

Zápisnica č.14 - Tím 12

Dátum a čas stretnutia: 17.3.2003 o 14:30

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:

- Martin Prokša a Ivan Varga informovali o postupe prác v implementácii kôl šifrátoru. Jeho prvotný opis je funkčný a momentálnym cieľom je optimalizovať štruktúru násobičky, tak aby bola ľahšie syntetizovať. Ako východisko sa javí použiť kolo s tromi alebo piatimi stupňami.
- Martin Zeman popísal stav riešenia implementácie deličky potrebnej na funkciu inverzného násobenia z managementu dešifrovacích kľúčov. Delička je navrhnutá na 64 taktov čo je vzhľadom na počet jej použití nepripustne veľa.
- Viliam Otepka informoval o oprave vytíkaných chýb z prezentácie

Plán práce:

- Ivan Varga, Martin Prokša - Testovanie implementácie celého šifrátoru a časová analýza náročnosti implementovanej násobičky
 - Dátum odovzdania: 24. marca 2003
 - Spôsob odovzdania: VHDL kód
- Martin Zeman – Implementácia deličky
 - Dátum odovzdania: 24. marca 2003
 - Spôsob odovzdania: VHDL kód
- Viliam Otepka – aktualizácia WEB stránky
 - Dátum odovzdania: 24.marca 2003
 - Spôsob odovzdania: web

Stav úloh z posledného stretnutia:

- Martin Prokša, Ivan Varga – Implementácia super prúdového prostriedku na šifrovanie
 - splnené
- Viliam Otepka – aktualizácia WEB stránky
 - Splnené
- Martin Zeman – návrh deličky pre manažment dešifrovacích kľúčov
 - splnené

Vypracoval: Bc.Martin Prokša