VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Informace o obhajobě doktorské disertační práce

Ing. Jakub Husa z Ústavu počítačových systémů Fakulty informačních technologií ve čtvrtek 31.10.2024 úspěšně obhájil svoji disertační práci.

Studijní program: Výpočetní technika a informatika

Název práce: Evoluce kryptograficky spolehlivých booleovských funkcí/ Evolution of cryptographically sound Boolean functions

Abstrakt/ Abstract:

Tato práce se zaměřuje na jeden ze dvou hlavních způsobů návrhu booleovských funkcí, obecně na heuristické vyhledávání pomocí evolučních algoritmů a konkrétně na genetické programování. Nejprve ukazuje, že tuto úlohu je možné snadno paralelizovat na více procesorech pomocí ostrovního modelu i modelu zaměstnavatel-pracovník. Dále zkoumá několik variant genetického programování (stromové, kartézské a lineární), aby ukázala, že jsou pro řešení této úlohy vhodnější než ostatní typy evolučních algoritmů, a že všechny tři tyto varianty jsou konkurenceschopné. Žádná z nich není striktně lepší než ostatní a její ideální výběr závisí na tom, jaká konkrétní podmnožina kryptografických vlastností je od navrhované funkce vyžadována. Pro ověření správnosti těchto závěrů byl proveden návrh několika typů jedno-výstupových kryptograficky spolehlivých booleovských funkcí, s využitím v proudových šifrách, a maskovacích funkcí, poskytujících ochranu proti útokům postranními kanály. Závěrem práce také ukazuje, že evoluční návrh booleovských funkcí lze zkombinovat s metodami z druhého hlavního způsobu jejich návrhu, známými jako algebraické konstrukce. Za tímto účelem byl navržen nový, sémantický genetický operátor mutace pro návrh jednoho konkrétního typu booleovských funkcí, známých jako ohnuté funkce, který vedl k masivnímu zlepšení efektivity jejich návrhu./ This thesis focuses on one of two main approaches to designing Boolean functions a heuristic search via evolutionary algorithms, in general, and genetic programming, in particular. First, it shows that the task can be easily parallelized on multiple processors, via an island or employer-worker model. Next, it examines multiple variants of genetic programming (tree-based, Cartesian, and linear), to show that they are more suitable for this task than other types of evolutionary algorithms and that all three of these variants are competitive. None of them is strictly better than the others, and the ideal choice depends on the specific subset of required properties. To verify these observations we design multiple types of single-output cryptographically sound Boolean functions, usable in stream ciphers, and masking functions useful for defense against side-channel attacks. Lastly, the thesis shows that the evolutionary design of Boolean functions can be combined with the other main design approach, known as algebraic construction. To do this, we propose a new semantic genetic mutation operator for the design of one specific type of Boolean

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Božetěchova 2, 612 66 Brno
tel.: +420-5-4114 1139, fax: +420-5-4114 1270, http://www.fit.vut.cz

Informace o obhajobě doktorské disertační práce

functions, known as bent functions, which resulted in a massive improvement in the efficiency of the design process.

Školitel: prof. Ing. Lukáš Sekanina, Ph.D., FIT VUT

Oponenti: prof. Domagoj Jakobović, Faculty og electrical engineering and computing, Zagreb, Croatia

prof. Ing. Pavol Zajac, Ph.D., Slovenská technická univerzita v Bratislavě, Slovenská republika