FCT Fundação para a Ciência e a Tecnologia

MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

## Concursos de Projetos de I&D

Calls for R&D Projects

- Voltar à descrição do projeto
  Back to project description
- Imprimir esta página
  Print this page

## Visão global da candidatura

Application overview

**Referência do projeto**
Project reference
PTDC/CCI-COM/1221/2021 **(Lacrado a 09-03-2021 às 19:01)**

**Ocultar todos as secções desta candidatura**
Hide all sections for this application
–

### 1. Identificação do projeto

1. Project description
–

**Área científica principal**
Main Area
Ciências da Computação e Ciências da Informação - Ciências da Computação
Computer and Information Sciences - Computer Sciences

**Área científica Secundária**
Secondary area
*(Vazio)*
*(Void)*

**Painel de Avaliação**
Evaluation Panel
Computer and Information Sciences and Informatics Evaluation Panel - 2021

**Acrónimo do projeto**
Project's Acronym
PRESTO

**Título do projeto (em português)**
Project title (in portuguese)
Software Confiável para Criptografia Pós-Quântica e Computação Segura Distribuída

**Título do projeto (em inglês)**
Project title (in english)
High-Assurance Cryptographic Software for Post-Quantum and Distributed Secure Computation

**Financiamento solicitado**
Requested funding
249.502,85€

**Palavra-chave 1**
Software Confiável para Criptografia

**Keyword 1**
High-Assurance Cryptographic Software

**Palavra-chave 2**
Verificação de Programas

**Keyword 2**
Program Verification

**Palavra-chave 3**
Criptografia Pós-Quantica

**Keyword 3**
Post-Quantum Cryptography

**Palavra-chave 4**
Computação Segura Distribuída

**Keyword 4**
Secure Distributed Computation

**Data de início do projeto**
Starting date
01-01-2022

**Duração do projeto em meses**
Duration in months
36

**Existem questões éticas identificadas neste projeto?**
Are there Ethics Issues identified in this project?
Não
No

**Objetivos de Desenvolvimento Sustentável das Nações Unidas – Agenda 2030**
United Nations Sustainable Development Goals – 2030 Agenda

Objetivo 10 - Reduzir as desigualdades no interior dos países e entre países
Goal 10 - Reduce inequality within and among countries

Objetivo 16 - Promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas a todos os níveis
Goal 16 - Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

Objetivo 17 - Reforçar os meios de implementação e revitalizar a Parceria Global para o Desenvolvimento Sustentável
Goal 17 - Strengthen the means of implementation and revitalize the global partnership for sustainable development

**Enquadramento da candidatura nos Objetivos de Desenvolvimento Sustentável**
Framework of the application for the United Nations Sustainable Development Goals

Cryptography is the technological centerpiece for ensuring freedom of expression and implementation of basic human rights in an ever-growing digital world. There is growing awareness that cryptography plays an important role in providing universal, affordable and trustworthy internet to least developed countries (Goal 9). Cryptographic techniques such as encryption and anonymity are fundamental pillars for establishing online security and provide all individuals equal means to protect their privacy, empowering them to read, develop and share information without interference and regardless of their origins, beliefs or ethnic, religious, sexual, gender or any other orientation (Goal 16).
This pivotal role shows high-assurance cryptographic software is of utmost importance. Although many crypto standards are well-established and widely accessible, there are much less freely accessible quality implementations, which are vital to guarantee that no security threats are introduced in practice, but require significant resources and expertise. Across the history of cryptography, there are many examples of real vulnerabilities that could seriously compromise encryption and anonymity guarantees but were only avoided or known by a few major actors, be it institutions or countries. The more recent potential threat of quantum computers is another element that may greatly tip the scale in favor of major actors, given the vast amount of resources and expertise necessary to perform a quantum attack. In order to mitigate the imminence of these risks, this project seeks to provide high-assurance implementations of post-quantum cryptographic constructions and to contribute to the dissemination of widely available quality implementations, therefore contributing to build capacity among developing countries by reducing the dependence on non-experts and commoditizing technology (Goal 17).
The concrete technological use cases explored in this project, such as secure multi-party computation, ZK proofs or distributed ledgers have a far-reaching social potential as they give technological answers to secure e-government e-voting and fraud detection, priorities of UNU-EGOV, reducing corruption and improving accountability, transparency and resilience of public institutions (Goal 16). By enabling collaborative confidential computation without trusted entities, secure outsourcing to the cloud and the creation public tamper-proof records that are viewed by an entire community, these technologies may also improve the regulation and monitoring of financial markets (Goal 10), promote global partnerships that can foster engagement in society and strengthen social equality (Goal 10), or endorse policy coherence and monitor sustainable development indices (Goal 17). For example, they may be used to conduct wide gender studies while protecting fundamental freedoms, or constructing a global digital trade platform whilst ensuring fair trade and non-reciprocity rights.

## 2. Instituições envolvidas
2. Institutions and their roles

### Instituição Proponente
Principal Contractor

**Inesc Tec - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)**
Campus da FEUP - Rua Dr. Roberto Frias, 378
4200-465Porto

**Descrição da Instituição**
INESC TEC is a private, non-profit association dedicated to scientific research and technological development, technology transfer, advanced consulting and training, and pre-incubation of new technology-based companies.

The University of Porto, INESC, the Polytechnic Institute of Porto, the University of Minho and the University of Trás-os-Montes e Alto Douro are INESC TEC's associates (UM and UTAD since February 2019). Presently, INESC TEC's main sites are located in the cities of Porto, Braga and Vila Real. At the end of 2020, INESC TEC's 13 R&D Centres hosted 732 integrated researchers (354 PhDs), including staff researchers, researchers from Higher Education Institutions, grant holders and affiliated researchers. INESC TEC's team also includes trainees and technical and administrative support staff.

INESC TEC's vision is to be a relevant international player in Science and Technology in the domains of Computer Science, Industrial and Systems Engineering, Networked Intelligent Systems, and Power and Energy.

As an institution operating at the interface between the academic and business worlds, bringing academia, companies, public administration, and society closer together, through its "managed science" model, INESC TEC leverages the knowledge and results generated as part of its research, in technology transfer projects, seeking impact both through value creation and social relevance.

### Instituição Participante
Participating Institution

**NOVA.ID.FCT - Associação para a Inovação e Desenvolvimento da FCT (NOVA.ID.FCT/FCTUNL/UNL)**
Campus de Caparica, da Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa
2829-516Caparica

**Descrição da Instituição**
NOVA.ID.FCT (Associação para a Inovação e Desenvolvimento da FCT) is a private non-profit research organisation devoted to R&D&I activities, recognised by the Portuguese System for Science and Technology of FCT (Fundação para a Ciência e Tecnologia).

NOVA.ID.FCT based at FCT NOVA acts as the legal institution of research units, carrying out research work and managing R&D&I projects. This entity forms qualified human resources training, consulting expertise, knowledge dissemination and technology transfer activities.

FCT NOVA has achieved extraordinary national relevance on several programmes, most of them pioneers. From 2011 to 2015, FCT NOVA published more than 5500 papers indexed in ISI Web of Science. FCT NOVA has a portfolio of around 50 patent families. This shows the visibility as a higher technical and science school engineering.

NOVA.ID.FCT has experience in managing FP7 projects and has already been awarded with 27 projects in H2020 adding up to 13€ million. This shows the visibility and competitiveness of the NOVA.ID.FCT at European and International level and strong experience in collaborative projects, working with partners from all over the world.

These numbers reflect the quality of research carrying out at NOVA.ID.FCT and the suitability of infrastructures and facilities to develop all R&D&I across all research units recognised by FCT.

In this project, the participation is through Research Unit NOVA LINCS.

### Unidade de Investigação

Research Unit

**Inesc Tec - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)**
Campus da FEUP - Rua Dr. Roberto Frias, 378
4200-465Porto

**Unidade de Investigação Adicional**
Additional Research Unit

**NOVA Laboratory for Computer Science and Informatics (NOVA LINCS)**
Faculdade de Ciências e Tecnologia - Universidade NOVA de Lisboa Departamento de Informática - Campus da Caparica
2829-516Caparica

## 3. Componente Científica

3. Scientific Component

–

### 3.1. Sumário

3.1 Abstract

### 3.1.a (Em português)

3.1.a (In Portuguese)

A Criptografia Assistida por Computador desenvolve ferramentas para a análise e implementação de protocolos criptográficos, incluindo linguagens de especificação e implementação, compiladores e ferramentas de verificação. A vertente de verificação formal abre caminho para o software criptográfico confiável, que se constitui como o objetivo primordial do PRESTO.

Um SoK [SoK] publicado recentemente na IEEE S&P 2021 apresenta os desafios nesta área; dois deles constituem a motivação central para o PRESTO: 1) remover entraves de escalabilidade na análise de protocolos distribuídos complexos e 2) permitir a transição para a criptografia pós-quântica.

O PRESTO debruça-se sobre estes desafios no cenário concreto da plataforma que conjuga HACSpec, Jasmin e EasyCrypt:

- HACSpec [HACS] é uma nova linguagem de especificação para criptografia, orientada para utilizadores não peritos em verificação formal; pretende tornar-se numa linguagem de especificação comum (e executável) que possa ser adotada em standards criptográficos. Especificações próprias para cada ferramenta podem ser automaticamente geradas a partir de uma especificação HACSpec, permitindo que resultados de diferentes ferramentas possam ser comparados e compostos ao nível da especificação.

- EasyCrypt [EC] é um motor de prova interativo para criptografia que utiliza a ferramenta Why3 para automação. Permite raciocinar sobre segurança e correção de programas criptográficos através de lógicas de programas expressivas que variam da lógica de Hoare clássica à lógica de Hoare relacional probabilística sobre programas abertos (i.e., programas parametrizados por algoritmos adversários). O EasyCrypt tem sido utilizado com sucesso na análise de protocolos industriais relevantes e standards criptográficos amplamente utilizados.

- Jasmin [JASM] é uma linguagem de programação para código criptográfico eficiente, que assenta num compilador certificado para código nativo. O Jasmin é orientado para verificação formal, sendo o compilador de Jasmin capaz de gerar descrições EasyCrypt do programa fonte. Um programa Jasmin pode ser verificado quanto a correção e segurança relacionando-a com uma especificação em EasyCrypt e, possivelmente, gerada a partir de código HACSpec.

O objetivo do PRESTO é avançar o estado da arte aos níveis fundamental e aplicado desenvolvendo novas extensões para estas ferramentas e demonstrando a sua aplicabilidade a exemplos relevantes e com impacto no mundo real.

O PRESTO focar-se-á em construções criptográficas concretas no domínio da criptografia pós-quântica (PQC) e da computação distribuída segura; as construções alvo poderão servir como contribuições para processos de standardização ou para bibliotecas e protocolos criptográficos amplamente difundidos.

Apresenta-se a seguir um sumário dos principais desafios.

Não é possível prever se e quando os computadores quânticos serão uma ameaça real. No entanto, como forma de contingência a longo prazo, a standardização e difusão em massa da criptografia pós-quântica é uma realidade. Não dispomos de ferramentas que suportem o raciocínio sobre construções PQC atualmente consideradas para standards [NIST]. Ao nível fundamental, necessitamos de novas lógicas de programas para o raciocínio mecânico sobre provas de segurança de PQC, nas quais atacantes dispõem de um computador quântico. Ao nível aplicacional, é necessário estender as ferramentas existentes para raciocinar sobre tipos de dados, distribuições e operações necessárias à implementação de PQC.

A análise de protocolos criptográficos distribuídos é um desafio, tanto no papel como em provas assistidas por computador. Raciocinar de forma composicional permite controlar a complexidade, existindo teorias já maduras para a construção modular de protocolos. No entanto, os modelos de execução distribuída são diferentes daqueles que são capturados na lógica de programas de ferramentas como EasyCrypt e Why3. Nos fundamentos, há necessidade de lógicas formais para raciocinar sobre protocolos distribuídos que permitam estender os existentes nas ferramentas atuais, de uma forma natural. Ao nível aplicado, iremos focar-nos inicialmente em protocolos que estão ao alcance das ferramentas atuais, considerando classes mais fracas de adversários e modelos de execução simplificados. Estes protocolos são relevantes na prática pela sua eficiência e são exemplos ideais para o estudo de formas de reduzir o esforço de verificação sistematizando padrões e desenvolvendo bibliotecas de suporte e automação.

A equipa do PRESTO tem um registo excelente de colaboração com as equipas internacionais que desenvolvem e mantêm as ferramentas HACSpec, Jasmin, EasyCrypt e Why3. Este projeto faz parte de um esforço conjunto para a resolução dos problemas acima identificados. Investigadores que lideram o desenvolvimento destas ferramentas são consultores desta proposta, garantindo que os resultados estão alinhados e contribuem para o impacto destas iniciativas.

### 3.1.b (Em inglês)

3.1.b (In English)

Computer Aided Cryptography (CAC) aims to develop tools for the analysis and implementation of cryptographic protocols, including specification and implementation languages, compilers and formal verification tools. The formal verification dimension opens the way for High-Assurance Cryptographic Software, the overarching goal of PRESTO.

A recent SoK paper [SoK] published at IEEE S&P 2021 summarises challenges in this area; two of these challenges serve as the main motivation for PRESTO: 1) removing scalability bottlenecks in the analysis of distributed cryptographic protocols and 2) enabling the transition to post-quantum cryptography.

PRESTO considers these challenges in the concrete setting of the tool-chain that combines HACSpec, Jasmin and EasyCrypt.

- HACSpec [HACS] is a new specification language for cryptography aimed at non-experts in formal verification. HACSpec aspires to be a common (executable) specification language that can be adopted in cryptographic standards. Tool-specific specifications can be automatically generated from a single HACSpec specification, so that formal verification results obtained using different tools can be compared and composed at the specification level.

- EasyCrypt [EC] is an interactive prover for cryptography; it uses Why3, a deductive verification tool, as a backend for automation. EasyCrypt allows reasoning both about security proofs and the correctness of crypto code using program logics, ranging from standard Hoare logic to probabilistic relational Hoare logic over open programs (i.e., programs parametrized by adversarial algorithms). EasyCrypt has been used to analyse a number of cryptographic constructions, including high-profile industrial protocols and widely used cryptographic standards.

- Jasmin [JASM] is an implementation language for high-speed cryptographic code, which comes with a certified (verified in Coq) compiler to assembly. Jasmin is formal verification friendly, as the Jasmin compiler can also generate EasyCrypt descriptions of source programs: Jasmin programs can be proved correct and secure by relating them to specifications analysed in EasyCrypt and, in particular, those generated from HACSpec tool-agnostic specifications.

The objective of PRESTO is to progress beyond the state of the art at both the foundational and applied research levels by developing new extensions to this tool-chain and demonstrating its applicability to concrete examples that can have real-world impact.

PRESTO will focus on concrete cryptographic constructions and implementations of post-quantum cryptography (PQC) and secure distributed computation that can serve as inputs to standardisation processes or as contributions to widely deployed cryptographic libraries and protocol software stacks.

We summarise the main challenges in both of these settings next.

We do not know if or when quantum computers will become a real threat, but standardisation and widespread deployment of post-quantum cryptography (PQC) is around the corner as a result of long-term risk management. However, we do not currently have CAC tools that support reasoning about PQC constructions currently considered for standardisation [NIST]. At the foundational level, we need new program logics for formal mechanised reasoning about PQC security proofs, where attackers can perform quantum computations. At the applied research level, we must extend the existing tools to support reasoning about data types, distributions and operations needed to implement PQC.

Reasoning about distributed cryptographic protocols is a challenge in both paper and machine-checked cryptographic proofs. Compositional reasoning permits taming complexity and there exists a mature theory in cryptography for constructing protocols modularly. However, the underlying distributed execution models are fundamentally different from those captured in the program logics of EasyCrypt and Why3. At the foundational level, we need new formal logics to reason about distributed protocols that permit extending those in existing tools in a natural way. At the applied research level, we can initially focus on classes of protocols that are within reach of current tools, considering weaker classes of adversaries and simplified execution models. Such protocols are relevant for practice due to their efficiency, and they are well suited for initial studies on how to reduce formal verification time by consolidating design patterns, developing support libraries and adding automation.

The PRESTO team has a strong track record in collaborating with the international teams that develop, maintain and deploy the HACSpec, Jasmin, EasyCrypt and Why3 tools. The PRESTO proposal is part of an ongoing joint effort to address the identified challenges. Researchers that lead the development of these tools are consultants in PRESTO to ensure that the results of the project are aligned with and contribute to the overall impact of these initiatives.

### 3.1.c Resumo para publicação (em português)

3.1.c Abstract for publication(in Portuguese)

A Criptografia Assistida por Computador desenvolve ferramentas para a análise e implementação de protocolos criptográficos, incluindo linguagens de especificação e implementação, compiladores e ferramentas de verificação. A vertente de verificação formal abre caminho para o software criptográfico confiável, que se constitui como o objetivo primordial do PRESTO. O objetivo do projeto PRESTO é avançar o estado da arte aos níveis fundamental e aplicado, desenvolvendo novas extensões para a cadeia de ferramentas Jasmin-EasyCrypt e demonstrando a sua aplicabilidade a exemplos relevantes e com impacto no mundo real. O projeto PRESTO irá também integrar estas ferramentas na infraestrutura HACSpec e promover a compatibilidade e interoperabilidade de artefactos de software verificados com projetos externos. Um SoK [SoK] publicado recentemente na IEEE S&P 2021 apresenta os desafios nesta área; dois deles constituem a motivação central para o PRESTO: 1) remover entraves de escalabilidade na análise de protocolos distribuídos complexos e 2) permitir a transição para a criptografia pós-quântica. O projeto PRESTO focar-se-á em construções criptográficas concretas no domínio da criptografia pós-quântica (PQC) e da computação distribuída segura; as construções alvo poderão servir como contribuições para processos de standardização ou para bibliotecas e protocolos criptográficos amplamente difundidos.

### 3.1.d Resumo para publicação (em inglês)

3.1.d Abstract for publication(in English)

Computer Aided Cryptography (CAC) aims to develop tools for the analysis and implementation of cryptographic protocols, including specification and implementation languages, compilers and formal verification tools. The formal verification dimension opens the way for High-Assurance Cryptographic Software, the overarching goal of PRESTO. The objective of PRESTO is to progress beyond the state of the art at both the foundational and applied research levels by developing new extensions to the Jasmin-EasyCrypt tool-chain and demonstrating its applicability to concrete examples that can have real-world impact. PRESTO will also integrate this tool-chain in the HACSpec framework and promote compatibility and interoperability of formally verified software artifacts with external developments. A recent SoK paper [SoK] published at IEEE S&P 2021 summarises challenges in this area; two of these challenges serve as the main motivation for PRESTO: 1) removing scalability bottlenecks in the analysis of distributed cryptographic protocols and 2) enabling the transition to post-quantum cryptography. PRESTO will focus on concrete cryptographic constructions and implementations of post-quantum cryptography (PQC) and secure distributed computation that can serve as inputs to standardisation processes or as contributions to widely deployed cryptographic libraries and protocol software stacks.

## 3.2. Descrição Técnica

3.2 Technical Description

### 3.2.1. Revisão da Literatura

3.2.1. Literature Review

Formal methods progressed to an impressive level of maturity, and several tools for systematically preventing entire classes of bugs in crypto software now exist. Frameworks like F* [FSTR], EasyCrypt [EC], and Coq [FIAT] are used to verify high-performance cryptographic code written in C and assembly. Tools like CryptoVerif [CVRF] and EasyCrypt are used to verify the correctness of crypto security proofs. In practice, protocol stacks for TLS [TLS], Signal [SIGN], Key Management [KMS] and crypto standards [SHA3,HACL] have been verified with these tools.

PRESTO focuses on a tool-chain that includes EasyCrypt, its backend Why3 [WHY3], and the Jasmin language. EasyCrypt is an interactive proof assistant for the verification of cryptographic security proofs. EasyCrypt adopts the code-based approach, where primitives, security goals and hardness assumptions are expressed as probabilistic programs. EasyCrypt offers logics to reason about programs written in an imperative language, as well as establishing relations between two program executions. Under the hood, EasyCrypt relies on Why3, a platform for deductive program verification; proof goals in the EasyCrypt logic are translated into Why3 for automated discharge using SMT solvers. The EasyCrypt logics have been successfully used to machine-check a number of relevant crypto security proofs and implementations [SHA3,EUC,MASK,DIFP].

Jasmin [JASM] is a programming language designed to allow “assembly in the head” (a mixture of high-level and low-level, platform-specific, programming); it is supported by a formally verified (certified in Coq), predictable, compiler which empowers programmers to write highly efficient fine-tuned code. The generated (verified) assembly code matches the performance of the best implementations for this primitive. Jasmin code can be proved correct and secure via an equivalence proof to a high-level specification in EasyCrypt: the Jasmin compiler is able to create an EasyCrypt translation of its source. End-to-end security and correctness follow from the certification of the Jasmin compiler (source-to-assembly) and from the EasyCrypt proof (source-to-spec).

Our experience using EasyCrypt and Jasmin [SoK] shows that both foundational and applied research are needed to tackle two classes of cryptographic protocols that are within our reach: 1) post-quantum cryptography (PQC) and 2) secure distributed (multiparty) computation. We now explain why this is the case.

PQC should not be confused with quantum computing or quantum cryptography; its goal is to create cryptographic schemes that can be used today and resist potential quantum attacks in the future. PQC relies on different maths abstractions and computational assumptions than classical crypto such as lattice-based [CRYS] and isogeny-based assumptions [SIKE]. These imply reasoning about distributions and complex maths objects for which little has been done in a machine-checking setting; indeed, proof techniques are still maturing in the cryptographic community to permit fine-tuning parameter sizes and improve performance. The majority of these proofs assume a quantum adversary interacting with a classical system, which can be formalized as an extension of the current EasyCrypt semantics, but this is currently lacking. Implementing these primitives also raises new challenges for the Jasmin framework; e.g., we have not yet considered rejection sampling mechanisms, which are crucial in PQC.

Orthogonal challenges arise in the verification of interactive protocols in Jasmin and EasyCrypt. Each cryptographic primitive is proved secure in a security model that captures its use in the real world. Primitives such as key exchange have been proved secure in a variety of models [KECR], with surprising complexity for two-party protocols: the goal is to capture concurrent executions and deal with composition within the security proof itself. General approaches to composability [UC] exist, but these exclude some of the more efficient instantiations, or require ad-hoc adaptations to capture the associated caveats.
Recent works [KMS,EUC,LMPC] have highlighted a mismatch between the security semantics of multiparty computation and the EasyCrypt framework. This is not surprising, as main use cases for EasyCrypt and the underlying Why3 backend are non-interactive primitives. What *is* surprising is that we can use EasyCrypt to reason about restricted classes of distributed protocols, such as those offering semi-honest security, or constant-round two-party computation [LMPC, EUC]. We have also explored more complex protocols [KMS], and identified the main bottlenecks: when the scheduling of executions becomes even moderately complex, the number of cases explodes and there is a large overhead in specifying and verifying global invariants by hand. These results point to new directions we explore in PRESTO; we stress the goal of obtaining verified proofs matching those written by cryptographers, rather than using a symbolic model (e.g., as in Tamarin or ProVerif), which are incomparable.

HACSpec [HACS] is a common specification language for cryptography that can be used by technical standards, software developers, and feed formal verification tools. Syntactically, HACSpec is a subset of Rust, and hence is familiar to developers; most importantly for standards, specifications are executable, they can be tested for correctness and interoperability, and to generate test vectors. HACSpec comes with a translator tool that can feed various formal verification frameworks. By using a common specification language, formal verification can be done by larger teams working on their tools of choice. At the moment, there is only a very simple proof of concept for generating EasyCrypt code. PRESTO will contribute to the HACSpec development and ensure that the extensions we make to EasyCrypt and Jasmin can have a greater impact via integration into the HACSpec tool-chain.

### 3.2.2. Plano e Métodos

3.2.2. Plan and Methods

PRESTO aims to progress beyond the SotA at both the foundational and applied research levels by 1) developing new extensions to the HACSpec, Jasmin and EasyCrypt/Why3 tool-chain and 2) demonstrating its applicability to concrete examples that can have real-world impact.

PRESTO will focus on concrete cryptographic constructions and implementations of PQC and secure distributed computation that can serve as inputs to standardisation or as contributions to widely deployed cryptographic libraries and software stacks. These use-cases are just outside the reach of existing CAC tool-chains, as described in the SotA analysis. In what follows, we explain the approach that we will adopt in PRESTO to change this state of affairs by working in the concrete setting of the HACSpec-Jasmin-EasyCrypt tool-chain to reduce scalability bottlenecks in the analysis of distributed cryptographic protocols and enable the transition to post-quantum cryptography.

The PRESTO technical work-plan is structured as four tasks:
T1: Integration and Interoperability with External Tools (M1-M36)
T2: Formal Reasoning About Secure Distributed Computation (M3-M30)
T3: Computer-Aided Post-Quantum Cryptography (M3-M30)
T4: Use-Case Implementation and Tool-Chain Validation (M1-M36)
We briefly outline the management structure at the end of this section and explain how it interacts with the technical activities.

We first give a summary of each task, and then explain the overall rationale.

T1: Integration and Interoperability with External Tools
The goal of this task is to ensure that PRESTO outputs are aligned with external initiatives. We will look to other tools and languages, so that the results we obtain can be compared and/or composed with results obtained in other tool-chains, namely those coexisting in the HACSpec ecosystem.
This task will guarantee the integration of EasyCrypt and Jasmin in the HACSpec framework, which we will use as a channel for compatibility/interoperability with external developments. We will start with legacy EasyCrypt/Jasmin code that needs to be updated and related to HACSpec specifications, and continue with new developments created in the project. We will also start a repository of developments to foster the creation of a community of users of these tools; this repository will promote the use of common APIs, such as those defined by SUPERCOP [SCOP] for drop-in implementations. The outputs of this task will ensure that the produced code is available for external use and has more potential impact. Dissemination will benefit from the guarantee that code artifacts come with a reproducibility and interoperability guarantee.

T2: Formal Reasoning About Secure Distributed Computation
In this task we will tackle the scalability challenges of verifying complex distributed protocols in EasyCrypt, which is based on program logics for reasoning about single programs. These challenges have been identified in prior work [KE, EUC, KMS]: 1) formalizing a communications and distributed execution model and 2) carrying out proofs that deal with an interactive system specified in one such model.
We will develop a set of libraries that capture common communications and distributed execution models. In EasyCrypt we will construct sound abstractions of the guarantees offered by these lower level protocols, which we will use in higher level proofs. EasyCrypt developments can be extracted to Why3 code; we will use Why3 to synthesize correct-by-construction OCaml code that calls verified Jasmin code or OCaml libraries when needed.
To deal with proof complexity, we will revisit existing EasyCrypt developments [KE, EUC, KMS], together with T1, investigate proof bottlenecks and solutions that were found to overcome them; we will also investigate the applicability of promising results such as state-separating proofs [SSP].
Ultimately, the goal is to explore the most successful design patterns to reduce proof effort: when possible, invariants on the global state that are trivially preserved should be discharged automatically or with minor user intervention.
Outputs will include extensions to the EasyCrypt-Why3 tool chain and associated libraries, as well as the foundational results that support them.

T3: Computer-Aided Post-Quantum Cryptography
In this task we will develop extensions to the Jasmin-EasyCrypt tool chain to address the security and correctness of PQC implementations. For concreteness, most of the effort will concentrate on the candidate submissions to the ongoing NIST competition.
Innovations will include EasyCrypt and Jasmin libraries with lacking data types, such as polynomials over rings and matrices and vectors thereof, and operators for dealing with distributions, rounding, low-norm values, etc.
We will also extend EasyCrypt to allow reasoning about attackers in possession of a quantum computer against crypto running classical computers; here we will leverage existing work both in the field of cryptography [PQRO,PQPR] and formal verification [PQEC]. This model is both relevant and a good target for our tools, as it allows maintaining backwards compatibility with the existing program logics.
Finally, we will look at PQC-specific proof techniques and potential automation support for dealing with parameter optimization.
Outputs will include extensions to the EasyCrypt-Jasmin tool chain and the foundational results and Jasmin implementations that support them.

T4: Use-Case Implementation and Tool-Chain Validation
In this task we will use the extended CAC tools developed in PRESTO in a number of use-cases. These use-cases will serve not only as a way to validate our results, but also as contributions of independent interest: 1) some artifacts will be contributions to standardization processes, by providing high-assurance security proofs and implementations of candidate constructions; 2) all implementations will be open-sourced as APIs that match third-party developments using SUPERCOP [SCOP] and/or HACSpec.
Use-cases will include NIST PQC candidates, and secure distributed computation protocols that will be used to test the extensions developed in T2 and T3, respectively. Moreover, we will also consider protocols that will require the extensions developed in *both* T2 and T3 to be used in an integrated manner.
Our ultimate goal is to construct end-to-end machine checked implementations, which are correct wrt a HACSpec specification, but we will progress to this goal by gradually building implementations, specifications and security proofs that are valuable contributions on their own. Outputs will include machine-checked proofs of security for each protocol, and functional correctness proofs for the implementations.

The rationale for the work plan above is as follows. T2 and T3 will concentrate efforts for each of the grand challenges that we propose to address. Task T4 will validate the results of T2 and T3, focusing on use-cases that will be contributions of independent interest. Moreover, T4 will guarantee that T2 and T3 must collaborate to provide one integrated tool-chain, by exploring use-cases that require both PQC and distributed protocol features. T1 serves as a connection to other CAC tool-chains, and to potential external consumers of the artifacts produced in PRESTO. T1 will make sure that what is produced by other tasks is compatible, comparable and inter-operable with external developments at both the specification and implementation levels. Task leaders have been assigned to each task, as described in the management structure; they will keep track of progress during the project duration and assist the PI with the necessary control and reporting activities.

The PRESTO team is built around a highly motivated and specialized group of researchers, that have long standing collaborations with the international teams developing the HACSpec, EasyCrypt, Why3 and Jasmin tools. Manuel Barbosa (PI) and José Almeida are experienced researchers with a strong track record of working in EasyCrypt and Jasmin, and integrate the team that proposed the Jasmin language. Jorge Pinto and Simão Sousa are experienced researchers with a strong background on program verification and long-standing collaboration with the developers of Why3. Mário Pereira (Co-PI) recently obtained his Ph.D. working in the Why3 development team, Hugo Pacheco has recently concluded a Post-Doc on the formalization of secure multiparty computation, and Bernardo Portela is an expert on distributed crypto protocols.

The HR are structured to have two full-time Ph.D. students, mostly dedicated to T2 and T3 (respectively) where the foundational challenges of the project are addressed. We structured the remaining HR as 8 tracks for young researchers, each track including an initiation grant for bachelors students and a research grant for masters students (1 track = 6 month BIC + 6 month BIL). Whenever possible we will try to attract candidates for BIL grants with a prior BIC grant in the project. Bachelors students will be assigned to small implementation projects in T1 and T4, whereas masters students will be uniformly distributed by all tasks. All researchers involved in the project are members of staff at state universities, which allows a smooth integration between grants and ongoing university education of grant holders, as required by FCT.

Finally, the management structure was planned to ensure a productive collaboration between the team members, who are based in three different University campi (Porto, Braga and

Caparica/Lisbon). We plan monthly remote meetings between PI, Co-PI and task leaders. We aim for an in-person meeting every three months. Three workshops will be organized during the project, once per year, and one at each of the locations. Workshops will include external consultants, long-term collaborators of PRESTO team-members, to guarantee that project activities are aligned with the work being done by international partners.

### 3.2.3. Tarefas
3.2.3. Tasks

**Lista de tarefas** (4)
Task list (4)

| **Designação da tarefa** | **Data de início** | **Data de fim** | **Duração** | **Pessoas * mês** |
|---|---|---|---|---|
| Task denomination | Start date | End date | Duration | Person * months |
| Integration and Interoperability with External Tools | 01-01-2022 | 31-12-2024 | 36 | 50,7 |

**Descrição da tarefa e Resultados Esperados**
Task description and Expected results

This task plays a dual role in the project: global consistency and long-term external availability. We will look outside of the project, to other tools and languages, to guarantee that our results can be compared and/or composed with those obtained in other tool-chains, namely those in the HACSpec effort.

Long-term compatibility has several aspects: 1) guaranteeing the integration of EasyCrypt and Jasmin in the HACSpec framework; 2) dealing with legacy EasyCrypt/Jasmin developments that need to be updated to current versions of the tools and connected to HACSpec specifications; and 3) creating a repository of developments that may foster the creation of a community of users. Achieving these goals implies interacting with all the other tasks, to propagate restrictions that may come from the outside, and to export produced artifacts.

Concretely, the following activities will be carried out:

- Integration into HACSpec. The PRESTO team will collaborate with the international team developing HACSpec by helping to further develop the specification language and creating new specifications that match the use cases developed in PRESTO. Additionally, EasyCrypt libraries will be developed to provide an axiomatic semantics of HACSpec in EasyCrypt, relating it to the EasyCrypt and Jasmin semantics, which will then allow proving correctness with respect to HACSpec specifications. The PRESTO team will also provide support in extending the HACSpec extraction mechanism to EasyCrypt, and guarantee support for this new back-end.

- A repository for artifacts. We will create a repository of Jasmin-EasyCrypt artifacts that will allow for two types of contributions: an archive of community uploads, from small libraries to large developments, that can serve as referenceable research outputs, similar to the Archive of Formal Proofs. A special mode to enable anonymity for double-blind reviews will also be considered. The archive will also promote the external integration of PRESTO artifacts. The goal here is very pragmatic: to combine the approach for common APIs and benchmarking of SUPERCOP [SCOP] in order to guarantee that implementations can serve as drop-in replacements for existing libraries, with the common specifications arising in HACSpec, which guarantees that implementations are providing comparable functionality and security.

- Legacy developments. Several existing EasyCrypt+Jasmin developments require maintenance to ensure they are up to date with the current tool versions. These developments will be useful in the future, and they should be connected to HACSpec specifications. For example, SHA-3 [SHA3] is used in many PQC schemes, the finite field implementations in Curve25519 [JASM] can be reused for other developments, and the abstractions created for the proof in [KMS] can be applied in other distributed protocols. A continuous activity during the project will guarantee that the new extensions to the EasyCrypt+Jasmin tool are backward compatible and, when needed, we will update and expand the existing results. These activities are also ideal for the integration of new students.

The project team is already collaborating in the HACSpec development and has a long-term close participation in the development of EasyCrypt/Why3 and Jasmin; this task is a natural extension of the collaboration with our international partners. We note that research projects are often exclusively focused on producing new artifacts for new publications, rather than ensuring interoperability or long-term availability. We believe that the type of outputs produced in this task are valuable to guarantee practical impact of our work. Moreover, this task will play a central role in feeding the dissemination activities for the project, by guaranteeing that code artifacts come with reproducibility and interoperability guarantees.

Attachment PRESTO_PM.pdf explains the persons*month value.

**Membros da equipa de investigação nesta tarefa**
Members of the research team in this task

(B) Bolsa 1; (B) Bolsa 13; (B) Bolsa 14; (B) Bolsa 5; (B) Bolsa 6; (B) Bolsa 8; (B) Bolsa 9; Bernardo Luís Fernandes Portela; Hugo José Pereira Pacheco; Jorge Miguel de Matos Sousa Pinto; José Carlos Bacelar Ferreira Junqueira de Almeida; Manuel Bernardo Martins Barbosa; Mário José Parreira Pereira; Simão Patrício Melo de Sousa;

| **Designação da tarefa** | **Data de início** | **Data de fim** | **Duração** | **Pessoas * mês** |
|---|---|---|---|---|
| Task denomination | Start date | End date | Duration | Person * months |
| Formal Reasoning About Secure Distributed Computation | 01-04-2022 | 30-06-2024 | 27 | 59,4 |

**Descrição da tarefa e Resultados Esperados**
Task description and Expected results

This task will tackle the scalability challenges in verifying complex distributed protocols in EasyCrypt, which is based on program logics for reasoning about single programs. These challenges have been identified in prior work [KE,EUC,KMS] and they can be seen as two sides of the same coin: 1) formalizing a communications and distributed execution model and 2) carrying out proofs that deal with an interactive system formalized over one such model. We will deal with these challenges as follows.

We will develop a set of libraries that capture common communications and distributed execution models such as point-to-point communications, broadcast communications, or public-bulletin boards. In EasyCrypt we will construct sound abstractions of the guarantees offered by the low level protocols that can be used in cryptographic security proofs. This work will provide the foundations on top of which to formalize the various communications and execution models used in cryptography for the use-cases in T4.

The libraries above will come with Jasmin and OCaml implementations, which can themselves be formally verified [OVR]. In Why3 we will deal with the integration of formal verification results constructed in different parts of the tool-chain: the EasyCrypt developments can be extracted to Why3 code; we will use the OCaml code generation functionalities in Why3 to synthethise correct-by-construction implementations that call verified Jasmin code or OCaml libraries when needed.

To deal with proof complexity, we will revisit existing developments and investigate proof bottlenecks and solutions that were found to overcome these difficulties. The goal is to identify design patterns that allow modularizing the proof effort and to provide libraries and tool automation to handle common transformations. A promising approach is that of state-separating proofs [SSProofs], which lays down the foundations for this kind of reasoning. Ultimately, the goal is to reduce the proof effort when proving equivalences (game hops) when one introduces a modification in a complex model that captures a full system execution; whenever possible, trivial invariants on the global state should be discharged automatically or with minor user intervention via annotations. The success of the approach very much depends on the way in which the communications and execution models are defined, and clearly cannot be achieved unless EasyCrypt provides native support for them. This is why we refer to the challenges addressed in this task as two sides of the same coin, and why they must be addressed in an integrated fashion.

The outputs of this task will include 1) a set of abstractions and design patterns for capturing the various kinds of security models used in interactive/distributed cryptographic protocols; 2) axiomatic semantics and automation that support reasoning about these models; and 3) verified libraries that can be used to instantiate the abstract execution models and achieve coordinated execution over unreliable communications networks. We note that all of these outputs should be compatible with the other extensions developed in the project, and they should not undermine the ability to express cryptographic proofs in a natural way.

The task team will include a full-time Ph.D. student. The PRESTO team at INESC TEC has a strong track record in formalizing the security proofs for complex cryptographic protocols in EasyCrypt and has long-term collaborations with the developers of the tool; to complement this expertise, the PRESTO team at NOVA ID bring in-depth know-how on program verification in Why3 and OCaml, and a long-term partnership with the developers (the co-PI is part of the Why3 development team and has extensive expertise in OCaml verification [OVR]).

Attachment PRESTO_PM.pdf explains the persons*month value.

**Membros da equipa de investigação nesta tarefa**
Members of the research team in this task

(B) Bolsa 1; (B) Bolsa 10; (B) Bolsa 2; (B) Bolsa 3; (B) Bolsa 8; Bernardo Luís Fernandes Portela; Hugo José Pereira Pacheco; Jorge Miguel de Matos Sousa Pinto; José Carlos Bacelar Ferreira Junqueira de Almeida; Manuel Bernardo Martins Barbosa; Mário José Parreira Pereira; Simão Patrício Melo de Sousa;

| **Designação da tarefa** | **Data de início** | **Data de fim** | **Duração** | **Pessoas * mês** |
|---|---|---|---|---|
| Task denomination | Start date | End date | Duration | Person * months |
| Computer-Aided Post-Quantum Cryptography | 01-04-2022 | 30-06-2024 | 27 | 58,2 |

**Descrição da tarefa e Resultados Esperados**
Task description and Expected results

In this task we will develop extensions to the Jasmin-EasyCrypt tool chain, so that it can be used to formally verify the security and correctness of state of the art post-quantum cryptography (PQC) implementations. For concreteness, most of our effort will concentrate on the candidate submissions to the ongoing NIST competition for PQC.
We have identified the following set of challenges at this level:

- To extend the EasyCrypt libraries with lacking data types and operators. To support the most efficient lattice-based schemes, we will need to cover polynomials over rings and finite fields, cyclotomic polynomials, matrices and vectors thereof. Important operations include the NTT transform, an analogue of the Fourier transform, norm computations, and sampling from non-uniform distributions, namely for dealing with low-norm noise. In parallel, Jasmin must be extended to deal with machine instructions that are sometimes used to optimize the implementations of these operations, namely (vectorized) floating point instructions.

- To develop new program logics to deal with quantum attackers. We will adopt the model where an attacker in possession of a quantum computer (say a large organization or a country) is trying to break cryptography implemented in classical computers. This model is particularly important for long-term security of data protected today. There is a growing number of results [PQPR,PQRO] in cryptography that extend classical constructions and generic transformations (e.g., those based on random oracles) to this setting, and some seminal work in formalizing some of these results [PQEC]. Our goal will be to distill these developments into extended EasyCrypt and Why3 logics, to enable the machine-checking of formal security proofs of some of the NIST candidates.

- To develop proof techniques and automation to deal with optimizations. PQC proofs are also challenging because they use aggressive parameter optimization in order to obtain a level of performance compatible with real-world use. This often implies adopting new proof techniques to improve the bounds, which deviate from the standard game-hopping approach. Two examples of this are the use of truncation and rounding to introduce noise and simultaneously compress public and secret keys. These techniques imply that schemes do not always work correctly, and it is necessary to perform intricate analysis of complex distributions to bound the probability of error. Similarly, improving bounds when adversaries interact with quantum random oracles and similar abstractions require reasoning about amortized bad event analysis, i.e., avoiding the use of coarse union bounds across potential occurrences when bounding the probability of a bad event.

The outputs of this task will feed task T4, where we will be tackling concrete use-cases of PQC schemes. All extensions to the program logics will need to be coordinated with the work done in task T3, so as to guarantee support for distributed PQC protocols such as key exchange and zero knowledge proofs. Finally, interaction with task T1 will guarantee that the extended tool-chain can be integrated into external developments.

The task team will include a full-time Ph.D. student. The PRESTO team at INESC TEC has a strong track record of working in machine-checked cryptography implementations. Mário Pereira (Co-PI) and Jorge Pinto will reinforce the expertise necessary to extend the program logics and, in particular, how to leverage the existing logics in Why3.

Attachment PRESTO_PM.pdf explains the persons*month value.

**Membros da equipa de investigação nesta tarefa**
Members of the research team in this task

(B) Bolsa 1; (B) Bolsa 11; (B) Bolsa 8; Bernardo Luís Fernandes Portela; Hugo José Pereira Pacheco; Jorge Miguel de Matos Sousa Pinto; José Carlos Bacelar Ferreira Junqueira de Almeida; Manuel Bernardo Martins Barbosa; Mário José Parreira Pereira; Simão Patrício Melo de Sousa;

| **Designação da tarefa** | **Data de início** | **Data de fim** | **Duração** | **Pessoas * mês** |
|---|---|---|---|---|
| Task denomination | Start date | End date | Duration | Person * months |
| Use Case Implementation and Tool-chain Validation | 01-01-2022 | 31-12-2024 | 36 | 57,9 |

**Descrição da tarefa e Resultados Esperados**
Task description and Expected results

In this task we will use the tools developed in PRESTO in a number of use-cases. These will serve not only as a way to validate our results, but also as contributions of independent interest: 1) some artifacts will support standardization by providing high-assurance security proofs and implementations of candidate constructions; 2) all implementations will be open-sourced as APIs that match third-party developments using SUPERCOP [SCOP] and/or HACSpec in coordination with task T1.

We do not give a closed set of target cryptography protocols, as these will be re-evaluated in the first 3 months of the project in light of the SotA. We provide likely choices for concreteness.

NIST PQC Candidates: the NIST competition is under the spotlight for PQC research, and contributions to this process have a high potential impact. We will look at Ring LWE-based constructions, such as CRYSTALS [CRYS], which provides a key exchange protocol Kyber and a signature Dilithium. Other constructions based on general lattices, namely Frodo KEM [FROD], and constructions based on Learning with Rounding such as SABER [SABE] pose similar challenges with some caveats, and may also be considered.
Our ultimate goal for these protocols is to construct end-to-end machine checked implementations, which are correct wrt a HACSpec specification, but we will progress to this goal by gradually building implementations, specifications and security proofs that are valuable contributions on their own.
On a more exploratory track, we will also look at hash-based construction SPHINCS (https://sphincs.org) and Isogeny-based SIKE [SIKE]; the former introduces new proof techniques for amortized bad event analysis and the latter is based on a new family of algebraic abstractions.

Practical MPC protocols: several secure multiparty computation protocols are being deployed in practice, which are analyzed in well-behaved communications models involving synchronous round-based execution and assuming authenticated channels. These protocols, which include for example the SPDZ [SPDZ] family and the Sharemind [SHRM] frameworks, are extremely efficient and hence are good candidates for implementation using Jasmin. They are also ideal use-cases for the validation of our work on distributed protocol verification, and in some cases also of our post-quantum features (homomorphic encryption from lattices is often used for preprocessing).

Interactive proofs: We will use interactive proofs to explore the application of our tool-chain to examples that jointly require reasoning about distributed protocols and post-quantum cryptography. We will look at zero-knowledge proofs offering post-quantum security, such as those resulting from the application of the MPC-in-the-Head transformation, and those developed as sub-components for some PQC signature schemes that use the Fiat-Shamir transformation. Indeed, generic transformations such as Fiat-Shamir and composition of interactive proofs are well suited as use-cases for the outputs of both tasks T2 and T3.

Connection to distributed ledger backbone: To further validate work carried out in T2, we will investigate cryptographic protocols that take advantage of a distributed ledger. There is a number of works trying to bridge the gap between blockchain-like protocols and higher level abstractions for PKI, public bulletin boards and timestamping, which could benefit from these use-cases. Concretely, we can consider MPC using public bulletin boards [PBB] and Single Secret Leader Election [SSLE]

This task will interact with all the other tasks wrt to validation, and it will interact with task T1 on the important goal of external interoperability. The PRESTO team has a strong track record of dealing with similar use-cases; the work in this task is ideally suited to create smaller self-contained spin-off projects that can be framed as masters dissertations and bachelors projects.

Attachment PRESTO_PM.pdf explains the persons*month value.

**Membros da equipa de investigação nesta tarefa**
Members of the research team in this task

(B) Bolsa 1; (B) Bolsa 12; (B) Bolsa 15; (B) Bolsa 16; (B) Bolsa 4; (B) Bolsa 7; (B) Bolsa 8; Hugo José Pereira Pacheco; Jorge Miguel de Matos Sousa Pinto; José Carlos Bacelar Ferreira Junqueira de Almeida; Manuel Bernardo Martins Barbosa; Mário José Parreira Pereira; Simão Patrício Melo de Sousa;

## 3.2.4. Calendarização e Gestão do Projeto

3.2.4. Project Timeline and Management

### 3.2.4.a Descrição da Estrutura de Gestão

3.2.4.a Description of the Management Structure

The project will be led by the PI (Manuel Barbosa) with support from the co-PI (Mário Pereira). Tasks are coordinated by different team members: T1 by Hugo Pacheco, T2 by the Co-PI, T3 by the PI and T4 by José Almeida. This task coordination assignment aims for the best combination of scientific expertise and skills, as well as individual motivation and commitment to the project. Note that all task coordinators are committing at least 25% of their time to the project. We believe this will be key for the success of PRESTO.

There will be monthly meetings between the PI, co-PI and the task coordinators to address planning issues, and ensure task integration. Meetings will occur mostly via web conference tools. Nonetheless, physical meetings are expected to happen every three months. During these meetings, PI and task leaders will discuss the progress of the ongoing task allocated thesis, as well as the strategies being followed towards achieving the expected scientific outcomes. The participants of these meetings will collaboratively write a cumulative progress report, which will help the PI to deliver the annual progress reports.

We propose to organize three annual workshops, each one happening by the end of a project year. The purpose of these workshops is to share the scientific progress amongst the different members of the project, as well as to discuss the best strategies to achieve next year’s milestones. The workshops will consist of a day-long run of scientific discussions and a small number of short scientific presentations.

We see this as an excellent opportunity to engage young students and researchers in the lifecycle of the project, hence we will make sure most of the talks are delivered by students. These workshops will also be used to publicise project results, as all talks will be open to the public. The PI will close each workshop by presenting a summary of the progress of the enclosing year. This will serve as the basis for the annual report.

The three workshops will be held at Braga (Y1), Lisbon/Caparica (Y2) and Porto (Y3).

Yearly workshops will be an important milestone in the project, since they will encourage further collaborations and will provide the team members with an external insight on the project development and implementation. Furthermore, we will use these workshops to interact in person with international collaborators: two external consultants will be invited for each workshop.

Finally, in order to mitigate physical distance, we will use remote collaboration tools (e.g., Slack) and versioning platforms such as github/gitlab. All team members have extensive experience with such platforms to manage and conduct remote research collaborations.

All our software will be open sourced.

### 3.2.4.b Lista de Milestones

3.2.4.b Milestone List

| **Data**<br>Date | **Designação da milestone**<br>Milestone denomination |
|---|---|
| 01-04-2022 | Project bootstrap completed |

**Descrição**
Description

Tasks T1 and T4 started in the beginning of the project and have prepared ground for the research work in tasks T2 and T3 to begin; in particular, the PRESTO team has produced HACSpec preliminary specifications and pinpointed the most relevant use-cases to guide the work.
PRESTO website online.

| **Data**<br>Date | **Designação da milestone**<br>Milestone denomination |
|---|---|
| 31-12-2022 | Year 1 completed: First extended tool-chain release. |

**Descrição**
Description

Activities planned for the first year have been completed and reported.
Legacy EasyCrypt and Jasmin developments intregrated into HACSpec and prototypes released.
First release of the extended HACSpec-EasyCrypt-Jasmin tools.
First versions of use-case formalisations and implementations available.

| **Data**<br>Date | **Designação da milestone**<br>Milestone denomination |
|---|---|
| 31-12-2023 | Year 2 completed: Second extended tool-chain release. |

**Descrição**
Description

Activities planned for the first two years have been completed and reported.
Repository of HACSpec-Jasmin-EasyCrypt artefacts available.
Second release of the extended HACSpec-EasyCrypt-Jasmin tools.
Use-case formalisations and implementations available.

| **Data**<br>Date | **Designação da milestone**<br>Milestone denomination |
|---|---|
| 30-06-2024 | Tool-chain completed |

**Descrição**
Description

Full HACSpec-EasyCrypt-Jasmin tool-chain with all extensions coming from T2 and T3.

| **Data**<br>Date | **Designação da milestone**<br>Milestone denomination |
|---|---|
| 31-12-2024 | Project terminates |

**Descrição**
Description

All project activities have been concluded and reported.

### 3.2.4.c Cronograma

3.2.4.c Timeline

*Ficheiro tipificado como "Cronograma", no 9. Ficheiros Anexos, desta Visão Global (caso exista).*
*File with "Timeline" type at 9. Attachments (if exists).*

## 3.3. Referências Bibliográficas

**3.3. Bibliographic References**

| **Nº de Ordem**<br>Order No. | **Referência**<br>Reference | **Ano**<br>Year | **Publicação**<br>Publication |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | [HACS] | 2018 | **K. Bhargavan, F. Kiefer, P.-Y. Strub:<br>HACSpec: Towards Verifiable Crypto Standards.<br>SSR 2018 and https://hacspec.github.io.** |
| 2 | [EC] | 2011 | **G. Barthe, B. Grégoire, S. Heraud, S. Zanella Béguelin:<br>Computer-Aided Security Proofs for the Working Cryptographer.<br>IACR CRYPTO 2011** |
| 3 | [NIST] | 2021 | **NIST Post Quantum Cryptography Competition** |
| 4 | [FSTR] | 2017 | **J. Protzenko, J. K. Zinzindohoué, A. Rastogi, T. Ramananandro, P. Wang, S. Zanella Béguelin, A. Delignat-Lavaud, C. Hritcu, K. Bhargavan, C. Fournet, N. Swamy:<br>Verified low-level programming embedded in F*.<br>ACM ICFP 2017.** |
| 5 | [FIAT] | 2019 | **A. Erbsen, J. Philipoom, J. Gross, R. Sloan, A. Chlipala:<br>Simple High-Level Code for Cryptographic Arithmetic - With Proofs, Without Compromises.<br>IEEE Symposium on Security and Privacy 2019** |
| 6 | [CVRF] | 2018 | **B. Blanchet:<br>Composition Theorems for CryptoVerif and Application to TLS 1.3.<br>IEEE CSF 2018.** |
| 7 | [SIGN] | 2017 | **N. Kobeissi, K. Bhargavan, B. Blanchet:<br>Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach.<br>Euro S&P 2017** |
| 8 | [TLS] | 2017 | **A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, J. Protzenko, A. Rastogi, N. Swamy, S. Zanella Béguelin, K. Bhargavan, J. Pan, J. K. Zinzindohoue:<br>Implementing and Proving the TLS 1.3 Record Layer.<br>IEEE Symposium on Security and Privacy 2017** |
| 9 | [HACL] | 2017 | **J. K. Zinzindohoué, K. Bhargavan, J. Protzenko, B. Beurdouche:<br>HACL*: A Verified Modern Cryptographic Library.<br>ACM CCS 2017** |
| 10 | [WHY3] | 2013 | **J.-C. Filliâtre, A. Paskevich:<br>Why3 - Where Programs Meet Provers.<br>ESOP 2013** |
| 11 | [EUC] | 2019 | **R. Canetti, A. Stoughton, M. Varia:<br>EasyUC: Using EasyCrypt to Mechanize Proofs of Universally Composable Security.<br>IEEE CSF 2019** |
| 12 | [MASK] | 2019 | **G. Barthe, S. Belaïd, G. Cassiers, P.-A. Fouque, B. Grégoire, F.-X. Standaert:<br>maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults.<br>ESORICS 2019** |
| 13 | [DIFP] | 2016 | **G. Barthe, N. Fong, M. Gaboardi, B. Grégoire, J. Hsu, P.-Y. Strub:<br>Advanced Probabilistic Couplings for Differential Privacy.<br>ACM CCS 2016** |
| 14 | [LMPC] | 2018 | **J. Almeida, M. Barbosa, G. Barthe, H. Pacheco, V. Pereira, B. Portela:<br>Enforcing Ideal-World Leakage Bounds in Real-World Secret Sharing MPC Frameworks.<br>IEEE CSF 2018** |
| 15 | [KE] | 2015 | **G. Barthe, J. M. Crespo, Y. Lakhnech, B. Schmidt:<br>Mind the Gap: Modular Machine-Checked Proofs of One-Round Key Exchange Protocols.<br>IACR EUROCRYPT 2015** |
| 16 | [SSP] | 2018 | **C. Brzuska, A. Delignat-Lavaud, C. Fournet, K. Kohbrok, M. Kohlweiss:<br>State Separation for Code-Based Game-Playing Proofs.<br>IACR ASIACRYPT 2018** |
| 17 | [PQRO] | 2011 | **D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, M. Zhandry:<br>Random Oracles in a Quantum World.<br>IACR ASIACRYPT 2011** |
| 18 | [PQPR] | 2013 | **D. Boneh, Mark Zhandry:<br>Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World.<br>IACR CRYPTO 2013** |
| 19 | [PQEC] | 2020 | **D. Unruh:<br>Post-Quantum Verification of Fujisaki-Okamoto.<br>IACR ASIACRYPT 2020** |
| 20 | [SCOP] | 2021 | **SUPERCOP: System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives** |
| 21 | [UC] | 2020 | **R. Canetti:<br>Universally Composable Security.<br>J. ACM 2020** |
| 22 | [KECR] | 2000 | **M. Bellare, D. Pointcheval, P. Rogaway:<br>Authenticated Key Exchange Secure against Dictionary Attacks.<br>IACR EUROCRYPT 2000** |
| 23 | [SPDZ] | 2020 | **M. Keller:<br>MP-SPDZ: A Versatile Framework for Multi-Party Computation.<br>ACM CCS 2020** |
| 24 | [SHRM] | 2008 | **D. Bogdanov, S. Laur, J. Willemson:<br>Sharemind: A Framework for Fast Privacy-Preserving Computations.<br>ESORICS 2008** |

| | | | |
|---|---|---|---|
| 25 | [PBB] | 2017 | **A. R. Choudhuri, M. Green, A. Jain, G. Kaptchuk, I. Miers:<br>Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards.<br>ACM CCS 2017** |
| 26 | [SSLE] | 2020 | **D. Boneh, S. Eskandarian, L. Hanzlik, N. Greco:<br>Single Secret Leader Election.<br>AFT 2020** |
| 27 | [CRYS] | 2021 | **CRYSTALS: Cryptographic Suite for Algebraic Lattices** |
| 28 | [SIKE] | 2021 | **SIKE: Supersingular Isogeny Key Encapsulation** |
| 29 | [SABE] | 2021 | **SABER: MLWR-based Key Encapsulation Mechanism** |
| 30 | [FROD] | 2021 | **FrodoKEM: Practical quantum-secure key encapsulation from generic lattices** |

### 3.4. Publicações Anteriores

3.4. Past Publications

| Nº de Ordem | Referência | Ano | Publicação |
|---|---|---|---|
| Order No. | Reference | Year | Publication |
| 1 | [SoK] | 2021 | **SoK: Computer-Aided Cryptography: M. Barbosa, G. Barthe, K. Bhargavan, B. Blanchet, C. Cremers, K. Liao, B. Parno IEEE Symposium on Security and Privacy 2021** |
| 2 | [OVR] | 2019 | **A. Charguéraud, J.-C. Filliâtre, C. Lourenço, Mário Pereira: GOSPEL - Providing OCaml with a Formal Specification Language. FM 2019** |
| 3 | [SHA3] | 2019 | **J. Almeida, C. Baritel-Ruet, M. Barbosa, G. Barthe, F. Dupressoir, B. Grégoire, V. Laporte, T. Oliveira, A. Stoughton, P.-Y. Strub: Machine-Checked Proofs for Cryptographic Standards: Indifferentiability of Sponge and Secure High-Assurance Implementations of SHA-3. ACM CCS 2019** |
| 4 | [KMS] | 2019 | **J. Almeida, M. Barbosa, G. Barthe, M. Campagna, E. Cohen, B. Grégoire, V. Pereira, B. Portela, P.-Y. Strub, S. Tasiran: A Machine-Checked Proof of Security for AWS Key Management Service. ACM CCS 2019** |
| 5 | [JASM] | 2017 | **J. Almeida, M. Barbosa, G. Barthe, A. Blot, B. Grégoire, V. Laporte, T. Oliveira, H. Pacheco, B. Schmidt, P.-Y. Strub: Jasmin: High-Assurance and High-Speed Cryptography ACM CCS 2017** |

## 4. Equipa de investigação

4. Research team

−

### 4.1 Lista de membros

4.1. Members list

| Nome | Função | Grau | Custos (€) | % de dedicação | CV nuclear | CV |
|---|---|---|---|---|---|---|
| Name | Role | Degree | Costs (€) | % of commitment | Core CV | |
| Manuel Barbosa | Inv. Responsável | - | 0,00 | 35 | ✓ | CIÊNCIAVITAE |
| Mário Pereira | Co-investigador Responsável | - | 0,00 | 35 | ✓ | CIÊNCIAVITAE |
| Bernardo Portela | Investigador | - | 0,00 | 25 | ✗ | CIÊNCIAVITAE |
| Hugo Pacheco | Investigador | - | 0,00 | 25 | ✗ | CIÊNCIAVITAE |
| JORGE PINTO | Investigador | - | 0,00 | 25 | ✗ | CIÊNCIAVITAE |
| José Almeida | Investigador | - | 0,00 | 25 | ✓ | CIÊNCIAVITAE |
| Simão Sousa | Investigador | - | 0,00 | 25 | ✓ | CIÊNCIAVITAE |

*(O curriculum vitae de cada membro da equipa está disponível clicando no nome correspondente)*

*(Curriculum vitae for each research team member is available by clicking on the corresponding name)*

**Total: 7**

### 4.2. Lista de membros a contratar durante a execução do projeto

4.2. Members list to hire during project"s execution

| Membro da equipa | Função | Duração | %tempo |
|---|---|---|---|
| Team member | Role | Duration | %time |
| (B) Bolsa 1 | Bolseiro | 36 | 100 |
| (B) Bolsa 10 | Bolseiro | 6 | 100 |
| (B) Bolsa 11 | Bolseiro | 6 | 100 |
| (B) Bolsa 12 | Bolseiro | 6 | 100 |
| (B) Bolsa 13 | Bolseiro | 6 | 100 |
| (B) Bolsa 14 | Bolseiro | 6 | 100 |
| (B) Bolsa 15 | Bolseiro | 6 | 100 |
| (B) Bolsa 16 | Bolseiro | 6 | 100 |
| (B) Bolsa 2 | Bolseiro | 6 | 100 |
| (B) Bolsa 3 | Bolseiro | 6 | 100 |
| (B) Bolsa 4 | Bolseiro | 6 | 100 |
| (B) Bolsa 5 | Bolseiro | 6 | 100 |
| (B) Bolsa 6 | Bolseiro | 6 | 100 |
| (B) Bolsa 7 | Bolseiro | 6 | 100 |
| (B) Bolsa 8 | Bolseiro | 36 | 100 |
| (B) Bolsa 9 | Bolseiro | 6 | 100 |

**Total: 16**

## 5. Outros projetos

5. Other projects

−

### 5.1. Projetos financiados

5.1. Funded projects

| Referência | Título | Estado |
|---|---|---|
| Reference | Title | Status |

**PTDC/CCI-INF/31698/2017** Em curso

*(Os detalhes de cada projetos estão disponíveis clicando na referência correspondente)*
*(Details for each project are available by clicking on the corresponding reference)*

**Total: 1**

### 5.2. Candidaturas similares
5.2. Similar applications

*(Sem Candidaturas Similares)*
*(No Similar applications)*

## 6. Indicadores previstos
6. Expected indicators

–

### Indicadores de realização previstos para o projeto
Expected output indicators

| **Descrição**<br>Description | **2021** | **2022** | **2023** | **2024** | **2025** | **Total** |
|---|---|---|---|---|---|---|
| **A - Publicações**<br>Publications | | | | | | |
| Livros<br>Books | 0 | 0 | 0 | 0 | 0 | **0** |
| Artigos em revistas internacionais<br>Papers in international journals | 0 | 0 | 0 | 2 | 0 | **2** |
| Artigos em revistas nacionais<br>Papers in national journals | 0 | 0 | 0 | 0 | 0 | **0** |
| **B - Comunicações**<br>Communications | | | | | | |
| Comunicações em encontros científicos internacionais<br>Communications in international meetings | 0 | 2 | 3 | 3 | 0 | **8** |
| Comunicações em encontros científicos nacionais<br>Communications in national meetings | 0 | 0 | 0 | 0 | 0 | **0** |
| **C - Relatórios**<br>Reports | 0 | 0 | 0 | 0 | 0 | **0** |
| **D - Organização de seminários e conferências**<br>Organization of seminars and conferences | 0 | 1 | 1 | 1 | 0 | **3** |
| **E - Formação avançada**<br>Advanced training | | | | | | |
| Teses de Doutoramento<br>PhD theses | 0 | 0 | 0 | 2 | 0 | **2** |
| Teses de Mestrado<br>Master theses | 0 | 2 | 2 | 3 | 0 | **7** |
| Outras<br>Others | 0 | 0 | 0 | 0 | 0 | **0** |
| **F - Modelos**<br>Models | 0 | 0 | 0 | 0 | 0 | **0** |
| **G - Aplicações computacionais**<br>Software | 0 | 0 | 0 | 0 | 0 | **0** |
| **H - Instalações piloto**<br>Pilot plants | 0 | 0 | 0 | 0 | 0 | **0** |
| **I - Protótipos laboratoriais**<br>Prototypes | 0 | 1 | 1 | 1 | 0 | **3** |
| **J - Patentes**<br>Patents | 0 | 0 | 0 | 0 | 0 | **0** |
| **L - Outros**<br>Other | | | | | | |
| | 0 | 0 | 0 | 0 | 0 | **0** |
| | 0 | 0 | 0 | 0 | 0 | **0** |
| | 0 | 0 | 0 | 0 | 0 | **0** |

### Acções de divulgação da actividade científica
Scientific activity spreading actions

We will release the PRESTO web site within the first 3 months. We will use it to provide continuous feedback on our progress to the community, disseminate our publications and prototypes, as well as making important announcements such as student and research hiring.

We will target audiences of younger students (high-school level) throughout the many already established scientific dissemination activities in Portugal. In particular, we will take advantage of the fact that European Researchers’ Night takes place both at Lisbon and Braga, as well as various Open Day activities in the various CS departments involved in the project. We will use such opportunities to explain to present and future CS students the need for reliable software, as well as motivational examples on why cryptographic protocols are of utmost importance in computational infrastructures.

Regarding academic dissemination, we aim to publish majoritarily in top teer international conferences, as is customary in our communities. Extended versions of conference papers will be published as journal articles by the end of the project.

The most relevant conferences for presenting the scientific results achieved during the project in the security and cryptography area are ACM CCS, IEEE S&P, USENIX Security, IACR CRYPTO, IACR EUROCRYPT, IACR PKC. On the programming languages side, we will aim for European Symposium on Programming (ESOP), International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), European Conference on Computer Systems (EuroSys), and International Symposium on Formal Methods (FM). Other top international venues include Symposium on Principle of Programming Languages (POPL), International Symposium on Principles of Distributed Computing (PODC) International Symposium on Reliable Distributed

Systems (SRDS), and International Conference on Programming Language Design and Implementation (PLDI). Furthermore, we will present the results of the project to college-level students in summer schools.

We will disseminate our results amongst industrial companies whose expertise is close to the subject of this project. Project members will disseminate PRESTO results using the HACS workshop (hacs-workshop.org), which promotes the interaction between researchers working in cryptography, programming languages and CAC with professionals working in the software industry, including giants such as Apple, Google, Microsoft, Amazon. (One of the initiatives stemming from the HACS workshops is the HACSpec language.) On a national level, we expect dissemination mainly via the VORTEX Co-Lab, in which both INESC TEC and NOVA are partners. VORTEX is a new collaborative laboratory with Altran/Capgemini, which focuses on the automotive and aerospace markets for technology transfer, where high-assurance software plays a crucial role. We attach an endorsement letter from VORTEX that explains the potential for technology transfer.

## 7. Orçamento
7. Budget

### Instituição Proponente
Principal Contractor

**Inesc Tec - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência**

| **Descrição**<br>Description | **2021** | **2022** | **2023** | **2024** | **2025** | **Total** |
|---|---|---|---|---|---|---|
| Recursos Humanos<br>Human resources | 0,00 | 23.828,28 | 27.225,00 | 29.564,16 | 0,00 | **80.617,44** |
| Missões<br>Missions | 0,00 | 1.500,00 | 2.500,00 | 1.500,00 | 0,00 | **5.500,00** |
| Subcontratos<br>Subcontract | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Registo de patentes<br>Patent registration | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Demonstração, Promoção e Divulgação<br>Demonstration, Promotion and Publication | 0,00 | 3.500,00 | 5.000,00 | 5.000,00 | 0,00 | **13.500,00** |
| Adaptação de edifícios e instalações<br>Adaptation of buildings and facilities | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Aquisição de Bens e Serviços<br>Service procurement and acquisitions | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Gastos gerais<br>Overheads | 0,00 | 9.457,07 | 8.681,25 | 9.016,04 | 0,00 | **27.154,36** |
| **TOTAL DESPESAS CORRENTES**<br>TOTAL CURRENT EXPENSES | **0,00** | **38.285,35** | **43.406,25** | **45.080,20** | **0,00** | **126.771,80** |
| Instrumentos e equipamento científico e técnico<br>Instruments and scientific and technical equipment | 0,00 | 9.000,00 | 0,00 | 0,00 | 0,00 | **9.000,00** |
| **Total** | **0,00** | **47.285,35** | **43.406,25** | **45.080,20** | **0,00** | **135.771,80** |

### Instituições Participantes
Participating Institutions

**NOVA.ID.FCT - Associação para a Inovação e Desenvolvimento da FCT**

| **Descrição**<br>Description | **2021** | **2022** | **2023** | **2024** | **2025** | **Total** |
|---|---|---|---|---|---|---|
| Recursos Humanos<br>Human resources | 0,00 | 18.092,40 | 27.225,00 | 26.167,44 | 0,00 | **71.484,84** |
| Missões<br>Missions | 0,00 | 1.500,00 | 1.500,00 | 1.500,00 | 0,00 | **4.500,00** |
| Subcontratos<br>Subcontract | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Registo de patentes<br>Patent registration | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Demonstração, Promoção e Divulgação<br>Demonstration, Promotion and Publication | 0,00 | 2.000,00 | 3.500,00 | 3.500,00 | 0,00 | **9.000,00** |
| Adaptação de edifícios e instalações<br>Adaptation of buildings and facilities | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Aquisição de Bens e Serviços<br>Service procurement and acquisitions | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Gastos gerais<br>Overheads | 0,00 | 6.898,10 | 8.056,25 | 7.791,86 | 0,00 | **22.746,21** |
| **TOTAL DESPESAS CORRENTES**<br>TOTAL CURRENT EXPENSES | **0,00** | **28.490,50** | **40.281,25** | **38.959,30** | **0,00** | **107.731,05** |
| Instrumentos e equipamento científico e técnico<br>Instruments and scientific and technical equipment | 0,00 | 6.000,00 | 0,00 | 0,00 | 0,00 | **6.000,00** |
| **Total** | **0,00** | **34.490,50** | **40.281,25** | **38.959,30** | **0,00** | **113.731,05** |

### Orçamento Global
Global budget

| **Descrição**<br>Description | **2021** | **2022** | **2023** | **2024** | **2025** | **Total** |
|---|---|---|---|---|---|---|
| Recursos Humanos | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Human resources | 0,00 | 41.920,68 | 54.450,00 | 55.731,60 | 0,00 | **152.102,28** |
| Missões<br>Missions | 0,00 | 3.000,00 | 4.000,00 | 3.000,00 | 0,00 | **10.000,00** |
| Subcontratos<br>Subcontract | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Registo de patentes<br>Patent registration | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Demonstração, Promoção e Divulgação<br>Demonstration, Promotion and Publication | 0,00 | 5.500,00 | 8.500,00 | 8.500,00 | 0,00 | **22.500,00** |
| Adaptação de edifícios e instalações<br>Adaptation of buildings and facilities | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Aquisição de Bens e Serviços<br>Service procurement and acquisitions | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Gastos gerais<br>Overheads | 0,00 | 16.355,17 | 16.737,50 | 16.807,90 | 0,00 | **49.900,57** |
| **TOTAL DESPESAS CORRENTES**<br>TOTAL CURRENT EXPENSES | **0,00** | **66.775,85** | **83.687,50** | **84.039,50** | **0,00** | **234.502,85** |
| Instrumentos e equipamento científico e técnico<br>Instruments and scientific and technical equipment | 0,00 | 15.000,00 | 0,00 | 0,00 | 0,00 | **15.000,00** |
| **Total** | **0,00** | **81.775,85** | **83.687,50** | **84.039,50** | **0,00** | **249.502,85** |

### Plano de financiamento

Finance plan

| **Descrição**<br>Description | **2021** | **2022** | **2023** | **2024** | **2025** | **Total** |
|---|---|---|---|---|---|---|
| Financiamento solicitado à FCT<br>Requested funding | 0,00 | 81.775,85 | 83.687,50 | 84.039,50 | 0,00 | **249.502,85** |
| Financiamento próprio<br>Own funding | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Outro financiamento público<br>Other public-sector funding | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| Outro financiamento privado<br>Other private funding | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | **0,00** |
| **Total do Projecto**<br>Total of the project | **0,00** | **81.775,85** | **83.687,50** | **84.039,50** | **0,00** | **249.502,85** |

## 8. Justificação do orçamento

8. Budget rationale

–

### 8.1. Justificação dos recursos humanos

8.1. Human resources rationale

| | | |
|---|---|---|
| **Tipo**<br>Type | | **Nº de pessoas**<br>No. of persons |
| (B) Bolsa | | 1 |
| **Duração (em meses)**<br>Duration (in months) | **Custo envolvido (€) *(calculado)***<br>Total cost (€) *(estimated)* | **Outros custos (€)**<br>Other costs (€) |
| 36 | 38.687,04 | 5.400,00 |

**Justificação do financiamento solicitado**

Rationale for requested funding

This grant will support a full-time Ph.D. student (BIM) during the entire duration of the project, working at NOVA ID.
Most of the effort (75%) will be dedicated to T2, working on distributed cryptographic protocols.
The remaining 25% are split by the other tasks as follows: T1 => 10%, T3 => 10% and T4 => 5%.

| | | |
|---|---|---|
| **Tipo**<br>Type | | **Nº de pessoas**<br>No. of persons |
| (B) Bolsa | | 3 |
| **Duração (em meses)**<br>Duration (in months) | **Custo envolvido (€) *(calculado)***<br>Total cost (€) *(estimated)* | **Outros custos (€)**<br>Other costs (€) |
| 6 | 14.507,64 | 2.700,00 |

**Justificação do financiamento solicitado**

Rationale for requested funding

Three grants for Masters students (BIL) working at NOVA ID. Two of these Masters Students will work in Task 2 and one in Task 4.

| | | |
|---|---|---|
| **Tipo**<br>Type | | **Nº de pessoas**<br>No. of persons |
| (B) Bolsa | | 3 |
| **Duração (em meses)**<br>Duration (in months) | **Custo envolvido (€) *(calculado)***<br>Total cost (€) *(estimated)* | **Outros custos (€)**<br>Other costs (€) |
| 6 | 7.490,16 | 2.700,00 |

**Justificação do financiamento solicitado**

Rationale for requested funding

Three grants for Bachelor's (BIC) students working at NOVA ID. One of these grants will be dedicated to Task 4, and the remaining two to Task 1.

| | | |
|---|---|---|
| **Tipo**<br>Type | | **Nº de pessoas**<br>No. of persons |
| (B) Bolsa | | 1 |
| **Duração (em meses)**<br>Duration (in months) | **Custo envolvido (€) *(calculado)***<br>Total cost (€) *(estimated)* | **Outros custos (€)**<br>Other costs (€) |
| 36 | 38.687,04 | 5.400,00 |

**Justificação do financiamento solicitado**

Rationale for requested funding

This grant will support a full-time Ph.D. student (BIM) during the entire duration of the project, working at NOVA ID.
Most of the effort (75%) will be dedicated to T3, working on post-quantum cryptography.
The remaining 25% are split by the other tasks as follows: T1 => 10%, T2 => 10% and T4 => 5%.

| | | |
|---|---|---|
| **Tipo**<br>Type<br>(B) Bolsa | | **Nº de pessoas**<br>No. of persons<br>4 |
| **Duração (em meses)**<br>Duration (in months)<br>6 | **Custo envolvido (€)** ***(calculado)***<br>Total cost (€) *(estimated)*<br>19.343,52 | **Outros custos (€)**<br>Other costs (€)<br>3.600,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

Four grants for Masters students (BIL) working at INESC TEC. One grant per project task.

| | | |
|---|---|---|
| **Tipo**<br>Type<br>(B) Bolsa | | **Nº de pessoas**<br>No. of persons<br>4 |
| **Duração (em meses)**<br>Duration (in months)<br>6 | **Custo envolvido (€)** ***(calculado)***<br>Total cost (€) *(estimated)*<br>9.986,88 | **Outros custos (€)**<br>Other costs (€)<br>3.600,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

Four grants for Bachelors students (BIC) working in Tasks 1 and 4 (2 per task) at INESC TEC.

## 8.2. Justificação de missões

8.2. Missions rationale

| **Designação**<br>Designation | **Custo envolvido (€)**<br>Cost (€) |
|---|---|
| Visits to/by external advisors | 10.000,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

Throughout the project we foresee at least 10 visits to/by external advisors. Often such visits are co-sponsored, so an average cost of 1000EUR per visit (all in Europe) is a conservative estimate.

We include as an attachment to this proposal a short justification for including the following international researchers as consultants in the PRESTO project: Gilles Barthe, Jean-Christophe Filliatre, Pierre-Yves Strub, Benjamin Grégoire, Peter Schwabe and Karthikeyan Bhargavan. All consultants agreed to this, and most were able to provide support letters, which are attached to this process.

## 8.3. Justificação de aquisição de bens e serviços

8.3. Service procurement and acquisitions

*(Vazio)*
*(Void)*

## 8.4. Justificação do Equipamento

8.4. Equipment rationale

### 8.4.1. Equipamento já disponível para a execução do projecto

8.4.1 Available equipment

*(Vazio)*
*(Void)*

### 8.4.2. Discriminação do equipamento a adquirir

8.4.2. New equipment requested

| **Tipo de equipamento**<br>Equipment type | **Custo (€)**<br>Cost (€) |
|---|---|
| Laptops and workstations for project team | 15.000,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

In the first year of the project we will require 5 high-performance laptops for the 2 PhD students and 3 senior researchers who need to renew their personal machines. Estimated average cost per laptop is 3000EUR. We note that the processing power required to run the tools we work with, namely SMT solvers, can be significant.

## 8.5. Justificação de registo de patentes

8.5. Patent registration

*(Vazio)*
*(Void)*

## 8.6. Justificação de adaptação de edifícios e instalações

8.6. Adaptation of buildings and facilities

*(Vazio)*
*(Void)*

## 8.7. Justificação Subcontratos

8.7. Subcontract

*(Vazio)*
*(Void)*

## 8.8. Justificação Demonstração, Promoção e Divulgação

8.8. Demonstration, Promotion and Publication

| **Tipo**<br>Type | **Custo (€)**<br>Cost (€) |
|---|---|
| Open Access Publications | 4.500,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

For publications that justify it, due to their potential impact, we reserve 4500 EUR for Open Access costs.

| | |
|---|---|
| **Tipo**<br>Type | **Custo (€)**<br>Cost (€) |
| Workshop coffee breaks | 1.000,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

A small amount for coffee-breaks during the anual workshops.

| | |
|---|---|
| **Tipo**<br>Type | **Custo (€)**<br>Cost (€) |
| Conferences amd workshops overseas (US, ASIA) | 8.000,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

We foresee 4 trips to conferences and workshops outside of Europe at a rate of 2000EUR each.

| | |
|---|---|
| **Tipo**<br>Type | **Custo (€)**<br>Cost (€) |
| Conferences and workshops in Europe | 9.000,00 |

**Justificação do financiamento solicitado**
Rationale for requested funding

We foresee 4 trips to conferences and workshops in Europe, at a cost of 1500EUR each.

## 9. Ficheiros Anexos

9. Attachments

−

| Nome<br>Name | Tipo<br>Type | Tamanho<br>Size |
|---|---|---|
| **CONSULTANTS.pdf** | Outros<br>Others | 78KB |
| **PRESTO_PM.pdf** | Outros<br>Others | 42KB |
| **SUPPORT_BG.pdf** | Outros<br>Others | 122KB |
| **SUPPORT_GB.pdf** | Outros<br>Others | 447KB |
| **SUPPORT_JCF.pdf** | Outros<br>Others | 253KB |
| **SUPPORT_PS.pdf** | Outros<br>Others | 392KB |
| **SUPPORT_PY.pdf** | Outros<br>Others | 59KB |
| **SUPPORT_VORTEX.pdf** | Outros<br>Others | 399KB |
| **timeline.pdf** | Cronograma<br>Timeline | 116KB |

09-03-2021 19:03:01

REPÚBLICA PORTUGUESA | CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR