1 Plán projektu

Na tomto projekte pracuje tým štyroch ľudí, počas dvoch semestrov, v rozsahu približne pätiny študijného času.

II.1.1 Úlohy členov tímu

Tímový projekt je zameraný spoluprácu tímu ľudí, preto je dôležité aby si dobre rozdelili prácu medzi sebou. Po preskúmaní zadania sme sa rozhodli, že spísať potrebné funkcie, ktoré budeme v tíme potrebovať. Náš projekt sa zaoberá šifrovaním a implementáciou šifry do programovateľného obvodu, takže budeme potrebovať odborníka na šifrovanie a špecialistu na VHDL. V zimnom semestri je potrebné vytvoriť ešte interaktívnu prezentáciu šifry IDEA, z toho vyplýva potreba človeka zaoberajúceho sa návrhom tejto prezentácie vo FLASHi.

Ako každý tím potrebujeme ešte vedúceho tímu a ľudí zaoberajúcich sa web prezentáciou a dokumentáciou. Keďže náš tím pozostáva iba zo štyroch ľudí museli sme niektoré funkcie rozdeliť medzi viacej ľudí, ktorý majú aj iné povinnosti. Ďalej prinášame tabuľku z funkciami pre jednotlivých členov tímu. Jednotlivé úlohy sú pri členovi tímu zapísané v poradí podľa priority s akou ich bude vykonávať. Každý člen tímu musí písať dokumentáciu vyplývajúcu z ostatných funkcií, ktoré vykonáva.

Viliam Otepka	web prezentácia, interaktívna prezentácia vo FLASHi
Martin Prokša	vedúci tímu, dokumentácia, VHDL
Ivan Varga	VHDL, dokumentácia
Martin Zeman	špecialista na šifru, interaktívna prezentácia vo FLASHi

Tabuľka č.II.1 Rozdelenie úloh v rámci tímu

II.1.2 Plán projektu na zimný semester

- Hrubý návrh šifrátora IDEA 8 týždeň
- Dokumentácia 8 týždeň
- Odovzdanie prezentácia šifrovania pomocou algoritmu IDEA

  10 týždeň
  - Návrh prezentácie 7 týždeň
  - Prototyp prezentácie 8 týždeň
  - Overenie funkčnosti 9 týždeň

II.1.2.1 Dokumentácia

Dokumentácie analýzy problému, špecifikácie požiadaviek riešenia spolu s hrubým návrhom. Odovzdáva sa v ôsmom týždni semestra.

II.1.2.2 Hrubý návrh šifrátora IDEA

Analýza problému, špecifikácia požiadaviek a hrubý návrh riešenia. Odovzdáva sa v ôsmom týždni semestra.

II.1.2.3 Odovzdanie prezentácia šifrovania pomocou algoritmu IDEA

Vytvorenie multimediálnej prezentácie na stránku. Túto časť je potrebné odovzdať najneskôr do 12 týždňa. Ponecháme si však rezervu na prípadné pripomienky zo strany vedúceho projektu a na odladenie prípadných chýb. Okrem prezentácie vo FLASHi je ešte potrebné vytvoriť písomný opis šifry IDAE, ktorý sa umiestni na stránku tímu.

1.2.3.1 Návrh prezentácie

Prvá úloha, vytvoriť vecný a grafický návrh multimediálnej prezentácie. Vytvára ho expert na šifrovanie (Martin Zeman) v spolupráci s členom tímu zodpovedným za web prezentáciu (Viliam Otepka).

1.2.3.2 Prototyp prezentácie

Viliam Otepka predloží prvý funkčný prototyp s grafickrovne.

1.2.3.3 Overenie funkčnosti

II.1.3 Plán projektu na letný semester

11 December, 2002	týždeň
Návrh prúdového spracovania	1
Návrh super prúdového spracovania	1
Návrh opisu správania komponentov	2
Implementácia opisu komponentov opisu správania	3
Implementácia šifry IDEA – opis správania	4
Simulácia opisu správania sa	6
Syntéza opisu správania sa	6
Návrh komponentov v opise štruktúry	8
Implementácia komponentov v opise štruktúry	9
Implementácia šifry IDEA – opis štruktúry	10
Simulácia opis štruktúry	11
Syntéza opis štruktúry	11

II.1.3.1 Návrh prúdového spracovania

Rozobratie závislostí v rámci šifrátora a určenie prirodzených blokov vhodných na implementáciu pomocou prúdového spracovania. (Kroky šifry)

Riešenia tejto úlohy sa zúčastnia všetci.

Dokončenie 1 týždeň.

II.1.3.2 Návrh super prúdového spracovania

Navrhnutie prúdového prúdového spracovania v rámci blokov krokov šifry.

Riešenia tejto úlohy sa zúčastnia všetci.

Dokončenie 1 týždeň.

II.1.3.3 Návrh opisu správania komponentov šifrátora IDEA

Návrh komponentov nachádzajúcich sa v šifrátore IDEA.

16 bit xor
16 bit sčítačka
16 bit násobička
Inverzné násobenie
Manažment kľúčov
krok
výstupná transformácia

Je potrebné urobiť návrh komponentov nachádzajúcich sa v systéme. Opis správania bude slúžiť ako referencia pri optimalizácii opisom štruktúry.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

Dokončenie 2 týždeň.

II.1.3.4 Implementácia opisu komponentov opisu správania

Implementácia opisu správania sa v jazyku VHDL. Implementácia je nezávislá od zvoleného prostriedku simulácie.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

Dokončenie 3 týždeň.

II.1.3.5 Implementácia šifry IDEA – opis správania

Aplikovanie výsledkov z predchádzajúcich krokov. Výsledkom bude funkčný prototyp šifrátora, od neho sa budú odvádzať optimalizované verzie.

Riešenia tejto úlohy: Martin Prokša

Dokončenie 4 týždeň.

II.1.3.6 Simulácia opisu správania sa

Testovanie opisu správania sa zo stránky správnosti výsledkov, ako aj skúmanie častí projektu potrebných urýchliť.

Riešenia tejto úlohy: Martin Zeman, Viliam Otepka

Dokončenie 6 týždeň.

II.1.3.7 Syntéza opisu správania sa

Skúmanie možnosti syntézy do programovateľného obvodu a možnosti urýchlenia. Prebieha súbežne so simuláciou.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

Dokončenie 6 týždeň.

II.1.3.8 Návrh komponentov v opise štruktúry

Časti systému, ktoré vývojový prostriedok nieje schopný optimálne syntetizovať, sa navrhnú v opise správania sa.

Riešenia tejto úlohy: všetci

Dokončenie 8 týždeň.

II.1.3.9 Implementácia komponentov v opise štruktúry

Časti systému, ktoré vývojový prostriedok nieje schopný optimálne syntetizovať, sa navrhnú v opise správania sa.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

Dokončenie 9 týždeň.

II.1.3.10 Implementácia šifry IDEA – opis štruktúry

Aplikovanie výsledkov z predchádzajúcich krokov. Výsledkom bude funkčný prototyp šifrátora, od neho sa budú odvádzať optimalizované verzie.

Riešenia tejto úlohy: Martin Prokša

Dokončenie 10 týždeň.

II.1.3.11 Simulácia opis štruktúry

Testovanie sa zo strany správnosti výsledkov, ako aj skúmanie častí projektu potrebných urýchliť.

Riešenia tejto úlohy: Martin Zeman, Viliam Otepka

Dokončenie 11 týždeň.

II.1.3.12 Syntéza opis štruktúry

Skúmanie možnosti syntézy daného opisu správania sa do programovateľného obvodu a možnosti urýchlenia. Prebieha súbežne so simuláciou.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

Dokončenie 11 týždeň.

II.1.4 Plán projektu na letný semester

3. marec 2003	týždeň
Návrh komponentov v opise štruktúry	1
Návrh super prúdového spracovania	3
Implementácia komponentov	4
Implementácia šifry IDEA	5
Simulácia	6
Syntéza	7
Implementácia dešifrovacích kľúčov	8
BIST - Návrh a implementácia Samotestovateľného obvodu	9
Optimalizácia celej štruktúry	10

II.1.4.1 Návrh komponentov v opise štruktúry

Návrh komponentov nachádzajúcich sa v šifrátore IDEA.

16 bit xor
16 bit sčítačka
16 bit násobička
Inverzné násobenie
Manažment kľúčov
krok
výstupná transformácia

Je potrebné urobiť návrh komponentov nachádzajúcich sa v systéme. Opis správania bude slúžiť ako referencia pri optimalizácii opisom štruktúry.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

II.1.4.2 Návrh super prúdového spracovania

Rozobratie závislostí v rámci šifrátora a určenie prirodzených blokov vhodných na implementáciu pomocou prúdového spracovania. (Kroky šifry)

Riešenia tejto úlohy sa zúčastnia všetci.

II.1.4.3 Implementácia komponentov

Implementácia opisu správania sa v jazyku VHDL. Implementácia je nezávislá od zvoleného prostriedku syntézy.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

II.1.4.4 Implementácia šifry IDEA

Aplikovanie výsledkov z predchádzajúcich krokov. Výsledkom bude funkčný prototyp šifrátora, od neho sa budú odvádzať optimalizované verzie.

Riešenia tejto úlohy: Martin Prokša

II.1.4.5 Simulácia

Testovanie opisu správania sa zo stránky správnosti výsledkov, ako aj skúmanie častí projektu potrebných urýchliť.

Riešenia tejto úlohy: Martin Zeman, Viliam Otepka

II.1.4.6 Syntéza

Skúmanie možnosti syntézy do programovateľného obvodu a možnosti urýchlenia. Prebieha súbežne so simuláciou.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

II.1.4.7 Implementácia dešifrovacích kľúčov

Implementácia opisom správania sa komponentov (inverzné sčítanie a násobenie) a celej štruktúry distribúcie kľúčov.

Riešenia tejto úlohy: Martin Zeman, Martin Prokša

II.1.4.8 BIST - Návrh a implementácia Samotestovateľného obvodu

Samočinná testovateľnosť.

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

II.1.4.9 Optimalizácia celej štruktúry

Riešenia tejto úlohy: Martin Prokša, Ivan Varga

II.1.5 Plán na letný semester

14. apríl 2003

	týždeň
Návrh komponentov v opise štruktúry	1
Návrh super prúdového spracovania	3
Implementácia komponentov	4
Implementácia šifry IDEA	5
Simulácia	6
Syntéza	7
Implementácia dešifrovacích kľúčov	8
BIST - Návrh a implementácia Samotestovateľného obvodu	10
Optimalizácia celej štruktúry	10