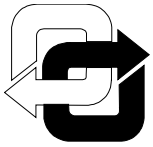
*AMETIALASEKS KASUTAMISEKS*



Küberneetika AS

# KRÜPTOKIIP PLD001

## KATSETE ARUANNE

DO-TD-X-16-0698

28 lk.

Koostas:
Jüri Põldre
Kooskõlastas:
Monika Oit

Tallinn 1998

# EESSÕNA

Käesolev katsete aruanne võtab kokku digitaalses andmesides võtmevahetuseks ning krüpteerimiseks kasutatava mikroskeemi PLD001 (edaspidi kiip) katseseeria 69075/A40110/01 testimise (24.08.1997) tulemused. Katsetuste aruanne on koostatud TTÜ Arvutitehnika Instituudis ja kooskõlastatud Küberneetika AS-i poolt

# SISUKORD

# 1. NORMATIIVVIITED

[KIIPSPETS] Krüptokiibi tehnospetsifikaat. Küberneetika AS DO-TD-X-15-1197, Red 1.

## 2. TERMINID, MÄÄRATLUSED, LÜHENDID

| | |
|---|---|
| ALU | Aritmeetika-loogikasõlm |
| IDEA | 64-bitise lähte- ning krüptotekstiga ja 128-bitise võtmega krüptoalgoritm |
| Prototüüp | Mikropskeem krüptokiibi katsepartiist (katse eksemplar) |
| SV | Sisend-väljund |

# 3. TESTIMISE KIRJELDUS

Kiibi testimiseks kasutati tehnospetsifikaadis [KIIPSPETS] ära toodud integreeritud testprogrammi ning SVM ISA liidest.
Testimine toimus Tallinna Tehikaülikoolis katseseeria iga prototüübi peal 24 augustil 1997 aastal. Testimise viisid läbi Jüri Põldre ja Ahto Buldas.
Kiibid on nummerdatud 1 kuni 20. Käesoleva katsetuste raames muudeti parameetritest ainult taktsagedust. Ülejäänud parameetrid olid keskkonna normaaltingimustel.

Testimine toimus kasutades järgnevat aparatuuri:

Testimise platvormarvuti:

| | |
|---|---|
| Protsessor: | i486DX2 |
| Taktsagedus: | 66 MHz |
| RAM: | 16 MB |
| OP-Süsteem: | WIN95 euroopa versioon |
| Tehase nr: | Microlink 005784 |

Testimise liides, liidese juhtprogramm ning kiibi testprogramm on kirjeldatud tehnospetsifikaadis.

Toiteallikas oli PC sisemine toiteplokk.

Pinge ning voolu mõõtmiseks kasutati numbrilist multimeetrit YF-3503 seerianumbriga 610.011.

Testri ja toiteploki parameetrid on nõutud piirides.

# 4. TESTIMISE TULEMUSED

Testimise kirjeldus järgib tehnospetsifikaadi p 5.2 Tabel 7 integreeritud testi alametappe.

## 4.1 KIIBI LÄHTESTAMINE

Integreeritud testi etapp 1.
Testi läbisid kõik kiibid v.a. prototüüp nr. 9. Tootmisviga on juhtautomaadis. Järgnevatel testidel prototüüpi nr. 9 ei kasutatud.

## 4.2 REGISTERMÄLU TEST

Integreeritud testi etapp 2.
Mälutestide RAM_C0, RAM_C1 ja RAM_CHKB resultaadid olid positiivsed.
Indekseeritud sisendjada mälutesti ei läbinud ükski kiip kahekümnesest partiist sõltumata töökiirusest, mida muudeti vahemikus 5 MHz kuni 34 MHz. See viitas rikkele mälu aadressdekoodris.
Väljundfaili RAM_INDX.dat (LISA A) uurides selgub, et mälupiirkonnad kattuvad poole mälu ulatuses. Seega jääb 16 pikast registrist alles 8 ning aritmeetika maksimaalne pikkus langeb 768lt 384 bitini. IDEA selle all ei kannta, kiibi registrid kattuvad aga järgnevalt:

| Register | | Kattub registriga | | | |
|---|---|---|---|---|---|
| Nr | Reg | Nr | Reg | Lo | Hi |
| 0 | Tr | 8 | PQ | P, | Q |
| 1 | T1 | 9 | PQu | Pu, | Qu |
| 2 | I0 | 10 | UL | Uu, | A5L |
| 3 | I1 | 11 | A0 | A0L, | A0H |
| 7 | Sr | 12 | A1 | A1L, | A1H |
| 5 | N | 13 | A2 | A2L, | A2H |
| 6 | M | 14 | A3 | A3L, | A3H |
| 7 | D | 15 | A4 | A4L, | A4H |

Samuti on akumulaator 768 biti asemel 384 bitine. See välistab pikkade registritega aritmeetikatehted, kuna pika registri laadimisel akumulaatorisse tekib järgmine viga:

ACCU(0..383):= R(384..767) ACCU(384..767):=R(384..767)

Pika registri kõrgem osa kopeeritakse nii akumulaatori madalamasse kui ka kõrgemasse osasse. Reaalselt akumulaatori kõrgem bitt ei tööta ja seetõttu kirjutatakse viimasena kõrgem osa, mis lugemisel antakse tagasi kaks korda.

Viga ei ole selle aruande lõpetamise ajaks veel lahendust leidnud. Selleteemaline kirjavahetus toimub praegu Europractice ja Tallinna Tehnikaülikooli vahel.

Kirjavahetuse praeguse seisuga ei ole EUROPRACTICE viga enda peale võtnud. Samuti on EPl raske seda viga meie peale suunata, kuna simuleerimisresultaadid näitavad, et kiip töötab. Kommenteeritud kirjavahetus EP ja TTU vahel on lisas (LISA B).

### 4.3 ARITMEETIKA TEST

Integreeritud testi etapid 3 kuni 7.
Kuna kogu aritmeetikatest oli algselt kirjutatud pikkade registritega, siis siinkohas pidi käsusüsteemi testi ümber kirjutama kasutades ainult lühikesti registreid.

Aritmeetikatesti lühikeste registritega läbisid kõik eelnevad testetapid läbinud prototüübid v.a. nr. 17. Tootmisviga on ALU andmevoo osas.

### 4.4 IDEA TEST

Integreeritud testi etapid 8 kuni 17.
IDEA aritmeetika ja sisend/väljundautomaadi testi läbisid kõik eelnevad testetpid läbinud kiibid.

### 4.5 MAKSIMAALSE TÖÖKIIRUSE TEST

Integreeritud testi kõik etapid.
Kiibi maksimaalset töökiirust kontrolliti kasutades liidese programeeritavat sagedusgeneraatorit. Sagedust muudeti etapiliselt vahemikus 5 MHz kuni 34 MHz. Arvutuslik maksimaalne töösagedus oli 20 MHz. Katsepartii tootmisvigadeta kiibid (kogu seeria v.a. kiibid nr. 9 ja 17) läbisid tõrgeteta integreeritud testi kuni välise sageduseni 33 MHz. Sellel sagedusel olid negatiivsed korraga nii IDEA kui ka aritmeetikatestid, mis viitasid liiga pikale viivitusele ALUs.

Reaalne töökiirus 33MHz on arvutatud töökiirusest 20 Mhz suurem. See on tingitud asjaolust, et arvutusliku mudeliga arvestasime me nn. *worst-case* parameetreid, mis eeldasid protsessi kõige halvemaid võimalikke parameetrite kõikumisi WCMIL, ehk *Worst case military.*

Vastavad parameetrid:

| | Tegelik | Simuleerimine |
|---|---|---|
| VDD: | 4.9 V | 4.5 V |
| TEMP: | 25 C | 125 C |

# 5. TESTIMISE KOKKUVÕTE

Krüptokiibi PLD001 20 eksemplarisest katsepartiist 69075/A40110/01 läbisid katsed positiivse tulemusega 18 kiipi, mis kinnitab üldiselt nende vastavust Tehnospetsifikaadi DO-TD-X-15-1997 (Red. 1) nõuetele v.a. p. 5.2. Kaks kiipi ei läbinud teste seoses juhuslike tootmisriketega.

## 5.1 KIIBI VASTAVUS FÜÜSILISTELE NÕUETELE

Katsed kinnitasid kiibi füüsiliste tingimuste ([KIIPSPETS], p. 4.2) vastavust nõetele.

## 5.2 KIIBI VASTAVUS FUNKTSIONAALSETELE NÕUETELE

Katsete käigus tuli ilmsiks kiibi registermälu rike, mille tõttu kiibi registrite plokk ja akumulaator on poole lühemad ( p.4.2 ).

## 5.3 TESTIMISAPARARUURI VASTAVUS NÕUETELE

Katseaparatuur vastas nõuetele.

## 5.4 ETTEPANEKUD

Pidada läbirääkimisi EUROPRACTICE'ga ning taodelda vea kõrvaldamist. Selleteemalised arutelud käivad (LISA B), kuid siiamaani ei ole nemad oma viga tunnistanud.

Viia läbi täiendav testimine keskkonna piirtingimustel toitepinge, taktsageduse ning temperatuuri halvimate piirtingimuste kombinatsioonil. Sellise testimine nõuab uue testliidese projekteerimist ning eriaparatuuri keskkonna parameetrite muutmiseks.

## 5.5 OTSUS

Krüptokiip PLD001 on realiseeritav (v.a. p. 5.2) ning teda võib suunata seeriatootmise ettevalmistavasse faasi.

Krptokiibi kristallis ja tarkvaras tuleb lahendada järgmised puudused:

1) Mooduli pikkus tuleb suurendada 2*768 bitini
2) IDEA teisenduse kiirus tuleb suurendada 100 Mbit/sec.
3) Tarkvara tuleb paigutada kiibi sisemisse koodimällu.
4) Lisada RS232 liides, mis võimaldab kiibi kasutamist kiipkaartide sees.
5) Lisada MAC koodi arvutamise võimalus, et testida läbiva andmevoo täielikkust.
6) Pakkida andmevoo osa tihedamalt kristallile kasutades andmevoo kompilaatorit.
7) Kasutada kiiremat tehnoloogiat.
8) Lisada sisemine juhuarvude generaator.

Krüptokiibi katsemetoodikat tuleb täiendada, lisades integreeritud testi uute funktsioonide testimise.

# LISA A Indekseeritud sisendjada testi tulemused: ram_indx.dat

```
00: Tr     -
800580048003800280018000;     800B800A8009800880078006;     80118010800F800E800D800C;
801780168015801480138012;     801D801C801B801A80198018;     802380228021802080 1F801E;
802980288027802680258024;     802F802E802D802C802B802A;
01: T1     -
900590049003900290019000;     900B900A9009900890079006;     90119010900F900E900D900C;
901790169015901490139012;     901D901C901B901A90199018;     902390229021902090 1F901E;
902990289027902690259024;     902F902E902D902C902B902A;
02: I0     -
A005A004A003A002A001A000;     A00BA00AA009A008A007A006;     A011A010A00FA00EA00DA00C;
A017A016A015A014A013A012;     A01DA01CA01BA01AA019A018;     A023A022A021A020A01FA01E;
A029A028A027A026A025A024;     A02FA02EA02DA02CA02BA02A;
03: I1     -
B005B004B003B002B001B000;     B00BB00AB009B008B007B006;     B011B010B00FB00EB00DB00C;
B017B016B015B014B013B012;     B01DB01CB01BB01AB019B018;     B023B022B021B020B01FB01E;
B029B028B027B026B025B024;     B02FB02EB02DB02CB02BB02A;
04: Sr     -
C005C004C003C002C001C000;     C00BC00AC009C008C007C006;     C011C010C00FC00EC00DC00C;
C017C016C015C014C013C012;     C01DC01CC01BC01AC019C018;     C023C022C021C020C01FC01E;
C029C028C027C026C025C024;     C02FC02EC02DC02CC02BC02A;
05: N      -
D005D004D003D002D001D000;     D00BD00AD009D008D007D006;     D011D010D00FD00ED00DD00C;
D017D016D015D014D013D012;     D01DD01CD01BD01AD019D018;     D023D022D021D020D01FD01E;
D029D028D027D026D025D024;     D02FD02ED02DD02CD02BD02A;
06: M      -
E005E004E003E002E001E000;     E00BE00AE009E008E007E006;     E011E010E00FE00EE00DE00C;
E017E016E015E014E013E012;     E01DE01CE01BE01AE019E018;     E023E022E021E020E01FE01E;
E029E028E027E026E025E024;     E02FE02EE02DE02CE02BE02A;
07: D      -
F005F004F003F002F001F000;     F00BF00AF009F008F007F006;     F011F010F00FF00EF00DF00C;
F017F016F015F014F013F012;     F01DF01CF01BF01AF019F018;     F023F022F021F020F01FF01E;
F029F028F027F026F025F024;     F02FF02EF02DF02CF02BF02A;
08: PQ     P/Q
800580048003800280018000;     800B800A8009800880078006;     80118010800F800E800D800C;
801780168015801480138012;     801D801C801B801A80198018;     802380228021802080 1F801E;
802980288027802680258024;     802F802E802D802C802B802A;
09: PQu  Pu/Qu
900590049003900290019000;     900B900A9009900890079006;     90119010900F900E900D900C;
901790169015901490139012;     901D901C901B901A90199018;     902390229021902090 1F901E;
902990289027902690259024;     902F902E902D902C902B902A;
10: Ul   Uu/A5l
A005A004A003A002A001A000;     A00BA00AA009A008A007A006;     A011A010A00FA00EA00DA00C;
A017A016A015A014A013A012;     A01DA01CA01BA01AA019A018;     A023A022A021A020A01FA01E;
A029A028A027A026A025A024;     A02FA02EA02DA02CA02BA02A;
11: A0   A0L/A0H
B005B004B003B002B001B000;     B00BB00AB009B008B007B006;     B011B010B00FB00EB00DB00C;
B017B016B015B014B013B012;     B01DB01CB01BB01AB019B018;     B023B022B021B020B01FB01E;
B029B028B027B026B025B024;     B02FB02EB02DB02CB02BB02A;
12: A1   A1L/A1H
C005C004C003C002C001C000;     C00BC00AC009C008C007C006;     C011C010C00FC00EC00DC00C;
C017C016C015C014C013C012;     C01DC01CC01BC01AC019C018;     C023C022C021C020C01FC01E;
C029C028C027C026C025C024;     C02FC02EC02DC02CC02BC02A;
13: A2   A2L/A2H
D005D004D003D002D001D000;     D00BD00AD009D008D007D006;     D011D010D00FD00ED00DD00C;
D017D016D015D014D013D012;     D01DD01CD01BD01AD019D018;     D023D022D021D020D01FD01E;
D029D028D027D026D025D024;     D02FD02ED02DD02CD02BD02A;
14: A3   A3L/A3H
E005E004E003E002E001E000;     E00BE00AE009E008E007E006;     E011E010E00FE00EE00DE00C;
E017E016E015E014E013E012;     E01DE01CE01BE01AE019E018;     E023E022E021E020E01FE01E;
E029E028E027E026E025E024;     E02FE02EE02DE02CE02BE02A;
15: A4   A4L/A4H
F005F004F003F002F001F000;     F00BF00AF009F008F007F006;     F011F010F00FF00EF00DF00C;
F017F016F015F014F013F012;     F01DF01CF01BF01AF019F018;     F023F022F021F020F01FF01E;
F029F028F027F026F025F024;     F02FF02EF02DF02CF02BF02A;
```

# LISA B Kirjavahetus EUROPRACTICE ja TTÜ vahel

Algne küsimus esitati 03.06.1997, nagu võib lugeda esimese kirja lõpus olevast suunamisest.

PLD_001_sim.doc on mälubloki testimise dokumentatsioon, mis saadeti EP. Kirja 6 lisana.

Europractice MPW protüübi tootmise kohta on informatsioon

http://www.imec.be:8000/europractice/on-line-docs/MPW/PC/MPW.P&C.TERM.html#RTFToC1

Sealt punkt number 4 ja 6.

4. Quality - Warranty
IMEC guarantee that prototypes are taken from wafers that meet the standard quality level of the foundry and have passed the parametric tests of that foundry. These parameters are within the min-max range of the technology. IMEC sends a copy of this test report together with the prototypes. IMEC can not guarantee that the prototypes will be functional. Customers should perform min-max simulations to take technology variations into account. IMEC distributes foundry information such as design rules and design kits. **IMEC can not be held responsible for malfunctioning circuits due to any faulty data in this foundry information**.

6. Liability
IMEC shall not be responsible for any direct, indirect, incidental or consequential damages the customer will suffer relating to the use of the MPW service. **IMEC is not responsible for the functional working of the prototypes.**

**Kiri 1. 05.09.97 Europractice (EP) -> TTÜ. Vastus küsimusele kiibi vea kohta**

From haddy@te.rl.ac.uk Wed Oct 15 17:53:05 1997
Date: Fri, 5 Sep 1997 11:27:25 +0100
From: Haddy's Cadence account <haddy@te.rl.ac.uk>
To: jp@pld.ttu.ee
Cc: europractice_sss@rl.ac.uk
Subject: Re: E6129 - Re: E-MAIL ENQUIRY

Dear Jyri,

I have had a look at your enquiry, and discussed with some colleagues of mine here at RAL, but nobody has reported anty problem similar to what you have discuused about. If the simulation shows everything is O.K. and LVS does not show any errors it is realy very hard to see whats going on, unless to do some detail rela-time testing as this is what your doing anyway. But if you could place a copy of your design working directoy on our anonymous ftp account, I will be glad to have a look at it.

Please place a copy of your design working directory on our anonymous ftp account, including a copy of the 'CDS.log' file.

To use the anonymous 'ftp' account (this is secure ftp account):

> ftp 130.246.17.140

> login name: anonymous

> password: your email address

> cd incoming/eurolib (Change directory into 'incoming/eurolib'.)

> binary

> put <your file>

Please leave/pick up files from here, and then inform me on what you have done.

> From epadmin@alice Fri Sep 5 08:50:49 1997
> Date: Fri, 5 Sep 97 08:50:46 BST
> X-Sender: epadmin@alice
> X-Mailer: Windows Eudora Pro Version 2.1.2
> Mime-Version: 1.0
> To: haddy@te.rl.ac.uk
> From: Jyri Poldre <jp@pld.ttu.ee> (by way of Europractice Admin <epadmin@alice>)

> Subject: E6129 - Re: E-MAIL ENQUIRY
>
> HADDY - PLEASE LOOK AT THIS - E6129 STILL SHOWS AS UNANSWERED IN OUR LOG -
> THANKS, RICHARD
>
>
>
>
> FROM: A40110
> Tallinn Technical University
> Jyri Poldre
>
> Dear Sirs.
>
> Some time ago I sent an enquiry and got back the following:
>
>
> On Thu, 3 Jul 1997, Europractice Admin wrote:
>
> > Thank you for your recent enquiry.
> >
> > DATED: 1/7/97
> > SUBJECT: ES2 MEMORY BLOCK
> > REF NO: E6129
> >
> > I confirm that this has now been forwarded to the necessary person for action.
> >
> > Yours respectfully
> >
> >
>
> But I have got no reply regarding the questiuon. I did not want to
> disturb before, putting it on summer vacation. But now already two
> months have passed. Could you please check if the letter has lost
> somewhere?
>
>
> Sincerely,
> Jyri Poldre,
> Tallinn Technical University.

Regards,
Haddy Samiy.
EUROPRACTICE Software Support Service

**Kiri 2. 05.09.97 TTÜ->EP. Kiibi kirjelduse saatmine**

From jp@jep.pld.ttu.eeWed Oct 15 18:00:04 1997
Date: Fri, 5 Sep 1997 15:48:17 +0300 (EET DST)
From: Jyri Poldre <jp@jep.pld.ttu.ee>
To: Haddy's Cadence account <haddy@te.rl.ac.uk>
Subject: Re: E6129 - Re: E-MAIL ENQUIRY

Dear Mr. Haddy Samiy,

I have started to load my design directory into
/incoming/eurolib/pld001.tar.gz

If it gets there intact in reasonable amount of time ( better idea could be to send tape via DHL :) then you should get 29866952 of zip file.
If you can open it then send me the descriptions what tests you would
like and I will write and send you these. Also If required we can send
chip and naked sample. Wa also did one taped-lid circuit.
It really is very important for me, because it is our first design and I did not except it to work as much as it did.
But then to have such a mistake.
And everything else works.
I would really like to get to the bottom of this.
If it does not require excessively much of your time.

Sincerely,

Jyri Poldre,
Tallinn Technical University.

**Kiri 3. 05.09.97 EP->TTÜ. Vastus kiibi kirjelduse saatmisele**

From haddy@te.rl.ac.ukWed Oct 15 18:01:58 1997
Date: Fri, 5 Sep 1997 14:13:47 +0100
From: Haddy's Cadence account <haddy@te.rl.ac.uk>
To: jp@pld.ttu.ee
Cc: europractice_sss@rl.ac.uk
Subject: Re: E6129 - Re: E-MAIL ENQUIRY

Dear Jyri,
I will wait for the zip file. All I will be able to look at is the possiblity thta there might have been a bug in either the Cadence software or the ES2 Design Kit which might have caused the failure of your design.

Regards,

441 919
Haddy Samiy.
EUROPRACTICE Software Support Service

**Kiri 4. 15.09.97 EP->TTÜ. Simuleerimise ja LVS (Layout versus Schematic) saatmine**

From haddy@te.rl.ac.ukWed Oct 15 18:02:38 1997
Date: Mon, 15 Sep 1997 16:26:58 +0100
From: Haddy's Cadence account <haddy@te.rl.ac.uk>
To: jp@pld.ttu.ee
Cc: europractice_sss@rl.ac.uk
Subject: Re: E6129

Dear Jyri,
I've been looking at your design, please can you provide me with the lvs run directory and simulation run directories.

To use the anonymous 'ftp' account (this is secure ftp account):

> ftp 130.246.17.140

> login name: anonymous

> password: your email address

> cd incoming/eurolib (Change directory into 'incoming/eurolib'.)

> binary

> put <your file>

Please leave/pick up files from here, and then inform me on what you have done.

**Kiri 5. 18.09.97 TTU->EP. LVS saatmine**

From jp@jep.pld.ttu.eeWed Oct 15 18:03:55 1997
Date: Thu, 18 Sep 1997 13:32:15 +0300 (EET DST)
From: Jyri Poldre <jp@jep.pld.ttu.ee>
To: Haddy's Cadence account <haddy@te.rl.ac.uk>
Subject: Re: E6129

> FROM: A40110
> Tallinn Technical University
> Jyri Poldre

On Mon, 15 Sep 1997, Haddy's Cadence account wrote:

> Dear Jyri,
> I've been looking at your design, please can you provide me with
> the lvs run directory and simulation run directories.

I started to download the lvs directory into
/incoming/eurolib/pld001_lvs.tar.gz

I have erased the simulation run directories and will rerun it. I will put the circuit into debug mode and will give to you the easiest stimuli to access RAM aadresses, what is to write into ram 0,1,.. and then read it back. If we can find out the problem with RAM128 then with great probability the short RAM8 has the same error.

Sincerely thanx for your effort,

Jyri Poldre,
Tallinn Technical University.

**Kiri 6. 18.09.97 TTU->EP. Testvektorite saatmine**

From jp@jep.pld.ttu.eeWed Oct 15 18:04:20 1997
Date: Fri, 26 Sep 1997 17:01:18 +0300 (EET DST)
From: Jyri Poldre <jp@jep.pld.ttu.ee>
To: Haddy's Cadence account <haddy@te.rl.ac.uk>
Subject: Re: E6129

On Mon, 15 Sep 1997, Haddy's Cadence account wrote:

> Dear Jyri,
> I've been looking at your design, please can you provide me with
> the lvs run directory and simulation run directories.

I have downloaded the simulation data and short documentation into

/incoming/eurolib/pld001_sim_doc.ps.gz - Packed postscript document
/incoming/eurolib/pld001_sim.tar.gz - Simulation run directory
and top level library

If anything else is required do not hesitate to contact us.

Once again, thank you for youre effort.

Jyri Poldre,
Tallinn Technical University.

**Kiri 7. 20.10.97 TTU->EP. Järelpärimine asjade arengu kohta**

Date: Mon, 20 Oct 1997 13:48:53 +0200 (EET)
From: Jyri Poldre <jp@jep.pld.ttu.ee>
To: Haddy's Cadence account <haddy@te.rl.ac.uk>
Subject: Re: E6129

> I've been looking at your design, please can you provide me with
> the lvs run directory and simulation run directories.

Dear Haddy,

did you receive these files? I sent them 26. of September and have not heard from you since then. Maybe there is something more I can do. In any case, let me know about the progress of events.

Jyri Poldre,
Tallinn Technical University.

**Kiri 8. 12.11.97 TTU->EP. Teine järelpärimine asjade arengu kohta**

Date: Wed, 12 Nov 1997 17:39:12 +0200 (EET)
From: Jyri Poldre <jp@pitsa.pldsise>
To: europractice_sss@rl.ac.uk
Subject: Lost contact with Mr. Haddy Samiy

From: Jyri Poldre
Tallinn Technical University
Europractice id: A40110

Dear Sirs,

I Discussed with Mr. Haddy Samiy about possible error in our submitted design. Now I have not received any messages from him over a month, although I have sent several mail. Could you please check if the address has changed.

Sincerely,
Jyri Poldre,
Tallinn Technical University.

**Kiri 8. 13.11.97 EP->TTU. Vastus järelpärimisele asjade arengu kohta**

Date: Thu, 13 Nov 97 13:02:26 GMT
From: Europractice Admin <epadmin@te.rl.ac.uk>
To: jp@pld.ttu.ee
Subject: E-MAIL ENQUIRY

Thank you for your recent enquiry.

DATED: 12/11/97
SUBJECT: LOST CONTACT WITH HADDY SAMIY
REF NO: E6129

I confirm that this has now been forwarded to Haddy for action.

Yours respectfully

**PLD_001_sim.doc**

Test Plan

The current test plan describes verilog simulation of ES2 RAM macroblock in IC PLD001(below IC) received from EUROPRACTICE MPW run 75. The unique device code is 9075/A40110/01.

The test uses IO state machine of IC to write 16 bit words into RAM memory and later read them back. The RAM aadress lines and IC IOs are checked for correct data. Delay back-annotation is used to get more precise results. Back-annotation is configured with maximal delays.

The comparison is carried out visually by inspecting the data lines on cWaves waweform display tool.

Test deliverables are:

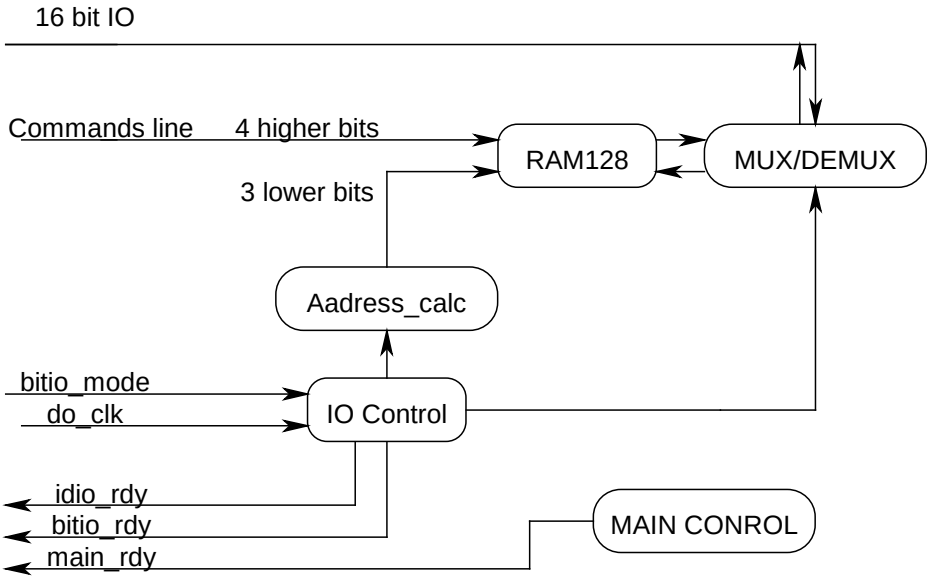
Test plan
Test design specification
Test case specification
Test summary report

Testing tasks consist of writing the verilog test program, simulating the design and interpreting the results. As simulating the design is straightforward and consists of running the simulator in batch mode it is not covered here. It is carried out though, with the result files available for inspection. If more information is needed about running simulation, the ES2 design kit maual and Cadence maual should provide the necessary information.
The simulation was carried out on SunOS 5.5 Sparcstation 20 computer with 320 Mbyte physical memory. The simulation took 100 Mb of RAM and ran 13.6 minutes. There were no events worth mentioning from testing point during this period.

Test design specification

The test must control the functionality of ES2 RAM macroblock RAM128. It is 128x96 static synchronous memory. This memory is used internally by IC for IDEA block algorithm keys storage and register file for modular calculations. The RAM block is organized into 16 registers each 8x96=768 bits wide.
IC has 3 main modes - IDEA, MODEX and IO. In IDEA mode the circuit calculates IDEA transform on input data. The keys must be present in RAM. It is possible to select the starting register and with that either decryption/encryption mode of IDEA algorithm. MODEX puts circuit into modular calculations mode, allowing user

externally run 32 internal control programs. These are selected with COMMANDS input. In IO mode it is possible to read and write internal registers directly. We will use this mode to test the memory functions.




Dwg. 1 The IO part of IC

In IO mode upper 4 bits of RAM aadress are supplied externally from commands line. The lower 3 bits of RAM and MUX/DEMUX control are generated internally depenging on bitio_mode signal, what enables us to use serial, 8-bit and 16-bit parallel IO modes.

To read/write the RAM contents it is neccesary to execute the following control flow:

1. Select IO mode
2. Commands := register number
3. To read the register use dataen := 0, to write dataen := 1
4. Pulse process trigger do_clock to enter bitio mode
5. After bitio_rdy = 1 read the 16-bit word from data bus or put the new word on data bus depending on step 3.
6. Pulse process trigger do_clk for next bitio item
7. Repeat 5 and 6 until all 16 bit data items are read/written.

The verilog program ( SIMUIT.RUN/chk_mem.v ) for it is the following:

- **Create the clock input to circuit**

```
always
 begin
 #250 RUN_CLK = 0;
 #250 RUN_CLK = 1;
 end

initial
begin
```

- **Initial values for enetring 16-bit IO mode**

```
BIST_CLK = 0;
BIST_SEL = 2'b00;
BIST_TEST = 0;                  // BIST, let it be for now
BITIO_MOD = 2'b10;        // 10 is 16 BIT IO MODE
COMMANDS = 5'b00000;            //   COMMANDS   and   also
register
                          // aadress, the high memory
                               // bits in IO mode
 IBUS=4'H0;                    // input bus initially zero
 DATAEN = 0;              // data diresction of IOBUS
 DO_CLK = 0;              // main activator
 EXT_ROM = 1;             // code ROM external,
                          // insignificant in io mode
 ID_CHNR = 1;             // IDEA channel number
 IO_RAM = 1;              //  IO  or  RAM,  used  for  ACCU
reading
 MAIN_MODE = 2'b01;              // 10 and 10 are both IO
modes
 RD_STATUS = 0;                // ROM Data direction
 RESET = 1;               // async reset
 RND_CLK = 0;                    // external rnd generator
input
 RUN = 0;                       // exit from wait mode

#1100   RESET = 0;        // exit from reset cycle

// now we will write 16 bits words into RAM registers
// using the following format   Byte nr  3   2   10
//                          Rnr 0   16 bit part in 768 bit
reg
//  0000,  0001,  ...,  0030,  1000,  1001,..,1030,  ...  F000,
F001,..F030.
```

- **Write the data to RAM**

```
DATAEN= 0;                      // write to ram

for(i=0; i<16; i=i+1) begin
@(posedge MAIN_RDY);             // wait for main ready
#100 DO_CLK = 1;                 // entrr register io mode
```

```
COMMANDS = i;              // register nr
@(posedge IDIO_RDY );           // IO state machine OK
#300 DO_CLK = 0;
@( posedge RUN_CLK );
#200  DO_CLK = 1;               // enter bitio mode
#100  DO_CLK = 0;
   for(j=0; j<((96*8)/16); j=j+1) begin
   IBUS[15:12]=i;
   IBUS[11: 0]=j;
   @( posedge BITIO_RDY );
   #100 DO_CLK=0;
   @( posedge RUN_CLK   );
   #100 DO_CLK=1;
   end
@( posedge IDIO_RDY );                    // wait for next
register IO
#100 DO_CLK = 0;
end

DATAEN = 1;                               // this changes
the bitio
                                        // direction from
write to read
```

- **Read from RAM**

```
for(i=0; i<16; i=i+1) begin
@(posedge MAIN_RDY);                      // wait for main
ready
#100 DO_CLK = 1;                         // enter register
IO mode
   COMMANDS = i;                        // register nr
@(posedge IDIO_RDY );                          //  IO  state
machine OK
#300 DO_CLK = 0;
@( posedge RUN_CLK );
#200  DO_CLK = 1;                          // enter bitio
mode
#100  DO_CLK = 0;
   for(j=0; j<((96*8)/16); j=j+1) begin
   IBUS[15:12]=i;                           //  these  are
needed for comare
   IBUS[11: 0]=j;                          // and to keep
code the same
   @( posedge BITIO_RDY );
   #100 DO_CLK=0;                          // here we have
valid output data
   @( posedge RUN_CLK );
   #100 DO_CLK=1;
   end
@( posedge IDIO_RDY );                    // wait for next
register IO
#100 DO_CLK = 0;
end

$stop;                           // stop the simulator
end
```

Test case specification

The testing top level is in PLD001_sim library.
The testing is carried out in SIMUIT.RUN directory.

The inputs to simulator are:

1. Netlist of design created by cadence verilog netlister.
2. Layout delays calculated by CDC in file top_ii.sdf.
3. Test fixture ES2testfixture.v
4. Verilog input test program chk_mem.v included from 3.
5. The list of signals to be saved in shmProbelist.
   It includes
   top level IO test.top
   RAM128 test.top.I0.U155.I0
6. Simulator control files provided by cadence and ES2.

The outputs are in waweform database and simulator log files.

To view the results waweform window should be opened. In file waves.wrf the run directory path /export/home1/admin/jp/JP_PROJETCS/… should be changed to local run directory. Then read the configuration file waves.wrf into cWaves from file->restore setup menu. The following signals are displayed:

| | |
|---|---|
| IDIO_RDY | IO state machine ready signal |
| BITIO_RDY | Bitio state machine ready signal |
| IBUS<15:0> | Input to IC |
| IOBUS<15:0> | Output from IC |
| DATAEN | IC IO direction |
| DO_CLK | IC processing trigger |
| test.top.I0.U155.I0.ADD[6:0] | RAM128 aadress |

If additional signals are required they can be selected from edit->browse display tool.

All of simulation data is contained in file simu_pld001.tar.gz It contains the top level library pld001_sim and simulation run directory SIMUIT.RUN.

Test summary report

As the visual inspection of cWawes waweform shows, the IC passes IO test. The real prototype however has only half memory active, with upper bit stuck at constant. To get the same simulation results as prototype we must disconnect RAM higher aadress bit and evaluate it to constant value. The same is also true about the second RAM block, RAM8. It is not included in this test, as it would require us to use the circuit in MODEX mode with external code rom. But as these are the only errors in design and they are similar it is highly predictable, that by solving RAM128 problem we will find solution to RAM8 also.
What makes it more interesting is the fact that we also use the fird macroblock inside the IC for code stack values. And it is error-free. The RAM_ME and read-write protocols are the same for all 3 RAM blocks.
The only difference in these memory blocks is that design crew did select the non-default configuration with RAM8 and RAM128. Due to fact that IC can run internal assembly programs to write and read from registers we did not include BIST testing for these blocks.