Title: Verification of Cost Bounds in Coq

Description: The goal of the project is to develop a checker that can formally prove, by using the Coq proof assistant, the correctness of the cost bounds inferred by an existing cost analysis tool (whose implementation has not been proven correct). We will follow a translation validation approach in which rather than verifying the cost analyzer, we verify the correctness of the bounds generated by it. Both proof assistants and static analysis tools will be studied in the courses of the Master.

Supervisors: Elvira Albert (elvira@sip.ucm.es) and Samir Genaim (sgenaim@ucm.es)

Title: Plugin for automatic testcase generation in Python

Description: Testing is an important activity of software developers. It improves code quality and detects bugs before releasing your program. Additionally, Python is one of the most popular programming languages. In this master thesis, you will implement a plugin for a popular IDE (Eclipse or IntelliJ). It will automatically generate a set of testcases for a Python program such that they fulfill a specific type of branch coverage.

Supervisors: Manuel Nuñez (mn@sip.ucm.es), José Ignacio Requeno (jrequeno@ucm.es)

Title: Study of Computability and/or Complexity

Description: the project will consist in developing some original research in Computability or Complexity areas in some topic to be agreed with the student. For instance, the following choices are possible: (a) considering a problem from the Computer Science area or out of it (e.g. Economics, Biology, Physics, Political Science, social sciences in general, etc.) whose Complexity or Computability properties have not been studied yet, and proving properties such as NP-hardness, approximability hardness, hardness beyond NP, Turing-completeness, etc.; (b) developing some new knowledge around the P vs NP problem, such as identifying properties of problems which cannot be solved with polynomial-size circuits (approaching P \neq NP via P/poly); (c) identifying new properties around central theorems of Complexity theory, such as the PCP theorem; etc.

Supervisor: Ismael Rodríguez Laguna (isrodrig@ucm.es).

Title: Formal testing of quantum programs

Description: The goal of this master's thesis is to review the state-of-the-art on formal approaches to test quantum programs and present a new proposal building on top of current work. Specifically, metamorphic testing, a testing technique used to validate systems where an oracle is not available, seems to be a very suitable candidate to work well with quantum programs. In order to carry out this thesis, the student does not need to have previous knowledge on quantum programming or formal testing.

Supervisors: Luis Llana (llana@ucm.es) and Manuel Núñez (mn@sip.ucm.es)

Title: Block-based graphical environments for structured data

Description: In the last few years, different formats for structured data, like XML, JSON or YAML have been proposed. These are textual formats, which typically define well-formedness constraints in some form to restrict the kind of documents considered valid (e.g., see https://json-schema.org/ for JSON). However, writing a correct document may become challenging for users without a technical background.
In this project, we will explore the use of graphical block languages for specifying structured data documents (JSON in particular). Block languages are popular nowadays, thanks to systems like Scratch (https://scratch.mit.edu/) which have lowered the entry barrier to programming for non-experts. We will use Google's Blockly (https://developers.google.com/blockly) as a basis for the project, since it allows defining block types, together with code generators that will be able to produce the desired JSON serialization. This way, given a JSON schema (https://json-schema.org/), the goal is the generate automatically a block-based environment enabling the graphical definition of JSON documents using specialized block types, which then can be serialized into correct-by-construction JSON textual documents.

Supervisor: Juan de Lara (Juan.deLara@uam.es)

Title: Verification of Dynamic Programming algorithms

Description: Dynamic programming algorithms are suitable to solve those problems that can be expressed by means of a recurrence that satisfies some properties, such as optimal substructure and overlapping subproblems. The goals of this master's thesis are (1) to verify a selection of usual dynamic programming algorithms with Dafny, a verification-aware programming language, (2) to identify the patterns that are common to a wide range of dynamic programming algorithms in order to devise a generic methodology for verifying them. Prior knowledge of Dafny is not required to address these goals, but it is advisable to be enrolled in the Computer-aided Program Verification elective course.

Supervisors: Clara Segura (csegura@sip.ucm.es), Manuel Montenegro (montenegro@fdi.ucm.es)

Title: Cryptographic Protocols for Interoperability of Payment Channels

Description: Payment channels (PC) have been proposed as a solution to the limited transaction throughput of blockchain technologies. More specifically, PC allow two users to make multiple transactions without committing all the transactions to the blockchain. In a typical PC, users first send a transaction to lock their coins in a deposit. Payments are then carried out by exchanging authorized agreements of redistributions of the deposit balance. Finally, the last agreed balance is transfer back to the users and the PC is closed. In this way, only two transactions are added to the blockchain but a nearly unlimited number of payments can be made between the two users. In order to extend this

functionality to any number of users, two different protocol families have been proposed: (i) Payment channel networks (PCN) where the sender and the receiver do not share a PC. A payment is routed instead through multiple PCs that form a path; and (ii) payment channel hubs (PCH) where the Hub acts as a central entity, which has a PC with each of the users in the system, and facilitates off-chain payments among the users. Cryptographic definitions for both the functionality as well as the security properties are available for both, PCN and PCH. The goal of this project is to investigate the interoperability of PCNs and PCHs and design a cryptographic protocol that enables an off-chain payment from a sender participating in one protocol family (e.g. a PCN) to a receiver participating in the other protocol family (e.g PCH). We call them "PCN-to-PCH" and "PCH-to-PCN" payment protocols.
Note: The TFM can be done in combination with a (curricular and/or extracurricular) internship at the IMDEA Software Institute. Having taken the master's course on cryptographic protocols is considered an important prerequisite to do this TFM.

Supervisors: Pedro Moreno Sánchez (pedro.moreno@imdea.org), Dimitrios Vasilopoulos (dimitrios.vasilopoulos@imdea.org), IMDEA Software Institute

---

Title: Zero-knowledge proofs for set membership

Description: Zero-knowledge proofs are cryptographic protocols that allow a prover to convince a verifier that a statement holds without revealing further information. This project concerns the study of zero-knowledge proofs for the problem of set membership, in which the prover wants to convince the verifier that it owns an element from a public large set without revealing which element. Another desired property of solutions to this problem is succinctness, which means that the size of the proof is short and does not depend on the size of the set. Solutions to this problems have applications to secure outsourcing of computation, and to privacy and anonymity in blockchains. The goal of the TFM is to study state of the art protocols in this area, and to investigate the design of new protocols that can achieve better efficiency and/or richer functionality. In particular, with respect to functionality, the project also focuses on the development of solutions that allow proving non-membership.
Note: The TFM can be done in combination with a (curricular and/or extracurricular) internship at the IMDEA Software Institute. Having taken the master's course on cryptographic protocols is considered an important prerequisite to do this TFM.

Supervisors: Dario Fiore (dario.fiore@imdea.org), Dimitris Kolonelos (dimitris.kolonelos@imdea.org), IMDEA Software Institute

---

Title: Publicly verifiable secret sharing schemes.

Description: Secret sharing schemes allow to distribute the knowledge of a secret among several parties, while keeping control about which subsets of parties can later reconstruct it. Publicly verifiable secret sharing is a variant of secret sharing where in addition the dealer of the secret proves that the secret has been correctly shared (without revealing the secret) and parties can later prove that they are reconstructing correctly. It has applications in domains such as distributed randomness generation. The goal of this project is first to study and compare some recent proposals based on discrete logarithm

assumptions, and then to investigate if the techniques in these proposals can be applied to construct publicly verifiable secret sharing schemes based on other assumptions, such as factoring related assumptions.
Note: The TFM can be done in combination with a (curricular and/or extracurricular) internship at the IMDEA Software Institute. Having taken the master's course on cryptographic protocols is considered an important prerequisite to do this TFM.

Supervisor: Ignacio Cascudo (ignacio.cascudo@imdea.org) , IMDEA Software Institute.
