Zápisnica č.4 – Tím 12

Dátum a čas stretnutia: 4.11.2002 o 15:00

Miesto stretnutia: miestnosť D109

Účasť:

Vedúci tímového projektu: doc. Ing. Ladislav Hudec, CSc.

Členovia tímu: Bc. Martin Prokša
Bc. Viliam Otepka
Bc. Ivan Varga
Bc. Martin Zeman

Priebeh stretnutia:

- Zhodnotenie stavu plnenia naplánovaných úloh z predchádzajúceho týždňa.
- Rozobranie efektívnejších metód výpočtu binárneho súčtu, binárneho súčinu a inverzného binárneho súčinu.
- Odporučenie novej literatúry a materiálov týkajúcich sa šifrovania a vhodných na štúdium šifry idea .
- Boli spresnené požiadavky na Web prezentáciu šifry IDEA, týkajúce sa zahrnutia výkladu neznámych pojmov a zameranie sa na interaktivitu prezentácie s používateľom.

Plán práce:

- Martin Prokša – začať prácu na dokumentácii k projektu.
    - Dátum odovzdania: 11. novembra 2002
- Viliam Otepka, Martin Zeman – aktualizácia stránky tímu. Vytvorenie prvých dvoch úrovní prezentácie šifry IDEA.
    - Dátum odovzdania: 11. novembra 2002
- Ivan Varga – analýza algoritmov sčítania a násobenia.
    - Dátum odovzdania: 11. novembra 2002
    - Spôsob odovzdania: písomne

Stav úloh z posledného stretnutia:

- Viliam Otepka – čo najskôr upraviť web stránku aby obsahovala e-mail adresy.
    - splnené

- Viliam Otepka – Navrhnúť hrubý náčrt Web prezentácie.
    - Náčrt prezentácie bol podaný ústne ale v nedostatočnej kvalite

- Ivan Varga – vyhľadať VHDL opis šifrovacieho algoritmu na Internete ak existuje.
    - splnené

- Ivan Varga – Vyhľadať a zhodnotiť možnosti WebPack-u. Treba nájsť maximálny možný PLD obvod podporovaný WebPack-om od firmy Xilinx.
    - splnené

- Martin Zeman – príprava prezentácie IDEA algoritmu aby sme mohli podrobne špecifikovať priebeh interaktívnej Web prezentácie.
    - splnené

Vypracoval: Bc. Viliam Otepka

PRÍLOHA D

správa o hardvérových implementáciách šifrovacieho algoritmu IDEA.

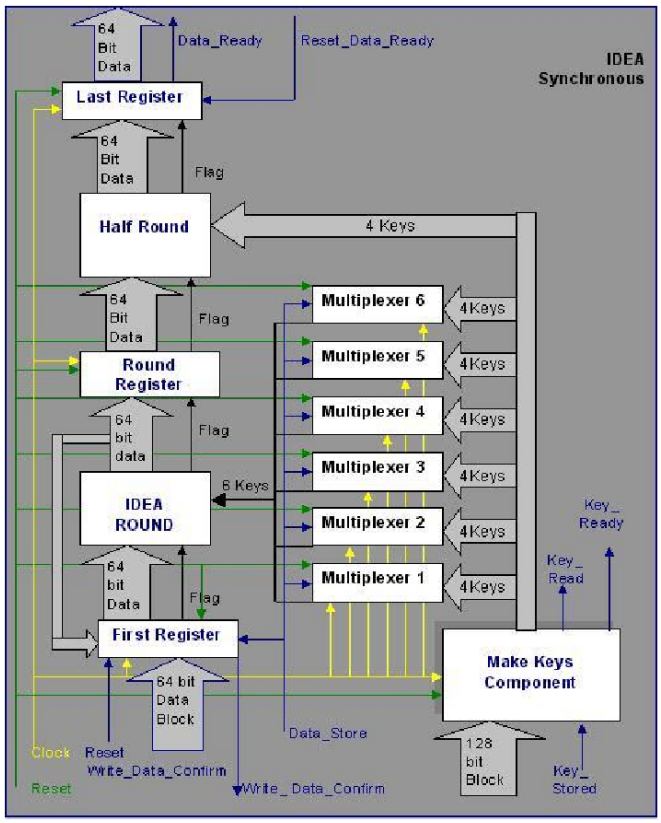
Všetky informácie vyskytujúce sa v tejto správe sú čerpané z prostredia Internetu. Podarilo sa mi nájsť tri VLSI implementácie ktoré popisuje táto dokumentácia.

AMIED - Final Project Report, Final Activity Report

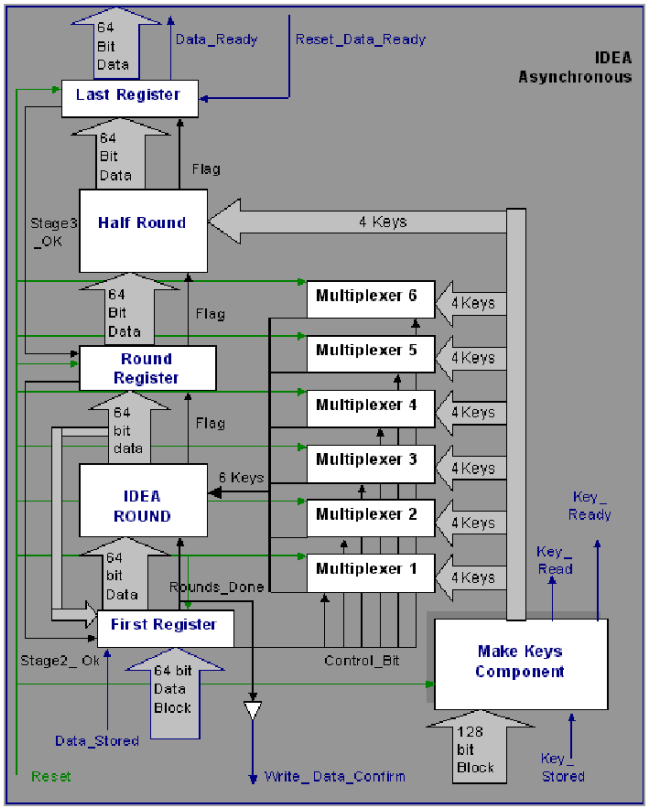
Projekt sa zaoberá synchrónnou a asynchrónnou verziou VLSI implementácie IDEA algoritmu. Celý projekt je navrhovaný a simulovaný pomocou VHDL jazyka. Výsledný produkt je syntetizovaný pomocou programu Synopsys, pričom vytvorený návrh je implementovaný na CMOS obvod vyrobený technológiou 0.6 mikrometra. Takt čipu beží na 8 MHz a napájanie je 5V. Čip sa skladá z dvoch častí. Prvou je interfejs na PCI zbernicu a druhou časťou je samotné IDEA jadro. Sú implementované dve verzie jadra:

- Asynchrónne jadro
- Synchrónne jadro

Architektúra pozostáva z 5 kôl. 4 kolá využíva IDEA algoritmus a 5. kolo je použité na výstupnú transformáciu. Na obr. 1 a 2 sú zobrazené jednotlivé implementácie.



Obr. 1 IDEA Core Block Diagram (Synchronous Version)



Obr.2 IDEA Core Block Diagram (Asynchronous Version)

Asynchrónny návrh

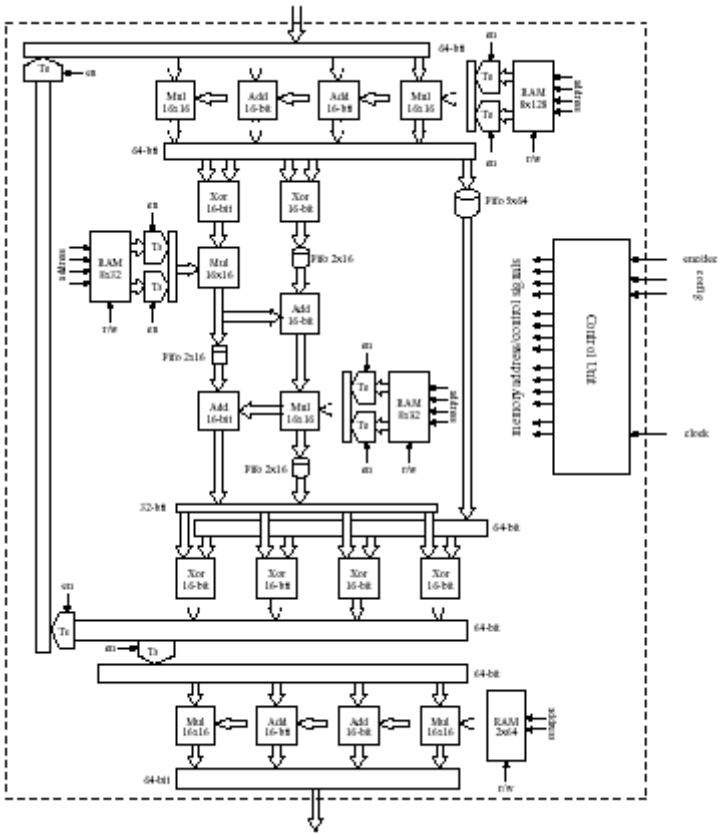
Rozdiel medzi synchrónnou a asynchrónnou verziou je, že asynchrónna verzia nemá implementované hodiny ktoré bi riadili celý proces šifrovania. Asynchrónna verzia má navrhnutý riadiaci obvod ktorý nahradzuje hodiny v synchrónnej verzii. Obvod je navrhnutý ako nedeterministický model správania bez hazardov. Veľa súbežných signálov je kontrolovaných arbitrom za účelom vyvarovania sa hazardom.

Synchrónny návrh

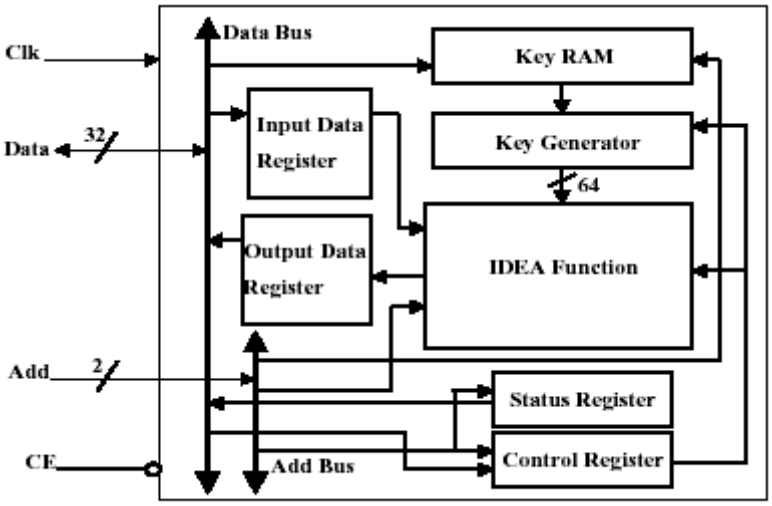
Táto verzia jadra je v oblasti návrhu a nebol ešte vytvorený prototyp.

Improved IDEA

Improved IDEA je založený na „HIPCrypto Chip“ [2] ktorého bloková schéma je na obr. 4.



Obr. 4 HIPCrypto Chip



Obr. 3 Bloková schéma IDEA čipu

Na obr. 3 je zobrazená bloková schéma čipu [3]. Jadro čipu je riešené pomocou „pipelines“ aby sa dosiahla maximálna priepustnosť šifrovania. V každej „pipeline stage“ sa inštrukcie vykonávajú nezávisle od inej „pipeline stage“.
Tento projekt je zaujímavý hlavne preto, lebo rozoberá viacero návrhov ako riešiť veľký problém v algoritme IDEA šifry. Je to problém matematickej operácie:

$$xy \bmod (2^n-1)$$

V tabuľke 1 je porovnanie 4 metód implementácie tejto matematickej operácie.

	Time Delay	Savings	Tranzistors
Special Method	81,2 ns		12910
Zimmermann	90 ns	9,8%	13694
Wrzyszcz	227,2 ns	62,3%	12396
Wang	184,8 ns	56,1%	12686

Tab. 1 Porovnanie div a mod operácií

Porovnanie rôznych implementácií:

Implementácia	MHz	Mbit/sec	efektívnosť
AMIED	5	64	12,8
High Performance IDEA Chip	8,25	66	8
HIPCrypto Chip	53	424	8
12 x Ultra-III processors	400	147,13	0,367825
Pentium III	400	28	0,07
Pentium II	450	23,53	0,052288889

Záver

Nepodarilo sa mi nájsť konkrétne implementácie či už VLSI alebo VHDL modelov šifry IDEA. Podarilo sa mi sústrediť viacero informácií ktoré by mohli viesť k efektívnejšiemu návrhu a implementácii.

Zdroje

[1] AMIED Final Project Activity Report - http://www.esdlpd.dimes.tudelft.nl/Deliverables/Public/AMIED/FinalProjectActivityReport.pdf
[2] http://www.cos.ufrj.br/~felipe/recentpapers/sbcci2000.pdf
[3] http://163.22.20.99/NTP/Thesis_Chen.pdf

Nepreskúmané zdroje

O.Y.H. Cheung, K.H. Tsoi, P.H.W. Leong, and M.P. Leong, "Tradeo®s in parallel and serial implementations of the international data encryption algorithm IDEA," *Lecture Notes in Computer Science*, vol. 2162, pp. 333–, 2001.

H. Bonnenberg, A. Curiger, N. Felber, H. Kaeslin, and X. Lai, "VLSI implementation of a new block cipher," *Proceedings of the IEEE International Confererence on Computer Design: VLSI in Computer and Processors*, pp. 501–513, 1991.

A. Curiger, H. Bonnenberg, R. Zimmermann, N. Felber, H. Kaeslin, and W. Fichtner, "VINCI: VLSI implementation of the new secret-key block cipher IDEA," *IEEE Custom Integrated Circuits Conference*, pp. 15.5.1–15.5.4, 1993.

R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner, "A 177mb/s VLSI implementation of the international data encryption algorithm," *IEEE Journal of Solid-State Circuits*, vol. 29, pp. 303–307, March 1994.

M.P. Leong, O.Y.H. Cheung, K.H. Tsoi, and P.H.W. Leong, "A bit-serial implementation of the international data encryption algorithm IDEA," *2000 IEEE Symposium on Field-Programmable Custom Computing Machines*, pp. 122 –131, 2000.

S. Wolter, H. Matz, A. Schubert, and R. Laur, "On the VLSI implementation of the international data encryption algorithm IDEA," *Proceedings of the IEEE Symposium on Circuits and Systems*, vol. 1, pp. 397–400, 1995.

S. L. C. Salomao, V. C. Alves, and E. M. C. Filho, "Hipcrypto: A high-performance VLSI cryptographic chip," *Proceedings of the Eleventh Annual IEEE ASIC Conference*, pp. 7–11, 1998.

A. V. Curiger, H. Bonnenberg, and H. Kaeslin, "Regular VLSI architectures for multiplication modulo (2*n* +1)," *IEEE Journal of Solid-State Circuits*, vol. 26, pp. 990–994, July 1991.

Výber obvodu vhodného na implementáciu IDEA algoritmu

Požiadavky

- Podpora vývojového nástroja WebPack od firmy XILINX
- Maximálna veľkosť čipu

Výsledok

Rozhodol som sa vybrať PLD čip XC95288XV z rodiny XC9500. Celá rodina čipov XC9500 je podporovaná vývojovým nástrojom WebPack a súčasne je najväčším typom z tejto rodiny.

Stručná charakteristika

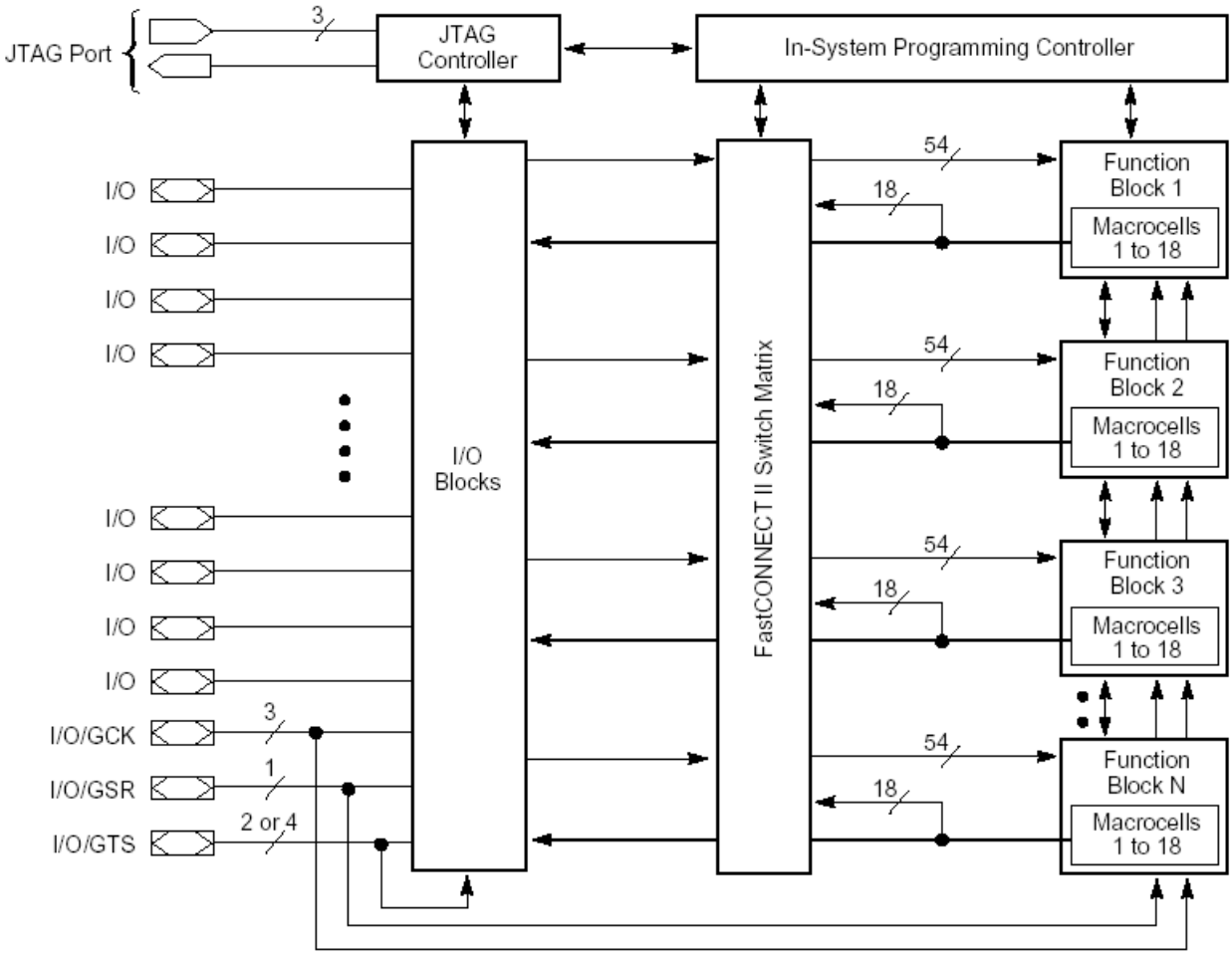
- Optimalizovaný pre vysoko výkonné 2.5V systémy
  - 3.5 ns oneskorenie pin-to-pin
  - FastFlash technológia
- In-system programmable – programovanie je možné v zapojenom obvode
- FastCONNECT II prepínacia sieť
- 54 vstupné funkčné bloky
- podpora IEEE Standard 1149.1 boundary-scan (JTAG)

Popis architektúry

Každý čip je tvorený viacnásobnými funkčnými blokmi a I/O blokmi prepojenými prepínacou sieťou typu FastCONNECT II. I/O bloky plnia funkciu vstupno výstupných registrov. Každý funkčný blok obsahuje 54 vstupov a 18 výstupov. Na Obr. 1 je bloková schéma z ktorej vychádzajú všetky verzie čipov rodiny XC9500.
Tabuľka 1 popisuje jednotlivé verzie čipov a obr. 2 zobrazuje jeden funkčný blok.

	XC9536XV	XC9572XV	XC95144XV	XC95288XV
Macrocells	36	72	144	288
Usable Gates	800	1,600	3,200	6,400
Registers	36	72	144	288
T_{PD} (ns)	3.5	4	4	5
T_{SU} (ns)	2.8	3.1	3.1	3.7
T_{CO} (ns)	1.8	2.0	2.0	2.5
f_{SYSTEM} (MHz)	278	250	250	222
Output Banks	1	1	2	4

Tab. 1 Popis verzií čipov rodiny XC9500



Obr.1 Bloková schéma XC9500 rodiny čipov

Každý funkčný blok obsahuje až 18 makrobuniek. Jedna makrobunka má konfigurovateľný D alebo flip-flop preklápací obvod s asynchrónnym set alebo reset-om.

Záver

Pre bližšie informácie o obvode je možné získať na stránkach firmy XILINX [1].

Zdroje

[1] XILINX homepage. http://www.xilinx.com