FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Výzkumné léto na FIT 2020 (VýLeT 2020): 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 2020.

Stručné informace k přihlášení do programu VýLeT 2020

Program má za cíl podpořit nadané studenty bakalářských a magisterských programů, zapojit je do vědecko-výzkumných aktivit na fakultě a vést je k samostatné vědecké práci a publikační činnosti.

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, do které dané téma spadá, zašlete na vylet@fit.cvut.cz e-mail s dotazem, zda je možné vypsat další zadání z dané oblasti. Do předmětu e-mailu uveďte "VýLeT 2020 – dotaz na rezervované téma". Komise programu VýLeT 2020 kontaktuje mentora a pokud mentor bude souhlasit s vypsáním nového podobného tématu z dané oblasti, téma bude doplněno do seznamu výzkumných témat programu Výlet 2020.

(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?

(a) Přihlášení probíhá emailem na vylet@fit.cvut.cz s předmětem „VýLeT 2020 - přihláška". Zájemce v emailu pošle

(1) celé jméno,

(2) uživatelské jméno ČVUT,

(3) stručný profesní životopis,

(4) popis svých studijních plánů na FIT (zda plánuje studium končit v roce 2020 nebo 2021, zda bude na FIT pokračovat, od kdy a v jaké formě),

(5) vybraná témata projektů,

(6) stručné průvodní prohlášení k výběru tématu obsahující popis vlastní motivace a návrh plánu práce na tématu (nepovinné), preferovaně formou přílohy v rozsahu 1 až 2 odstavce na jedno vybrané výzkumné téma.

Do kdy je třeba se přihlásit?

Je třeba se přihlásit v lhůtě určené pro přihlašování. Tato lhůta končí **31.5. 2020.**

Komise programu VýLeT 2020

doc. Ing. Štěpán Starosta, Ph.D
doc. Ing. Pavel Kordík, Ph.D
Mgr. Ing. Ladislava Smítková Janků, Ph.D.
doc. Ing. Jan Janoušek, Ph.D.
doc. Ing. Hana Kubátová, CSc.

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 2020 naleznete v dokumentu **„Výzkumné léto na FIT 2020 (VýLeT 2020): Program podpory letního studentského výzkumu na FIT ČVUT – Propozice.“**

Vypsaná témata

Číslo: 001

Název tématu: **Homomorfní šifrování s podporou FPGA**
FPGA-supported Homomorphic Encryption

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

Seznamte se s algoritmem TFHE (Torus Fully Homomorhic Encryption). Vzhledem ke složitosti algoritmu neumožňují současné prostředky jeho softwarovou implementaci, která by dosahovala přijatelného stupně bezpečnosti a zároveň byla prakticky použitelná (tj. byla dostatečně rychlá). Prozkoumejte, jakým způsobem je možné využít prostředky programovatelého hardware (FPGA) při implementaci tohoto algoritmu. Algoritmus implementujte v FPGA. Prozkoumejte prostorovou a časovou náročnost algoritmu implementovaného v soudobém FPGA. Dále prozkoumejte, kolik úrovní rozlišení je vhodné použít. Shrňte zjištěné skutečnosti v konferenčním nebo časopiseckém článku.

Study the TFHE (Torus Fully Homomorhic Encryption) algorithm. The complexity of the algorithm prevents its practical softwafre implementation with contemporary resources. Explore the possibilities to exploit the resources available in contemporary configurable hardware (FPGA). Implement the algorithm in FPGA. Explore the space and time complexity of the algorithm implemented in contemporary FPGA. Further, investigate how many levels of resolution shall be used. Summarize all findings in conference or journal paper.

Plánované výstupy (konference a časopisy):

International Conference on Cryptographic Hardware and Embedded Systems, CHES, https://ches.iacr.org/
IACR - International Association for Cryptologic Research, https://iacr.org/
Euromicro Conference on Digital System Design

Téma je rezervováno pro konkrétního studenta.

Číslo: 002

Název tématu: **Adaptace modelů strojového učení pro nová data**
Adaptation of machine learning models for new data

Mentor: Martin Holeňa <holenmar@fit.cvut.cz>

Díky velké popularitě, kterou v posledních 5-10 letech zažívají hluboké neuronové sítě, se do širšího povědomí dostala i možnost adaptovat již naučenou síť pro data nepříliš odlišná od těch, na kterých se učila. Tuto schopnost lze vysvětlit tím, že při učení se v síti zakóduje znalost rozdělení pravděpodobnosti, které generovalo trénovací data. Tato znalost platí do značné míry i pro podobná rozdělení a ke korekci jejího zakódování stačí mnohem méně dat. V této souvislosti se používají pojmy přenos znalostí (knowledge transfer) a učení přenosem (transfer learning). Ty se však netýkají jen hlubokých neuronových sítí, ale i dalších metod strojového učení, a souvisí nejenom s hlubokým supervizovaným učením, ale i se semisupervizovaným učením a s aktivním učením.
Student se seznámí s nejúspěšnějšími obecnými algoritmy pro přenos znalostí v literatuře dodané vedoucím práce a 1-2 z nich porovná teoreticky a na datech s algoritmem navrženým a implementovaným na Ústavu formální a aplikované lingvistiky (UFAL) specificky pro data z oblasti strojového překladu. Přitom k porovnání na datech použije také data z oblasti strojového překladu, s cílem vyhodnotit, o kolik úspěšnější je algoritmus zkonstruovaný specificky pro tato data ve srovnání s obecnými algoritmy pro přenos znalostí. Může též zkusit hybridizovat specifický algoritmus s některými prvky srovnávaných obecných algoritmů, pokud se bude domnívat, že by se tím úspěšnost specifického algoritmu mohla dále zvýšit.

Plánované výstupy (konference a časopisy):

WCIDM 2021: 9th International Workshop on Computational Intelligence and Data Minig
Údaje k WCIDM 2021 ještě nejsou známy, předpokládám stav jako u WCIDM 2020, viz http://itat.ics.upjs.sk/index.php?id=ws/CIDM

Téma je rezervováno pro konkrétního studenta.

Číslo: 003

Název tématu: **Parametrizované algoritmy pro strukturální parametr shrub-depth**

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

Shrub-depth je relativně obecný strukturální parametr, který (například):

- je-li omezený, pak je omezená kliková šířka,
- je neporovnatelný se stromovou šířkou a
- je-li omezená stromová hloubka (treedepth), pak je omezený i shrub-depth.

Bohužel je definice shrub-depth do značné míry technická (proto ji zde neuvádíme) a tak nám není známo mnoho alegoritmů využívajících tento parametr.
Cílem práce je zaměřit se speciálně na problémy, u kterých bylo prokázáno, že existuje efektivní parameterizovaný algoritmus (problém náleží do třídy FPT) vzhledem ke stromové hloubce, ale které jsou těžké pro stromovou šířku. Zde se domníváme, že by jak algoritmické tak negativní výsledky znamenaly pokrok v poznání tohoto (velmi obecného) strukturálního parametru a jeho větší popularizaci ve vědecké komunitě. Jako příklad takového problémů uveďme kupříkladu tzv. L-omezený řez, kde je cílem naleznout co nejmenší množinu hran daného grafu takovou, že po jejím odebrání neexistuje cesta kratší než L mezi dvěma zadanými vrcholy. V práci se budeme zabývat timto, ale i podobnými problémy (s podobnými algoritmickými vlastnostmi).

Plánované výstupy (konference a časopisy):

konference - International Symposium on Parameterized and Exact Computation IPEC / Information Processing Letters nebo Theoretical Computer Science

Téma je rezervováno pro konkrétního studenta.

Číslo: 004

Název tématu: **Jádro problému stabilního párování v instancích založených na různorodosti**

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

Problém stabilního párování v instancích založených na různorodosti je následující problém. Mějme pevné číslo k a n agentů na vstupu (n je dělitelné k). Každý agent má přiřazenou jednu barvu - pro začátek budeme uvažovat dvě barvy, řekněme modrou a červenou. Našim úkolem pak je rozdělit agenty do (disjunktních) k-tic -- tedy zobecněné párování. Každý agent má ale navíc na vstupu své preference (lineární uspořádání) o "barevnosti k-tice". Pro příklad uvažme k=3: jeden červený agent prefereuje 3/3 červených agentů v k-tici, poté 2/3 červených agentů a nakonec 1/3. Rozdělení do k-tic je **stabilní**, pokud neexistuje (nová) k-tice agentů, kteří, pokud by se odtrhli a zformovali tuto k-tici budou striktně spokojenější.
Je známo, že instance s k=2 mají neprázdné jádro. Tedy pro každý vstup existuje přiřazení do stabilních k-tic. Poznamenejme, že tento výsledek je konstruktivní - je tedy znám algoritmus. Dále se ví, že pro k=4 existují instance, které nemají stabilní párování (tedy mají prázdné jádro). My se chceme zabývat připadem k=3, kde není známo zda je jádro prázdné či nikoliv. Konkrétně budeme cílit buď na algoritmus, který vždy nalezne stabilní párování nebo příklad vstupu bez stabilního párování. Zároveň s tímto bychom se zabývali rozšířením výše popsaného modelu pro tři barvy se speciálním zaměřením na k=2 a k=3.

Plánované výstupy (konference a časopisy):

Operations Research Letters ORL (popřípadě konference EUMAS)
Elsevier

Téma je rezervováno pro konkrétního studenta.

Číslo: 005

Název tématu: **Vliv syntézních parametrů na odolnost vůči útokům postranními kanály**
Influence of synthesis parameters on vulnerability to side-channel attacks

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

Prozkoumejte vliv symtézních parametrů na odolnost vůči útokům postranními kanály. Zaměřte se na syntézy do programovatelných hradlových polí (FPGA). Sesyntetizujte a implementujte totožný VHDL popis Vámi zvolené šifry (např. AES) do FPGA za různých nastavení syntézních parametrů. Zanalyzujte, která nastavení syntéznách parametrů vyústila do totožných a která do rozdílných implementací. Porovnejte různé implementace pomocí Welchova t-testu. Pokud to bude možné, pokuste se okomentovat vliv jednotlivých parametrů (nebo jejich ombinací) na odolnost vůči útokům postranními kanály. Výsledky Vašeho výzkumu by měly být publikovány na mezinárnodní konferenci nebo časopise.

Student pracoval na tématu již v rámci loňského VýLetu. Vzhledem k náročnosti tématu pokračuje na práci i letos.

Explore the influence of synthesis parameters setup on vulnerability to side-channel attacks. Focus on synthesis to field-programmable gate arrays (FPGAs). Identical VHDL description of a chosen cipher (e.g. AES) synthesize and implement in FPGA under various combinations of synthesis parameters. Analyze what combinations of synthesis parameters resulted in identical and what in different implementations. Analyze and compare different implementations via Welch t-test. If possible, discuss the influence of sole parameters or their combinations on vulnerability to side-channel attacks. Results of your research shall be published at international conference or journal.

Plánované výstupy (konference a časopisy):

Journal of Cryptology
IACR, International Association for Cryptologic Research, https://iacr.org/
CHES, Conference on Cryptographic Hardware and Embedded Systems, https://ches.iacr.org/

Téma je rezervováno pro konkrétního studenta.

Číslo: 006

Název tématu: **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):

Design, Automation and Test in Europe (DATE) - A*
IEEE/ACM
24th IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS) - A

Téma je volné a je možné se na něj přihlásit.

Číslo: 007

Název tématu: **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):

Design, Automation and Test in Europe (DATE) - A*
IEEE/ACM
24th IEEE Design and Diagnostics of Electronic Circuits and Systems (DDECS) - A

Téma je volné a je možné se na něj přihlásit.

Číslo: 008

Název tématu: **Dokreslování obrázků pomocí generativních adversariálních sítí Image Inpainting Using GANs**

Mentor: Ing. Magda Friedjungová <friedmag@fit.cvut.cz>
Mentor specialista: Ing. Daniel Vašata, Ph.D.

Doplňování (dokreslování) chybějících částí obrázků je velmi zajímavou úlohou ve strojovém učení. V dosavadních výzkumech bylo ukázáno, že lze tuto úlohu řešit i pomocí generativních adversariálních sítí (GAN), které se v poslední době těší velkému zájmu. Cílem tohoto výzkumu je blíže prozkoumat možnosti řešení doplňování obrázků pomocí GANů a námi navrženého WGAINu se zaměřením se na různé scénáře trénování těchto sítí.

1. Proveďte rešerši algoritmů pro dokreslování obrázků se zaměřením na konvoluční GANy.
2. Dle dvou vybraných článků reimplementujte prezentované algoritmy. Srovnejte jejich úspěšnost se dalšími metodami strojového učení. Demonstrujte výsledky na veřejně dostupných datasetech.
3. Proveďte experimenty s různým nastavením masky - pro případ, že chybí geometrický tvar nebo náhodné pixely. Chybějící data uvažujte v rozsahu od 10 do 50%.
4. Vysvětlete dosažené výsledky a popište omezení jednotlivých algoritmů.
5. Experimentálně srovnejte dosažené výsledky s WGAIN, který je představen v článku "Missing Features Reconstruction Using a Wasserstein Generative Adversarial Imputation Network".
6. Zaměřte se na proces trénování. Experimentálně analyzujte chování různých modelů v různých scénářích dokreslování obrázků.

Repairing of damaged images has been an important topic in machine learning for a long time. Generative adversarial networks (GANs) have proved to be a suitable tool to repair images and fill the missing part with created "content" (context encoder).

1. Survey state of the art algorithms for image inpainting focused on convolutional generative adversarial networks.
2. Implement at least one surveyed algorithm using generative adversarial learning. Compare its performance to different machine learning approaches on publicly accessible image datasets.
3. Test these models and experiment with different region mask settings - center, corners, and random noise in range from 10% to 50% of the images.
4. Examine particular errors and describe the limitations of current algorithms.
5. Experimentally compare achieved results with WGAIN proposed in the preprint of "Missing Features Reconstruction Using a Wasserstein Generative Adversarial Imputation Network" paper.
6. Focus on the training process. Experimentally analyze training of different models used to solve different scenarios of image inpainting.

Plánované výstupy (konference a časopisy):

INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE 2021, ICCS 2021
Není doposud stanoven, viz www.iccs-meeting.org
European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning 2021, ESANN 2021

Téma je rezervováno pro konkrétního studenta.

Číslo: 009

Název tématu: **Balancování dat pomocí generativních modelů**
Deep Generative Models for Balancing

Mentor: Ing. Magda Friedjungová <friedmag@fit.cvut.cz>
Mentor specialista: Ing. Daniel Vašata, Ph.D.

Nevyvážená data mohou být velkým problémem při trénování klasifikačních modelů kvůli nerovnoměrném rozložení tříd. Jednou z možností, jak tento problém vyřešit, je vygenerovat syntetická data pro vyvážení datasetu, tzn. využít technik augmentace dat. V současné době tato úloha může být řešena i pomocí generativních adversariálních sítí (GAN), které jsou trénovány tak, aby vytvářely nová syntetická data co nejvíce podobná datům originálním.

1. Proveďte rešerši stávajících metod pro augmentaci dat.
2. Dle dvou vybraných článků reimplementujte prezentované algoritmy. Srovnejte jejich úspěšnost s dalšími metodami v oblasti augmentace dat (např. autoenkodéry, geometrické transformace apod.). Demonstrujte výsledky na veřejně dostupných datasetech.
3. Rozšiřte experimenty o syntetické obrázky z latentního prostoru, které získáte pomocí metod založených na interpolaci.
4. Uvažujte datasety nevyvážené v různých poměrech. Pomocí klasifikačních modelů srovnejte metody pro augmentaci dat.
5. Vysvětlete dosažené výsledky a popište omezení zvolených metod.

Imbalanced data typically refers to a problem with classification tasks where the classes are not represented equally. One of the possible ways how to solve this problem is to generate artificial training data to balance the dataset, i.e. use data augmentation techniques. Nowadays, this task can be solved via generative adversarial network (GAN) where one network is trained to generate real-looking training data (the generator), and the other is trained to distinguish artificial-looking data (the discriminator). Both try to beat the other and at the end of the training process, the generator network can be used for the purpose of new training datasets.

1. Survey common and state-of-the-art algorithms for data augmentation.
2. Implement at least two surveyed algorithms using GANs and compare their performance to different approaches used in the data augmentation domain (e.g. variational autoencoders and common techniques such as rotation, shift, etc.) on publicly accessible image datasets.
3. Extend provided experiments by artificial images acquired in latent representation using techniques based on interpolation.
4. Consider (synthetically) imbalanced datasets in different ratio. Comparison of data augmentation methods will be done using classification models learned on both, original (balanced) and synthetically imbalanced data, and the performance of methods will be compared to both.

5. Examine particular errors and describe the limitations of the algorithms used.

Plánované výstupy (konference a časopisy):

INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE 2021, ICCS 2021
Není doposud stanoven, viz www.iccs-meeting.org
European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning 2021, ESANN 2021

Téma je rezervováno pro konkrétního studenta.

Číslo: 010

Název tématu: **Rešerše zálohovaných vestavných systémů**
Analysis of backuped embedded systems

Mentor: Ing. Matěj Bartík <bartimat@fit.cvut.cz>

Je potřeba provést porovnání běžného systému pracující jako "duplex" se systémem hybridního duplexu, u kterého jsou nekritické části systému sdílené.

A comparisson between regular and hybrid "duplex" system, where non-critical parts are shared among both systems.

Plánované výstupy (konference a časopisy):

IEEE Access, IEEE ReConFig, ACM FPGA, DATE

Téma je volné a je možné se na něj přihlásit.

Číslo: 011

Název tématu: **Spektrální analýza Schrödingerových operátorů na rovinných oblastech**
Spectral analysis of Schrödinger operators on planar domains

Mentor: Ing. Tomáš Kalvoda, Ph.D. <kalvotom@fit.cvut.cz>

Spektrální analýza, tedy hledání vlastních funkcí a vlastních vektorů, parciálních diferenciálních operátorů je úloha zajímavá nejen z matematického, ale i z fyzikálního hlediska a s aplikacemi i ve výpočetní geometrii při rozpoznávání tvarů.

Cílem tohoto projektu je vytvořit robustní, snadno použitelný a udržovatelný nástroj umožňující uživateli zadat rovinnou oblast a Schrödingerův operátor (Laplaceův operátor plus potenciál). Výstupem výpočtu pak bude jistá část spektra (množiny vlastních čísel) a příslušných vlastních vektorů. Tyto spektrální objekty hrají důležitou roli v kvantové fyzice, při modelování vedení tepla, nebo ve zmíněném rozpoznávání tvarů (například spektrum je isometricky invariantní). Dále existuje několik hypotéz o vlastnostech tzv. nodálních čar (nulové křivky vlastních funkcí) v závislosti na tvaru uvažované oblasti. Ty lze experimentálně ověřovat, případně se pokoušet je vyvracet. Navíc lze vlastní funkce atraktivně vizualizovat.

Uvedený problém samozřejmě, vzhledem k své důležitosti, není nový. V drtivé většině případů ovšem není analyticky řešitelný a je potřeba se uchýlit k numerickým výpočtům. Bohužel však neexistuje open-source nástroj, který by navíc byl uživatelsky přívětivý a umožňoval uživateli snadno prozkoumávat spektrum a vlastní funkce uvažovaného operátoru.

Prvním krokem k řešení tohoto projektu by bylo (pod vedením mentora) seznámení se s potřebnými matematickými pojmy a metodami výpočtu numerických aproximací vlastních čísel a vektorů parciálních diferenciálních operátorů. Tématicky jde o úlohy numerické lineární algebry a/nebo obecné optimalizační úlohy (typicky kvadratického programování) často využívající nástroje výpočetní geometrie. Druhým krokem by byla implementace uvažovaného programu v moderním prostředí Julia určeném pro věděcké výpočty, jehož výhodou je rychlost, čitelnost kódu a v neposlední řadě dostupnost celé řady nástrojů využitelných k řešení zde popsaného problému.

Primárním cílem je vytvoření zmíněného open-source programu. V případě kvalitního výsledku lze uvažovat i o jeho propagaci formou publikace v uvedených časopisech. Své uživatele by si program jistě našel. Uvedená verze problému je základní, alternativně lze uvažovat operátory (například Laplace-Beltramiho) na plochách v trojrozměrném prostoru, nebo nad operátory s komplexními potenciály majícími reálné spektrum.

Plánované výstupy (konference a časopisy):

Journal of Open Source Software + JOSS
https://joss.theoj.org
SoftwareX + ?

Téma je volné a je možné se na něj přihlásit.

Číslo: 012

Název tématu: **Struktura pevných bodů AR morfismů**

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 poslnoupnnosti, 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. Ve zkoumání velmi pomůže experimentování za pomocí počítače.

Plánované výstupy (konference a časopisy):

Theoretical Computer Science
Elsevier

Téma je volné a je možné se na něj přihlásit.

Číslo: 013

Název tématu: **Multi-agentní hledání cest**
Multi-agent Path Finding

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

Úkolem studenta bude ve spolupráci s mentorem identifikovat zajímavý podproblém v rámci optimálních řešících algoritmů pro multi-agentní hledání cest (MAPF). Nabízí se například balancování míry lenosti/snaživosti v neúplných kódováních problému MAPF jako výrokové splnitelnosti (SAT).

The task for a student is to identify interesting sub-problems in optimal algorithms for multi-agent path finding (MAPF). The problem identification/specification will be done in cooperation with the mentor. The example of a suitable problem is balacing of laziness/eagerness of incomplete propositional encodings of MAPF as propositional satisfiability (SAT).

Plánované výstupy (konference a časopisy):

ICTAI 2020: International Conference on Tools with Artificial Intelligence
IEEE
ICRA 2021: International Conference on Robotics and Automation

Téma je volné a je možné se na něj přihlásit.

Číslo: 014

Název tématu: **Útoky vyšších řádů na hardwarové kryptografické implementace s ochranami proti útokům postranními kanály**
Higher-Order Attacks on Hardware Cryptographic Implementations with Side-Channel Countermeasures

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

Útoky postranními kanály představují významnou hrozbu pro kryptografické implementace napříč celým spektrem informačních technologií, včetně klasických počítačů a vestavných systémů. Tyto útoky, stejně jako ochrany proti takovým útokům, jsou středem zájmu mnoha současných výzkumných týmů; v prostředí IoT a chytrých měst totiž představuje jejich zneužití kritický problém. Implementace zabezpečené pomocí maskování (jehož vlastnosti jsou formálně dokázané) sice odolávají klasickým útokům, jsou ovšem prolomitelné pomocí tzv. útoků vyšších řádů. Jejich výpočetní složitost oproti klasickým útokům roste typicky exponenciálně, patrně díky efektu „zesílení šumu". Současné práce tedy naznačují, že právě dostatečná hladina šumu je kritickou vlastností při zabezpečení implementací prostřednictvím maskování. V současnosti také není dostatečně prozkoumaný vliv výrobní technologie na úroveň šumu a úspěšnost takových útoků. Cílem této práce je porovnání reálné složitosti útoku na několik implementací zvolené symetrické šifry (AES/Rijndael, PRESENT,...), a to bez ochran proti útokům, a se škálovatelnými state-of-the-art ochranami (Threshold Implementation nebo Domain Oriented Masking), na nám dostupných FPGA čipech (Spartan 6, tj. 45nm, Artix 7, tj. 28nm). Pro porovnání složitosti útoku by měla být použita validní experimentální metodologie (např. SNR + guessing entropy). Výstup práce povede k lepšímu pochopení reálné složitosti útoků vyšších řádů a její závislosti na naměřeném šumu, a umožní tím řádné srovnání reálné bezpečnosti protiopatření v poměru k požadavkům na plochu a latenci. Student bude při řešení využívat zázemí Laboratoře vestavné bezpečnosti při KČN.

Plánované výstupy (konference a časopisy):

International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)
Pořadatel ročníku zatím neznámý, proceedings Springer LNCS
Euromicro Conference on Digital System Design – Architecture and Hardware for Security Applications (DSD-AHSA)

Téma je rezervováno pro konkrétního studenta.

Číslo: 015

Název tématu: **Analýza postranních kanálů implementace postkvantového podpisového schéma Rainbow: útok a protiopatření**
Rainbow Post-Quantum Signature Scheme Side-Channel Analysis: Attack and Countermeasures

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 aktuálně postupivších kandidátů je podpisové schéma Rainbow, založené na NP-těžkém problému řešení soustav kvadratických rovnic nad konečným tělesem („multivariate quadratic problem“). Implementace Rainbow, podobně jako jiné kryptografické implementace, je ve své naivní podobně zranitelná vůči útokům postranními kanály, jak bylo v nedávné době prezentováno na zcela naivní 8-bitové implementaci. Cílem této práce je mj. zaútočit skrze postranní kanály na referenční 32-bitovou implementaci Rainbow, dodanou autory algoritmu do soutěže NIST, tj. extrahovat z mikročipu soukromý klíč a popsat útok. Dále je cílem práce navrhnout protiopatření proti útokům postranními kanály aplikovatelné na podpisové schéma Rainbow, implementovat je a vyhodnotit úspěšnost protiopatření s použitím validní experimentální metodologie (např. specifický nebo nespecifický t-test, nebo analýza vzájemné informace). Výstup práce může, krom teoretických poznatků, posloužit jako vodítko v současném rozhodovacím procesu NIST. Popsaný útok i protiopatření by mělo být navíc snadno aplikovatelné na další algoritmy, které jsou podobně jako Rainbow odvozené od schématu Unbalanced Oil and Vinegar, jako například LUOV, další z kandidátů NIST. Student bude při řešení využívat zázemí Laboratoře vestavné bezpečnosti při KČN.

Plánované výstupy (konference a časopisy):

Conference on Cryptographic Hardware and Embedded Systems (CHES)
IACR & Springer
International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)

Téma je rezervováno pro konkrétního studenta.

Číslo: 016

Název tématu: **Implementace postkvantového podpisového schéma Rainbow na SoC FPGA**
Acceleration of Rainbow Post-Quantum Signature Scheme on SoC FPGA

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 aktuálně postupivších kandidátů je podpisové schéma Rainbow, založené na NP-těžkém problému řešení soustav kvadratických rovnic nad konečným tělesem („multivariate quadratic problem"). Cílem této práce je implementace podpisového schéma Rainbow na FPGA. Výsledkem by měl být IP blok, připojitelný např. prostřednictvím sběrnice AXI, který může sloužit jako akcelerátor ve společném hardware/software návrhu (hw/sw co-design) v systému na čipu (SoC). Výstup práce bude jednou z velmi málo doposud dostupných hardwarových implementací Rainbow a poskytne tak prostor pro nezávislé srovnání. Implementace v podobě SoC akcelerátoru bude za současných podmínek zcela unikátní. Práce poslouží také jako odrazový můstek pro související výzkum bezpečnosti postranních kanálů hardwarové implementace Rainbow. Výstup může také sloužit jako vodítko v rozhodovacím procesu NIST. Student bude při řešení využívat zázemí Laboratoře vestavné bezpečnosti při KČN.

Plánované výstupy (konference a časopisy):

Conference on Cryptographic Hardware and Embedded Systems (CHES)
IACR & Springer
International Conference on Reconfigurable Computing and FPGAs (ReConFig)

Téma je rezervováno pro konkrétního studenta.

Číslo: 017

Název tématu: **Rozpoznávání textu v historických archiváliích ze 17.-19. století**
Recognition of text in historical archival records from 17th-19th century

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

1. Vytvořte webový portál pro testování úspěšnosti algoritmů pro optické rozpoznávání znaků (OCR) nad historickými písemnými materiály z období 17. až 19. století z Čech, Moravy a Slezka. V archiváliích lze počítat se staročeštinou a různými nářečími.
2. Vytvořte dataset pro testování algoritmů na základě dat z digitálního archívu Národní knihovny ČR.
3. Vyhledejte a zprovozněte různé implementace různých relevantních algoritmů pro optické rozpoznávání textu. Umožněte běh s různými parametry podle typu archiválie.
4. Proveďte srovnání všech algoritmů na vytvořeném datasetu. Prostředí pro testování je třeba vytvořit tak, aby bylo možno jednoduše přidávat nové algoritmy, testovat je a prezentovat jejich výsledky.

1. Create a web portal to test the success of optical character recognition (OCR) algorithms using historical written materials from the 17th to 19th centuries from Bohemia, Moravia and Silesia. In these materials, old Czech language and many different dialects are used.
2. Create a dataset for testing algorithms based on data from the digital archive of the National Library of the Czech Republic.
3. Find and run different implementations of different relevant optical text recognition algorithms. Allow running with different parameters depending on the type of archive materials.
4. Compare all algorithms on the created dataset. The testing environment needs to be easy to use, so new algorithms can be easily added, tested and their results presented.

Plánované výstupy (konference a časopisy):

INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE 2021, ICCS 2021 ICCS
European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning 2021, ESANN 2021

Téma je volné a je možné se na něj přihlásit.

Číslo: 018

Název tématu: **Návrh vybavení interiéru nábytkem pomocí metod umělé inteligence**

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

Ve spolupráci s mentorem navrhněte vhodnou reprezentaci pro popis prvků vybavení interiéru a pro popis podmínek jejich umístění a vzájemných vazeb a navrhněte algoritmus pro generování podmínek pro rozmístění prvků vybavení interiéru z údajů získaných z databáze návrhů existujících interiérů. Implementujte rozhraní pro zadání podmínek uživatele na prvky vybavení interiéru. Navrhněte algoritmus pro automatické generování návrhu vybavení interiéru pro náhodně generované půdorysy s různým počtem místností.

Plánované výstupy (konference a časopisy):

IEA/AIE: Industrial and Engineering Applications of Artificial Intelligence and Expert Systems IEA/ AIE (Core Rank B)
International Society of Applied Intelligence (ISAI)
International Conference on Tools with Artificial Intelligence - ICTAI (Core Rank B)

Téma je volné a je možné se na něj přihlásit.

Číslo: 019

Název tématu: **Rekomendační systémy pro predikci dalšího nákupu**
Recommender systems predicting next shopping cart

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

Úspěšní účastníci soutěže v rámci předmětu ADM https://courses.fit.cvut.cz/MI-ADM/competition/index.html, kteří se dobře umístí, a mají chuť to dotáhnout do článku.

Based on datasets available https://courses.fit.cvut.cz/MI-ADM/competition/index.html experiment with novel approaches to shopping cart prediction and publish comparison of algorithms on this unique dataset.

Plánované výstupy (konference a časopisy):

RecSYS 2021
ACM
WCCI 2021

Téma je volné a je možné se na něj přihlásit.

Číslo: 020

Název tématu: **Automatický „profiling“ expertů a organizaci**
Automatic "profiling" of experts and organisation

Mentor: Ing. Stanislav Kuznetsov <kuznesta@fit.cvut.cz>

Ve své disertační práce se zabývám řešením cold start problému v rekomendačních systémech pomocí ontologii. Moje data hlavně představuji výsledky výzkumu (Patenty, Publikace, Projekty), který získávám z různých zdrojů (starfos.tacr.cz, skcris.sk, polon.nauka.gov.pl). Všechno jsou to reálná data (ne syntetická) a tudíž obsahuji velké množství „bordelu“.
V tomto projektu bych se chtěl se studentem zaměřit na tzv. automatický „profiling“ expertů a organizaci. Bude se jednat o kombinaci metod text miningu s pravděpodobnostním modelem, kdy od určité hranice pravděpodobnosti nám dokáže model vrátit doporučení o tom, že 2 záznamy jsou si podobný a následně je spojit.

In my dissertation, I'm working at the cold start problem in the recommendation systems through ontology. My data mainly represents the results of research (Patents, Publications, Projects), which I get from various sources (starfos.tacr.cz, skcris.sk, polon.nauka.gov.pl). These are all real data (not synthetic), and therefore contains a large amount of "mess".
In this project, I would like to focus on automatic "profiling" of experts and organisation. It will be a combination of text-mining methods with a probability model where, from a particular probability threshold, the model can return a recommendation that two records are similar to each other and then automatically claim them.

Plánované výstupy (konference a časopisy):

Výsledkem projektu bude universální program, který dokáže automatický čistit data o výzkumu. Tento program můžeme nabízet jako open source.

Téma je volné a je možné se na něj přihlásit.

Číslo: 021

Název tématu: **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: doc. Ing. Pavel Kordík, Ph.D. <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):

WCCI 2021
IEEE

Téma je volné a je možné se na něj přihlásit.

Číslo: 022

Název tématu: **Detekce útoků v Active Directory prostředí s využitím Machine Learning technik**
Detection of cyber attacks in Active Directory environment using Machine Larning Techniques

Mentor: Buchovecká, Simona, Ing. <buchosim@fit.cvut.cz>

Active Directory je dnes rozšířenou technologií využívanou v mnoha organizacích, a tradiční, dnes využívaný, "signature-based" přístup vykazuje velké množství falešných poplachů. Využití pokročilých metod, jako např. technik Machine Learningu by mohlo přispět k zpřesnění detekcí.

Zadání navazuje na téma z Výletu 2019. V minulém roce se student zaměřil na specifický útok v prostředí Active Directory - Kerberoasting. Výstupy práce byly publikované na konferenci ICISSP 2020, ohodnoceny oceněním za nejlepší poster konference.

Letos bychom se chtěli zaměřit na vybrané metody machine learningu, a jiné typy útoků v Active Directory prostředí, jako například Pass the Hash, Pass the Ticket či Golden/Silver tickety.

Plánované výstupy (konference a časopisy):

International Conference on Information Systems Security and Privacy - ICISSP

Téma je rezervováno pro konkrétního studenta.

Číslo: 023

Název tématu: **Reducing model checking overapproximation by advanced value propagation**

Mentor: Stefan Ratschan <ratscste@fit.cvut.cz>

The student intended to work on this project already implemented an explicit state model checker for binary embedded code. He also implemented a technique that radically improves the efficiency of such model checkers by representing bits of states using three-valued logic (0, 1, unknown). However, this technique may result in undesired over-approximation and, as a consequence, may claim correct code to be incorrect. The goal of project he will be to study this phenomenon, to implement a technique to reduce over-approximation, for example, based on value propagation, and to summarize the results in a publication.

Plánované výstupy (konference a časopisy):

International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA)
Springer LNCS (http://www.isola-conference.org/)
International Conference on Formal Methods for Industrial Critical Systems (FMICS)

Téma je rezervováno pro konkrétního studenta.

Číslo: 024

Název tématu: **Rozšíření prostředí pro vizuální modelování a generování blockchain smart kontraktů**
Enhancement of the environment for visual modeling and generating of blockchain smart contracts

Mentor: Ing. Marek Skotnica <skotnmar@fit.cvut.cz>

Tento projekt navazuje na výzkumné téma kterým se zabývá ing. Marek Skotnica v rámci své dizertační práce a vědeckovýzkumného projektu. Projekt se zabývá uplatněním znalostí technik používaných v rámci vědecké skupiny CCMi na aktuálně hodně diskutovanou technologii blockchain smart kontraktů. Vzniká open-source vizuální editor pro smart kontrakty, generátor zdrojového kódu a následně je na případových studiích ukázáno jak by takové kontrakty mohly fungovat v praxi. V současné chvíli se pracuje na příkladu elektronických voleb do evropského parlamentu a možnost uzavření hypotéky bez nutnosti centrální autority (banky).

Předchozí publikovaný výzkum:
https://doi.org/10.1007/978-3-030-06097-8_7
http://dx.doi.org/10.1007/978-3-030-37933-9_10

Repozitáře:
https://github.com/CCMiResearch/DasContract
https://github.com/CCMiResearch/DEMOCaseStudies/tree/master/Blockchain/Mortgage

V rámci tohoto projektu by mělo vzniknout:

- Výzkum rozšíření jazyka DasContract o další prvky z jazyka BPMN - Messages, Event Subprocess, Subprocess, Compensations.
- Výzkum provázanosti smart kontraktů na ověřené zdroje dat (Oracles) např. technologie Chainlink.
- Výzkum provázanosti smart kontraktů na decentralizovanou identitu.
- Sepsání úvodní studie výše uvedených témat.
- Sepsání podkladů pro článek do časopisu nebo na vhodnou konferenci.
- Sepsání popularizačního článku a výroba krátkého videa které předvede příklad hypotéky.

Plánované výstupy (konference a časopisy):

Enterprise Engineering Working Converence (EEWC)
Springer
Business & Information Systems Engineering (BISE)

Téma je rezervováno pro konkrétního studenta.

Číslo: 025

Název tématu: **Efektivní sběr dat z čidel pro SMART systémy 4.0**

Mentor: Ing. Martin Daňhel, Ph.D. <danhema1@fit.cvut.cz>

Prozkoumejte možnosti zabezpečení objektů pomocí drátových čidel vs. bezdrátových čidel a systémů IoT. Jako příklad uvažujte zabezpečení garáže či vinného sklípku výše uvedenými možnostmi (literaturu dodá vedoucí práce). Uvažujte napadnutelnost a zranitelnost systému, množství elektroinstalace či spotřebu energie. Pokuste se analyzovat množství dat přenesené ze senzorů (drát, vs. bezdrát či přímo IoT senzor) a navrhněte efektivní sběr dat pro jednotlivé možnosti. Výstupem může být návrh vlastního komunikačního protokolu, který zajistí efektivní sběr dat. Diskutujte, které z uvedených možností zabezpečení, je nejefektivnější z hlediska financí, spotřeby, náročnosti na instalaci apod.

Plánované výstupy (konference a časopisy):

Výsledek bude použit jednak pro další pokračování závěrečných prací s tematikou SMART zabezpečení. Momentálně máme problém se sběrem a organizací dat. Nicméně toto téma chceme publikovat i na níže uvedených konferencích

Prague Embedded Systems Workshop (PESW), sekce: Security issues of Internet of Things

Téma je rezervováno pro konkrétního studenta.

Číslo: 026

Název tématu: **Využití jazyka TCL pro testování jednotek v automobilovém průmyslu**

Mentor: Ing. Martin Daňhel, Ph.D. <danhema1@fit.cvut.cz>

Cílem práce je ověřit, zda lze efektivně pomocí jazyka TCL generovat sady testů určené pro automobilový průmysl (předpokládá se tedy komunikace přes CAN sběrnici). Udělejte analýzu současného State-of-the-Art v oblasti testování funkčních jednotek v automobilovém průmyslu, zaměřte se především na automatické generování sad testů. Popište vývojový cyklus grafického rozhraní infotainment jednotky v automobilu a vysvětlete důležitost automatického testování. Vytvořte model testovacího stavu pro testování grafiky infotainment jednotek skrze sběrnice CAN. Pro vytvořený model navrhněte základní sadu testů (předpokládá se použití jazyka TCL) a zaměřte se na výslednou efektivitu procesu testování (rychlost testování, maximální možné pokrytí při minimalizaci testovacích vektorů).

Plánované výstupy (konference a časopisy):

Jedná se o rozšíření DP, kde je výsledek cílen na vývoj nových možností testování v automobilovém průmyslu (jedná se o reálnou firmu), nicméně by rád své nápady publikoval na konferenci, kvůli zpětné vazbě

Euromicro Conference on Digital System Design (DSD) 2020, sekce: Architectures and Systems for Automotive, Aeronautic, Space and Intelligent Transportation či DTFT: Dependability, Testing and Fault Tolerance in Digital Systems

Téma je rezervováno pro konkrétního studenta.

Číslo: 027

Název tématu: **SMART květináč 4.0**

Mentor: Ing. Martin Daňhel, Ph.D. <danhema1@fit.cvut.cz>

Prozkoumejte možnosti řízení životních podmínek (světelného toku, tepla, vlhkosti vzduchu apod.) za účelem zvýšené efektivity růstu domácích plodin (vhodnou plodinu si vyberte dle svého uvážení – klasicky pěstovaná v našich podmínkách)). Analyzujte růst této plodiny v klasických domácích podmínkách (ve skleníku, venku apod.) vůči růstu v tzv. chytrém květináči (květináč dodá vedoucí práce). Proveďte experimenty s růstem plodin v chytrém květináči vs ve standardních podmínkách, abyste ověřil použitelnost chytrého květináče.
Proveďte detailní analýzu zaměřenou na měření spotřeby (energie a vody) chytrého květináče a pozorujte rozdíly růstu zkoumané plodiny. Cílem práce je získat podklady pro návrh a realizaci chytrého květináče vlastní výroby, který se bude vyznačovat detailním sběrem a sdílením dat pěstované rostliny, sníženou spotřebou oproti současným produktům a bude podporovat zrychlený růst jedné konkrétní plodiny.

Plánované výstupy (konference a časopisy):

Jedná se o teoreticky zaměřenou práci na kterou navazuje BP stejného studenta s cílem vytvořit funkční vzorek, který budeme dále rozvíjet (ve smyslu Průmysl 4.0).

Euromicro Conference on Digital System Design (DSD) 2020 , sekce: ESSAFE: Electronic systems for smart agriculture, food chain and sustainable environments nebo HASF: Hardware and System Architectures for Smart Farming

Téma je rezervováno pro konkrétního studenta.

Číslo: 028

Název tématu: **Návrh nástroje pro spolehlivostní modely HDM**

Mentor: Ing. Martin Daňhel, Ph.D. <danhema1@fit.cvut.cz>

Nastudujte teorii spolehlivosti (rozsah vymezí vedoucí práce) zaměřte se zejména na problematiku popisu systémů pomocí HDM. Vzhledem k tomu, že zatím pro tyto modely neexistuje žádný vhodný nástroj, který by usnadňoval práci s těmito hierarchickými modely, analyzujte možnosti, jak uživatelsky přívětivě vytvářet HDM pomocí webového rozhraní, předpokládejte možnost reálného nasazení. Dle analýzy vytvořte koncept webové aplikace pro popis systémů pomocí HDM modelů z nastudovaných zdrojů, dle těchto kroků:

Nástroj by měl umožňovat sdílet projekty a výstupy mezi více autorů a také publikovat výsledné projekty. Cílem práce není vytvořit nástroj, ale pouze návrh tohoto nástroje a následně jej publikovat odborné veřejnosti.

Plánované výstupy (konference a časopisy):

POSTER 2021
FEL ČVUT v Praze
Prague Embedded Systems Workshop (PESW)

Téma je rezervováno pro konkrétního studenta.

Číslo: 029

Název tématu: **Analýza veřejných investic do dopravní infrastruktury v ČR**
Analysis of public spending on transport infrastructure in the Czech Republic

Mentor: Mgr. Ing. Pavla Vozárová, Ph.D. <nikolpav@fit.cvut.cz>
Mentor specialista: Ing. Peter Bolcha, Ph.D.

V roce 2016 vstoupil v platnost Zákon o zadávání veřejných zakázek (134/2016 Sb.), který má přispět k transparentnějšímu hospodaření s veřejnými zdroji. Cílem této práce bude v níže uvedených dílčích bodech ověřit a analyzovat stávající datovou dostupnost na dotčených veřejně přístupných portálech. Práce bude součástí většího mezinárodního výzkumného projektu zabývajícího se efektivitou v oblasti veřejných investic, proto bude mentorem-specialistou Ing. Peter Bolcha, Ph.D. z Anglo-americké univerzity v Praze, který tento výzkumný projekt vede. Výstupem výzkumu bude samostatný článek i příprava dat pro detailnější analýzu v rámci výše zmíněného projektu.

Prozkoumejte možnosti analýzy dat o investicích do dopravní infrastruktury v kontextu povinně zveřejňovaných údajů veřejných institucí. Zaměřte se na následující body:

1) Seznamte se s problematikou financování investic do dopravní infrastruktury v ČR a s tím, jaká data v této oblasti jsou instituce povinny zveřejňovat.
2) Pomocí web scrapingu stáhněte data z veřejného registru smluv (https://smlouvy.gov.cz) včetně textových příloh. Porovnejte s možností získání těchto dat z platformy https://www.hlidacstatu.cz - zaměřte se zejména na problematiku dodatků ke smlouvám a jejich uživatelsky přívětivého dohledání ve zpracovaných datech.
3) Navrhněte metody, jak v datech vyfiltrovat pouze smlouvy týkající se dopravní infrastruktury.
4) Prozkoumejte, do jaké míry je možné provázat data z registru smluv s daty z Věstníku veřejných zakázek (https://www.isvz.cz).
5) Proveďte základní statistickou analýzu vámi získaných dat o investicích do dopravní infrastruktury.
6) Na základě vaší analýzy navrhněte, jaké další údaje by bylo možné a vhodné zveřejňovat na platformě https://www.hlidacstatu.cz pro větší transparentnost hospodaření státu v oblasti dopravní infrastruktury.

In 2016, a new legislative on public procurement was introduced with the aim of improving the transparency of the management of public resources. The goal of the proposed analysis is to verify and analyze the current data availability according to the points below. The analysis will be part of a larger international research project studying the efficiency of public investment processes, which is why Ing. Peter Bolcha, Ph.D. from Anglo-American university, the project leader, will be the mentor – specialist. The outcome of

the research will be an autonomous paper as well as data preparation for a more detailed analysis within the above mentioned project.

Explore the possibilities of analyzing data on transport infrastructure in the context of mandatory data publication. Focus on the following points:

1) Get acquainted with how transport infrastructure in the Czech Republic is financed and what data are the concerned institutions required to publish.
2) Using web scrapping techniques, download the data from public contract register (https://smlouvy.gov.cz) including text attachements. Compare with the possibility of obtaining this data from the platform https://www.hlidacstatu.cz - focus especially on the issue of amendments to the contracts and a user-friendly way of searching for these in the processed data.
3) Suggest methods how to filter out contracts related to public infrastructure only.
4) Explore to what extent the data from contract register can be linked to data from public procurement register (https://www.isvz.cz).
5) Provide a basic statistical analysis of the data you obtain on investment in transport infrastructure.
6) Based on your analysis, suggest what other data could and should be published on the platform https://www.hlidacstatu.cz in order to increase the transparency of management of public spending on transport infrastructure.

Plánované výstupy (konference a časopisy):

Current Trends in Public Sector Research conference (http://ctpsr.econ.muni.cz/cs)
Masaryk University in Brno
IFRS: Global Rules & Local Use (https://www.aauni.edu/ifrs-conference-2020/)

Téma je volné a je možné se na něj přihlásit.

Číslo: 030

Název tématu: **Detekce oblastí obličeje pro inteligentní zrcadlo (Smart Mirror)**

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

Inteligentní zrcadlo je zařízení sestavené z polopropustného zrcadla, pod kterým je umístěno zobrazovací zařízení, a z počítače. Uživatel vidí obraz, který je kombinací odrazu a obrazu zobrazovaného na zobrazovacím zařízení. Současně je kamerami umístěnými na rámu zrcadla snímán uživatel.

V rámci výzkumu vyřešte:

a) detekci významných bodů v záznamu z kamery,
b) prozkoumejte překrytí těchto bodů s odrazem,
c) navrhněte úpravu algoritmů tak, aby se detekované body obličeje kryly s příslušnými body odrazu,
d) experimenty provádějte pro různá místa na ploše zrcadla, nejen pro střed zrcadla.

Omezení: zdrojové kódy vytvořte v prostředí Qt.

Plánované výstupy (konference a časopisy):

IEA/AIE: Industrial and Engineering Applications of Artificial Intelligence and Expert Systems IEA/ AIE (Core Rank B)
International Society of Applied Intelligence (ISAI)
International Conference on Acoustics, Speech, and Signal Processing ICASSP

Téma je volné a je možné se na něj přihlásit.