FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Výzkumné léto na FIT 2022 (VýLeT 2022): Program podpory letního studentského výzkumu na FIT ČVUT

Vypsaná témata

Část 1: Základní informace k přihlášení do programu VýLeT 2022

Tento dokument obsahuje **soupis výzkumných témat vypsaných v rámci programu VýLeT pro rok 2022.**

Podrobné informace k programu VýLeT 2022 a pravidla programu jsou uvedeny v samostatném dokumentu „Výzkumné léto na FIT 2022 (VýLeT 2022): Program podpory letního studentského výzkumu na FIT ČVUT – PROPOZICE“ zveřejněném na stránce programu na webových stránkách FIT ČVUT.

Kdo se může přihlásit?

1. Přihlásit do programu se může student **bakalářského** nebo **navazujícího magisterského** programu na ČVUT, a to v období stanoveném v harmonogramu.
2. 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.
3. Kterýkoliv student, který je studentem dle bodu (1) tohoto odstavce se může přihlásit na jakékoliv volné téma.
4. Jeden student se může přihlásit na více témat, vlastní přiřazení zájemců k tématům proběhne až ve výběrovém řízení.
5. Student se může přihlásit a následně řešit výzkumné téma, které je v překryvu s tématem jeho závěrečné práce.
6. Student se může přihlásit a následně řešit výzkumné téma, a posléze si toto téma zvolit jako téma závěrečné práce.
7. Během doby, kdy je program otevřen pro příjem přihlášek od studentů, se **student může přihlásit s vlastním tématem**, a to za následujících podmínek: student si najde mentora, který bude ochoten studenta vést při práci na daném tématu, mentor zpracuje zadání navržené studentem a přihlásí jej do programu přes formulář pro mentory pro zadávání témat, student se posléze na toto téma přihlásí.
8. Během doby, kdy je program otevřen pro příjem přihlášek od studentů, je možné přidávat témata pouze podle bodu (7) Není možné přidávat témata volná, neurčená pro žádného studenta.

Jak se přihlásit?

Přihlášení probíhá odesláním elektronického formuláře. Odkaz na formulář je uveden na webu FIT na stránce programu VýLet 2022. 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 studentů. **Tato lhůta končí 8. 5. 2022.**

Část 2: Vypsaná výzkumná témata

Název zadání: **Zvyšování interoperability konceptuálních modelů pomocí technologií RDF**
Increasing the interoperability of conceptual models using RDF technologies

Mentor: Ing. Marek Suchánek

Existuje velké množství jazyků pro konceptuální modelování. Různé jazyky se hodí v rozdílných situacích a umožňují zaměření se na specifické aspekty problémové domény v potřebné míře detailu. Problém nastává když je potřeba znalosti zachycené v různých modelech integrovat. Některé modelovací jazyky dokonce ani nemají podporu standardizovaných formátů pro jejich reprezentaci. Cílem tohoto projektu je navrhnout OWL ontologii pro metamodel vybraného modelovacího jazyka a převod modelů z klíčových formátů do RDF. Součástí výstupů by měla být také demonstrace použití v rámci sémantické integrace či analýzy modelů pomocí SPARQL.

There are many languages for conceptual modeling. Different languages are useful in different situations and allow you to focus on specific aspects of the problem domain in the necessary level of detail. The problem arises when the knowledge captured in different models needs to be integrated. Some modeling languages do not even have support for standardized formats for their representation. The aim of this project is to design an OWL ontology for the metamodel of a selected modeling language and to convert models from key formats to RDF. The outputs should also include a demonstration of the use in semantic integration or analysis of models using SPARQL.

Plánované výstupy (konference a časopisy):

Applied Ontology
IOS Press

International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (KEOD)
INSTICC

Název zadání: **Vysvětlitelnost doporučovacích systémů**
Explainability of recommender systems

Mentor: doc. Ing. Pavel Kordík, Ph.D.

Increase trust of EU citizens in established media houses by researching and developing trustworthy and explainable recommender systems with explainable user interfaces to both content producers and consumers.

Plánované výstupy (konference a časopisy):

ECML PKDD 2023

Název zadání: **Porovnání adversarial learning technik pro detekci malware**
A Comparison of Adversarial Learning Techniques for Malware Detection

Mentor: Mgr. Martin Jureček, Ph.D.

Cílem adversarial learning technik je záměrná modifikace vstupních dat, která způsobí snížení přesnosti klasifikace. State-of-the-art metody pro vytváření adversariálních vzorků patří do různých oblastí, jako např. reinforcement learning, genetické algoritmy nebo gradientní metody. Cílem této práce bude aplikovat některé existující metody z oblasti adversarial learning na vybrané detekční systémy škodlivého kódu a porovnat je z hlediska úspěšnosti a využitelnosti v praxi.

The aim of the adversarial learning technique is the deliberate modification of input data, which causes a reduction in the accuracy of classification. State-of-the-art methods for creating adversarial examples fall into various areas, such as reinforcement learning, genetic algorithms, or gradient-based techniques. The contribution of this work would be to apply some existing methods in the field of adversarial learning to selected malware detection systems and compare them in terms of accuracy and usability in practice.

Plánované výstupy (konference a časopisy):

International Conference on Security and Cryptography (SECRYPT)
Institute for Systems and Technologies of Information, Control and Communication (INSTICC)

International Conference on Artificial Intelligence Applications and Innovations (AIAI)
International Federation for Information Processing (IFIP)

IEEE Access
IEEE

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Algebraická kryptoanalýza proudové šifry E0**
Algebraic Cryptanalysis of Stream Cipher E0

Mentor: Mgr. Martin Jureček, Ph.D.

Proudová šifra E0 se používá k zabezpečení komunikace v protokolu Bluetooth. Mezi State-of-the-art útoky patří techniky z oblasti lineární kryptoanalýzy a také korelační útoky. V posledních letech si také čím dál více našla uplatnění algebraická kryptoanalýza, která převádí šifru na soustavu polynomiálních rovnic více proměnných nad konečným tělesem, jejímž řešením je tajný klíč šifry. Cílem této práce bude aplikace standardních technik z oblasti algebraické kryptoanalýzy a pokus o prolomení šifry E0, případně její zjednodušené verze.

The E0 stream cipher is used to secure Bluetooth communication. State-of-the-art attacks include linear cryptanalysis techniques as well as correlation attacks. In recent years, algebraic cryptanalysis, which converts a cipher into a set of polynomial equations of several variables over a finite field, whose solution is a secret key, has also found increasing use. The contribution of this work will be the application of standard techniques in the field of algebraic cryptanalysis and try to break the E0 cipher or its simplified version.

Plánované výstupy (konference a časopisy):

International Conference on Security and Cryptography (SECRYPT)
Institute for Systems and Technologies of Information, Control and Communication (INSTICC)

Applied Cryptography and Network Security (ACNS)
Springer

IEEE Access
IEEE

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Velmi líná kompilace pro multi-agentní hledání cest**
Very Lazy Compilation for Multi-agent Path Finding

Mentor: doc. RNDr. Pavel Surynek, Ph.D.

Při líné kompilaci multi-agentního hledání cest do jiného formalismu, jako je například výroková splnitelnost, určitá omezení zakódujeme, zatímco jiná ponecháme, aby se je řešič naučil sám, tj. jsme při kódování líní. Co kdybychom byli ještě línější, tj. nezakódovali nic, a nechali řešič, ať se kódování problému naučí úplně sám.

When lazily compiling a multi-agent search for paths to another formalism, such as propositional satisfiability, we encode certain constraints, while we leave others to be learned by the solver himself, ie we are lazy in coding. What if we were even lazier, ie we didn't encode anything, and let the solver learn to encode the problem himself.

Plánované výstupy (konference a časopisy):

ICAART 2023
INSTICC

ICAPS 2023
ICAPS

ICTAI 2023
IEEE

Název zadání: **Resilientní multi-agetní hledání cest s reálnými roboty**
Resilient Multi-agent Path Finding with Real Robots

Mentor: doc. RNDr. Pavel Surynek, Ph.D.

Představme si vykonávání plánů pro multi-agentní hledání cest se skutečnými roboty, jako jsou roboti, které máme v laboratoři RoboAgeLab, tj. Ozoboti, ePucky a drony Crazyflie. Při vykonávání plánu se občas něco nepovede. Chtěli bychom se zabývat otázkou, jak na nezdar ve vykonávání plánu reagovat změnou plánu, resp. jak zajistit, aby už původní plán byl na takové změny připraven.

Consider execution of multi-agent path finding plans with real robots, such as the robots we have in the RoboAgeLab lab, ie Ozobots, ePucks and Crazyflie UAVs. Sometimes things go wrong with the plan. We would like to address the question of how to respond to a failure in the execution of the plan by changing the plan or how to ensure that the original plan is ready for such changes.

Plánované výstupy (konference a časopisy):

ICAART 2023
INSTICC

ICAPS 2023 (+demo)
ICAPS

ICTAI 2023
IEEE

Název zadání: **Hledání cesty s omezeními pomocí smíšeného celočíselného lineárního programování**
Constrained Path Finding Using Mixed Integer Linear Programming

Mentor: doc. RNDr. Pavel Surynek, Ph.D.

Zabývejme se otázkou nalezení cesty, ne úplně obyčejné, například takové, která se bude vyhýbat pohybujícím se překážkám. Prozkoumáme možnosti formulace problému ve formalismu smíšeného celočíselného lineárního programování. Případně lze vymyslet nějakou zajímavou interakci řešiče a hlavního algoritmy, tj. otázka na existenci cesty se může skládat z mnoha postupně se upřesňujících otázek na řešič.

Let us deal with the question of finding a way, not entirely ordinary, such as one that avoids moving obstacles. We will explore the possibilities of problem formulation in the formalism of mixed integer linear programming. Alternatively, some interesting interaction between the solver and the main algorithm can be devised, ie the question of the existence of the path can consist of many iteratively refined questions to the solver.

Plánované výstupy (konference a časopisy):

ICAART 2023
INSTICC

ICAPS 2023
ICAPS

ICTAI 2023
IEEE

Název zadání: **Rozšířené modely spolehlivosti**
Advanced Dependability Models

Mentor: prof. Ing. Hana Kubátová, CSc.

Využití různých formálních i prakticky používaných modelů pro jejich zahrnutí do našeho současného "Heterogeneous Dependability Model" (např. využití znalosti UML) a zhodnocení výhod a nevýhod jejich využívání pro modelování a výpočty spolehlivostních parametrů.

Utilization of various formal and practically used models for their inclusion in our current "Heterogeneous Dependability Model" (eg use of UML knowledge) and evaluation of advantages and disadvantages of their use for modeling and calculation of reliability parameters.

Plánované výstupy (konference a časopisy):

Euromicro DSD/SEAA
EUROMICRO

DDECS
IEEE

MICPRO journal
ELSEVIER

Název zadání: **Anonymizing User Data: A Parameterized Perspective**

Mentor: doc. RNDr. Dušan Knop, Ph.D.

The input to the clustering problems we are about to investigate contains a (multi-)set of n points in D ⊆ R d , where d is a constant fixed in advance. The dimension d is selected to represent d different features of the agents (i.e., the entities we focus on such as, e.g., human users). The task is to group these data into groups, that is, the output consists of groups (multisets) C 1 , C 2 , . . . , C_ell possibly together with their representatives r 1 , r 2 , . . . , r_ell for some ell. A common practice is to select the representatives to be the central point (usually in the geometric sense; indeed, one could also aim for a representative being a member of its cluster). There are many practically motivated desirable properties of the groups one could measure: the minimum size of a cluster, the difference between the sizes of a largest and a smallest cluster, the number of clusters—to name just a few. The goal is
usually some global measure of the quality of the groups, e.g., the sum of isrepresentations of the points or the maximum misrepresentation; see, e.g., [AB09, BA08] for examples of these measures and their properties (axioms).Our aim is to design algorithms for specific problems of interest that. The central mission of the work will be aimed at designing new fixed-parameter algorithms, that is, algorithms that are well-scalable to large data as long as certain quantities of the input remain small (which is often the case in real-world instances). Let us mention a few new parameters we would like to propose for the initial study along with the study of clustering. This can shed new light on already established results in this field. We would like to investigate structural parameters based on (unit) circle graph of the given points. The vertex set of such graph is the set of data points. There is an edge between two points if and only if their distance is at most some constant r. It is straightforward that r should be at least the smallest distance in the dataset. The closer the points are in the global meaning, the denser the graph is (and the easier it should be to partition the dataset in reasonable clusters). What if r is set based on the smallest distance in the dataset (e.g., twice that value)? What if r is set based on the maximum distance between a data point and its cluster representative in the output?

Our aim is to design algorithms for specific problems of interest that are captured by the general framework outlined above. The central mission of the work will be aimed at designing new fixed-parameter algorithms, that is, algorithms that are well-scalable to large data as long as certain quantities of the input remain small (which is often the case in real-world instances). Let us mention a few new parameters we would like to propose for the initial study along with the study of clustering. This can shed new light on already established results in this field. We would like to investigate structural parameters based on (unit) circle graph of the given points. The vertex set of such graph is the set of data points. There is an edge between two points if and only if their distance is at most some constant r. It is straightforward that r should be at least the smallest distance in the dataset. The closer the points are in the global meaning, the denser the graph is (and
the easier it should be to partition the dataset in reasonable clusters). What if r is set based on the
smallest distance in the dataset (e.g., twice that value)? What if r is set based on the maximum distance between a data point and its cluster representative in the output?

Plánované výstupy (konference a časopisy):

IWOCA
pořadatel pro rok 2023 zatím nebyl určen

WG
pořadatel pro rok 2023 zatím nebyl určen

arXiv
online

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Dvojjazyčný Word2Vec model**
Bilingual Word2Vec model

Mentor: Ing. David Bernhauer

Bezkontextové word embeddingy se staly populární pro svoji jednoduchost a akceptovatelnou přesnost. Některé metody přichází s možností natrénování více modelů v různých jazycích, které jsou následně zarovnány s využitím slovníkového přístupu. Cílem tohoto projektu je ověřit, zda by bylo možné využít zdroje jako jsou nařízení evropského parlamentu nebo jiné zdroje ověřených překladů pro vytvoření vícejazyčného word embeddingu bez využití zarovnávací metody. Výstupem by měla být rešerše aktuálních přístupů k problému a proof-of-concept, zda je možné s využitím takových dat natrénovat jednoduchý dvojjazyčný Word2Vec model.

Context-free word embeddings have become popular for their simplicity and acceptable accuracy. Some methods come with the ability to train multiple models in different languages, which are then aligned using a dictionary approach. The aim of this project is to test whether it would be possible to use resources such as European Parliament regulations or other sources of validated translations to create multilingual word embeddings without using the alignment method. The output should be a survey of current approaches to the problem and a proof-of-concept of whether a simple bilingual Word2Vec model can be trained using such data.

Plánované výstupy (konference a časopisy):

International Conference on Database and Expert Systems Applications
Letošní je (Vienna University of Economics and Business), cílíme spíše na příští rok.

2022 IEEE International Conference on Big Data
IEEE, hostující univerzitu se mi nepodařilo dohledat

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Kernelizace problému Target Set Selection**

Mentor: doc. RNDr. Dušan Knop, Ph.D.

Budeme zkoumat problém Target Set Selection, který popisuje přirozený model šíření názoru (názorů) na sociálních sítích. V nav rženém projektu se hodláme soustředit na řídké strukturální parametry a jejich význam pro existenci tzv. polynomiálního kernelu (případně aproximačního kernelu/algoritmu).

Plánované výstupy (konference a časopisy):

INTERNATIONAL WORKSHOP ON GRAPH-THEORETIC CONCEPTS IN COMPUTER SCIENCE (WG)

International Workshop on Combinatorial Algorithms (IWOCA)

Information Processing Letters (IPL)
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Stabilita 3D kauzálních autoregresních modelů v aplikacích modelování multispektrálních textur**
3D causal autoregressive models stability in multispectral texture modeling

Mentor: Prof. Ing. Michal Haindl, DrSc.

Vypracujte přehled metod ověření stability 3D kauzálních autoregresních modelů. Naprogramujte algoritmus pro ověření a vizualizaci stability 3D kauzálního autoregresního modelu v závislosti na bayesovsky odhadnutých parametrech modelu. Ověřte naprogramovaný algoritmus na zadaných modelech barevných textur. Ukažte vliv stabilizace modelu na vizuální vlastnosti jím generovaných textur.

Develop an overview of methods for verifying the stability of 3D causal autoregressive models. Program an algorithm to verify and visualize the stability of a 3D causal autoregressive model depending on the Bayesian estimated model parameters. Verify the programmed algorithm on the specified color texture models. Show the effect of model stabilization on the visual properties of the textures generated by it.

Plánované výstupy (konference a časopisy):

European Conference on Computer Vision ECCV / IEEE International Conference on Image Processing ICIP / IAPR International Conference on Pattern Recognition ICPR / IEEE International Conference on Computer Vision ICCV
SPRINGER / IEEE / IAPR

Název zadání: **Multispektrální texturní benchmark**
Multispectral texture benchmark

Mentor: Prof. Ing. Michal Haindl, DrSc.

Vypracujte přehled metod texturních příznaků včetně jejich vlastností a zobecněte je do multispektrálního datového prostoru. Ověřte jejich informační hodnotu a robustnost na zadaných měřeních s proměnlivými úhly osvětlení a pozorování a při změně měřítka. Naprogramujte vhodný příznakový online benchmark, který spojí dodané generátory příznaků s některými nově naprogramovanými. Ověřte naprogramované algoritmy generovaní příznaků pomocí alternativních programových zdrojů (openCV, Matlab) na zadaných barevných texturách.

Develop an overview of textural features, including their properties, and generalize them to a multispectral data space. . Verify their information value and robustness on specified measurements with variable lighting and observation angles and when scaling. Program a suitable online feature benchmark that combines the supplied feature generators with some of the newly programmed ones. Verify the programmed algorithms for generating features using alternative program sources (openCV, Matlab) on the specified color textures.

Plánované výstupy (konference a časopisy):

European Conference on Computer Vision ECCV / IEEE International Conference on Image Processing ICIP / IAPR International Conference on Pattern Recognition ICPR / IEEE International Conference on Computer Vision ICCV
SPRINGER / IEEE / IAPR

Název zadání: **Aproximace víceměřítkových MRF modelů**
Approximation of multi-resolution MRF models

Mentor: Prof. Ing. Michal Haindl, DrSc.

Ověřte možnost aproximace více měřítkového MRF modelu pomocí pyramidové faktorizace, kumulantní nebo bond-moving aproximace. Ověřte informační hodnotu jednotlivých možných aproximací a jejich robustnost na zadaných měřeních s proměnlivým měřítkem.

Verify the possibility of approximating a multi-scale MRF model using pyramid factorization, cumulant or bond-moving approximation. Verify the information value of individual possible approximations and their robustness on the given measurements with a variable scale.

Plánované výstupy (konference a časopisy):

European Conference on Computer Vision ECCV / IEEE International Conference on Image Processing ICIP / IAPR International Conference on Pattern Recognition ICPR / IEEE International Conference on Computer Vision ICCV
SPRINGER / IEEE / IAPR

Název zadání: **Měření BRDF materiálů z dronu**
Material BRDF measurement from dron observation

Mentor: Prof. Ing. Michal Haindl, DrSc.

Navrhněte a realizujte vhodný způsob měření BRDF přírodních materiálů z měření dronem. Práce představuje naprogramování vhodné letové dráhy, registraci a geometrickou korekci snímků a aproximaci nemožnosti měnit úhel a spektrum osvětlení.

Design and implement a suitable method for measuring BRDF natural materials from drone measurements. The work presents the programming of a suitable flight path, registration and geometric correction of images and the approximation of the impossibility of changing the angle and spectrum of lighting.

Plánované výstupy (konference a časopisy):

European Conference on Computer Vision ECCV / IEEE International Conference on Image Processing ICIP / IAPR International Conference on Pattern Recognition ICPR / IEEE International Conference on Computer Vision ICCV
SPRINGER / IEEE / IAPR

Název zadání: **Finding spatial patterns in recommender systems**

Mentor: Rodrigo Augusto da Silva Alves, Ph.D.

Regionalization is a classification technique that groups spatial items having areal representations into homogenous continuous regions. A reasonable assumption in recommender systems (RSs) is that the rows (users) and columns (items) of the rating matrix can be regionalized into spatial communities (clusters). Such a task can assist providers in a variety of complex problems, such as picking warehouse locations, producing effective geo-marketing campaigns and produce fair geo-based recommendation. In this project, we aim to investigate methods that take into account location of users and (or) items, regionalize them and use the spatial information to improve recommender systems. The main outcome here is a research article that should be submitted for a qualified conference or journal.

Plánované výstupy (konference a časopisy):

ACM Recommender System Conference
ACM

ACM Transactions on Knowledge Discovery from Data (TKDD)
ACM

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Perl-kompatibilní regulární výrazy**
Perl-compatible regular expressions

Mentor: Ing. Ondřej Guth, Ph.D.

Klasické regulární výrazy, popisující právě regulární jazyky, jsou teoreticky velmi dobře popsané. To však neplatí pro všechny syntaxe výrazů používané v nástrojích a knihovnách a zejména pro jejich nadregulární rozšíření. V navrhovaném projektu se zaměříme na PCRE (Perl-compatible regular expressions), jaké třídy jazyků dokáží popsat, případně na vylepšení algoritmů, které s nimi pracují.

Classical regular expressions (those describing regular languages) have long established theoretical background. Unlike RE, expressions used in real-world tools are usually theoretically examined after their implementation. This project focuses on PCRE (Perl-compatible regular expressions), their expressive power (equivalence to some language class) or improvement of algorithms used for their compilation or matching.

Plánované výstupy (konference a časopisy):

International Conference on Implementation and Application of Automata (CIAA)

Annual Symposium on Combinatorial Pattern Matching (CPM)

International Workshop on Combinatorial Algorithms (IWOCA)

Název zadání: **Strukturální parametry pro barvení bez monochromatických cyklů**

Mentor: RNDr. Ondřej Suchý, Ph.D.

Budeme zkoumat barvení bez monochromatických cyklů vzhledem ke strukturálním parametrům vstupního grafu, zejména v případě, že délka zakázaných cyklů je součástí vstupu. Zároveň budeme zkoumat kernelizace problému.

Plánované výstupy (konference a časopisy):

International Workshop on Combinatorial Algorithms (IWOCA)

International Conference and Workshops on Algorithms and Computing (WALCOM)

Information Processing Letters
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Analýza TPM komunikace za pomoci FPGA**
Analysis of TPM Communication Using FPGA

Mentor: Ing. Martin Daňhel, Ph.D.

Trusted Platform Module (TPM) is a HW solution that allows to increase the security level of a computing system (for example used in Windows 11). Analyze TPM behavior on LPC bus (Intel Low Pin Count). Design and implement an FPGA solution that will return values of LPC-TPM transactions over serial line. Create sufficient test cases of the implementation. Capture the LPC communication using the solution and interpret it according to the analysis.

The aim of the research is to analyze the behavior of TMP on LPC using FPGA in order to obtain (sensitive) information.

The expected output of this assignment is usable designed HW (with possibility of further extension) and interpretation of the obtained data for further research.

Plánované výstupy (konference a časopisy):

MECO: Mediterranean Conference on Embedded Computing
MECO: https://mecoconference.me/meco2022/

DSD: Euromicro Conference on Digital System Design
Euromicro: https://www.euromicro.org/cms/

MICPRO: Microprocessors and Microsystems Embedded Hardware Design
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Odběrová analýza kryptografického procesoru CEC 1702**
Power Analysis of Cryptographic Processor CEC 1702

Mentor: Dr.-Ing. Martin Novotný

Make the firmware development flow of Microchip CEC 1702 cryptographic processor functional. Use either the Clicker2 development kit by Mikroelektronika or the ChipWhisperer kit by NewAE, compare the two systems, and choose one for further work.
Implement the AES cipher on the CEC 1702. Examine the resistance of the CEC 1702 to power analysis attacks. The research goal is to compare the resistance of the software version of the AES cipher and the hardware version of the AES cipher using the built-in hardware accelerator. The other research goal is to compare the resistance of the Microchip CEC 1702 cryptographic processor and the STM32 processor. Research results will be published at international conference or in journal.

Plánované výstupy (konference a časopisy):

Design and Diagnostics of Electronic Circuits and Systems 2023
IEEE

Digital Systems Design 2023
Euromicro

Mediterranean Conference on Embedded Computing 2023
MANT

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Implementace Paillierova kryptosystému a útok injekcí chyb na procesoru CEC 1702**

Mentor: Dr.-Ing. Martin Novotný

Implementujte Paillierův kryptosystém na procesoru Microchip CEC 1702. Použijte knihovnu „bigi“ určenou pro implementaci kryptografických algoritmů na mikrokontrolérech a proveďte nezbytné úpravy. Při implementaci Paillierova kryptosystému vyjděte z jeho stávající implementace pro CEC 1302 a proveďte nezbytné úpravy. Vytvořte čistě softwarovou variantu firmware a variantu využívající vestavěný hardwarový akcelerátor RSA. Firmware má podporovat různé šířky klíčů.
Dále s pomocí knihovny „bigi“ vytvořte pro procesor CEC 1702 čistě softwarovou variantu RSA-CRT a variantu RSA-CRT využívající jeho vestavěný hardwarový akcelerátor. Výzkumným cílem je s pomocí těchto variant prozkoumat možnosti provedení útoku injekcí chyb (fault-injection attack) prostřednictvím soupravy ChipWhisperer. Dalším výzkumným cílem je porovnání útoku na procesor CEC1702 s útokem na procesor STM32. Výzkumné výsledky prezentujte na mezinárodní konferenci nebo v časopise.

Plánované výstupy (konference a časopisy):

Design and Diagnostics of Electronic Circuits and Systems 2023
IEEE

Digital System Design 2023
Euromicro

Mediterranean Conference on Embedded Computing 2023
MANT

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Pravidelnosti a kvazipravidelnosti na řetězcích**
Regularities and Quasiperiodicities on Strings

Mentor: prof. Ing. Jan Holub, Ph.D.

Cílem práce je prozkoumat a rozšířit algoritmy na vyhledávání kvaziregularit v řetězcích, speciálně pak prozkoumat a vylepšit algoritmy pro vyhledávání enhanced seedů, enhanced restricted seedů a k-aproximační varianty těchto problémů jako6 i prozkoumat algoritmy pro hledání kvaziregularit z indexovaných textů.
Druhým cílem je pak prozkoumat možnosti aplikace teorie parametrizované složitosti na NP těžké problémy v oblasti pravidelností řetězců.

Téma navazuje na články:
Kędzierski, A., Radoszewski, J. k-Approximate Quasiperiodicity Under Hamming and Edit Distance. Algorithmica 84, 566–589 (2022). https://doi.org/10.1007/s00453-021-00842-7,

Tomáš Flouri, Costas S. Iliopoulos, Tomasz Kociumaka, Solon P. Pissis, Simon J. Puglisi, W.F. Smyth, Wojciech Tyczyński, Enhanced string covering, Theoretical Computer Science 506, 102-114 (2013). https://doi.org/10.1016/j.tcs.2013.08.013.

Očekávaným výstupem je publikace na mezinárodní konferenci nebo v časopise.

The goal of the work is to study and extend the algorithms seaching for quasiregularities in strings; especially to study and extend the algorithms for enhanced seeds, enhanced restricted seeds, and k-approximate variants of the problems. We would like also to study algorithms for searching for quasiperiodicities in indexed texts.
The second goal is to explore the possibility to apply parameterized complexity on NP-hard problems in the area of string regularities.

The topics extend the following papers:
Kędzierski, A., Radoszewski, J. k-Approximate Quasiperiodicity Under Hamming and Edit Distance. Algorithmica 84, 566–589 (2022). https://doi.org/10.1007/s00453-021-00842-7,

Tomáš Flouri, Costas S. Iliopoulos, Tomasz Kociumaka, Solon P. Pissis, Simon J. Puglisi, W.F. Smyth, Wojciech Tyczyński, Enhanced string covering, Theoretical Computer Science 506, 102-114 (2013). https://doi.org/10.1016/j.tcs.2013.08.013.

An expected result will be a publication in international conference or in journal.

Plánované výstupy (konference a časopisy):

Combinatorial Pattern Matching
Theoretical Computer Science - Elsevier
Discrete Applied Mathematics - Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Identifikace sledovaného šifrovaného videostreamu prostřednictvím sond síťového provozu**
Identification of the monitored encrypted video stream via network traffic probes

Mentor: Ing. Jan Fesl, Ph.D.

Šifrování síťového provozu zásadní měrou dovoluje na jedné straně uživateli zachovávat anonymitu resp. nemožnost detekce jeho konkrétních aktivit, na druhou stranu umožňuje i relativně beztrestně páchat nelegální činnosti. V tomto případě se nelegální činností myslí sledování nelegálních (např. retransmise videostreamů placených sportovních přenosů, nových filmů, atd.) či škodlivých (např. dětská pornografie, terorismus, atd.) videí, kterou je vhodné omezit. Úkolem navrženého projektu je zapojit se do výzkumného týmu v rámci grantu řešeného ve spolupráce se sdružením CESNET a přispět k návrhu spolehlivé detekční metody.

Encryption of network traffic to a large extent allows the user to maintain anonymity or the impossibility of detecting its specific activities, on the other hand, allows it to commit illegal activities relatively with impunity. In this case, illegal activity means watching illegal (eg retransmission of video streams of paid sports, new films, etc.) or harmful (eg child pornography, terrorism, etc.) videos, which should be limited. The task of the proposed project is to join the research team within the grant solved in cooperation with the CESNET association and to contribute to the design of a reliable detection method.

Plánované výstupy (konference a časopisy):

IEEE-ISNCC , International Symposium on Networks, Computers and Communications
IEEE

Future Internet
MDPI

Název zadání: **Inteligentni detekce aktivních IPv6 adres**
Intelligent detection of active IPv6 addresses

Mentor: Ing. Jan Fesl, Ph.D.

Protokol IPv6 přináší řadu výhod a nových mechanismů, které jednoznačně zlepšují možnosti doručování dat na síťové vrstvě - dostatek veřejných adres, mobilita, šifrování atd. Vzhledem k ohromnému počtu adres, které mohou být přidělovány klientským stanicím (typicky prefix /64) není ovšem bez znalosti příslušné pouze lokálním směrovačům snadné vzdáleně monitorovat aktivní IPv6 adresy. Tento problém je možné částečně vyřešit pomocí známých heuristik (např. běžné zvyklosti správců sítí, příbuznost MAC adres rozhraní v rámci jedné organizace, rozložení MAC adres dle výrobců atd.) a hrubé síly. Úkolem projektu bude prakticky implementovat dané heuristiky, vyhodnotit jejich přínos a pokusit se navrhnout nové. Řešení bude finálně otestováno nad autonomním systémem ČVUT.

The IPv6 protocol brings a number of advantages and new mechanisms that clearly improve the possibilities of data delivery at the network layer - sufficient public addresses, mobility, encryption, etc. However, due to the huge number of addresses that can be assigned to client stations (typically prefix / 64) appropriate only for local routers easy to remotely monitor active IPv6 addresses. This problem can be partially solved using known heuristics (eg common practices of network administrators, affinity of MAC addresses of interfaces within one organization, distribution of MAC addresses according to manufacturers, etc.) and brute force. The task of the project will be to practically implement the given heuristics, evaluate their contribution and try to design new ones. The solution will finally be tested on the CTU autonomous system.

Plánované výstupy (konference a časopisy):

IEEE International Conference on Computer Communications (INFOCOM)
IEEE

Future Internet
MDPI

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

Mentor: Ing. Tomáš Vondra, Ph.D.

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 včasovém limitu za dodržení instrukcí. Druhý test je Purdue Pegboard, který spočívá v zasouvání kolíčků do dírek v desce, opět dle přesných 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 jeden z těchto testů 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. Na téma se mohou přihlásit až 4 studenti.

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 second test is Purdue Pegboard which consists in inserting pegs into holes in the board, also according to strict 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 one of the tests 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. The topic can accomodate up to 4 students.

Plánované výstupy (konference a časopisy):

European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database ECML PKDD 2023
Nezávislá konference / Springer

IEEE Congress on Evolutionary Computation CEC 2023
IEEE

Rehabilitace a fyzikální lékařství
Česká lékařská společnost J. E. Purkyně

Název zadání: **Rozpoznání textu pro neziskovou TV**
Text recognition for a non-profit TV

Mentor: Ing. Tomáš Vondra, Ph.D.

Czech-American TV, nezisková televize českých krajanů v USA, nás požádala o vylepšení webové prezentace www.catvusa.com pro američany o České Republice nebo stránky www.americantravelshow.com pro čechy o Americe. Slovy zadavatele:
Konkrétně bychom chtěli rozšířit nas WP plugin Genealogy na nasem webu tím, že by tam byla další funkce, která by dokázala přepsat německý text tištěný ve fontu Kurent a Schwabach do latinky a pokud to bude možné i přeložit do angličtiny za použití například Google translate. Prostě že by nekdo oscanoval text v kurentu (třeba staré noviny) a pak by přes náš plugin získal tento text v latince a popřípadě přeložený do angličtiny.
Tento plugin chceme rozšířit o výše uvedenou funkci se čtením scanu a s překladem https://catvusa.com/genealogy/german-czech/
Předpokládáme, že by se zadání dalo řešit zabudováním open-source OCR enginu a jeho naučením na archaické znakové sady.

Czech-American TV, a non-profit television of Czech compatriots in the USA, asked us to improve the website www.catvusa.com for Americans about the Czech Republic or www.americantravelshow.com for Czechs about America. In the words of the requester:
We'd like to extend our WP plugin genealogy on our website with the fact that there would be another function that could transcribe the German text printed in the Kurent and Schwabach fonts into Latin and, if possible, translate it into English using, for example, Google Translate. Simply, someone would scan the text in Kurent (for example, an old newspaper) and then through us the plugin would get this text in Latin and possibly translated into English.
We want to extend this plugin with the above function with scan reading and translation https://catvusa.com/genealogy/german-czech/
We presume that the solution would be to embed an open-source OCR engine and teach it the archaic fonts.

Plánované výstupy (konference a časopisy):

European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database ECML PKDD 2023
Nezávislá konference / Springer

ProInflow
Kabinet informačních studií a knihovnictví Filozofické fakulty Masarykovy univerzity v Brně

Název zadání: **Testování Markovských modelů pomocí Monte Carlo simulace na grafické kartě**
Testing of Markov models using Monte Carlo simulation on GPU

Mentor: Ing. Martin Kohlík, Ph.D.

V rámci projektu bude vytvořen algoritmus pro testování Markovských modelů pomocí Monte Carlo simulace, který poběží v paralelním prostředí na grafické kartě. Výsledkem práce budou nasimulovaná data, která budou použita pro publikaci článků na konferencích a/nebo časopise. Tento výzkum navazuje na téma disertační práce mentora specialisty a také na výzkum, kterým se zabývá Laboratoř spolehlivosti.

An algorithm for testing Markov models using Monte Carlo simulation, which will run in a parallel environment on a GPU, will be created within the project. The result of the work will be simulation data, which will be used for the publication of the article at the conferences and/or journal. This research follows up on the topic of the dissertation of a Mentor specialist and also on the research dealt with by the SafetyLab.

Plánované výstupy (konference a časopisy):

The International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)
IEEE

Digital System Design (DSD)
Euromicro

Microprocessors and Microsystems (MICPRO)
Elsevier

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

Mentor: Ing. Pavel Hrabák, Ph.D.

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 FEMTC 2022 (https://www.femtc.com/events/2022), případně i do uvedeného časopisu.

Plánované výstupy (konference a časopisy):

Fire and Evacuation Modeling Technical Conference - Thunderhead Engineering

Simulation Modelling Practice and Theory, SIMUL MODEL PRACT TH - Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Klasifikace Windows malware založena na samoorganizačních mapách**
Windows Malware Classification Based on Self-Organizing Maps

Mentor: Mgr. Olha Jurečková

Samoorganizační mapy si už našli uplatnění v systémech pro odhalení průniků, které monitorují síťový provoz, avšak jejich využití pro klasifikaci škodlivých binárních souborů není ještě dostatečně prozkoumáno. Cílem práce je prozkoumat možnosti užití samoorganizačních map i pro problém klasifikace malware, konkrétně pod operačním systémem Windows. Výstupem práce bude porovnání dosažených výsledku založených na samoorganizačních mapách s výsledky získanými ze state-of-the-art technik založených na strojovém učení.

Plánované výstupy (konference a časopisy):

International Conference on Security and Cryptography (SECRYPT)
Institute for Systems and Technologies of Information, Control and Communication (INSTICC)

International Conference on Knowledge Based and Intelligent information and Engineering Systems (KES)
KES International

IEEE Access
IEEE

Název zadání: **Obejít nebo se protlačit davem? Strategie v CA popsané směsí rozdělení**
Bypassing or pushing through the crowd? Distribution mixture describing strategies in CA

Mentor: Ing. Pavel Hrabák, Ph.D.

Celulární modely pohybu chodců se stále těší velké oblibě pro svou jednoduchost a schopnost postihnout důležité fenomény evakuace a pohybu chodců. Student v rámci své bakalářské práce prozkoumal jednoduchý celulární model umožňující simulovat heterogenní strategie pohybu v davu před úzkým hrdlem: obcházení a protlačování se. Cílem projektu je detailně prozkoumat tyto strategie a jejich důsledek v simulaci evakuace, tj. dopad na pozorovatelné veličiny jako totální evakuační čas a tok. Projekt cílí především na heterogenitu agentů, která je reprezentovaná nehomogenním rozdělením odpovídajících parametrů.
Výsledky projektu bychom rádi prezentovali v rámci Complex collective systems workshopu conference PPAM 2022 a v případě úspěchu se ucházeli o special issue časopisu Journal of Computational Science.

Plánované výstupy (konference a časopisy):

14th INTERNATIONAL CONFERENCE ON PARALLEL PROCESSING AND APPLIED MATHEMATICS
prof. Roman Wyrzykowski, Czestochowa University of Technology

Journal of Computational Science
Elsevier

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Implementace algoritmů pro výzkum pohyblivých grafů**
Implementation of algorithms for studying flexible frameworks

Mentor: Dr. techn. Ing. Jan Legerský

Umístění vrcholů grafu v rovině se nazývá pohyblivé, pokud jej lze spojitě deformovat při zachování vzdáleností sousedních vrcholů. Existence takovéhoto umístění pro daný graf je charakterizována existencí jistého obarvení hran zvaného NAC-obarvení (Grasegger, L., Schicho. 2019). Mentor spolu s Georgem Graseggerem vytvořili SageMath balíček FlexRiLoG za účelem zkoumání pohyblivých umístění grafů pomocí NAC-obarvení. Další výsledky rozšiřující teorii NAC-obarvení na pohyblivá symetrická a obdélníková umístění byly publikovány a částečně implementovány v tomto balíčku, ale kód potřebuje revizi a doplnění. Cílem tohoto výzkumu je tudíž balíček optimalizovat a otestovat, doplnit chybějící části a implementovat také další algoritmy z teorie pohyblivosti/pevnosti. Článek popisující kompletní balíček bude odeslán do časopisu zaměřeného na software.

A realization of a graph, i.e., the placement of the vertices in the plane, is called flexible if it can be continuously deformed while preserving the distances between adjacent vertices. The existence of a flexible realization for a given graph is characterized by the existence of a certain edge coloring, called NAC-coloring (Grasegger, L., Schicho. 2019). The mentor together with Georg Grasegger have implemented the SageMath package FlexRiLoG for studying flexible realizations using NAC-colorings. Futher results extending the theory of NAC-colorings to symmetric and parallelogram realizations have been published and partially implemented in the package, but the code needs to be revised and completed. Hence, the goal is to optimize and test the package, add the missing parts and to implement also other algorithms from rigidity/flexibility theory. A paper describing the package will be submitted to a journal publishing software.

Plánované výstupy (konference a časopisy):

SoftwareX
Elsevier

The Journal of Open Source Software (JOSS)
Journal of Open Source Software, United States

Název zadání: **Detekce nežádoucího chování v grafových reprezentacích dat s využitím časové dimenze**

Mentor: Ing. Jaroslav Kuchař, Ph.D.

Grafové reprezentace dat mají oproti jiným reprezentacím velkou výhodu ve své schopnosti popisovat situace, ve kterých dochází k časté interakci mezi určenými entitami. Za tyto entity lze v řadě problémů spojených s aktivitou na internetu považovat uživatele, případně objekty jejich zájmu jako jsou webové stránky, produkty, jejich recenze a další. V mnoha oblastech však dochází k nežádoucímu chování uživatelů. Typickým příkladem jsou stránky obsahující recenze produktů a služeb - častým jevem je podvodné chování, kdy osoby zakládají falešné účty a píší smyšlené recenze (cílem je buďto zlepšení hodnocení vlastního produktu nebo očernění konkurenčního).

Takové a podobné situace lze odhalit pomocí technik detekce anomálií v grafových reprezentacích. Jejich využití je tématem této práce. Velmi důležitou a méně používanou složkou je časová dimenze - práce by měla cílit na její využití. Časovou dimenzí se typicky myslí údaje o čase interakcí, případně posloupnost těchto interakcí. Zpracovávat dynamicky se měnící grafy je náročnější, nicméně se jedná o přístup s potenciálem výrazně zlepšit výslednou úspěšnost. Pozornost by měla být věnována srovnání dostupných metod, případně návrhu vlastních. Úspěšnost těchto metod by měla být vyhodnocena nad reálnými daty. V úvahu připadají již existující datasety, případně nově vytvořené.

Plánované výstupy (konference a časopisy):

CIKM: International Conference on Information and Knowledge Management
ACM

WCIDM: International Workshop on Computational Intelligence and Data Mining
ITAT

Případně CIKM, WSDM, KDD, ICML, WWW a jejich workshopy

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Trvale udržitelný cloud**
Sustainable cloud

Mentor: Ing. Jan Fesl, Ph.D.

Svět virtualizačních infrastruktur a cloudů je velice rozmanitý, avšak technologicky se rychle měnící a zastarávající. Účelem projektu je navrhnout obecné požadavky na fyzickou infrastrukturu (virtualizéry, různí výrobci CPU, datová úložiště) a virtualizační software (možnosti orchestrace, ukládání dat napojení na technologie), na základě kterých bude možné původní zastaralé řešení postupně obměňovat, elasticky rozšiřovat a doplňovat dlouhou (ideálně nekonečnou) dobu resp. postupně transformovat na zcela nové řešení.

The world of virtualization infrastructures and clouds is very diverse, but technologically rapidly changing and obsolete. The purpose of the project is to design general requirements for physical infrastructure (virtualizers, various CPU vendors, data storage) and virtualization software (orchestration options, data storing, technology connection), based on which it will be possible to gradually change the original obsolete solution, elastically extend and add long (ideally infinite) time resp. gradually transform into a completely new solution.

Plánované výstupy (konference a časopisy):

International Conference on Future Internet of Things and Cloud, www.ficloud.org
IEEE

Název zadání: **Experimentální porovnání implementací protokolů PTP a WhiteRabbit**
Experimental evaluation of PTP and White Rabbit protocal implementations

Mentor: RNDr. Ing. Vladimír Smotlacha, Ph.D.

Experimentální porovnání implementací protokolů PTP a WhiteRabbit

Protokol PTP (Precise Time Protocol) slouží pro distribuci přesného času síťovým zařízením s využitím Ethernetu, tedy na linkové vrstvě ISO/OSI. Největší fluktuace ve zpoždění rámců vzniká ve frontách síťových přepínačů. Protokol předpokládá podporu přímo v přepínačích, kdy je doba zpoždění změřena a předána cílovému zařízení. Existují různé implementace jednotlivých výrobců, je proto potřebné znát jejich přesnost a kompatibilitu. Pro porovnání jsou k dispozici Ethernetové přepínače tří výrobců a dále software implementace v Linuxu. Měření se bude provádět v laboratorních podmínkách i v reálné optické síti mezi uzly vzdálenými několik set kilometrů. Do prováděných experimentů bude dále zahrnut i systém WR (White Rabbit), který z PTP také vychází, ale dosahuje řádově lepší přesnosti.

Ověřte interoperabilitu dostupných zařízení, změřte a vyhodnoťte dosaženou přesnost přenosu času. Výsledky zpracujte do podoby, která umožní jejich prezentaci na konferenci spolu s článkem ve sborníku. Konečným cílem, po doplnění dalších měření navržených na základě zjištěných vlastností, je článek v odborném časopise.

The Precise Time Protocol (PTP) is used to distribute accurate time to network devices using Ethernet, i.e. at the ISO/OSI link layer. The greatest fluctuations in the frame delay occur in network switch queues. The protocol assumes support directly in the switches, when the delay time is evaluated and reported to the target device. There are different implementations of individual manufacturers, so it is necessary to know their performance and compatibility. Subject of the evaluation will be Ethernet switches from three manufacturers and also the software implementations in Linux. The measurement will be performed in laboratory conditions and in a real optical network between nodes several hundred kilometers away. The WR (White Rabbit) system, based on PTP but providing much better accuracy, will also be included in the performed experiments.

Verify the interoperability of all available devices, measure and evaluate the achieved parameters of time transfer accuracy. Process the results into a form that will allow their presentation at a conference and an article in conference proceedings. After extending by other measurements designed on the basis of the identified performance, the ultimate goal is an article in a scientific journal.

Plánované výstupy (konference a časopisy):

IMEKO TC10 - Measurement for Diagnostics, Optimization & Control
pořadatel pro rok 2023 není dosud znám

IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control
IEEE

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Paralelní vícecestný quicksort algoritmus pro OpenMP**
Parallel multiway quicksort algorithm in OpenMP

Mentor: doc. Ing. Ivan Šimeček, Ph.D.

Předmětem výzkumu bude návrh a implementace paralelního vícecestného quicksort algoritmu pro HPC. Navžený algoritmus by měl být buď in-place nebo konstatní množství pomocných datových bloků. Následně by implementace měla být porovnána s ostatními implementacemi

A new multi-threaded variant of the parallel multiway quicksort algorithm and its C++/OpenMP implementation are presented. Designed sorting algorithm should operate either in place or with a constant amount of auxiliary data blocks. It is primarily designed for high-performance computing (HPC) runtime environments. We evaluate AQsort experimentally and compare its performance with modern multi-threaded implementations of in-place and out-of-place sorting algorithms.

Plánované výstupy (konference a časopisy):

Concurrency and Computation: Practice and Experience,
Wiley Online Library

www.scpe.org
https://www.scpe.org/index.php/scpe/about

International Journal of Parallel Programming
Springer

Název zadání: **Cold-start items based recommendation**

Mentor: Rodrigo Augusto da Silva Alves

We want to investigate algorithms that handle the recommendation of new items (or for new users) in a comprehensive approach. To accomplish this, we intend to look for methods that exploit and transfer the multiple properties of items (or users) with recognized behavior to recently introduced ones.

Plánované výstupy (konference a časopisy):

ACM Recommender Systems Conference - RECSYS
ACM

ACM Transactions on Knowledge Discovery from Data (TKDD)
ACM

Název zadání: **Temporální interpretace Stable Marriage problému**
Temporal Interpretations of the Stable Marriage Problem

Mentor: Ing. Šimon Schierreich

Stable Marriage je fundamentální problém teorie stabilních párování. Vstupem problému jsou dvě stejně velké množiny agentu M a F. Každý z agentů má preference vyjádřené jako lineární uspořádání na všech agentech z opačné množiny. Cílem je najít takové párování mezi agenty, že nebude existovat dvojice m\in M a f\in F taková, že m preferuje f před aktuálně přiřazeným párem a to samé pro f. Pro tento problém existuje slavný polynomiální algoritmus, se kterým přišli v roce 1962 Gale a Shapley. Shapley za výzkum v oblasti stabilních párování dokonce získal Nobelovu cenu.

Cílem projektu je podívat se na problém z hlediska temporálních grafů, které velice dobře zachycují dynamicky se měnící svět. Společně tak budeme pracovat na několika temporálních interpretacích tohoto problému, zajímat nás budou zejména nové algoritmy a těžkostní důkazy.

Stable Marriage is a fundamental problem in the stable matchings area. The input of the problem is two sets M and F of agents. Every agent has a preference relation (linear order, in fact) overall agents from the second set. Our goal is to find matching between agents from different sets such that there is no pair of agents m\in M and f\in F such that m preferers f over the currently assigned agent and f prefers m over the currently assigned agent. There is a famous polynomial-time algorithm by Gale and Shapley solving this problem. It is worth mentioning that Shapley obtained a Nobel prize for his research in stable matchings.

The goal of this project is to study the Stable Marriage problem from the viewpoint of temporal graphs which captures very naturally the dynamics of the real world. I would like to study algorithmic upper bounds and complexity lower bounds of at least three different natural interpretations of the Stable Marriage problem in temporal graphs.

Plánované výstupy (konference a časopisy):

Symposium on Algorithmic Foundations of Dynamic Networks (SAND)

International Conference on Algorithmic Decision Theory (ADT)
EURO WG - Preference Handling

European Conference on Multi-Agent Systems
European Association for Multi-Agent Systems

Název zadání: **Neurální celulární automat pro (NCA) pro modelování fyzikálních dějů**
Neural cellular automata for modeling of physics

Mentor: Mgr. Petr Šimánek

Neurální celulární automat NCA (https://distill.pub/2020/growing-ca/) je jednoduchý, ale velmi zajímavý přístup k řešení různých problémů. Využívá koletivních výpočtů založených na komunikaci malých neurálních buněk (malé neuronové sítě), jejichž chování je naučené pomocí gradient descentu. Mezi známé aplikace patří morfogeneze, vytváření pohyblivých textur nebo jednoduché kontrolní problémy. NCA umožňují velmi robustní (samo-opravné) výpočty. Tato vlastnost a některé další vlastnosti NCA mohou být velmi užitečné při simulaci proudění tekutiny.

Úkolem je aplikovat, adaptovat a vylepšit stávající implementaci NCA a vyřešit benchmarkový problém v dynamice tekutin (proudění v doméně s pobyujícím se víkem). Cílem je ukázat, že NCA takové výpočty umožňují a že NCA dokáže generalizovat a řešit různé varianty podobného problému. Posledním úkolem je analýza výsledků.

Neural cellular automata NCA (https://distill.pub/2020/growing-ca/) is a simple but a very interesting approach to solve various problems by distributed collective calculation done multiple simple neural cells that learn by gradient descent. The known applications are morphogenesis, creation of moving textures or simple control protocols. NCA allow very robust (self-repairing) computation. Some properties of NCA may be helpful in simulation of fluid flow.

The task is to apply, adapt and improve NCA to solve a simple benchmark problem in fluid dynamics (moving lid). We want to show that NCA allow this computation and that NCA also truly learn how to solve the fluid flow. The latter would be tested by various perturbations of the original problem. The last task is to provide some analysis of the results.

Plánované výstupy (konference a časopisy):

Alife
International Society for Artificial Life

PARALLEL PROBLEM SOLVING FROM NATURE - PPSN

International Joint Conference on Neural Network IJCNN
International Neural Network Society

Název zadání: **Using Neural Cellular Automata to create Turing patterns**

Mentor: Mgr. Petr Šimánek

Neural Cellular Automata (NCA) (https://distill.pub/2020/growing-ca/) were recently introduced. The idea of NCA is to use a small CNN to learn the transition rule of a 2D cellular automata with a continuous and multi-dimensional state space, which they interpret as an image. In particular, they trained the NCA to converge to a specific image. They showed that, with proper training, NCA could reconstruct missing patches of the target image and were resilient to many classes of state perturbations. Randazzo et al. also showed that NCA can be used to classify MNIST digits. This is an example of local behaviour leading to a global agreement about the overall structure of the system.

This collective behavior is very interesting and could in principle explain some very difficult natural effects. One of the problems that appear in nature is a creating of Turing Patterns. These patterns could be found in nature as jaguar/cheetah/tiger/zebras spots or stripes. The development of these patterns is usually modeled by differential equations.

We believe that these spots and stripes are created by a different mechanism, which is much more local and works on cellular level. NCA can be the way forward. The task is apply, adapt and improve implementation of NCA for the Turing patterns, evolve some of these patterns and compare the resulting behavior to recent literature.

Plánované výstupy (konference a časopisy):

Alife
ISAL

Název zadání: **Integration of a test-case reducer into an application-level fuzzer**

Mentor: Prof. Ing. Pavel Tvrdik, CSc.

V tomto projektu se zaměříme na techniky redukce testovacích případů a jejich použití ve fuzzeru na aplikační úrovni. V minulosti jsme vyvinuli fuzzer na aplikační úrovni, který je schopen najít chyby v produkčním softwaru. Pro správce i penetračního testera je však klíčové identifikovat zdroje chyb a následně je opravit. Nicméně se ukázalo, že identifikace zdroje chyby je v moderních vícevrstvých komplexních softwarových systémech obtížná. Proto se snažíme o minimální vstupy, které přesto způsobují chybné chování softwaru. Tuto minimalizaci může zkušený tester provést ručně, je však časově náročná. Několik nedávných studií navrhlo zapojit techniky redukce testovacích případů. Jedná se o aktivní oblast výzkumu a v tomto projektu se na tyto techniky zaměříme. Ačkoli se ukázalo, že techniky minimalizace testovacích případů jsou užitečné v několika scénářích, nebyly dosud zkoumány v kontextu fuzzingu na aplikační úrovni. Naším cílem je integrovat náš fuzzer na aplikační úrovni s takovými technikami redukce testovacích případů tak, aby systém byl schopen nejen najít chyby v softwaru, ale také vytvořit minimální vstup, který chybu spustí. Výstupem projektu by měla být prototypová implementace nového fuzzeru na aplikační úrovni s integrovanými technikami redukce testovacích případů.

In this project, we will focus on test case reduction and its use in an application-level fuzzer. In the past, we have developed an application-level fuzzer that is able to find bugs in production-grade software. However, it is crucial for the maintainer, as well as the penetration tester, to identify the source of the bugs and subsequently fix them. Nevertheless, the identification of source of a bug has been proven to be difficult in modern multilayer complex software systems. Therefore, we strive for minimal input that still causes the software to misbehave. This minimization can be done manually by an experienced tester, but it is time-consuming. Several recent studies proposed to engage test case reduction techniques. This is an active area of research and in this project we will focus on these techniques. Though test case minimization techniques have been shown to be useful in several scenarios, they have not been explored in the context of application-level fuzzing. Our goal is to integrate our application-level fuzzer with such test case reduction techniques so that the system will not only be able to find bugs in the software but to produce a minimal input that triggers the bug too. The output of the project should be a prototype implementation of novel application-level fuzzer with test case reduction techniques.

Plánované výstupy (konference a časopisy):

ACM SIGSOFT International Symposium on Software Testing and Analysis
ACM

International Joint Conference on SoftwareTechnologies
INSTICC

Téma je rezervováno konkrétnímu studentovi.

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

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D.

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
IJCAI

International Joint Conference on Artificial Intelligence
IJCAI

International Journal of Operational Research
ELSEVIER

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Podpora práce s bioinformatickmi ontologiemi na platformě OpenPonk**
Supporting Bioinformatic Ontologies on the OpenPonk Platform

Mentor: doc. Ing. Robert Pergl, Ph.D.

Cílem projektu je vývoj a ověření podpory pro modelování bioinformatických ontologií ve formátu RDF/OWL pro platformu https://openponk.org. Vyvinutý nástroj by měl umět načítat a zobrazovat ontologie a poskytovat možnosti dotazování a manipulací pomocí jazyka Pharo. Výstupem budou:
1. Vlastní implementace + testy + dokumentace
2. Ověření na vhodné ukázkové studii
2. Vědecký článek popisující dosažené výsledky a jejich přínos pro bioinformatickou komunitu.

The aim of the project is to develop and verify support for modeling bioinformatic ontologies in RDF / OWL for the https://openponk.org platform. The developed tool should be able to load and display ontologies and provide functions for manipulating and querying them using the Pharo language. The outputs will be:
1. The implementation + tests + documentation
2. Verification on a suitable case study
2. Scientific article describing the results achieved and their contribution to the bioinformatic community.

Plánované výstupy (konference a časopisy):

Výsledek bude uplatněn v rámci mezinárodní infrastruktury ELIXIR CZ a publikován na bioinformatické konferenci / časopise

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Fyzicky neklonovatelné funkce**
Physical Unclonable Functions

Mentor: Ing. Filip Kodýtek, PhD.

Návrh nových případně implementace již existujících řešení PUF (fyzicky neklonovatelné funkce) a analýza jejich chování.

Plánované výstupy (konference a časopisy):

Digital System Design (DSD)

Design and Diagnostics of Electronic Circuits and Systems (DDECS)

Materiály pro výuku v předmětech BI-HWB/NI-HWB

Název zadání: **Generování klíčů pomocí fyzicky neklonovatelných funkcí**

Mentor: Ing. Filip Kodýtek, PhD.

Cílem bude implementace vybrané fyzicky neklonovatelné funkce (PUF) a její následné využití pro generování klíčů. To zahrnuje výběr účelu, pro jaký klíč bude sloužit a následně návrh zpracování výstupu PUF tak, aby jej šlo pro generování klíčů využít.

Plánované výstupy (konference a časopisy):

Design and Diagnostics of Electronic Circuits and Systems (DDECS)

Digital System Design (DSD)

Materiály pro výuku předmětů BI-HWB/NI-HWB

Název zadání: **Generátory skutečně náhodných čísel**

Mentor: Ing. Filip Kodýtek, PhD.

Implementace již existující (případně návrh nové) architektury skutečně náhodného generátoru (TRNG). Analýza vlastností implementovaného TRNG a vyhodnocení jeho náhodnosti.

Plánované výstupy (konference a časopisy):

Výstupem budou primárně materiály pro výuku předmětů BI-HWB/NI-HWB. Eventuelně bude snaha o publikaci, pokud bude dostatečná inovace.

Název zadání: **Využití generativních neuronových sítí**

Mentor: Ing. Jaroslav Kuchař, Ph.D.

V současné době existuje velké množství generativních modelů jako jsou např. variatonal autoencoders (VA), generative adversarial nets (GAN) a další. Jejich aplikaci nalezneme v mnoha oblastech. V případě GAN se jedná zejména o oblasti spojené se zpracováním obrazu (computer vision apod.).

Cílem tohoto tématu je zaměřit se na využití GAN i v jiných oblastech než je přímo práce s obrazovými daty, ale může v těchto situacích existovat analogie. Jedním z příkladů může být např. dvojrozměrná data reprezentující pozice hry, rozložení prvků aplikace, grafy a jejich maticové reprezentace a další. Očekávaným výstupem je provést rešerši, využít GAN a vyhodnotit jejich vhodnost v takovýchto případech.

- Seznamte se s problematikou generativních modelů
- Proveďte rešerši přístupů se zaměřením na GAN
- Navrhněte vhodné oblasti využití GAN mimo zpracování obrazu
- Navrhněte vhodné metody řešení pro zvolené oblasti
- Proveďte experimenty
- Vyhodnoťte kvalitu navržených přístupů

Plánované výstupy (konference a časopisy):

CIKM: International Conference on Information and Knowledge Management
ACM

WCIDM: International Workshop on Computational Intelligence and Data Mining
ITAT

Případně CIKM, WSDM, KDD, ICML, WWW a jejich workshopy

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Improving time integration in Meshraphnets**

Mentor: Mgr. Vojtěch Rybář

Meshgraphnets [1] is powerful approach to modelling complex physical systems with graph neural networks for mesh-based simulations.

Right now, it uses simple forward Euler rule for time stepping. The goal of this project is to improve time integration in meshgraphnets by introducing adaptive time stepping and/or different approach to time integration, e.g. [2].

[1] Pfaff, T., Fortunato, M., Sanchez-Gonzalez, A., & Battaglia, P. W. Learning mesh-based simulation with graph networks. ICLR 2021
[2] Chen, Ricky TQ, et al. "Neural ordinary differential equations." Advances in neural information processing systems 31 (2018).

Plánované výstupy (konference a časopisy):

International Joint Conference on Neural Networks (IJCNN)
IEEE

AISTATS: International Conference on Artificial Intelligence and Statistics

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Srovnávací studie různých typů rekurentních a konvolučních neuronových sítí pro predikci vývoje cen akcií v čase**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D.

Vypracujte rešerši použití různých typů neuronových sítí (různé typy RNN, CNN) aplikovaných na problém predikce cen akcií. Navrhněte sérii experimentů umožňujících provést srovnání jednotlivých přístupů. Algoritmy implementujte a proveďte experimenty, výsledky srovnávací studie zpracujte formou článku na konferenci nebo do časopisu.

Plánované výstupy (konference a časopisy):

European Symposium on Neural Networks
ENNS

European Conference on Artificial Intelligence
IJCAI

Téma je rezervováno konkrétnímu studentovi.

Název zadání: **Hierarchický model pro rozpoznávání textu v ručně psaných záznamech v matrikách ze 17., 18. a 19. století**

Mentor: Mgr. Ing. Ladislava Smítková Janků, Ph.D.

Výzkum zaměřený na kombinaci metod statistické relační umělé inteligence, metod pro zpracování obrazu a neuronových sítí realizovaný na datech získaných z ručně psaných záznamů z matrik ze 17., 18. a 19. století. Student by se měl zaměřit na tvorbu hierarchického modelu, kde na nejvyšší úrovni pracuje s pravděpodobnostními modely zohledňujícími pravděpodobnost výskytu konkrétních frází a slov, na nižší úrovni pak použít modelování znaků pomocí neuronových sítí. Předpokládaným výstupem je článek na konferenci nebo do časopisu.

Plánované výstupy (konference a časopisy):

European Symposium on Neural Networks
ENNS

European Conference on Artificial Intelligence
IJCAI

Název zadání: **Automatizovaná extrakce vzorku pneumatiky vozidla**
Automated vehicle tyre treads extraction

Mentor: doc. RNDr. Ing. Marcel Jiřina, Ph.D.

Vzorky pneumatik jsou velmi různorodé a do značné míry identifikující konkrétní vozidlo nebo alespoň jeho typ. Srovnání vzorku pneumatiky s neznámým otiskem pneumatiky tak může významně zúžit skupinu aut, které mají stejný vzorek.
Cíle projektu vychází a navazují na bakalářskou práci studenta, který v ní navrhl, implementoval o ověřil kamerový systém pro snímání pneumatik vozidel v reálném prostředí.
Projekt výzkumného léta se zaměří na návrh a ověření metod zpracování obrazu, které umožní snímky převést do definované podoby a využití je pro další analýzy. Vzhledem k tomu, že měření v reálném externím prostředí je obtížné, kvůli zajištění konstantních podmínek měření (počasí, osvětlení, poloha vozidla, jeho vzdálenost, geometrické zkreslení...), bude cílem výzkumu během léta návrh robustních metod, které umožní eliminovat nebo aspoň výrazně snížit tyto externí vlivy a automatizovaně poskytnout extrahovaný vzorek pneumatiky v jednotné podobě jako rozvinutý pás (rastrový šedotónový snímek) pro další zpracování.
Student se zaměří zejména na tyto aktivity a výzkumné cíle:

1) geometrické a jasové transformace snímků,
2) identifikaci (výběr) vhodného snímku (zejm. nejostřejší a s přítomnou pneumatikou),
3) automatizovanou lokalizaci pneumatiky ve snímku,
4) sestavení modelu a nalezení vhodné geometrické transformace (transformace 3D válce/kuželu na 2D obdélník se vzorkem pneumatiky),
5) identifikaci parametrů modelu pro konkrétní pneumatiku a
6) jasové transformace navazující na geometrické transformace extrahovaného vzorku.
Výstupem projektu bude
1) soubor implementovaných a ověřených metod pro extrakci vzorku pneumatiky,
2) soubor vzorových ukázek extrahovaných vzorků pneumatik z reálných měření a
3) připravená publikace do časopisu/na konferenci.

The tyre treads are very diverse and to a large extent identify a particular vehicle or at least its type. Thus, comparing a tyre treads with an unknown tyre print can significantly narrow the group of cars that have the same treads.
The objectives of the project are based on and build upon the student's bachelor thesis, in which he designed, implemented, and verified a camera system for capturing vehicle tires in a real-world environment.
The research summer project will focus on the design and validation of image processing methods that will allow the images to be converted into a defined form and used for further analysis. Since measurements in real external environments are difficult due to the provision of constant measurement conditions (weather, illumination, vehicle position, vehicle distance, geometric distortion...), the aim of the research during the summer will be to design robust methods to eliminate or at least significantly reduce these external influences and to provide the extracted tire treads in a uniform form as a developed strip (raster grayscale image) for further processing in an automated way.

In particular, the student will focus on the following activities and research objectives:
1) geometric and luminance transformations of images,
2) identification (selection) of an appropriate image (especially the sharpest one and with the tire present in the image),
3) automated localization of the tyre in the image,
4) model design and finding a suitable geometric transformation (transformation of a 3D cylinder/cone into a 2D rectangle with a tire treads),
5) identification of the model parameters for a specific tire and
6) the brightness transformations related to the geometric transformations of the extracted sample.
The output of the project will be
1) a set of implemented and validated methods for tire sample extraction,
2) a set of sample tire samples extracted from real measurements; and

3) a prepared journal/conference publication.

Plánované výstupy (konference a časopisy):

International Journal of Computer Vision

Computer Vision and Image Understanding

International Machine Vision and Image Processing Conference (ICMV 2022)

Téma je rezervováno konkrétnímu studentovi.