Výzkumné léto na FIT 2021 (VýLeT 2021):
Program podpory letního studentského výzkumu
na FIT ČVUT

Vypsaná témata

O čem je tento dokument?

Tento dokument obsahuje soupis výzkumných témat vypsaných v rámci programu VýLeT pro rok 2021.

Stručné informace k přihlášení do programu VýLeT 2021

Kdo se může přihlásit?

(a) Přihlásit do programu se může student bakalářského nebo navazujícího magisterského programu na ČVUT, a to v období stanoveném v harmonogramu.

(b) Témata se dělí na volná a rezervovaná. Rezervovaná témata jsou určena pro konkrétní studenty vybrané mentorem. Zvolit si rezervované téma může pouze student, pro kterého je téma rezervováno. Pokud nejste studentem, pro kterého je téma rezervováno, a máte vážný zájem o oblast vědy, do které dané téma spadá , kontaktujte mentora s dotazem, zda je možné vypsat další zadání z dané oblasti.

(c) Kterýkoliv student, který je studentem dle bodu a. tohoto odstavce se může přihlásit na jakékoliv volné téma.

(d) Jeden student se může přihlásit na více témat, vlastní přiřazení zájemců k tématům proběhne až ve výběrovém řízení.

(e) Student se může přihlásit a následně řešit výzkumné téma, které je v překryvu s tématem jeho závěrečné práce.

Jak se přihlásit?

Přihlášení probíhá zasláním e-mailu na vylet@fit.cvut.cz s předmětem “VýLeT 2021 - přihláška”. Zájemce zašle v příloze e-mailu vyplněný soubor přihláška.xlsx / přihláška.ods (ke stažení na webové stránce VýLeTu – viz https://fit.cvut.cz).

Soubor s přihláškou obsahuje tyto údaje:

1. jméno a příjmení,
2. uživatelské jméno ČVUT,
3. ročník a studijní program
4. popis svých studijních plánů na FIT ČVUT/ jiné fakultě ČVUT (zda plánuje studium končit v roce 2021 nebo 2022, zda bude na FIT ČVUT pokračovat, od kdy a v jaké formě),
5. vybraná témata projektů,
6. popis vlastní motivace.

Volitelně může zájemce přiložit profesní životopis. Tento způsob přihlášení je jediný možný a jediný platný. Přihlášení prostřednictvím jiného komunikačního kanálu nebude považováno za platné.

Do kdy je třeba se přihlásit?

Je třeba se přihlásit v lhůtě určené pro přihlašování. Tato lhůta končí **7. 5. 2021**.

Jak proběhne výběrové řízení?

Přiřazení přihlášených zájemců k tématům podléhá schválení ve výběrovém řízení, a to takto:

i. Přiřazení přihlášených zájemcům k jednomu tématu provádí na základě přihlášek a zadání Komise.
ii. Komise vytváří pořadí vybraných přiřazení zájemců k tématům v závislosti na vhodnosti jejich financování vzhledem k potenciálu splnit všechny cíle programu, odborné kvalitě nebo aplikovatelnosti předpokládaného výstupu.
iii. Komise dále schvaluje podpořená témata a jim přiřazené řešitele-studenty na základě možného počtu podpořených projektů.

Podrobné informace k Programu VýLeT 2021 naleznete v dokumentu **„Výzkumné léto na FIT 2021 (VýLeT 2021): Program podpory letního studentského výzkumu na FIT ČVUT – Propozice.“**

Vypsaná výzkumná témata

Název zadání: **Vyhodnocení efektivity SAT řešičů pro obvodový SAT**

Mentor: doc. Ing. Petr Fišer, Ph.D. <fiserp@fit.cvut.cz>

Cílem práce je provést experimentální vyhodnocení efektivity (rychlosti) dostupných open-source řešičů problému splnitelnosti booleovské formule (SAT) pro instance získané transformací z obvodu (netlistu), tj. pro tzv. „circuit-SAT“. Tyto instance jsou svojí povahou specifické. Jsou sice „lehké“ (spíše se blíží 2-SATu), ale objevují se v nich těžké části. SAT řešiče se proto pro ně mohou chovat jinak, než pro běžné zkušební instance. Účinnost dostupných SAT řešičů pro tyto instance zatím nebyla dostatečně zkoumána.
Jedná se o čistě experimentální práci. Programování pravděpodobně nebude zapotřebí. Generátor instancí je k dispozici. Naučíte se pracovat s výpočetním clusterem CESNET MetaCentrum (OS Linux).
Výstupem budou příslušné statistiky, doporučení a (pevně doufám) článek na konferenci.

Plánované výstupy (konference a časopisy):

IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS)
Euromicro

IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS)
IEEE

The International Conferences on Theory and Applications of Satisfiability Testing (SAT)
ACM

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Použití logické syntézy pro usnadnění řešení SAT problému**

Mentor: doc. Ing. Petr Fišer, Ph.D. <fiserp@fit.cvut.cz>

Cílem práce je vyzkoušet vliv logické syntézy na řešení problému splnitelnosti booleovské formule (SAT). Tj. prozkoumat, zda a jaká zjednodušení (resp. transformace) booleovské formule vedou ke zrychlení řešení SATu. V literatuře se objevují zmínky o pozitivním i negativním vlivu, dosud ale tento problém nebyl zkoumán dostatečně komplexně.
Jedná se o čistě experimentální práci. Programování pravděpodobně nebude zapotřebí. Naučíte se pracovat s výpočetním clusterem CESNET MetaCentrum (OS Linux) a nástroji pro logickou syntézu.
Výstupem budou příslušné statistiky, doporučení a (pevně doufám) článek na konferenci.

Plánované výstupy (konference a časopisy):

IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS)
IEEE

Euromicro Conference on Digital System Design (DSD)
Euromicro

The International Conferences on Theory and Applications of Satisfiability Testing (SAT)
ACM

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Zjišťování podobnosti obvodů**

Mentor: doc. Ing. Petr Fišer, Ph.D. <fiserp@fit.cvut.cz>

Cílem práce je navrhnout algoritmus a naimplementovat nástroj pro stanovení podobnosti dvou kombinačních logických obvodů, které jsou funkčně ekvivalentní, ale strukturně rozdílné. Možností řešení je mnoho. Jedna z možností (možná preferovaná) je navázat na letos obhájenou DP, použít zde prezentovaný algoritmus, lépe jej vyhodnotit a případně vylepšit.
Znalost číslicového návrhu není nutná, je to problém spíše z oblasti teoretické informatiky (grafový problém). Naučíte se pracovat s výpočetním clusterem CESNET MetaCentrum (OS Linux).
Výstupem bude článek na konferenci.

Plánované výstupy (konference a časopisy):

IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS)
IEEE

Euromicro Conference on Digital System Design (DSD)
Euromicro

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Multi-agentní hledání cest pro skutečné roboty**
Multi-agent Path Finding for Real Robots

Mentor: doc. RNDr. Pavel Surynek, Ph.D. <surynpav@fit.cvut.cz>

Tématem práce je multi-agentní hledání cest, kdy je úkolem najít pro mobilní agenty nekonfliktní cesty tak, že každého agenta dovede jeho cesta bezpečně na cílové místo. Speciálně budeme zkoumat rozšíření problému, která je nutné uvažovat, pokud chceme výsledné plány používat na skutečných robotech, například spojitý čas. Výstupem výzkumu by například mohl být algoritmus pracující se spojitým časem, jehož plány lze použít pro roboty typu Ozobot EVO.

Multi-agent path finding is the task is to find non-conflict paths for mobile agents so that each agent can navigate itself via his path safely to its destination. We will specifically examine the extension of the problem that must be considered if we want to use the resulting plans on real robots, such as continuous time. For example, the output of the research could be a continuous-time algorithm whose plans can be used for Ozobot EVO robots.

Plánované výstupy (konference a časopisy):

ICAART 2022, the International Conference on Agents and Artificial Intelligence
INSTICC

IJAIT, International Journal on Artificial Intelligence Tools
World Scientific

ICTAI 2022, the International Conference on Tools with Artificial Intellignce
IEEE

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Unsupervised Source Code Pattern Matching**

Mentor: Mgr. Alexander Kovalenko Ph.D. <kovalale@fit.cvut.cz>

Source code pattern recognition is an important task that can help in many tasks, such as: bug detection and fix, code optimization, semantic code autocompletion, clone detection etc. Thus, the current research problem aimed to develop the method for efficient pattern recognition of the source code. The student will explore possibilities to use Siamese architecture and/or attention mechanisms for source code pattern matching. Additionally, the form of input data (raw code, abstract syntax tree, dependence graph, etc.) is a subject to investigate.

Plánované výstupy (konference a časopisy):

Pattern Recognition, ISSN: 0031-3203
Elsevier

International Journal of Pattern Recognition and Artificial Intelligence, ISSN: 1793-6381
World Scientific

AI, ISSN 2673-2688
MDPI

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Linear Attention is all we need!**

Mentor: Mgr. Alexander Kovalenko Ph.D. <kovalale@fit.cvut.cz>

Quadratic complexity of attention in transformer architecture places high hardware demand on processing long sequences. Therefore, the goal of this research is to explore possibilities of linear attention in transformer-like architecture and implement new methods (own or provided by the supervisor).

Plánované výstupy (konference a časopisy):

The International Conference on Learning Representations (ICLR)

The International Conference on Machine Learning (ICML)
International Machine Learning Society (IMLS)

European Conference on Artificial Intelligence (ECAI)) ()

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Útok na schéma VeraGreg prostřednictvím analýzy postranních kanálů**

Mentor: Dr.-Ing, Martin Novotný <novotnym@fit.cvut.cz>

Seznamte se se schématem VeraGreg a jeho implementací na mikrokontroléru. Prozkoumejte možnosti útoku na tuto implemementaci postřednictvím postranních kanálů. Zkoumejte, jaký vliv na odolnost má implementace klíčových operací v zabezpečeném hardwarovém akcelerátoru. Očekávaným výstupem je publikace na mezinárodní konferenci nebo v časopise.

Plánované výstupy (konference a časopisy):

Euromicro Conference on Digital System Design, DSD 2022
Euromicro

Microprocessors and Microsystems, MICPRO
Elsevier

International Conference on Cryptographic Hardware and Embedded Systems, CHES
IACR

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Útok na Paillierův kryptosystém prostřednictvím analýzy postranních kanálů**

Mentor: Dr.-Ing, Martin Novotný <novotnym@fit.cvut.cz>

Seznamte se Paillierovým kryptosystémem a jeho implementací na mikrokontroléru. Prozkoumejte možnosti útoku na tuto implemementaci postřednictvím postranních kanálů. Zkoumejte, jaký vliv na odolnost má implementace klíčových operací v zabezpečeném hardwarovém akcelerátoru. Očekávaným výstupem je publikace na mezinárodní konferenci nebo v časopise.

Plánované výstupy (konference a časopisy):

Euromicro Conference on Digital System Design, DSD 2022
Euromicro

Microprocessors and Microsystems, MICPRO
Elsevier

International Conference on Cryptographic Hardware and Embedded Systems, CHES
IACR

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Evakuace vlaku - citlivostní analýza multi-agentních modelů**
Train Evacuation - Sensitivity Analysis of Multi-Agent Models

Mentor: Ing. Pavel Hrabák, Ph.D. <hrabapav@fit.cvut.cz>

Multiagentní modely evakuace mohou sloužit jako užitečný nástroj pro posouzení bezpečnosti prostředků veřejné dopravy, jako je například osobní vlak. Pomocí simulací je možné analyzovat bezpečnost prostředku bez nutnosti nákladných evakuačních cvičení. Ve srovnání s evakuací budov je prostředí vlaku typické uzavřeným prostorem s úzkými uličkami, omezeným počtem východů a nestandardními únikovými cestami. Klasické postupy a simulační nástroje pro evakuaci budov tak není možné bez bližší analýzy pro simulaci evakuace takového prostoru využít.
Cílem tohoto projektu je prozkoumat možnosti vybraných evakuačních modelů pro použití k simulaci evakuace osobního vlaku a pomocí nástrojů variační citlivostní analýzy kvantifikovat vliv jednotlivých parametrů modelů na pozorovatelné veličiny jako je totální evakuační čas a tok hlavním východem. Výstupy simulací budou porovnány s daty z experimentální evakuace železničního vozu elektrické jednotky 471 (CityElefant), která se uskutečnila v roce 2018.
V současné době existuje model výše zmíněného experimentu evakuace železničního vozu vytvořený v softwaru Pathfinder (https://www.thunderheadeng.com/pathfinder/) validovaný proti experimentálním datům.

Dílčí úlohy projektu jsou:

- Vytvořit skript, který bude pouštět a zaznamenávat výsledky simulací Pathfinderu opakovaně a to tak, aby bylo možné strojově měnit parametry modelu včetně dílčích parametrů jednotlivých agentů.
- Pomocí citlivostní analýzy kvantifikovat vliv jednotlivých parametrů modelu na klíčové veličiny, nastudovat za tímto účelem vhodné vzorkování parametrického prostoru. Porovnat závěry s citlivostní analýzou evakuace budov. Např. použitím balíčku https://salib.readthedocs.io/.
- Pokusit se vytvořit model tohoto experimentu v nějakém open-source simulátoru (např. https://www.jupedsim.org/ nebo http://www.vadere.org/), provést citlivostní analýzu a porovnat s předchozími výsledky.

Projekt bude zpracováván ve spolupráci s Ing. Hankou Najmanovou (FSv) a Ing. Danielem Vašatou, Ph.D. (FIT). Kromě výše zmíněné analýzy bude aplikovatelným výstupem doporučení, které parametry agentů v modelu Pathfinder hrají pro evakuaci vlaku klíčovou roli a je jim tedy potřeba věnovat dostatečnou pozornost při kalibraci modelu.
Výstupy projektu by měli být prezentovány na konferenci Traffic and Granullar Flow 2022 a zaslány do jednoho z uvedených časopisů.

Multiagent evacuation models can serve as a useful tool for assessing the safety of public transport vehicles, such as a passenger train. With the help of simulations, it is possible to analyse the safety of the vehicle without the need for costly evacuation trials. Compared to the evacuation of buildings, the train environment is characterized by confined space with narrow aisles, a limited number of exits, and non-standard exit routes. Classical procedures and simulation tools designed for the evacuation of buildings cannot be used to simulate the evacuation of such a space without further analysis.
The aim of this project is to explore the possibilities of selected evacuation models for simulation of the evacuation of a passenger train and to quantify the influence of individual model parameters on

observables (such as total evacuation time and main exit flow) by means of variance -based sensitivity analysis. The outputs of the simulations will be compared with data from the experimental evacuation of the railway car of the electric unit 471 (CityElefant) conducted in 2018. Currently, there is a model of the above-mentioned rail-car evacuation experiment created in Pathfinder software (https://www.thunderheadeng.com/pathfinder/) validated against experimental data.

The partial tasks of the project are:

- Create a script that will run and record the results of Pathfinder simulations repeatedly so that it is possible to automatically change the parameters of the model, including partial parameters of individual agents.
- Using sensitivity analysis, quantify the influence of individual parameters of the model on key quantities, study the appropriate sampling of parametric space for this purpose. Compare the conclusions with the sensitivity analysis for the evacuation of buildings. E.g. using the https://salib.readthedocs.io/ package.
- Try to create a model of this experiment in some open-source simulator (e.g. https://www.jupedsim.org/ or http://www.vadere.org/), perform a sensitivity analysis and compare with previous results.

The project will be processed in cooperation with Ing. Hanka Najmanová (FSv) and Ing. Daniel Vašata, Ph.D. (FIT). In addition to the above analysis, the applicable output will be a recommendation, which agent parameters in the Pathfinder model play a key role in train evacuation and therefore need sufficient attention when calibrating the model.
The outputs of the project should be presented at the Traffic and Granullar Flow 2022 conference and sent to one of the mentioned journals.

Plánované výstupy (konference a časopisy):

Traffic and Granular Flow, TGF 2022
K. Ramachandra Rao, Indian Institute of Technology Delhi

Transportmetrica A: Transport Science, TRANSPORTMETRICA A
Taylor&Francis

Simulation Modelling Practice and Theory, SIMUL MODEL PRACT TH
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **FitCloud VM consolidator**

Mentor: Ing. Jan Fesl, Ph.D. <fesljan@fit.cvut.cz>

Účelem výzkumu bude studium algoritmů pro dynamickou konsolidaci virtuálních počítačů pro pozdější využití na platformě FITCloud. Budou studovány a optimalizovány algoritmy za účelem:

1) Snížení spotřeby celé infrastruktury prostřednictvím live migrace virtuálních strojů, popř. částečné hibernace některých virtualizačních uzlů.
2) Dosažení maximálního výpočetního výkonu infrastruktury.

Oba scénáře optimalizovat i s ohledem na celkové nutné změny rozmístění virtuálních počítačů, které přímo souvisí s nutnou dobou na provedení změn.

The purpose of the research will be to study algorithms for dynamic consolidation of virtual machines for later use on the FITCloud platform. Algorithms will be studied and optimized in order to:

1) Reducing the consumption of the entire infrastructure through live migration of virtual machines, or partial hibernation of some virtualization nodes.
2) Achieving maximum computing power of the infrastructure.

Optimize both scenarios with regard to the overall necessary changes in the deployment of virtual machines, which are directly related to the necessary time to make changes.

Plánované výstupy (konference a časopisy):

Journal of Cloud Computing
Springer Nature

International Symposium on Grids & Clouds
Academia Sinica Grid Computing Centre (ASGC)

Conference on Innovation in Clouds, Internet and Networks (ICIN)
DNAC

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Struktura pevných bodů Arnouxových-Rauzyových morfismů**
Structure of Arnoux-Rauzy fixed points

Mentor: doc. Ing. Štěpán Starosta, Ph.D. <staroste@fit.cvut.cz>

Výzkumným tématem je zkoumání pevných bodů Arnouxových-Rauzyových (AR) morfismů: jedná se o nekonečné posloupnosti, které nejsou periodické ale ani naprosto chaotické. AR morfismy jsou zobecněním dobře prozkoumaných Sturmovských morfismů, a lze je chápat jako jednoduchá přepisovací pravidla typu a -> ab, b -> a (pevný bod takového přepisovacího pravidla pak začíná na abaababaab ...). Cílem je zkoumat strukturu tzv. návratových slov. První krokem je vytvoření experimentů na počítači a vytvoření hypotéz o struktuře návratových slov za pomoci geometrické reprezentace těchto pevných bodů.

The goal is an investigation of fixed points of Arnoux-Rauzy (AR) morphisms. These are infinite sequences that are neither periodic neither chaotic. AR morphisms are a generalization of well-known Sturmian morphisms, and can be understood as rewriting rules of the type a -> ab, b -> a (a fixed point of such rewriting rule starts with abaababaab ...). The goal is to study the structure of so-called return words. The first step is to create computer experiments and obtain a conjecture on the structure using the geometrical representation of these fixed points.

Plánované výstupy (konference a časopisy):

European Journal of Compinatorics
Academic Press Inc.

Theoretical Computer Science
Elsevier

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Použití konvolučních a generativních NN pro výběr vzorů v procesu designu interiérů**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D. <jankul@fit.cvut.cz>

Prozkoumejte možnosti užití konvolučních a generativních NN pro výběr vzorů v procesu designu interiérů. Vytvořte dataset vzorových interiérů a z nich extrahovaných vzorů, navrhněte atributy popisující způsoby užití vzoru. Vytvořte databanku vzorů, proveďte experimenty se skupinou dobrovolníků ohledně vnímání kombinace vzorů, výsledky využijte při trénování NN.

Plánované výstupy (konference a časopisy):

International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems IEA/AIE (Core B)

International Conference on Engineering Applications of Neural Networks (EANN, Core C)

IEEE International Joint Conference on Neural Networks (Core A)

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Morfismy zachovávající dané vlastnosti**
Morphisms preserving given properties

Mentor: doc. Ing. Štěpán Starosta, Ph.D. <staroste@fit.cvut.cz>

Morfismus lze chápat například jako jednoduchá přepisovací pravidla typu a -> ab, b -> a, která působí na nekonečnou posloupnost (nekonečné slovo) z prvků z abecedy {a, b}. Obraz takové zobrazení je také nějaké nekonečné slovo, a zajímavým jevem je, pokud jsou tímto zobrazením zachovány některé netriviální vlastnosti. Cílem práce by bylo zkoumat právě takové morfismy, které vždy nějakou vlastnost zachovají. První zkoumanou vlastností bude palindromická bohatost, u které existují teoretické výstupy, které umožňují generovat kandidáty na takové morfismy. Zkoumání je vhodné založit na počítačových experimentech.

Plánované výstupy (konference a časopisy):

European Journal of Compinatorics
Academic Press Inc.

Theoretical Computer Science
Elsevier

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Pomocné metody vytváření nových faktů v generickém dokazovacím asistentu Isabelle/HOL pro seznamy/slova**
Helper methods creating new fact in the generic proof assistant Isabelle/HOL for lists/words

Mentor: doc. Ing. Štěpán Starosta, Ph.D. <staroste@fit.cvut.cz>

Isabelle/HOL je generický dokazovací asistent. Umožňuje provést formalizaci matematické věty a strojové ověření jejího důkazů, vše zapsané v relativně dobře lidsky čitelné podobně (podobně jako na tabuli). Takto dokázaná věta se pak v systému stáva faktem, a z faktu lze algoritmicky vytvořit jiný fakt, např. symetrický (například z faktu "x = y" vytvoří fakt "y = x"). Cílem práce by bylo navrhnout a vytvořit algoritmus, který vytváří jiné fakty podobným způsobem a to v kontextu uspořádaných seznamů (slov), kde lze využít nějaké další symetrie (např. reverze slova). Práce se případně také může věnovat algoritmům, které usnadní důkazy některých faktů týkajících se slov (např. algoritmus, který pozná, že se slova nerovnají, a pak spustí adekvátní formální důkaz).

Plánované výstupy (konference a časopisy):

Interactive Theorem Proving 2022
https://itp-conference.github.io/

ACM Transactions on Computational Logic
Association for Computing Machinery (ACM)

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Výzkum v oblasti hyperheuristik a rozšíření frameworku SEAGE**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D. <jankul@fit.cvut.cz>

Výzkum v oblasti hyper-heuristik a rozšíření frameworku SEAGE. V návaznosti na zhodnocení optimalizačního frameworku SEAGE z pohledu aktuálního stavu výzkumu v oblasti hyper-heuristik, se zaměřte na vývoj metodiky pro evaluaci hyper-heuristiky/meta-heuristik, dále se věnujte problematice vylepšení hyper-heuristik, implementujte toto/ tato vylepšení a otestujte ho.

Plánované výstupy (konference a časopisy):

European Conference on Artificial Intelligence (ECAI, core A)

International Joint Conference on Artificial Intelligence (IJCAI, Core A*)

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Výzkum užití metod umělé inteligence pro automatický výběr a rozmístění nábytku v designu interiérů**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D. <jankul@fit.cvut.cz>

Výzkum použití metod AI v systému pro výběr a rozmístění nábytku ve vnitřních prostorách definovaných stavebními plány (půdorys, užití místností, přípojky sítí, možností budování sítí) s předem danými omezujícími podmínkami. Navažte na vlastní existující výzkum zahrnující formalizaci úlohy pro její řešení pomocí AI a použití genetických algoritmů k řešení daného problému.

Plánované výstupy (konference a časopisy):

International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (Core B)

European Conference on Artificial Intelligence (Core A)

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Multi-agentní systémy pro automatizovaný návrh vybavení interiéru nábytkem**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D. <jankul@fit.cvut.cz>

Výzkum použití multiagentních systémů a aplikace metod plánování pro vytvoření systému pro výběr a rozmístění nábytku ve vnitřních prostorách definovaných stavebními plány (půdorys, užití místností, přípojky sítí, možností budování sítí) s předem danými omezujícími podmínkami. Zaměřte se na propojení agentních systému a NN s LTSM.

Plánované výstupy (konference a časopisy):

International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE, Core B)

European Conference on Artificial Intelligence (ECAI, Core A)

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Analýza dat o využití prostředků pro automatizované testování softwaru za účelem optimalizace v cloudu**
Analysis of data on the utilization of automated software testing resources for the purpose of cloud optimization

Mentor: Ing. Tomáš Vondra, Ph.D. <vondrto6@fit.cvut.cz>

Společnost Pure Storage vyrábí vysoce spolehlivá úložná pole. Aby toho dosáhli, provádějí rozsáhlé testování softwaru. Existuje několik typů testovacích sad, některé hardwarové a některé virtuální, a mohou je interaktivně používat vývojáři nebo automaticky úlohy ze systémů CI (Continuous Integration). Virtuální testovací sady jsou bohužel statické, přestože běží na cloudovém systému, takže jejich využití pravděpodobně není optimální.

Charakterizujte data o využití testovacích sad v čase a identifikujte užitečné vzory a korelace. (Data obsahují stavy testovací sady, uživatele, testované větve kódu, trvání testů atd.)

Navrhněte způsoby, jak optimalizovat distribuci testovacích sad tak, aby interaktivní uživatelé získali volnou testovací sadu rychleji nebo aby automatické úlohy získaly lepší propustnost.

Poskytnuté údaje budou anonymizovány, ale stále obsahují všechny informace. Cílem je především publikovat výzkumný článek s charakterizací dat, sekundárně navrhnout společnosti potenciální optimalizaci jejich vzorců využití. Komunikace se zadavatelem dat např. za účelem doplnění datového souboru nebo vysvětlení bude možná.

The company Pure Storage manufactures highly dependable storage arrays. To achieve that, they do extensive software testing. There are several testbed types, some hardware and some virtual, and they can be used interactively by the developers or automatically by jobs from CI (Continuous Integration) systems. Unfortunately the virtual testbeds are static, even though they run on a cloud system, so their utilization is probably not optimal.

Characterize the data on testbed usage in time to find useful patterns and correlations. (The data contains testbed states, users, feature branches tested, test durations, etc.)

Propose ways to optimize the testbed distribution so that interactive users get a free testbed faster or so that automatic jobs get better throughput.

The provided data will be anonymized, but still contain all information. The goal is primarily to publish a research article with the characterization of the data, secondarily to propose to the company potential optimization of their usage patterns. Communication with the company providing the data e.g. for amendment of the dataset or explanation will be possible.

Plánované výstupy (konference a časopisy):

European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database ECML PKDD 2022
Nezávislá konference / Springer

IEEE Congress on Evolutionary Computation CEC 2022
IEEE

Výsledek bude předán firmě, ze které pochází zkoumaná data.

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Vliv pozice těla na úspěšnost střelby z luku**
Influence of body position on the success of archery

Mentor: Ing. Jakub Novák <novakj67@fit.cvut.cz>

Prozkoumejte zásady střelby z luku a vliv různých parametrů na úspěšnost výstřelu. Soustřeďte se hlavně na parametry těla, např. pohyb rukou ve chvíli výstřelu šípu. K měření využijte vysokorychlostní kamery a metody počítačového vidění. Zkoumejte vliv parametrů na výsledný zásah terče.

Investigate the principles of archery and the influence of various parameters on the success of the shot. Focus mainly on the parameters of the body, such as the movement of the hands at the time of the arrow shot. Use high-speed cameras and computer vision methods to measure. Investigate the influence of parameters on the final impact of the target.

Plánované výstupy (konference a časopisy):

ICB: International Conference on Biometrics
IEEE Biometrics Council and the IAPR TC-4

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Adversarial learning pro detekci malware**
Adversarial learning for malware detection

Mentor: Mgr. Martin Jureček <jurecmar@fit.cvut.cz>

Cílem techniky adversarial learning je záměrná modifikace vstupních dat, která způsobí snížení přenosti klasifikace. Modifikaci dat pro problém detekce malwaru je možné provést buď na úrovni vektoru příznaků, nebo na úrovni samotných vzorků, z kterých se extrahují vektory příznaků. Druhá zmíněná modifikace je technicky náročnější, ale v praxi použitelnější. Přínosem této práce by bylo vytvořit nové metody z oblasti adversarial learning a otestovat jejich efektivitu na některých detekčních systémech škodlivého kódu.

The aim of the adversarial learning technique is the deliberate modification of input data, which causes a reduction in the accuracy of classification. Data modification for the malware detection problem can be done, either at the level of the feature vector or at the level of the samples themselves from which the feature vectors are extracted. The latter modification is technically more demanding but more applicable in practice. The benefit of this work would be to create new methods of adversarial learning and to test their effectiveness on some malicious code detection systems.

Plánované výstupy (konference a časopisy):

International Conference on Information Systems Security and Privacy - ICISSP

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Interpretovatelnost výsledků detekce malware založených na strojovém učení pomocí sady pravidel**
Interpretability of machine learning-based results of malware detection using a set of rules

Mentor: Mgr. Martin Jureček <jurecmar@fit.cvut.cz>

V dnešní době patří algoritmy strojového učení mezi standardní techniky používané k detekci malware. Algoritmy strojového učení však nejsou přímo začleněny do antivirových programů nainstalovaných v operačních systémech uživatelů. Proto je vhodné interpretovat výsledky strojového učení (získané v cloudu) jako sadu detekčních pravidel (např. jako pravidla ve tvaru: (x_1 o_1 h_1) AND ... AND (x_n o_n h_n), kde x_i jsou příznaky, o_i relační operátory a h_i hodnoty), aby se zabránilo nutnosti udržovat velké databáze. Cílem je vytvořit pravidla, na jejichž základě bude malware detekován co nejpřesněji a s co nejnižším počtem falešně pozitivních výsledků.

Nowadays, machine learning (ML) algorithms are common techniques used to detect malware. However, ML algorithms are not directly incorporated into antivirus programs installed on users' systems. Therefore, it is convenient to interpret the ML results (obtained in the cloud) as a set of detection rules (e.g., as formulas: (x_1 o_1 h_1) AND ... AND (x_n o_n h_n), where x_i are features, o_i relational operators, and h_i values) to avoid the need to maintain large databases. The goal is to create formulas based on which malware will be detected as accurately as possible and with the lowest false positive rate.

Plánované výstupy (konference a časopisy):

International Conference on Information Systems Security and Privacy - ICISSP

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Bezpečnost v IoT**
IoT Security

Mentor: Ing. Jiří Dostál, Ph.D. <dostaji2@fit.cvut.cz>

Seznamte se s problematikou specifické kybernetické bezpečnosti v IoT. Na základě předešlých prací si zvolte konkrétní rozpracované téma (např. SDR, IoT protkoly, FW over the air update, wireless, lifecycle management, 4G/5G sítě) a analyzujte danou problematiku v prostředí IoT. Výsledek může obsahovat PoC code nebo komplexnější analýzu daného tématu.

Plánované výstupy (konference a časopisy):

Konferenční příspěvek podle konečného výsledku.

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Algoritmy pro video analýzu chování zákazníků před vstupem do retailové pobočky na platformě NVIDIA Jetson**

Mentor: Ing. Lukáš Brchl <brchlluk@fit.cvut.cz>

Cílem práce je návrh a implementace algoritmů, jejichž cílem je umožnit detekovat a sledovat osoby ve videozáznamu pro analytické výstupy vhodné v retailovém prostředí. K dosažení cíle je nutné rešeršovat existující metody detekce osob, extrakce obrazových charaketristik a biometrie, a sledovacích algoritmů. Na základě této rešreše pak navrhnout vlastní sledovací algoritmus, který bude vhodný pro retailové prostředí poboček/prodejen a ten optimalizovat pro real-time běh na platformě NVIDIA Jetson.

Plánovaným výstupem je open-source GitHub repozitář s implementací daných algoritmů se zdokumentovanými postupy.

Plánované výstupy (konference a časopisy):

International Journal of Computer Vision (Journal)
Springer

Image and Vision Computing
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Analýza vibrací pro detekci anomálií bezpilotních prostředků**

Mentor: Ing. Lukáš Brchl <brchlluk@fit.cvut.cz>

Cílem práce je návrh a implementace algoritmů, jejichž cílem je detekovat anomálie letícího dronu pomocí analýzy vibrací. To se hodí k prevenci závad a nehod, které se mohou stát obvyklým používáním dronu, během kterého dochází k opotřebení pohybujících se součástek (např. vrtule, motory) nebo povolování šroubků. Vibrace lze měřit pomocí IMU jednotky, která se nachází již uvnitř dronu nebo je k tomu vhodnější využít externí zařízení s akcelerometrem. Podstatnou součástí práce je i vybudování metodiky měření na dronu během letu.

Plánovaným výstupem je open-source GitHub repozitář s implementací daných algoritmů se zdokumentovanými postupy a testovací rameno dronu, na kterém bude možné vyvinuté metody testovat.

Plánované výstupy (konference a časopisy):

Pattern Recognition (Journal)
Elsevier

IEEE Sensors (Journal)
IEEE

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Detekce rizik vegetace v blízkosti distribučních sítí za pomocí dat z dronu**

Mentor: Ing. Lukáš Brchl <brchlluk@fit.cvut.cz>

Vegetační management je jedna z významných činností, které distribuční společnosti musí neustále řešit. Jde zejména o monitoring lesních porostů v blízkostí drátů vysokého napětí, aby byla zmírněna rizika požáru nebo výpadku proudu. Cílem práce je tedy návrh a implementace algoritmů, jejichž cílem je umožnit detekovat vegetaci (např. stromy) v nebezpečné vzdálenosti od distribuční sítě za pomocí algoritmů počítačového vidění. Zdrojem dat k této úloze bývaji nejčastěji satelitní snímky. Ukazuje se však, že tyto data disponují nedostatečným rozlišením a absencí 3D pohledu. Z tohoto důvodu bude využit v práci dron, který dokáže data nasnímat v požadované kvalitě.

Plánovaným výstupem je open-source GitHub repozitář s implementací daných algoritmů se zdokumentovanými postupy.

Plánované výstupy (konference a časopisy):

IEEE International Geoscience and Remote Sensing Symposium
IEEE

International Society for Photogrammetry and Remote Sensing

International Journal of Remote Sensing

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Témata z oblasti meta-learningu, automl, optimalizace neuronových sítí, explainable AI**
Various topics in the area of meta-learningu, automl, neural net optimization, explainable AI

Mentor: Pavel Kordík <kordikp@fit.cvut.cz>

Pokud vás zajímá některá z oblastí, vymyslíme spolu konkrétní zadání.

In case you are interested in some of the above domains, we can finetune assignment together.

Plánované výstupy (konference a časopisy):

ICANN 2022

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Metody strojového učení pro analýzu logů serverů**
Machine learning methods for server logs analytics

Mentor: Doc. Ing. Tomáš Vitvar, Ph.D. <vitvatom@fit.cvut.cz>

Cílem projektu je vyvinout metody pro analýzu logů ze serverů z velkých prostředí za účelem filtrování zpráv, detekce typů chyb, frekvence výskytů chyb a korelace s metrikami výkonu systémů během provozu. Tento projekt zahrnuje použití metod založených na NLP a neuronových sítí. Student pracuje na tomto tématu v rámci své diplomové práce a plánuje pracovat na publikaci výsledků ve vybrané konferenci. Student se bude hlásit do doktorského studia do zimního semestru 2021.

The goal of the project is to develop methods for analysis of server logs from large-scale systems to filter messages, understand the error types, their frequencies and correlations with other performance data of systems during runtime. This covers the use of methods based on NLP and neural networks. Student works on this topic as part of his master thesis and he plans to work on a publication of the results in a selected conference. The student plans to work on his PhD starting from winter semester 2021.

Plánované výstupy (konference a časopisy):

5th IEEE International Conference On Software Architecture
https://icsa-conferences.org/2021/organization/

IEEE International Conference On Service-Oriented System Engineering
http://www.ieeesose.net/

European Conference on Technology Enhanced Learning
https://ea-tel.eu/ectel2021

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Spolehlivý vestavný systém reálného času**
Realible Embedded Real-Time System

Mentor: doc. Ing. Hana Kubátová, CSc. <kubatova@fit.cvut.cz>

Prostudujte metody a způsoby, jak zajistit spolehlivou funkci vestavného řídícího systému, který pracuje v reálném čase. Prozkoumejte možnosti, jak požadovanou úroveň spolehlivosti garantovat s ohledem na možné řízení v kritických aplikacích. Uvažujte využití vhodných modelů pro celkový hardware/software codesign včetně možného využití vhodných operačních systémů reálného času (RTOS). Cílem je výběr vhodného modelu a jeho experimentální ověření.

Study the methods how to ensure reliable operation of a real-time embedded control system. Explore the possibilities how to guarantee required level of dependability parameters with respect to mission-critical applications. Consider using suitable models for the overall hardware/software codesign including the possible use of appropriate open-source RTOS for embedded systems. The main aim is proper model selection and its experimental evaluation.

Plánované výstupy (konference a časopisy):

Konference MECO/CPSIOT (http://embeddedcomputing.meconet.me/meco2021/)
Montenegrin Association for New Technologies (MANT) + IEEE, EUROMICRO

PESW: Prague Emebedded System Workshop
FIT ČVUT + Student Chapter IEEE

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Návrh nové kryptoměny zaměřené na převody autorských práv k digitálním uměleckým dílům, virtuálním předmětům či k jiným digitálním entitám**

Mentor: Ing. Jiří Smítka <xsmitka@fit.cvut.cz>

Prozkoumejte principy fungování a zabezpečení současných kryptoměn, které umožňují začlenění jedinečného tokenu do svého blockchainu (např. Ethereum + NFT).
Tento jedinečný token by měl být důkazem o vlastnictví nějaké entity, např. digitálního uměleckého díla nebo třeba virtuálního předmětu ve virtuálním počítačovém prostředí (dále jen Entita).

Navrhněte novou kryptoměnu, která:

- bude mít vyšší než obvyklé zabezpečení odpovídající aktuální síle výpočetní techniky,
- umožní velmi rychlé potvrzování transakcí,
- umožní vkládat jedinečné tokeny jako důkaz vlastnictví uměleckého díla.

Kryptoměna by měla umožňovat svázat transakci s převodem vlastnictví tokenu (důkaz vlastnictví Entity) a finanční transakci (s úhradou ceny Entity).

Navrhněte strukturu blockchainu, způsoby těžby a komunikační protokoly. Návrh by měl klást důraz na co nejvyšší bezpečnost, odolnost proti útokům a zároveň preferovat jednoduchost řešení.

Plánované výstupy (konference a časopisy):

International Conference on the Theory and Application of Cryptographic Techniques
(Core ranking A*)
International Association for Cryptologic Research (IACR)

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Predikce náhlého nárůstu zátěže na webovém serveru**
Prediction of sudden load increases in a web server

Mentor: Ing. Tomáš Vondra, Ph.D. <vondrto6@fit.cvut.cz>

Některé webové aplikace zažívají mimo pravidelných změn řízených denní seasonalitou také náhlé špičky v návštěvnosti. Moderní aplikace běží na škálovatelné cloudové platformě, ale běžné reaktivní formy škálování reagují na přetížení se zpožděním a prediktivní škálování umí předpovídat hlavně denní křivky a nikoli špičky. Proveďte analýzu dat o provozu ze serveru Novinky.cz, která zahrnují anonymizovaná ID jednotlivých zdrojů. Opravte případné anomálie v datech. Proveďte jejich rozklad na jednotlivé časové řady návštěvnosti daných zdrojů a zdroje roztřiďte na takové, které existují dlouhodobě a takové, které představují články s časově omezenou zajímavostí pro čtenáře. U dat představujících články popište způsob náběhu časových řad od začátku do prvního maxima. Navrhněte metodu, jak u nově vzniklého zdroje odhadnout s předstihem v řádu minut jeho maximum, pokud to z dat bude možné. Zjistěte, zda by tato metoda byla přínosná pro prediktivní škálování serverů dané zpravodajské aplikace.

Some web applications experience not only regular changes driven by daily seasonality but also sudden peaks in traffic. Modern applications run on a scalable cloud platform, but common reactive forms of scaling respond to congestion with latency, and predictive scaling can predict mainly daily curves rather than peaks. Analyze traffic data from the Novinky.cz server, which includes the anonymized ID of individual sources. Fix
possible anomalies in the data. Break the data down into individual time series of traffic to the given resources and expand the resources into two classes, ones that have existed for a long time and those that contain articles with a time-limited interest for readers. For data representing articles, describe how the time series behave from the beginning to the first maximum. Suggest a method for estimating the maximum of a newly created source in advance of its maximum, if possible from the data. Find out if this method would be beneficial for predictive scaling of servers providing news applications.

Plánované výstupy (konference a časopisy):

European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database ECML PKDD 2022
Nezávislá konference / Springer

Výsledek bude předán firmě, ze které pochází zkoumaná data.

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Učení pomocí metody gradient descent s naučenou délkou kroku a velikosti batch.**
Learning to optimize with gradient descent with learned update and batch size.

Mentor: Mgr. Petr Šimánek <simanpe2@fit.cvut.cz>

V současné době se intenzivně vyvíjí metody učení jak optimalizovat (meta-učení). Tyto metody se snaží vylepšit standardní metody gradinet descent pomocí rekurentních neurálních sítí (např.LSTM), které by se měly naučit aktualizovat váhy neuronové sítě. Existují přesvědčivé důkazy, že velikost batch ve vztahu k rychlosti učení je pro metody SGD a Adam velmi důležitá a tento vztah bychom se pokusili pomocí meta-učení naučit a využít. V této práci očekáváme použití standardního metod "Learning to optimze" k optimalizaci několika klasifikačních úloh (MNIST atd.) a navržení, implementaci, testování a analýzu metod pro učení i velikosti dávky. Implementujte a otestujte výše uvedené metody také s Legendre memory unit (LMU) namísto bežně používaného LSTM.

Learning to optimize methods (also known as meta-learning) are currently intensively developed. These methods try to improve a standard gradient descent methods by a recurrent neural network (e.g. LSTM) that should learn how to update weights of a neural network. There is a strong evidence that batch size in relation to learning rate is a very important for SGD and Adam methods. In this work we expect to apply some standard "learning to optimize" methods to optimize a few classification tasks (MNIST etc.) and suggest, implement, test and analyze methods for learning also the batch size together with the learning rate. Implement and test the above methods also with Legendre memory unit instead of standard LSTM.

Plánované výstupy (konference a časopisy):

International Joint Conference on Neural Networks - IJCNN 2022, International Neural Networks Society

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Automatické vyhodnocení testů manuální zručnosti podle videozáznamu**
Automatic evaluation of manual dexterity tests from video recording

Mentor: Ing. Tomáš Vondra, Ph.D. <vondrto6@fit.cvut.cz>

Na Klinice rehabilitačního lékařství 1.LF UK a VFN v Praze probíhá výzkum zaměřený na standardizované testy hodnotící funkcí horních končetin. Jedním z nich je Box and Block Test, kterým se hodnotí obratnost rukou pacientů. Test spočívá v co nejrychlejším přemísťování kostek z krabice přes přepážku do druhé krabice tak, aby se pacient konečky prstů držících přemisťovanou kostku dostal za přepážku, než kostku upustí. Výsledkem je počet kostek jednotlivě přemístěných v časovém limitu za dodržení instrukcí. Vyhodnocování se v současné době provádí v reálném čase s pacientem, s kontrolou druhým hodnotitelem podle videa. Vyhodnocení je velmi náročné na pozornost hodnotitelů a náchylné na chyby. Navrhněte způsob, jak automaticky vyhodnocovat tento test pomocí technik strojového vidění. Srovnejte výsledky s lidskými hodnotiteli. Práce je interdisciplinární; výsledek je možné uplatnit jak na konferencích na téma umělé inteligence, tak těch rehabilitačních. Výsledný program by se mohl využívat v klinické praxi rehabilitačních zařízení, která tento test běžně používají, a odstranil by potřebu druhého hodnotitele.

The Department of Rehabilitation Medicine of the First Faculty of Medicine, Charles University and the General Hospital in Prague is conducting research focused on standardized tests evaluating the function of the upper limbs. One of them is the Box and Block Test, which assesses the dexterity of patients' hands. The test consists of moving the dice from the box across the partition to the second box as quickly as possible so that the patient must get over the partition with the fingertips holding the moved dice before dropping the dice. The result is the number of dice individually moved within the time limit while following the instructions. The evaluation is currently performed in real time with the patient, with the reevaluation of a second evaluator using video. The evaluation is very demanding on the attention of evaluators and prone to errors. Suggest a way to automatically evaluate this test using machine vision techniques. Compare the results with human evaluators. The work is interdisciplinary; the result can be applied both at conferences on the topic of artificial intelligence and rehabilitation ones. The resulting program could be used in the clinical practice of rehabilitation facilities that commonly use this test, and would remove the need of the second evaluator.

Plánované výstupy (konference a časopisy):

European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database ECML PKDD 2022
Nezávislá konference / Springer

IEEE Congress on Evolutionary Computation CEC 2022
IEEE

International Society of Physical and Rehabilitation Medicine - World Congress ISPRM 2022
International Society of Physical and Rehabilitation Medicine

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Algoritmy elektronové krystalografie**
Algorithms of electron crystalography

Mentor: doc. Ing. Ivan Šimeček, Ph.D. <xsimecek@fit.cvut.cz>

Vstupními daty pro elektronovou krystalografii jsou kolekce bodů v 2D rovině, které zachycují difrakci elektronů na krystalické mřížce. Cílem je provést tzv. indexaci, to znamená stanovit parametry krystalu (max. 3 délky a max. úhly), jejichž fyzikální model nejlépe odpovídá naměřeným bodům. Popis a implementace algoritmu indexace by byl dobře publikovatelný jak v oblasti el. krystalografie tak v oblasti fyzikálních HPC výpočtů.

Plánované výstupy (konference a časopisy):

Journal of Applied Crystallography
International Union of Crystallography

Physical Communication
Elsevier

Zeitschrift für Kristallographie
De Gruyter

Téma je volné a je možné se na něj přihlásit.

Název zadání: **Target Set Selection in Graph Classes**

Mentor: RNDr. Dušan Knop, Ph.D. <knopdusa@fit.cvut.cz>

Target Set Selection (TSS) je praxí motivovaný problém modelující direct marketing či kupříkladu (dnes často zmiňované) šíření chorob v populaci. Grafový model (zavedený Kleibergem a Tardosovou) tohoto problému se struduje již řadu let a je dobré podotknout, že TSS je považován za velice těžký problém (je těžký už na subkubických grafech). Je tedy celkem s podivem, že studium tohoto problému dosud nezahrnovalo speciální grafové třídy (jako jsou Intervalové nebo Diskové grafy). Tomuto studiu bychom se v navrhovaném projektu rádi věnovali. Doufáme, že alespoň některé třídy těchto grafů umožní svou strukturou polynomiální algoritmus (alespoň pro tvz. Majoritní variantu TSS) a z pohledu parametrizované složitosti tak značně rozšíří počet tříd grafů vůči kterým lze tento problém studovat pro parametrizaci distance-to-triviality.

Plánované výstupy (konference a časopisy):

EUMAS: European Workshop on Multi-Agent Systems

WG: International Workshop on Graph-Theoretic Concepts in Computer Science

IWOCA: International Workshop on Combinatorial Algorithms

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **HW akcelerace digitálního podpisu nad Edwardsovou křivkou**
HW Acceleration of Digital Signature over Edwards Curve

Mentor: Dr.-Ing. Martin Novotný <novotnym@fit.cvut.cz>

Seznamte se s algoritmem digitálního podpisu. V prostředí SoC (System-on-a-Chip) navrhněte a implementujte hardwarový akcelerátor pro alespoň některé procedury digitálního podpisu. Hardwarový akcelerátor bude následně zkoumán z hlediska odolnosti proti útokům postranními kanály a budou pro něj navržena protiopatření proti těmto útokům. Zaměřte se na digitální podpis nad Edwardsovou křivkou. Očekávaným výstupem je publikace na mezinárodní konferenci nebo v časopise.

Plánované výstupy (konference a časopisy):

Euromicro Conference on Digital System Design, DSD 2022
Euromicro

Microprocessors and Microsystems, MICPRO
Elsevier

International Conference on Cryptographic Hardware and Embedded Systems, CHES
IACR

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Obohacování pojmů o významy s využitím Linked Data**

Mentor: Ing. Jaroslav Kuchař, Ph.D. <kuchajar@fit.cvut.cz>

Tématem je problematika práce s propojenými daty na webu (linked data) či znalostních bází a jejich využití pro obohacení dalších dat. V prostředí propojených dat existuje velké množství zdrojů, které se dají využít pro obohacení např. na úrovni přiřazení typů či kategorií k různým entitám. Tato práce je zaměřena na přiřazení definice/významu/výkladu či vysvětlení pro různé pojmy nacházející se v daném jazyce. Cílem je tedy navrhnout způsob využití propojených dat pro generování slovníků (ideálně pro různé jazykové varianty) zahrnující slova/pojmy a jejich definice, kategorizace, případně popularita a další metriky vyjadřující kvalitu či důležitost pojmu/definice. Předpokládáme využití přístupů z oblasti statistických metod, text mining, grafových algoritmů či grafových embeddingů.
Plánované výstupy jsou v podobě přístupů jak získat definice pojmů včetně různých metrik důležitosti. Výstupem může být i možnost zapojení výsledků zpátky do propojených dat a přispět tak zpětně do znalostních bází. Praktickým využitím může být také následné použití např. pro generování křížovek.
- Seznamte se s problematikou extrakce významů pojmů
- Proveďte rešerši přístupů s využitím Linked Data
- Navrhněte způsob pro získání významů pro pojmy (ideálně pro různé jazyky)
- Proveďte experimenty
- Vyhodnoťte kvalitu navržených přístupů

Téma bude řešeno ve spolupráci s Ing. Milan Dojčinovski, Ph.D.

Plánované výstupy (konference a časopisy):

CIKM: International Conference on Information and Knowledge Management
ACM

WCIDM: International Workshop on Computational Intelligence and Data Mining
ITAT

ESWC: Extended Semantic Web Conference; SEMANTiCS; LREC
Springer

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Testování robustnosti a bezpečnosti řídicích jednotek na sběrnici CAN**

Mentor: Ing. Vojtěch Miškovský, Ph.D. <miskovoj@fit.cvut.cz>

Testování robustnosti a bezpečnosti řídicích jednotek na sběrnici CAN

Cílem práce bude vyhodnocení bezpečnosti řídících jednotek automobilů využívajících komunikaci prostřednictvím sběrnice CAN. Výzkum bude probíhat na existujících řídících jednotkách reálně provozovaných v automobilech. Student si přístup k těmto jednotkám zařídí sám.

Student bude zkoumat tři oblasti zabezpečení řídících jednotek:
1) Kontrola reakcí jednotek na nestandardní situace, například posílání duplicitních zpráv, posílání poškozených zpráv, zahlcení sběrnice nebo připojení špatně nastaveného zařízení na sběrnici
2) Analýza implementace šifrování, například hledání možnosti neoprávněného vyčtení klíče nebo ovlivnění generátoru náhodnosti
3) Analýza postranních kanálů, konkrétně vyhodnocení informačního úniku a pokus o získání šifrovacího klíče pomocí existujících útoků, například DPA, CPA, MIA nebo TA

Výsledkem práce by pak mělo být komplexní vyhodnocení bezpečnosti existujících řídících jednotek a analýza možností jejich vylepšení pro zvýšení úrovně zabezpečení.

Plánované výstupy (konference a časopisy):

Design, Automation and Test in Europe Conference (DATE)

Microprocessors and Microsystems
Elsevier

Euromicro Conference on Digital System Design (DSD)

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Hardwarově-akcelerované kontejnery**
Hardware-accelerated containers

Mentor: Ing. Jan Fesl, Ph.D. <fesljan@fit.cvut.cz>

V oblasti cloud computing se používají aktuálně dva různé koncepty - virtualizace a kontejnerizace. Virtualizace je již maturovaná a hardwarově akcelerovaná, kontejnerizace je sice řešena pouze softwarově, nicméně oproti virtualizaci značně redukuje nutnou režii běhu.

Účelem projektu je navrhnout a zhodnotit koncept, který by umožňil zároveň využít přednosti obou způsobů. To znamená, jak prostřednictvím hardwarové akcelerace ještě dále zvýšit výkon kontejnerizace.

Schopnosti navrženého konceptu by měly být ověřeny prostřednictvím simulace popřípadě exaktním výpočtem.

In the field of cloud computing, two different concepts are currently used - virtualization and containerization. Virtualization is already mature and hardware-accelerated, although containerization is solved only by software, however, compared to virtualization, it significantly reduces the necessary overhead.

The purpose of the project is to design and evaluate a concept that would allow the simultaneous use of the advantages of both methods. This means how to further increase containerization performance through hardware acceleration.

The capabilities of the proposed concept should be verified through simulation or exact calculation.

Plánované výstupy (konference a časopisy):

International Journal of Cloud Computing
Springer Nature

ACS/IEEE International Conference on Computer Systems and Applications
IEEE

International Conference on Innovations for Community Services
Springer

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Zabezpečení postkvantového podpisového schéma Rainbow proti útokům postranními kanály**

Mentor: Ing. Petr Socha <sochapet@fit.cvut.cz>

Zatímco v odvětvích jako zdravotnictví a farmacie může kvantový počítač být počátkem zásadního průlomu, v myslích kryptografů představuje čtvrtého jezdce apokalypsy pro svou schopnost efektivní faktorizace čísel, jež ohrožuje zejména asymetrické kryptoalgoritmy jako RSA. Vzhledem k rychlému technologickému pokroku kvantového počítání je jednou ze současných priorit nalezení a co nejvčasnější nasazení alternativních (tzv. postkvantových) kryptografických algoritmů, což je také tématem právě probíhající soutěže vyhlášené Národním institutem pro standardy a technologii Spojených států (NIST). Jedním z finálních kandidátů je podpisové schéma Rainbow, založené na NP-těžkém problému řešení soustav kvadratických rovnic nad konečným tělesem („multivariate quadratic problem“).
Tato práce navazuje na loňský úspěšný projekt [1], jehož výsledkem byl úspěšný útok na 32bitovou referenční implementaci Rainbow, dodanou autory algoritmu do soutěže NIST. Cílem této práce je návrh protiopatření proti takovému útoku, založeného na principu maskování. Výstupem může být jedno nebo více maskovacích schémat, založených na principu aditivního nebo multiplikativního maskování, a randomizujících vstupní data nebo soukromý klíč. Navržená opatření by měla být ověřena a srovnána jak experimentálně, tak na základě formálně popsaných vlastností. Student bude při řešení využívat zázemí Laboratoře vestavné bezpečnosti při KČN.
[1] Pokorný, D., Socha, P., & Novotný, M. (2021, February). Side-channel attack on Rainbow post-quantum signature. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE.

Plánované výstupy (konference a časopisy):

Cryptography (journal)
MDPI

Smart Card Research and Advanced Application Conference (CARDIS)
Universität zu Lübeck in Lübeck (proceedings Springer LNCS)

Side-channel analysis (SCA) and implementation attacks (COSADE)
Università della Svizzera italiana (proceedings Springer LNCS)

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Softwarové modely hardwarových implementací šifer, zejména za použití metody Dummy Rounds**
Software models of crypto implementations in hardware, especially with Dummy Rounds

Mentor: Ing. Stanislav Jeřábek <jerabst1@fit.cvut.cz>

Student bude mít za úkol zkoumat vztah mezi vybranými parametry v softwarovém modelu (primárně Hammingova vzdálenost mezivýsledků šifrování) a empiricky zjištěnými výsledky (primárně naměřená spotřeba) hardwarové implementace šifrovacích algoritmů.
Cílem je potvrdit či vyvrátit hypotézu o silné korelaci spotřeby obvodu s Hammingovou vzdáleností hodnot v klopných obvodech rundovních šifer, a to konkrétně pro metodu Dummy Rounds a šifru Present. Potvrzení hypotézy pro daný případ nebo nalezení jiné korelace by umožnilo zrychlení dalšího výzkumu Dummy Rounds v podobě měření na snáze modifikovatelném softwarovém modelu.

The student will have to investigate the relationship between selected parameters in the software model (essentially Hamming distance of intermediate encryption results) and empiric results (measured consumption) of the hardware implementation of encryption algorithms.
The aim is to confirm or refute the hypothesis of a strong circuit power consumption and intermediate flip-flop values Hamming distance correlation for hardware round ciphers implementation, specifically for the Dummy Rounds method and the Present cipher. Confirming the hypothesis for a given case or finding another correlation would speed up further research on Dummy Rounds in the form of measurements on a more easily modifiable software model.

Plánované výstupy (konference a časopisy):

Euromicro Conference on Digital Systems Design, DSD
Euromicro

International Symposium on Design and Diagnostics of Electronic Circuits and Systems, DDECS
Evropské univerzity

Mediterranean Conference on Embedded Computing, MECO
Montenegrin Association for New Technologies (MANT) a další