog bita. Dakle, *Hamming*-ova težina nekog niza predstavlja ukupan broj simbola koji su različiti od nule, a tipičan slučaj je niz bitova gdje *Hamming*-ova težina označava broj jedinica [104]. Pored *Hamming*-ove težine, često se koristi i pojam *Hamming*-ove udaljenosti (*Hamming distance*) koja kod dva niza jednake dužine predstavlja broj pozicija u kojima su odgovarajući simboli različiti. U teoriji informacija i kodova, korišćenjem gore navedenih pojmova, mogu se definisati uslovi koje određeni kod mora zadovoljiti kako bi se koristio za detekciju i korekciju greške pri prenosu poruka. Inače, model *Hamming*-ove težine je jednostavniji od modela *Hamming*-ove udaljenosti, jer se može primijeniti i u situaciji kada nijesu poznate uzastopne vrijednosti procesuiranih podataka.

Tabela V.2 – Struja curenja kroz 4-bitni registar za različite vrijednosti ulaznog podatka

Ulaz *X*	*Hamming*ova težina *w=H(X)*	$I_{leak.TOT}[nA]$
0000	0	39.44
0001	1	47.05
0010		
0100		
1000		
0011	2	54.01
0101		
0110		
1001		
1010		
1100		

0111	**3**	**63.39**
1011		
1101		
1110		
1111	**4**	**74.30**

Primjer zavisnosti struja curenja od *Hamming*-ove težine ulaznih podataka potvrđen je rezultatima simulacija 4-bitnog registra dizajniranog u 65nm-skoj tehnologiji, pri radnoj temperaturi T=27°, u Tabeli V.2. Analizirajući dobijene rezultate u toj tabeli, očigledno je da struje curenja zavise samo od *Hamming*-ove težine w ulaznih podataka pri čemu je ta zavisnost linearna (Slika 5.5). Parametri I_L i I_H u jednačini (5.2) koje odgovaraju krivoj na Slici 5.5 iznose 9.86nA i 18.58nA, respektivno.



Slika 5.5 – Simulirana struja curenja u funkciji *Hamming*-ove težine ulaznih podataka u 4-bitnim registrima u 65nm-skoj tehnologiji (T=27°)

§ *V.3 Zaključci*

Ovo poglavlje je posvećeno analizi glavnog parametra na osnovu koga se izvode *side-channel* napadi bazirani na analizi struja curenja u hardveru pametne kartice. U tu svrhu, istraženi su izvori struja curenja i primijenjena je tehnika za smanjenje struja curenja u CMOS kolima kontrolom vrijednosti ulaznog podatka. Sva testirana CMOS kola implementirana su i simulirana u programu Cadence, a procijenjena je zavisnost njihovih struja curenja od implementirane tehnologije (90nm-ska i 65nm-ska). Naime, evidentna je značajna zavisnost struja curenja od ulaznih vrijednosti u svim 90nm-skim i 65nm-skim CMOS kolima. Testiranje je izvršeno za pet različitih temperatura, pri čemu je faktor među vrijednostima struja za istu radnu temperaturu veći kod kola sa implementiranom 65nm-skom tehnologijom. Jedan od rezultata analize prikazuje da je rast struja curenja u 90nm-skoj tehnologiji znatno veći u odnosu na 65nm-sku tehnologiju, tj. zavisnost struja curenja od radne temperature slabija je za 65nm-sku tehnologiju u odnosu na 90nm-sku tehnologiju. U okviru ovog poglavlja ispitivana je i utvrđena linearna zavisnost struja curenja od *Hamming*-ove težine ulaznih podataka u *bit-sliced* strukturama na primjeru 4-bitnog CMOS registra dizajniranog u 65nm-skoj tehnologiji.

VI Karakteristike i uspješnost CLA napada i uticaj procesnih varijacija na njegovu efektivnost

Kao što je prikazano u Poglavlju V, struja curenja otkriva *Hamming*-ovu težinu *m*-bitnih podataka X koji su procesuirani unutar dijela kriptografskog jezgra. Otuda, struja curenja obezbjeđuje korisnu informaciju za rekonstrukciju tajnog ključa k kriptografskog uređaja ukoliko procesuirani podaci X, koji su pod uticajem napada, predstavljaju funkciju (ili su dio) tajnog ključa k. Stoga, napad baziran na analizi struja curenja CLA (*Correlation Leakage Analysis*) upravo eksploatiše simulirane i izmjerene struje curenja kriptografskog uređaja.

U pravim kriptografskim uređajima, procesuirani podaci X koji su pod uticajem napada generisani su unutar jednog bloka logičkih kola, koji predstavlja samo dio cjelokupnog čipa. U praktičnim primjerima čvorovi napona napajanja svih blokova unutar čipa nijesu dostupni, tako da mjerni uređaj može mjeriti samo ukupnu struju curenja čipa, koja sadrži i doprinos struje curenja posmatranog bloka. Dakle, ukupna struja curenja u čipu $I_{leak.TOT}$ zavisi od *Hamming*-ove težine $w = H(X)$ signala X koji je napadnut (pri čemu je H operator *Hamming*-ove težine), ali takođe zavisi i od struja curenja svih ostalih blokova logičkih kola koja su implementirana u okviru istog čipa. Kao posljedica, prilikom primjene nasumičnih, ali poznatih ulaznih vrijednosti, struja curenja u čipu $I_{leak.TOT}$ i $H(X)$ su statistički korelisani. Upravo je ovo glavna premisa u CLA napadima. Slična procedura napada može se primijeniti i u CPA (*Correlation Power Analysis*) napadima, kao i u napadima koji su bazirani na analizama dinamičke struje i snage.

Inače, korelacija (lat. *con* = sa, *relatio* = veza) označava povezanost između promjenljivih, a koeficijent korelacije predstavlja mjeru zavisnosti dvije slučajne promjenljive. Najjednostavniji oblik primjene korelacijske analize je kada su promjenljive (npr. promjenljiva X i promjenljiva Y) u linearnom odnosu, što je uzeto i u slučaju analize korelacije u ovom radu, pa će se u nastavku rada podrazumijevati da se radi o linearnom koeficijentu korelacije. Korelacija je manja što ima više različitih vrijednosti promjenljive Y

koje se vežu uz određenu vrijednost promjenljive X, dok je korelacija veća što ima manje takvih vrijednosti promjenljive Y. Pozitivan smjer korelacije pokazuje da porast vrijednosti promjenljive X prati porast vrijednosti promjenljive Y, dok negativan smjer korelacije pokazuje da porast vrijednosti promjenljive X prati opadanje vrijednosti promjenljive Y. Koeficijent korelacije efikasno može biti izračunat preko *Pearson*-ovog koeficijenta korelacije r koji se kreće se u opsegu od -1 do 1, za koji se često koristi formula sljedećeg oblika:

$$r = \frac{\sum XY - \frac{\sum X \sum Y}{N}}{\sqrt{\left(\sum X^2 - \frac{(\sum X)^2}{N}\right)\left(\sum Y^2 - \frac{(\sum Y)^2}{N}\right)}} \tag{6.1}$$

pri čemu je N broj uzoraka, Σ označava sumu, X označava vrijednost na x osi i Y vrijednost na y osi. Svake dvije nezavisne slučajne promjenljive su nekorelisane ($r = 0$), dok obrnuto ne mora da važi, jer je moguće da r ima vrijednost 0, ali da su X i Y povezane nekom relacijom. Kao empirijsko pravilo prihvata se sljedeće:

- $|r| < 0.3$ – postoji sasvim neznatna linearna korelacija između posmatranih veličina i nesigurnog je značenja, naročito ako je obim uzoraka mali;
- $0.3 < |r| < 0.6$ – postoji značajna linearna korelacija koja ima praktičnu primjenu;
- $0.6 < |r| < 0.9$ – pokazuje tijesnu linearnu korelaciju;
- $|r| > 0.9$ – znači vrlo tijesnu linearnu korelaciju.

Procedura izvršenja CLA napada prikazana je u pet koraka (Slika 6.1) i slična je proceduri koja se odnosi na napade bazirane na analizi dinamičkih struja u kriptografskom

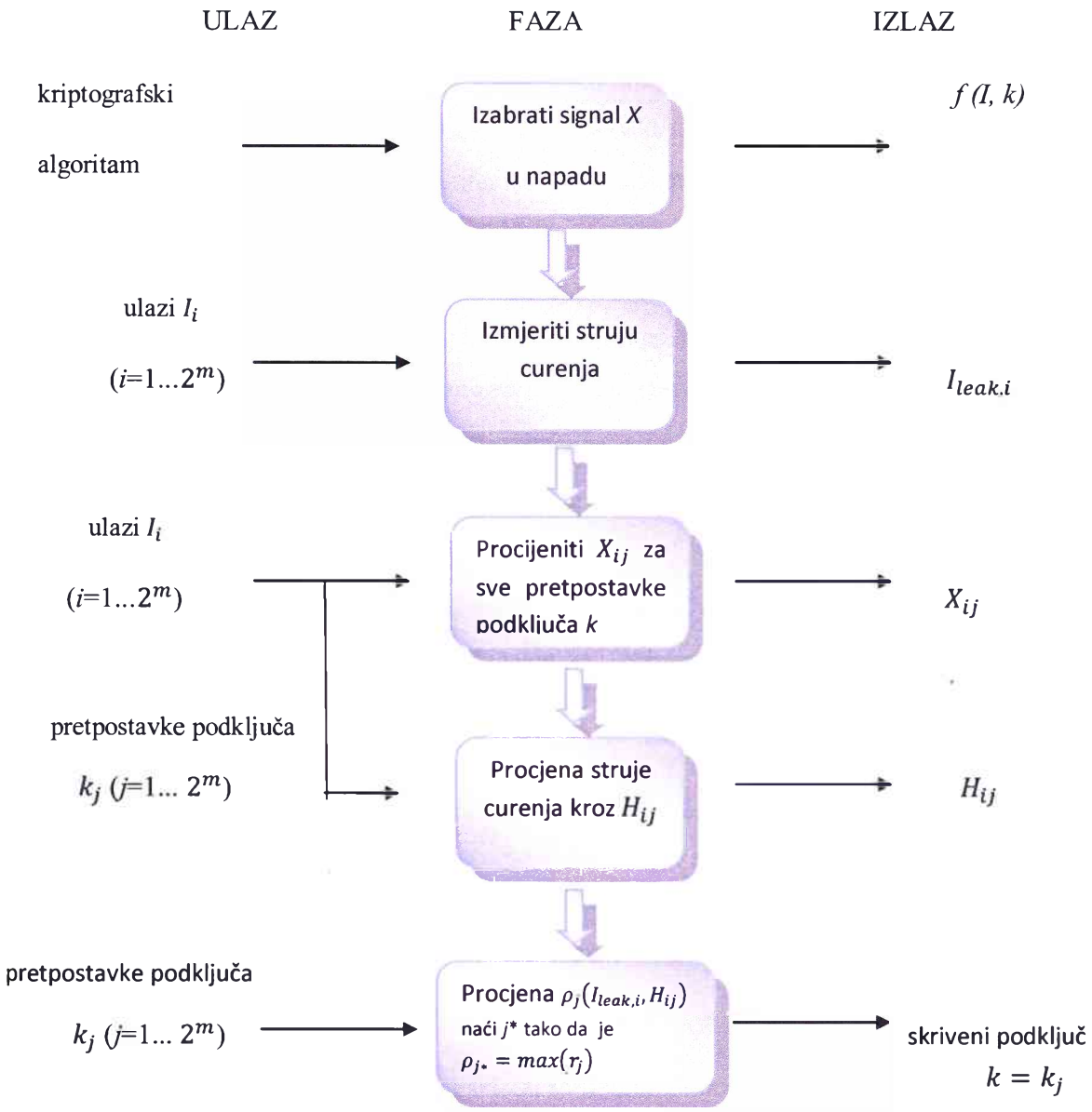
jezgru [42]. Strategija CLA napada se može primijeniti u bilo kom okruženju [35], [105]. Generalno, cilj CLA napada je da otkrije tajne podključeve ili djelove tajnog ključa upotrijebljene u kriptografskom uređaju. Otkrivanje podključa ili dijela ključa je bazirano na velikom broju podataka o strujama curenja (vrijednosti i tragovi struja curenja) koji su snimljeni dok uređaj enkriptuje ili dekriptuje različite blokove podataka. Prednost CLA napada u odnosu na već pomenute SPA napade je ta što nije potrebno detaljno poznavanje kriptografskog uređaja. Često je nepotrebno znati koji je kriptografski algoritam implementiran u kriptografskom uređaju.

U prvom koraku CLA napada potrebno je izabrati interni m-bitni signal X koji je fizički generisan unutar dijela kriptografskog uređaja koji je napadnut. Uobičajena je praksa da signal X zavisi i od ulaza I i od tajnog podključa k prema unaprijed definisanoj funkciji f određenoj od strane kriptografskog algoritma:

$$X = f(I, k) \tag{6.2}$$

U drugom koraku se za različite ulazne vrijednosti I_i (i=1...2^m) mjeri odgovarajuća struja curenja $I_{leak,i}$ u kriptografskom čipu i to u vremenskom trenutku kada se bira signal X. Fizička vrijednost signala X unutar čipa procjenjuje se u sljedećem koraku na osnovu ulaznog signala I_i prema (6.2). Pošto je opšti ulazni podatak obezbijeđen od strane uređaja koji vrši napad, jedina nepoznata vrijednost u (6.2) je tajni podključ k, pa se iz tog razloga on mora nagađati. Za svaku moguću pretpostavku k_j tajnog podključa (j=1... 2^m), rezultirajuća vrijednost $X_{ij} = f(I_i, k_j)$ sa opštim ulazom I_i nađena je prema (6.2). Rezultat ovog koraka je formiranje 2-D niza X_{ij}.

U četvrtom koraku se zahvaljujući linearnoj vezi između struja curenja (unutar bloka koji generiše signal X) i *Hamming*-ove težine $H(X)$ procjenjuje struja curenja prema vrijednosti $H(X)$. Drugim riječima, $H(X)$ se razlikuje od izmjerene struje u nepoznatoj muliplikativnoj konstanti. Rezultat ovog koraka je 2-D niz $H_{ij} = H(X_{ij})$, gdje je (i=1...2^m), (j=1... 2^m), koji se sastoji od *Hamming*-ove težine signala X za sve moguće kombinacije ulaznog signala i podključa.



Slika 6.1 – Procedura CLA napada

U posljednjem koraku se porede vrijednosti izmjerene struje curenja $I_{leak.\,i}$ i procijenjene struje H_{ij}. Za određenu pretpostavku ključa k_j, sekvence $I_{leak,i}$ i H_{ij} povezane nasumičnom, ali poznatom ulaznom sekvencom I_i (i=1... 2^m), mogu se posmatrati kao nasumične promjenljive. U slučaju kada je pretpostavka ključa tačna ($k_j = k$), izmjerena i

procijenjena struja curenja su maksimalno korelisane. Teoretski, u idealnim uslovima, tj. ukoliko bi linearna zavisnost $I_{leak,i}$ od *H(X)* bila precizna i ne bi postojalo drugih strujnih doprinosa, koeficijent korelacije $\rho_j(I_{leak,i}, H_{ij})$ između $I_{leak,i}$ i H_{ij} za vrijednost podključa $k_j = k$ bi tačno iznosio 1 prema zakonima osnovne statistike [106]. Sa druge strane, ukoliko je pretpostavka podključa pogrešna ($k_j \neq k$) izmjerena struja curenja nije u linearnoj vezi sa procijenjenim *H(X),* tj. izmjerena struja i *H(X)* su labavo korelisani i koeficijent korelacije mora biti manji od 1. Ovo znači da se za tačnu pretpostavku podključa dolazi do najveće vrijednosti $\rho_j(I_{leak.i}, H_{ij})$ među svim mogućim pretpostavkama podključa k_j. Dakle, zadatak napadača i uređaja koji vrši napad je da izračuna $\rho_j(I_{leak,i}, H_{ij})$ između izmjerenih struja curenja $I_{leak,i}$ i *Hamming*-ovih težina H_{ij} za (j=1... 2^m), i da identifikuje vrijednost j^* koja daje najveću vrijednost ρ_j:

$$\rho_{j^*} = \max_j \rho_j \tag{6.3}$$

dok vrijednost podključa jednostavno iznosi:

$$k = k_{j^*} \tag{6.4}$$

Ova procedura CLA napada je u skladu sa finalnim korakom CPA napada, iako su CPA bazirani na mjerenjima snage.

§ VI.1 Mjerenje uticaja "intra-die" procesnih varijacija kroz Monte Carlo simulacije

U ovoj disertaciji CLA napadi biće analizirani kroz vidove složenih eksperimentalnih uslova koji su dio realnih napada na kriptografske uređaje pametnih kartica. U cilju boljeg

razumijevanja suštine funkcionisanja CLA napada, biće analiziran uticaj procesnih varijacija u eksperimentalnim rezultatima.

U dizajnu digitalnih kola uparivanje komponenti i postojanje šuma utiču na *layout* (raspored komponenti) analognih integrisanih kola. Uparivanje karakteriše električna razlika između komponenti koje su deklarisane kao identične i ono se smatra najvećom brigom u dizajnu analognih kola. Zapravo, gotovo sve tehnike analognog *layout*-a predstavljaju metode za poboljšanje uparivanja između različitih uređaja na čipu. Na primjer, dva otpornika postavljena jedan blizu drugog istih dimenzija, obično pokazuju razliku u vrijednosti otpornosti. Takođe, dva tranzistora istih dimenzija će najvjerovatnije pokazivati razliku u vrijednosti V_{GS} kada je potrebno postići jednake I_D pri istim vrijednostima V_{DS}. Stoga uparivanje komponenti u analognim integrisanim kolima i integrisanim kolima sa kombinovanim signalima mora biti pažljivo razmatrano [107], [108].

U tipičnom CMOS procesu, apsolutna parametarska tačnost komponenti u odnosu na deklarisanu kao što su tranzistori, otpornici i kondenzatori varira do 20%, dok parametarski odnosi dozvoljavaju uparivanje do 0.1%. Iz tog razloga, implementacija analognih kola se uglavnom bazira na uparivanju komponenti, prije nego li na apsolutnoj tačnosti. I pored izbora odgovarajućih dimenzija tranzistora radi dobrog uparivanja, pažljivo projektovanje *layout*-a mora biti uzeto u obzir.

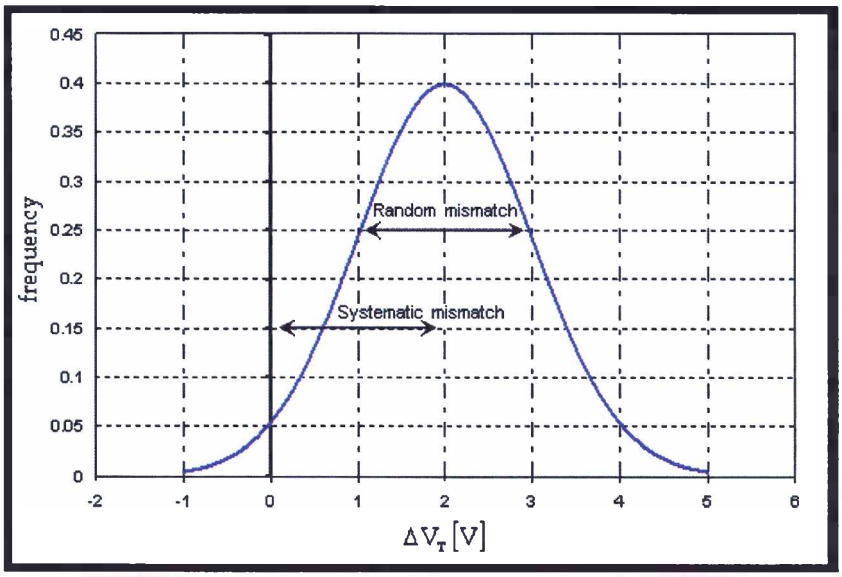
§ *VI.1.1 Procesne varijacije - opis*

Postoje fundamentalno dva različita tipa grešaka koje se javljaju prilikom uparivanja komponenti: sistematične greške i nasumične greške. Sistematične i nasumične greške zajedno čine ukupnu neuparenost (*mismatch*), iako su njihovi uzroci različite prirode.

Sistematična greška je greška koja se ponavlja na isti način u kolima koja su locirana u određenom dijelu *wafer*-a. Pretpostavimo da imamo par uređaja nazvanih A i B (ovi uređaji mogu biti tranzistori, kondenzatori, otpornici). Ovi uređaji će biti sistematično neupareni ukoliko kvantitet izmjeren na uređaju A teži da bude veći/manji nego kvantitet izmjeren na

uređaju *B*, ili obrnuto, a to može biti posljedica komponenti koje nijesu postavljene identično, koje su različito orjentisane, koje su postavljene na prevelikoj udaljenosti. Ključ u eliminisanju sistematične neuparenosti su tehnike pravilnog *layout*-a. Neki od uzroka sistematičnih grešaka mogu biti:

- različito okruženje uređaja (prisustvo termalnih izvora, mehaničkog stresa, parazitnih uređaja);
- neidealnost procesa (obično ono što se nacrta nije ono što se dobije);
- procesne varijacije usljed postojanja susjednih elemenata (uzrokovane gravurom i neželjenim dopiranjem);
- neporavnanje maske koja dovodi do varijacija parazitnih parametara; itd.



Slika 6.2 – Hipotetička distribucija pojave neuparenosti

Drugi tip neuparenosti je nasumična neuparenost. Ukoliko opet posmatramo par uređaja *A* i *B*, kvantitet izmjeren na uređaju *A* nikad neće biti identičan kvantitetu izmjerenom na uređaju *B*, pri čemu postoji jednaka vjerovatnoća da kvantitet na uređaju *A* bude veći/manji od kvantiteta na uređaju *B*, i obratno. Nasumične greške potiču od mikroskopskih fluktuacija

u materijalu, kao što su efekti ivica (hrapavost ivica), nesavršenost materijala (nestalnost dopanta), varijacije u mobilnosti (procesne varijacije). Za razliku od sistematične neuparenosti, nasumična neuparenost se ne može eliminisati. Iz tog razloga će u ovom radu biti analiziran uticaj nasumične neuparenosti, nastao pod uticajem procesnih varijacija u eksperimentalnim uslovima, na efektivnost CLA napada.

Pojava neuparenosti tipično prati normalnu (Gausovu) raspodjelu vjerovatnoće (Slika 6.2). Sistematična greška se matematički izražava kroz srednju vrijednost, dok se nasumična greška matematički izražava kroz standardnu devijaciju mjerene distribucije. Kod dobro projektovanog *layout*-a uređaja, sistematična greška jednaka je nuli. Nasumična greška je statistička mjera i predstavlja standardnu devijaciju neuparenosti mjerenu na velikom broju primjeraka.

Karakteristike neuparenosti usljed nasumične greške možemo sagledati kroz generalnu teoriju o neuparenosti MOS tranzistora koji čine značajan segment u dizajnu CMOS aplikacija [109]. Neuparenost između tranzistorskih parametara koji su od interesa za grupu jednako dizajniranih komponenti je posljedica više nasumičnih procesa koji se javljaju tokom svake faze fabrikacije tranzistora. Sljedeća analiza ukazuje na neuparenost MOS tranzistora kao posljedicu fluktuacije pojedinih parametara u toku fabrikacije, kao i na povezanost različitih parametara usljed te fluktuacije. Ukoliko vrijednost nekog tranzistorskog parametra podijelimo na fiksni dio P (dizajnirana vrijednost parametra) i na nasumično promjenljivi dio ΔP (usljed neuparenosti), varijansa parametra ΔP između dva tranzistora će iznositi:

$$\sigma^2(\Delta P) = \frac{A_p^2}{WL} + S_p^2 D_x^2 \tag{6.5}$$

gdje su W i L širina i dužina komponente, respektivno, A_p je površina proporcionalno konstantna za parametar P, dok S_p definiše varijaciju parametra P sa razmakom D_x među komponentama [110].

Na primjeru rada MOS tranzistora u oblasti zasićenja, gdje je veza struja-napon data izrazom:

$$I_D = \frac{\beta}{2} (V_{GS} - V_T)^2 \tag{6.6}$$

pri čemu su I_D struja drejna, β strujni faktor, a V_T napon praga. Parametri β i V_T su zavisni od implementirane tehnologije izrade i mogu se izraziti kao:

$$\beta = \mu C_{OX} \frac{W}{L} \tag{6.7}$$

$$V_T = V_{T0} + \gamma\left(\sqrt{|V_{SB}| + 2\varphi_F} - \sqrt{|2\varphi_F|}\right) \tag{6.8}$$

gdje je μ pokretljivost u kanalu, C_{OX} je kapacitivnost oksida gejta, V_{T0} je napon praga provođenja kada je V_{SB}=0V, φ_F je Fermijev potencijal, γ je tehnološka konstanta – faktor tijela. Pošto zavise od implementirane tehnologije, oba ova parametra β i V_T utiču na neuparenost.

Na osnovu jendačine (6.5), možemo okaraterisati varijansu parametra V_{T0} [111]:

$$\sigma^2(\Delta V_{T0}) = \frac{A_{V_{T0}}^2}{WL} + S_{V_{T0}}^2 D^2 \tag{6.9}$$

Pokazuje se da je standardna devijacija neuparenosti ovog parametra inverzno proporcionalna korijenu efektivne površine kanala tranzistora. Drugi dio jednačine se može zanemariti, jer je uticaj distance D na totalnu neuparenost značajan samo za uređaje sa velikom površinom kod kojih imamo velika rastojanja među komponentama.

Karakteristike neuparenosti strujnog faktora β mogu se izvesti ispitijući uzajamno nezavisne komponente W, L, μ, C_{OX} [108]:

$$\frac{\sigma^2(\beta)}{\beta^2} = \frac{\sigma^2(W)}{W^2} + \frac{\sigma^2(L)}{L^2} + \frac{\sigma^2(C_{OX})}{{C_{OX}}^2} + \frac{\sigma^2(\mu)}{\mu^2} \tag{6.10}$$

što se može prikazati i kao:

$$\frac{\sigma^2(\beta)}{\beta^2} = \frac{A_W^2}{W^2 L} + \frac{A_L^2}{WL^2} + \frac{A_{C_{OX}}^2}{WL} + \frac{A_\mu^2}{WL} + S_\beta^2 D^2 \tag{6.11}$$

Dakle, neuparenost kod MOS tranzistora se bazira na činjenici da se vrijednost parametara (W, L, β, V_T, itd.) u toku fabrikacije mijenja u odnosu na njihovu nominalnu

vrijednost. Ukoliko je npr. vrijednost napona praga provođenja u tranzistorima V_T =0.4V, može se desiti da na jednom čipu dva identična MOS uređaja imaju vrijednosti napona praga npr. 0.39V i 0.405V. Ova asimetrija uzrokuje neuparenost, jer se očekuje da dva identična MOS tranzistora imaju iste struje, što se ne dešava u ovim uslovima.

Procesne varijacije se dijele na *inter-die* i *intra-die* varijacije [112], [113]. *Inter-die* varijacije se javljaju između različitih čipova u istom ili različitim *wafer*-ima, dok se *intra-die* (*within-die*) varijacije javljaju između različitih kola i međukonekcija unutar istog čipa. Predmet posebne analize u ovom radu biće kako i u kojoj mjeri *intra-die* varijacije utiču na efektivnost CLA napada na CMOS kriptografsko jezgro. Drugim riječima treba naći odgovor na pitanje da li je prisustvo i uticaj procesnih *intra-die* varijacija tako veliki da ih treba uzeti u obzir u napadačevom modelu radi realizacije uspješnog CLA napada, ili je pak uticaj ovih varijacija tako minoran da se može zanemariti, tj. da on nema uticaja na modelovanje uspješnog CLA napada.

Realni model neuparenosti pod uticajem procesnih varijacija može biti itekako kompleksan. Broj parametara koji se mijenja i koji prouzrokuje neuparenost može biti ogroman. Na primjer, struje curenja, brzine zasićenja nosilaca, izlazne otpornosti, itd. mogu da budu neupareni svi u isto vrijeme. Parametri koji se mijenjaju usljed procesnih varijacija zavise prije svega od implementirane tehnologije. Radi poređenja realnog izlaza *side-channel*-a sa hipotetičkim izlazom modela *side-channel*-a, u hipotetičkom modelu su uzete u obzir promjene parametara pod uticajem procesnih varijacija. Svaki od parametara, podložnih promjeni usljed procesnih varijacija se nasumično mijenja, a pomoću *Monte Carlo* simulatora procjenjuje se srednja vrijednost i standardna devijacija tih parametara u skladu sa statističkom teorijom. Za naša istraživanja korišćen je *Monte Carlo* simulator u Cadence okruženju.

§ *VI.1.2 Monte Carlo metoda i simulacije*

Monte Carlo metoda je utemeljena na upotrebi slučajnih brojeva i statističke vjerovatnoće [114]. Može se koristiti u širokom spektru naučnih disciplina, od ekonomije do

nuklearne fizike. Naravno, način upotrebe ove metode široko varira od polja do polja upotrebe, ali da bi nešto nazvali *Monte Carlo* eksperimentom, dovoljno je koristiti slučajne brojeve za istraživanje nekog problema. Upotreba *Monte Carlo* metode za simuliranje fizičkih pojava nam omogućava rješavanje kompleksnih problema. Rješavanje jednačina koje opisuju odnose između dvije pojave je prilično jednostavno, ali rješavanje jednačina za stotine i hiljade slučajeva je jako komplikovano, i u tome nam pomaže *Monte Carlo* simulator koji uključuje brojna ponavljanja eksperimenta.

Sistemska upotreba metode, kao i njen naziv, datiraju iz 40-tih godina prošlog vijeka iz škole matematičara i fizičara u Los Alamosu, a posebno u radu *von Neumana*, *Ulma*, *Metropolisa*, *Fremija* i *Kahna*. Zasluge za osmišljavanje *Monte Carlo* metode pripisuju se poljskom matematičaru *Stanislavu Ulmu* koji je tokom Drugog svjetskog rata, igrajući popularnu igru karata "solitare", pokušao da odgonetne kolike su šanse da se 52 karte podijele tako da je u igri moguće pobijediti [115]. Nakon mnogo vremena utrošenog na ispitivanje kombinatorike rješenja, počeo se pitati da li postoji jednostavnije rješenje datog problema. Uočio je da je mnogo jednostavnije podijeliti karte stotinu puta, pa prebrojati koliko je bilo uspješnih ishoda. Taj postupak bi čovjeku oduzeo puno vremena, ali pomoću kompjutera do rezultata bi se došlo relativno brzo. To je *Ulmu* dalo ideju kako prilagoditi procese opisane diferencijalnim jednačinama u ekvivalentnim oblicima koji se zasnivaju na operacijama nad slučajnom promjenljivom. Radeći sa *Neumanom* i *Metropolisom* smislio je algoritam za programsku implementaciju. Njime je predložio način da se problemi koji nemaju definiciju pretvore u problem pogodan za statističko uzorkovanje, a *Metropolis* je imenovao novu metodologiju prema lancu kazina *Monte Carlo*. Veliki doprinos *Ulama* je taj što je prepoznao potencijal elektronskih kompjutera za automatizaciju stvaranja statističkog uzorkovanja.

Razlikujemo sljedeće tipove primjene *Monte Carlo* simulacije:

- Deterministički problemi koje je teško ili skupo rješavati – tipičan primjer je računanje vrijednosti određenih integrala koji se ne mogu riješiti analitički, tj. čija je podintegralna funkcija takva da se ne može naći rješenje u obliku analitičkog izraza. *Monte Carlo* simulacija pristupa proračunu integrala tako što se generiše niz slučajnih tačaka (x_j, y_j) sa jednakim vjerovatnoćama unutar određenog pravougaonog intervala i potom ispituje koliko je generisanih tačaka unutar površine koja odgovara integralu.

Ovakav pristup koji se zasniva na generisanju slučajnih brojeva analogan je onom koji se koristi kod simulacije sistema sa diskretnim događajima.

- Složeni fenomeni koji nijesu dovoljno poznati – ovo je druga klasa problema koji se rješavaju *Monte Carlo* simulacijom. Za njih je karakteristično da nije poznat način uzajamnog djelovanja između elemenata, već su poznate samo vjerovatnoće njegovog ishoda koje se koriste za izvođenje niza eksperimenata koji daju uzorke mogućih stanja zavisnih promjenljivih. Statističkom analizom takvih uzoraka dobija se raspodjela vjerovatnoća zavisnih promjenljivih koje su od interesa.

- Statistički problemi koji nemaju analitička rješenja – (npr. procjene kritičnih vrijednosti ili testiranje novih hipoteza) su jedna specifična klasa problema koji se rješavaju *Monte Carlo* simulacijom. Prilikom rješavanja takvih problema takođe se koristi generisanje slučajnih brojeva i promjenljivih.

Preliminarna analiza uticaja *intra-die* procesnih varijacija izvršena je na osnovnim CMOS kolima i CMOS S-kutiji. Nakon toga, vršena je analiza uticaja *intra-die* procesnih varijacija na efektivnost CLA napada na modelu kriptografskog jezgra. Osnovna CMOS kola simulirana su koristeći 65nm-sku CMOS biblioteku od firme STMicroelectronics u Cadence okruženju. *Bsim4* modeli h-tipa tranzistora imaju statističke parametre definisane uputstvima proizvođača, koji obezbjeđuju najveću tačnost simulacionih rezultata koji se tiču i struja curenja i *intra-die* procesnih varijacija. Detalji o statističkim parametrima ne mogu biti objelodanjeni zbog NDA (*Non Disclosure Agreement*) sporazumnog dokumenta između proizvođača i La Sapienza Univerziteta, gdje je vršena ova analiza.

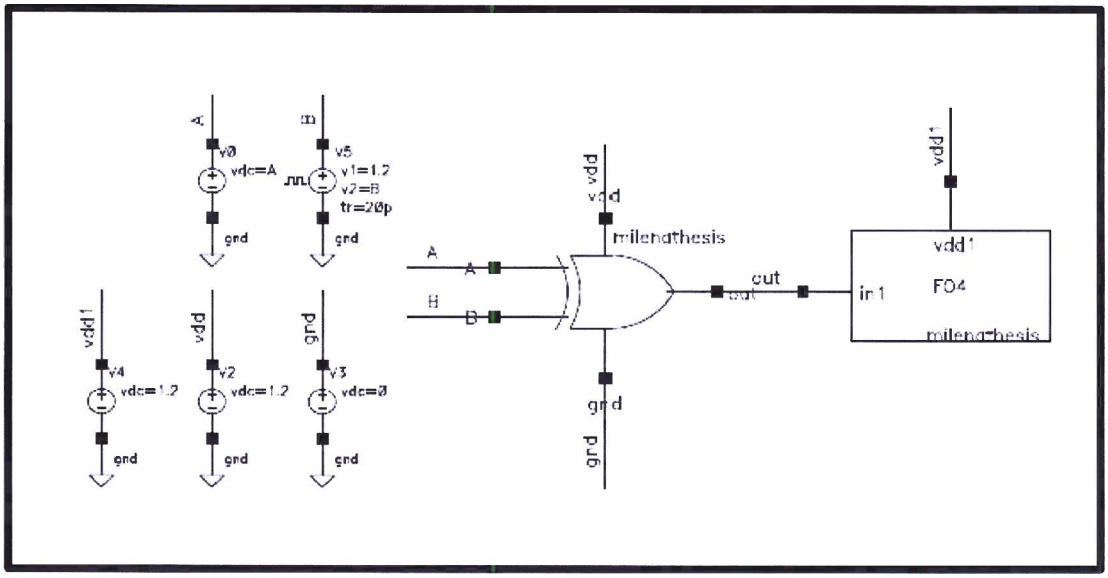
Monte Carlo simulacije omogućavaju procjenu uticaja promjene parametara komponenti na performanse kola. Statistička teorija precizira koliko srednja vrijednost i standardna devijacija nekog realnog sistema mogu biti procijenjene kroz *Monte Carlo* simulacije. Na primjer, ukoliko imamo srednju vrijednost neke veličine od 1000 i standardnu devijaciju od 30 sa 100 *Monte Carlo* iteracija, teorija kaže da je 1000 najbolje procijenjena srednja vrijednost te veličine sa greškom $\frac{30}{\sqrt{100}}$, tj. 1000 ± 3. Sa većim brojem iteracija se postiže bolja procjena, ali je potrebno i mnogo više vremena za njihovo izvršenje. Za osnovna

CMOS kola, pošto su jednostavne strukture i *Monte Carlo* iteracije se relativno brzo izvode, počelo se takođe sa 100 *Monte Carlo* iteracija. Sljedeći korak je bio provjera da li je standardna devijacija nakon 200 *Monte Carlo* iteracija ista, za recimo CMOS NAND kolo sa ulazima 00, kao i nakon 100 *Monte Carlo* iteracija. Tek kada dođe do poklapanja te vrijednosti za različiti broj iteracija, znači da je *Monte Carlo* simulator uzeo dovoljno veliki broj iteracija koje će dati dobru procjenu u rezultatima. Za osnovna CMOS kola, na kojima su vršene analize, došlo se do zaključka da je dovoljan broj *Monte Carlo* iteracija 400. Dakle, u svakom eksperimentu pojedinačno, tj. za svaku kombinaciju ulaza svakog od analiziranih osnovnih CMOS kola, generiše se 400 uzoraka (probnih CMOS kola) koje tretira *Monte Carlo* simulator.

U postavkama *Monte Carlo* okruženja unutar okvira za definisanje simulacije (*Simulator Window*), pored izbora iteracija (*Number of Runs*), potrebno je podesiti i sljedeće parametre: početna iteracija (*Starting Run*=1), tip varijacije (*Analysis Variation=Mismatch*), da li je neophodno čuvati grafike i rezultate svih iteracija (*Save Data Between Runs to Allow Family Plots=yes*), definisati koje izlaze je potrebno prikazati (*Ouputs=AutoPlot wave leakage current*), radna temperatura na kojoj će se vršiti simulacije (*Temperature=25°C*). Prije početka simulacije, potrebno je zadati i vrijednosti tolerancije tokom *Monte Carlo* simulacija koje moraju biti veće od uobičajenih, jer je izlaz struja curenja koja inače ima male vrijednosti, pa je potrebna manja tolerancija:

- reltol (*relative tolerance*) – ukoliko ova vrijednost nije dovoljno velika, simulacija je nemoguća. Ovaj parametar karakteriše razliku svake dvije susjedne iteracije kod strujnih ili naponskih grafika. Zadata je tolerancija od 1e-6 (podrazumijevana vrijednost, tzv. *default* =1e-4), što znači da ako je npr. vrijednost napona kod prvog grafika 1V, vrijednost kod sljedećeg ne smije preći 1V+1μV.
- vabstol (*voltage absolute tolerance convergence options*) – karakteriše apsolutnu grešku u naponskim simulacijama. Zadata vrijednost je 1e-8 (*default*=1e-6).
- iabstol (*current absolute tolerance convergence options*) – karakteriše apsolutnu grešku u simulacijama struje. Zadata vrijednost je 1e-14 (*default* 1e-12).

Kako je kriptografsko jezgro građeno od velikog broja osnovnih CMOS kola, da bi se stvorilo što realnije ekperimentalno okruženje, na kraj analiziranog CMOS kola nije vezan kondenzator, već testno kolo FO4 (*Fanout-of-4*). Ovo kolo se sastoji od četiri ista paralelno vezana CMOS invertora, također implementirana u 65nm-skoj tehnologiji (šematski prikazi su u folderu Dodaci na priloženom CD-u). Sada mjerena struja curenja ne potiče samo od osnovnog CMOS kola, već i od FO4 kola, što bi se desilo i u realnom kriptografskom okruženju (Slika 6.3).



Slika 6.3 – Eksperimentalno okruženje za izvođenje *MC* simulacija nad CMOS XOR kolom

Nakon izvršenih *Monte Carlo* (*MC*) simulacija dobija se grafik sa strujama curenja od 400 uzoraka za određeni ulaz za koji zadajemo opciju čuvanja tih rezultata u vidu *comma-separated values* fajla koji ima ekstenziju .csv i koji se može otvoriti u Excel-u (svi rezultati MC simulacija nalaze se u folderu Dodaci na priloženom CD-u). Ove podatke potrebno je obraditi u Matlabu, tj. na osnovu prikupljenih 400 struja curenja za svaku kombinaciju ulaza svakog analiziranog CMOS kola potrebno je naći srednju vrijednost struje curenja, standardnu devijaciju, maksimalnu i minimalnu struju curenja među 400 uzoraka (Dodatak A).

U Tabeli VI.1 dati su rezultati za vrijednosti struja curenja pri običnim simulacijama, *MC* simulacijama (srednja vrijednost struja curenja nakon *MC* simulacija), standardne devijacije, kao i maksimalne i minimalne vrijednosti tih struja. Na osnovu analize dobijenih rezultata može se doći do sljedećih zaključaka:

- za NOT kolo, struja curenja za ulaz ′0′ (izlaz ′1′) se jasno razlikuje od struje curenja za ulaz ′1′ (izlaz ′0′) i pored uzimanja u obzir efekata neuparenosti,

- za NAND kolo, struje curenja za ulazne kombinacije ′00′, ′01′ i ′10′ (izlaz ′1′) se jasno razlikuju od struje curenja za ulaz ′11′ (izlaz ′0′) i pored uzimanja u obzir efekata neuparenosti,

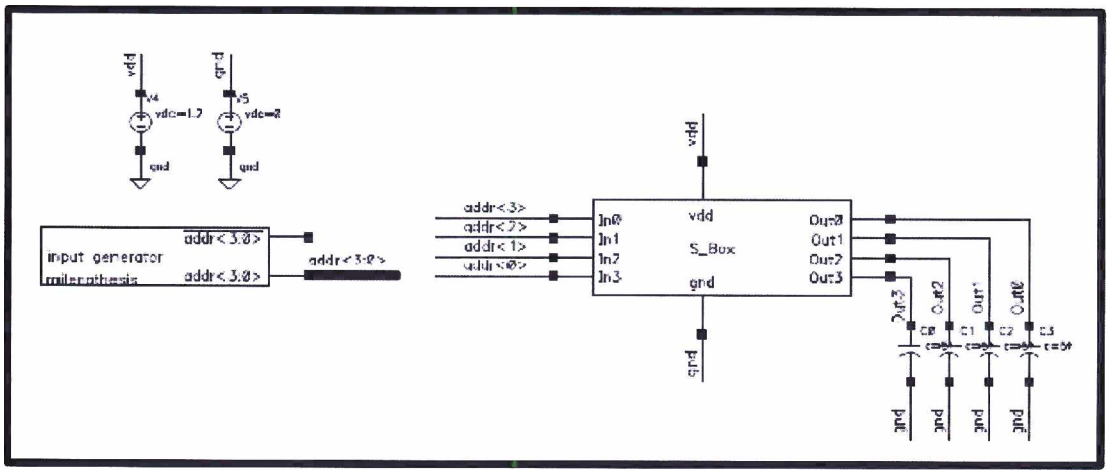
- za XOR kolo, struje curenja za ulazne kombinacije ulaza ′10′ i ′01′ (izlaz ′1′) se jasno razlikuju od struja curenja za ulazne kombinacije ′00′ i ′11′ (izlaz ′0′) i pored uzimanja u obzir efekata neuparenosti.

Tabela VI.1 – Rezultati simulacija za osnovna CMOS kola

NOT Gate CMOS 065 @ 25°, [*A*]						
A		*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0		7.877n	8.412n	1.51n	19.95n	6.065n
1		0.813n	0.923n	0.50n	3.251n	0.176n
NAND Gate CMOS 065 @ 25°, [*A*]						
A	**B**	*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0	**0**	7.623n	7.919n	0.729n	11.14n	5.935n
0	**1**	7.842n	8.724n	1.666n	21.63n	5.77n
1	**0**	7.444n	7.953n	1.032n	12.39n	5.66n
1	**1**	1.641n	1.856n	0.725n	5.32n	0.624n
XOR Gate CMOS 065 @ 25°, [*A*]						
A	**B**	*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0	**0**	7.623n	7.919n	0.729n	11.14n	5.935n
0	**1**	15.89n	17.155n	2.895n	28.67n	11.57n
1	**0**	13.51n	15.32n	2.841n	27.06n	10.72n
1	**1**	8.179n	9.088n	3.409n	17.81n	3.176n

Naime, srednja vrijednost struje curenja (vrijednost *MC* simulacije u Tabeli VI.1) i standardna devijacija su parametri koji nam daju mogućnost procjene efikasnosti određene zaštitne mjere u hardveru.

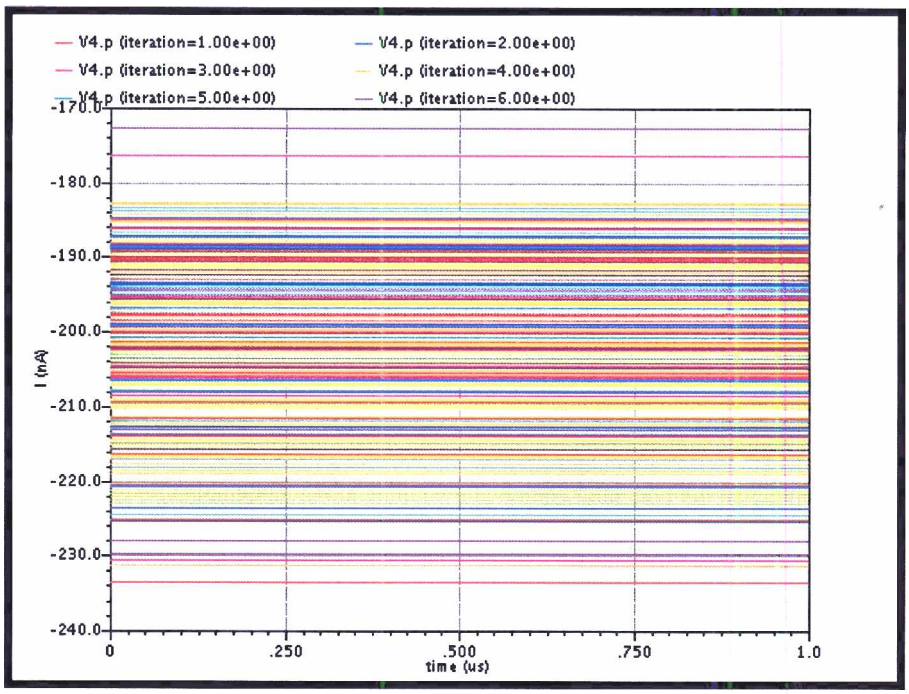
Za realizaciju CMOS S-kutije upotrijebljena je jedna od osam 4x4 Serpent-ovih S-kutija (Dodatak A) [116]. Kako bi se što lakše simulirale struje curenja za različite ulazne kombinacije S-kutije, generisano je kolo *input_generator* (Slika 6.4), koje se može koristiti kasnije i za TDPL S-kutiju, jer ima dva invertovana ulaza (šematski prikazi ovog kola nalaze se u folderu Dodaci na priloženom CD-u). Ovo kolo ima dva parametra (*i, j*) koja definišu ulaz u S-kutiju i zadaju se u zavisnosti od toga da li mjerimo struju curenja ili dinamičku struju i na koji način želimo da izvršimo mjerenje (npr. uvođenjem kašnjenja). Ukoliko bismo mjerili dinamičku struju na prelazu ulaznog podatka npr. sa 0001 na 1001, parametar *i* bi iznosio 1, a parametar *j* 9. Kako se u našem slučaju mjeri struja curenja, *i* i *j* parametar uvijek imaju istu vrijednost (npr. ako su *i* i *j* brojevi 1, to je zapravo konstantan ulaz u S-kutiju 0001).



Slika 6.4 – Eksperimentalno okruženje za izvođenje *MC* simulacija nad CMOS S-kutijom

Da bi se simulirale struje curenja CMOS S-kutije i prikazao uticaj neuparenosti na njih, korišćen je moćan alat Cadence-a - programski jezik OCEAN *(Open Command Environment for Analysis)* koji dozvoljava dizajneru veću kontrolu nad simulacijama i analizu tih simulacija, kao i smještanje više simulacija u okviru jednog programa (Slika 6.5) [117]. Naime, pomoću tzv. OCEAN skripte potrebno je definisati određene parametre prije samih

simulacija: temperaturu (T=25°C), vrijednosti ulaznih podataka u S-kutiju (svaki od parametara i i j ima vrijednost od 0 do 15), vrijednosti parametara tolerancije (*reltol*, *vabstol*, *iabstol*), itd (Dodatak A). Rezultati standardnih simulacija struja curenja zajedno se smještaju u izlazni fajl *sbox_results.txt*. Kompleksniji dio OCEAN koda je konkretno programiranje *Monte Carlo* simulacija i smještanje podataka o srednjim vrijednostima struja curenja i standardnim devijacijama nakon 400 *Monte Carlo* iteracija u izlazni fajl *sbox_mc_results.txt*. Simuliranje i smještanje podataka u okviru stvorenog OCEAN programskog koda je vremenski zahtjevno (rezultati su dati u Tabeli VI.2).



Slika 6.5 – Grafik dobijen nakon 400 MC iteracija struja curenja

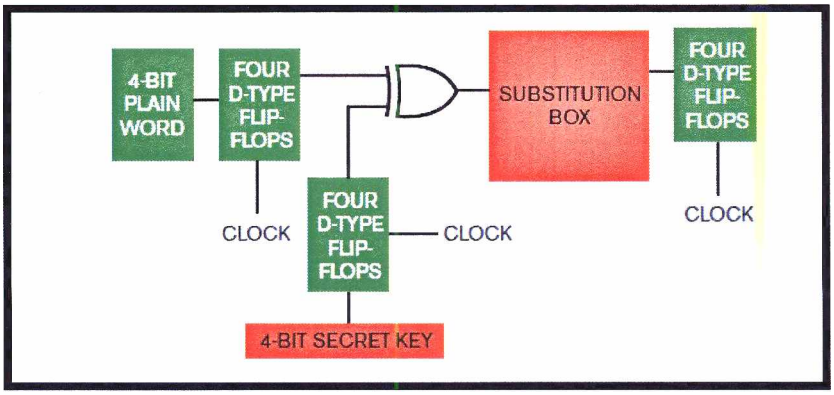
Analizirajući rezultate dobijene programiranjem OCEAN skripte radi procjene uticaja neuparenosti na CMOS S-kutiju, dolazi se do zaključka da se ulazni podaci S-kutije na osnovu izmjerenih struja curenja ne mogu međusobno razlikovati pod uticajem procesnih varijacija, ali će se pokazati dalje u radu da je i pored ovakvih rezultata dobijenih za CMOS S-kutiju, napad na kriptografsko jezgro uspješan.

Tabela VI.2 – Rezultati *Monte Carlo* simulacija za CMOS S-kutiju

Ulazni podatak	Izlazni podatak	Obična simulacija 065 @25°, [A]	MC simulacija 065 @25°, [A]	standardna devijacija 065 @25°, [A]
0000	**0011**	182.4002n	207.4273n	10.520n
0001	**1000**	175.8396n	201.0933n	9.683n
0010	**1111**	159.8369n	183.8888n	9.556n
0011	**0001**	159.2726n	184.3944n	9.582n
0100	**1010**	167.2636n	191.6261n	10.082n
0101	**0110**	160.2410n	183.7441n	9.224n
0110	**0101**	151.1494n	175.9541n	9.901n
0111	**1011**	147.1836n	171.3345n	9.597n
1000	**1110**	174.2304n	198.4120n	9.874n
1001	**1101**	162.0959n	184.9996n	9.424n
1010	**0100**	161.6234n	187.0615n	9.338n
1011	**0010**	152.1645n	177.2633n	9.402n
1100	**0111**	157.0160n	179.5096n	9.373n
1101	**0000**	152.4295n	174.4303n	8.606n
1110	**1001**	146.6428n	170.5242n	9.292n
1111	**1100**	140.0150n	161.5464n	8.327n

§ *VI.2 CLA napad na 65nm-sko CMOS kriptografsko jezgro*

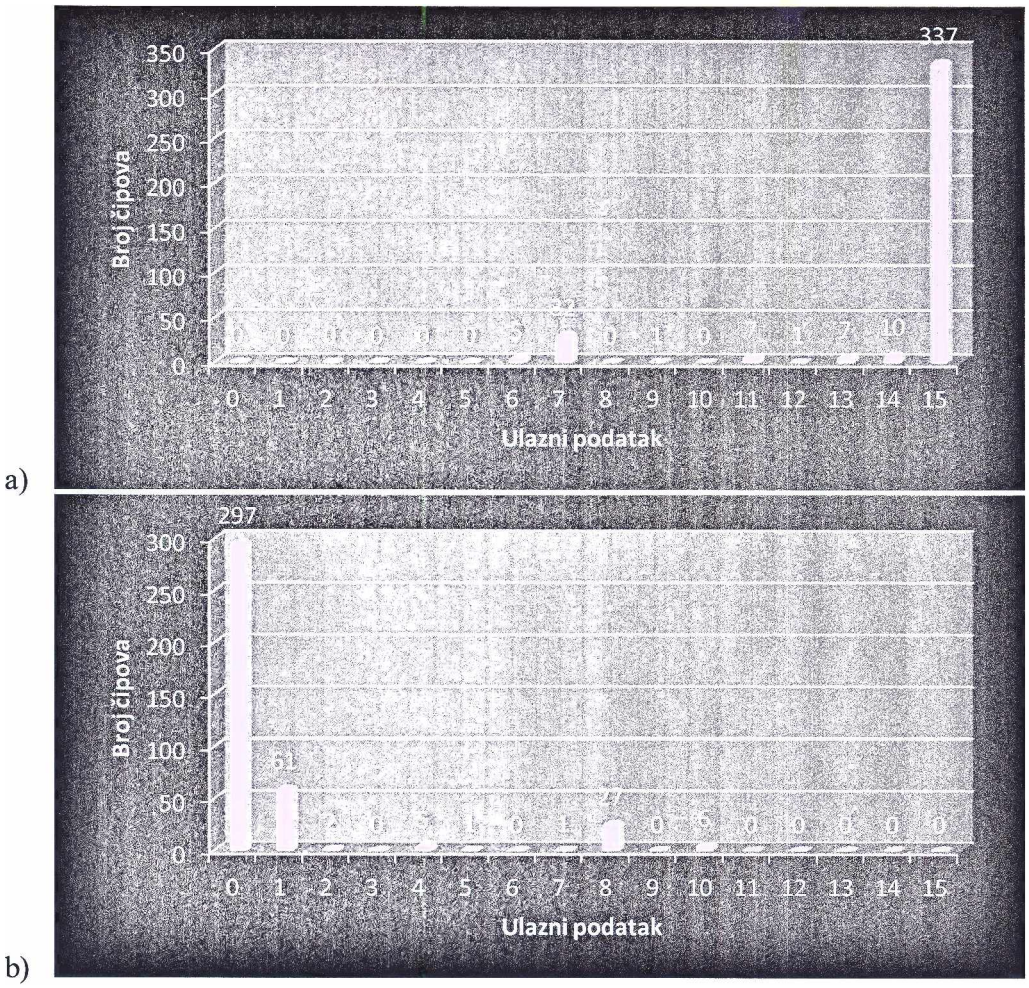
Prema prethodno objašnjenoj proceduri CLA napada koja se sastoji iz pet koraka, izvršen je napad na projektovano kriptografsko jezgro u 65nm-skoj tehnologiji (Slika 6.6), (Dodatak A). Projektovano kriptografsko jezgro sastoji se iz kombinatornog i sekvencijalnog dijela. Kombinatorna logika kriptografskog jezgra realizovana je povezivanjem četiri XOR kola sa četiri ulaza Serpent S-kutije: bitovi ulaznog podatka i ključa se "miksuju" u dvo-ulaznim XOR kolima čiji se izlazi mapiraju u S-kutiji. Rezultat XOR operacije između najnižeg bita ključa i najnižeg bita ulaznog podatka se dovodi na nulti ulaz S-kutije. Slično se postupa i sa preostalim bitovima ključa i ulaznog podatka. Sekvencijalni dio kriptografskog jezgra sastoji se iz D flip-flopova (u folderu Dodaci na priloženom CD-u) i oni obezbjeđuju vremensku sinhronizovanost operacije XOR nad ključem i ulaznim podatkom.



Slika 6.6 – Eksperimentalno okruženje za izvođenje CLA napada nad kriptografskim jezgrom [34]

Prvi korak u realizaciji CLA napada je postavljanje vrijednosti ključa (npr. postavljen je ključ 0101), nakon čega se prikupljaju podaci o vrijednostima struja curenja izvodeći 400 *Monte Carlo* iteracija za svaku kombinaciju ulaznog podatka (od 0 do 15, decimalno). Bitno je naglasiti da svaka od 400 *Monte Carlo* iteracija predstavlja realizaciju modela kriptografskog jezgra nad kojim se vrši analiza, sa posebnom konfiguracijom nasumičnih procesnih varijacija. Rezultati *Monte Carlo* simulacija zajedno čine matricu 16x400 struja curenja u kojoj element (i, j) predstavlja vrijednost struje curenja za ulaz i ($0 \leq i \leq 15$) u čipu j ($1 \leq j \leq 400$), (svi fajlovi sa rezultatima simulacija nalaze se u folderu Dodaci na priloženom CD-u).

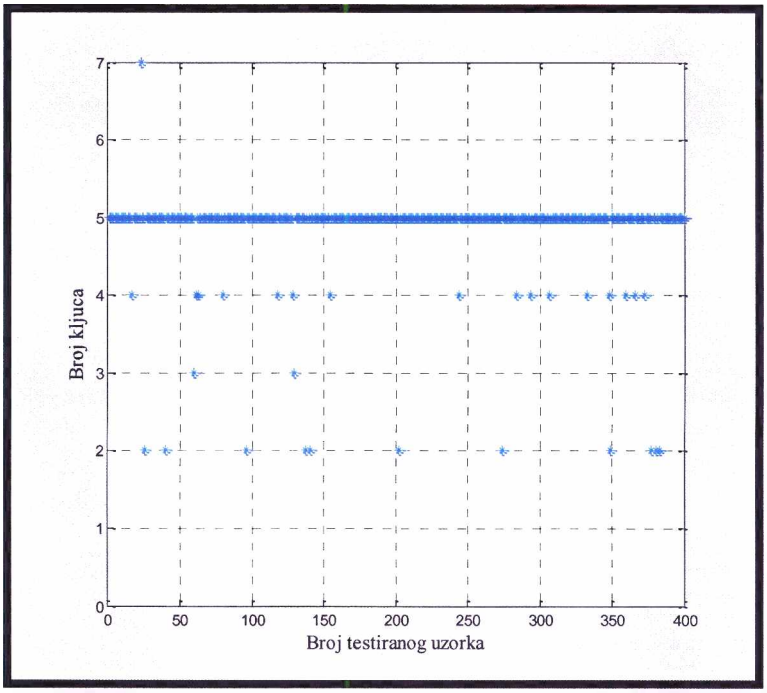
Jedna od analiza dobijenih podataka uključuje raspoređivanje struja curenja u svih 400 fajlova od najmanje ka najvećoj vrijednosti, tako da su u funkciji ulaznog podatka. Takvom analizom se došlo do interesantnih rezultata: 337 od 400 testiranih uzoraka generišu najmanju vrijednost struje curenja za ulazni podatak 1111 (*Hamming*-ova težina w=4), dok 297 od njih 400 generiše najveću vrijednost struje curenja za ulazni podatak 0000 (*Hamming*-ova težina w=0), (Dodatak A), (Slika 6.7).



Slika 6.7 – Uticaj ulaznog podatka na generisanje: a) najmanje struje, b) najveće struje u 400 testiranih čipova

U daljim analizama za svaku hipotezu ključa izračunat je koeficijent korelacije ρ između vektora struja curenja i vektora odgovarajućih *Hamming*-ovih težina (koje su rezultat XOR operacije između ulaznog podatka i hipoteze ključa). Na taj način generisana je 16x400 matrica u kojoj je element (i, j) koeficijent korelacije za hipotezu ključa i na napadnuti čip j. Pri tome, dovoljno je posmatrati samo pola dobijene matrice (prvih 8 redova), zbog simetrije usljed XOR operacije (Dodatak A). Na Slici 6.8 prikazani su rezultati CLA napada dobijeni prema najvećoj vrijednosti koeficijenta korelacije za svaki od 400 testnih uzoraka pod uticajem procesnih varijacija [118]. Za 370 od 400 testnih uzoraka najveća vrijednost

koeficijenta korelacije odgovara implementiranom ključu broj 5 (*Key*=1001). Detaljni rezultati koji podrazumijevaju i distribuciju "netačnih" ključeva za 30 testnih uzoraka za koje napad nije uspio prikazani su u Tabeli VI.3 .



Slika 6.8 – Rezultati CLA napada prema najvećoj vrijednosti koeficijenta korelacije na 400 testnih CMOS uzoraka

Idealni CLA napad podrazumijeva da je izračunati koeficijent korelacije za integrisani ključ u svim napadnutim uzorcima najveći i da se ne preklapa sa koeficijentima korelacije za druge hipoteze ključa. Međutim, postoje slučajevi kada CLA napad nije 100% uspješan, ali to ne čini CLA napad neuspješnim, već ga čini neuspješnim samo u određen broj slučajeva. Ovaj CLA napad je uspješan u 92,5% slučajeva, tj. za 370 testnih uzoraka od 400 napadnutih. Takođe, bitno je istaći da kod 30 čipova kod kojih nije uspio CLA napad, drugi po redu najveći koeficijent korelacije je u funkciji pravog ključa (*Key*=0101) za 24 testna uzorka (Tabela VI.3). Dakle, ukoliko napadač uzme u obzir ključeve za dva najveća koeficijenta

korelacije, CLA napad je uspješan u 394 testnih uzoraka od 400 napadnutih, tj. u 98,5% slučajeva.

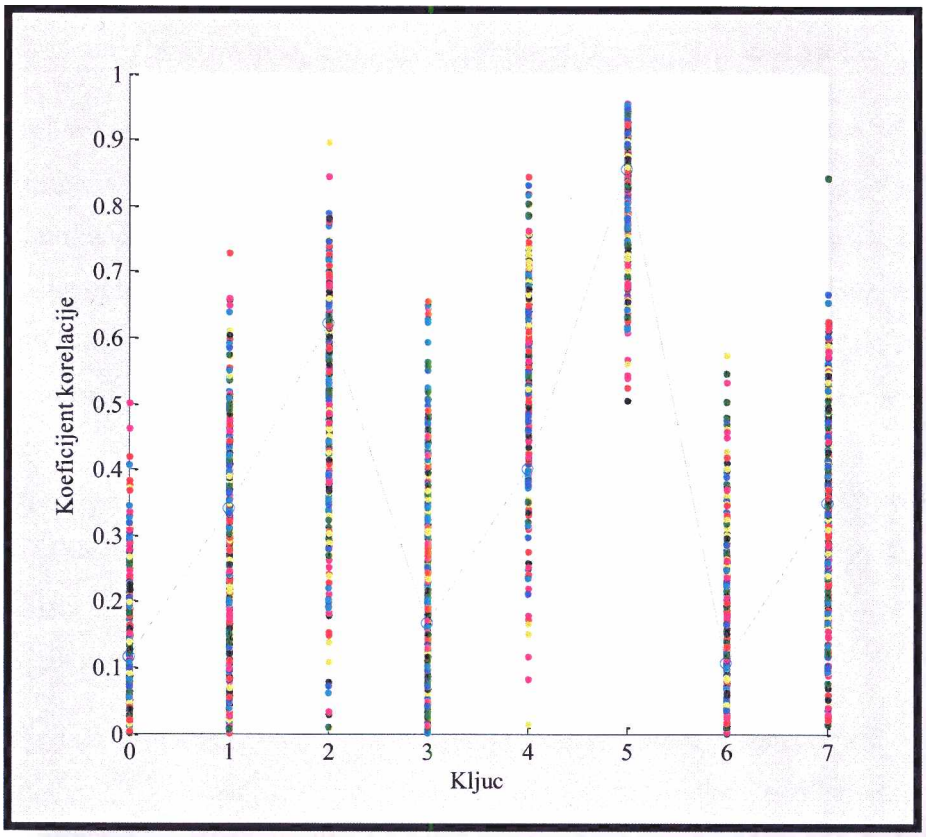
Tabela VI.3 – Broj napadnutih testnih uzoraka u odnosu na dva najveća koeficijenta korelacije

Broj ključa	Ključ	Broj napadnutih testnih uzoraka od 400 (prvi max koef. korelacije)	Broj napadnutih testnih uzoraka od 30 (drugi max koef. korelacije)
0	0000	0	0
1	0001	0	0
2	0010	11	0
3	0011	2	3
4	0100	16	2
5	0101	370	24
6	0110	0	1
7	0111	1	0

Već je napomenuto da je za uspješan napad bitno da se koeficijent korelacije za pravi ključ ne poklapa sa koeficijentima korelacije za druge hipoteze ključa, kao što je uočljivo na Slici 6.9, gdje su prikazane vrijednosti koeficijenata korelacije za 400 testnih uzoraka u funkciji odgovarajuće hipoteze ključa. Takođe, na slici su prikazane i povezane vrijednosti koeficijenata korelacije za testni uzorak broj 135, za koga se CLA napad pokazao uspješnim, tj. najveća dobijena vrijednost koeficijenta korelacije (ρ=0.8542) vezana je za hipotezu pravog ključa 5 (*Key*=0101).

Pokazalo se da prisustvo procesnih varijacija nije imalo uticaja na uspješnost CLA napada. Drugim riječima, uticaj ovih varijacija je tako minoran da se može zanemariti u napadačevom modelu, tj. nije ga potrebno uzimati u obzir pri modelovanju uspješnog CLA napada. Takođe, pokazalo se da implementirana CMOS tehnologija nije dovoljno dobra mjera zaštite protiv napada baziranih na analizama struja curenja koji se izvode u realnim eksperimentalnim uslovima. Odnosno, napadi bazirani na analizi struja curenja (CLA napadi)

su se pokazali izuzetno uspješnim na velikom broju testnih uzoraka kriptografskog uređaja izvedenog u 65nm-skoj CMOS tehnologiji. Iz tog razloga, potrebno je naći adekvatnu mjeru zaštite u odnosu na CLA napade, što će biti predmet daljeg istraživanja u okviru ove disertacije.



Slika 6.9 – Uspješno napadnut čip broj 135, *Key*=0101

§ *VI.3 Zaključci*

U ovom poglavlju je definisana korelacija među parametrima koji su od značaja za napad baziran na analizi struja curenja - CLA (*Correlation Leakage Analysis*). Ta vrsta napada eksploatiše simulirane i izmjerene vrijednosti struje curenja kriptografskog uređaja sa ciljem nalaženja tajnog ključa. Detaljno su objašnjeni potrebni koraci CLA napada. Izvršena

je klasifikacija grešaka kod uparivanja komponenti. Objašnjeni su uzroci i karakteristike sistematičnih i nasumičnih grešaka. Radi boljeg razumijevanja suštine funkcionisanja, kao i preciznije simulacije CLA napada u eksperimentalnim uslovima, analiziran je uticaj procesnih varijacija na rezultate napada. S obzirom na to da je Monte Carlo simulator u Cadence okruženju upotrijebljen za analizu promjene parametara pod uticajem procesnih varijacija, opisana je Monte Carlo metoda, kao i tipovi primjene Monte Carlo simulacije.

Preliminarna analiza uticaja *intra-die* procesnih varijacija izvršena je na osnovnim CMOS kolima i CMOS S-kutiji, koristeći *Bsim4* tranzistore h-tipa, koji obezbjeđuju najveću tačnost simulacionih rezultata koji se tiču i struja curenja i procesnih varijacija. Na osnovu analize struja curenja nakon MC simulacija, i pored uzimanja u obzir efekata neuparenosti, u osnovnim CMOS kolima došlo se do sljedećih zaključaka: za NOT kolo struja curenja za ulaz ′0′ se jasno razlikuje od struje curenja za ulaz ′1′, za NAND kolo struje curenja za ulazne kombinacije ′00′, ′01′ i ′10′ se jasno razlikuju od struje curenja za ulaz ′11′, za XOR kolo struje curenja za ulazne kombinacije ulaza ′10′ i ′01′ se jasno razlikuju od struja curenja za ulazne kombinacije ′00′ i ′11′. Rezultati istih analiza u CMOS S-kutiji pokazali su da se ulazni podaci S-kutije na osnovu izmjerenih struja curenja ne mogu međusobno razlikovati pod uticajem procesnih varijacija.

Sljedeća grupa istraživanja obuhvatila je analizu uticaja *intra-die* procesnih varijacija na efektivnost CLA napada na projektovano kriptografsko jezgro u 65nm-skoj tehnologiji. Svaka od 400 izvršenih *Monte Carlo* iteracija predstavlja realizaciju modela kriptografskog jezgra nad kojim se vrši analiza, sa posebnom konfiguracijom nasumičnih procesnih varijacija. Jedna od analiza dobijenih podataka prikazuje zavisnost struja curenja od ulaznog podatka: 337 od 400 testiranih uzoraka generišu najmanju vrijednost struje curenja za ulazni podatak 1111 (*Hamming*-ova težina w=4), dok 297 od njih 400 generiše najveću vrijednost struje curenja za ulazni podatak 0000 (*Hamming*-ova težina w=0). CLA napad na CMOS kriptografsko jezgro pokazao se uspješnim u 92,5% slučajeva (370/400). Značajan rezultat napada je i da kod 30 čipova kod kojih nije uspio CLA napad, drugi po redu najveći koeficijent korelacije je u funkciji pravog ključa za 24 testna uzorka. Dakle, CLA napadi su se pokazali izuzetno uspješnim na velikom broju testnih uzoraka CMOS kriptografskog uređaja, čime se pokazalo da CMOS tehnologija ne predstavlja dovoljno dobru mjeru zaštite protiv CLA napada.

VII Procjena uspješnosti CLA napada na TDPL kirptografsko jezgro pod uticajem procesnih varijacija i poređenje sa CMOS logikom

U ovom poglavlju je analizirano da li je i u kojoj mjeri implementacija TDPL logike umjesto CMOS logike u hardveru pametnih kartica bolja mjera zaštite u odnosu na napade bazirane na analizi struja curenja. Iz tog razloga, sprovedena su dva tipa istraživanja. Prvi tip se odnosi na poređenja standardnih *Bsim4* TDPL i CMOS l-tip-a tranzistora simulirajući struje curenja u programu Cadence u STMicroelectronics 65nm-skoj tehnologiji. Poređenje CMOS i TDPL logike, kao i njihova efikasnost u ulozi hardverskih mjera zaštite od CLA napada, izvršiće se kroz faktore NCD (*Normalized Current Deviation*) i NSD (*Normalized Standard Deviation*). U ovom dijelu istraživanja prikazaće se i komparacija CMOS/TDPL S-kutije l-tipa u odnosu na struje curenja i njihova zavisnost od *Hamming*-ove težine ulaznih, odnosno izlaznih podataka iz S-kutije, uzimajući u obzir i temperaturnu zavisnost. Drugi tip istraživanja podrazumijeva izvršenje CLA napada na 65nm-sko TDPL kriptografsko jezgro pod uticajem procesnih varijacija. Dobijeni rezultati napada uporediće se sa odgovarajućim rezultatima CLA napada na 65nm-sko CMOS kriptografsko jezgro. Na osnovu tih rezultata procijeniće se stepen efikasnosti TDPL logike i eventualna potreba za njenom implementacijom u hardveru pametnih kartica radi zaštite od napada baziranih na analizama struja curenja.

§ *VII.1 Komparacija CMOS/TDPL logike koristeći l-tip tranzistore u 65nm-skoj tehnologiji*

Analiza se odnosi na logička kola bazirana na l-tipu tranzistora, za razliku od analize izvedene sa h-tipom tranzistora u Poglavlju V. Rezultati simulacija za CMOS NOT, NAND i

XOR kola prikazani su u Tabeli VII.1, (šematski prikazi nalaze se u folderu Dodaci na priloženom CD-u). Naime, parametri korišćeni za l-tip CMOS NOT i NAND kolo u 65nm-skoj tehnologiji su: V_{DD} = 1.2V, L = 600nm, W_{NMOS} = 120nm, W_{PMOS} = 2.5 x 120nm = 300nm, C_L = 5fF. Za XOR kolo čija je struktura preuzeta iz STMicroelectronics biblioteke, parametri su: V_{DD} = 1.2V, L = 600nm, W_{NMOS1} = 120nm, W_{NMOS2} = 240nm, W_{NMOS3} = 360nm, W_{PMOS1} = 360nm, W_{PMOS2} = 720nm, C_L = 5fF. Takođe, uzeto je u obzir pet različitih temperatura (0°, 25°, 50°, 75°, 100°) da bi se ustanovila zavisnost struje curenja od temperature. Na osnovu dobijenih rezultata zaključuje se da postoji značajna zavisnost struja curenja od vrijednosti ulaznih podataka i vrijednosti temperature, slično kao u Poglavlju V.

Tabela VII.1 – Struja curenja kroz CMOS osnovna kola

NOT Gate CMOS065 [A]					
A	T=0°	T=25°	T=50°	T=75°	T=100°
0	23.148n	37.561n	58.893n	88.319n	126.7n
1	40.99n	92.921n	183.933n	327.11n	533.9n

NAND Gate CMOS065 [A]						
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	14.333n	16.471n	19.834n	24.992n	32.585n
0	1	23.132n	37.508n	58.752n	87.992n	126.034n
1	0	19.169n	30.869n	48.485n	73.167n	105.825n
1	1	81.963n	185.732n	367.426n	652.807n	1.064u

XOR Gate CMOS065 [A]						
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	110.27n	210.491n	381.362n	647.347n	1.031u
0	1	164.661n	294.857n	501.278n	802.646n	1.213u
1	0	134.977n	245.566n	422.669n	684.022n	1.045u
1	1	140.628n	309.366n	608.781n	1.082u	1.768u

TDPL logika je do sada proučavana samo u sferi napada baziranih na analizi dinamičke disipacije snage i dinamičkih struja - DPA (*Differential Power Analysis*) napada [91]. Većina DPA logičkih stilova, koji se primjenjuju kao mjere zaštite od DPA napada, koristi ćelije iz postojećih standardnih bilblioteka, npr. WDDL kriptografsko jezgro se može realizovati koristeći standardnu CMOS biblioteku [87]. To nije slučaj sa TDPL logikom, gdje

je potreban razvoj biblioteke TDPL ćelija (u folderu Dodaci na priloženom CD-u). U Tabeli VII.2 prikazane su struje curenja za TDPL NOT, NAND i XOR kola, simulirane u programu Cadence u STMicroelectronics 65nm-skoj tehnologiji (šematski prikazi nalaze se u folderu Dodaci na priloženom CD-u). I ovdje su rađene simulacije za pet različitih temperatura (0°, 25°, 50°, 75°, 100°).

Tabela VII.2 – Struja curenja kroz TDPL osnovna kola

NOT Gate TDPL065 [A]					
A	T=0°	T=25°	T=50°	T=75°	T=100°
0	117.338n	235.887n	437.36n	745.162n	1.176u
1	117.338n	235.887n	437.36n	745.162n	1.176u
NAND Gate TDPL065 [A]					
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	116.847n	234.771n	435.177n	741.389n	1.17u
0	1	117.336n	235.884n	437.354n	745.149n	1.176u
1	0	116.459n	234.361n	435.527n	743.206n	1.174u
1	1	118.002n	237.423n	440.404n	750.463n	1.184u
XOR Gate TDPL065 [A]					
A	B	T=0°	T=25°	T=50°	T=75°	T=100°
0	0	116.977n	236.748n	440.885n	752.813n	1.189u
0	1	116.977n	236.748n	440.885n	752.813n	1.189u
1	0	116.977n	236.748n	440.885n	752.813n	1.189u
1	1	116.977n	236.748n	440.885n	752.813n	1.189u

Vrijednosti simuliranih struja curenja za osnovna TDPL kola l-tipa ukazuju da sa porastom temperature srazmjerno rastu i struje curenja za sve kombinacije ulaznog podatka. Važan zaključak je da su za TDPL NOT i XOR kola struje curenja, pri konstantnoj temperaturi, identične za sve kombinacije ulaznih podataka, dok se neznatno razlikuju za TDPL NAND kolo. Razlog ovakvih vrijednosti struja curenja kod TDPL NAND kola leži u strukturi ovog kola, koja je za razliku od TDPL NOT i XOR kola, asimetrična.

Poređenje CMOS i TDPL logike i njihova efiksanost u ulozi mjera zaštite od CLA napada može se izvršiti i kroz faktore NCD (*Normalized Current Deviation*) i NSD (*Normalized Standard Deviation*) [119], [120]. U Tabeli VII.3, pored vrijednosti NCD i NSD faktora, prikazane su i vrijednosti maksimalne struje curenja - *max(I),* minimalne struje

curenja - *min(I)*, srednje vrijednosti struje curenja - $\bar{I}$, i standardne devijacije struja curenja - σ_I. Faktor NCD prikazuje u kojoj mjeri struja curenja u CMOS, tj. TDPL kolu zavisi od vrijednosti ulaznog podatka i definiše se kao $\left(\max(I_{leakage}) - \min(I_{leakage})\right)/\max(I_{leakage})$, a ima vrijednost između 0 i 1. Drugi faktor NSD predstavlja normalizovanu standardnu devijaciju i definiše se kao odnos standardne devijacije σ_I i srednje vrijednosti struja curenja u kolu $\bar{I}$. Što su vrijednosti faktora NCD i NSD manje, podrazumijeva se da je teže izvući *side-channel* informaciju iz implementirane logike. Vrijednosti NCD i NSD faktora, koje su kod TDPL kola jednake ili približno jednake nultoj vrijednosti, označavaju invarijantnost veličine struje curenja na različite ulaze, a to znači da se ponavljanem napada sa različitim vrijednostima ulaza ne dobija nikakav novi podatak, koji bi vodio lakšem dešifrovanju ključa.

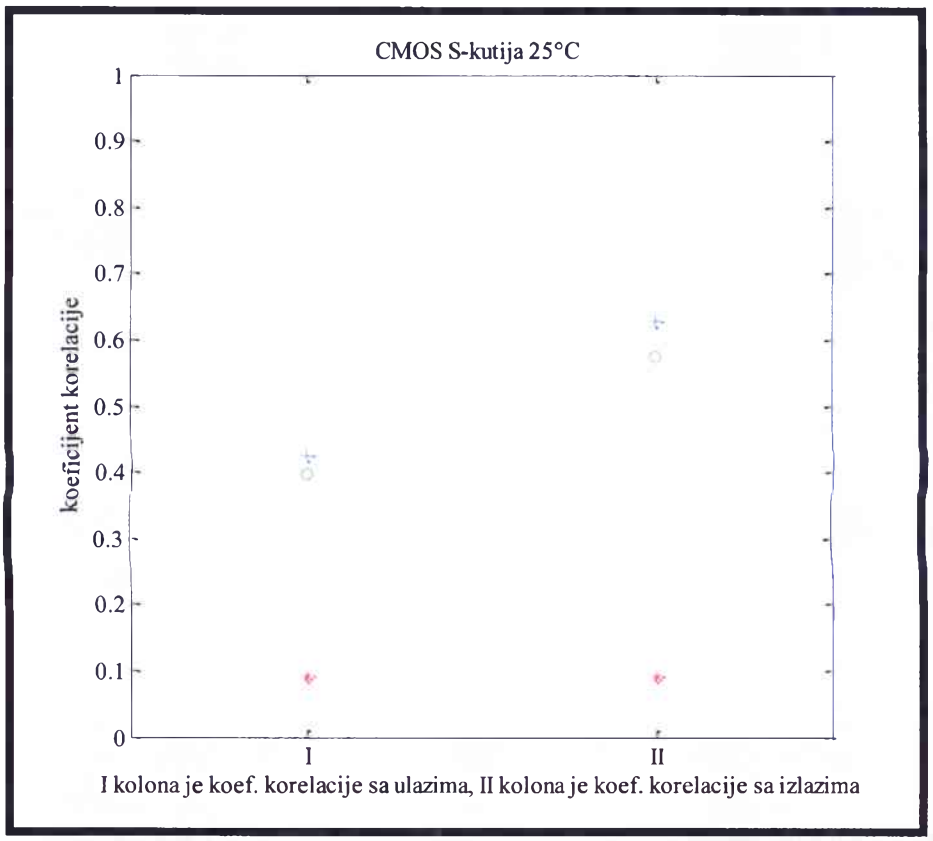
Tabela VII.3 – Poređenje rezultata struje curenja za CMOS i TDPL osnovna kola na temperaturi 25°

	CMOS NOT	TDPL NOT	CMOS NAND	TDPL NAND/AND	CMOS XOR	TDPL XOR/NXOR
max(I)[nA]	92.921	235.887	185.732	237.423	309.366	236.748
min(I)[nA]	37.561	235.887	16.471	234.361	210.491	236.748
NCD	59.5%	0%	91.1%	1.2%	31.9%	0%
$\bar{I}$ [nA]	65.241	235.887	67.645	235.609	265.07	236.748
σ_I[nA]	27.68	0	68.6	1.185	39.396	0
NSD	42.4%	0%	101.4%	0.5%	14.862%	0%

Analizirajući faktore NCD i NSD u Tabeli VII.3 lako se dolazi do zaključka da je TDPL logika mnogo bolja zaštitna mjera od CLA napada u odnosu na CMOS logiku. Ovaj zaključak donešen za osnovna kola, dalje će se testirati u okruženju eksperimentalnih uslova sa složenim TDPL kriptografskim jezgrom.

U ovom dijelu analize prikazana je zavisnost struje curenja od tačnosti *Hamming*-ove težine ulaznih, tj. izlaznih podataka, na primjeru 65nm-ske CMOS S-kutije. Ista S-kutija, kao u Poglavlju VI, upotrijebljena je i ovdje, pri čemu je njena struktura sastavljena od l-tipa tranzistora. Izvršene su simulacije struja curenja za četiri različite temperature (25°C, 50°C, 75°C, 100°C), (Dodatak B). Kada se vrijednosti struje curenja poređaju u rastućem

redosljedu, tj. od manje ka većoj, primjećuje se da je i raspored ulaznih podataka u S-kutiju, tj. izlaznih podataka iz S-kutije jako sličan. Podrazumijeva se da struje curenja rastu sa porastom temperature. Na Slici 7.1 prikazana je jednostavna analiza vezana za korelaciju struja curenja CMOS S-kutije i *Hamming*-ove težine ulaznih podataka CMOS S-kutije, tj. izlaznih podataka CMOS S-kutije (Dodatak B, folder Dodaci na priloženom CD-u). Analiza je rađena za temperaturu 25°C.



Slika 7.1 – Korelacija struja curenja i *Hamming*-ove težine ulaznih, tj. izlaznih podataka S-kutije

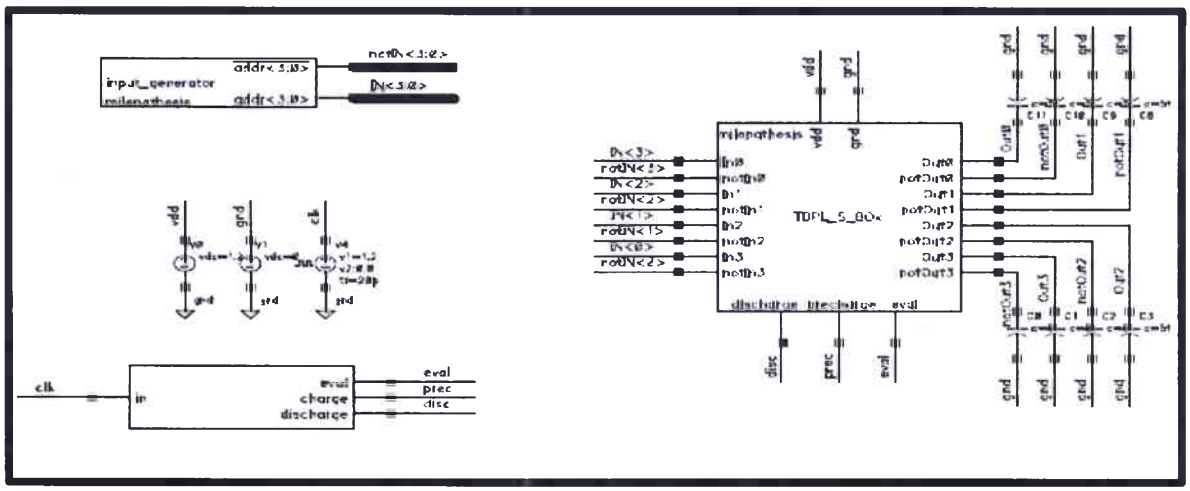
Naime, u I koloni su predstavljeni koeficijenti korelacije između struja curenja i *Hamming*-ove težine ulaznih podataka S-kutije, i to na sljedeći način:

- sa tačnom vrijednošću *Hamming*-ove težine ulaznih podataka u CMOS S-kutiju (obilježeno znakom „+“),

- sa vrijednošću *Hamming*-ove težine ulaznih podataka u CMOS S-kutiju, koja se razlikuje od tačne u promjeni jednog bita ulaznog podatka (obilježeno znakom „o“),
- sa potpuno nasumičnim izborom *Hamming*-ovih težina, ali koje odgovaraju ulaznim podacima CMOS S-kutije (obilježeno znakom „*“).

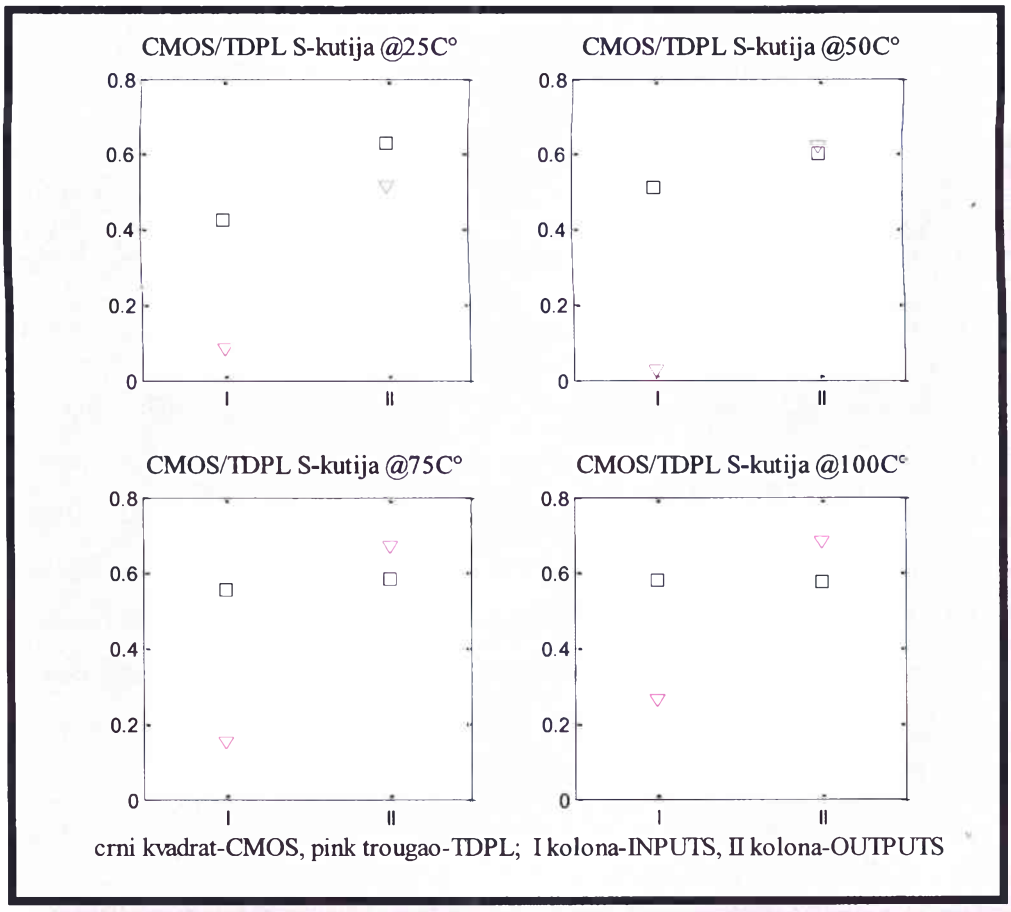
Isti ti koraci odrađeni su i za *Hamming*-ovu težinu izlaznih podataka S-kutije i predstavljeni u II koloni. Na osnovu dobijenih koeficijenata korelacije može se zaključiti da struje curenja značajno zavise od tačnosti *Hamming*-ove težine, kako ulaznih, tako i izlaznih podataka iz CMOS S-kutije l-tipa. Zato su koeficijenti korelacije u slučajevima „+“ i „o“ bliski, jer su bliske po veličini odgovarajuće vrijednosti *Hamming*-ove težine.

Dalja istraživanja podrazumijevaju poređenje dobijenih korelacija između struja curenja i *Hamming*-ove težine ulaznih, tj. izlaznih podataka S-kutije sačinjene od l-tipa tranzistora 65-nmske CMOS i TDPL logike. Da bi to bilo moguće, potrebno je simulirati struje curenja TDPL S-kutije za sve kombinacije ulaznih podataka (Slika 7.2). Za generisanje *precharge*, *evaluation* i *discharge* signala korišćen je specijalno dizajniran tzv. *clock_generator*, a za zadavanje ulaznih vrijednosti korišćeno je kolo *input_generator*-a, kao i kod CMOS S-kutije, sa tom razlikom što su sada oba invertovana izlaza aktivna, kako bi se omogućile sve kombinacije ulaza u TDPL S-kutiju (folder Dodaci na priloženom CD-u).



Slika 7.2 – Testno okruženje TDPL S-kutije

Simulirane su struje curenja TDPL S-kutije za četiri različite temperature (25°C, 50°C, 75°C, 100°C), (Dodatak B). Za sve četiri testirane temperature izvršeno je poređenje sa CMOS S-kutijom, i to tako što se u svakom kvadrantu Slike 7.3 u I koloni nalazi koeficijent korelacije između struja curenja i *Hamming*-ove težine ulaznih podataka S-kutije, a u II koloni je prikazan koeficijent korelacije između struja curenja i *Hamming*-ove težine izlaznih podataka S-kutije (Matlab kod se nalazi u folderu Dodaci na priloženom CD-u). Korelacije dobijene za CMOS S-kutiju označene su crnim kvadratićem, a korelacije dobijene za TDPL S-kutiju označene su pink trouglićem.



Slika 7.3 – Poređenje CMOS/TDPL S-kutije

Korelacije koje su vezane za ulazne podatke S-kutije daju očekivane rezultate. Za sve četiri testirane temperature korelacija između struja curenja i *Hamming*-ove težine ulaznih podataka u S-kutiju je značajno veća za CMOS nego za TDPL logiku. Veći stepen korelacije ovih veličina za CMOS kola znači i veću mogućnost nalaženja pravog ključa na osnovu snimljenih struja curenja. To dalje vodi do zaključka da bi se CMOS S-kutija mogla lakše napasti od TDPL S-kutije. Korelacije dobijene između struja curenja i *Hamming*-ovih težina izlaznih podataka S-kutije ne idu u prilog TDPL logike. Ali, i ti rezultati su donekle očekivani, jer izlazni podatak dolazi iz S-kutije koja predstavlja nelinearan operator. Informacija o korelaciji se ne gubi (ne mijenja) samo u slučaju kada se izvode linearne operacije. Iz tog razloga je CLA napad na ulazne podatke S-kutije u Poglavlju VI pokazao odlične rezultate. U većini slučajeva uspješnih CLA napada, meta napada su ulazni, a ne izlazni podaci kriptografskog jezgra.

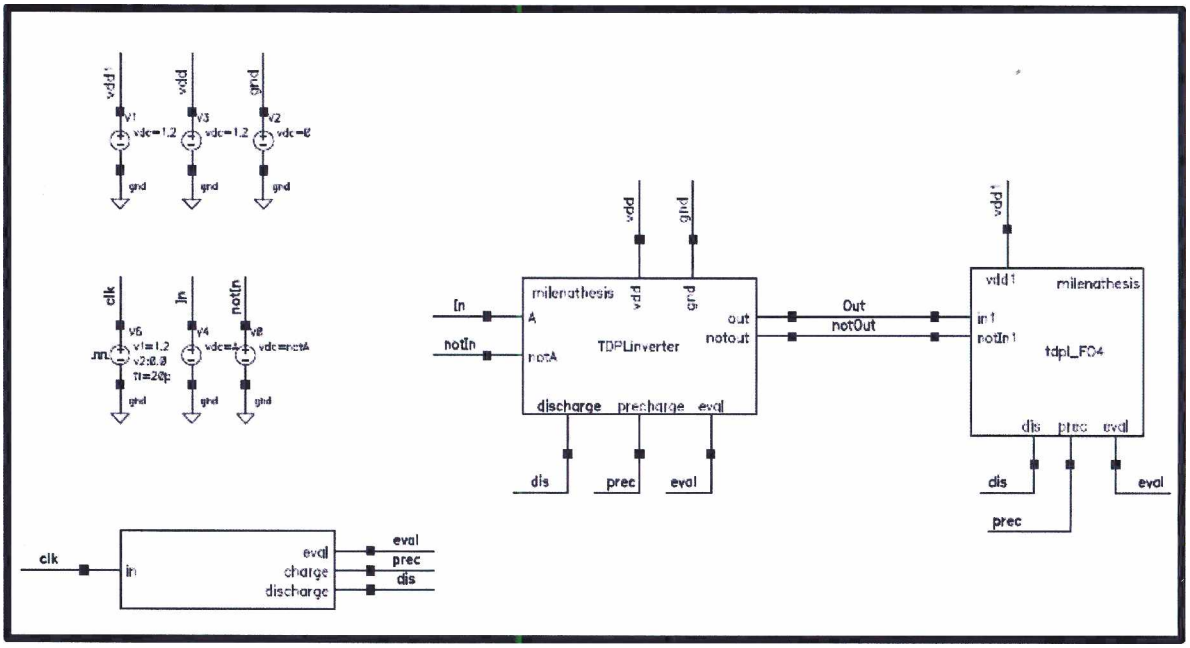
§ *VII.2 CLA napad na 65nm-sko TDPL kriptografsko jezgro*

TDPL (*Three- Phase Dual-Rail Pre-Charge Logic*) logika se do sada pokazala kao najefikasniji vid zaštite hardvera na tranzistorskom nivou od DPA napada, tj. napada koji eksploatišu postojeću zavisnost dinamičke snage disipacije (ili dinamičkih struja) kriptografskog jezgra od procesuiranih podataka [121]. Za razliku od pomenute reference [121], analize u ovoj doktorskoj tezi fokusirane su na poređenje isključivo CMOS i TDPL logike kao hardverskih mjera zaštite, i to metodom *step-by-step*, tj. od najniže strukturne jedinice - osnovnih logičkih kola, preko složenijih blokova - S-kutije, pa do finalnog dizajna kriptografskog jezgra. Takođe, analize su vršene za dva tipa tranzistora, l-tip i h-tip. Za tranzistore h-tipa, okruženje za izvršenje napada je najkompleksnije, jer su struje curenja najmanje vrijednosti. Za tranzistore l-tipa, struje curenja su znatno veće, ali je svakako potrebno provjeriti da li logika funkcionisanja napada baziranog na analizi struja curenja funkcioniše kako je prognozirano.

Dosadašnji rezultati su pokazali da se CMOS logika nije pokazala efikasnom u odbrani od CLA napada (Poglavlje VI), kao i da bi se CMOS S-kutija ulaznih podataka mogla

lakše napasti od odgovarajuće TDPL S-kutije (Poglavlje VII.1). Ovaj dio poglavlja podrobnije analizira opis i procedure napada, obavljene simulacije, kao i rezultate koji preciznije upućuju i razjašnjavaju u kojoj se mjeri TDPL logika, dokazano efikasnija od CMOS, može koristiti kao efikasna zaštita u hardveru od CLA napada.

Koraci CLA napada na 65nm-sko TDPL kriptografsko jezgro isti su kao i za CLA napad na 65nm-sko CMOS kriptografsko jezgro (Poglavlje VI). Prije nego li se počne sa egzekucijom CLA napada, potrebno je izanalizirati zavisnost struja curenja djelova TDPL kriptografskog jezgra (TDPL osnovna kola, TDPL S-kutija) od procesuiranih podataka. Također, treba izvršiti poređenje sa rezultatima odgovarajućih CMOS komponenti (CMOS osnovna kola, CMOS S-kutija).



Slika 7.4 – Eksperimentalno okruženje za izvođenje *MC* simulacija nad TDPL NOT kolom

Da bi se mogla napraviti realna komparacija 65nm-skih TDPL osnovnih kola sa 65nm-skim CMOS osnovnim kolima upotrijebljeni su tranzistori h-tipa, kao i testno kolo FO4 (*Fanout-of-4*) koje je povezano sa krajem svakog TDPL osnovnog kola (Slika 7.4). Ovo kolo se sastoji od četiri ista paralelno vezana TDPL invertora, također implementirana u 65nm-skoj

tehnologiji (šematski prikazi su u folderu Dodaci na priloženom CD-u). Simulacije za TDPL osnovna kola vršena su u prisustvu procesnih varijacija, a postavke *Monte Carlo* okruženja unutar okvira za definisanje simulacije (*Simulator Window*) su identične kao i za CMOS osnovna kola:

- izbor broja iteracija (*Number of Runs=400*),
- početna iteracija (*Starting Run*=1),
- tip varijacije (*Analysis Variation=Mismatch*),
- čuvanje grafika i rezultata svih iteracija (*Save Data Between Runs to Allow Family Plots=yes*),
- definisanje izlaza je potrebno prikazati (*Ouputs=AutoPlot wave leakage current*),
- radna temperatura na kojoj će se vršiti simulacije (*Temperature=25°C*),
- zadavanje vrijednosti parametrima tolerancije (*reltol*=1e-6, *vabstol*=1e-8, *iabstol*=1e-14).

Tabela VII.4 – Rezultati *Monte Carlo* simulacija za osnovna TDPL kola

NOT Gate TDPL 065 @ 25°						
A		*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0		14.7813n	16.0668n	1.8635n	25.0900n	12.6700n
1		14.7813n	16.2080n	2.2269n	35.6100n	12.3700n
NAND Gate TDPL 065 @ 25°						
A	**B**	*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0	**0**	14.9039n	15.7454n	1.6650n	24.9200n	12.5400n
0	**1**	14.8704n	15.7438n	1.6684n	24.8500n	12.5300n
1	**0**	14.8310n	15.7346n	1.6678n	24.8800n	12.5800n
1	**1**	14.7766n	15.7388n	1.4314n	21.1900n	12.6400n
XOR Gate TDPL 065 @ 25°						
A	**B**	*obična simulacija*	*MC simulacija*	*standardna devijacija*	*max struja*	*min struja*
0	**0**	14.8903n	15.6765n	1.9032n	25.9500n	12.4800n
0	**1**	14.8903n	15.9148n	2.2529n	39.9600n	12.6700n
1	**0**	14.8903n	15.9158n	2.2540n	39.9700n	12.6100n
1	**1**	14.8903n	15.6772n	1.9011n	25.9900n	12.4700n

Na osnovu dobijenih rezultata prikazanih u Tabeli VII.4, koji predstavljaju srednju vrijednost struje curenja, standardnu devijaciju, maksimalnu i minimalnu struju curenja među 400 uzoraka TDPL osnovnih kola može se zaključiti da su struje curenja nakon standardnih i *MC* simulacija jako slične za sve kombinacije ulaza. Na primjer, za TDPL XOR kolo struje curenja nakon standardne simulacije u Cadence softveru imaju iste vrijednosti za sve četiri kombinacije ulaznog podatka. Nakon izvršenih *MC* simulacija, vrijednosti struja curenja nijesu identične, ali su zato previše slične da bi se ulazni podaci mogli jasno razlikovati.

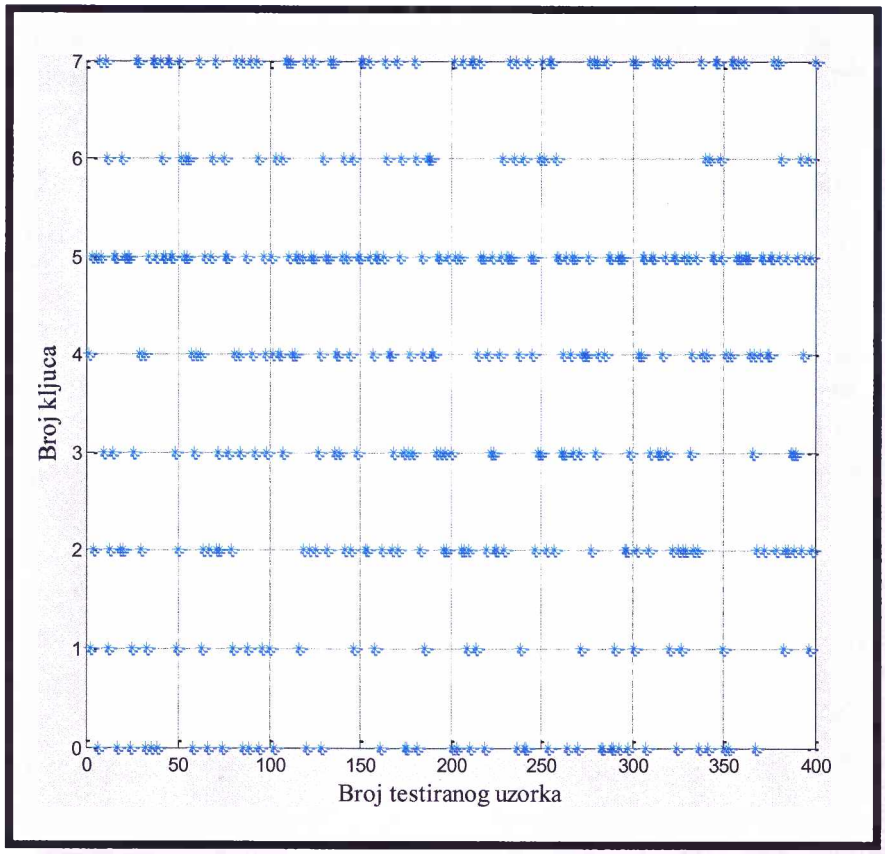
Za realizaciju 65nm-ske TDPL S-kutije upotrijebljena je identična fiksna S-kutija Serpent-ovog algoritma, kao i za realizaciju 65nm-ske CMOS S-kutije (Dodatak A). Testno okruženje 65nm-ske TDPL S-kutije za izvođenje standardnih i *MC* simulacija struja curenja izgleda kao na Slici 7.2, sa tom razlikom što su umjesto l-tipa tranzistora upotrijebljeni tranzistori h-tipa. Sve simulacije su izvedene na temperaturi od 25°C. Kako je testno okruženje za TDPL S-kutiju znatno složenije nego za CMOS S-kutija, treba otprilike 5-7 puta više vremena za izvršenje *MC* simulacija u Cadence softveru.

Posmatrajući rezultate standardnih i *MC* simulacija 65nm-ske TDPL S-kutije (Tabela VII.5), dobijaju se isti zaključci kao i za 65nm-sku CMOS S-kutiju, a to je da se ulazni podaci S-kutije na osnovu izmjerenih struja curenja ne mogu međusobno razlikovati pod uticajem procesnih varijacija (svi rezultati *MC* simulacija za osnovna TDPL kola i TDPL S-kutiju nalaze se u folderu Dodaci na priloženom CD-u).

Tabela VII.5 – Rezultati *Monte Carlo* simulacija za TDPL S-kutiju

Ulazni podatak	Izlazni podatak	Obična simulacija 065 @25°	MC simulacija 065 @25°	standardna devijacija 065 @25°
0000	0011	571.7696n	599.4740n	17.2392n
0001	1000	571.1768n	598.8834n	17.8818n
0010	1111	573.3521n	603.8795n	17.7725n
0011	0001	576.0051n	600.3099n	17.9052n
0100	1010	567.2071n	597.0837n	17.4082n
0101	0110	569.2978n	594.6012n	17.7766n
0110	0101	565.0612n	605.0017n	17.0559n
0111	1011	571.7697n	594.0404n	17.5237n

1000	**1110**	571.1772n	596.6582n	16.8189n
1001	**1101**	569.0563n	598.6282n	17.6184n
1010	**0100**	575.7609n	603.8484n	17.8551n
1011	**0010**	575.7071n	604.0324n	17.8091n
1100	**0111**	534.2399n	601.2327n	16.8835n
1101	**0000**	538.3948n	599.9972n	16.2009n
1110	**1001**	536.4798n	602.6249n	16.5040n
1111	**1100**	540.4403n	603.1312n	16.6789n



Slika 7.5 – Rezultati CLA napada prema najvećoj vrijednosti koeficijenta korelacije na 400 testnih TDPL uzoraka

Projektovano 65nm-sko TDPL kriptografsko jezgro ima identičnu strukturu kao i 65nm-sko CMOS kriptografsko jezgro, koje se sastoji iz kombinatornog i sekvencijalnog dijela. Unutar jezgra zadata je vrijednost ključa kao i kod CMOS jezgra (*Key*=0101), kako bi

se mogli porediti rezultati. Nad TDPL kriptografskim jezgrom izvršeno je 400 *Monte Carlo* iteracija struja curenja jezgra, sa posebnom konfiguracijom nasumičnih procesnih varijacija. I ovdje, rezultati *Monte Carlo* simulacija zajedno čine matricu 16x400 struja curenja u kojoj element (i, j) predstavlja vrijednost struje curenja za ulaz i ($0 \leq i \leq 15$) u čipu j ($1 \leq j \leq 400$).

Rezultati CLA napada na TDPL kriptografsko jezgro mogu se analizirati posmatrajući Sliku 7.5 na kojoj su prikazane vrijednosti koeficijenta korelacije za svaki od 400 TDPL testnih uzoraka pod uticajem procesnih varijacija u odnosu na vrijednost ključa [122]. Ne može se sa sigurnošću reći da je CLA napad uspio za neki od ovih ključeva.

Tek posmatrajući Tabelu VII.6 vidimo da je CLA napad uspio za pravi ključ broj 5 (*Key*=0101), ali svakako nije efikasan kao napad na CMOS kriptografsko jezgro. TDPL logika je efikasnija mjera zaštite od CMOS logike u odnosu na CLA napade, mada ne toliko efikasna kao u slučaju zaštite od DPA napada.

Tabela VII.6 – Broj napadnutih testnih uzoraka u odnosu na najveći koeficijent korelacije

Broj ključa	Ključ	Broj napadnutih testnih uzoraka od 400 (max koef. korelacije)
0	0000	42
1	0001	25
2	0010	54
3	0011	42
4	0100	52
5	0101	94
6	0110	32
7	0111	59

Dakle, ovaj CLA napad uspješan je u 23,5% slučajeva, tj. za 94 testna TDPL uzorka od 400 napadnutih. Ukoliko bi napadač uzeo u obzir ključeve za dva najveća koeficijenta korelacije, CLA napad bi bio uspješan u 150 testnih uzoraka od 400 napadnutih, tj. u 37,5%

slučajeva. Za tri najveća koeficijenta korelacije napad bi bio uspješan u 198 testnih uzoraka od 400 napadnutih, što je neznatno manje od polovine broja napadnutih čipova. Na osnovu ovih rezultata jasno je da TDPL logika nije dovoljno pouzdana mjera zaštite od CLA napada.

I pored očekivanja da će se TDPL logika pokazati uspješnom zaštitom od CLA napada, to se nije ostvarilo. Sada pametne kartice u kojima je implementirana TDPL logika predstavljaju sigurnu zaštitu od najaktuelnijih side-channel napada - DPA napada, ali nijesu pouzdana zaštita od CLA napada. Zavisnost struje curenja kriptografskog jezgra od *Hamming*-ove težine ulaznih podataka jezgra pokazala se kao dobra *side-channel* informacija koja dovodi do probijanja kriptografskog algoritma i nalaženja tajnog ključa.

U budućnosti, značajni istraživački napori biće neophodni kako bi se našla bolja rješenja i mjere zaštite od CLA napada.

§ *VII.3 Zaključci*

Kako se CLA napad pokazao uspješnim na CMOS kriptografsko jezgro, u ovom poglavlju je izvršena analiza jedne od najnovijih i najperspektivnijih hardverskih mjera zaštite na tranzistorskom nivou - TDPL logike, koja je prvobitno kreirana kao protivmjera napadima baziranim na analizi dinamičke disipacije snage i dinamičkih struja - DPA (*Differential Power Analysis*) napadima.

Iz tog razloga, sprovedena su dva tipa istraživanja. Prvi tip se odnosi na poređenja standardnih *Bsim4* TDPL i CMOS l-tip-a tranzistora simulirajući struje curenja u programu Cadence u STMicroelectronics 65nm-skoj tehnologiji. Poređenje CMOS i TDPL logike, kao i njihova efikasnost u ulozi hardverskih mjera zaštite od CLA napada, izvršeno je kroz dobijene vrijednosti NCD i NSD faktora. Za TDPL kola, vrijednost ovih faktora je jednaka ili približno jednaka nultoj vrijednosti, čime se označava invarijantnost veličine struje curenja na različite ulaze, a to znači da se ponavljanem napada sa različitim vrijednostima ulaza ne dobija nikakav novi podatak, koji bi vodio lakšem dešifrovanju ključa. Shodno tome, TDPL logika je mnogo bolja zaštitna mjera od CLA napada na kriptografsko jezgro pametnih kartica u odnosu na CMOS logiku, što predstavlja poseban doprinos disertacije. U ovom dijelu

istraživanja izvršena je i komparacija CMOS i TDPL S-kutije l-tipa u odnosu na struje curenja i njihova zavisnost od *Hamming*-ove težine ulaznih, odnosno izlaznih podataka iz S-kutije, uzimajući u obzir i temperaturnu zavisnost.

Drugi tip istraživanja podrazumijevao je izvršenje CLA napada na 65nm-sko TDPL kriptografsko jezgro pod uticajem procesnih varijacija. Dobijeni rezultati su upoređeni sa prethodno dobijenim rezultatima za CLA napad na 65nm-sko CMOS kriptografsko jezgro. Uspješnost CLA napada na 65nm-sko TDPL kriptografsko jezgro (94/400) je znatno manjeg nivoa u odnosu na slučaj CLA napada na 65nm-sko CMOS kriptografsko jezgro (370/400). Drugim riječima, 65nm-sko TDPL kriptografsko jezgro pametne kartice je značajno pouzdanija zaštita od 65nm-skog CMOS kriptografskog jezgra, ali ujedno ne i dovoljno pouzdana. Zaključak, koji predstavlja poseban doprinos disertacije, je da dok sa jedne strane pametne kartice sa implementiranom TDPL logikom predstavljaju sigurnu zaštitu od *side-channel* napada - DPA napada, sa druge strane ta ista logika, na osnovu dobijenih rezultata, iako pouzdanija u odnosu na CMOS, ne može biti prihvaćena kao pouzdana zaštita od CLA napada.

VIII Zaključak

Nastojanje da se pronađu nove tehnike napada iz klase *side-channel* napada, kao i odgovarajuće mjere zaštite (*countermeasures*) u vidu odgovora na te napade, predstavljaju fundamentalne izazove vezane za razvoj pametnih kartica (*smart cards*). O tome svjedoči veliki broj, u novije vrijeme, objavljenih naučnih radova na ovu temu. Upravo istraživanje tehnika *side-channel* napada na hardver pametne kartice i odgovarajuće mjere hardverske zaštite predstavljaju temu ove doktorske disertacije.

Side-channel napadi eksploatišu informaciju koja "curi" iz kriptografskog uređaja u toku izvršavanja algoritma, a jedna grupa *side-channel* napada posebno dobija na značaju u posljednje vrijeme - pasivni napadi bazirani na analizi statičke disipacije snage i struja curenja. Sa implementacijom novih tehnologija (90nm-skom, 65nm-skom, 45nm-skom) unutar hardvera pametne kartice, statička disipacija snage ima dominantan udio u ukupnoj snazi disipacije, čime se stvaraju mogućnosti za formiranje efikasnih vrsta napada baziranih upravo na analizi ove pojave. Jedan od doprinosa ove disertacije ogleda se u analizi i implementaciji nove tehnike pasivnih napada koja je bazirana na analizi struja curenja hardvera pametne kartice - CLA (*Correlation Leakage Analysis*) napad. Istraživanja su potkrijepljena velikim brojem opsežnih eksperimentalnih rezultata i kompleksnih simulacija. Dobijeni rezultati, ostvareni u složenim eksperimentalnim uslovima koji definišu ambijent izvođenja realnih napada, pokazali su visoku efikasnost CLA napada na CMOS kriptografsko jezgro. Istraživanja su obuhvatila takođe i analizu uticaja *intra-die* procesnih varijacija na uspješnost CLA napada na 65nm-sko CMOS kriptografsko jezgro. Eksperimentalni rezultati, bazirani na *Monte Carlo* simulacijama, su pokazali da je uticaj ovih varijacija minoran tj. da ga nije potrebno uzimati u obzir pri modelovanju uspješnog CLA napada. Generalno, CLA napadi su se pokazali izuzetno uspješnim na velikom broju testnih uzoraka (400) kriptografskog uređaja izvedenog u CMOS tehnologiji, čime se pokazalo da CMOS tehnologija ne predstavlja dovoljno dobru mjeru zaštite protiv CLA napada.

Sa druge strane, u disertaciji je dat poseban doprinos analizi adekvatnih mjera zaštite u odnosu na CLA napade na hardver pametne kartice. U tom smislu razmatrana je najnovija i najperspektivnija hardverska mjera zaštite na tranzistorskom nivou - TDPL (*Three-Phase Dual-Rail Pre-Charge Logic*) logike, koja je prvobitno kreirana kao vrlo efikasna protivmjera napadima baziranim na analizi dinamičke disipacije snage i dinamičkih struja, tzv. DPA (*Differential Power Analysis*) napadima. U tu svrhu je modelovan CLA napad na 65nm-sko TDPL kriptografsko jezgro sa uzimanjem u obzir procesnih varijacija. Dobijeni rezultati su upoređeni sa prethodno dobijenim rezultatima za CLA napad na 65nm-sko CMOS kriptografsko jezgro. Uspješnost CLA napada na 65nm-sko TDPL kriptografsko jezgro nije bila takvog nivoa uspješnosti kao u slučaju CLA napada na 65nm-sko CMOS kriptografsko jezgro. Zaključak je da dok sa jedne strane pametne kartice sa implementiranom TDPL logikom predstavljaju sigurnu zaštitu od *side-channel* napada - DPA napada, sa druge strane ta ista logika, na osnovu dobijenih rezultata, iako nešto pouzdanija u odnosu na CMOS, ne može biti prihvaćena kao pouzdana zaštita od CLA napada.

Zavisnost struje curenja kriptografskog jezgra, kao i sastavnih djelova kriptografskog jezgra, od *Hamming*-ove težine ulaznih podataka jezgra pokazala se kao dobra *side-channel* informacija koja se može koristiti za probijanje kriptografskog algoritma i nalaženja tajnog ključa. U disertaciji je prikazana i zavisnost struja curenja od implementirane tehnologije (90nm-ska i 65nm-ska), tipa tranzistora (h-tip i l-tip), temperature (0°C, 25°C, 50°C, 75°C, 100°C), tipa podataka (ulazni ili izlazni podaci), itd. Takođe, izvršena je komparacija 65nm-ske CMOS/TDPL logike putem faktora NCD (*Normalized Current Deviation*) i NSD (*Normalized Standard Deviation*) sa aspekta njihove efikasnosti kao mjera zaštite od CLA napada. Analiza putem ovih faktora je potvrdila prethodno iznijet zaključak koji se odnosi na veću pouzdanost TDPL logike u odnosu na CMOS logiku kada se govori o CLA napadima, ali ne u tolikoj mjeri da bi TDPL logika mogla biti prihvaćena kao pouzdana zaštita od CLA napada.

Dalje istraživanje bi moglo biti fokusirano u sljedećim pravcima:

- testiranje tehnike CLA napada na 45nm-sko i 35nm-sko CMOS i TDPL kriptografsko jezgro;
- kombinovanje CLA napada sa drugim *side-channel* informacijama radi formiranja novih, tj. uspješnijih tehnika *side-channel* napada;

- traženje boljih rješenja i hardverskih mjera zaštite od CLA napada;
- istraživanje i razvoj boljih hardverskih mjera zaštite koje će pratiti razvoj naprednijih tehnika *side-channel* napada.

Literatura:

[1] Y. Haghiri, T. Tarantino: „Smart Card Manufacturing: A Practical Guide“, John Wiley & Sons, 2002.

[2] S. Dhar, „Introduction to Smart Cards“, Auerbach Publications, CRC Press LLC, 2003.

[3] J. Pelkmans, „The GSM Standard: Explaining a Success Story“, Centre for European Policy Studies, 2000.

[4] A. Haddad, „A New Way to Pay: Creating Competitive Advantage through the EMV Smart Card Standard“, Gower Publishng Company, 2005.

[5] T. M. Jurgensen, S. B. Guthery: „Smart Cards: the developer's toolkit“, Prentice Hall PTR, 2002.

[6] A. P. Godse, D. A. Godse: „Microprocessor, Microcontroller and Embedded Systems“, Techical Publications, 2009.

[7] B. Stanford-Smith: „Business and work in the information society: new technologies and applications“, IOS Press, 1999.

[8] K. Finkenzeller: „RFID handbook: fundamentals and applications in contactless smart cards and indentification“, John Wiley & Sons, 2003.

[9] K. Finkenezeller: „RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication“, John Wiley & Sons, 2010.

[10] P. Saha: „Handbook of Enterprise Systems Architecture in Practise“, Idea Group Inc. (IGI), 2007.

[11] W. Rankl: „Smart card applications: design models for using and programming smart cards“, John Wiley & Sons, 2007.

[12] B. Williams: „Intelligent Transport System Standards“, Artech House, 2008.

[13] Vedder, F. Weikmann: „Smart Cards - Requirments, Properties and Applications“, Springer, 1998.

[14] N. Nedjah, L. De Macedo Mourelle: „Embedded cryptographic hardware: design & security“, Nova Publishers, 2005.

[15] L. F. Cranor, S. Garfinkel: „Security and usability: designing secure systems that people can use“, O'Reilly Media Inc, 2005.

[16] A. D'Agapeyeff: „Codes and Ciphers – A History of Cryptography“, Read Books, 2008

[17] J. L. Smith: „The Design of Lucifer, A Cryptographic Device for Data Communications“, IBM Research Report, 1972.

[18] C. Paar, J. Pelzl, „The Data Encryption Standard (DES) and Alternatives“, Chapter 3 of „Understanding Cryptography, A Textbook for Students and Practitioners“, Springer, 2009.

[19] National Institute of Standards and Technology, „Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher“, NIST Special Publication 800-67, May 2008.

[20] J. Daemen, V. Rijmen, „The Design of Rijndael: AES - The Advanced Encryption Standard“, Springer, 2002.

[21] W. Diffie, M. Hellman: „New Directions in Cryptography“, IEEE International Symposium on Information Theory, Sweden, 1976.

[22] R. L. Rivest, A. Shamir, L. M. Adleman, ``A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Feb. 1978, pp. 120-126.

[23] P. R. Zimmermann, „PGP: Sorce Code and Internals“, The MIT Press, 1995.

[24] P. R. Zimmermann, „The Official PGP User's Guide“, The MIT Press, 1996.

[25] W. Rankl, W. Effing: „Smart Card Handbook“, Third Edition, John Wiley & Sons, 2003.

[26] K. E. Mayes, K. Markantonakis: „Smart Cards, Tokens, Security and Applications“, Springer, 2008.

[27] Electronic Frontier Foundation, „Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design“, Oreilly and Associates Inc, 1998.

[28] K. Vedder, F. Weikmann: „Smart Cards - Requirments, Properties and Applications“, Springer, 1998.

[29] H. Bar-El: „Known Attacks Against Smart Cards“, Discretix Technologies, 2008.

[30] O. Kommerling, M. G. Kuhn, „Design Principles for Tamper-Resistant Smartcard Processors“, USENIX Workshop on Smartcard Technology (Smartcard '99), pages 9-20, May 1999.

[31] R. J. Anderson, „Security Engineering: A Guide to Building Dependable Distributed Systems“, Wiley, 2001. ISBN 0-471-38922-6.

[32] S. P. Skorobogatov, „Semi invasive attacks – A new approach to hardware security analysis“, Doctoral thesis, University of Cambridge, 2005. Available online at http://www.cl.cam.ac.uk/TechReports/

[33] D. Samyde, S. P. Skorobogatov, R. J. Anderson, J. J. Quisquater, „On a New Way to Read Data from Memory“, IEEE Security in Storage Workshop (SISW'02), pages 65-69, IEEE Computer Society, 2002.

[34] S. P. Skorobogatov, R. J. Anderson, „Optical Fault Induction Attacks“, Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, vol. 2523 of Lecture Notes in Computer Science, pages 2-12, Springer, 2003

[35] M. Jovanovic, „Leakage Power Analysis (LPA) Attack on Cryptographic Device Realized in CMOS 90-nanometer Technology", Electronic Design News, vol. 54, Issue 10, pp. 23-26, May 2009.

[36] P. Kocher, J. Jaffe, B. Jun: „Differential Power Analysis“, Advances in Cryptology – CRYPTO '99, 19th Anual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings, volume 1666 of Lecture Notes in Computer Science, pages 388-397, Springer, 1999.

[37] S. Mangard: „Overview of Side-Channel Analysis Attacks“, Institute for Applied Information Processing and Communications (IAIK), 2005.

[38] M. Djukanovic, V. Vujicic, „Ways of Attacking Smart Cards and their Countermeasures“, VIPSI Conference '11, September 23.-26. 2010, Venice, Italy, in print in IPSI Journal – Tranasactions on Internet Research, January 2012, volume 8, Number 1.

[39] L. Giancane: „Power Analysis Techniques and Countermeasures Designing Secure Devices“, Master Degree Thesis at La Sapienza University, Rome, Italy, 2005.

[40] P. Kocher: „Timing Attacks on Implementations of Diffie-Hellman, RSA, DSA and Other Systems“, Advances in Cryptology, CRYPTO '96, volume 1109 of LNCS, pages 104-113, Springer, 1996.

[41] P. Wayner: „Code Breaker Cracks Smart Cards' Digital Safe“, New York Times, page D1, 22. jun 1998.

[42] P. Kocher, B. Jun: „Introduction to Differential Power Analysis and Related Attacks“, Technical Report, Cryptography Research Inc., 1998.

[43] T. S. Messerges, „Power Analysis Attack Countermeasures and their weaknesses“, Doctoral thesis, Security Technology Research Laboratory Motorola, 2000.

[44] J. M. Rabaey, A. Chandrakasan, B. Nikolić, „Digital Integrated Circuits“, Prentice Hall, Second Edition, 2003.

[45] S. Mangard, E. Oswald, T. Popp: „Power Analysis Attacks: Revealing the Secrets of Smart Cards“, Springer Science +Business Media, 2007.

[46] N. Weste, K. Eshraghian: „Principles of CMOS VLSI Design: A Systems Perspective“, Addison-Wesley, 1994.

[47] L. Giancane: „Power Analysis Techniques and Countermeasures Designing Secure Devices“, Master Degree Thesis at La Sapienza University, Rome, Italy, 2005.

[48] J. J. Quisquater, D. Samyde, „ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards“, Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security, Lecture Notes In Computer Science, Vol. 2140, Pages 200-210, Springer, 2001.

[49] K. Gandolfi, C. Mourtel, F. Olivier, „Electromagnetic analysis: Concrete results“. In C. K. Koc, D. Naccache, C. Paar, editors, CHES, 2001.

[50] D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi, „The EM side-channel(s): Attacks and assessments methodologies“, in Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), B.S. Kaliski Jr., C. K. Koc, C. Paar, Eds., 2002, vol 2523 of LNCS, pp. 29-45, Springer-Verlag

[51] D. Agrawal, J. R. Rao, P. Rohatgi, „Multi channel attacks“, Proceedings of 5th Interantional Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2770 of LNCS, pages 2-16, 2003, Springer-Verlag

[52] D. Agrawal, B. Archambeault. S. Chari, J. R. Rao, P. Rohatgi, „Advances in side-channel cryptanalysis“, RSA Laboratories Crybtobytes, vol. 6, no. 1, pp. 20-32, 2003.

[53] D. Boneh, R. A. De Millo, R. J. Lipton, „On the Importance of checking cryptographic protocols for faults“, Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques, Lecture Notes In Computer Science, pages 37-51, Springer-Verlag, 1997.

[54] M. Otto, „Fault Attacks and Countermeasures“, PhD Thesis, University of Paderborn, December 2004.

[55] H. Bar-El, H. Choukri, D, Naccache, M. Tunstall, C. Whelan, „The Sorcerer's Apprentice Guide to Fault Attacks“, Proceedings of the IEEE, Volume 94, pages 370-382, February 2006.

[56] E. Oswald, S. Mangard, N. Pramstaller, "Secure and Efficient Masking of AES – A Mission Impossible?", SCA – Lab Technical Report Series, 2003.

[57] S. Chari, C. S. Jutla, J. R. Rao, P. Rohatgi, „A Cautionary Note Regarding Evaluation of AES Candidates on Smart CardsPro“, Second Advanced Encryption Standard (AES) Candidate Conference, Rome, Italy, 1999.

[58] A. Shamir, „Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies“, Proc. Workshop Cryptographic Hardware and Embedded Systems (*CHES 2000*), volume 1965 of Lecture Notes in Compute Science (LNCS), pp. 71-77, Springer, 2000.

[59] P. Waymen, „Code Breaker Cracks Smart Card's Digital Safe“, New York Times, pp. C1, June 1998.

[60] T. Messerges, E. Dabbish, R. Sloan, „Investigations on Power Analysis Attacks on Smartcards“, Proc. USENIX Workshop on Smartcard Technology (Smartcard '99), pp. 151-161, 1999.

[61] T. Messerges, E. Dabbish, R. Sloan, „Examining Smart-Card Security under the Threat of Power Analysis Attacks“, IEEE Trans. Computers, vol. 51, no. 5, May 2002.

[62] J. Daemen, V. Rijmen, „Resistance against Implementation Attacks: A Comparative Study of the AES Proposals“, Second Advanced Encryption Standard

(AES) Candidate Conference. Available online at http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

[63] P. Rackers, L. Connell, T. Collins, D. Russell, „Secure Contactless Smartcard ASIC with DPA Protection“, IEEE Journal of Solid-State Circuits, pp. 559-565, March 2001

[64] M. L. Akkar, R. Bevan, P. Dischamp, D. Moyart, „Power Analysis, What Is Now Possible“, Proc. Sixth Int. Conf. the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT 2000), pp. 489-502, 2000.

[65] C. Clavier, J. S. Coron, N. Dabbous, „Differential Power Analysis in the Presence of Hardware Countermeasures“, Proc. Second Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 2000), pp. 78-92, 2000.

[66] S. Mangard, T. Popp, B. M. Gammel, „Side-Channel Leakage of Masked CMOS Gates“, The Cryptographer's Track at the RSA Conference, San Francisco, CA, USA, February 2005.

[67] J. Dj. Golic, R. Menicocci, „Universal masking on logic gate level“, Electronics Letters, vol. 40, no. 9, April 2004.

[68] R. Menicocci, J. Pascal, „Elaborazione crittografica di dati digitali mascherati“, Italian patent pending MI2003A001375, July 2003.

[69] E. Trichina, E. De Seta, D. Germani, „Simplified Multiplicative Maskingfor AES and its secure implementation“, in Cryptographic Hardwave and Embedded Systems: CHES 2002, vol. 2523 of Lecture Notes in Computer Science, pp. 277-285, Springer-Verlag, 2002.

[70] M. Bucci, M. Giglielmo, R. Luzzi, A. Trifiletti, „A Countermeasure against Differential Power Analysis based on Random Delay Insertion“, Cicuits and systems 2005, ISCAS 2005, vol. 4, pp.3547-3550, 2005.

[71] V. Bagini, M. Bucci, „A design od reliable true random number generator for cryptographic applications“, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES 99), Heidelberg, Germany, Springer-Verlag, 1999, vol. 1717, pp. 204-218.

[72] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, „A high speed random number source for cryptographic applications on a SmartCard“, IEEE Trans. Comput., vol. 52, pp. 403-409, April 2003.

[73] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, M. Varanonuovo, „A high speed IC random number source for SmartCard microcontrollers“, Circuit and Systems I: Fundamental Theory and Applications, vol. 50, Issue 11, November 2003, 1373-1380.

[74] H. Bock, M. Bucci, R. Luzzi, „An offset-compensated oscillator based random bit source for security applications“, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '04), Lecture Notes on Computer Science, Springer-Verlag, vol. 3156, pp. 268-281, 2004.

[75] M Bucci, R. Luzzi, „A Leakage-Based Random Bit Generator with On-line Fault Detection“, Design and Diagnostics of Electronic Circuits and systems, 2006 IEEE, April 18-21, 2006, pp. 232-233

[76] M. Bucci, M. Guglielmo, R. Luzzi, A. Trifiletti, „A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors“, 14th International Workshop on Integrated Circuit and System Design, Power and Timing Modeling, Optimization and Simulation, PATMOS 2004, Santorini, Greece, September 15-17, 2004, Proceedings, vol. 3254 of Lecture Notes in Compute Science, pp. 481-490, Springer, 2004.

[77] D. May, H. L. Muller, N. P. Smart, „Random Register Renaming to Foil DPA“, in Cryptographic Hardware and Embedded Systems – CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings, vol. 2161 of Lecture Notes in Computer Science Lecture Notes in Computer Science, pp. 28-38, Springer, 2001.

[78] L. Benini, A. Galati, A. Macii, E. Macii, M. Poncino, „Energy-Efficient Data Scrambling on Memory-Processor Interfaces“, International Symposium on Low Power Electronics and Design, 2003, Seoul, Korea, August 25-27, 2003, Proceedings, pp. 26-29, ACM Press, 2003.

[79] J. D. Golic, „A New Paradigm for Key-Dependent Reversible Circuits“, Cryptographic Hardware and Embedded Systems – CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings, vol. 2779 of Lecture Notes in Computer Science, pp.98-112, Springer, 2003.

[80] R. Elbaz, L. Torres, G. Sassatelli, P. Guillemin, C. Anguille, M. Bardouillet, C. Buatois, J. B. Rigaud, „Hardware Engines for Bus Encription: A Survey of Existing Techniques“, Design, Automation and Test in Europe Conference and Exposition (DATE 2005), 7-11 March 2005, Munich, Germany, pp. 44-45, IEEE Computer Society, 2005.

[81] S. Mangard, N. Pramstaller, E. Oswald, „Successfully Attacking Masked AES Hardware Implementations“, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 157-171, 2005.

[82] K. Tiri, I. Verbauwhede, „Place and Route for Secure Standard Cell Design“, Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS'04), August 2004, Toulouse, France, pages 143-158. Kluwer Academic Publishers, August 2004.

[83] K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, I. Verbauwhede, „Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment“, Cryptographic Hardware and Embedded Systems – CHES 2005, 7th International Workshop, Edinburgh, UK, August 29-September 1, 2005, Proceedings, volume 3659 of Lecture Notes in Computer Science, pages 354-365, Springer, 2005.

[84] K. Tiri, M. Akmal, I Verbauwhede, „A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards“, Proc. IEEE 28th European Solid-State Circuit Conference (ESSCIRC'02), 2002.

[85] K. Tiri, I. Verbauwhede, „Securnig Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology“, Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, volume 2523 of Lecture Notes in Computer Science, pp. 187-197, Springer, 2003.

[86] K. Tiri, I. Verbauwhede, „A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation“, Design, Automation and Test in Europe Conference and Exposition (DATE 2004), 16-20 February, 2004, Paris, France, volume 1, pp. 246-251, IEEE Computer Society, 2004.

[87] K. Tiri, I Verbauwhede, „Secure Logic Synthesis“, Field Programmable Logic and Appliaction, 14th International Conference, FPL 2004, Leuven, Belgium, August 30-September 1, 2004, Proceedings, volume 3203 of Lecture Notes in Computer Science, pp. 1052-1056, Springer, August 2004.

[88] M. Aigner, S. Mangard, R. Menacocci, M. Olivieri, G. Scotti, A. Trifiletti, „A Novel CMOS Logic Style with Data Independent Power Consumption“, in International Symposium on Circuits and Systems (ISCAS 2005), Kobe, Japan, May 2005, Proceedings, volume 2, pages 1066-1069, IEEE 2005.

[89] A. Bystov, D. Sokolov, A. Yakovlev, A. Koelmans, „Balancing Power Signature in Secure Systems“, in 14th UK Asynchronous Forum, Newcastle, June 2003, 2003.

[90] D. Sokolov, J. Murphy, A. Bystrov, A. Yakovlev, „Design and Analysis of Dual-Rail Circuits for Security Applications“, IEEE Transactions on Computers, 54(4):449-460, April 2005. ISSN 0018-9340.

[91] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti, „Three-Phase Dual-Rail Pre-Charge Logic“, in Cryptographic Harware and Embedded Systems –CHES 2006, 8th International Workshop, Yokohama, Japan, October 2006, Proceedings, Lecture Notes in Computer Science, Springer 2006.

[92] G. E. Moore, „Cramming more components onto integrated circuits“, Electronics, volume 38, no.8, April 19, 1965.

[93] V. De, S. Borkar, „Technology and Design Challenges for Low Power & High Performance“, Intl. Symp. Low Power Electronics and Design, pp. 163-168, Aug. 1999.

[94] N. S. Kim, T. Austin, D. Baauw, T. Mudge, K. Flautner, J. S. Hu, M. J. Irwin, M. Kandemir, V. Narayanan, „Leakage current: Moore's Law meets static power“, Computer, IEEE Computer Society, vol. 36, pp. 68-75, December 2003.

[95] Y. Taur, T. H. Ning, „Fundamentals of Modern VLSI Transistors“, Cambridge University Press, 1998.

[96] N. R. Mohapatra, M. P. Desai, S. Narendra, V. R. Rao, „The effect of high-K gate dielectrics on deep submicrometer CMOS transistor and and circuit performance“, IEEE Transactions on Electron Transistors, vol. 49, pp. 826-831, May 2002.

[97] A. Ferre, J. Figueras, „Characterization of leakage power in CMOS technologies“, Proc. IEEE Int. Conf. On Electronics, Circuits and Systems, vol. 2, 1998, pp. 85-188.

[98] L. Wei, Z. Chen, M. Johnson, K. Roy, V. De, „Design and optimization of low voltage high performance dual treshold CMOS circuits“, Proc. 35th Design Automation Conf., Jun 1998, pp. 489-494

[99] A. Chandrakasan, W. Bowhill, F. Fox, „Design of High Performance Microprocessor Circuits“, Piscataway, NJ: IEEE Press, 2000.

[100] Z. Cheng, M. Johnson, L. Wei, K. Roy, „Estimation of standby leakage power in CMOS circuits considering accurate modeling of transistor stacks“, Int. Symp. On Low Power Electronics and Design, Aug. 1998, pp. 239-244.

[101] M. Johnson, D. Somasekhar, K. Roy, „Models and algorithms for bounds in CMOS circuits“, IEEE Trans. Computer-Aided Design, vol. 18, pp. 714-725, June 1999.

[102] http://www-device.eecs.berkeley.edu /~bsim3/bsim4.html.

[103] S. Bobba, I. N. Hajj, „Maximum Leakage Power Estimation for CMOS Circuits“, IEEE Alessandro Volta Memorial Workshop on Low-Power Design, pp. 116-124, 1999.

[104] L. M. Surhone, M. T. Tennoe, S. F. Henssonow, „Hamming weight“, VDM Verlag Dr. Mueller AG & Co, 2010.

[105] M. Aliotto, L. Giancane, G. Scotti, A. Trifiletti, „Leakage Power Analysis Attacks: a Novel Class of Attacks to Nanometer Cryptographic Circuits“, IEEE Transactions on Circuits and Systems – part I, vol. 57, no. 2, pp. 355-367, February 2010.

[106] R. E. Walpole, R. H. Myers, S. L. Myers, K. Ye, „Probability and Statistics for Engineers & Scientists“, Prentice Hall, 2006.

[107] R. Naiknaware, T. S. Fiez, „Automated Hierarchical CMOS Analog Circuit Stack Generation with Intramodule Connectivity and Matching Considerations“, IEEE Journal of Solid-State Circuits, vol. 34, no. 3, March 1999.

[108] M. J. Pelgrom, A. C. J. Duinmaijer, A. P. G. Welbers, „Matching Properties of MOS Transistors“, IEEE Journal of Solid-State Circuits, vol. 33, no. 1, January 1998.

[109] S. J. Lovett, M. Welten, A. Mathewson, B. Mason, „Optimizing MOS Modelling of Mismatch for Precision Analog Design“, IEEE Journal of Solid-State Circuits, vol. 21, no. 6, December 1986.

[110] B. L. Barranco, T. S. Gottaredona, „A Physical Interpretation of the Distance Term in Pelgrom's Mismatch Model results in very Efficient CAD“, IEEE International Symposium on Circuits and Systems (ISCAS), New Orleans, USA, May 2007.

[111] K. R. Lakshmikumar, R. A. Hadaway, M. A. Copeland, „Characterization and Modelling of Mismatch for Precision Analog Design“, IEEE Journal of Solid-State Circuits, vol. 21, No. 6, December 1986.

[112] D. Boning, S. Nassif, „Models of Process Variations in Device and Interconnect“, in Design of High- Performance Microprocessor Circuits, IEEE Press, 2011, pp. 98-115.

[113] K. Okada, H. Onodera, „Statistical Parameter Extraction for Intra- and Inter-Chip Variabilities of Metal-Oxide-Semiconductor Field-Effect Transistor Characteristics“, Japanese Journal of Applied Physics, vol. 44, pp. 131-134, 2005.

[114] J. M. Hammersley, D. C. Handscomb, „Monte Carlo methods“, Methuen & Co, 1975.

[115] G. S. Fishman, „Monte Carlo Concepts, Algorithms and Applications“, Springer-Verlag New York, 1999.

[116] R. Anderson, E. Biham, L. Knudsen, „Serpent: A proposal for the Advanced Encryption Standard“, National Institute of Standards and Technology, 1998.

[117] Tutorijal o OCEAN programiranju, „OCEAN Reference“, Cadence Design Systems, 2004.

[118] M. Djukanovic, L. Giancane, G. Scotti, A. Trifiletti, „Impact of Process Variations on LPA Attacks Effectiveness“, The 2nd International Conference on Computer and Electrical Engineering (ICCEE 2009), Dubai, UAE, December 2009.

[119] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti, „A Dynamic and Differential CMOS Lookup Table with Data-Independent Power Consumption for Cryptographic

Applications on Chip Cards“, IEEE Trans. on Dependable and Secure Computing, vol. 4, no. 4, December 2007.

[120] F. Mace, F. X. Standaert, I. Hassoune, J. D. Legat, J. J. Quisquater, „A Dynamic Current Mode Logic to Counteract Power Analysis Attacks“, DCIS, November 2004.

[121] L. Giancane, „Design techniques of secure IC's devices for Smart Card based cryptographic applications“, Doctoral Degree Thesis at La Sapienza University, Rome, Italy, 2010.

[122] M. Djukanovic, L. Giancane, G. Scotti, A. Trifiletti, M. Alioto, "Leakage Power Analysis Attacks: Effectiveness on DPA Resistant Logic Styles under Process Variations", 2011 IEEE International Symposium on Circuits and Systems (ISCAS2011), Rio de Janeiro, Brazil, May 2011.

DODATAK A:

1.) Matlab kod za nalaženje srednje vrijednosti struja curenja, standardne devijacije, maksimalne i minimalne vrijednosti struja curenja među rezultatima 400 MC iteracija

Primjer za NAND kolo sa ulazom 01:

```
x=load('Desktop\cmosnandFO4\A0B1.csv');
x=x(:,2);
mean_value=mean(x)%%srednja vrijednost struja curenja
standard=std(x)%%standardna devijacija
max_value=max(x)%%max vrijednost struja curenja
min_value=min(x)%%min vrijednost struja curenja
format long
```

2.) Matlab kod za grafičko prikazivanje rezultata srednje vrijednosti i standardne devijacije

Primjer za NAND kolo:

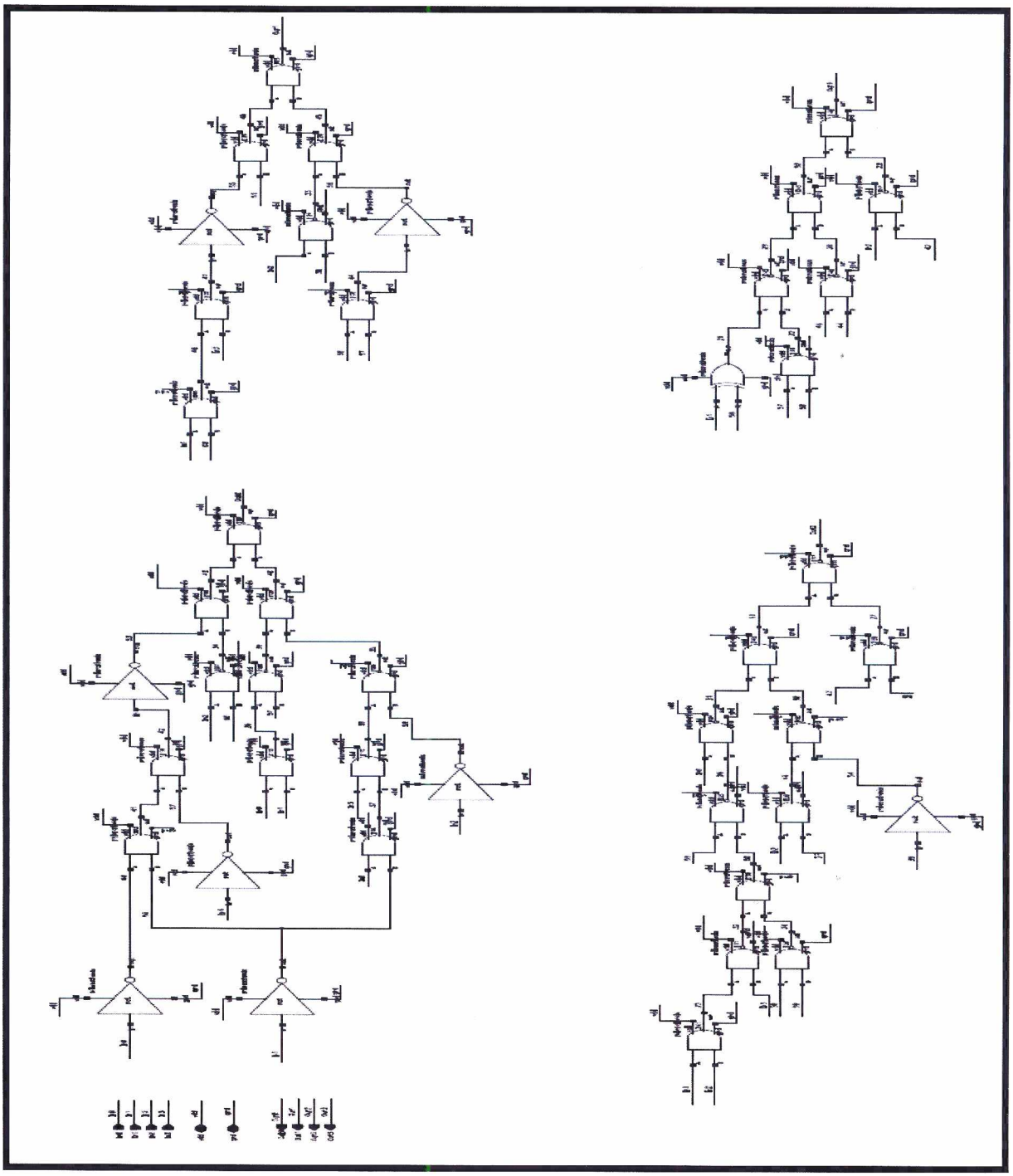
```
clc;
clear all;
close all;
media= [7.919e-9 8.724e-9 7.953e-9 1.856e-9]; %% srednja vrijednost struja curenja
sigma= [0.729e-9 1.666e-9 1.032e-9 0.725e-9]; %%standardna devijacija
M=str2num(input('U koliko tacaka? ', 's'));
for i=1:4
  I(i,:)=randn(1,M)*sigma(i)+media(i);
end
figure; hold on;
for i=1:4
  hist(I(i,:));
end
```

3.) Upotrijebljena Serpent S-kutija

Ulaz A	Ulaz B	Ulaz C	Ulaz D	Izlaz 3	Izlaz 2	Izlaz 1	Izlaz 0
0	0	0	0	0	0	1	1
0	0	0	1	1	0	0	0
0	0	1	0	1	1	1	1
0	0	1	1	0	0	0	1
0	1	0	0	1	0	1	0
0	1	0	1	0	1	1	0
0	1	1	0	0	1	0	1
0	1	1	1	1	0	1	1
1	0	0	0	1	1	1	0
1	0	0	1	1	1	0	1
1	0	1	0	0	1	0	0

1	0	1	1	0	0	1	0
1	1	0	0	0	1	1	1
1	1	0	1	0	0	0	0
1	1	1	0	1	0	0	1
1	1	1	1	1	1	0	0

4.) Struktura upotrijebljene Serpent S-kutije



5.) Programirana Ocean skripta za simuliranje struja curenja za sve ulazne vrijednosti S-kutije, odrađivanje Monte Carlo simulacija, čuvanje srednjih vrijednosti struja curenja i standardnih devijacija

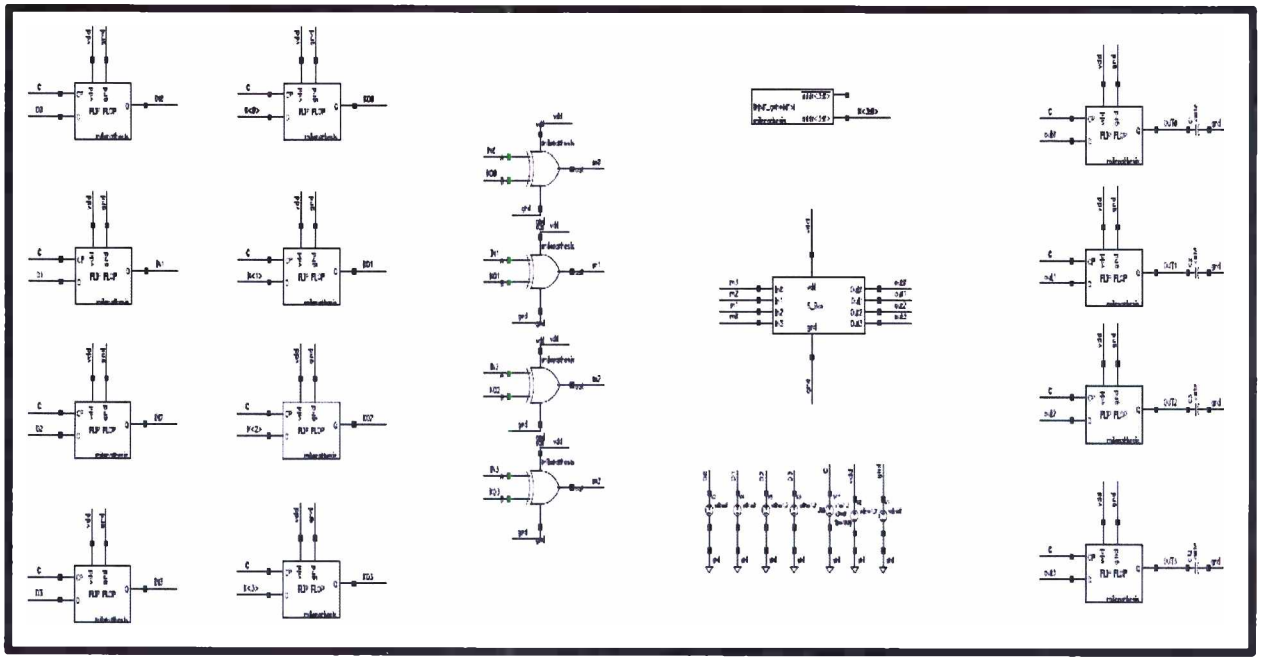
```
ocnWaveformTool( 'wavescan )
simulator( 'spectre )
design(  "/home/scard/simulation/CMOSSbox_test_new_htype/spectre/schematic/netlist/netlist")
resultsDir( "/home/scard/simulation/CMOSSbox_test_new_htype/spectre/schematic" )
definitionFile(
   "models.scs")
desVar(  "tclk" 1u )
desVar(  "del" 200n )
option( 'temp  "25.0"
          'iabstol  "1e-14"
          'vabstol  "1e-8"
          'reltol  "1e-6" )
save( 'i "/V4/PLUS" )
temp( 25.0 )
analysis('tran ?stop "1u" )
results = outfile( "/home/scard/results/SBOX_htypefinal/sbox_results.txt" "w")
MCresults = outfile( "/home/scard/results/SBOX_mc_htypefinal/sbox_mc_results.txt" "w")
monteCarlo( ?numIters "400" ?startIter "1" ?analysisVariation 'mismatch ?sweptParam "None"
?sweptParamVals "25" ?saveData t ?nomRun "yes" ?append nil)
foreach(j
'( 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 )
desVar(  "j" j     )
run()
selectResult('tran)
Int= -average(clip(i("/V4/PLUS" ?result "tran") 5e-07 1e-06))
fprintf( results "%d \t\t %3.4f \n" j Int*1e9 );
close(results)
results = outfile( "/home/scard/results/SBOX_htypefinal/sbox_results.txt" "a")
monteRun()
Imc_mean = average(-average(clip(i("/V4/PLUS" ?result "tran") 5e-07 1e-06)))
Imc_std = stddev(-average(clip(i("/V4/PLUS" ?result "tran") 5e-07 1e-06)))
fprintf( MCresults "%d \t\t %3.4f \t\t %2.3f \n" j Imc_mean*1e9 Imc_std*1e9 );
close(MCresults);
MCresults = outfile( "/home/scard/results/SBOX_mc_htypefinal/sbox_mc_results.txt" "a"))
close(MCresults)
```

6.) Sređivanje podataka o strujama curenja nakon 400 MC iteracija za svaku kombinaciju ulaznog podatka, kao i analiza uticaja ulaznog podatka na generisanje najmanje tj. najveće struje u 400 testiranih čipova

```
B=zeros(400,16)
for i=0:1
T=strcat('C:\Documents and
Settings\Administrator\Desktop\MonteCarlosim\Input',num2str(i),'.csv');
A=load(T);
```

```
B(:,i+1)=A(:,2);
end
W=zeros(16,400);
V=zeros(16,2);
for i=1:400
W(:,i)=B(i,:)';
V(:,1)=(0:15)';
V(:,2)=W(:,i);
L=strcat('C:\MATLAB6p5\work\Circuititxt\Circuit',num2str(i),'.txt');
save(L, 'V', '-ascii')
end
for i=1:400
L=strcat('C:\MATLAB6p5\work\Circuititxt\Circuit',num2str(i),'.txt');
G=load(L);
[C,D]=sort(G(:,2));
U(:,1)=D-1;
U(:,2)=C;
M=strcat('C:\MATLAB6p5\work\Nuovoctxt\Nuovoc',num2str(i),'.txt');
save(M, 'U', '-ascii')
end
F=zeros(16,16);
for k=1:16
for i=1:400
M=strcat('C:\MATLAB6p5\work\Nuovoctxt\Nuovoc',num2str(i),'.txt');
G=load(M);
for j=1:16
if G(k,1)==j-1
F(j,k)=F(j,k)+1;
end
end
end
end
X=strcat('C:\MATLAB6p5\work\Struje','.txt');
save(X, 'F', '-ascii');
X=strcat('C:\MATLAB6p5\work\Struje','.txt');
save(X, 'F', '-ascii');
Smallest=F(:,1);
Biggest=F(:,16);
Y=strcat('C:\Documents and Settings\Administrator\Desktop\Smallest','.txt');
save(Y, 'Smallest', '-ascii');
Z=strcat('C:\Documents and Settings\Administrator\Desktop\Biggest','.txt');
save(Z, 'Biggest', '-ascii');
```

7.) CMOS kriptografsko jezgro u 65nm-skoj tehnologiji



8.) CLA napad na 400 testnih uzoraka

```
B=zeros(400,16);
for i=0:15
T=strcat('C:\Documents and
Settings\Administrator\Desktop\MonteCarlosim\Input',num2str(i),'.csv');
A=load(T);
B(:,i+1)=A(:,2);
end
Ileak=B;
W=zeros(16,400);
V=zeros(16,2);
for i=1:400
W(:,i)=B(i,:)';
V(:,1)=(0:15)';
V(:,2)=W(:,i);
L=strcat('C:\MATLAB6p5\work\Circuititxt\Circuit',num2str(i),'.txt');
save(L, 'V', '-ascii')
end
key=5;
for i=1:400
 L=strcat('C:\MATLAB6p5\work\Circuititxt\Circuit',num2str(i),'.txt');
G=load(L);
for j=1:16
G(j,1)=bitxor((G(j,1)),key);
end
```

```
[C,D]=sort(G(:,1));
U(:,1)=C;
U(:,2)=G(D,2);
Leak=strcat('C:\MATLAB6p5\work\Leakagestxt\Leak',num2str(i),'.txt');
save(Leak, 'U', '-ascii')
end
Key=zeros(16,1);
for i=1:16
Key(:,1)=i-1;
Keys=strcat('C:\MATLAB6p5\work\Keystxt\Key',num2str(i-1),'.txt');
save(Keys, 'Key', '-ascii')
end
Hammweight=zeros(16,1);
KeyHamm=zeros(16,16);
for i=1:400
 L=strcat('C:\MATLAB6p5\work\Leakagestxt\Leak',num2str(i),'.txt');
M=load(L);
for k=1:16
Keyload=load(Keys);
for j=1:16
K=zeros(1,4);
K=dec2bin(bitxor(M(j,1), Keyload(j,1)),4);
count=0;
for n=1:4
if K(1,n)=='1' count=count+1;
end
end
Hammweight(j,1)=count;
end
KeyHamm(:,k)=Hammweight;
end
KeyHamming=strcat('C:\MATLAB6p5\work\Hammingstxt\Hamm',num2str(i),'.txt');
save(KeyHamming, 'KeyHamm', '-ascii')
end
Results=zeros(16,400);
for i=1:400
Res=zeros(16,1);
L=strcat('C:\MATLAB6p5\work\Leakagestxt\Leak',num2str(i),'.txt');
M=load(L);
KeyHamming=strcat('C:\MATLAB6p5\work\Hammingstxt\Hamm',num2str(k),'.txt');
KeyHamm=load(KeyHamming);
for k=1:16
correlation =abs(corrcoef(M(:,2),KeyHamm(:,k)));
Results(k,i)=correlation(1,2);
end
Res=Results(:,i);
FinalResults=strcat('C:\MATLAB6p5\work\Results\Res',num2str(i),'.txt');
save(FinalResults, 'Res', '-ascii')
end
```

```
Corr=zeros(8,400);
Corr=Results(1:8,:);
Distance=zeros(400);
for c=1:400
[M,P]=max(Corr(:,c));
CorrrCoef(c)=M;
Keyfound(c)=P-1;
if (P-1)~=key
bc=Corr(:,c);
ck=bc(key+1);
bc=sort(bc);
for i=0:7
if bc(8-i)==ck
Distance(c)=i;
end
end
end
end
Chip=[1:400];
plot(Chip, Keyfound, '*');
xlabel('Chip'); ylabel('Key');
axis([0 400 0 7]);
figure; hold on;
C=zeros(400,8);
for i=1:8
C(:,i)=(randn(400,1).*VarVal(i))+MeanVal(i);
C(:,i)=Corr(i,:)';
hist(C(:,i));
pause
end
x=[0:7];
figure; plot(x, C(:,1:8)', '.')
figure; plot(C(:,1:8), '.')
figure; hold on; xlabel('Key'); ylabel('r', 'Fontname', 'Symbol');
plot(x, C(:,1:8)', '.'); plot(x, C(135,1:8)', 'o')
figure; hold on; xlabel('Key'); ylabel('r', 'Fontname', 'Symbol');
plot(x, C(:,1:8)', '.'); plot(x, C(135,1:8)', 'o:')
countKey1=0;
for i=1:400
FinalResults=strcat('C:\MATLAB6p5\work\Results\Res',num2str(i),'.txt');
R=load(FinalResults);
if R(6,:)==max(R) countKey1=countKey1+1
end
end
countKey1
```

DODATAK B:

1.) Zavisnost struja curenja 65nm-ske CMOS S-kutije od tačnosti Hamming-ove težine ulaznih, tj. izlaznih podataka S-kutije

```
for i=1:2
   leakage_value_cmos(:,i)=load('LeakagesCMOSSBOX25.txt');
end
% 1st column of HW matrix consists of Hamming weights of Input vector for CMOS S_BOX
logic_vector_cmos(:,1)=load('HWIN_CMOSSBOX25.txt');
% 2nd column of HW matrix consists of Hamming weights of Output vector for CMOS S_BOX
logic_vector_cmos(:,2)=load('HWOUT_CMOSSBOX25.txt');
% matrix's columns are same random vectors
randvector=randperm(16);
randvector=randvector-1;
randvect=randvector';
randvectim=zeros(size (randvect));
for i=1:16
   if randvect(i)==0
      randvectim(i)=0;
   end
   if  randvect(i)==1
      randvectim(i)=1;
   end
   if  randvect(i)==2
      randvectim(i)=1;
   end
   if randvect(i)==4
      randvectim(i)=1;
   end
   if randvect(i)==8
      randvectim(i)=1;
   end
   if randvect(i)==3
      randvectim(i)=2;
   end
   if randvect(i)==5
      randvectim(i)=2;
   end
   if randvect(i)==6
      randvectim(i)=2;
   end
   if randvect(i)==9
      randvectim(i)=2;
   end
```

```
  if randvect(i)==10
    randvectim(i)=2;
  end
  if randvect(i)==12
    randvectim(i)=2;
  end
  if randvect(i)==7
    randvectim(i)=3;
  end
  if randvect(i)==11
    randvectim(i)=3;
  end
  if randvect(i)==13
    randvectim(i)=3;
  end
  if randvect(i)==14
    randvectim(i)=3;
  end
  if randvect(i)==15
    randvectim(i)=4;
  end
end

for i=1:2
  logic_vector_random_cmos(:,i)=randvectim;
end
% 1st column of this third matrix is a vector from CMOS HW Input vector in HW=1 regarding each
element
logic_vector_random_cmos_diff_one(:,1)=load('HWIN_CMOSSBOX25_diff_one.txt');
% 2nd column is a vector that is different from CMOS HW Output vector in HW=1 regarding each
element
logic_vector_random_cmos_diff_one(:,2)=load('HWOUT_CMOSSBOX25_diff_one.txt');
% calculating Pearson's correlation coefficient between leackage_value_cmos and different logic
vectors
for i=1:2
  correlation =abs(corrcoef(logic_vector_cmos(:,i), leakage_value_cmos(:,i)));
  c_cmos(i)=correlation(1,2);
end
for i=1:2
  correlation =abs(corrcoef(logic_vector_random_cmos(:,i), leakage_value_cmos(:,i)));
  c_random_cmos(i)=correlation(1,2);
end
for i=1:2
  correlation =abs(corrcoef(logic_vector_random_cmos_diff_one(:,i), leakage_value_cmos(:,i)));
  c_random_cmos_diff_one(i)=correlation(1,2);
end
plot(c_cmos,'+')
hold on
plot(c_random_cmos,'*r')
```


```
hold on
plot(c_random_cmos_diff_one,'Og')
```

2.) Rezultati struja curenja izraženi u uA za CMOS S-kutiju za 4 različite temperature, poređani od manje ka većoj vrijednosti

IN	OUT	25°[uA]	IN	OUT	50°[uA]	IN	OUT	75°[uA]	IN	OUT	100°[uA]
0001	1110	5.091	0001	1110	8.993	0001	1110	14.759	0001	1110	22.668
0011	0111	5.144	0011	0111	9.2	0000	0011	15.139	0000	0011	23.237
1001	1101	5.187	1001	1101	9.227	1001	1101	15.222	1001	1101	23.471
0000	0011	5.228	0000	0011	9.229	0011	0111	15.234	0011	0111	23.546
1110	1011	5.234	1110	1011	9.361	1110	1011	15.484	1000	1000	23.852
0100	1111	5.32	1000	1000	9.433	1000	1000	15.511	1110	1011	23.907
1000	1000	5.325	0100	1111	9.504	0100	1111	15.723	0010	1111	24.291
0010	1010	5.367	0010	1010	9.583	0010	1010	15.844	0100	1010	24.457
1111	1100	5.367u	1100	0001	9.607	1100	0001	15.893	1100	0001	24.546
1100	0001	5.375	1111	1100	9.672	1111	1100	16.096	1111	1100	24.977
1010	0110	5.498	0101	0100	9.856	0101	0100	16.309	0101	0100	25.191
0101	0100	5.51	1010	0110	9.863	1010	0110	16.353	1010	0110	25.292
1101	0010	5.523	1101	0010	9.919	1101	0010	16.459	1101	0010	25.475
0111	1001	5.59	0111	1001	10.053	0111	1001	16.692	0111	1001	25.846
1011	0000	5.645	0110	0101	10.166	0110	0101	16.86	0110	0101	26.079
0110	0101	5.661	1011	0000	10.2	1011	0000	17.008	1011	0000	26.425

3.) Rezultati struja curenja izraženi u uA za TDPL S-kutiju za 4 različite temperature, poređani od manje ka većoj vrijednosti

IN	OUT	25°[uA]	IN	OUT	50°[uA]	IN	OUT	75°[uA]	IN	OUT	100°[uA]
0011	0111	10.631	0011	0111	19.51	0011	0111	33.084	0011	0111	52.12
1110	1011	10.633	1001	1101	19.515	1001	1101	33.09	0001	1110	52.127
1001	1101	10.634	1110	1011	19.516	0001	1110	33.091	1001	1101	52.129
0110	0101	10.635	0001	1110	19.518	1110	1011	33.095	0000	0011	52.136
0010	1010	10.635	1111	1100	19.519	1111	1100	33.097	1110	1011	52.14
0111	1001	10.637	0010	1010	19.52	0000	0011	33.098	1111	1100	52.141
0001	1110	10.638	0000	0011	19.522	0010	1010	33.102	0100	1111	52.145
1010	0110	10.638	0111	1001	19.524	0100	1111	33.104	0010	1010	52.15
1111	1100	10.638	1010	0110	19.524	1000	1000	33.108	1000	1000	52.155
0000	0011	10.641	0110	0101	19.524	1010	0110	33.108	1010	0110	52.159
1011	0000	10.641	1011	0000	19.525	1011	0000	33.109	1011	0000	52.162
1000	1000	10.642	0100	1111	19.526	0111	1001	33.11	0111	1001	52.166
0100	1111	10.644	1000	1000	19.526	0110	0101	33.114	1100	0001	52.168
1100	0001	10.647	1100	0001	19.532	1100	0001	33.116	0110	0101	52.174
1101	0010	10.647	1101	0010	19.534	1101	0010	33.12	1101	0010	52.177
0101	0100	10.648	0101	0100	19.536	0101	0100	33.124	0101	0100	52.183

PODACI POTREBNI ZA DIGITALIZACIJU DOKTORSKE DISERTACIJE

Ime i prezime autora Milena Đukanović

Godina rođenja 08.06.1983.

E-mail milenadj@ac.me

Organizaciona jedinica Univerziteta Crne Gore
Elektrotehnički fakultet

Naslov doktorske disertacije

Tehnike side-channel napada na hardver pametne kartice i hardverske mjere zaštite

Prevod naslova na engleski jezik

Side-channel Attacks on Hardware of Smart Cards and Hardware Countermeasures

Datum odbrane 21. jun 2012.

Signatura u Univerzitetskoj biblioteci[1]

Naslov, sažeci, ključne riječi (priložiti dokument sa podacima potrebnim za unos doktorske disertacije u Digitalni arhiv Univerziteta Crne Gore)

Izjava o korišćenju (priložiti potpisanu izjavu)

Napomena

[1] Podatak o signaturi (lokaciji) može ispuniti biblioteka organizacione jedinice/Univerzitetska biblioteka

PODACI POTREBNI ZA UNOS DOKTORSKE DISERTACIJE U DIGITALNI ARHIV UNIVERZITETA CRNE GORE

Prevod naslova disertacije na engleski jezik

Side-channel Attacks on Hardware of Smart Cards and Hardware Countermeasures

Mentor i članovi komisija (za ocjenu i odbranu)

Mentor Prof. dr Vladan Vujičić
Komisija za ocjenu doktorske disertacije: Prof. dr Alessandro Trifiletti
Prof. dr Vladan Vujičić
Prof. dr Dejan Vukobratović

Komisija za odbranu doktorske disertacije: Prof. dr Igr Đurović
Prof. dr Vladan Vujičić
Prof. dr Alessandro Trifiletti
Prof. dr Veljko Milutinović
Prof. dr Zoran Mijanović

Sažetak*

U radu je analizirana najefikasnija klasa napada na pametne kartice u protekloj deceniji (side-channel napac koja se zasniva na slabostima u hardverskoj implementaciji algoritma i eksploatiše informacije koja "cure" kriptografskog uređaja u toku izvršavanja algoritma. Među njima najmanje proučavani napadi baziraju se analizi statičke disipacije snage i struja curenja u hardveru. Njihova aktuelnost dobija na značaju sa primjenc novih tehnologija zbog dominantnog udijela statičke disipacije snage u ukupnoj snazi disipacije, a samim tir odlučujućeg uticaja na performanse dizajna pametne kartice. Iz tog razloga izvršena je analiza implementacija nove tehnike pasivnih napada na 65nm-sko CMOS kriptografsko jezgro, koja je bazirana analizi struja curenja hardvera pametne kartice – tzv. CLA (Correlation Leakage Analysis) napad. Istraživanja obuhvatila takođe i analizu uticaja intra-die procesnih varijacija na efektivnost ovog napada. CLA napadi su pokazali izuzetno uspješnim na značajnom broju testnih uzoraka CMOS kriptografskog uređaja, čime pokazalo da CMOS tehnologija ne predstavlja dovoljno dobru mjeru zaštite protiv CLA napada.

Značajan dio rada posvećen je i analizi adekvatnih mjera zaštite u odnosu na CLA napade na hardv pametne kartice. U tom smislu, razmatrana je i veoma aktuelna hardverska mjera zaštite na tranzistorskc nivou bazirana na TDPL (Three-Phase Dual-Rail Pre-Charge Logic) logici, koja je prvobitno kreirana kao vi efikasna protivmjera napadima baziranim na analizi dinamičke disipacije snage i dinamičkih struja, tzv. DI (Differential Power Analysis) napadima. U tu svrhu je modelovan CLA napad na 65nm-sko TDPL kriptografs jezgro sa uzimanjem u obzir intra-die procesnih varijacija, a dobijeni rezultati su upoređeni sa prethod dobijenim rezultatima za CLA napad na 65nm-sko CMOS kriptografsko jezgro.

Na kraju, prikazana je i zavisnost struja curenja od implementirane tehnologije (90nm-ska i 65nm-sk tipa tranzistora (h-tip i l-tip), temperature (0°C, 25°C, 50°C, 75°C, 100°C), tipa podataka (ulazni ili izla podaci), itd. Takođe, izvršena je komparacija 65nm-ske CMOS i TDPL logike putem faktora NCD (Normaliz Current Deviation) i NSD (Normalized Standard Deviation) sa aspekta njihove efikasnosti kao mjera zaštite CLA napada.

Sažetak na engleskom (njemačkom ili francuskom) jeziku

This work analyzes the most efficient class of attacks on smart cards in the last decade (side-channel attack that is based on weaknesses in the hardware implementation of encryption modules and exploits t information that "leak" from crypto-core devices while executing the algorithm. The least studied amo them are the attacks based on analysis of static power consumption and leakage currents in the hardwa Their actuality brings on importance with the use of new technologies where static power consumption pla

major part in overall power consumption and therefore decisive influence on design performances of smi
cards. For that reason, analysis and implementation of passive attack's new technique on 65-nm CM
crypto-core, which is based on analysis of leakage currents in the hardware of smart card - so-called C
(Correlation Leakage Analysis) attack. Influence of intra-die process variations on efectiveness of this atta
has also been included in research. CLA attacks have proven to be extremely successfull on significant numb
of test samples of CMOS crypto-cores, thus proved that CMOS technology does not represent
countermeasure enough durable against CLA attacks.

Significant part of thesis is dedicated to analysis of adequate countermeasures regarding CLA attac
on smart card's hardware. In this respect, a current countermeasure at transistor level based on TDPL (Thre
Phase Dual-Rail Pre-Charge Logic) logic has been considered, originally created as a very efficie
countermeasure for attacks based on analysis of dynamic power consumption and dynamic currents, s
called DPA (Differential Power Analysis) attacks. For this purpose, a CLA attack on 65-nm TDPL crypto-core h
been modeled, with taking into account intra-die process variations. These results have been compared wi
the previously obtained results for CLA attack on 65-nm CMOS crypto-core.

Finally, dependence of leakage currents on implemented technology (90-nm and 65-nm), transist
type (h-type and l-type), temperature (0°C, 25°C, 50°C, 75°C, 100°C), data type (input or output data), etc.
presented. Also, a comparison of 65-nm CMOS and TDPL logics through factors NCD (Normalized Curre
Deviation) and NSD (Normalized Standard Deviation) was done from the aspect of their efficiency as a C
attacks' countermeasure.

Ključne riječi

Hardverska sigurnost, side-channel napadi, pametne kartice, kriptografija

Ključne riječi na engleskom jeziku

Hardware security, side-channel attacks, smart cards, cryptography

Naučna oblast/uža naučna oblast

Elektronika

Naučna oblast/uža naučna oblast na engleskom jeziku

Electronics

Ostali podaci

* Ukoliko je predviđeni prostor za polja Sažetak, Sažetak na engleskom jeziku, Ključne riječi i Ključne riječi na engleskom jeziku nedovoljan, prilož
ih u posebnom prilogu

IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku da u **Digitalni arhiv Univerziteta Crne Gore** unese doktorsku disertaciju pod naslovom

Tehnike side-channel napada na hardver pametne kartice i hardverske mjere zaštite

koja je moj autorski rad.

Doktorska disertacija, pohranjena u Digitalni arhiv Univerziteta Crne Gore, može se koristiti pod uslovima definisanim licencom Kreativne zajednice (Creative Commmons), za koju sam se odlučio/la[1].

Autorstvo
Autorstvo – bez prerada
Autorstvo – dijeliti pod istim uslovima
Autorstvo – nekomercijalno
Autorstvo – nekomercijalno – bez prerada
Autorstvo – nekomercijalno – dijeliti pod istim uslovima

Potpis doktoranda

Doc. dr M. Đurović

U

[1] Odabrati (čekirati) jednu od šest ponuđenih licenci (kratak opis licenci dat je na poleđini ovog priloga)

Autorstvo
Licenca sa najširim obimom prava korišćenja. Dozvoljavaju se prerade, umnožavanje, distribucija i javno saopštavanje djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio).

Djelo se može koristiti i u komercijalne svrhe.

Autorstvo – bez prerada
Dozvoljava se umnožavanje, distribucija i javno saopštavanje djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio). Djelo se ne može mijenjati, preoblikovati ili koristiti u drugom djelu.

Licenca dozvoljava komercijalnu upotrebu djela.

Autorstvo – dijeliti pod istim uslovima
Dozvoljava se umnožavanje, distribucija i javno saopštavanje djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio). Ukoliko se djelo mijenja, preoblikuje ili koristi u drugom djelu, prerade se moraju distribuirati pod istom ili sličnom licencom.

Ova licenca dozvoljava komercijalnu upotrebu djela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.

Autorstvo – nekomercijalno
Dozvoljavaju se prerade, umnožavanje, distribucija i javno saopštavanje djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio).

Komercijalna upotreba djela nije dozvoljena.

Autorstvo – nekomercijalno – bez prerada
Licenca kojom se u najvećoj mjeri ograničavaju prava korišćenja djela. Dozvoljava se umnožavanje, distribucija i javno saopštavanje djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio). Djelo se ne može mijenjati, preoblikovati ili koristiti u drugom djelu.

Komercijalna upotreba djela nije dozvoljena.

Autorstvo – nekomercijalno – dijeliti pod istim uslovima
Dozvoljava se umnožavanje, distribucija, javno saopštavanje i prerada djela, pod uslovom da se navede ime izvornog autora (onako kako je izvorni autor ili davalac licence odredio). Ukoliko se djelo mijenja, preoblikuje ili koristi u drugom djelu, prerada se mora distribuirati pod istom ili sličnom licencom.

Djelo i prerade se ne mogu koristiti u komercijalne svrhe.