DigiCosme

2018 ***Update Project***

2. PROJECT DESCRIPTION AND EXPECTED IMPACT

2.1. SCIENTIFIC SCOPE AND CONTENTS OF THE PROJECT FOR THE NEXT FINANCING PERIOD, EXPECTED IMPACT

The digital revolution impacts nearly all aspects of our lives, in all sectors, and the economic impact of IST in all sectors is ever growing. In this context, societal challenges such as E-health, cybersecurity, smart mobility, industry of the future, to name but a few, require to study and develop a new generation of tools in IST. Even though DigiCosme does not cover the whole IST field, our work may have a significant impact on these challenges. The goal of Labex DigiCosme is therefore to contribute methodological and applied research to define networks, models, algorithms and programs with an increased number of capabilities and guarantees that will serve as the necessary basis for a trusted and useful digital society.

DigiCosme holds a privileged position to make relevant contributions as none of these issues can be efficiently solved by as single approach or technology, but on the contrary requires the combination of a wide range of tools coming from different subfields of IST. As an example, some of the crucial properties that networks and software should possess are security and reliability. Undoubtedly, some progress towards these targets has been already achieved by formal methods and cryptography, as witnessed by the first outcomes of the Labex. However, other contributions now come from information theory, machine learning and data protection method. Proposing a global understanding of solutions to such problems therefore seems a good target for the Labex.

More globally, new generations of systems tend to be more “intelligent”, pushed by recent advances in machine learning and in data and knowledge management that have increased expectations for “smart” systems. However, crucial properties are still open research areas: (i) The ubiquity of connected devices with their massive datasets calls for efficient, reliable transmission and exploitation tools; (ii) Many critical applications call for transparent, interpretable / explainable decision systems; (iii) Many applications need user expertise, therefore requiring to extract knowledge and insights from the activity of these systems. All these research areas should be addressed through strong cooperation between teams belonging to the three DigiCosme axis.

In the DigiCosme extension, emerging applications such as cybersecurity, e-health, smart cities, industry 4.0, e-sciences and life sciences will serve as guidelines for proposing topics where teams from the three axes will combine their knowledge in order to provide appropriate answers. In other words, after the promotion of cooperation among teams within each axis, we will enforce cooperation between axes, which will take full advantage from the wide knowledge of the DigiCosme community to propose innovative algorithms and methods. This cooperation will be enforced by Transversal Initiatives, a new research action involving teams from at least two axes. Moreover, in order to meet our scientific objectives, we will also enlarge the current perimeter of the labex by including more researchers from algorithmics and optimization in a broad sense, as well as from life science applications.

DigiCosme will also emphasize Reproducible Science by encouraging all projects to fulfill the standards of reproducible research with a special attention to the dissemination of software libraries at the international level.

SCILEX axis: Software Reliability and Security

The Scilex axis aims at providing robust tools and methods for delivering strong software reliability and security guarantees. This requires to express and prove properties at all conception levels: models, algorithms, programs, systems and execution environments, as well as the transversal issue of security. While formal methods (in their broadest sense) and security are at the core of Scilex, this renewal allows us to expand towards surrounding communities, namely algorithmics, control and high-performance computing, to tackle transversal challenges such as bio-informatics or dynamical systems. More precisely, the objective of this axis is to provide fundamental methods for proving properties about sequential, concurrent or distributed programs. This objective is articulated around five topics according to the level at which the properties are expressed. How to define models and their properties and how to prove them is addressed first. Then, properties of algorithms, including high-performance computing ones, and computation theories issues are described. Devices that involve both physical (continuous) components and software (discrete) control are then studied. Next, verification and validation techniques for programs are described. Finally, we focus on providing guarantees on the security and privacy of communications and applications regardless of their execution environment.

Properties of Models: The definition of models and their properties, as well as techniques for proving them, covers a wide range of formal methods. We aim at improving and combining both automatic and interactive modeling techniques such as model checking, abstract interpretation, deductive verification or the use of proof assistants. We will design new modeling languages or axiomatized models, study their expressive power and properties, the decidability of certain classes of problems (such as reachability), and develop efficient verification algorithms.

Properties of Algorithms: Regarding algorithm design and related computation theory issues, we will develop suitable models of computation assuming continuous or discrete time with centralized, concurrent, or distributed control. Tractable problems are given exact complexity bounds (in time, space or energy). Intractable problems are quantified and weakened towards tractability. For optimization or in a distributed setting, we prove convergence and quantify the quality of the reached equilibrium. Regarding high-performance computing, we aim at developing efficient algorithms (in scientific computing or data analytics) for the upcoming Exascale supercomputers. The main topics studied are: optimal performance on heterogeneous CPU-GPU systems, fault-tolerance in algorithms, minimal energy consumption, mixed-precision, and (new) quantum computing. This topic is now attracting new researchers from the various Algorithmics teams on the site. Note that the theoretical aspects of optimization algorithms linked to machine learning will be studied in connection with IID axis.

Properties of Dynamical Systems: We will also focus on dynamical systems that may be modeled by discrete-time parts, such as finite-state machines or software which may be distributed over a network, by continuous-time parts, such as differential equations defining the physical part of the system, or by both parts with strong interactions. This setting includes real-time systems, hybrid systems, biological systems and control-command systems. We aim at guaranteeing and proving the functional properties of the system such as: accuracy, robustness, resilience and performance.

Properties of Programs: There are many program properties to be certified, such as absence of errors, good behavior or numerical quality, for which we rely on many techniques: refinement, theorem proving, model-checking, static analysis by deductive verification or abstract interpretation, stochastic or static error analysis, runtime verification, testing, and so on. We aim both at improving these techniques and at making them cooperate across program types, properties, and languages. This know-how could possibly be propagated to other subfields of IST such as machine learning programs with a new collaboration with the IID axis.

Security Properties: We want to strengthen practical and theoretical knowledge in fundamental cryptology, either leveraging mathematical primitives or assessing those with cryptanalysis, while taking into account more demanding security models and more complex features. To create digital trust, we want to tackle security and privacy issues related to infrastructures and personal data handling in environments such as cloud computing, embedded systems, the Internet of Things, blockchain technologies and quantum technologies, in collaboration with Comex. We will also rely on formal methods to rigorously prove many properties at different levels.

Smart Networks Axis

We are entering a world integrating a variety of "things" connected to the Internet and outfitted with expanded digital features to create a true Internet of Everything. Many sectors, including manufacturing, transportation, utilities, energy management, healthcare, or automotive will be impacted in the coming years. At the same time, network operators are extending their business models to provide contents (video, music…) and services (storage, processing, localization…) with higher added-value compared to "simple" data forwarding. Networks need to evolve, not only to cope with increased traffic, but also to address new services with heterogeneous characteristics and demands that are being developed or will emerge soon. To face these challenges, novel architectures that can cope with high heterogeneity of applications are needed. This evolution leads to several open challenges about network architecture and management.

- Developing **service-aware communication protocols and network architectures**, to cope with a wide variety of requirements not only in terms of data rate, latency, energy consumption and complexity, but also in terms of application aware criteria. Multi-Access Edge Computing, which will bring intelligence to the edge of the network along with higher processing and storage capabilities, as well as Network Function Virtualization (NFV) and Software Defined Network (SDN) will be tools of choice to design such architectures. Their interaction requires addressing many crucial challenges at the core network and at the edge nodes (resource allocation, network connectivity, scalability, energy efficiency), as well as analysis of contextual and societal impact.
- Designing **intelligent network management** mechanisms to efficiently control these novel architectures. The goal is to effectively improve network resource usage, energy efficiency, scalability, as well as Quality of Experience (QoE). These mechanisms should be able to learn from past experience. All involved partners have a large experience in optimization, Markov Decision Process, game theory, or reinforcement learning. We need to further expand these methods to analyze and anticipate traffic load variations and service demands in general. Artificial Intelligence can have a large impact here. To answer these two challenging network evolutions, several directions will be investigated:

1- Efficiently exploiting the variety of resources (technologies, cell size and bandwidth -sub-6GHz, mmWave, etc.-) and the various ways of accessing them (optimal preprocessing, decoding, and resource allocation) depending on the situation (open/closed loop, full/partial/statistical CSI, complexity ability, MIMO or massive MIMO…)

2- Performing traffic engineering and network slicing at core network by benefitting from the multiple technologies provided by the 5G access cloud to adapt to all sorts of backhaul links in order to realize more flexible deployment and efficient radio resource management.

3- Lowering energy consumption by the infrastructure while ensuring QoE, e.g., by a joint optimization of spectrum sensing, spectrum aggregation and access with Game Theory.

4- Addressing new security and privacy issues raised by IoT applications such as crowdsensing as well as by flexible network management using slicing. For that purpose, we will leverage insights provided by information theory on physical-layer security, network coding and lattice coding,

5- Developing and integrating quantum communication technologies that can act as a physical-layer security anchor for the digital infrastructure. We will study and demonstrate the convergence and coexistence of quantum and classical communications on modern telecommunication networks.

6- Increasing network capacity by leveraging the improvements in optical fiber communication using more spatial parallel channels through wavelengths, polarization, modes and cores. Mitigating non-linear effects, especially by the new tool of Nonlinear Fourier transform and by using involved decision-feedback receivers, is also a challenging but promising direction.

7- Participating in the development of URLLC (Ultra Reliable Low Latency Communication), which will be of paramount importance in the context of intelligent vehicular (terrestrial or aerial) networks. Such networks can leverage 5G networks to process and mine data in real time. Coding schemes for very short packets containing vehicular measurements or control information have to be designed. Joint source-channel coding schemes may also limit the latency in this context.

This research will help to grasp the theory of intelligent and resource efficient wireless networks and develop relevant key mechanisms and algorithms. All recent progress in the various dimensions of Artificial Intelligence will be useful and security / reliability issues will be addressed with Scilex.

Intelligence, Interaction, Data (IID) Axis (formerly DATASENSE)

The availability of massive datasets, large computing and storage resources with the recent advances in machine learning now make it possible to resolve hitherto unaffordable issues. The design of intelligent systems is one of the most essential ones. We will focus on **machine learning**, **natural language processing**, **data and knowledge management, knowledge representation** to represent, process and interpret data and knowledge, in connection with human users through **human-computer interaction**. The design of intelligent systems conveys an additional degree of complexity: it aims at building end-to-end solutions, i.e. to compose individual steps into **workflows** that meet the constraints and priorities of the application, be they soundness, reproducibility, robustness, reliability, explainability, privacy preservation in addition to performance. Operational intelligent systems should use background knowledge, cope with various data quantity and quality, and adapt over time. **Visualisation methods and human-machine interaction** are critical means to ensure the effective usability of such systems.

Machine learning. Current challenges concern the development of richer, **more expressive models** —aka deep learning— that leverage the complexity of large-scale data. Ensuring an efficient learning on the available computational architectures and a seamless composition of such models remain open questions. In data-rich settings, abstractions can be learned from data, leading to **end-to-end learning** frameworks, where learning procedures handle the full data processing. Real-life learning systems are operated in open-loop mode, a setting also called continuous or lifelong learning. The counterpart of enhanced expressivity is the instability of learning systems that are subject to overfitting and sensitiveness to biases; ensuring **robustness** in learning is thus a major endeavour. The **performance characterization** of such systems is a fundamental question, that we will address with concepts borrowed from information theory in collaboration with COMEX and SCILEX. Beyond reliability, learning systems should provide **interpretable and explainable models**, enabling users to understand the reasons of an outcome: a pending challenge here is the **causal structure** inherent to complex data. Solutions to these problems are expected at the cross-road of machine learning and symbolic artificial intelligence. **Computer vision** and **machine listening** will provide a favorable ground to combine high level, symbolic representations and reasoning with machine learning. Applications to E-health and life science, fields where interpretability matters equally as performance, will be targeted.

Data also come with limitations: missing data, heterogeneity and more generally, **dirty data**, are not handled by most standard procedures. In the **weak data limit**, generalization to unseen categories (aka zero-shot learning) is actually needed. Transfer learning and semi-supervised learning will be developed, as well as representation learning in this context. Finally, the reliance on existing knowledge bases is a mean to deal with data shortage.

Optimization. Any learning problem ends up as a minimization procedure. Optimization is mostly concerned with accuracy, computational efficiency, and robustness while machine learning focuses on achieving efficiency via possibly simpler formulations that are computationally efficient and scalable for a well-defined class of instances. We wish to push forward the interaction between these two domains, especially in the perspective of problems constrained by resource (memory, energy consumption) or by properties (transparency, interpretability, privacy, bias-free). **Distributed optimization** is now a pervasive topic that has gained importance within the DigiCosme perimeter. **Discrete optimization** and mixed approaches will help to re-visit unsolved problems.

Data management, knowledge representation and reasoning. Data understanding involves to deal with highly heterogeneous data (text, relational, graphs, streams), from various domains (life sciences, astronomy, culture) and with knowledge encoded through many formalisms (graphs, ontologies, linked open data). Challenges to be tackled by DigiCosme are data integration, knowledge acquisition, data and knowledge **reconciliation**, data **quality** assessment. Our originality will lie in combining techniques from **graph and database theories,** NLP, data mining, machine learning, knowledge representation (based on logics, ontologies, …), and reasoning. Collaborations with SCILEX (formal methods) and COMEX (information theory) are key to our approaches.

Human Computer interaction. A number of important issues for interaction and visualization are raised by the recent explosion of ML techniques. This topic will strengthen the fruitful **synergy with the DIGISCOPE** Equipex and develop research on collaborative interaction and visualization within and across large interactive rooms. Challenges include (i) designing better visualization tools to help understand how such systems work and contribute to the transparency and accountability of (machine-learning) algorithms; (ii) designing interaction modalities for robots and intelligent systems that strike a balance between mimicking human-human communication and augmenting human capabilities through the power of computation; (iii) developing interaction modalities that leverage **emotional channels** between humans and machines (or between humans via machines). Collaboration with COMEX and SCILEX are again key aspects of our future approaches, to better take into account human needs in future computer systems. Examples include combining human-centered design with secure-by-design approaches, using the tools of Information Theory to model, design and evaluate interactive techniques, adapting ML techniques to work in interactive time and be robust even with scarce examples, opening new possibilities for gesture-based and full body real-time interactions (e.g. for creative professionals).

Natural Language Processing (NLP). Natural Language Processing (NLP) designs algorithms for accessing knowledge conveyed by unstructured, heterogeneous texts and for language-mediated human-machine communication. Building up on the very active community in this field, we aim at creating NLP algorithms that can **process and produce language in its context**, in all its modalities (**spoken**, **written**, and **signed**), take advantage of **both linguistic and domain knowledge**, draw **inferences** when extracting knowledge from language input, and **explain** themselves, in a **robust**, **scalable** way. NLP combines many challenges from data, knowledge, machine learning, and human interaction. We will explore promising joint research opportunities with Machine Learning (e.g., distributional representations), Data and Knowledge (information extraction, ontology construction and use, entity linking), and Human-Computer Interaction (chatbots).

Implementation of the research program

We will continue some of the actions that worked well in the past and introduce new ones in our bi-annual call for projects. Among the planned activities, some will remain “bottom-up” to promote creativity and encourage new research topics. As before, funding for Ph.D. theses will only require to involve at least two researchers from different laboratories and to focus on one of the topics of the axes. The Working Groups will remain a privileged instrument of scientific strategy with a fast-track call for creation and renewal. They will be selected according to the forces present in the site and their importance regarding the challenges of Digital Revolution.

We will introduce a new action, called Transversal Initiative, in order to promote collaborations among researchers of different axes on hot topics. In fact, DigiCosme is the only instrument on the campus IST ecosystem to have the ability to make subfields of IST cross-fertilize. We will not provide a closed list of potential topics for these TI actions. For examples, one can cite “reliability of machine learning algorithms”, “artificial intelligence for smart networks” , “security of systems through natural language interactions”, …This TI action will involve at least two research teams in different axes as well as two laboratories. It will be endowed with a substantial funding corresponding to two Ph.D. theses and a one-year post-doc to provide the necessary impulse for the collaboration. Existing teams as well as new incoming researchers will be welcome for these actions. To ensure the success of these actions and their mid-term effects, we will define a specific accompaniment program (see paragraph in 3.1) to monitor them. To promote such projects, the call for Working Groups will encourage Transversal Working groups that could foreshadow the definition of a Transversal Initiative.

Education project

Considering the results of this first step of DigiCosme, we consider that existing education instruments are successful and efficient and we propose to continue them.

Links with other PIA tools

On targeted topics such as the development of tools for privacy-preserving, transparent and secure intelligent systems, it is planned to cooperate with DATAIA to rapidly develop new competencies on the site. In Artificial intelligence, the actions of DATAIA (projects at the interface of social sciences and IST/mathematics) and DigiCosme (e.g. Transversal Initiatives) differ in their spirit but can be complementary. Joint actions with the Labex LHM or other Labex will continue to be organized.