Slovenská technická univerzita
Katedra informatiky a výpočtovej techniky, Fakulta elektrotechniky a informatiky
Ilkovičova 3, 812 19 Bratislava

Tímový Projekt
PONUKA

Téma: Implementácia blokového šifrátora pomocou PLD

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

Študijný odbor: Informatika – Počítačové systémy a siete
Ročník: 1. inž.
Školský rok: 2002/2003

V dnešnej dobe patrí ochrana údajov k dôležitým faktorom informačnej spoločnosti. Jedným zo spôsob ochrany je práve šifrovanie využitím rôznych šifrovacích algoritmov. Zdokonaľovaním šifrovacích algoritmov narastá zložitosť výpočtu takéhoto algoritmu a šifrovaním veľkého množstva správ aj výrazné zaťaženie hostiteľského systému. Preto je vhodné implementovať šifrovací algoritmus hardvérovo, čím sa výrazne urýchli šifrovanie. Takýto hardvérový šifrátor je možné potom použiť nielen v počítačoch, ale aj v rôznych mobilných a komunikačných zariadeniach, v ktorých by mohlo dôjsť k odposluchu a následnému zneužitiu získaných správ.

Tím

Bc. Martin Zeman

Vyštudoval strednú priemyselnú školu elektrotechnickú, kde sa zameral na odbor elektronické počítačové systémy. Získané vedomosti z oblasti návrhu logických obvodov ďalej rozširoval v rámci absolvovaného bakalárskeho štúdia na FEI STU v Bratislave. Tu sa oboznámil s modernými metódami návrhu logických obvodov, ich testovaním a simuláciou. Získal praktické skúsenosti s návrhom a opisom logických obvodov v jazyku VHDL vo viacerých systémoch, ako ActiveVHDL, PeakVHDL, Synopsys. V rámci záverečného projektu bakalárskeho štúdia riešil projekt programovej podpory výučby jazyka VHDL. Pri riešení toho projektu získal vedomosti z návrhu a implementácie webových stránok, podrobne sa zoznámil s návrhovým systémom Synopsys v ktorom implementoval a simuloval niekoľko kombinačných aj sekvenčných obvodov.
V rámci svojich schopností chce tím výrazne podporiť pri návrhu a implementácii v jazyku VHDL a takisto chce prispieť ku kvalitnej webovej prezentácii projektu.

Bc. Ivan Varga

Vyštudoval Strednú priemyselnú školu v Trnave odbor Elektrotechnika a automatizácia. Je absolventom bakalárskeho štúdia na FEI STU v Bratislave, odbor informatika, špecializácia počítačové systémy a siete.
Počas programátorskej praxe si osvojil algoritmizáciu problémov. Má skúsenosti s prácou s kombinačnými a sekvenčnými logickými obvodmi. Svoje skúsenosti využil aj pri práci s jednočipovými mikroprocesormi. Medzi jeho produkty v oblasti hardvéru patrí napr. univerzálny programátor pamätí alebo jednočipových procesorov. V oblasti softvéru je to napr. softvér na interpretáciu jazyka HPGL na ploter za účelom vytvárania dosiek plošných spojov.
Navrhovaná úloha v tíme: hlavný návrhár a programátor

Bc. Viliam Otepka

Je absolventom bakalárskeho štúdia na FEI STU v Bratislave, odbor informatika, špecializácia počítačové systémy a siete.
Ovláda jazyky C, C++, HTML. Počas štúdia na vysokej škole sa naučil pracovať s jazykom VHDL a oboznámil sa s problematikou programovateľných logických polí v rámci predmetov špecifikačné a opisné jazyky a programovateľné obvody. Počas štúdia nadobudol skúsenosti s návrhom logických obvodov a ich testovaním. S prácou v tímoch nemá (okrem práce v škole) žiadne skúsenosti.
Svoj prínos do tímu vidí práve v svojich skúsenostiach s jazykom VHDL.
Navrhovaná úloha v tíme: dizajnér rozhraní webovej prezentácie, navrhár.

Bc. Martin Prokša

Je absolventom bakalárskeho štúdia na FEI STU v Bratislave, odbor informatika, špecializácia počítačové systémy a siete.

Počas bakalárskeho štúdia absolvoval všetky predmety súvisiace s danou témou. Má teda dobré skúsenosti s návrhom logických obvodov a ich simuláciou, jazykom VHDL.
Navrhovaná úloha v tíme: vedúci tímu.

Veľkou výhodou tímu je fakt, že sa všetci dobre poznajú, čo určite významne uľahčí komunikáciu v rámci tímu a tým pádom prispeje k vytvoreniu kvalitného projektu.

Návrh riešenia projektu

Hlavným dôvodom na výber témy bola snaha o rozšírenie vedomostí v oblasti kódovania a princípu práce šifier, rovnako aj zaujímavá problematika návrhu čo najrýchlejšej a najefektívnejšej implementácie šifrátora. V tejto téme by sme si radi vyskúšali znalosti nadobudnuté štúdiom v oblasti programovateľných logických obvodov a využili skúsenosti práce v jazyku VHDL, ktoré majú všetci členovia nášho tímu. V neposlednej rade je motiváciou vízia možnej hardvérovej implementácie a praktického využitia navrhnutého obvodu v prípade, že navrhnutý obvod bude ponúkať dostatočnú kvalitu a rýchlosť šifrovania.

Projekt bude rozdelený na viacero vývojových etáp:

1. štúdium šifrovacích algoritmov

- oboznámenie sa so všeobecnými princípmi šifrovania
- podrobné naštudovanie princípu šifrovacieho algoritmu IDEA

2. vytvorenie web prezentácie

- prezentácia vo forme aby jej porozumel aj laik - technik
- základné informácie o histórii šifrovania
- vizuálna interaktívna prezentácia algoritmu
- možnosť zadávania vstupných dát používateľom

Na vytvorenie interaktívnej prezentácie by sme chceli využiť prostredie internetu. Pre internet sme sa rozhodli z dôvodu voľnej dostupnosti z akéhokoľvek miesta, ako aj z dôvodu veľkého množstva vizualizačných techník ako napr. FLASH, DHTML, JAVA a podobne.

3. návrh štruktúry šifrátora v jazyku VHDL

- návrh s cieľom zistiť či je navrhnutý algoritmus správny
- návrh a simulácia základnej štruktúry šifrátora
- návrh s prihliadnutím na možnosti PLD obvodov
- zistenie nedostatkov
- odstránenie porúch

4. optimalizácia návrhu na rýchlosť

- zníženie počtu jednotiek
- preskúmanie možnosti využiť paralelizmus
- optimalizácia počtu cyklov vykonávania
- výber vhodného PLD

5. výsledné testovanie

- kompletné testovanie výsledného systému
- nájdenie všetkých možných chýb
- odstránenie chýb a následné kompletné znovutestovanie

Požiadavky na realizáciu projektu

Na vytvorenie webovej prezentácie:

- počítač s pripojením na Internet
- prístup na server kde umiestnime prezentáciu
- kancelársky balík Office na tvorbu dokumentácie
- dostupnosť vizualizačných technológií (FLASH, JAVA ...)

Na implementáciu šifrátora:

- softvér podporujúci VHDL napr. ActiveVHDL
- softvér na časovú simuláciu XILINX ISE WebPACK
- počítač s dostatočným výkonom, aby bolo možné s týmito softvérmi rozumne pracovať

Zoradenie tém podľa priority

Tím sa zhodol na nasledovnom poradí od najväčšej priority:

1. Implementácia blokového šifrátora pomocou PLD
2. Monitorovanie systému harmonogramu výučby
3. Simulátor jazyka VHDL

Rozvrh členov tímu:

	1 7:20	2 8:15	3 9:15	4 10:10	5 11:10	6 12:05	7 13:05	8 14:00	9 15:00	10 15:55	11 16:55	12 17:50
Pondelok			**EMK** VO IV				**RPvI** MZ MP VO IV		1. Preferovaný čas			
Utorok	**APS2** MZ MP VO IV			**EMK** VO IV			**TK** MZ MP		2. Preferovaný čas			
Streda		**OP** MP MZ				**PS3** MZ MP VO IV		**ZK** VO IV		3. Preferovaný čas		
Štvrtok	**ZK** VO IV		**ASS** MZ MP VO IV				**TČS** MP					
Piatok	**TK** MZ MP		**OP** VO IV		**PS3** MZ MP VO IV		**PS3** MZ MP VO IV		4. Preferovaný čas			

Skratky mien:

MZ – Martin Zeman
MP – Martin Prokša
IV – Ivan Varga
VO – Viliam Otepka

Skratky predmetov:

EMK – Elektromagnetická kompatibilita
RpvI – Riadenie projektov v informatike
APS2 – Architektúra počítačových systémov 2
TK – Teória kódovania
OP – Odborné praktikum
PS3 – Počítačové siete 3
ZK – Základy kryptológie
ASS – Architektúra softvérových systémov
TČS – Testovanie číslicových systémov