Používateľská príručka programu IdeaTest

Účel programu

Pri návrhu a vytváraní opisu šifrátora Idea, vznikla potreba priebežne testovať jednotlivé verzie implementácie. Na otestovanie činnosti šifrátora, ktorého správanie je opísané pomocou jazyka VHDL, sa používa tzv. „testbench“. Tento testbench je rovnako ako celý opis správania šifrátora, zapísaný pomocou jazyka VHDL a jeho účelom je na zadané vstupy šifrátora posielať testovacie dátové vzorky pri zvolenom časovaní a prípadné porovnávanie výsledkov spracovania.

S postupom vývoja a zmien vytváraných v šifrátore bolo nutné rovnako meniť aj hodnoty a štruktúru testu ako aj v niektorých prípadoch zväčšiť počet vzoriek v teste aby bolo možné odskúšat šifrátor počas dlhšej periódy. V týchto podmienkach by bolo časovo náročné ručne prepisovať testovací súbor najmä v prípade potreby väčšieho množsva vzoriek. Z tohto dôvodu vznikla potreba automatizovať proces generovania testovacieho súboru s kódom VHDL podla meniacich sa požiadaviek na časovanie, počet vzoriek a meniacu sa štruktúru testu. Výsledkom snahy o zjednodušenie tohto procesu je program IdeaTest, ktorý zjednodušuje generovanie testov pri uvedených podmienkach.

Činnosť programu

Ako sme uviedli vyššie cielom programu bolo cielom nielen zmenu hodnôt a počtu vzoriek ale aj umožniť vykonať zmeny v štruktúre testovacieho súboru bez nutnosti upraviť program na generovanie testov. Za týmto účelom program na svoju činnosť využíva vzorový súbor s testom. Tento súbor má pevne určené meno *ideatb_vzor* a musí byť pre správnu činnosť programu umiestnený v rovnakom adresáry ak samotný program.

Súbor ideatb_vzor je, upravený súbor s testom pre šifrátor. Úprava súboru spočíva v pridaní špeciálnych sekvencií znakov v miestach na ktoré budú zapísané zadané hodnoty programu IdeaTest. Program rozoznáva nasledujúce špeciálne sekvencie znakov:

- ##clk1## - používaná ako čas nábežnej hrany
- ##clk0## - používaná ako čas dobežnej hrany
- ##zaccas## - používaná ako čas zadania prvej vzorky
- ##rep## - symbol opakovania od miesta značky po koniec riadku, pričom program ukončuje všetky riadky čiarkou a poslednú bodkočiarkou
- ##x1## až ##x4## - nahrádza 64 bitovou hodnotou vygenerovanej vsupnej vzorky, rozdelenej na štyri 16 bitové bloky, zapísanej v binárnej sústave
- ##y1## až ##y4## - nahrádza 64 bitovou hodnotou vypočítanej zašifrovanej vzorky, rozdelenej na štyri 16 bitové bloky, zapísanej v binárnej sústave
- ##index## - používa sa v spojení so značkou opakovania a je nahrádzaný číslom iterácie opakovania
- ##inkey## - je nahradený 128 bitovým šifrovacím kľúčom zapísaným v binárnom tvare

Pri potrebe zmeny štruktúry testovacieho súboru je teda možné zmeniť vzorový súbor programu a tým dosiahnuť generovanie nových testovacích súborov bez nutnosti zmeny programu IdeaTest.

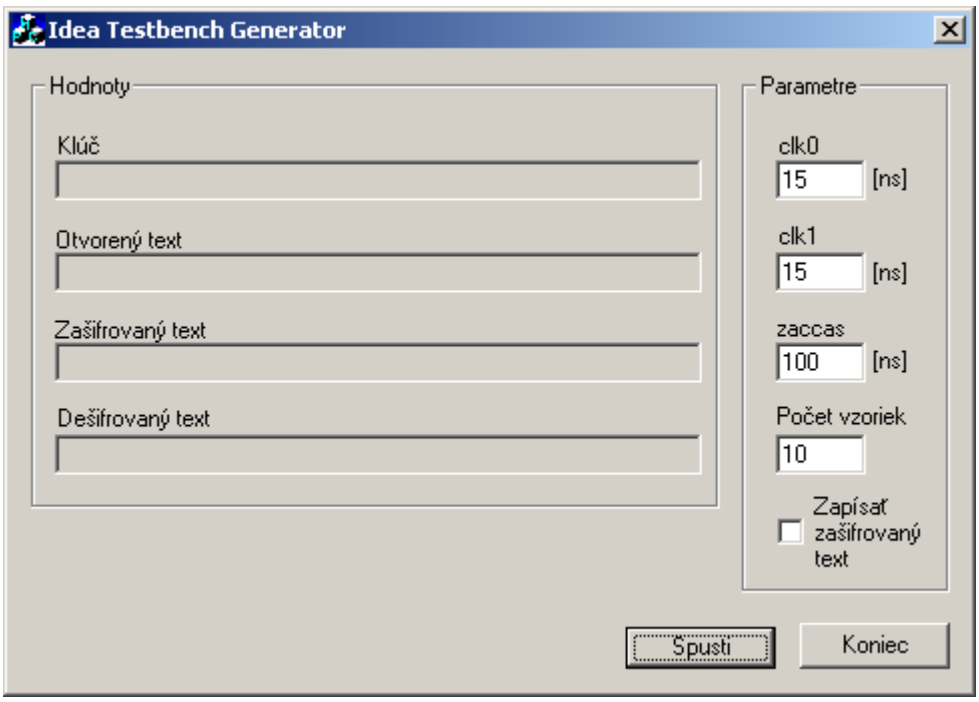
Pri výpočte zašifrovaných hodnôt je z dôvodu overenia správnosti šifrovania vzorky najskôr vygenerovaná hodnota testovacej vzorky vstupného testu zašifrovaná a následne dešifrovaná táto hodnota je porovnaná s pôvodnou vygenerovanou hodnotou a program pokrčuje iba v prípade, že sú tieto hodnoty rovnaké.

Prostredie programu

Program je dialógová aplikácia ktorá je rozdelená na dve časti. V pravej časti – parametre program umožnuje zadávať vstupné hodnoty ktoré budú vkladané do testovacieho súboru. Konkrétne sú to hodnoty:

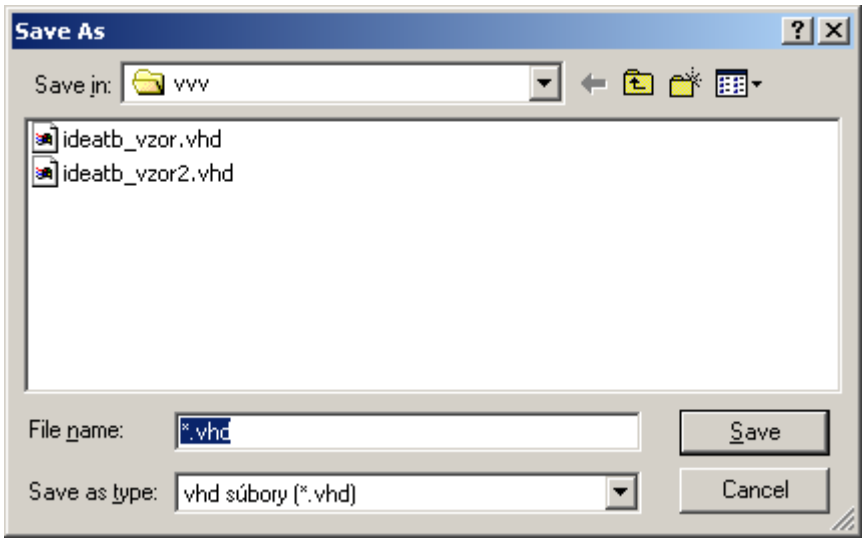
- clk0 – nahrádza hodnotou značku ##clk0##
- clk1 – nahrádza hodnotou značku ##clk1##
- zaccas – nahrádza hodnotou značku ##zaccas##
- pocet vzoriek – určuje počet vygenerovaných testovacích vzoriek
- zapísať zašifrovaný text – po povolení tejto volby sú do súboru zapísané aj zašifrované vzorky pre jednoduché porovnávanie výsledkov zo šifrátora.

V ľavej časti – hodnoty, sa zobrazujú generované vzorky spolu so zodpovedajúcimi zašifrovanými a opätovne dešifrovanými hodnotami a hodnotou kľúča. Obr. 1.



Obr. 1. Okno programu IdeaTest.

V dolnej časti okna sa nachádzajú tlačítka pre ukončenie programu a spustenie generovania testovacieho súboru. Po spustení generovania sa otvorí dialógové okno ktoré umožnuje zadať miesto a názov nového vygenerovaného testovacieho súboru, (obr. 2). Po potvrdení výberu je súbor vygenerovaný a program zobrazí hlásenie o uspešnom vytvorení testovacieho súboru.



Obr. 2. určenie miesta a názvu nového súboru.