

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Analýza výkonu řešiče systému generálního klíče a hlavních klíčů
Jméno autora:	Martin Hořeňovský
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	RNDr. Jiří Vyskočil Ph.D.
Pracoviště oponenta práce:	CIIRC ČVUT

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	náročnější
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
Vzhledem k tomu, že tato diplomová práce má za úkol analyzovat a vylepšit současnou implementaci řešiče systému generálního klíče a hlavních klíčů, která je na Katedře počítačů vyvíjena týmem pedagogů a studentů s nezanedbatelnými úspěchy již několik posledních let, považuji zadání práce za náročnější až mimořádně náročné.	

Splnění zadání	splněno
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.</i>	
Zadání práce bylo splněno ve všech bodech.	

Zvolený postup řešení	správný
<i>Posuďte, zda student zvolil správný postup nebo metody řešení.</i>	
Zvolený postup řešení pokládám za správný.	

Odborná úroveň	A - výborně
<i>Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.</i>	
Odborná úroveň práce je výborná a zcela naplnila moje očekávání jako oponenta.	

Formální a jazyková úroveň, rozsah práce	B - velmi dobře
<i>Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.</i>	
Práce byla vypracována v anglickém jazyce s vysokou jazykovou úrovní, je celkově dobře čitelná a svým rozsahem plně odpovídá požadavkům, které jsou kladeny na diplomovou práci. Nicméně lze zde nalézt i několik překlepů a na některých místech se velmi zřídka objevují i chybějící určité a neurčité členy a další drobné jazykové nepřesnosti. K formální úrovni práce mám pouze jedinou výhradu, která se týká definic funkcí na stranách 8 a 10. Funkce se totiž v matematice obvykle definují jako zobrazení z množiny pro definiční obor do množiny pro obor hodnot. Rovněž je možné definovat funkce explicitním vyjádřením, implicitně, parametricky, grafem, atd., ale kombinace, kde je definiční obor popsán množinou a obor hodnot je popsán nějakou generickou hodnotou, pokládám za velmi matoucí.	

Výběr zdrojů, korektnost citací	A - výborně
<i>Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.</i>	
Výběr zdrojů považuji za vhodný a relevantní. Citace jsou v práci korektně provedeny. Původní myšlenky jsou v práci dobře rozlišitelné.	

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

V úvodu se diplomová práce se zabývá popisem problému hledání řešení systému generálního klíče a hlavních klíčů. Rád bych zde zmínil, že tento velmi konkrétní kombinatorický a optimalizační problém je na Katedře počítačů intenzivně řešen několik posledních let se signifikantními výsledky.

Dále práce popisuje současný stav poznání na tomto projektu/problému a navrhuje možná vylepšení v několika následujících oblastech:

1. Popisuje a analyzuje stávající a nové způsoby zakódování problému do CNF (konjunktivně normální formy), kterou pak následně zpracovává SAT řešič.
2. Zavádí metodu pro „náповědu“ SAT řešičům, která využívá určitých specifických doménových znalostí problému.
3. Navrhuje možnosti vylepšení paměťové a časové náročnosti tzv. kompilátoru (programu, který převádí původní problém na SAT)
4. Srovnává výkon na několika nejlepších dostupných SAT řešičích a navrhuje jejich možná vylepšení.

Za hlavní výsledek práce považuji vyřešení dvou rozsáhlých a doposud nevyřešených instancí problému v cca. 10 minutách běhu systému.

I přes poměrně náročné zadání přinesla tato diplomové práce nové směry a podněty pro další možná vylepšení a rozšíření současného stavu poznání o problému řešení systému generálního klíče a hlavních klíčů.

Otázky: Na straně 35 2. odstavec 2. věta se píše, že veškerá náhodnost uvnitř SAT řešičů byla vypnuta pro zachování opakovatelnosti výsledků. Toto tvrzení je poměrně nepřesné a zavádějící. Znamená to, že při startu každého SAT řešiče bylo zafixováno náhodné semínko (random seed)? Pokud ano, jak? Nebo byl snad úplně vypnut generátor náhodných čísel, který některé SAT řešiče s výhodou využívají?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně**.

Datum: 24.1.2018

Podpis: